Minuta de Contrato regida pela Lei Federal nº 14.133/2021

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO NGFW, XXX.XXXX.X.X, QUE ENTRE SI CELEBRAM [*Nome do Participante*] E A [*Detentora da Ata de Registro de Preços*]

PROCESSO ADMINISTRATIVO Nº xx.xxx.xxx/xx-xx
PROCESSO LICITATÓRIO Nº xx.xxx.xxx/xx-xx
PREGÃO ELETRÔNICO Nº xxxxx/xxxx
ATA DE REGISTRO DE PREÇOS Nº xxxxxx/xxxx

A **[***Nome do Participante***]**, estabelecida na [*endereço completo*], CNPJ nº [*nº do CNPJ*], doravante denominada **CONTRATANTE**, neste ato representada por [*Cargo e Responsável Legal do Órgão Participante*], CPF nº [*nº do CPF*], e a [***razão social da CONTRATADA***], CNPJ/MF nº [*nº do CNPJ*], estabelecida na [*endereço completo*], neste ato representada por seu [*cargo e nome completo do Representante Legal*], CPF nº [*nº do CPF*], doravante denominada **CONTRATADA**, celebram, em decorrência da Ata de Registro de Preços xxxxxx/xxxx, o presente Contrato que é regulado pelas suas cláusulas, pela Lei Federal nº 14.133/2021 e pelos preceitos de direito privado, conforme condições a seguir especificadas, reciprocamente estipuladas e aceitas, vinculando-se ao Edital de Licitação Pregão Eletrônico xxxxx/xxxx, parte integrante deste instrumento independente de transcrição.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. Promover o registro de preço para Aquisição de solução especializada e integrada de segurança de rede do tipo Next Generation Firewall (NGFW) com suporte a funcionalidades de SD-WAN, incluindo fornecimento de equipamentos, licenças de software, plataforma de gerenciamento centralizado, serviços de implantação, suporte técnico, treinamento e garantia de 60 meses, conforme especificações técnicas descritas no Anexo I deste Termo de Referência e quantidades definidas abaixo:

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD
X	Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	UN	x

1.2. Considera-se como unidade de fornecimento a solução completa de Next Generation Firewall (NGFW) com funcionalidades de SD-WAN plenamente operacional, incluindo equipamentos, licenças, serviços de implantação, treinamento e suporte necessários ao funcionamento da solução.

CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES DO FORNECIMENTO

2.1. A CONTRATADA deverá fornecer o objeto deste Contrato conforme especificações descritas no Anexo I deste Contrato e do Termo de Referência.

CLÁUSULA TERCEIRA - DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

3.1. O objeto do presente Contrato será recebido conforme definido na presente Cláusula, no Termo de Referência e seus anexos.

3.1.1. Provisoriamente, para efeito de posterior verificação da sua conformidade com as especificações e quantidades no prazo de 05 (cinco) dias úteis a contar da data do recebimento dos equipamentos pela CONTRATANTE;

3.1.2. Definitivamente, após a verificação da observância pela CONTRATADA à integralidade das condições estabelecidas no Anexo I deste Contrato e do Termo de Referência, incluindo o treinamento.

3.2. Os itens que compõem o objeto devem ser novos, sem uso anterior e compatíveis com as especificações técnicas deste Contrato.

3.3. Poderão ser realizados testes pela CONTRATANTE ou equipe por ela indicada para averiguação do cumprimento da especificação técnica, no prazo de até 10 (dez) dias úteis contados da entrega, após o que será emitido o Termo de Aceite Definitivo e o respectivo ateste da Nota Fiscal.

3.4. Encontrando irregularidades, o produto deverá ser reparado no prazo de até 10 (dez) dias corridos, contados da data da notificação pela CONTRATANTE.

3.4.1. Aprovados, serão recebidos definitivamente, mediante ateste aposto na Nota Fiscal respectiva.

3.5. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o item do objeto em que se verificarem vícios, defeitos ou incorreções.

CLÁUSULA QUARTA - DAS CONDIÇÕES DE GARANTIA/ASSISTÊNCIA TÉCNICA DO OBJETO

4.1. Cabe à CONTRATADA garantir o suporte e apoio técnico para instalação e configuração da solução e o atendimento para manutenção corretiva e identificação de falhas ou inconsistências detectadas no objeto, incluindo ainda, o esclarecimento de

dúvidas, de forma a garantir o funcionamento do software e hardware durante o período de 60 (sessenta) meses a partir da disponibilização da solução.

4.2. Também é responsabilidade da CONTRATADA, durante o período de garantia, promover:

4.2.1. Atualizações de firmware;

4.2.2. Correções de segurança;

4.2.3. Atualizações necessárias ao funcionamento da solução.

4.3. A CONTRATADA deverá proceder a substituição, reparo ou correção no prazo máximo de 15 (quinze) dias corridos, contados do recebimento da notificação respectiva que também poderá ser enviