EDITAL DE LICITAÇÃO

PREGÃO SESC/DR/AP Nº 24/0035-PG

O **SERVIÇO SOCIAL DO COMÉRCIO – SESC,** Administração Regional no Estado do Amapá, Pessoa Jurídica de direito privado, inscrito no CNPJ/MF sob o nº 03.593.251/0001-15, com sede na Rua Jovino Dinoá, nº 4311, Bairro Beirol, Macapá – AP, CEP 68.902-030, por intermédio de sua Comissão Permanente de Licitações, constituída pela Portaria n° 0120/2024, datada de 17 de julho de 2024, torna público, para ciência dos interessados, que, por mediação de seu pregoeiro, realizará licitação na modalidade **PREGÃO**, formato **ELETRÔNICO**.

A presente Licitação, do tipo **MENOR PREÇO GLOBAL,** será integralmente conduzida pelo pregoeiro e regida pelo Regulamento de Licitações e Contratos do Sesc/DR/AP, instituído pela Resolução Sesc nº 1.593/2024, do Conselho Nacional do Serviço Social do Comércio.

As instruções estabelecidas neste Edital de Licitação determinam os procedimentos que orientarão o presente processo licitatório até a assinatura do respectivo contrato ou documento equivalente. Alegações de desconhecimento destas instruções, bem como das disposições legais acima especificadas, não serão aceitas como razões válidas para justificar quaisquer erros ou divergências encontradas em seus documentos de HABILITAÇÃO e/ ou PROPOSTA (S) DE PREÇO (S), ressaltando-se que o processo decorrente não é regido pela Lei nº 14.133/2021 (Licitações e Contratos da Administração Pública) ou outra norma similar, exceto pelas aqui referenciadas.

A documentação necessária à **HABILITAÇÃO** e as **PROPOSTAS DE PREÇOS** deverão atender a todas as exigências contidas no Edital. Qualquer descumprimento por parte do proponente implicará na sua inabilitação ou desclassificação.

O edital estará disponível, gratuitamente, nos seguintes endereços eletrônicos:
a) www.licitacoes-e.com.br.
b) www.sescamapa.com.br.

1. DA ABERTURA

1.1. Acolhimento das Propostas: Das **09h**. do dia **03/09/2024** até às **08h59horas** do dia **12/09/2024**
1.2. Abertura das Propostas: Às 09 horas do dia 12/09/2024.
1.3. Início da Sessão Pública de Disputa de Preços: Às 15 horas do dia 12/09/2024.
1.4. Local da Disputa: sítio eletrônico www.licitacoes-e.com.br.
1.5. Código Licitacoes-e: 1054134.
1.6. Todas as referências de horário no Edital, no aviso e durante a Sessão Pública observarão obrigatoriamente o **horário de Brasília/DF** e desta forma, serão registradas no sistema eletrônico e na documentação do certame.

2. DO OBJETO

2.1. O objeto deste Pregão é selecionar a proposta mais vantajosa para o Sesc/DR/AP, segundo os critérios estabelecidos neste instrumento convocatório e seus anexos, para a **aquisição de solução de segurança com características de Next Generation Firewall – NGFW, para proteção de informações perimetral e de rede interna.**
2.2. O Sesc/DR/AP não está obrigado a adquirir o objeto desta licitação, podendo até realizar contratações com terceiros, se for mais vantajoso a entidade esse procedimento.

2.3. As especificações técnicas referentes ao objeto constam no ANEXO I (Termo de Referência) deste edital.

2.4. Em caso de discordância existente entre as especificações deste objeto descritas no portal eletrônico - www.licitacoes-e.com.br - e as especificações técnicas constantes deste edital, prevalecerão estas.

2.5. Mesmo em caso de expressa contradição entre as especificações acima citadas, não se alegará indução ao erro, devendo a licitante se atentar unicamente às descrições do objeto contidas neste edital.

2.6. Este edital de licitação estará disponível nos sítios do Sesc/DR/AP - www.sescamapa.com.br - e no www.licitacoes-e.com.br.

3. DA DOTAÇÃO ORÇAMENTÁRIA

3.1. As despesas decorrentes do objeto deste Termo de Referência correrão à conta 5.1.2.3 – Infraestrutura de Tecnologia da Informação e Telecomunicação, sendo subsidiado pelo Departamento Nacional, conforme correspondência de nº 001452/2024, expedida em 29/02/2024.

4. DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. PODERÃO PARTICIPAR DA LICITAÇÃO:

4.1.1. Quaisquer Pessoas Jurídicas de Direito Privado, observada a necessária qualificação, qual seja, a pertinência da atividade mercantil com o objeto desta licitação.

4.2. NÃO PODERÃO PARTICIPAR DA LICITAÇÃO:

4.2.1. Pessoa Jurídica que esteja sob decretação de falência, concordata, recuperação judicial ou extrajudicial (conforme Lei n.º 11.101/2005), dissolução ou liquidação.

4.2.2. Estejam impedidas de licitar ou de contratar com o Sistema Sesc/Senac.

4.2.3. Estejam reunidas em consórcio.

4.3. Na presente licitação somente poderá se manifestar em nome da licitante o sócio ou dirigente, com poderes conferidos pelo Estatuto ou Contrato Social para representá-la, ativa e passivamente, em juízo ou fora dele, ou ainda, o procurador devidamente credenciado.

4.3.1. Entende-se como procurador credenciado aquele com poderes outorgados através de procuração para representar a licitante em processo licitatório, ou ainda, aquele credenciado através da Carta de Credenciamento **ANEXO II** deste edital.

5. CREDECIAMENTO

5.1. Somente poderão participar deste **PREGÃO ELETRÔNICO** as licitantes devidamente credenciadas junto ao provedor do sistema "Licitações-e" na página eletrônica www.licitacoes-e.com.br.

5.2. O credenciamento dar-se-á pela atribuição de chaves de identificação e de senhas individuais a serem fornecidas pelo provedor do sistema quando do credenciamento.

5.3. Os interessados deverão obter maiores informações, principalmente sobre a apresentação de documentação e credenciamento de representantes, junto a quaisquer agências do Banco do Brasil S/A ou pelo telefone 4004-0001 para Capitais e Regiões Metropolitanas e 0800 729 0001 demais localidades (Central de Atendimento).

5.4. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Sesc/DR/AP responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

5.5. O credenciamento da empresa e de seu representante legal junto ao sistema eletrônico implica na responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao Pregão Eletrônico**.**

6. DA CONEXÃO COM O SISTEMA

6.1. A participação no Pregão Eletrônico dar-se-á por meio de conexão da licitante ao sistema eletrônico acima citado, mediante digitação de sua senha privativa (emitida nos termos do subitem **5.2.** deste Edital) e subsequente encaminhamento da **Proposta de Preços**, **exclusivamente** por meio do referido sistema eletrônico, observadas datas e horários limites estabelecidos neste Edital;

6.2. A empresa Licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiros sua proposta e seus lances;

6.3. Incumbirá, ainda, à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;

6.4. No caso de desconexão com o (a) pregoeiro (a), no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível às licitantes para a recepção dos lances, retomando o (a) Pregoeiro (a), quando possível, sua atuação no certame, sem prejuízo dos atos realizados;

6.4.1. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão do **Pregão Eletrônico** será suspensa e terá reinício somente após comunicação expressa do (a) pregoeiro (a) às licitantes, mediante mensagem eletrônica postada no portal eletrônico "licitações-e" e no site do Sesc/DR/AP, divulgando data e hora da reabertura da sessão.

7. DA DOCUMENTAÇÃO DE HABILITAÇÃO

7.1. HABILITAÇÃO JURÍDICA:

7.1.1. Ato Constitutivo, Estatuto ou Contrato Social em vigor, acompanhado da última Alteração Contratual, ou a última Alteração Contratual Consolidada, se houver, devidamente registrados em se tratando de Sociedade Empresarial e, no caso de Sociedade Civil ou por Ações, os documentos comprobatórios do mandato de diretoria em exercício ou da eleição de seus administradores.

7.1.2. Documentos comprobatórios do **Representante Legal da Licitante,** a fim de comprovar que as assinaturas dos documentos de habilitação são de pessoa com poderes para tal, sabendo que o CPF poderá ser comprovado caso o número de registro conste na Cédula de Identidade.

7.1.2.1. Cópia da cédula de identidade e CPF.

7.1.2.2. Carta de Credenciamento (**ANEXO II**) ou **Procuração,** com firma reconhecida, acompanhada dos documentos citados no item **7.1.1**, caso a licitante se faça representar por procurador ou credenciado.

7.1.3. A ausência do credenciamento do representante legal, a não apresentação ou incorreção do documento de credenciamento, não inabilitará a licitante, mas impedirá o portador da proposta quando for o caso, de se manifestar durante as reuniões.

7.1.4. Nenhuma pessoa, ainda que munida de procuração, poderá representar mais de uma empresa junto ao Sesc/DR/AP, sob pena de exclusão sumária das licitantes representadas.

7.2. HABILITAÇÃO DA REGULARIDADE FISCAL E TRABALHISTA:

7.2.1. Provas de inscrição no Cadastro Nacional de Pessoas Jurídicas **(CNPJ)**;

7.2.2. Prova de inscrição no **Cadastro de Contribuinte Estadual**, relativo a domicilio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

7.2.3. Prova de regularidade para com:

7.2.3.1. **Fazenda Federal**: Certidão Conjunta Negativa de Débitos ou Certidão Conjunta Positiva, com Efeitos Negativos, relativos aos Tributos Federais e à Dívida Ativa da União, emitida pela

Secretaria da Receita Federal do Brasil. Podendo ser considerado também o novo modelo da certidão expedida pela Receita Federal do Brasil (RFB) e pela Procuradoria Geral da Fazenda Nacional, a qual inclui as contribuições sociais, conforme portaria conjunta RFB/PGFN nº 1.751, de 2 de outubro de 2014.

7.2.3.2. **Fazenda Estadual – ICMS**: - Certidão Negativa de Débitos ou Certidão Positiva, com efeitos negativos, emitida pela Secretaria de Fazenda Estadual, da sede da empresa licitante.

7.2.3.3. **Certidão de Regularidade do Fundo de Garantia por Tempo de Serviço (FGTS)**, emitida pela Caixa Econômica Federal.

7.2.3.4. A empresa licitante deverá apresentar **Certidão Negativa de Débitos Trabalhistas - CNDT**, conforme ordenado pela lei nº 12.440, de 07.07.2011. Esta certidão poderá ser impressa gratuitamente através do site www.tst.jus.br/certidao;

7.2.4. Caso as certidões expedidas pelas fazendas federais e estadual sejam positivas, o Sesc/DR/AP se reserva o direito de só aceitá-las se as mesmas contiverem expressamente o efeito negativo, nos termos do art. 206 do código tributário nacional, passado pelo seu emitente.

7.3. QUALIFICAÇÃO TÉCNICA:

7.3.1. Comprovar, através de, no mínimo 01 (um), **Atestado de Capacitação Técnica**, ter a empresa executado com qualidade o objeto deste edital.

7.3.2. Esse documento deverá ser emitido, em papel timbrado, pelo órgão público ou pela empresa privada que foi atendida, estando as informações ali contidas sujeitas a verificação de veracidade por parte do (a) Pregoeiro (a) e equipe de apoio;

7.3.3. **revogado.**

7.3.4. **Declaração de Que Não Emprega Menor de Idade (Anexo V)**, em papel timbrado da empresa vencedora, assinada pelo seu representante legal, em cumprimento do disposto no inciso XXXIII do art. 7º da Constituição da República Federativa do Brasil 1988, que dispõe sobre a proibição de trabalho noturno, perigoso ou insalubre aos menores de dezoito anos e de qualquer trabalho a menores de quatorze anos, salvo na condição de aprendiz;

7.3.5. **Declaração de Pleno Conhecimento do Edital e seus Anexos (Anexo IV)** e aceitou previamente todas as condições estipuladas na referida licitação**,** em papel timbrado da empresa Licitante e assinado pelo representante legal.

7.4. QUALIFICAÇÃO ECONÔMICA FINANCEIRA:

7.4.1. **Certidão Negativa de Falência e Concordata** (conforme a Lei nº 11.101/2005) expedida pelo distribuidor da sede da Pessoa Jurídica, no prazo máximo de 90 (noventa) dias a contar de sua expedição, ou em data válida indicada na própria certidão.

7.5. CONSIDERAÇÕES GERAIS SOBRE OS DOCUMENTOS

7.5.1. Os documentos não poderão apresentar emendas, rasuras ou entrelinhas, podendo ser apresentados na ordem em que estão descritos acima, evitando-se folhas soltas e sem identificação;

7.5.2. No caso de a Licitante possuir filiais, as documentações apresentadas deverão referir-se apenas a uma das filiais ou apenas à matriz, salvo disposição em contrário, sendo que a contratação será realizada com a pessoa jurídica que apresentou a documentação;

7.5.3. Não serão aceitos "protocolos de entrega" ou solicitação de documento em substituição aos documentos requeridos no presente Edital;

7.5.4. A Comissão Permanente de Licitação reserva-se o direito de solicitar o original de qualquer documento, sempre que tiver dúvida e julgar necessário;

7.5.5. As Microempresas e Empresas de Pequeno Porte, que se enquadrem como tal e desejarem obter os benefícios da Lei Complementar nº. 123 de 14 de dezembro de 2006, deverão comprovar essa condição mediante Certidão expedida pela Junta Comercial, nos termos do art. 8º da Instrução Normativa n.º 103, de 30.04.2007;

7.5.6. As microempresas e empresas de pequeno porte, por ocasião da participação em certames licitatórios, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, atendendo o que determina os art. 42 e 43 da Lei Complementar 123/06;

7.5.7. Havendo alguma restrição na comprovação da regularidade fiscal das microempresas e empresas de pequeno porte será assegurado o prazo de 05 (cinco) dias úteis, podendo ser prorrogado por igual e sucessivos períodos, a critério da comissão, para a regularização da documentação, conforme redação alterada do §1º do Art.43 da LC 147/2014;

7.5.8. A não regularização da documentação no prazo previsto no subitem supracitado implicará decadência do direito à contratação, sem prejuízo das sanções previstas no Regulamento de Licitações e Contratos do Serviço Social do Comércio – Sesc, Resolução Sesc nº 1.593/2024, sendo facultado à instituição convocar os licitantes remanescentes na ordem de classificação, para a assinatura do contrato, ou revogar a licitação;

7.5.9. A não apresentação de qualquer documento exigido para a habilitação implicará na automática inabilitação do licitante;

7.5.10. Os documentos que forem emitidos pela Internet estarão sujeitos à conferência na página eletrônica do órgão emissor. A CPL conferirá a sua autenticidade durante a sessão;

7.5.11. Os documentos relacionados nos itens **7.1, 7.2, 7.3** e **7.4** deverão estar devidamente atualizados e dentro dos respectivos prazos de validade. O disposto neste dispositivo não se aplicará ao item **7.3.1.**

7.5.12. Todos os documentos de habilitação poderão ser autenticados pela Comissão Permanente de Licitação, com a apresentação dos originais. Os documentos retirados através da internet não necessitarão de autenticação, desde que no mesmo possa ser identificado o órgão emissor e a data de emissão;

7.5.13. Serão habilitadas as licitantes que apresentarem todos os documentos em conformidade com as exigências deste Edital dentro do prazo previsto.

8. DO PREENCHIMENTO DA PROPOSTA DE PREÇO NO SISTEMA ELETRÔNICO

8.1. A **Proposta de Preço Inicial** deverá ser enviada, **exclusivamente**, por meio do sistema eletrônico, observando-se os prazos e condições estabelecidas neste edital.

8.2. A **Proposta de Preço Inicial** inserida no sistema eletrônico, durante o período definido neste edital como **"Recebimento (ACOLHIMENTO) das Propostas"**, deverá atender aos quantitativos e especificações técnicas, conforme Termo de Referência **(Anexo I).**

8.3. A apresentação de proposta eletrônica presumir-se-á o cumprimento das condições estabelecidas neste edital e seus anexos, devendo constar no sistema:

8.3.1. VALOR TOTAL GLOBAL.

8.3.2. DESCRIÇÃO GLOBAL.

8.4. Os dados acima deverão ser inseridos em campo próprio da proposta eletrônica. Caso não sejam inseridos, **a proposta poderá ser desclassificada**.

8.5. É VEDADA A IDENTIFICAÇÃO DA LICITANTE. Caso anexe a proposta, esta não poderá conter a identificação da licitante, como: nome da empresa, CNPJ, assinatura, logomarca etc., bem como nos documentos apensos à mesma; ou qualquer outra informação que infrinja o anonimato da proponente.

8.5.1. Havendo a identificação, a licitante será imediatamente desclassificada.

8.6. Os documentos de habilitação serão solicitados posteriormente à empresa arrematante, após o encerramento da fase de lances.

8.7. O valor proposto englobará todas as despesas relativas ao objeto do contrato ou documento equivalente, bem como os respectivos custos diretos e indiretos, tributos, fretes, remunerações, despesas fiscais e financeiras e quaisquer outras necessárias ao fornecimento.

8.8. A proposta deverá limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preços ou qualquer outra condição não prevista neste edital.

8.9. Não serão aceitas propostas distintas provenientes da mesma empresa.

8.10. A Comissão de Permanente de Licitações analisará as **PROPOSTAS DE PREÇOS** encaminhadas, desclassificando aquelas que não estiveram em consonância com o estabelecido pelo presente edital e seus anexos, cabendo ao pregoeiro registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real pelos licitantes.

8.11. A Comissão Permanente de Licitações poderá desclassificar, fundamentadamente, as propostas que não atenderem às exigências do edital ou forem manifestamente inexequíveis.

8.12. Serão, ainda, desclassificadas as propostas que sejam omissas, vagas ou que apresentem irregularidades capazes de dificultar o julgamento.

9. DA ABERTURA DA PROPOSTA DE PREÇOS, DOS LANCES E DA NEGOCIAÇÃO

9.1. Até o horário previsto neste edital, os interessados poderão inserir ou substituir suas propostas iniciais dentro do sistema.

9.2. Finalizado o período de recebimento das propostas, iniciar-se-á a fase de **"Abertura das Propostas"**, de acordo com o horário previsto no sistema, momento no qual a Comissão de Licitação avaliará a aceitabilidade de cada uma das propostas enviadas, desclassificando aquelas que estejam em desconformidade com as exigências deste edital.

9.3. O sistema ordenará, automaticamente, as propostas classificadas pela Comissão Permanente de Licitação.

9.4. Ordenada as propostas, dar-se-á início, no horário e local designados neste edital, à Sessão Pública de Disputa de Lances, da qual somente poderão participar as licitantes que tiveram suas propostas de preços classificadas na fase anterior.

9.5. Todas as propostas classificadas serão consideradas como lances na fase da disputa e ordenadas de forma crescente.

9.5.1. Será considerada como primeiro lance a proposta classificada de **MENOR VALOR**.

9.5.2. Em caso de empate entre duas ou mais propostas e não havendo lances, prevalecerá como de menor valor a proposta que tiver sido primeiramente registrada no sistema.

9.6. Em relação a participação de microempresas e empresas de pequeno porte, encerrada a etapa de lances, o sistema procederá à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos artigos 44 e 45 da LC nº 123, de 2006.

9.6.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

9.6.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

9.6.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

9.7. Na fase da Sessão Pública de Disputa de Preços, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances, isto é, somente serão aceitos novos lances enviados exclusivamente por meio do sistema eletrônico.

9.8. A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado pelo sistema eletrônico.

9.9. Não serão aceitos dois ou mais lances do mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar pelo sistema eletrônico.

9.10. Os lances ofertados serão no VALOR TOTAL DO GLOBAL, sendo consideradas somente 02 (duas) casas decimais, desprezando-se as demais.

9.11. Durante o transcurso da "Sessão Pública de Disputa de Preços", os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais licitantes.

9.12. O pregoeiro está autorizado, no momento da sessão de lances, a fixar diferença mínima entre lances, sempre respeitando o princípio da razoabilidade.

9.13. O tempo normal da etapa de lances da "Sessão Pública de Disputa de Preços" será encerrado, por decisão do pregoeiro, que informará do término com no mínimo 03 (três) minutos de antecedência, através de mensagem aos participantes.

9.14. Encerrado o tempo normal, terá início ao tempo extra (randômico), que é gerado pelo sistema de forma aleatória, podendo variar de 01 (um) segundo a 30 (trinta) minutos.

9.14.1. O tempo extra (randômico) é desconhecido tanto pelos licitantes como pelo pregoeiro.

9.14.2. Face à imprevisão do tempo extra (randômico), os licitantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando-se, assim, cálculos de última hora, que poderá resultar em uma disputa frustrada por falta de tempo hábil.

9.15. Se algum licitante fizer um lance que esteja em desacordo com o edital ou oferta inexequível, o mesmo poderá ser cancelado pelo pregoeiro através do sistema.

9.16. No caso de não haver lances na "Sessão Pública de Disputa de Preços", serão considerados válidos os valores obtidos na fase de "Abertura das Propostas" entre as propostas classificadas.

9.17. Quando houver uma única proposta válida, caberá à Comissão Permanente de Licitação verificar a aceitabilidade do preço ofertado.

9.18. O sistema informará a proposta de menor preço por (lote/item) imediatamente após o encerramento da etapa de lances.

9.19. É vedada a desistência dos lances já ofertados, sujeitando-se o proponente às sanções previstas neste edital, exceto se a justificativa apresentada durante a etapa de formulação dos lances for aceita pela Comissão Permanente de Licitação.

9.20. O sistema eletrônico gerará ata circunstanciada da sessão, na qual estará registrada a indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à "Sessão Pública de Disputa de Preços" do Pregão Eletrônico.

9.21. Negociação:

9.21.1. O pregoeiro poderá encaminhar contraproposta diretamente à licitante que tenha apresentado o lance mais vantajoso, observado o critério de julgamento.

9.21.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais licitantes.

9.21.3. A contraproposta deve ser respondida no prazo máximo de 60 (sessenta) minutos, podendo este prazo ser prorrogado, a critério do pregoeiro e mediante solicitação encaminhada no chat. Caso a contraproposta não seja respondida no prazo, a proposta poderá ser recusada.

9.21.4. Não sendo compatível o preço e havendo recusa de contraproposta, o pregoeiro recusará a proposta e direcionará a contraproposta à licitante imediatamente classificada, assim sucessivamente, até a obtenção do preço julgado aceitável.

9.21.5. A contraproposta será baseada no valor estimado para aquisição.

9.21.6. O Sesc/DR/AP poderá aceitar proposta com preços superiores ao preço estimado, desde que, mediante diligência, verifique-se que as especificações do objeto proposto atendem às características mínimas do objeto licitado, não sendo excessivas e desnecessárias, bem como, seja o preço compatível com o mercado.

10. DO ENVIO DA PROPOSTA DE PREÇO AJUSTADA E DA DOCUMENTAÇÃO DE HABILITAÇÃO

10.1. Encerrada a fase de lances, a licitante classificada provisoriamente em primeiro lugar, quando solicitada pelo pregoeiro, deverá anexar, ao portal licitações-e (www.licitacoes-e.com.br), toda a documentação referente a **Habilitação** e **Proposta de Preço Ajustada ao Último Lance**, conforme **ANEXO III**, em **até 02 (duas) horas úteis**.

10.1.1. Não sendo possível o envio na forma estabelecido anteriormente, a licitante poderá encaminhar a documentação exigida para o e-mail: **cpl@sescamapa.com.br**, devendo justificar no portal licitações-e as dificuldades encontradas.

10.2. O prazo estabelecido poderá ser prorrogado mediante solicitação ao pregoeiro, desde que solicitada antes de findo o prazo estabelecido, e formalmente aceito pelo pregoeiro.

10.3. **A Proposta de Preço Ajustada e seus Anexos**, bem como os **documentos de Habilitação**, quando aplicado a estes, e sempre que possível, **deverão ser assinados digitalmente**, desde que a veracidade da assinatura possa ser verificada.

10.4. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema e/ou e-mail, no prazo de 02 (duas) horas, sob pena de inabilitação.

10.4.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais ou cópias autenticadas quando houver dúvida em relação à integridade do documento digital.

10.4.1.1. Caso solicitado, o documento deverá ser encaminhado à Comissão de Licitações do Sesc/DR/AP, situada na Rua Jovino Dinoá, nº 4311, Bairro Beirol, Macapá-AP, CEP: 68.902-030.

10.5. A não apresentação da Proposta de Preços Ajustada e/ou a documentação de Habilitação exigidos, por parte da empresa classificada em primeiro lugar, dentro dos prazos e formas estabelecidos neste edital, acarretará em sua desclassificação e/ou inabilitação, sendo convocados, por ordem de classificação, os demais participantes do processo licitatório.

10.6. A arrematante, caso solicitada, deverá incluir, juntamente a sua Proposta de Preços Ajustada, informações adicionais, catálogos e quaisquer outros elementos elucidativos, pertinentes aos serviços/produtos ofertados.

10.7. Deverá constar na proposta os dados para depósito em conta, obrigatoriamente, em nome da empresa (nome do banco, nome e número da agência e número da conta corrente), e seu e-mail comercial, para o qual serão enviados comunicados e/ou outras informações pertinentes ao processo.

11. DA PROPOSTA AJUSTADA, DO JULGAMENTO E DA ACEITABILIDADE

11.1. O julgamento obedecerá ao critério de **MENOR PREÇO**.

11.2. A licitante vencedora deverá ater-se aos quantitativos e especificações técnicas para o item escolhido, em conformidade com Termo de Referência (Anexo I).

11.3. A validade da proposta não poderá ser inferior a 60 (sessenta) dias, contados da data de abertura da Sessão Pública de Lances. Na ausência de indicação expressa do prazo de validade, considerar-se-á tacitamente indicado o prazo de 60 (sessenta) dias.

11.4. O frete deverá estar incluso no preço do produto, considerando-se o frete CIF/AP.

11.5. A Proposta Comercial Ajustada deverá indicar a marca e/o modelo do produto, bem como as especificações exatas do produto ofertado e não uma reprodução do texto do edital.

11.6. Recebido a proposta ajustada, o pregoeiro analisará a melhor proposta classificada quanto a compatibilidade do preço ofertado com o praticado no mercado, bem como o cumprimento das especificações do objeto.

11.7. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

11.8. Caso a proposta de preço seja considerada inexequível, com base na realidade do mercado, o pregoeiro poderá diligenciar, convocando a licitante para que demonstre a exequibilidade do seu preço, sob pena de desclassificação.

11.8.1. A licitante poderá valer-se de qualquer tipo de prova fidedigna e suficiente para demonstrar a exequibilidade do preço ofertado, a exemplo de planilhas aberta de custos, tabela de preços oficiais, cópia de contratos de objetos similares ao licitado com outras entidades, etc.

11.9. A Comissão poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Sesc/DR/AP ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

11.10. É facultado à Comissão Permanente de Licitação promover diligências para sanar falhas formais da proposta e/ou documentos.

11.11. O Sesc/DR/AP poderá determinar à licitante vencedora, mediante diligência, que promova ajustes na proposta, se possível, para que reflita corretamente os custos envolvidos na contratação, desde que não haja majoração do preço unitário e total propostos na fase de lances e/ou negociado.

11.12. Não sendo a Proposta Comercial Ajustada aceita ou se a licitante não atender às exigências habilitatórias, a Comissão de Licitação examinará a proposta comercial subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital.

11.13. Havendo discrepância entre os preços unitários e totais da proposta ajustada prevalecerá o valor unitário arrematado; havendo discordância entre o valor da proposta em algarismo e o total por extenso, prevalecerá aquele que se equivaler ao valor arrematado.

11.14. A Comissão Permanente de Licitação desclassificará a licitante que apresentar proposta que:

11.14.1. Não estiver em conformidade com as exigências deste edital e seus anexos.

11.14.2. Com preços excessivos ou manifestamente inexequíveis.

11.14.3. Seja omissa ou vaga, bem como a que apresentar irregularidades ou defeitos capazes de impedir o julgamento.

11.14.4. Impuser condições, ressalvas, ofertas de vantagens em relação às condições estabelecidas neste edital e anexos, ou propostas das demais licitantes.

11.15. A elaboração da proposta é de inteira responsabilidade da licitante, não lhe cabendo a desistência, sob pena de aplicação das sanções previstas neste edital e anexos.

11.16. Constatado o atendimento às exigências fixadas neste edital, a licitante será declarada vencedora.

12. DO ACRÉSCIMO

12.1. No interesse da Administração do Sesc/DR/AP, o valor inicial atualizado do contrato poderá ser acrescido até o limite de 50% (cinquenta por cento), com fundamento do Art. 38 da Resolução Sesc 1.593/2024, que passou a vigorar no dia 02 de maio de 2024.

12.1.1. A contratada poderá aceitar o acréscimo ou complemento, nas mesmas condições licitadas, que se fizerem necessários.

13. DA IMPUGNAÇÃO E DOS ESCLARECIMENTOS

13.1. No que tange a **impugnação** do presente instrumento, o prazo será de até 02 (dois) dias úteis antes da data fixada para abertura da Sessão Pública, tendo como horário limite até às 23h59min do último dia do prazo (horário oficial de Brasília/DF), qualquer pessoa física ou jurídica, poderá impugnar o ato convocatório deste pregão, mediante petição a ser enviada **exclusivamente** por meio eletrônico, via internet, para o seguinte endereço: cpl@sescamapa.com.br.

13.2. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame.

13.3. Os pedidos de esclarecimentos referentes ao presente instrumento convocatório, deverão ser enviados ao(à) Pregoeiro(a) no prazo máximo de 03 (três) dias úteis, anteriores a data informada para abertura da sessão pública, tendo como horário limite até às 23h59min do último dia do prazo (horário oficial de Brasília/DF), exclusivamente por meio eletrônico, no endereço cpl@sescamapa.com.br, contendo o número da licitação e as questões a serem esclarecidas, não constituindo, necessariamente, motivos para que se altere a data e horário do pregão.

13.4. O tempo de publicação das respostas às impugnações e aos esclarecimentos ficará a critério da CPL e serão disponibilizadas para conhecimento das licitantes e da sociedade em geral no portal www.licitacoes-e.com.br e no sítio do Sesc/DR/AP - www.sescamapa.com.br.

14. DOS RECURSOS

14.1. Encerrada a etapa de lances, as Licitantes deverão consultar regularmente o sistema para verificar quem foi (ram) declarado (s) o (s) vencedor (es) e se estará liberada a opção para interposição de recursos.

14.1.1. O prazo para a licitante manifestar sua intenção de interpor recurso, exclusivamente no campo próprio do portal eletrônico (www.licitacoes-e.com.br), será de até 24 (vinte e quatro) horas, a contar da data e hora da declaração do vencedor licitante.

14.2. Declarado(s) o(s) vencedor(es), qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema eletrônico, manifestar sua intenção de recorrer, registrando a síntese de suas razões, quando lhe será concedido o prazo de 02 (dois) dias úteis para apresentar as razões do recurso, ficando os demais licitantes desde logo, intimados para apresentarem suas contrarrazões em igual prazo, o qual começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

14.2.1. Após a manifestação, através do sistema eletrônico, de interpor recurso, a licitante deverá encaminhar as suas razões por meio eletrônico, via Internet, para o endereço cpl@sescamapa.com.br, em nome da Comissão Permanente de Licitação, no prazo máximo de até 02 (dois) dias úteis posteriores ao fim do prazo da intenção de manifestar recurso.

14.2.2. Não serão aceitos, para análise, os recursos que chegarem fora dos prazos previstos acima.

14.3. A falta de manifestação imediata e motivada da Licitante quanto à intenção de recorrer, nos termos acima, importará na decadência desse direito, ficando a Comissão Permanente de Licitação autorizada a adjudicar o (s) objeto (s) ao (s) licitante (s) declarado (s) vencedor (es).

14.3.1. Para efeito do disposto no parágrafo anterior, manifestação imediata é aquela efetuada via eletrônica – Internet, no período máximo de 24 (vinte e quatro) horas depois de declarado (s) o (s) vencedor (es); e manifestação motivada é a descrição sucinta e clara do fato que motivou a licitante a recorrer.

14.4. Observado o disposto no subitem **14.2**, os autos do Processo permanecerão com vista franqueada aos interessados, no Setor de Licitações e Contratos do Sesc/DR/AP, situado na Rua Jovino Dinoá, nº 4311, Bairro Beirol, Macapá-AP.

14.5. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento. Aqueles vícios ou omissões consideradas irrelevantes, facilmente sanáveis ou desprezíveis poderão ser sanados, a critério da comissão, se demonstrada a vantajosidade da proposta.

14.6. O recurso contra a decisão da Comissão Permanente de Licitação terá efeito suspensivo.

14.7. Havendo recurso, a Comissão Permanente de Licitação, apreciará os mesmos no prazo máximo de 10 (dez) dias úteis, a contar do recebimento, e caso não reconsidere sua posição, caberá à Autoridade Competente a decisão em grau final.

14.8. As respostas aos recursos recebidos, com relação ao presente PREGÃO ELETRÔNICO, serão disponibilizadas para consulta de todos os interessados no portal eletrônico - www.licitacoes-e.com.br e no sítio do Sesc/DR/AP - www.sescamapa.com.br.

15. DA ADJUDICAÇÃO

15.1. Após homologação e adjudicação do processo pela Administração Regional do Sesc/DR/AP, a empresa vencedora será convidada a retirar a Ordem de Compra - OC e/ou Assinar Contrato pelo seu preço proposto, irreajustável, assinado pelo Sesc/DR/AP, observadas as condições estipuladas neste edital e seus anexos.

16. DO CONTRATO

16.1. A licitante vencedora firmará com o Sesc/DR/AP instrumento contratual, devidamente assinado pelas partes através de seus representantes, pelo qual se obrigará a prestar o serviço objeto desta Licitação, nas condições constantes do presente Edital, Anexos e na PROPOSTA DE PREÇO da empresa contratada.

16.2. Nos casos em que não houver instrumento contratual complexo, a Ordem de Compra tornar-se-á documento a ele equivalente, ocorrendo, nestes casos, a obrigatoriedade de entrega do produto/serviço contratado, já que será, inevitavelmente, utilizado para solicitar o produto/serviço e seu cumprimento é imprescindível ao pagamento da Nota Fiscal.

16.3. O prazo para que a vencedora subscreva o contrato será de até 10 (dez) dias, contados da data de convocação para assinatura, que será realizada pelo Setor de Contratos e Convênios do Sesc/DR/AP.

16.3.1. O prazo para assinatura do contrato poderá ser prorrogado mediante solicitação do arrematante, dentro do prazo inicial, e aceite da Comissão Permanente de Licitação, sob pena de decair o direito à contratação.

16.4. A vigência do contrato será de 12 (doze) meses e iniciará na data de sua assinatura.

16.5. O contrato poderá ser prorrogado até o limite máximo de 120 meses, desde que pesquisa de mercado demonstre que o preço contratado atualizado se mantém vantajoso para prorrogação, conforme art. 33, da Resolução.

16.6. A CONTRATADA fica obrigada a manter, durante a integralidade da vigência contratual, todas as condições de participação e habilitação exigidas na presente licitação, em especial, aquelas relativas à sua regularidade fiscal.

16.7. Verificada a recusa em assinar o contrato, o Sesc/DR/AP reserva o direito de convocar as licitantes remanescentes, obedecendo à ordenação final, para assinar o contrato, em igual prazo e nas mesmas condições propostas pelo primeiro classificado, ficando a licitante convidada livre para aceitar ou não a contratação.

17. DAS PENALIDADES

17.1. Quando participar da licitação, o proponente estará sujeito às penalidades pelos atos de seu preposto ou representante, inclusive depois de assinado o contrato por: conduta inapropriada, recusa da proposta, falha, irregularidade, não cumprimento de prazo, outros casos a critério do Sesc que venham a frustrar ou inviabilizar o objeto da presente licitação;

17.2. A recusa injustificada da licitante em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estipulado, caracteriza o descumprimento total da obrigação assumida, podendo acarretar às licitantes as seguintes penalidades:

17.2.1. Perda do direito a contratação;

17.2.2. Suspensão do direito de licitar ou contratar com a contratante pelo prazo não superior a 03 (três) anos;

17.3. O inadimplemento total ou parcial das obrigações assumidas, dará ao contratante o direito de penalizar com:

17.3.1. Advertência;

17.3.2. Multa compensatória de 10% (dez por cento) sobre o valor do contrato;

17.3.3. Multa moratória de 0,2 (dois) décimos por dia de atraso no cumprimento da obrigação;

17.4. As penalidades poderão ser aplicadas cumulativamente e deverão considerar os princípios do contraditório, ampla defesa, razoabilidade e proporcionalidade;

17.5. Diante da inexecução total ou parcial do objeto deste instrumento contratual, decorrente de dolo ou culpa da CONTRATADA, fica garantido a CONTRANTE o direito à rescisão unilateral do contrato sem direito a indenização de qualquer natureza à parte que deu ensejo a inexecução;

17.6. Fica estabelecido que a rescisão se dê, imediata e independentemente de qualquer aviso, extrajudicial ou interpelação judicial, no seguinte caso:

17.6.1. Falência ou dissolução da contratada;

18. DAS OBRIGAÇÕES DAS PARTES

18.1. OBRIGAÇÕES DO SESC/DR/AP:

18.1.1. Assegurar os recursos orçamentários e financeiros para custear o contrato,

18.1.2. Exercer o acompanhamento e a fiscalização dos serviços, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

18.1.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

18.1.4. Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

18.1.5. Efetuar o pagamento pelo fornecimento realizado, após devidamente atestada a nota fiscal/fatura, de acordo com as condições e preços pactuados, em até 15 dias úteis;

18.1.6. Rejeitar, no todo ou em parte, os materiais que a empresa vencedora entregar fora das especificações exigidas;

18.1.7. Prestar informações e esclarecimentos que venham a ser solicitados pela contratada.

18.2. OBRIGAÇÕES DA LICITANTE VENCEDORA:

18.2.1. Fornecer os produtos do presente termo a partir da ordem de compra emitida pelo Setor de Compras;

18.2.2. A Licitante vencedora se obriga a fornecer os produtos deste termo ao Sesc/DR/AP, a partir da Ordem de Compra – OC, emitida pela Coordenadoria de Material e Patrimônio;

18.2.3. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

18.2.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14, 17 e 18 a 27 do Código de Defesa do Consumidor (Lei nº 8.078/1990), ficando a Contratante autorizada a descontar da garantia, caso exigido no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

18.2.5. Responsabilizar-se por todas as despesas decorrentes da contratação do objeto deste termo, inclusive locomoção, seguro de acidentes, obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

18.2.6. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

18.2.7. Qualquer atraso na execução das obrigações assumidas deverá obrigatoriamente constar de justificativa protocolada no Setor de Protocolo do Sesc/DR/AP, dirigida ao fiscal do contrato, no prazo de 48 (quarenta e oito) horas anterior à data prevista para a execução da obrigação;

18.2.8. Responsabilizar-se pelo fiel cumprimento de todas as disposições e acordos relativos à legislação social e trabalhista em vigor, especialmente no que se refere ao pessoal;

18.2.9. Efetuar o pagamento de todos os impostos, taxas e demais obrigações fiscais incidentes ou que vierem a incidir;

18.2.10. Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação, apresentando os documentos com validade em dia que comprovem tal regularidade junto com a nota fiscal/fatura resultante do fornecimento do contrato, quais sejam:

18.2.10.1. Certidão Conjunta Relativa aos Tributos Federais e à Dívida Ativa da União;

18.2.10.2. Certidões de Regularidade perante a Fazenda Estadual, Municipal ou Distrital, conforme o tipo de prestação;

18.2.10.3. Certidão de Regularidade do FGTS; e

18.2.10.4. Certidão Negativa de Débitos Trabalhistas;

18.2.11. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação;

18.2.12. Fornecer produtos livres de quaisquer tipos de vício ou características que venham a prejudicar o desenvolvimento das atividades do Sesc/DR/AP;

18.2.13. Manter atualizados junto ao Setor de Contratos de Sesc/DR/AP seu endereço e telefone de contato;

18.2.14. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

18.2.15. Relatar à Contratante toda e qualquer irregularidade verificada no decorrer do fornecimento dos produtos;

18.2.16. Garantir a boa qualidade do objeto deste termo, os quais devem estar de acordo com as normas vigentes;

18.2.17. Repor, às suas expensas, os itens nos quais forem constatadas irregularidades, imediatamente após notificação feita pelo Sesc/DR/AP e sem ônus para a CONTRATANTE.

18.2.18. A Licitante, deverá atentar-se ainda as Especificações Detalhadas e Técnicas do Serviço, bem como, ao Suporte Técnico contidas no Termo de Referência (Anexo I), seguindo rigorosamente todos os seus termos.

19. PAGAMENTO

19.1. O pagamento à licitante vencedora será efetuado em moeda corrente nacional, através de depósito ou transferência bancária, por sistema online ou cheque nominal a empresa (de acordo com as normas do Sesc/DR/AP), devendo se ser informado, obrigatoriamente, na nota fiscal o número e nome do banco, número da agência e conta corrente;

19.1.1. As Notas fiscais deverão vir acompanhadas das certidões de regularidade fiscal exigidas no Termo de Referência;

19.1.1.1. Ao proprietário da empresa mediante apresentação do contrato social, documento de identificação com foto e carimbo da empresa com CNPJ;

19.1.1.2. Ou, procurador mediante apresentação da procuração, contrato social, documento de identificação com foto e carimbo da empresa com CNPJ.

19.2. A contratante terá o prazo máximo de **até 15 (quinze) dias úteis para efetuar o pagamento**, após o recebimento da nota fiscal e após ter sido atestada e correspondente ao fornecimento no Sesc/DR/AP.

19.3. Caso não haja expediente no Sesc/DR/AP no dia do vencimento da Nota Fiscal, fica o pagamento prorrogado para o 1º dia útil subsequente;

19.3.1. As empresas que tiverem seu CNAE previsto no Protocolo ICMS nº 42, de 03 de julho de 2009, deverão emitir a nota fiscal conforme legislação vigente.

19.4. O Sesc/DR/AP se reserva o direito de não aceitar notas fiscais que não estejam acompanhadas dos documentos que comprovem quitação de obrigações concernentes à certidão Negativa de Débitos do INSS, certificado de Regularidade do FGTS, Prova de Regularidade relativos a Tributos e Contribuições Federais, Certidão de débitos trabalhistas e ainda autorizações em cumprimento a legislação vigente. O não aceite das referidas notas fiscais não gera o dever de pagar, enquanto houver pendências de obrigações que tenham sido impostas, em virtude de penalidades ou inadimplemento apontados pela fiscalização.

19.4.1. O SESC/AP poderá suspender o pagamento após notificação ao CONTRATADO enquanto houver pendências de obrigações que tenham sido impostas, em virtude de penalidades ou inadimplemento apontado pela fiscalização. Cessadas estas causas, e a nota fiscal tenha sido devidamente atestada pelo setor competente, os pagamentos serão retomados sem que haja qualquer direito a atualização monetária;

19.5. A inobservância de quaisquer condições de pagamento não gera ao Sesc/AP o dever de pagar.

20. DA FISCALIZAÇÃO

20.1. O acompanhamento e a fiscalização do Sesc/DR/AP sobre o cumprimento das obrigações contratuais serão exercidos pela Coordenação de Tecnologia da Informação - CTIN;

20.2. Durante a fiscalização, é garantido ao fiscal exigir a substituição de produtos que sejam considerados defeituosos, inadequados ou inaplicáveis.

20.3. A carga e descarga deve ser realizada de forma a não acarretar dano ao produto, e é de responsabilidade da CONTRATADA.

20.4. Fiscal do Contrato certificará a nota fiscal/fatura do fornecimento correspondente, ficando a contratada responsável por todo e qualquer dano causado ao patrimônio da CONTRATANTE ou a terceiros, decorrente do não cumprimento das observações constantes neste termo.

20.5. No caso de defeitos ou imperfeições nos produtos, os mesmos serão recusados, cabendo a adjudicatária substituí-los por outros com as mesmas características exigidas neste Termo de Referência e Edital, no prazo a ser determinado pela Coordenadoria de Apoio Operacional - CAO. As embalagens devem estar isentas de deformação ou ferrugens.

20.6. A comunicação entre a FISCALIZAÇÃO e a CONTRATADA será realizada através de correspondência oficial, telefone ou e-mail.

21. DAS DISPOSIÇÕES FINAIS

21.1. As Licitantes deverão examinar cuidadosamente os termos e condições da presente Licitação, para que tenham ciência de todos os detalhes que possam afetar de algum modo o fornecimento do objeto desta licitação;

21.2. As empresas licitantes assumem todos os custos de preparação de suas propostas e o Sesc/DR/AP não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório;

21.3. As empresas licitantes são responsáveis pela fidedignidade e legitimidade das informações e dos documentos apresentados na proposta;

21.4. Após a apresentação da PROPOSTA DE PREÇO escrita, não cabe desistência de proposta, salvo por motivo justo decorrente de fato superveniente e aceito pelo Sesc/DR/AP;

21.5. É facultada à Comissão Permanente de Licitação ou a autoridade superior, em qualquer fase da licitação, promover **diligências** destinadas a esclarecer ou complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos ou informações que deveriam constar no ato da Sessão Pública;

21.6. Simples omissões ou irregularidades irrelevantes, sanáveis ou desprezíveis, a exclusivo critério da Comissão Permanente de Licitação, e que não causem prejuízo ao Sesc/DR/AP e as Licitantes, poderão ser relevadas;

21.7. Na contagem dos prazos estabelecidos na presente Licitação excluir-se-á o dia do início e incluir-se-á o dia do vencimento;

21.8. Os prazos estabelecidos nesta licitação só se iniciam e vencem nos dias em que houver expediente no Sesc/DR/AP;

21.9. A licitante homologada vencedora, depois de receber a Ordem de Compra (OC), deverá devolvê-la ao Sesc/DR/AP, assinada, em até 10 (dez) dias úteis de seu recebimento, do contrário, caracterizará descumprimento total da obrigação assumida, sujeitando-se as penalidades previstas; podendo ser convidada a assiná-la as demais licitantes, na ordem de classificação geral, com igual prazo e condições propostas pela primeira homologada vencedora;

21.10. O Sesc/DR/AP reserva-se o direito de rejeitar a (s) proposta (s) que não atender (em) às especificações do presente edital, contratar a totalidade do objeto ora licitado ou somente parte dele, em função de conveniência administrativa, sem que deste ato caiba direito a qualquer espécie de recurso, indenização ou reclamação da (s) proponente (s), bem como cancelar a presente licitação de ofício ou por interposição de recursos de terceiros;

21.11. A empresa licitante poderá obter informações sobre o objeto da licitação e outros elementos de caráter legal ou interpretação necessária ao perfeito conhecimento desta licitação junto a Comissão Permanente de Licitação, de segunda à sexta feira, no horário das 8h às 12h e das 14h às 18h, através do fone (96) 3241- 4440, ramal 246, e-mail: cpl@sescamapa.com.br;

21.12. O Sesc/DR/AP não se responsabilizará por e-mails que, por qualquer motivo, não forem recebidos por ele em virtude de problemas no servidor ou navegador, tanto do Sesc/DR/AP quanto do emissor, bem como se exime de qualquer responsabilidade quanto aos esclarecimentos, avisos de alterações e inclusões no edital e seus anexos, uma vez que cabe aos licitantes o acompanhamento das alterações no Portal Eletrônico do Sesc www.sescamapa.com.br, no link Licitações;

21.13. A apresentação da proposta e habilitação indicará que o Proponente conhece e aceita todo o conteúdo deste edital, seus anexos e normativos;

21.14. Os casos não previstos neste edital serão decididos pela Comissão Permanente de Licitação, com base na legislação vigente;

21.15. Este edital, seus anexos, Ordem de Compra (OC) e/ou Contrato e a proposta da empresa vencedora, formam entre si um único documento.

22. DOS ANEXOS

22.1. O dossiê para esta Licitação constituir-se-á dos seguintes documentos:

22.1.1. ANEXO I - Termo de Referência;

22.1.2. ANEXO II - Carta de Credenciamento;

22.1.3. ANEXO III - Modelo de proposta;

22.1.4. ANEXO IV - Declaração de conhecimento do edital e seus anexos;

22.1.5. ANEXO V - Declaração de que não emprega menor;

22.1.6. ANEXO VI - Declaração de dados bancários;

22.1.7. ANEXO VII - Minuta do Contrato.

Macapá-AP, 29 de agosto 2024.

Êmilie Cristine Alves Pereira
Diretora Regional
Sesc/DR/AP

Amanda Karina de Souza Pereira
Presidente da CPL
Sesc/DR/AP

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO I

TERMO DE REFERÊNCIA

Coordenadoria de Tecnologia daInformação – CTIN	TERMO DE REFERÊNCIA Nº 002/2024

1. OBJETO:

1.1. O presente Termo de Referência destina-se a aquisição de solução de segurança com características de Next Generation Firewall – NGFW, para proteção de informações perimetral e de rede interna, incluindo as seguintes características: Firewall, controle de aplicações, administração de largura de banda (Quality of Service – QoS), Virtual Private Network – VPN, Intrusion Prevent System – IPS,prevenção contra ameaças de vírus, spywares e malwares, ataques "Zero Day e Advanced Persistent Threat – APTs, filtro de endereço (Uniform Resource Locator – URL), gerenciamento integrado e criação de relatórios, compondo assim uma plataforma de segurança integrada e robusta.

2. JUSTIFICATIVA:

2.1. Em virtude da iminente necessidade de adequações constantes na infraestrutura de rede local, visando abarcar a crescente demanda de suporte em novas tecnologias e resguardar o atual ambiente de rede de dados deste Serviço Social do Comércio do Amapá - SESC/DR/AP, faz-se necessário investir em estratégias que ampliem a segurança das informações, para o alcance dos objetivos e níveis de satisfação dos serviços planejados.

2.2. A atual conjectura expõe a rede de computadores e sua acessibilidade, ou seja, a rede de dados deve estar disponível initerruptamente, garantindo integridade das informações trafegadas e armazenadas. Os usuários da rede, em sua maioria, não mais dependem de limites físicos para usufruir dos mecanismos de autenticação transparentes e acesso seguro, elevando a necessidade de controles de acessos e políticas aplicadas, tornando o ambiente de rede mais complexo de ser administrado.

2.3. A aquisição de uma nova tecnologia de suíte de segurança complementa um conjunto de medidas essenciais para a modernização da Rede de Dados do SESC/AP, com o intuito de entregar aos usuários finais, maior segurança, confiabilidade, credibilidade e robustez, essa aquisição almeja ser capaz de abranger as necessidades de visibilidade total nos eventos e ameaças de segurança e ainda comportar a infraestrutura em constante expansão.

2.4. Com a aquisição da solução de Next Generation Firewall – NGFW para o SESC/AP espera-se que todos os serviços disponibilizados para os usuários da rede, possam admitir e garantir os seguintes resultados e benefícios:

2.5. Implementação de políticas de segurança personalizadas e gerenciáveis;

2.6. Alta disponibilidade dos serviços de rede local;

2.7. Menor tempo de resposta aos incidentes de segurança;

2.8. Total visibilidade do tráfego e ameaças recorrentes na rede;
2.9. Gerenciamento integrado entre as redes locais do SESC/DR/AP (Sede e Unidades Operacionais);
2.10. Acesso remoto controlado e autenticado (VPN);
2.11. Filtros INTERNET de acesso e de conteúdo;
2.12. Controle de acesso de utilização de banda (link de dados) INTERNET;
2.13. Monitoramento e disponibilização de evidências (relatórios);
2.14. Suporte e garantia especializada.

3. FUNDAMENTAÇÃO LEGAL:

3.1. O referido termo será regido pelo Regulamento de Licitações e Contratos do SESC e pela Resolução Sesc nº 1.593 de 2024, que altera, modifica e consolida o citado regulamento.

4. DOTAÇÃO ORÇAMENTÁRIA:

4.1. As despesas decorrentes do objeto deste Termo de Referência correrão à conta 5.1.2.3 – Infraestrutura de Tecnologia da Informação e Telecomunicação, sendo subsidiado pelo Departamento Nacional, conforme correspondência de nº **001452/2024**, expedida em **29/02/2024.**

5. DETALHAMENTO DO OBJETO:

5.1. Lote 01:

ITEM	DESCRIÇÃO TÉCNICA	UNIDADE	QTD
1	PONTO DE ACESSO SEM FIO	HARDWARE	40
2	EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 1 COM LICENÇA DE SOFTWARE E GARANTIA DO FABRICANTE PELO PERÍODO DE 36 MESES	HARDWARE	02
3	EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 2 COM LICENÇA DE SOFTWARE E GARANTIA DO FABRICANTE PELO PERÍODO DE 36 MESES	HARDWARE	03
4	INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO ASSISTIDA	SERVIÇO	01
5	CAPACITAÇÃO TECNICA	SERVIÇO	02
6	BANCO DE HORAS TÉCNICA	SERVIÇO	300

6. ESPECIFICAÇÕES DETALHADAS E TÉCNICAS DOS MATERIAIS E EQUIPAMENTOS:

6.1. Os equipamentos devem ser novos, sem uso prévio e em perfeito estado de funcionamento. Não devem ser remanufaturado recondicionados, ou possuir reparos de qualquer espécie;
6.2. Todos os equipamentos devem ser acompanhados de todos os manuais e acessórios fornecidos pelo fabricante da solução;
6.3. Equipamentos, módulos, componentes, ou qualquer outra parte do OBJETO que a CONTRATANTE constate terem sido entregues já com defeito ou danificados devem ser trocados por outro equipamento, componente ou item novo, de mesma marca e modelo, com número de série diferente, em no máximo 30 dias úteis;
6.4. Equipamentos que a CONTRATANTE constate terem sido entregues com outras irregularidades (como, por exemplo, falta de manuais, software ou firmware incorreto, configuração de hardware incorreta, equipamento incorreto), devem se sanadas em no máximo 10 dias úteis;

6.5. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta.

6.6. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da empresa proponente.

6.7. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades.

6.8. Todos os equipamentos deverão ser fornecidos, instalados e configurados de forma que a solução final entregue esteja disponível para pleno funcionamento.

6.9. A empresa deverá comprovar possuir a qualificação técnica do fabricante necessária para a execução do pleno serviço de instalação do produto ofertado.

6.10. Deverá ser comprovado em proposta, obrigatoriamente, todos os itens e subitens das especificações técnicas, apontado a página do documento onde consta a comprovação do item/subitem proposto. A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da proponente;

6.11. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede, e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.);

6.12. Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem qualquer ônus adicionais e independentemente da existência de contrato de manutenção;

6.13. Todos os equipamentos devem possuir selo de certificação/homologação pela Anatel;

6.14. A garantia de funcionamento dos equipamentos deverá ser contada a partir do Recebimento Definitivo e as condições de garantia exigidas neste Termo de Referência serão de responsabilidade do fabricante.

6.15. Para todos os equipamentos, durante o prazo de garantia, deverá ser substituída, sem ônus para o CONTRATANTE, parte ou peça defeituosa, **com prazo máximo para atendimento no local (on-site)** e reparo/solução do problema que ocasionou o chamado, contado a partir da abertura do chamado, de até **48 (quarenta e oito) horas**.

6.16. Os chamados abertos terão seus tempos contabilizados a partir do momento em que o prestador do serviço for notificado da anomalia pela área técnica deste Licitante, seja por contato telefônico, ou sistema de abertura de chamados técnicos por meio eletrônico (via Internet);

6.17. O período de disponibilidade para serviços de suporte e manutenção deverá ser de 24/7 (24 horas por dia, 7 dias da semana), e atendimento de solução de hardware a ser prestado pelo próprio fabricante, comprovada através de declaração com firma reconhecida.

6.18. Para todos os equipamentos, caso o fornecedor não seja o próprio fabricante, deverá apresentar o seguinte documento: Declaração do fabricante de que o licitante é revendedor autorizado, que todos os produtos ofertados são de sua fabricação (própria ou OEM), que a configuração ofertada é totalmente funcional, que todas as condições de garantia exigidas neste termo serão de responsabilidade do fabricante.

6.19. Os equipamentos descritos, devem ser do mesmo fabricante;

6.20. Proteção ao Investimento:

6.21. Os equipamentos ofertados não podem estar em condição de fim-de-vida (end-of-life), isto é, devem estar em linha atual do fabricante.

6.22. Em caso de o equipamento entrar em condição de fim-de-vida (end-of-life), o fabricante deverá manter todo o suporte de hardware e atualização de firmware pelo período de 5 anos a contar da data da publicação do fim-devida (end-of-life) no site do fabricante;

6.23. Suporte Técnico:

6.24. Deverá ser fornecido o serviço de suporte técnico do fabricante por telefone (DDG) ou e-mail para abertura de chamado por todo o período de garantia ON SITE e manutenção dos equipamentos;

6.25. Deve incluir suporte à operação e configuração do equipamento, troubleshooting de problemas de configuração, firmware e hardware;

6.26. Período do serviço do fabricante com pelo menos 36 (trinta e seis) meses com cobertura 24/7 (24 horas por dia, 7 dias por semana);

6.27. Possuir suporte remoto para a solução de problemas comuns de suporte;

6.28. A proponente deve realizar atendimento on-site em até 05 (cinco) dias úteis, com tempo de atendimento contado a partir da abertura do chamado;

6.29. O FABRICANTE deverá possuir Central de Atendimento online para abertura dos chamados de garantia, comprometendo-se a manter estes registros constando a descrição do problema;

6.30. Todos os itens de software que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do FABRICANTE.

6.31. O serviço de garantia e suporte deverá ser do FABRICANTE do equipamento ou por assistência técnica qualificada e indicada por este através de declaração.

7. DESCRIÇÃO E ESPECIFICAÇÕES TÉCNICAS (MÍNIMAS):

7.1. ITEM 01 - PONTO DE ACESSO SEM FIO:

7.1.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador sem fio;

7.1.2. Com o intuito de garantir total compatibilidade, gestão facilitada e integração, a solução de ponto de acesso sem fio deve ser da mesma marca dos ITENS 2 e 3 deste termo de referência;

7.1.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

7.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

7.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

7.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

7.1.7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

7.1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

7.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

7.1.10. Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente;

7.1.11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

7.1.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

7.1.13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

7.1.14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

7.1.15. Cada ponto de acesso sem fio deverá ser entregue com 01(um) injetor PoE totalmente compatível ao modelo de ponto de acesso sem fio ofertado;

7.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

7.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

7.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

7.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

7.1.20. Deve permitir operação em modo Mesh;

7.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

7.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

7.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

7.1.24. Deve suportar OFDMA;
7.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
7.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
7.1.27. Deve suportar BSS Coloring;
7.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
7.1.29. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);
7.1.30. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;
7.1.31. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
7.1.32. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
7.1.33. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
7.1.34. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
7.1.35. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
7.1.36. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
7.1.37. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
7.1.38. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
7.1.39. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
7.1.40. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
7.1.41. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
7.1.42. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
7.1.43. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
7.1.44. Deve implementar o padrão IEEE 802.11e;

7.1.45. Deve implementar o padrão IEEE 802.11h;
7.1.46. Deve implementar o padrão IEEE 802.3az;
7.1.47. Deve suportar ser gerenciado via SNMP;
7.1.48. Deve suportar consultas via REST API;
7.1.49. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
7.1.50. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
7.1.51. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
7.1.52. Deve possuir indicadores luminosos (LED) para indicação de status;
7.1.53. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
7.1.54. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
7.1.55. Deve possuir certificado emitido pela Wi-Fi Alliance;
7.1.56. Deve estar homologado pela ANATEL na data de execução do pregão;

7.2. ITEM 02 - EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 1

7.2.1. O equipamento deve possuir, no mínimo, as seguintes características:
7.2.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
7.2.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
7.2.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
7.2.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
7.2.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
7.2.1.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações.

7.2.2. FUNCIONALIDADES DE REDE E FIREWALL

7.2.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
7.2.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
7.2.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
7.2.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

7.2.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

7.2.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

7.2.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

7.2.2.8. Deverá suportar sFlow ou Netflow;

7.2.2.9. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

7.2.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

7.2.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

7.2.2.12. Deve implementar o protocolo ECMP;

7.2.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

7.2.2.14. Enviar log para sistemas de monitoração externos;

7.2.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

7.2.2.16. Deve possui mecanismos de proteção anti-spoofing;

7.2.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

7.2.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.2.2.19. Suportar OSPF graceful restart;

7.2.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.2.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

7.2.2.22. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

7.2.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

7.2.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

7.2.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

7.2.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

7.2.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

7.2.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

7.2.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

7.2.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
7.2.2.31. Deverá suportar controle por zonas de segurança;
7.2.2.32. Deverá suportar controles de políticas por porta e protocolo;
7.2.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
7.2.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
7.2.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
7.2.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
7.2.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
7.2.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
7.2.2.39. Suporte a objetos e regras IPV6;
7.2.2.40. Suporte a objetos e regras multicast;
7.2.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

7.2.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

7.2.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
7.2.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
7.2.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
7.2.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
7.2.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
7.2.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
7.2.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
7.2.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
7.2.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

7.2.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

7.2.3.11. Atualizar a base de assinaturas de aplicações automaticamente;

7.2.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.2.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

7.2.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

7.2.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

7.2.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.2.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;

7.2.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

7.2.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

7.2.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

7.2.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

7.2.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

7.2.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

7.2.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

7.2.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

7.2.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

7.2.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

7.2.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.2.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

7.2.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

7.2.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.2.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

7.2.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

7.2.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

7.2.4.9. Deve permitir o bloqueio de vulnerabilidades;

7.2.4.10. Deve permitir o bloqueio de exploits conhecidos;

7.2.4.11. Deve incluir proteção contra-ataques de negação de serviços;

7.2.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

7.2.4.13. Detectar e bloquear a origem de portscans;

7.2.4.14. Bloquear ataques efetuados por worms conhecidos;

7.2.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.2.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

7.2.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

7.2.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

7.2.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.4.20. Identificar e bloquear comunicação com botnets;

7.2.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

7.2.4.22. Os eventos devem identificar o país de onde partiu a ameaça;

7.2.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

7.2.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

7.2.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.2.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

7.2.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

7.2.4.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

7.2.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

7.2.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

7.2.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

7.2.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

7.2.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

7.2.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

7.2.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

7.2.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;

7.2.5.8. Deve possuir a função de exclusão de URLs do bloqueio;

7.2.5.9. Permitir a customização de página de bloqueio;

7.2.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

7.2.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

7.2.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

7.2.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

7.2.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

7.2.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

7.2.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.2.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

7.2.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

7.2.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.2.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

7.2.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

7.2.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

7.2.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

7.2.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

7.2.7. FUNCIONALIDADE DE FILTRO DE DADOS

7.2.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

7.2.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.2.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.2.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

7.2.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

7.2.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

7.2.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

7.2.9. FUNCIONALIDADE DE VPN

7.2.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;

7.2.9.2. Suportar IPSec VPN;

7.2.9.3. Suportar SSL VPN;

7.2.9.4. A VPN IPSEc deve suportar 3DES;

7.2.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

7.2.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

7.2.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

7.2.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

7.2.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

7.2.9.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper,

Palo Alto Networks, Fortinet, SonicWall;

7.2.9.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

7.2.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

7.2.9.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

7.2.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

7.2.9.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

7.2.9.16. Atribuição de DNS nos clientes remotos de VPN;

7.2.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

7.2.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

7.2.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);

7.2.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

7.2.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;

7.2.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

7.2.9.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

7.2.9.24. Deverá manter uma conexão segura com o portal durante a sessão;

7.2.9.25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

7.2.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

7.2.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.2.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

7.2.10.3. Endereço de origem;

7.2.10.4. Endereço de destino;

7.2.10.5. Usuário e grupo;

7.2.10.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.2.10.7. Por porta;

7.2.10.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

7.2.10.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima

permitida para aplicações do tipo best-effort não corporativas, tais como YouTube, Facebook, entre outros;

7.2.10.10. O QoS deve possibilitar a definição de fila de prioridade;

7.2.10.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

7.2.10.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.2.10.13. Suportar modificação de valores DSCP para o Diffserv;

7.2.10.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);

7.2.10.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

7.2.10.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

7.2.10.17. Deve possibilitar a definição de bandas distintas para download e upload;

7.2.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

7.2.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

7.2.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

7.2.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

7.2.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

7.2.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

7.2.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

7.2.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

7.2.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

7.2.11.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

7.2.11.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou

largura de banda;

7.2.11.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

7.2.11.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

7.2.11.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

7.2.11.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

7.2.11.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

7.2.11.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

7.2.11.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

7.2.11.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

7.2.11.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

7.2.11.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

7.2.11.21. A solução deve suportar nativamente conectores com clouds públicas;

7.2.11.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

7.2.11.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

7.2.11.24. Deve implementar balanceamento de link por hash do IP de origem;

7.2.11.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

7.2.11.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

7.2.11.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet,

e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

7.2.11.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

7.2.12. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

7.2.12.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

7.2.12.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

7.2.12.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

7.2.12.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

7.2.12.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

7.2.12.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

7.2.12.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

7.2.12.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

7.2.12.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

7.2.12.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

7.2.12.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado

localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

7.2.12.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

7.2.12.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

7.2.12.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

7.2.12.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

7.2.12.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

7.2.12.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

7.2.12.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

7.2.12.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

7.2.12.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

7.2.12.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

7.2.12.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso

devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

7.2.12.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

7.2.12.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

7.2.12.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

7.2.12.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

7.2.12.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

7.2.12.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

7.2.12.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

7.2.12.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

7.2.12.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

7.2.12.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

7.2.12.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

7.2.12.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

7.2.12.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

7.2.12.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

7.2.12.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos

de acesso que tenham este recurso;

7.2.12.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

7.2.12.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

7.2.12.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

7.2.12.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

7.2.12.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

7.2.12.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

7.2.12.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

7.2.12.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

7.2.12.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

7.2.12.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

7.2.12.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

7.2.12.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

7.2.12.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

7.2.12.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

7.2.12.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

7.2.12.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

7.2.12.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

7.2.12.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

7.2.12.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

7.2.12.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

7.2.12.58. A solução deve permitir a configuração do captive portal com endereço IPv6;

7.2.12.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

7.2.12.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

7.2.12.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

7.2.12.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

7.2.12.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

7.2.12.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

7.2.12.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

7.2.12.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

7.2.12.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

7.2.12.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

7.2.12.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

7.2.12.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

7.2.12.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

7.2.12.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

7.2.12.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

7.2.12.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

7.2.12.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

7.2.12.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

7.2.12.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

7.2.12.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

7.2.12.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

7.2.12.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

7.2.12.81. A solução deve possuir ferramentas de diagnósticos e debug;

7.2.12.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

7.2.12.83. A solução deve suportar comunicação com elementos externos através de REST API;

7.2.12.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

7.2.13. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

7.2.13.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

7.2.13.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

7.2.13.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

7.2.13.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

7.2.13.5. Deve montar a topologia da rede de maneira automática;

7.2.13.6. Deve ser capaz de configurar os switches da rede;

7.2.13.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

7.2.13.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

7.2.13.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

7.2.13.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

7.2.13.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

7.2.13.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

7.2.13.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

7.2.13.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

7.2.13.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

7.2.13.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

7.2.13.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

7.2.13.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

7.2.13.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

7.2.13.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

7.2.13.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

7.2.13.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

7.2.13.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

7.2.13.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

7.2.14. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE

7.2.14.1. Solução baseada em appliance. **Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais pode-riam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.**

7.2.14.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.

7.2.14.3. Deverá possuir licenças de Garantia, Atualizações de firmware, VPN, SD-WAN, pelo período exigido;

7.2.14.4. Capacidade mínima:

7.2.14.5. Firewall com capacidade mínima de processamento de 18 (dezoito) Gbps;

7.2.14.6. IPS com capacidade mínima de processamento de 2,5 (dois virgula cinco) Gbps

7.2.14.7. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de

processamento de 1 (um) Gbps.

7.2.14.8. Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps.

7.2.14.9. VPN com capacidade de, pelo menos, 11 (onze) Gbps de tráfego IPSec.

7.2.14.10. VPN SSL com capacidade de, pelo menos, 1 (um) Gbps de tráfego.

7.2.14.11. Deverá suportar, pelo menos, 1.300.000 (1 milhão e trezentos mil) conexões simultâneas.

7.2.14.12. Deverão ser licenciados para suportar, pelo menos, 500 (quinhentos) usuários de VPN SSL.

7.2.14.13. Deverá suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.

7.2.14.14. Deverá suportar, pelo menos, 1900 (mil e novecentos) túneis de VPN Site-Site.

7.2.14.15. Deverá suportar, pelo menos, 15.500 (quinze mil e quinhentos) túneis de VPN Client-Site.

7.2.15. INTERFACES DE REDE:

7.2.15.1. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45 e 2 (dois) 10ge SFP+

7.2.15.2. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade ativo-ativo e estar licenciados para operar desta forma.

7.2.15.3. Deverá possuir licença para número ilimitado de usuários e endereços IP.

7.2.15.4. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 64 (sessenta e quatro) Pontos de Acesso sem fio.

7.2.15.5. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 32(trinta e dois) equipamentos.

7.2.15.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.

7.2.15.7. Deverá incluir licença para a funcionalidade de VPN SSL.

7.2.15.8. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

7.3. ITEM 03 - EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 2

7.3.1. O equipamento deve possuir, no mínimo, as seguintes características:

7.3.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

7.3.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.3.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

7.3.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

7.3.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

7.3.1.6. Deverá possuir e estar licenciado pelo período de 36 (TRINTA E SEIS) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

7.3.2. FUNCIONALIDADES DE REDE E FIREWALL

7.3.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

7.3.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

7.3.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

7.3.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

7.3.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

7.3.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

7.3.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

7.3.2.8. Deverá suportar sFlow ou Netflow;

7.3.2.9. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

7.3.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

7.3.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

7.3.2.12. Deve implementar o protocolo ECMP;

7.3.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

7.3.2.14. Enviar log para sistemas de monitoração externos;

7.3.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

7.3.2.16. Deve possui mecanismos de proteção anti-spoofing;

7.3.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

7.3.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.3.2.19. Suportar OSPF graceful restart;

7.3.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.3.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

7.3.2.22. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

7.3.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

7.3.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

7.3.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

7.3.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

7.3.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

7.3.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

7.3.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

7.3.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

7.3.2.31. Deverá suportar controle por zonas de segurança;

7.3.2.32. Deverá suportar controles de políticas por porta e protocolo;

7.3.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

7.3.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

7.3.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

7.3.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

7.3.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

7.3.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

7.3.2.39. Suporte a objetos e regras IPV6;

7.3.2.40. Suporte a objetos e regras multicast;

7.3.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

7.3.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

7.3.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

7.3.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

7.3.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

7.3.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

7.3.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp,

rpc over http, gotomeeting, webex, evernote, google-docs;

7.3.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

7.3.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

7.3.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

7.3.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

7.3.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

7.3.3.11. Atualizar a base de assinaturas de aplicações automaticamente;

7.3.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.3.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

7.3.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

7.3.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

7.3.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.3.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;

7.3.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

7.3.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

7.3.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

7.3.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

7.3.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

7.3.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

7.3.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características

das aplicações como: Categoria da aplicação;

7.3.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

7.3.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

7.3.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

7.3.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.3.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

7.3.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

7.3.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.3.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

7.3.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

7.3.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

7.3.4.9. Deve permitir o bloqueio de vulnerabilidades;

7.3.4.10. Deve permitir o bloqueio de exploits conhecidos;

7.3.4.11. Deve incluir proteção contra-ataques de negação de serviços;

7.3.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

7.3.4.13. Detectar e bloquear a origem de portscans;

7.3.4.14. Bloquear ataques efetuados por worms conhecidos;

7.3.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.3.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

7.3.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

7.3.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

7.3.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.3.4.20. Identificar e bloquear comunicação com botnets;

7.3.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

7.3.4.22. Os eventos devem identificar o país de onde partiu a ameaça;

7.3.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

7.3.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e

maliciosos;

7.3.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.3.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

7.3.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

7.3.4.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

7.3.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

7.3.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

7.3.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

7.3.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

7.3.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

7.3.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

7.3.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

7.3.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;

7.3.5.8. Deve possuir a função de exclusão de URLs do bloqueio;

7.3.5.9. Permitir a customização de página de bloqueio;

7.3.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

7.3.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

7.3.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

7.3.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

7.3.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

7.3.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

7.3.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.3.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

7.3.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

7.3.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.3.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

7.3.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

7.3.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

7.3.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

7.3.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

7.3.7. FUNCIONALIDADE DE FILTRO DE DADOS

7.3.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

7.3.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.3.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.3.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

7.3.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

7.3.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

7.3.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

7.3.9. FUNCIONALIDADE DE VPN

7.3.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;
7.3.9.2. Suportar IPSec VPN;
7.3.9.3. Suportar SSL VPN;
7.3.9.4. A VPN IPSEc deve suportar 3DES;
7.3.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
7.3.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
7.3.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7.3.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
7.3.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
7.3.9.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
7.3.9.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
7.3.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
7.3.9.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
7.3.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
7.3.9.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
7.3.9.16. Atribuição de DNS nos clientes remotos de VPN;
7.3.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
7.3.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
7.3.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
7.3.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
7.3.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
7.3.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
7.3.9.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
7.3.9.24. Deverá manter uma conexão segura com o portal durante a sessão;
7.3.9.25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

7.3.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

7.3.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de

controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.3.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

7.3.10.3. Endereço de origem;

7.3.10.4. Endereço de destino;

7.3.10.5. Usuário e grupo;

7.3.10.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.3.10.7. Por porta;

7.3.10.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

7.3.10.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

7.3.10.10. O QoS deve possibilitar a definição de fila de prioridade;

7.3.10.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

7.3.10.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.3.10.13. Suportar modificação de valores DSCP para o Diffserv;

7.3.10.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);

7.3.10.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

7.3.10.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

7.3.10.17. Deve possibilitar a definição de bandas distintas para download e upload;

7.3.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

7.3.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

7.3.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

7.3.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

7.3.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

7.3.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

7.3.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

7.3.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

7.3.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

7.3.11.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

7.3.11.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

7.3.11.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

7.3.11.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

7.3.11.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

7.3.11.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

7.3.11.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

7.3.11.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

7.3.11.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade sede;

7.3.11.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

7.3.11.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

7.3.11.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

7.3.11.21. A solução deve suportar nativamente conectores com clouds públicas;

7.3.11.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

7.3.11.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

7.3.11.24. Deve implementar balanceamento de link por hash do IP de origem;

7.3.11.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

7.3.11.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

7.3.11.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

7.3.11.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

7.3.12. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

7.3.12.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

7.3.12.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

7.3.12.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

7.3.12.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

7.3.12.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

7.3.12.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

7.3.12.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

7.3.12.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

7.3.12.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a

integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

7.3.12.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

7.3.12.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

7.3.12.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

7.3.12.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

7.3.12.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

7.3.12.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

7.3.12.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

7.3.12.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

7.3.12.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

7.3.12.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

7.3.12.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

7.3.12.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

7.3.12.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

7.3.12.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub-redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

7.3.12.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

7.3.12.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

7.3.12.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

7.3.12.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

7.3.12.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

7.3.12.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

7.3.12.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

7.3.12.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

7.3.12.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

7.3.12.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído

em dB (SNR), capacidade MIMO e horário da associação;

7.3.12.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

7.3.12.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

7.3.12.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

7.3.12.37. A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;

7.3.12.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

7.3.12.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

7.3.12.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

7.3.12.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

7.3.12.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

7.3.12.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

7.3.12.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

7.3.12.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

7.3.12.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

7.3.12.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

7.3.12.48. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;

7.3.12.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

7.3.12.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

7.3.12.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

7.3.12.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

7.3.12.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

7.3.12.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

7.3.12.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

7.3.12.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

7.3.12.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

7.3.12.58. A solução deve permitir a configuração do captive portal com endereço IPv6;

7.3.12.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

7.3.12.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

7.3.12.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

7.3.12.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

7.3.12.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

7.3.12.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

7.3.12.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

7.3.12.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

7.3.12.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

7.3.12.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de

acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

7.3.12.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

7.3.12.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

7.3.12.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

7.3.12.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

7.3.12.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

7.3.12.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

7.3.12.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

7.3.12.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

7.3.12.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

7.3.12.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

7.3.12.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

7.3.12.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

7.3.12.81. A solução deve possuir ferramentas de diagnósticos e debug;

7.3.12.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

7.3.12.83. A solução deve suportar comunicação com elementos externos através de REST API;

7.3.12.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

7.3.13. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

7.3.13.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

7.3.13.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

7.3.13.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

7.3.13.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

7.3.13.5. Deve montar a topologia da rede de maneira automática;

7.3.13.6. Deve ser capaz de configurar os switches da rede;

7.3.13.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

7.3.13.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

7.3.13.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

7.3.13.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

7.3.13.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

7.3.13.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

7.3.13.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

7.3.13.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

7.3.13.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

7.3.13.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

7.3.13.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

7.3.13.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

7.3.13.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

7.3.13.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

7.3.13.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

7.3.13.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

7.3.13.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

7.3.13.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;8

7.3.14. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE

7.3.14.1. Solução baseada em appliance. **Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.**

7.3.14.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.

7.3.14.3. Deverá possuir licenças de Garantia, Atualizações de firmware, VPN, SD-WAN, pelo período exigido;

7.3.14.4. Capacidade mínima:

7.3.14.5. Firewall com capacidade mínima de processamento de 5 (cinco) Gbps;

7.3.14.6. IPS com capacidade mínima de processamento de 1 (um) Gbps.

7.3.14.7. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps.

7.3.14.8. Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps.

7.3.14.9. VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPSec.

7.3.14.10. VPN SSL com capacidade de, pelo menos, 450 (quatrocentos e cinquenta) Mbps de tráfego.

7.3.14.11. Deverá suportar 600.000 (seiscentos mil) conexões simultâneas.

7.3.14.12. Deverão ser licenciados para suportar, pelo menos, 190 (cento e noventa) usuários de VPN SSL.

7.3.14.13. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

7.3.14.14. Deverá suportar, pelo menos, 190 (cento e noventa) túneis de VPN Site-Site.

7.3.14.15. Deverá suportar, pelo menos, 220 (duzentos e vinte) túneis de VPN Client-Site.

7.3.15. INTERFACES DE REDE:

7.3.15.1. Deverá possuir, pelo menos, 05 (cinco) interfaces RJ 45.

7.3.15.2. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade ativo-ativo e estar licenciados para operar desta forma.

7.3.15.3. Deverá possuir licença para número ilimitado de usuários e endereços IP.

7.3.15.4. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 06 (seis) Pontos de Acesso sem fio.

7.3.15.5. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 06 (seis) equipamentos.

7.3.15.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.

7.3.15.7. Deverá incluir licença para a funcionalidade de VPN SSL.

7.3.15.8. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

7.4. ITEM 04 – INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO ASSISTIDA

7.4.1. PARA TODOS OS ITENS:

7.4.1.1. A CONTRATANTE deverá disponibilizar os pontos elétricos e lógicos necessários para a

realização da instalação física necessária.

7.4.1.2. Os equipamentos HARDWARE devem ser instalados fisicamente e configurados pela CONTRATADA de forma que após a conclusão estejam aptos ao uso.

7.4.1.3. Os locais a serem instalados serão definidos pela CONTRATANTE e sua equipe de TI;

7.4.1.4. A etapa de instalação deverá ocorrer com os seguintes critérios:

1	Planejamento da instalação incluindo identificação de pré-requisitos e plano de *rollback*;
2	Instalação física dos equipamentos no rack;
3	Atualização de drivers e *firmwares* dos equipamentos;
4	Realização de testes de conectividade;
5	Integração com *Microsoft Active Directory (single sign-on*);
6	Regras de roteamento, utilizando como base as regras atualmente em uso pela CONTRATANTE;
7	Regras de firewall, utilizando como base as regras atualmente em uso pela CONTRATANTE;
8	VPN: Configuração dos acessos externos
10	IPS, deverá ser configurado de acordo com os níveis de proteção e ações a serem definidas pela CONTRATANTE;
11	Filtro de conteúdo, de acordo com as categorias e ações de bloqueio definidas pela CONTRATANTE:
12	Proteção contra *Malwares*, deverá ser configurado de acordo com os níveis de proteção e ações a serem definidas pela CONTRATANTE;
13	Controle de aplicações, deverá ser configurado para bloquear ou liberar aplicações específicas de acordo com as informações fornecidas pela CONTRATANTE;
14	Balanceamento de carga entre dois links de internet dedicados de acordo com as configurações e parâmetros fornecidos pela CONTRATANTE;
15	Instalação e configuração da plataforma de emissão de relatórios da ferramenta;
16	Configuração de relatórios customizados, de acordo com a necessidade da CONTRATANTE;
17	Realizar backup das configurações;
18	Documentar todas as alterações realizadas no ambiente;

7.4.1.5. Instalar fisicamente os equipamentos em rack 19" (dezenove polegadas), bem como as interligações/conexões físicas que sejam necessárias. O rack de servidores localiza-se

atualmente no Datacenter SESC AMAPÁ; Atualizar Firmware dos equipamentos para a última versão estável recomendada;

7.4.1.6. Caso A licitante vencedora através de sua representatividade e legitimidade em pertencer ao programa de Parceiros do Fabricante e, ainda, ser declarado o Parceiro registrado no formulário de pré-engajamento emitido pelo Fabricante de que executará o atendimento das solicitações de instalação e migração, devendo portanto, a mesma possuir profissional qualificado e certificado pela fabricante, ao menos, com as certificações compatíveis ao Objeto desta licitação até a assinatura do contrato ou apresentar até a assinatura do contrato, os documentos da qualificação técnico-operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.

7.4.1.7. A comprovação do item anterior imediato, no caso do CMMI-Svc, se dará por meio de cópia autenticada do certificado emitido por uma agência certificadora independente (agências credenciadas pelo Software Engineering Institute - http://www.sei.cmu.edu) ou seu representante no Brasil;

7.4.1.8. Para a certificação MPS/BR-Serviços, a comprovação se dará por meio de cópia autenticada do certificado de qualidade MPS-BR-Sv emitido pela SOFTEX ou parceiro autorizado.

7.4.1.9. A qualquer tempo, o time técnico da CONTRATANTE poderá realizar visita às instalações da CONTRATADA para comprovar a adoção de processos aderentes à norma ISO NBR 20.000 na execução dos serviços previstos neste edital

7.4.1.10. Esta execução da instalação física e logica deverá ser de no máximo 72 (setenta e duas) horas uteis.

7.4.2. MIGRAÇÃO:

7.4.2.1. Deverá ser ofertado serviço de migração das regras de segurança do Firewall existente no equipamento atual de segurança deste REGIONAL DO SESC para o modelo ofertado neste edital.

7.4.2.2. Visando eliminar erros humano e redundâncias, deverá ser ofertado juntamente com o serviço de instalação, o serviço de migração com uso de ferramentas (software) que garantam a segurança e a automação do processo de forma a mitigar falhas de migração assim como o emprego de metodologias avançadas de processos automatizados por software.

7.4.2.3. Deverá ser informada a ferramenta de migração usada neste processo.

7.4.2.4. O tempo de execução do serviço de migração deve ser de no máximo 40 (quarenta) horas uteis;

7.4.3. OPERAÇÃO ASSISTIDA:

7.4.3.1. Para garantir a sustentação e o pleno funcionamento da solução, a CONTRATADA deverá

realizar, durante 10 (DEZ dias) corridos, após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida no ambiente instalado, esclarecendo dúvidas e realizando ajustes nas configurações visando a melhor utilização dos recursos oferecidos nos equipamentos que compõem a solução;

7.4.3.2. O serviço de operação assistida deverá ser realizado por técnico(s) plenamente qualificado(s), devendo possuir certificação emitida pelos fabricantes da solução ofertada, devendo ser prestada com acompanhamento da equipe técnica do Contratante

7.4.3.3. O período de operação assistida faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE;

7.4.3.4. A operação assistida da solução será utilizada para monitoria do ambiente, melhoria no ambiente, continuidade da solução, desenvolvimento de competências técnicas, e o seu escopo compreende:

7.4.3.5. Orientações sobre o ciclo de vida dos produtos adquiridos, contando com acesso ao conhecimento privilegiado de recursos acerca de arquitetura tecnológica, viabilizando a definição de parâmetros objetivos para o dimensionamento da infraestrutura;

7.4.3.6. Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (hardware e software);

7.4.3.7. Orientação quanto às melhores práticas para o correto ciclo de vida dos produtos adquiridos;

7.4.3.8. Análise técnica qualificada da compatibilidade e interoperabilidade dos produtos;

7.4.3.9. Aplicação de melhores práticas para o correto uso produtos adquiridos;

7.4.3.10. Estudo e reconfiguração do ambiente, quando esta demandar redimensionamento;

7.4.3.11. Estudo de revisão de arquitetura para melhoria de desempenho e disponibilidade;

7.4.3.12. Indicação de modelos de uso e planejamento de capacidade;

7.4.3.13. Identificação de melhorias e respectivo tratamento;

7.4.3.14. Suporte avançado técnico para estratégia e adequações nos ambientes;

7.4.3.15. Suporte avançado técnico para primeiro atendimento de anomalias dos produtos adquirido s e o correto repasse de atendimento de anomalias ao fabricante do produto caso seja necessário;

7.5. ITEM 05 - CAPACITAÇÃO TÉCNICA

7.5.1. CARACTERISTICAS GERAIS:

7.5.1.1. A capacitação técnica do tipo HANDS ON, deverá abordar todos os componentes da solução fornecida nos itens 1, 2 e 3, devendo ainda estar conforme a utilização da solução instalada no ambiente do SESC/AP, incluindo parametrizações e customizações, considerando os seguintes tópicos: Introdução, Instalação e Configuração, Administração e Gerenciamento, Implementação e Solução de Problemas

7.5.1.2. Requisitos dos serviços de instalação, configuração, documentação e treinamento do tipo hands-on, com os seguintes requisitos mínimos:

7.5.1.3. Registrar e licenciar o equipamento no portal do fabricante; configurar e habilitar os recursos de profiles de UTM (IPS, Application Control, Web Filter, Inspeção de SSL, Antivirus);

7.5.1.4. Configurar integração com o Active Directory;

7.5.1.5. Configurar alta disponibilidade (HA);

7.5.1.6. O acesso deverá ser baseado nos grupos de Active Directory;
7.5.1.7. Configurar Redes DMZ, Rede Local e Rede de Servidores;
7.5.1.8. Configurar SSLVPN integrada com o Active Directory;
7.5.1.9. Configurar VPN site-to-site;
7.5.1.10. Configurar todas as portas de conectividades dos equipamentos;
7.5.1.11. Exportar e migrar para o novo firewall todas as regras de acesso, serviços, endereços e configurações do firewall em PRODUÇÃO utilizado atualmente;
7.5.1.12. Revisar todas as regras de acesso utilizadas atualmente no firewall do SESC AP
7.5.1.13. Realizar todas as configurações necessárias para a implantação de todas as funcionalidades permitidas pelo novo firewall;
7.5.1.14. Treinamento hands-on para 2 (dois) participantes com no mínimo 16 (dezesseis) horas;
7.5.1.15. Ao final do processo deve ser entregue documentação formal de todas as configurações, procedimentos de backup e restore, desastre e recuperação do ambiente firewall e de gerência, e definições utilizadas na instalação e ativação do conjunto, com detalhamento suficiente que permita aos técnicos responsáveis a reprodução das ações, se necessário;
7.5.1.16. Os serviços deverão ser prestados por profissionais qualificados pela fabricante, ao menos, com as certificações Network Security.

7.6. BANCO DE HORAS TÉCNICA

7.6.1. CARACTERÍSTICAS GERAIS:

13.1.1. Serviços especializados para novas demandas ou correção de problemas não previstos após instalação da solução contendo no mínimo, os seguintes requisitos:

7.6.1.1. Visando garantir o perfeito funcionamento da solução após implementação, levando em consideração de ser uma solução nova para o time técnico da CONTRATANTE, mesmo após treinamento sobre as funcionalidades e operação assistida, deverá ser ofertado serviço de banco de horas técnica em caso de intercorrências que prejudiquem o bom funcionamento e que necessitem de intervenção no ambiente da CONTRATANTE por time técnico qualificado para tal resolução por parte da CONTRATADA.
7.6.1.2. O serviço deverá ser prestado preferencialmente de forma remota;
7.6.1.3. O serviço especializado será demandado através de Ordens de Serviço (OS) prevendo o quantitativo a serem consumidos, o período de execução e a descrição dos serviços a serem executados.
7.6.1.4. O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculadas ao item da OS. Qualquer alteração na quantidade de horas deverá ser justificada e previamente aprovada pela CONTRATANTE.
7.6.1.5. Os serviços proporcionais de gerenciamento de projetos e liderança técnica deverão estar incluídos dentro do valor da hora.
7.6.1.6. O serviço especializado abrange as seguintes atividades, podendo através de livre acordo entre as partes através de comunicação formal abrangerem itens não contemplados neste edital:
7.6.1.7. Resolução de problemas críticos na infraestrutura de processamento, armazenamento, backup, firewall, virtualização e redes;

7.6.1.8. Revisões e/ou Alterações de configurações, novas instalações, atualização de versões de softwares ou firmwares;

7.6.1.9. Execução de testes programados de recuperação de desastres visando validar o plano de continuidade de negócios;

7.6.1.10. Treinamento para conscientização sobre ameaças cibernéticas.

7.6.1.11. Serviços consultivos, para apoiar a avaliar, melhorar e testar processos de resposta a incidentes críticos de segurança;

7.6.1.12. Serviço de consolidação em dashboard com inúmeros fatores de riscos externos, como: serviços e portas divulgados publicamente, credenciais vazadas, identificação de páginas web, domínios e perfis de redes sociais que tentem se passar por este SESC/DR/AP;

7.6.1.13. Serviço de Implantação e Configuração para Solução De Segurança e Gerência De Redes;

7.6.1.14. Serviço de Implantação e Configuração para Unidade Centralizada de Armazenamento de Logs e Relatoria;

7.6.1.15. Serviços Profissionais de Implantação e Configuração Unidade de Gerência Centralizada de Equipamentos

7.6.1.16. Treinamento para Solução de Segurança e Gerência de Redes NGFW

7.6.1.17. Instalação e configuração de Solução de Segurança e Gerência de Redes NGFW

7.6.1.18. Treinamento de Unidade de Gerência Centralizada de Equipamentos

7.6.1.19. Treinamento de Unidade Centralizada de Armazenamento de Logs e Relatoria Migrações de dados;

7.6.1.20. Diagnóstico de problemas de desempenho e planejamento de capacidade;

7.6.1.21. Recuperação de dados através de Software de Backup e Replicação

7.6.1.22. Recuperação de solução de segurança de dados em ambiente VMware.

7.6.1.23. Implementação de regras de segurança;

7.6.1.24. Configurações em ativos de rede;

7.6.1.25. Elaboração de documentação técnica e de usuário;

7.6.1.26. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE.

7.6.1.27. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas.

7.6.1.28. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;

7.6.1.29. Realização de operação assistida e monitoramento de ambientes entregues com a solução.

7.6.1.30. Orientar na utilização dos softwares instalados no CONTRATANTE com a utilização das melhores práticas e orientações dos fabricantes;

7.6.1.31. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no CONTRATANTE minimizando impactos;

7.6.1.32. Apoiar na configuração/parametrização do sistema em novas máquinas;

7.6.1.33. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do CONTRATANTE;

7.6.1.34. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;

7.6.1.35. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning,

disponibilidade e confiabilidade em ambientes;

7.6.1.36. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;

7.6.1.37. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE;

7.6.1.38. Esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE.

7.6.1.39. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;

7.6.1.40. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;

7.6.1.41. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;

7.6.1.42. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;

7.6.1.43. A licitante deverá possuir uma ferramenta de SERVICE DESK on-line e que siga as melhores práticas da certificação ITIL para a abertura e gerenciamento de chamados na utilização dos bancos de horas, a fim de acompanhar o tempo de resolução para cada atividade (SLA), bem como disponibilizá-los em filas de priorizações para cada ocorrência, serviço e/ou incidente.

7.6.1.44. A ferramenta mencionada deverá permitir que a CONTRATANTE realize abertura de chamados através de e-mail, portal na Internet e/ou aplicativo de celular, sendo que cada chamado deverá possuir um código de identificação único que permita a sua rápida identificação.

7.6.1.45. O sistema deverá permitir o acompanhamento em tempo real pela CONTRATANTE dos chamados abertos e seus respectivos status, além de permitir a visualização do histórico de todos os chamados finalizados.

7.6.1.46. Para melhor gerenciamento dos chamados pela CONTRATADA, o sistema deverá possuir um painel (dashboard) que possua gráficos e outros tipos de visualizadores, além de permitir a geração de relatórios conforme necessidade e solicitação da CONTRATANTE.

7.6.1.47. Para fins de comprovação, o licitante deverá informar o nome da ferramenta de service desk utilizada.

7.6.1.48. Todo processo do serviço realizado deverá ser demonstrado em relatórios com todos os seus detalhes da sua execução.

7.6.1.49. Após a abertura de um chamado no sistema, o primeiro atendimento deverá ocorrer de forma remota para melhor entendimento do cenário e sua possível solução. Todavia, caso o atendimento remoto não seja suficiente para conclusão do chamado, então o atendimento deverá ser realizado de forma on-site, ou seja, de forma presencial no endereço da CONTRATANTE.

7.6.1.50. Quanto remoto, o atendimento será feito por ferramenta que irá contabilizar o tempo de acesso e trabalho, a fim de validar a consumação do banco de horas;

8. QUALIFICAÇÃO TÉCNICA

8.1. Para fins de demonstração de aptidão técnica e garantir a contratação de uma empresa que detenha a expertise mínima necessária e qualificação para entrega dos objetos e os serviços solicitados neste termo, será exigido das proponentes licitantes, a comprovação de expertise em objeto pertinente e compatível.

8.2. A Empresa deverá comprovar, através de, no mínimo 01 (um) Atestado de Capacidade Técnica (ACT), emitido por pessoa jurídica de direito público ou de direito privado, ter fornecido e instalado, configurado por meio de equipamentos e softwares, solução(ões) de porte similar ou igual ao objeto descrito neste Termo de Referência. O referido atestado deverá ser emitido em papel timbrado do emissor, contendo a identificação do órgão e do responsável pelo atestado, detalhamento do objeto e dos itens fornecidos, contendo ainda nome, telefone e e-mail do responsável pela emissão do atestado, para fins de diligência. Tal exigência se faz necessária também, para verificar a experiência e a habilidade técnica da Licitante na execução do objeto desta licitação.

8.3. A licitante deverá ser autorizada, através de certificados atualizados do fabricante do produto a ser entregue e compatíveis ao objeto e/ou declarações de parcerias com o(s) fabricante(s) dos equipamentos e softwares, a comercializar e implementar estas soluções ofertadas.

8.4. Tal previsão se faz necessária, tendo em vista os riscos relacionados à manutenção, apoio, atualizações e demais exigências técnicas necessárias que são providas pelo fabricante da solução e uma empresa que somente comercializa não pode se responsabilizar.

8.5. Na apresentação da proposta, é obrigatória a comprovação técnica de todas as características exigidas nos itens e subitens, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da empresa proponente.

8.6. Como condição para atender os requisitos de qualificação técnica na prestação dos serviços do presente lote, a licitante vencedora deverá apresentar até a assinatura do contrato, os documentos da qualificação técnico-operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.

8.7. A comprovação do item anterior imediato, no caso do CMMI-Svc, se dará por meio de cópia autenticada do certificado emitido por uma agência certificadora independente (agências credenciadas pelo Software Engineering Institute - http://www.sei.cmu.edu) ou seu representante no Brasil;

8.8. Para a certificação MPS/BR-Serviços, a comprovação se dará por meio de cópia autenticada do certificado de qualidade MPS-BR-Sv emitido pela SOFTEX ou parceiro autorizado.

8.9. A qualquer tempo, o time técnico da CONTRATANTE poderá realizar visita às instalações da CONTRATADA para comprovar a adoção de processos aderentes à norma ISO NBR 20.000 na

execução dos serviços previstos neste edital

8.10. A licitante deverá possuir uma ferramenta de SERVICE DESK on-line e que siga as melhores práticas da certificação ITIL para a abertura e gerenciamento de chamados na utilização dos bancos de horas, a fim de acompanhar o tempo de resolução para cada atividade (SLA), bem como disponibilizá-los em filas de priorizações para cada ocorrência, serviço e/ou incidente.

8.11. Em caso de a licitante vencedora através de sua representatividade e legitimidade em pertencer ao programa de Parceiros do Fabricante do produto ofertado, tiver como Executante do Projeto o próprio Fabricante para atender aos requisitos de serviço dos ITENS do presente lote, as exigências mencionadas nos itens **8.10** ficam desobrigadas de suas exigências e apresentação de certificações de serviço, uma vez que o próprio Fabricante da Solução de segurança é quem executará os serviços do supracitado lote, conforme discriminado neste Termo de Referência em cada uma de suas etapas. Logo, a licitante vencedora deverá apresentar o formulário de pré-engajamento emitido pelo fabricante que contenha o compromisso de execução do projeto pelo fabricante direcionado a este edital.

8.12. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta.

8.13. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades.

9. CONDIÇÕES DE ENTREGA COM SERVIÇO DE INSTALAÇÃO DO FIREWALL:

9.1. A entrega do objeto deste instrumento deverá ser realizada no prazo de até 60 (sessenta) dias corridos, a contar da data de recebimento da Ordem de Compra – OC, expedido pela Coordenadoria de Material e Patrimônio do Sesc Amapá, onde constará o item e a quantidade conforme necessidade do SESC/AP;

9.2. O equipamento deve no ato da entrega estar acompanhado da nota fiscal;

9.3. O objeto deste Termo de Referência deverá ser entregue na sala da Coordenadoria de Tecnologia da Informação - CTIN do Sesc Amapá, localizado na Rua Jovino Dinoá, nº 4311, Bairro: Beirol, Macapá-AP, CEP: 68.902-030, nos seguintes dias e horários: de segunda-feira a sexta-feira das 08h às 11h e das 14h às 17h;

9.4. O recebimento provisório será realizado dentro do prazo máximo de 03 (três) dias úteis, contados da data de entrega no SESC/AP para verificação e validação dos equipamentos com as especificações exigidas;

9.5. O recebimento definitivo será realizado dentro do prazo máximo de 05 (cinco) dias úteis, contados do recebimento provisório, para verificação da qualidade e quantidade do equipamento e consequente aceitação;

9.6. O objeto deverá ser entregue devidamente embalado, de forma a não ser danificado durante as operações de transporte, carga e descarga, contendo na embalagem marca, prazo de validade, procedência e demais características que o identifiquem. Não sendo aceitos, de imediato, produtos

cuja embalagem apresente sinais de violação;

9.7. O aceite do objeto deste instrumento pelo Sesc Amapá, não exclui a responsabilidade civil do fornecedor, por vícios de quantidade, de qualidade ou técnico dos produtos, ou por desacordo com as especificações estabelecidas neste instrumento e edital, verificadas posteriormente;

9.8. O Fornecedor deverá entregar o produto rigorosamente dentro do prazo estipulado e com validade não inferior a 36 (trinta e seis) meses, de acordo com as especificações constantes neste instrumento;

9.9. As despesas de frete/embalagem deverão estar inclusas no preço proposto, e em hipótese alguma poderão ser destacadas quando da emissão da nota fiscal/fatura.

10. OBRIGAÇÕES DA CONTRATANTE:

10.1. Comunicar à Contratada toda e quaisquer ocorrências relacionadas com a contratação dos serviços.

10.2. Promover o acompanhamento e fiscalização, comunicando por escrito ou por telefone a CONTRATADA quaisquer ocorrências, irregularidade ou deficiência, relacionada com o fornecimento do equipamento;

10.3. Efetuar o pagamento pelo fornecimento realizado, após devidamente atestada a nota fiscal/fatura, de acordo com as condições e preços pactuados;

10.4. Verificar a qualidade do serviço em conformidade com as especificações técnicas exigidas neste Termo de Referência;

10.5. Notificar, formal e tempestivamente, a CONTRATADA sobre irregularidades observadas no cumprimento do Contrato.

10.6. . Designar um colaborador como Fiscal de Contrato, que deverá acompanhar e fiscalizar os técnicos da CONTRATADA em todas as visitas, comprovar e relatar, por escrito, as eventuais irregularidades na prestação de serviços, sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado, ou por outro motivo que caracterize a necessidade de tal medida;

10.7. Rejeitar, no todo ou em parte, o equipamento que a empresa vencedora entregar fora das especificações exigidas;

10.8. Solicitar o afastamento de qualquer profissional que não estiver apto às obrigações estabelecidas no contrato ou que não tenha comportamento adequado no serviço;

10.9. Prestar informações e esclarecimentos que venham a ser solicitados pela Contratada.

11. OBRIGAÇÕES DA CONTRATADA:

11.1. Realizar as entregas e prestar os serviços de acordo com todas as exigências contidas no Termo de Referência;

11.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;

11.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízo, de qualquer natureza, que causar a CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas;

11.4. Atender às determinações e exigências formuladas pela CONTRATANTE;

11.5. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

11.6. A CONTRATADA responderá por todos os vícios e defeitos dos serviços durante o período de vigência do contrato;

11.7. Efetuar o pagamento de todos os impostos, taxas e demais obrigações fiscais incidentes ou que vierem a incidir;

11.8. Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação, apresentando os documentos que comprovem tal regularidade junto com a nota fiscal/fatura resultante do fornecimento do contrato, quais sejam:

11.9. Prova de regularidade relativa à Seguridade Social;

11.10. Certidão conjunta relativa aos tributos federais e a Dívida Ativa da União;

11.11. Certidões de regularidade perante a Fazenda Estadual, Municipal ou Distrital, conforme o tipo de prestação;

11.12. Certidão de regularidade do FGTS;

11.13. Certidão negativa de débitos trabalhistas.

11.14. Não transferir a outrem, no todo ou em parte, a responsabilidade assumida, sem prévia e expressa anuência do Sesc/AP;

11.15. Repor as suas expensas os produtos nos quais forem constatadas irregularidades imediatamente, contados da notificação feita pelo SESC/AP sem ônus para a CONTRATANTE;

11.16. Efetuar a entrega do equipamento de acordo com os prazos, especificações e demais condições de fornecimento constantes no edital;

11.17. Apresentar justificativa dirigida à autoridade competente no prazo de 24 (vinte e quatro horas) anterior à data prevista para entrega do objeto quando da previsão de eventual atraso na entrega;

11.18. Arcar com todas as despesas decorrentes da contratação do objeto deste termo, inclusive locomoção, seguro de acidentes, impostos, contribuição previdenciárias, encargos trabalhistas, comerciais e outras decorrentes do fornecimento dos equipamentos;

11.19. Fornecer produtos livres de quaisquer tipos de vício ou características que venham a prejudicar o desenvolvimento das atividades do Sesc/DR/AP;

11.20. Equipamentos, módulos, componentes, ou qualquer outra parte do OBJETO que a CONTRATANTE constate terem sido entregues já com defeito ou danificados devem ser trocados por outro equipamento, componente ou item novo, de mesma marca e modelo, com número de série diferente, em no máximo 30 dias úteis;

11.21. Responsabilizar-se a qualquer tempo pela qualidade do equipamento fornecido ao CONTRATANTE, inclusive no tocante a eventuais problemas e prejuízos posteriores, ocorridos pela inobservância de especificações constantes no Edital e nesse contrato;

11.22. Responsabilizar-se pelos prejuízos financeiros decorrentes da não entrega dos equipamentos solicitados;

11.23. Entregar o equipamento com garantia de, no mínimo 36 (trinta e seis) meses;

11.24. Cumprir fielmente com todas as condições ora pactuadas, neste instrumento, e de acordo com as exigências desse termo de referência.

12. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

12.1. Durante a vigência do Contrato, a execução dos serviços será acompanhada e fiscalizada pela Coordenação de Tecnologia da Informação - CTIN;

12.2. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada pelos danos causados ao Contratante ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos;

12.3. O Sesc/DR/AP se reserva o direito de rejeitar, no todo ou em parte, o serviço prestado, se em desacordo com o Contrato, e o pagamento só será realizado após o aceite do serviço;

12.4. Quaisquer exigências da fiscalização, inerentes ao objeto do Contrato, deverão ser prontamente atendidas pela Contratada, sem ônus adicional para o Contratante.

13. CONDIÇÕES DE PAGAMENTO

13.1. O pagamento efetuado através de transferência bancaria à empresa serão realizados na Coordenadoria de Tesouraria do Sesc/DR/AP, nos seguintes dias e horários: segundas-feiras das 15h às 17h30; nas quartas-feiras das 9h às 11h30 e das 15h às 17h30 e nas sextas-feiras das 9h às 11h30, devendo, a CONTRATADA, apresentar os seguintes documentos:

13.2. Carimbo contendo CNPJ e razão social da empresa e documento oficial com foto, em se tratando do proprietário/sócio da CONTRATADA;

13.3. Carimbo contendo CNPJ e razão social da empresa, documento oficial com foto e procuração com poderes especiais devidamente registrados em cartório, em se tratando de procurador.

13.4. O Sesc/AP se reserva o direito de não aceitar notas fiscais que não estejam acompanhadas dos documentos que comprovem quitação das obrigações. O não aceite das referidas notas fiscais não gera o dever de pagar enquanto houver pendência de obrigação que tenha sido imposta em virtude de penalidade ou inadimplemento apontando pela fiscalização. Cessadas essas causas, os pagamentos serão retomados sem que haja qualquer direito a atualização monetária;

13.5. O Sesc/AP terá o prazo máximo de até 20 (vinte) dias para efetuar o pagamento, após o recebimento da nota fiscal e após ter sido atestada e correspondente ao fornecimento do objeto desta licitação;

13.6. Caso não haja expediente no Sesc/DR/AP no dia do vencimento da Nota Fiscal, fica o pagamento prorrogado para o 1º dia útil subsequente;

13.7. A CONTRATADA poderá optar em receber o pagamento através de depósito bancário, devendo ser informado na Nota Fiscal o número da conta, agência e nome do banco;

13.8. Não serão pagas as notas fiscais que estiverem eivadas de vícios, desacompanhadas dos documentos comprobatórios de regularidades fiscais, trabalhistas e previdenciárias e seguintes, acompanhadas de documentos falsos/forjados ou quando da dependência de obrigações que tenham sido impostas em virtude de penalidades ou inadimplemento apontados pela fiscalização. Cessadas essas causas, o pagamento será retomado sem que haja direito a atualização monetária;

13.9. A inobservância de quaisquer condições de pagamento não gera ao Sesc/AP o dever de pagar.

14. PENALIDADES

14.1. O descumprimento de quaisquer cláusulas, bem como o atraso na prestação do serviço, sujeita

a CONTRATADA às seguintes sanções:

14.1.1. Advertência;

14.1.2. Multa compensatória de 10% (dez por cento) sobre o valor total do contrato;

14.1.3. Multa moratória de 0,2% (dois décimos por cento) por dia de atraso no cumprimento da obrigação sobre o valor total do contrato;

14.1.4. Rescisão unilateral do contrato;

14.1.5. Suspensão de licitar/contratar com o Sesc por prazo não superior a 03(dois) anos.

14.1.6. A critério do Sesc/AP as sanções poderão ser aplicadas cumulativamente ou não, de acordo com a gravidade da falta cometida, observados os princípios do contraditório e da ampla defesa.

15. RESCISÃO

15.1. O Contrato poderá ser rescindido unilateralmente pelo SESC/DR/AP, independente de notificação ou interpelação judicial, no caso de inadimplemento de qualquer de suas cláusulas ou condições, sujeitando à CONTRATADA às penalidades previstas na cláusula anterior deste instrumento, e em especial pelo (a):

15.1.1. Não cumprimento ou cumprimento irregular de cláusulas pactuadas, especificações ou prazos;

15.1.2. Subcontratação, total ou parcial do objeto deste Termo de Referência, sem prévia autorização escrita do Sesc/DR/AP, associação da CONTRATADA com outrem, cessão ou transferência total ou parcial, bem como a fusão, cisão ou incorporação, que afetem a boa execução do Contrato;

15.1.3. A morosidade do seu cumprimento, levando o Sesc/DR/AP a comprovar a impossibilidade da conclusão dos serviços nos 0s estipulados;

15.1.4. Paralisação dos serviços, sem justa causa ou prévia comunicação ao Sesc/AP;

15.1.5. Cometimento reiterado de falhas na execução do Contrato;

15.1.6. Decretação de Falência;

15.1.7. Dissolução da Empresa;

15.1.8. Razões de interesse público de alta relevância e amplo conhecimento;

15.1.9. Ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do Contrato;

15.1.10. Alteração social ou modificação da finalidade ou da estrutura da CONTRATADA, que prejudique a execução do Contrato;

15.1.11. Em qualquer das hipóteses acima referidas, a CONTRATADA deverá reparar integralmente os prejuízos causados ao Sesc/DR/AP, independente da aplicação das penalidades previstas neste instrumento, que poderão ser aplicadas no todo ou em parte, a critério exclusivo do Sesc/DR/AP;

15.1.12. Rescindido o Contrato por culpa da CONTRATADA, o Sesc/AP entregará os serviços, objeto deste instrumento, a quem julgar conveniente, sem qualquer consulta ou interferência da CONTRATADA, que responderá na forma legal e contratual pela infração ou execução inadequada que tenha dado causa à rescisão.

16. DA COMPLEMENTAÇÃO OU ACRESCIMO

16.1. No interesse da Administração do Sesc/DR/AP, o valor inicial atualizado do contrato poderá ser acrescido até o limite de 50% (cinquenta por cento), com fundamento do Art. 38 da Resolução Sesc 1.593/2024;

16.2. A contratada poderá a aceitar, nas mesmas condições licitada os acréscimos que se fizerem necessários.

17. DO REEQUILÍBRIO ECONÔMICO FINANCEIRO

17.1. A CONTRATADA deverá protocolar no setor de protocolo deste SESC/AP documento formal pleiteando o reequilíbrio econômico financeiro, especificando com clareza seus argumentos, fatos e documentos comprobatórios;

17.2. Nos casos de reajuste de preços, consignado no contrato, serão corrigidos mediante formalização do pedido pela CONTRATADA, observado o interregno mínimo de um ano, contado a partir da data de apresentação da proposta, pela variação do INPC Índice Nacional de Preços ao Consumidor, ocorrida nos últimos 12 (doze) meses;

17.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste;

17.4. Havendo a extinção deste índice, o contrato poderá ser reajustado por outro índice, mediante acordo entre as partes.

17.5. Nos casos revisão de preços, independentemente de prazos, não se pautando em índices específicos ou setoriais, a contratada deverá comprovar a alteração dos custos e insumos do contratado mediante apresentação de planilhas e documentos que demonstrem que, diante de fatos imprevisíveis ou previsíveis, mas de consequências incalculáveis, restou alterada a proporção entre encargos e vantagens originalmente prevista na proposta apresentada à época da licitação, não sendo suficiente a mera alegação de que houve a majoração dos preços pelo fornecedor.

18. VIGÊNCIA DO CONTRATO

18.1. A vigência do contrato será de 12 (doze) meses, podendo ser prorrogada até o limite de 60(sessenta) meses, de acordo com a Resolução Sesc 1.593/2024.

19. PRAZO DE VALIDADE DA PROPOSTA:

19.1. A proposta apresentada pelo licitante terá validade de 60 (sessenta) dias;

Informações validadas por:

Fábio Morais de oliveira
Coordenador de Tecnologia da Informação
SESC/DR/AP

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO II

CARTA DE CREDENCIAMENTO
(MODELO)

Em atendimento ao disposto no item **7.1.2** da Licitação na modalidade **Pregão Nº 24/0035-PG**, credenciamos o (a) Sr (a) ....., portador (a) da Carteira de Identidade nº..... e do CPF nº....., para que represente nossa empresa nesta Licitação, com poderes plenos para prestar esclarecimentos, assinar Atas, propostas e contratos, interpor recursos ou renunciar ao direito de interpô-lo e praticar tudo mais que seja necessário à participação de nossa empresa na Licitação.

Macapá-AP, ..…de.....de 2024.

_____
(Assinatura do representante legal da empresa)
(Nome do representante legal da empresa)

OBSERVAÇÃO: este documento deverá estar datado, ser preenchido em papel timbrado da empresa licitante, estar devidamente assinado por seu representante legal e reconhecido.

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO III

MODELO DE PROPOSTA
(em papel timbrado da empresa)

Ao
Serviço Social do Comércio - Sesc/DR/AP
Comissão Permanente de Licitação
Edital de Pregão Nº 24/0035-PG

DADOS DA EMPRESA	
RAZÃO SOCIAL:	**CNPJ:**
ENDEREÇO:	
CIDADE/ESTADO:	**CEP:**
TELEFONE:	**E-MAIL:**
NOME DA PESSOA QUE IRÁ ASSINAR O CONTRATO E OU ORDEM DE COMPRA	
RG:	**CPF:**

DADOS BANCÁRIOS PARA DEPÓSITO	
BANCO:	
AGÊNCIA:	
CONTA CORRENTE:	

A presente proposta tem como objeto o ***(descrever objeto)***, de acordo com as especificações mínimas obrigatórias constantes no termo de referência do Pregão nº. **24/0035-PG** do Departamento Regional do Sesc/DR/AP.

Item	**Quant.**	**Unid.**	**Marca**	**Descrição**	**Valor Unitário**
Valor Total					

Valor Global da Proposta: R$_____ (_____)

1. Validade da proposta: 60 (sessenta) dias.
2. Tipo de frete: CIF-Macapá;
3. Prazo limite de entrega: 60 (sessenta) dias corridos, a contar da data de recebimento da Ordem de Compra - OC

Informamos, por oportuno, que nos preços acima já estão computados todos os custos necessários decorrentes do fornecimento do objeto desta licitação, bem como, já estão inclusos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes e seguros (se for o caso), deslocamentos de pessoal e quaisquer outros que incidam direta e indiretamente nesta proposta.
LOCAL DE ENTREGA: SESC ARAXÁ, ALMOXARIFADO, sito a Rua Jovino Dinoá, 4311, Bairro Beirol, Macapá-AP, CEP 68.902-030.

Local, data

Assinatura do representante legal.

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO IV

DECLARAÇÃO DE CONHECIMENTO DO EDITAL E SEUS ANEXOS
(MODELO)

(Nome da empresa), CNPJ nº _____, sediada (endereço completo), declara para os devidos fins de comprovação junto à Comissão de Licitação, que referente ao processo licitatório na modalidade **Pregão Nº 24/0035-PG**, tomou conhecimento e aceitou previamente todas as condições estipuladas na referida licitação, bem como, expressar que o preço ofertado engloba todos os tributos, embalagens, encargos sociais, frete (CIF-Macapá), seguro e quaisquer outras despesas que incidam ou venham incidir sobre (o objeto desta licitação) _____ e a obrigatoriedade em realizar a entrega, conforme solicitado pelo Setor de Compras e Contratos do Sesc/DR/AP.

Local, data.

_____
Carimbo da empresa e assinatura do representante legal

OBSERVAÇÃO: A presente declaração **deverá** estar contida no envelope ‘’Documentos de Habilitação e Proposta’’, depois de elaborada em papel timbrado da licitante e devidamente assinada.

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO V

DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE IDADE
(MODELO)

Declara para os devidos fins de comprovação junto à Comissão de Licitação referente ao processo licitatório na modalidade **Pregão Nº 24/0035-PG**, que em atendimento ao disposto no **inciso XXXIII do art. 7º da Constituição Federal/88**, não possui em seu quadro de pessoal empregado com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 14 (quatorze) anos em qualquer trabalho, salvo na condição de aprendiz.

Declara, finalmente, que possui as condições operacionais necessárias à perfeita execução do objeto.

Local, data.

_____
Carimbo da empresa e assinatura do representante legal

OBSERVAÇÃO: A presente declaração **deverá** estar contida no envelope ‘’Documentos de Habilitação e Proposta’’, depois de elaborada em papel timbrado da licitante e devidamente assinada.

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO VI

MODELO DE DECLARAÇÃO DE DADOS BANCÁRIOS
(em papel timbrado da empresa)

A empresa _____, CNPJ: _____, com sede _____, DECLARA junto ao Sesc/DR/AP, que os dados bancários destinados ao recebimento de valores referentes ao fornecimento de material ou serviço prestado ao Sesc/DR/AP, são os informados abaixo:

PESSOA JURÍDICA CONTA CORRENTE		**PESSOA JURÍDICA POUPANÇA**	
BANCO Nº		**BANCO Nº**	
AGÊNCIA Nº		**AGÊNCIA Nº**	
CONTA CORRENTE Nº		**CONTA POUPANÇA Nº**	
VARIAÇÃO/OPERAÇÃO Nº		**VARIAÇÃO/OPERAÇÃO Nº**	
CNPJ Nº		**CNPJ Nº**	
DEPÓSITO IDENTIFICADO	**SIM ( ) NÃO ( )**		
CHAVE PIX			

E-mail:
Responsável Setor Financeiro:

O DEPÓSITO SERÁ EFETUADO CONFORME OS DADOS BANCÁRIOS INFORMADOS NESTA DECLARAÇÃO.

Obs.: Em caso de mudança das informações para depósito, fica o fornecedor responsável por encaminhar nova declaração para atualizar os dados.

Local e data:

_____
Assinatura do Representante Legal da Empresa
ou Rubrica com Carimbo.

PREGÃO SESC/DR/AP Nº 24/0035-PG

ANEXO VII

MINUTA DO CONTRATO

CONTRATO Nº _____

O **SERVIÇO SOCIAL DO COMÉRCIO - DEPARTAMENTO REGIONAL NO ESTADO DO AMAPÁ,** instituição de direito privado sem fins lucrativos, instituída pelo Decreto Federal nº 61.836, de 05 de dezembro de 1967, inscrita no CNPJ/MF sob o nº 03.593.251/0001-15, localizada na Rua Jovino Dinoá, n° 4311, bairro Beirol, CEP 68.902-030, Macapá-AP, doravante denominada **CONTRATANTE,** neste ato representado pelo **(QUALIFICAÇÃO COMPLETA)** e **(QUALIFICAÇÃO COMPLETA),** resolvem, nos termos que dispõe a legislação aplicável à espécie, e consoante às cláusulas e condições seguintes:

1. DA FUNDAMENTAÇÃO:

1.1. O contrato é regido pelo Regulamento de Licitações e Contratos do SESC, a Resolução SESC **nº 1.593/2024**, de 02 de maio de 2024.

2. DO OBJETO:

2.1. O objeto da presente contrato é o aquisição de solução de segurança com características de NEXT GENERATION Firewall - NGFW, para proteção de informações perimetral e de rede interna,incluindo as seguintes características: Firewall, controle de aplicações, administração de largura de banda (Quality of Service - QoS), Virtual Private Network - VPN, Intrusion Prevent System - IPS,prevenção contra ameaças de vírus, spywares e malwares, ataques “Zero Day e Advanced Persistent Threat - APTs, filtro de endereço (Uniform Resource Locator - URL), gerenciamento integrado e criação de relatórios, compondo assim uma plataforma de segurança integrada e robusta;

3. DA VIGÊNCIA:

3.1. A vigência deste Instrumento tem duração de 12 (doze) meses, a partir da data de sua assinatura, podendo ser prorrogado por até 36 (trinta e seis) meses, conforme art. 45 da resolução SESC **nº 1.593/2024**.

4. DA CLÁUSULA INTEGRANTE:

4.1. Constituem partes integrantes desta Ata, independentemente de transcrição, as condições estabelecidas no **Processo Licitatório SESC-DR/AP 24/0018-PG** e seus anexos, bem como as propostas de preço por item e documentos apresentados pelos participantes, devendo ser mantida a validade desses documentos durante toda a vigência deste instrumento, sendo facultado ao SESC-DR/AP solicitar, a qualquer momento, a apresentação dos documentos de forma a verificar se o participante ainda mantém as condições de habilitação.

5. DA DOTAÇÃO ORÇAMENTÁRIA:

5.1. As despesas decorrentes do objeto desta Ata de Registro de Preço correrão à conta 5.1.2.3 - Infraestrutura de Tecnologia da Informação e Telecomunicação, sendo subsidiado pelo Departamento Nacional.

6. DO REGISTRO DE MENOR PREÇO:

6.1. O valor total do Registro de Preço é de **R$ 000,00** (XXXXXXXXX);

6.2. O preço registrado, as especificações do objeto, a quantidade, fornecedor (es) e as demais condições ofertadas na (s) proposta (s) são as que seguem:

RAZÃO SOCIAL: XXXXXXXXXX

CNPJ: 0000000000

ENDEREÇO: XXXXXXXXXXXXXXXX

VALOR TOTAL: R$ 000,00

ITEM	DESCRIÇÃO TÉCNICA	UNIDADE	QTD
1	PONTO DE ACESSO SEM FIO	HARDWARE	40
2	EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 1 COM LICENÇA DE SOFTWARE E GARANTIA DO FABRICANTE PELO PERÍODO DE 36 MESES	HARDWARE	02
3	EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO – TIPO 2 COM LICENÇA DE SOFTWARE E GARANTIA DO FABRICANTE PELO PERÍODO DE 36 MESES	HARDWARE	03
4	INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO ASSISTIDA	SERVIÇO	01
5	CAPACITAÇÃO TECNICA	SERVIÇO	02
6	BANCO DE HORAS TÉCNICA	SERVIÇO	300

7. ESPECIFICAÇÕES DETALHADAS E TÉCNICAS DOS MATERIAIS E EQUIPAMENTOS:

7.1. Os equipamentos devem ser novos, sem uso prévio e em perfeito estado de funcionamento. Não devem ser remanufaturado recondicionados, ou possuir reparos de qualquer espécie;

7.2. Todos os equipamentos devem ser acompanhados de todos os manuais e acessórios fornecidos pelo fabricante da solução;

7.3. Equipamentos, módulos, componentes, ou qualquer outra parte do OBJETO que a CONTRATANTE constate terem sido entregues já com defeito ou danificados devem ser trocados por outro equipamento, componente ou item novo, de mesma marca e modelo, com número de série diferente, em no máximo 30 dias útil;

7.4. Equipamentos que a CONTRATANTE constate terem sido entregues com outras irregularidades (como, por exemplo, falta de manuais, software ou firmware incorreto, configuração de hardware incorreta, equipamento incorreto), devem se sanadas em no máximo 10 dias úteis;

7.5. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do

equipamento. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta;

7.6. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do contrato sem a devida comprovação acarretará a desclassificação da empresa proponente;

7.7. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades;

7.8. Todos os equipamentos deverão ser fornecidos, instalados e configurados de forma que a solução final entregue esteja disponível para pleno funcionamento;

7.9. A empresa deverá comprovar possuir a qualificação técnica do fabricante necessária para a execução do pleno serviço de instalação do produto ofertado;

7.10. Deverá ser comprovado em proposta, obrigatoriamente, todos os itens e subitens das especificações técnicas, apontado a página do documento onde consta a comprovação do item/subitem proposto. A simples repetição das especificações do acordo sem a devida comprovação acarretará a desclassificação da proponente;

7.11. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede, e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.);

7.12. Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem qualquer ônus adicionais e independentemente da existência de contrato de manutenção;

7.13. Todos os equipamentos devem possuir selo de certificação/homologação pela Anatel;

7.14. A garantia de funcionamento dos equipamentos deverá ser contada a partir do Recebimento Definitivo e as condições de garantia exigidas neste acordo serão de responsabilidade do fabricante;

7.15. Para todos os equipamentos, durante o prazo de garantia, deverá ser substituída, sem ônus para o CONTRATANTE, parte ou peça defeituosa, **com prazo máximo para atendimento no local (on-site)** e reparo/solução do problema que ocasionou o chamado, contado a partir da abertura do chamado, de até **48 (quarenta e oito) horas;**

7.16. Os chamados abertos terão seus tempos contabilizados a partir do momento em que o prestador do serviço for notificado da anomalia pela área técnica deste Licitante, seja por contato telefônico, ou sistema de abertura de chamados técnicos por meio eletrônico (via Internet);

7.17. O período de disponibilidade para serviços de suporte e manutenção deverá ser de 24/7 (24 horas por dia, 7 dias da semana), e atendimento de solução de hardware a ser prestado pelo próprio fabricante, comprovada através de declaração com firma reconhecida;

7.18. Para todos os equipamentos, caso o fornecedor não seja o próprio fabricante, deverá apresentar o seguinte documento: Declaração do fabricante de que o licitante é revendedor autorizado, que todos os produtos ofertados são de sua fabricação (própria ou OEM), que a configuração ofertada é totalmente funcional, que todas as condições de garantia exigidas neste acordo serão de responsabilidade do

fabricante;

7.19. Os equipamentos descritos, devem ser do mesmo fabricante;

7.20. Proteção ao Investimento;

7.21. Os equipamentos ofertados não podem estar em condição de fim-de-vida (end-of-life), isto é, devem estar em linha atual do fabricante;

7.22. Em caso de o equipamento entrar em condição de fim-de-vida (end-of-life), o fabricante deverá manter todo o suporte de hardware e atualização de firmware pelo período de 5 anos a contar da data da publicação do fim-devida (end-of-life) no site do fabricante;

7.23. Suporte Técnico;

7.24. Deverá ser fornecido o serviço de suporte técnico do fabricante por telefone (DDG) ou e-mail para abertura de chamado por todo o período de garantia ON SITE e manutenção dos equipamentos;

7.25. Deve incluir suporte à operação e configuração do equipamento, troubleshooting de problemas de configuração, firmware e hardware;

7.26. Período do serviço do fabricante com pelo menos 36 (trinta e seis) meses com cobertura 24/7 (24 horas por dia, 7 dias por semana);

7.27. Possuir suporte remoto para a solução de problemas comuns de suporte;

7.28. A proponente deve realizar atendimento on-site em até 05 (cinco) dias úteis, com tempo de atendimento contado a partir da abertura do chamado;

7.29. O FABRICANTE deverá possuir Central de Atendimento online para abertura dos chamados de garantia, comprometendo-se a manter estes registros constando a descrição do problema;

7.30. Todos os itens de software que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do FABRICANTE;

7.31. O serviço de garantia e suporte deverá ser do FABRICANTE do equipamento ou por assistência técnica qualificada e indicada por este através de declaração;

8. DESCRIÇÃO E ESPECIFICAÇÕES TÉCNICAS (MÍNIMAS):

8.1. ITEM 01 - PONTO DE ACESSO SEM FIO:

8.1.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador sem fio;

8.1.2. Com o intuito de garantir total compatibilidade, gestão facilitada e integração, a solução de ponto de acesso sem fio deve ser da mesma marca dos ITENS 2 e 3 deste acordo;

8.1.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

8.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

8.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

8.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

8.1.7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

8.1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de

segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

8.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

8.1.10. Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente;

8.1.11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

8.1.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

8.1.13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

8.1.14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC**;**

8.1.15. Cada ponto de acesso sem fio deverá ser entregue com 01(um) injetor PoE totalmente compatível ao modelo de ponto de acesso sem fio ofertado;

8.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

8.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.1.20. Deve permitir operação em modo Mesh;

8.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

8.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

8.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

8.1.24. Deve suportar OFDMA;

8.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

8.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

8.1.27. Deve suportar BSS Coloring;

8.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

8.1.29. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

8.1.30. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;
8.1.31. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
8.1.32. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
8.1.33. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
8.1.34. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
8.1.35. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
8.1.36. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
8.1.37. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
8.1.38. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
8.1.39. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
8.1.40. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
8.1.41. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
8.1.42. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
8.1.43. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
8.1.44. Deve implementar o padrão IEEE 802.11e;
8.1.45. Deve implementar o padrão IEEE 802.11h;
8.1.46. Deve implementar o padrão IEEE 802.3az;
8.1.47. Deve suportar ser gerenciado via SNMP;
8.1.48. Deve suportar consultas via REST API;
8.1.49. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
8.1.50. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

8.1.51. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
8.1.52. Deve possuir indicadores luminosos (LED) para indicação de status;
8.1.53. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
8.1.54. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste acordo deverão ser fornecidos,
8.1.55. Deve possuir certificado emitido pela Wi-Fi Alliance;
8.1.56. Deve estar homologado pela ANATEL na data de execução do pregão

8.2. ITEM 02 - EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO - TIPO 1:
8.2.1. O equipamento deve possuir, no mínimo, as seguintes características:
8.2.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração;
8.2.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
8.2.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
8.2.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
8.2.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
8.2.1.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações.
8.2.2. FUNCIONALIDADES DE REDE E FIREWALL
8.2.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
8.2.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
8.2.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
8.2.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
8.2.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
8.2.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
8.2.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
8.2.2.8. Deverá suportar sFlow ou Netflow;
8.2.2.9. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.2.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
8.2.2.11. Deve suportar o protocolo padrão da indústria VXLAN;
8.2.2.12. Deve implementar o protocolo ECMP;
8.2.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
8.2.2.14. Enviar log para sistemas de monitoração externos;
8.2.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
8.2.2.16. Deve possui mecanismos de proteção anti-spoofing;
8.2.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
8.2.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
8.2.2.19. Suportar OSPF graceful restart;
8.2.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
8.2.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
8.2.2.22. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
8.2.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
8.2.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;
8.2.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
8.2.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
8.2.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
8.2.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
8.2.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
8.2.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
8.2.2.31. Deverá suportar controle por zonas de segurança;
8.2.2.32. Deverá suportar controles de políticas por porta e protocolo;
8.2.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
8.2.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
8.2.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
8.2.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound):
8.2.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.2.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
8.2.2.39. Suporte a objetos e regras IPV6;
8.2.2.40. Suporte a objetos e regras multicast;
8.2.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente
8.2.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
8.2.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
8.2.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
8.2.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
8.2.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
8.2.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
8.2.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
8.2.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
8.2.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
8.2.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
8.2.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
8.2.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
8.2.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
8.2.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
8.2.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
8.2.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do

fabricante;
8.2.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
8.2.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;
8.2.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
8.2.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
8.2.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
8.2.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
8.2.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
8.2.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
8.2.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
8.2.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações

8.2.4. FUNCIONALIDADE DE PREVENÇÃODE INTRUSÃO E AMEAÇAS

8.2.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
8.2.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
8.2.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
8.2.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
8.2.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
8.2.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
8.2.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
8.2.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
8.2.4.9. Deve permitir o bloqueio de vulnerabilidades;
8.2.4.10. Deve permitir o bloqueio de exploits conhecidos;
8.2.4.11. Deve incluir proteção contra-ataques de negação de serviços;

8.2.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
8.2.4.13. Detectar e bloquear a origem de portscans;
8.2.4.14. Bloquear ataques efetuados por worms conhecidos;
8.2.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
8.2.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
8.2.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
8.2.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
8.2.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
8.2.4.20. Identificar e bloquear comunicação com botnets;
8.2.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
8.2.4.22. Os eventos devem identificar o país de onde partiu a ameaça;
8.2.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms;
8.2.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
8.2.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
8.2.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;
8.2.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
8.2.4.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

8.2.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

8.2.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
8.2.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
8.2.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
8.2.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
8.2.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.2.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
8.2.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;
8.2.5.8. Deve possuir a função de exclusão de URLs do bloqueio;
8.2.5.9. Permitir a customização de página de bloqueio;
8.2.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
8.2.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
8.2.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
8.2.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

8.2.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

8.2.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
8.2.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
8.2.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
8.2.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
8.2.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
8.2.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
8.2.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
8.2.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
8.2.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
8.2.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

8.2.7. FUNCIONALIDADE DE FILTRO DE DADOS

8.2.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS

Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
8.2.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.2.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.2.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

8.2.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

8.2.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
8.2.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

8.2.9. FUNCIONALIDADE DE VPN

8.2.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;
8.2.9.2. Suportar IPSec VPN;
8.2.9.3. Suportar SSL VPN;
8.2.9.4. A VPN IPSEc deve suportar 3DES;
8.2.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
8.2.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
8.2.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
8.2.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8.2.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
8.2.9.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
8.2.9.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
8.2.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
8.2.9.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
8.2.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
8.2.9.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
8.2.9.16. Atribuição de DNS nos clientes remotos de VPN;
8.2.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
8.2.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
8.2.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
8.2.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
8.2.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do

usuário autenticar na estação;
8.2.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
8.2.9.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
8.2.9.24. Deverá manter uma conexão segura com o portal durante a sessão;
8.2.9.25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

8.2.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

8.2.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
8.2.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
8.2.10.3. Endereço de origem;
8.2.10.4. Endereço de destino;
8.2.10.5. Usuário e grupo;
8.2.10.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
8.2.10.7. Por porta;
8.2.10.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
8.2.10.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort não corporativas, tais como YouTube, Facebook, entre outros;
8.2.10.10. O QoS deve possibilitar a definição de fila de prioridade;
8.2.10.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
8.2.10.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
8.2.10.13. Suportar modificação de valores DSCP para o Diffserv;
8.2.10.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);
8.2.10.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
8.2.10.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
8.2.10.17. Deve possibilitar a definição de bandas distintas para download e upload;

8.2.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

8.2.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
8.2.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
8.2.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de

usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

8.2.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

8.2.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

8.2.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

8.2.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

8.2.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

8.2.11.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

8.2.11.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

8.2.11.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

8.2.11.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

8.2.11.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

8.2.11.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

8.2.11.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

8.2.11.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

8.2.11.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

8.2.11.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

8.2.11.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
8.2.11.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;
8.2.11.21. A solução deve suportar nativamente conectores com clouds públicas;
8.2.11.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
8.2.11.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
8.2.11.24. Deve implementar balanceamento de link por hash do IP de origem;
8.2.11.25. Deve implementar balanceamento de link por hash do IP de origem e destino;
8.2.11.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
8.2.11.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;
8.2.11.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

8.2.12. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

8.2.12.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste acordo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
8.2.12.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
8.2.12.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
8.2.12.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
8.2.12.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
8.2.12.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
8.2.12.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8.2.12.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de

forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

8.2.12.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.2.12.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.2.12.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.2.12.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

8.2.12.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

8.2.12.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

8.2.12.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.2.12.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.2.12.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

8.2.12.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

8.2.12.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso

mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

8.2.12.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

8.2.12.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

8.2.12.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

8.2.12.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

8.2.12.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

8.2.12.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

8.2.12.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

8.2.12.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

8.2.12.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

8.2.12.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

8.2.12.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

8.2.12.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

8.2.12.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

8.2.12.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de

acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

8.2.12.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

8.2.12.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

8.2.12.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

8.2.12.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;

8.2.12.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

8.2.12.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

8.2.12.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

8.2.12.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

8.2.12.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

8.2.12.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

8.2.12.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

8.2.12.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

8.2.12.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

8.2.12.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

8.2.12.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

8.2.12.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

8.2.12.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs

para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
8.2.12.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
8.2.12.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
8.2.12.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
8.2.12.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
8.2.12.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
8.2.12.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
8.2.12.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
8.2.12.58. A solução deve permitir a configuração do captive portal com endereço IPv6;
8.2.12.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
8.2.12.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
8.2.12.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
8.2.12.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
8.2.12.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
8.2.12.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
8.2.12.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
8.2.12.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
8.2.12.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
8.2.12.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
8.2.12.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

8.2.12.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
8.2.12.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
8.2.12.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
8.2.12.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
8.2.12.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
8.2.12.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
8.2.12.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
8.2.12.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
8.2.12.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
8.2.12.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
8.2.12.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
8.2.12.81. A solução deve possuir ferramentas de diagnósticos e debug;
8.2.12.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
8.2.12.83. A solução deve suportar comunicação com elementos externos através de REST API;
8.2.12.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

8.2.13. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

8.2.13.1. Deve operar como ponto central para automação e gerenciamento dos switches deste acordo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
8.2.13.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
8.2.13.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
8.2.13.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
8.2.13.5. Deve montar a topologia da rede de maneira automática;
8.2.13.6. Deve ser capaz de configurar os switches da rede;
8.2.13.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

8.2.13.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
8.2.13.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
8.2.13.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
8.2.13.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
8.2.13.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
8.2.13.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
8.2.13.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
8.2.13.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
8.2.13.16. Deve ser capaz de configurar parâmetros SNMP dos switches;
8.2.13.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
8.2.13.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
8.2.13.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
8.2.13.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
8.2.13.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
8.2.13.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
8.2.13.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
8.2.13.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

8.2.14. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE

8.2.14.1. Solução baseada em appliance. **Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais pode-riam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.**
8.2.14.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.
8.2.14.3. Deverá possuir licenças de Garantia, Atualizações de firmware, VPN, SD-WAN, pelo período exigido;
8.2.14.4. Capacidade mínima:

8.2.14.5. Firewall com capacidade mínima de processamento de 18 (dezoito) Gbps;
8.2.14.6. IPS com capacidade mínima de processamento de 2,5 (dois virgula cinco) Gbps
8.2.14.7. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps.
8.2.14.8. Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps.
8.2.14.9. VPN com capacidade de, pelo menos, 11 (onze) Gbps de tráfego IPSec.
8.2.14.10. VPN SSL com capacidade de, pelo menos, 1 (um) Gbps de tráfego.
8.2.14.11. Deverá suportar, pelo menos, 1.300.000 (1 milhão e trezentos mil) conexões simultâneas.
8.2.14.12. Deverão ser licenciados para suportar, pelo menos, 500 (quinhentos) usuários de VPN SSL.
8.2.14.13. Deverá suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.
8.2.14.14. Deverá suportar, pelo menos, 1900 (mil e novecentos) túneis de VPN Site-Site.
8.2.14.15. Deverá suportar, pelo menos, 15.500 (quinze mil e quinhentos) túneis de VPN Client-Site.

8.2.15. INTERFACES DE REDE:
8.2.15.1. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45 e 2 (dois) 10ge SFP+
8.2.15.2. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade ativo-ativo e estar licenciados para operar desta forma.
8.2.15.3. Deverá possuir licença para número ilimitado de usuários e endereços IP.
8.2.15.4. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 64 (sessenta e quatro) Pontos de Acesso sem fio.
8.2.15.5. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 32(trinta e dois) equipamentos.
8.2.15.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.
8.2.15.7. Deverá incluir licença para a funcionalidade de VPN SSL.
8.2.15.8. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

8.3. ITEM 03 - EQUIPAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO - TIPO 2
8.3.1. O equipamento deve possuir, no mínimo, as seguintes características:
8.3.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
8.3.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
8.3.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
8.3.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
8.3.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

8.3.1.6. Deverá possuir e estar licenciado pelo período de 36 (TRINTA E SEIS) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

8.3.2. FUNCIONALIDADES DE REDE E FIREWALL

8.3.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.3.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

8.3.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.3.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

8.3.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.3.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

8.3.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.3.2.8. Deverá suportar sFlow ou Netflow;

8.3.2.9. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.3.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

8.3.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.3.2.12. Deve implementar o protocolo ECMP;

8.3.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.3.2.14. Enviar log para sistemas de monitoração externos;

8.3.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

8.3.2.16. Deve possui mecanismos de proteção anti-spoofing;

8.3.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

8.3.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

8.3.2.19. Suportar OSPF graceful restart;

8.3.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

8.3.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

8.3.2.22. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

8.3.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.3.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

8.3.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo

Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

8.3.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

8.3.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

8.3.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

8.3.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

8.3.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

8.3.2.31. Deverá suportar controle por zonas de segurança;

8.3.2.32. Deverá suportar controles de políticas por porta e protocolo;

8.3.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.3.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.3.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.3.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.3.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.3.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.3.2.39. Suporte a objetos e regras IPV6;

8.3.2.40. Suporte a objetos e regras multicast;

8.3.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

8.3.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

8.3.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

8.3.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.3.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

8.3.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

8.3.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

8.3.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de

aplicações conhecidas pelo fabricante independente de porta e protocolo;
8.3.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
8.3.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
8.3.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
8.3.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
8.3.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
8.3.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
8.3.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
8.3.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
8.3.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
8.3.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
8.3.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;
8.3.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
8.3.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
8.3.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
8.3.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
8.3.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
8.3.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
8.3.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
8.3.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

8.3.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

8.3.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

8.3.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.3.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.3.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

8.3.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

8.3.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.3.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.3.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.3.4.9. Deve permitir o bloqueio de vulnerabilidades;

8.3.4.10. Deve permitir o bloqueio de exploits conhecidos;

8.3.4.11. Deve incluir proteção contra-ataques de negação de serviços;

8.3.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

8.3.4.13. Detectar e bloquear a origem de portscans;

8.3.4.14. Bloquear ataques efetuados por worms conhecidos;

8.3.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

8.3.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.3.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

8.3.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

8.3.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

8.3.4.20. Identificar e bloquear comunicação com botnets;

8.3.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.3.4.22. Os eventos devem identificar o país de onde partiu a ameaça;

8.3.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

8.3.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

8.3.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques

baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

8.3.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

8.3.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

8.3.4.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

8.3.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

8.3.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

8.3.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

8.3.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.3.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

8.3.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.3.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

8.3.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;

8.3.5.8. Deve possuir a função de exclusão de URLs do bloqueio;

8.3.5.9. Permitir a customização de página de bloqueio;

8.3.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

8.3.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

8.3.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

8.3.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

8.3.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

8.3.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

8.3.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
8.3.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
8.3.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
8.3.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
8.3.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
8.3.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
8.3.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
8.3.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
8.3.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

8.3.7. FUNCIONALIDADE DE FILTRO DE DADOS

8.3.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
8.3.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.3.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.3.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

8.3.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

8.3.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
8.3.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

8.3.9. FUNCIONALIDADE DE VPN

8.3.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;
8.3.9.2. Suportar IPSec VPN;
8.3.9.3. Suportar SSL VPN;
8.3.9.4. A VPN IPSEc deve suportar 3DES;
8.3.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

8.3.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
8.3.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
8.3.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8.3.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
8.3.9.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
8.3.9.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
8.3.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
8.3.9.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
8.3.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
8.3.9.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
8.3.9.16. Atribuição de DNS nos clientes remotos de VPN;
8.3.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
8.3.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
8.3.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
8.3.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
8.3.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
8.3.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
8.3.9.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
8.3.9.24. Deverá manter uma conexão segura com o portal durante a sessão;
8.3.9.25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

8.3.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

8.3.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
8.3.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
8.3.10.3. Endereço de origem;
8.3.10.4. Endereço de destino;
8.3.10.5. Usuário e grupo;
8.3.10.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.3.10.7. Por porta;
8.3.10.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
8.3.10.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
8.3.10.10. O QoS deve possibilitar a definição de fila de prioridade;
8.3.10.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
8.3.10.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
8.3.10.13. Suportar modificação de valores DSCP para o Diffserv;
8.3.10.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);
8.3.10.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
8.3.10.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
8.3.10.17. Deve possibilitar a definição de bandas distintas para download e upload;

8.3.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

8.3.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
8.3.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
8.3.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
8.3.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
8.3.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
8.3.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
8.3.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
8.3.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
8.3.11.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
8.3.11.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na

qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
8.3.11.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
8.3.11.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
8.3.11.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
8.3.11.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
8.3.11.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
8.3.11.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
8.3.11.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade sede;
8.3.11.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
8.3.11.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
8.3.11.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;
8.3.11.21. A solução deve suportar nativamente conectores com clouds públicas;
8.3.11.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
8.3.11.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
8.3.11.24. Deve implementar balanceamento de link por hash do IP de origem;
8.3.11.25. Deve implementar balanceamento de link por hash do IP de origem e destino;
8.3.11.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
8.3.11.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de

falha no link principal;

8.3.11.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

8.3.12. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

8.3.12.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste acordo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

8.3.12.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

8.3.12.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

8.3.12.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

8.3.12.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

8.3.12.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

8.3.12.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

8.3.12.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

8.3.12.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.3.12.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.3.12.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.3.12.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para

garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

8.3.12.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

8.3.12.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

8.3.12.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.3.12.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.3.12.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

8.3.12.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

8.3.12.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

8.3.12.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

8.3.12.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

8.3.12.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

8.3.12.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub-redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

8.3.12.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso

ou grupos de pontos de acesso que cada domínio será habilitado;
8.3.12.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
8.3.12.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
8.3.12.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
8.3.12.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
8.3.12.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
8.3.12.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
8.3.12.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
8.3.12.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
8.3.12.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
8.3.12.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
8.3.12.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
8.3.12.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
8.3.12.37. A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;
8.3.12.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
8.3.12.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
8.3.12.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
8.3.12.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar

o uso de airtime nos SSIDs;
8.3.12.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
8.3.12.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
8.3.12.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
8.3.12.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
8.3.12.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
8.3.12.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
8.3.12.48. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
8.3.12.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
8.3.12.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
8.3.12.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
8.3.12.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
8.3.12.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
8.3.12.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
8.3.12.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
8.3.12.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
8.3.12.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
8.3.12.58. A solução deve permitir a configuração do captive portal com endereço IPv6;
8.3.12.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
8.3.12.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas

de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
8.3.12.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
8.3.12.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
8.3.12.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
8.3.12.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
8.3.12.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
8.3.12.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
8.3.12.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
8.3.12.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
8.3.12.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
8.3.12.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
8.3.12.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
8.3.12.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
8.3.12.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
8.3.12.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
8.3.12.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
8.3.12.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
8.3.12.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
8.3.12.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
8.3.12.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

8.3.12.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
8.3.12.81. A solução deve possuir ferramentas de diagnósticos e debug;
8.3.12.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
8.3.12.83. A solução deve suportar comunicação com elementos externos através de REST API;
8.3.12.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

8.3.13. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

8.3.13.1. Deve operar como ponto central para automação e gerenciamento dos switches deste contrato, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
8.3.13.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
8.3.13.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
8.3.13.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
8.3.13.5. Deve montar a topologia da rede de maneira automática;
8.3.13.6. Deve ser capaz de configurar os switches da rede;
8.3.13.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
8.3.13.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
8.3.13.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
8.3.13.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
8.3.13.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
8.3.13.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
8.3.13.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
8.3.13.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
8.3.13.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
8.3.13.16. Deve ser capaz de configurar parâmetros SNMP dos switches;
8.3.13.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches

individualmente;
8.3.13.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
8.3.13.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
8.3.13.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
8.3.13.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
8.3.13.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
8.3.13.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
8.3.13.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;8

8.3.14. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE

8.3.14.1. Solução baseada em appliance. **Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.**
8.3.14.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.
8.3.14.3. Deverá possuir licenças de Garantia, Atualizações de firmware, VPN, SD-WAN, pelo período exigido;
8.3.14.4. Capacidade mínima:
8.3.14.5. Firewall com capacidade mínima de processamento de 5 (cinco) Gbps;
8.3.14.6. IPS com capacidade mínima de processamento de 1 (um) Gbps.
8.3.14.7. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps.
8.3.14.8. Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps.
8.3.14.9. VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPSec.
8.3.14.10. VPN SSL com capacidade de, pelo menos, 450 (quatrocentos e cinquenta) Mbps de tráfego.
8.3.14.11. Deverá suportar 600.000 (seiscentos mil) conexões simultâneas.
8.3.14.12. Deverão ser licenciados para suportar, pelo menos, 190 (cento e noventa) usuários de VPN SSL.
8.3.14.13. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.
8.3.14.14. Deverá suportar, pelo menos, 190 (cento e noventa) túneis de VPN Site-Site.
8.3.14.15. Deverá suportar, pelo menos, 220 (duzentos e vinte) túneis de VPN Client-Site.

8.3.15. INTERFACES DE REDE:

8.3.15.1. Deverá possuir, pelo menos, 05 (cinco) interfaces RJ 45.
8.3.15.2. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade ativo-ativo e estar licenciados para operar desta forma.

8.3.15.3. Deverá possuir licença para número ilimitado de usuários e endereços IP.
8.3.15.4. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 06 (seis) Pontos de Acesso sem fio.
8.3.15.5. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 06 (seis) equipamentos.
8.3.15.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.
8.3.15.7. Deverá incluir licença para a funcionalidade de VPN SSL.
8.3.15.8. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

8.4. ITEM 04 - INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO ASSISTIDA

8.4.1. PARA TODOS OS ITENS:
8.4.1.1. A CONTRATANTE deverá disponibilizar os pontos elétricos e lógicos necessários para a realização da instalação física necessária.
8.4.1.2. Os equipamentos HARDWARE devem ser instalados fisicamente e configurados pela CONTRATADA de forma que após a conclusão estejam aptos ao uso.
8.4.1.3. Os locais a serem instalados serão definidos pela CONTRATANTE e sua equipe de TI;
8.4.1.4. A etapa de instalação deverá ocorrer com os seguintes critérios:

	Planejamento da instalação incluindo identificação de pré-requisitos e plano de *rollback*;
	Instalação física dos equipamentos no rack;
	Atualização de drivers e *firmwares* dos equipamentos;
	Realização de testes de conectividade;
	Integração com *Microsoft Active Directory (single sign-on*);
	Regras de roteamento, utilizando como base as regras atualmente em uso pela CONTRATANTE;
	Regras de firewall, utilizando como base as regras atualmente em uso pela CONTRATANTE;
	VPN: Configuração dos acessos externos
0	IPS, deverá ser configurado de acordo com os níveis de proteção e ações a serem definidas pela CONTRATANTE;
1	Filtro de conteúdo, de acordo com as categorias e ações de bloqueio definidas pela CONTRATANTE:
2	Proteção contra *Malwares*, deverá ser configurado de acordo com os níveis de proteção e ações a serem definidas pela CONTRATANTE;

3	Controle de aplicações, deverá ser configurado para bloquear ou liberar aplicações específicas de acordo com as informações fornecidas pela CONTRATANTE;
4	Balanceamento de carga entre dois links de internet dedicados de acordo com as configurações e parâmetros fornecidos pela CONTRATANTE;
5	Instalação e configuração da plataforma de emissão de relatórios da ferramenta;
6	Configuração de relatórios customizados, de acordo com a necessidade da CONTRATANTE;
7	Realizar backup das configurações;
8	Documentar todas as alterações realizadas no ambiente;

8.4.1.5. Instalar fisicamente os equipamentos em rack 19" (dezenove polegadas), bem como as interligações/conexões físicas que sejam necessárias. O rack de servidores localiza-se atualmente no Datacenter SESC AMAPÁ; Atualizar Firmware dos equipamentos para a última versão estável recomendada;

8.4.1.6. Caso A licitante vencedora através de sua representatividade e legitimidade em pertencer ao programa de Parceiros do Fabricante e, ainda, ser declarado o Parceiro registrado no formulário de pré-engajamento emitido pelo Fabricante de que executará o atendimento das solicitações de instalação e migração, devendo portanto, a mesma possuir profissional qualificado e certificado pela fabricante, ao menos, com as certificações compatíveis ao Objeto desta licitação até a assinatura do contrato ou apresentar até a assinatura do contrato, os documentos da qualificação técnico-operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.

8.4.1.7. A comprovação do item anterior imediato, no caso do CMMI-Svc, se dará por meio de cópia autenticada do certificado emitido por uma agência certificadora independente (agências credenciadas pelo Software Engineering Institute - http://www.sei.cmu.edu) ou seu representante no Brasil;

8.4.1.8. Para a certificação MPS/BR-Serviços, a comprovação se dará por meio de cópia autenticada do certificado de qualidade MPS-BR-Sv emitido pela SOFTEX ou parceiro autorizado.

8.4.1.9. A qualquer tempo, o time técnico da CONTRATANTE poderá realizar visita às instalações da CONTRATADA para comprovar a adoção de processos aderentes à norma ISO NBR 20.000 na execução dos serviços previstos neste edital

8.4.1.10. Esta execução da instalação física e logica deverá ser de no máximo 72 (setenta e duas) horas uteis.

8.4.2. MIGRAÇÃO:

8.4.2.1. Deverá ser ofertado serviço de migração das regras de segurança do Firewall existente no

equipamento atual de segurança deste REGIONAL DO SESC para o modelo ofertado neste edital.
8.4.2.2. Visando eliminar erros humano e redundâncias, deverá ser ofertado juntamente com o serviço de instalação, o serviço de migração com uso de ferramentas (software) que garantam a segurança e a automação do processo de forma a mitigar falhas de migração assim como o emprego de metodologias avançadas de processos automatizados por software.
8.4.2.3. Deverá ser informada a ferramenta de migração usada neste processo.
8.4.2.4. O tempo de execução do serviço de migração deve ser de no máximo 40 (quarenta) horas uteis;

8.4.3. OPERAÇÃO ASSISTIDA:
8.4.3.1. Para garantir a sustentação e o pleno funcionamento da solução, a CONTRATADA deverá realizar, durante 10 (DEZ dias) corridos, após a emissão da Termo de Recebimento Definitivo (TRD), operação assistida no ambiente instalado, esclarecendo dúvidas e realizando ajustes nas configurações visando a melhor utilização dos recursos oferecidos nos equipamentos que compõem a solução;
8.4.3.2. O serviço de operação assistida deverá ser realizado por técnico(s) plenamente qualificado(s), devendo possuir certificação emitida pelos fabricantes da solução ofertada, devendo ser prestada com acompanhamento da equipe técnica do Contratante
8.4.3.3. O período de operação assistida faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE;
8.4.3.4. A operação assistida da solução será utilizada para monitoria do ambiente, melhoria no ambiente, continuidade da solução, desenvolvimento de competências técnicas, e o seu escopo compreende:
8.4.3.5. Orientações sobre o ciclo de vida dos produtos adquiridos, contando com acesso ao conhecimento privilegiado de recursos acerca de arquitetura tecnológica, viabilizando a definição de parâmetros objetivos para o dimensionamento da infraestrutura;
8.4.3.6. Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (hardware e software);
8.4.3.7. Orientação quanto às melhores práticas para o correto ciclo de vida dos produtos adquiridos;
8.4.3.8. Análise técnica qualificada da compatibilidade e interoperabilidade dos produtos;
8.4.3.9. Aplicação de melhores práticas para o correto uso produtos adquiridos;
8.4.3.10. Estudo e reconfiguração do ambiente, quando esta demandar redimensionamento;
8.4.3.11. Estudo de revisão de arquitetura para melhoria de desempenho e disponibilidade;
8.4.3.12. Indicação de modelos de uso e planejamento de capacidade;
8.4.3.13. Identificação de melhorias e respectivo tratamento;
8.4.3.14. Suporte avançado técnico para estratégia e adequações nos ambientes;
8.4.3.15. Suporte avançado técnico para primeiro atendimento de anomalias dos produtos adquirido s e o correto repasse de atendimento de anomalias ao fabricante do produto caso seja necessário;

8.5. ITEM 05 - CAPACITAÇÃO TÉCNICA
8.5.1. CARACTERISTICAS GERAIS:
8.5.1.1. A capacitação técnica do tipo HANDS ON, deverá abordar todos os componentes da solução fornecida nos itens 1, 2 e 3, devendo ainda estar conforme a utilização da solução instalada no ambiente

do SESC/AP, incluindo parametrizações e customizações, considerando os seguintes tópicos: Introdução, Instalação e Configuração, Administração e Gerenciamento, Implementação e Solução de Problemas

8.5.1.2. Requisitos dos serviços de instalação, configuração, documentação e treinamento do tipo hands-on, com os seguintes requisitos mínimos:

8.5.1.3. Registrar e licenciar o equipamento no portal do fabricante; configurar e habilitar os recursos de profiles de UTM (IPS, Application Control, Web Filter, Inspeção de SSL, Antivirus);

8.5.1.4. Configurar integração com o Active Directory;

8.5.1.5. Configurar alta disponibilidade (HA);

8.5.1.6. O acesso deverá ser baseado nos grupos de Active Directory;

8.5.1.7. Configurar Redes DMZ, Rede Local e Rede de Servidores;

8.5.1.8. Configurar SSLVPN integrada com o Active Directory;

8.5.1.9. Configurar VPN site-to-site;

8.5.1.10. Configurar todas as portas de conectividades dos equipamentos;

8.5.1.11. Exportar e migrar para o novo firewall todas as regras de acesso, serviços, endereços e configurações do firewall em PRODUÇÃO utilizado atualmente;

8.5.1.12. Revisar todas as regras de acesso utilizadas atualmente no firewall do SESC AP

8.5.1.13. Realizar todas as configurações necessárias para a implantação de todas as funcionalidades permitidas pelo novo firewall;

8.5.1.14. Treinamento hands-on para 2 (dois) participantes com no mínimo 16 (dezesseis) horas;

8.5.1.15. Ao final do processo deve ser entregue documentação formal de todas as configurações, procedimentos de backup e restore, desastre e recuperação do ambiente firewall e de gerência, e definições utilizadas na instalação e ativação do conjunto, com detalhamento suficiente que permita aos técnicos responsáveis a reprodução das ações, se necessário;

8.5.1.16. Os serviços deverão ser prestados por profissionais qualificados pela fabricante, ao menos, com as certificações Network Security.

8.6. BANCO DE HORAS TÉCNICA

8.6.1. CARACTERÍSTICAS GERAIS:

8.6.1.1. Serviços especializados para novas demandas ou correção de problemas não previstos após instalação da solução contendo no mínimo, os seguintes requisitos:

8.6.1.2. Visando garantir o perfeito funcionamento da solução após implementação, levando em consideração de ser uma solução nova para o time técnico da CONTRATANTE, mesmo após treinamento sobre as funcionalidades e operação assistida, deverá ser ofertado serviço de banco de horas técnica em caso de intercorrências que prejudiquem o bom funcionamento e que necessitem de intervenção no ambiente da CONTRATANTE por time técnico qualificado para tal resolução por parte da CONTRATADA.

8.6.1.3. O serviço deverá ser prestado preferencialmente de forma remota;

8.6.1.4. O serviço especializado será demandado através de Ordens de Serviço (OS) prevendo o quantitativo a serem consumidos, o período de execução e a descrição dos serviços a serem executados.

8.6.1.5. O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculadas ao item

da OS. Qualquer alteração na quantidade de horas deverá ser justificada e previamente aprovada pela CONTRATANTE.

8.6.1.6. Os serviços proporcionais de gerenciamento de projetos e liderança técnica deverão estar incluídos dentro do valor da hora.

8.6.1.7. O serviço especializado abrange as seguintes atividades, podendo através de livre acordo entre as partes através de comunicação formal abrangerem itens não contemplados neste edital:

8.6.1.8. Resolução de problemas críticos na infraestrutura de processamento, armazenamento, backup, firewall, virtualização e redes;

8.6.1.9. Revisões e/ou Alterações de configurações, novas instalações, atualização de versões de softwares ou firmwares;

8.6.1.10. Execução de testes programados de recuperação de desastres visando validar o plano de continuidade de negócios;

8.6.1.11. Treinamento para conscientização sobre ameaças cibernéticas.

8.6.1.12. Serviços consultivos, para apoiar a avaliar, melhorar e testar processos de resposta a incidentes críticos de segurança;

8.6.1.13. Serviço de consolidação em dashboard com inúmeros fatores de riscos externos, como: serviços e portas divulgados publicamente, credenciais vazadas, identificação de páginas web, domínios e perfis de redes sociais que tentem se passar por este SESC/DR/AP;

8.6.1.14. Serviço de Implantação e Configuração para Solução De Segurança e Gerência De Redes;

8.6.1.15. Serviço de Implantação e Configuração para Unidade Centralizada de Armazenamento de Logs e Relatoria;

8.6.1.16. Serviços Profissionais de Implantação e Configuração Unidade de Gerência Centralizada de Equipamentos

8.6.1.17. Treinamento para Solução de Segurança e Gerência de Redes NGFW

8.6.1.18. Instalação e configuração de Solução de Segurança e Gerência de Redes NGFW

8.6.1.19. Treinamento de Unidade de Gerência Centralizada de Equipamentos

8.6.1.20. Treinamento de Unidade Centralizada de Armazenamento de Logs e Relatoria Migrações de dados;

8.6.1.21. Diagnóstico de problemas de desempenho e planejamento de capacidade;

8.6.1.22. Recuperação de dados através de Software de Backup e Replicação

8.6.1.23. Recuperação de solução de segurança de dados em ambiente VMware.

8.6.1.24. Implementação de regras de segurança;

8.6.1.25. Configurações em ativos de rede;

8.6.1.26. Elaboração de documentação técnica e de usuário;

8.6.1.27. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE.

8.6.1.28. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas.

8.6.1.29. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;

8.6.1.30. Realização de operação assistida e monitoramento de ambientes entregues com a solução.

8.6.1.31. Orientar na utilização dos softwares instalados no CONTRATANTE com a utilização das melhores práticas e orientações dos fabricantes;

8.6.1.32. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no CONTRATANTE minimizando impactos;
8.6.1.33. Apoiar na configuração/parametrização do sistema em novas máquinas;
8.6.1.34. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do CONTRATANTE;
8.6.1.35. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;
8.6.1.36. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;
8.6.1.37. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;
8.6.1.38. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE;
8.6.1.39. Esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE.
8.6.1.40. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
8.6.1.41. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;
8.6.1.42. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;
8.6.1.43. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;
8.6.1.44. A licitante deverá possuir uma ferramenta de SERVICE DESK on-line e que siga as melhores práticas da certificação ITIL para a abertura e gerenciamento de chamados na utilização dos bancos de horas, a fim de acompanhar o tempo de resolução para cada atividade (SLA), bem como disponibilizá-los em filas de priorizações para cada ocorrência, serviço e/ou incidente.
8.6.1.45. A ferramenta mencionada deverá permitir que a CONTRATANTE realize abertura de chamados através de e-mail, portal na Internet e/ou aplicativo de celular, sendo que cada chamado deverá possuir um código de identificação único que permita a sua rápida identificação.
8.6.1.46. O sistema deverá permitir o acompanhamento em tempo real pela CONTRATANTE dos chamados abertos e seus respectivos status, além de permitir a visualização do histórico de todos os chamados finalizados.
8.6.1.47. Para melhor gerenciamento dos chamados pela CONTRATADA, o sistema deverá possuir um painel (dashboard) que possua gráficos e outros tipos de visualizadores, além de permitir a geração de relatórios conforme necessidade e solicitação da CONTRATANTE.
8.6.1.48. Para fins de comprovação, o licitante deverá informar o nome da ferramenta de service desk utilizada.
8.6.1.49. Todo processo do serviço realizado deverá ser demonstrado em relatórios com todos os seus detalhes da sua execução.

8.6.1.50. Após a abertura de um chamado no sistema, o primeiro atendimento deverá ocorrer de forma remota para melhor entendimento do cenário e sua possível solução. Todavia, caso o atendimento remoto não seja suficiente para conclusão do chamado, então o atendimento deverá ser realizado de forma on-site, ou seja, de forma presencial no endereço da CONTRATANTE.

8.6.1.51. Quanto remoto, o atendimento será feito por ferramenta que irá contabilizar o tempo de acesso e trabalho, a fim de validar a consumação do banco de horas;

9. CONDIÇÕES DE ENTREGA COM SERVIÇO DE INSTALAÇÃO DO FIREWALL:

9.6. A entrega do objeto deste instrumento deverá ser realizada no prazo de até 60 (sessenta) dias corridos, a contar da data de recebimento da Ordem de Compra – OC, expedido pela Coordenadoria de Material e Patrimônio do SESC Amapá, onde constará o item e a quantidade conforme necessidade do SESC/AP;

9.7. O equipamento deve no ato da entrega estar acompanhado da nota fiscal;

9.8. O objeto deste contrato deverá ser entregue na sala da Coordenadoria de Tecnologia da Informação - CTIN do SESC Amapá, localizado na Rua Jovino Dinoá, nº 4311, Bairro: Beirol, Macapá-AP, CEP: 68.902-030, nos seguintes dias e horários: de segunda-feira a sexta-feira das 08h às 11h e das 14h às 17h;

9.9. O recebimento provisório será realizado dentro do prazo máximo de 03 (três) dias úteis, contados da data de entrega no SESC/AP para verificação e validação dos equipamentos com as especificações exigidas;

9.10. O recebimento definitivo será realizado dentro do prazo máximo de 05 (cinco) dias úteis, contados do recebimento provisório, para verificação da qualidade e quantidade do equipamento e consequente aceitação;

9.11. O objeto deverá ser entregue devidamente embalado, de forma a não ser danificado durante as operações de transporte, carga e descarga, contendo na embalagem marca, prazo de validade, procedência e demais características que o identifiquem. Não sendo aceitos, de imediato, produtos cuja embalagem apresente sinais de violação;

9.12. O aceite do objeto deste instrumento pelo SESC Amapá, não exclui a responsabilidade civil do fornecedor, por vícios de quantidade, de qualidade ou técnico dos produtos, ou por desacordo com as especificações estabelecidas neste instrumento e edital, verificadas posteriormente;

9.13. O Fornecedor deverá entregar o produto rigorosamente dentro do prazo estipulado e com validade não inferior a 36 (trinta e seis) meses, de acordo com as especificações constantes neste instrumento;

9.14. As despesas de frete/embalagem deverão estar inclusas no preço proposto, e em hipótese alguma poderão ser destacadas quando da emissão da nota fiscal/fatura.

10. OBRIGAÇÕES DA CONTRATANTE:

10.1. Comunicar à Contratada toda e quaisquer ocorrências relacionadas com a contratação dos serviços.

10.2. Promover o acompanhamento e fiscalização, comunicando por escrito ou por telefone a CONTRATADA quaisquer ocorrências, irregularidade ou deficiência, relacionada com o fornecimento do equipamento;

10.3. Efetuar o pagamento pelo fornecimento realizado, após devidamente atestada a nota fiscal/fatura, de acordo com as condições e preços pactuados;
10.4. Verificar a qualidade do serviço em conformidade com as especificações técnicas exigidas neste contrato;
10.5. Notificar, formal e tempestivamente, a CONTRATADA sobre irregularidades observadas no cumprimento do Contrato.
10.6. Designar um colaborador como Fiscal de Contrato, que deverá acompanhar e fiscalizar os técnicos da CONTRATADA em todas as visitas, comprovar e relatar, por escrito, as eventuais irregularidades na prestação de serviços, sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado, ou por outro motivo que caracterize a necessidade de tal medida;
10.7. Rejeitar, no todo ou em parte, o equipamento que a empresa vencedora entregar fora das especificações exigidas;
10.8. Solicitar o afastamento de qualquer profissional que não estiver apto às obrigações estabelecidas no contrato ou que não tenha comportamento adequado no serviço;
10.9. Prestar informações e esclarecimentos que venham a ser solicitados pela Contratada.

11. OBRIGAÇÕES DA CONTRATADA:

11.1. Realizar as entregas e prestar os serviços de acordo com todas as exigências contidas no acordo;
11.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;
11.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízo, de qualquer natureza, que causar a CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas;
11.4. Atender às determinações e exigências formuladas pela CONTRATANTE;
11.5. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;
11.6. A CONTRATADA responderá por todos os vícios e defeitos dos serviços durante o período de vigência do contrato;
11.7. Efetuar o pagamento de todos os impostos, taxas e demais obrigações fiscais incidentes ou que vierem a incidir;
11.8. Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação, apresentando os documentos que comprovem tal regularidade junto com a nota fiscal/fatura resultante do fornecimento do contrato, quais sejam:
11.9. Prova de regularidade relativa à Seguridade Social;
11.10. Certidão conjunta relativa aos tributos federais e a Dívida Ativa da União;
11.11. Certidões de regularidade perante a Fazenda Estadual, Municipal ou Distrital, conforme o tipo de prestação;
11.12. Certidão de regularidade do FGTS;
11.13. Certidão negativa de débitos trabalhistas.

11.14. Não transferir a outrem, no todo ou em parte, a responsabilidade assumida, sem prévia e expressa anuência do SESC/AP;

11.15. Repor as suas expensas os produtos nos quais forem constatadas irregularidades imediatamente, contados da notificação feita pelo SESC/AP sem ônus para a CONTRATANTE;

11.16. Efetuar a entrega do equipamento de acordo com os prazos, especificações e demais condições de fornecimento constantes no edital;

11.17. Apresentar justificativa dirigida à autoridade competente no prazo de 24 (vinte e quatro horas) anterior à data prevista para entrega do objeto quando da previsão de eventual atraso na entrega;

11.18. Arcar com todas as despesas decorrentes da contratação do objeto deste acordo, inclusive locomoção, seguro de acidentes, impostos, contribuição previdenciárias, encargos trabalhistas, comerciais e outras decorrentes do fornecimento dos equipamentos;

11.19. Fornecer produtos livres de quaisquer tipos de vício ou características que venham a prejudicar o desenvolvimento das atividades do SESC/DR/AP;

11.20. Equipamentos, módulos, componentes, ou qualquer outra parte do OBJETO que a CONTRATANTE constate terem sido entregues já com defeito ou danificados devem ser trocados por outro equipamento, componente ou item novo, de mesma marca e modelo, com número de série diferente, em no máximo 30 dias úteis;

11.21. Responsabilizar-se a qualquer tempo pela qualidade do equipamento fornecido ao CONTRATANTE, inclusive no tocante a eventuais problemas e prejuízos posteriores, ocorridos pela inobservância de especificações constantes no Edital e nesse contrato;

11.22. Responsabilizar-se pelos prejuízos financeiros decorrentes da não entrega dos equipamentos solicitados;

11.23. Entregar o equipamento com garantia de, no mínimo 36 (trinta e seis) meses;

11.24. Cumprir fielmente com todas as condições ora pactuadas, neste instrumento, e de acordo com as exigências desse acordo.

12. DAS CONDIÇÕES DE PAGAMENTO:

12.1. O pagamento à contratada será efetuado em moeda corrente nacional à empresa (de acordo com as normas da Contratante), em **até 15 (quinze) dias úteis** após o recebimento da nota fiscal devidamente atestada pelo Fiscal do Contrato e acompanhada dos documentos de regularidade fiscal e demais documentos referentes ao cumprimento da execução do contrato.

12.2. A contratada, obrigatoriamente, deverá ser informar na nota fiscal o número e nome do banco, número da agência e conta corrente;

12.3. O prazo para pagamento contará a partir da data de atesto da nota fiscal pelo fiscal do contrato. Se o fiscal detectar a ausência de algum documento ou erro na nota fiscal poderá rejeitar de imediato;

12.4. Caso não haja expediente no SESC-DR/AP no dia do vencimento da nota fiscal, fica o pagamento prorrogado para o 1º dia útil subsequente;

12.5. O SESC-DR/AP se reserva o direito de não aceitar notas fiscais que NÃO estejam acompanhadas dos documentos que comprovem quitação das obrigações. O não aceite das referidas notas fiscais não gera o dever de pagar enquanto houver pendência de obrigação que tenha sido imposta em virtude de penalidade ou inadimplemento apontado pela fiscalização. Cessadas essas causas, os pagamentos serão retomados sem que haja qualquer direito a atualização monetária;

12.6. O recebimento da nota não configura o aceite da nota fiscal, devendo, para tanto, ter a atestação do fiscal do contrato;

12.7. As empresas que tiverem seu CNAE previsto no Protocolo ICMS nº 42, de 03 de julho de 2009, deverão emitir a nota fiscal conforme legislação vigente.

13. DA REGULARIDADE FISCAL:

13.1. A contratada fica obrigada manter-se durante toda a execução deste Registro de Preços, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação, apresentando os documentos que comprovem tal regularidade junto com a nota fiscal/fatura resultante do fornecimento do objeto contratado e sempre que solicitado pela contratante, quais sejam:

13.1.1. Certidão conjunta relativa aos tributos federais e a Dívida Ativa da União;

13.1.2. Certidões de regularidade perante a Fazenda Estadual, Municipal ou Distrital, conforme o tipo de prestação;

13.1.3. Certidão de regularidade do FGTS; e

13.1.4. Certidão negativa de débitos trabalhistas.

14. DA FISCALIZAÇÃO:

14.1. A fiscalização do presente instrumento será exercida pela **Coordenadoria de Tecnologia da Informação - CTI**, designado para este fim;

14.2. O representante do SESC/DR/AP anotará em registro próprio todas as ocorrências relacionadas com a execução do objeto desta ata, determinando o que for necessário à regularização das falhas ou impropriedades observadas;

14.3. As decisões e providências que ultrapassarem a competência do representante do SESC-DR/AP deverão ser solicitadas ao seu superior, em tempo hábil, para adoção das medidas convenientes;

14.4. Caberá ao fiscal do contrato requisitar que a contratada realize a imediata substituição do item que não estiver em consonância com os parâmetros estabelecidos neste instrumento, na OC – Ordem de Compra ou no edital, se obrigando, a CONTRATADA, a realizar a troca, não restando qualquer ônus à CONTRATANTE;

14.5. Obter da Contratada a garantia explicita dos produtos de modo a verificar a sua efetiva utilização;

14.6. A comunicação feita entre a contratada e a contratante será mediante e-mail, contato telefônico e correspondência oficial.

15. DAS PENALIDADES:

15.1. A recusa injustificada em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo legalmente fixado, caracterizará o descumprimento total da obrigação assumida e poderá acarretar a Contratada as seguintes penalidades:

15.1.1. Perda do direito à contratação;

15.1.2. Perda da caução em dinheiro ou execução das demais garantias de propostas oferecidas, quando for o caso;

15.2. Verificada a recusa em assinar a Ata de Registro de Preço, o SESC-DR/AP poderá convocar as Licitantes remanescentes, obedecendo à ordenação final;

15.3. A licitante deixará de ter o seu preço registrado quando:

15.3.1. Descumprir as condições assumidas no instrumento por ela assinado;
15.3.2. Não aceitar reduzir o preço registrado, quando se tornar superior ao praticado no mercado;
15.3.3. Quando justificadamente, não for mais do interesse do SESC;
15.4. O inadimplemento total ou parcial ou o atraso no cumprimento das obrigações assumidas ensejará na aplicação das seguintes penalidades:
15.4.1. Advertência;
15.4.2. Multa compensatória de 10% (dez por cento) sobre o valor do contrato;
15.4.3. Multa moratória de 0,2 (dois) décimos por dia de atraso sobre o valor total do contrato;
15.4.4. Baixa no contrato;
15.4.5. Suspensão de licitar com o SESC/DR/AP por prazo não superior a 03 (três) anos.
15.5. As penalidades poderão ser aplicadas cumulativamente e deverão considerar os princípios do contraditório, ampla defesa, razoabilidade e proporcionalidade;

16. DA RENÚNCIA OU ALTERAÇÃO DE DISPOSITIVOS CONTRATUAIS:

16.1. Toda alteração, supressão, renúncia ou ato que importe na mudança nos termos deste acordo ou na aplicação dos seus dispositivos deverá constar em Termo Aditivo, o qual deverá ser assinado por todos os signatários desta Ata, exceto aqueles que tiverem seu registro de preço removido. O fato de uma das partes tolerar qualquer falta ou descumprimento de obrigações da outra não importa em alteração deste instrumento, nem induz à novação, ficando mantido o direito de se exigir da parte faltosa ou inadimplente, a qualquer tempo, a cessação da falta ou cumprimento integral de tal obrigação.

17. RESCIÇÃO:

17.1. O presente Contrato poderá ser rescindido unilateralmente pelo SESC/AP, independentemente de notificação ou interpelação judicial, no caso de inadimplemento de qualquer de suas cláusulas ou condições, sujeitando à Contratada às penalidades previstas na cláusula anterior deste instrumento, e em especial pelo:

17.2. Não cumprimento ou cumprimento irregular de cláusulas pactuadas, especificações ou prazos;
17.3. Subcontratação, total ou parcial do objeto deste contrato, sem prévia autorização escrita do SESC/AP, associação da contratada com outrem, cessão ou transferência total ou parcial, bem como a fusão, cisão ou incorporação, que afetem a boa execução do Contrato;
17.3.1. A morosidade do seu cumprimento, levando o SESC/AP a comprovar a impossibilidade da conclusão dos serviços nos prazos estipulados;
17.3.2. Paralisação dos serviços, sem justa causa ou prévia comunicação ao SESC/AP;
17.3.3. Cometimento reiterado de falhas na execução deste contrato;
17.3.4. Decretação de falência;
17.3.5. Dissolução da empresa;
17.3.6. Razões de interesse público de alta relevância e amplo conhecimento;
17.3.7. Ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução desse contrato;
17.3.8. Alteração social ou modificação da finalidade ou da estrutura da contratada, que prejudique a execução do contrato.

17.4. Em qualquer das hipóteses acima referidas, a contratada deverá reparar integralmente os prejuízos causados ao SESC/AP, independente da aplicação das penalidades previstas neste instrumento, que poderão ser aplicadas no todo ou em parte, a critério exclusivo da CONTRATANTE;

17.5. Rescindido o presente contrato por culpa da contratada, o SESC/AP entregará os serviços, objeto deste instrumento, a quem julgar conveniente, sem qualquer consulta ou interferência da contratada, que responderá na forma legal e contratual pela infração ou execução inadequada que tenha dado causa à rescisão.

18. DA REVISÃO DE PREÇOS:

18.3. A contratada deverá protocolar no setor de protocolo deste SESC/DR/AP documento formal pleiteando o reequilíbrio econômico-financeiro, especificando com clareza seus argumentos, fatos e documentos comprobatórios;

18.4. Nos casos de **reajuste de preços**, consignado no contrato, serão corrigidos mediante formalização do pedido pela CONTRATADA, observado o interregno mínimo de um ano, contado a partir da data de apresentação da proposta, pela variação do INPC - Índice Nacional de Preços ao Consumidor, ocorrida nos últimos 12 (doze) meses;

18.4.1. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste;

18.5. Nos casos **revisão de preços**, independentemente de prazos, não se pautando em índices específicos ou setoriais, a contratada deverá comprovar a alteração dos custos e insumos do contratado mediante apresentação de planilhas e documentos que demonstrem que, diante de fatos imprevisíveis ou previsíveis, mas de consequências incalculáveis, restou alterada a proporção entre encargos e vantagens originalmente prevista na proposta apresentada à época da licitação, não sendo suficiente a mera alegação de que houve a majoração dos preços pelo fornecedor.

19. DA COMPLEMENTAÇÃO OU ACRÉSCIMO:

19.3. No interesse da Administração do SESC-DR/AP, o valor inicial atualizado da Ata de registro de preço poderá ser aumentado até o limite de 50% (cinquenta por cento), com fundamento do Art. 38 da Resolução SESC **1.593/2024**;

19.4. A contratada poderá aceitar, nas mesmas condições licitadas, os acréscimos que se fizerem necessários.

20. DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS:

20.3. Em atendimento ao disposto na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), o SESC/AP, para a execução do serviço objeto deste instrumento contratual, terá acesso aos dados pessoais dos representantes da CONTRATADA, tais como: número do CPF e RG, e-mail, contato, entre outros que possam ser exigidos para a execução contratual;

20.4. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

20.5. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução

contratual, em consonância com o disposto na Lei n. 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual;

20.6. As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD;

20.7. A CONTRATADA, declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo SESC/AP;

20.8. A CONTRATADA, fica obrigada a comunicar ao SESC/AP, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

21. DO FORO:

21.3. Fica eleito o Foro da Comarca da Capital do Estado do Amapá, para nele resolverem quaisquer questões ou atos oriundos do presente instrumento e em decorrência, renunciando qualquer outro por mais privilegiado que for;

E por estarem assim justos e contratados, na presença das testemunhas abaixo assinadas e para efeitos legais, firmam em 02 (duas) vias, o presente instrumento.

Macapá – AP, _____ de _____ de 2024.

(...)	(...)
Presidente do Conselho	Representante da Empresa
Regional do SESC/DR/AP	CONTRATADA
CONTRATANTE	

(...)	(...)
Fiscal do contrato – SESC/DR/AP	Gestora do contrato – SESC/DR/AP

Testemunhas:

1._____	2._____
CPF:	CPF: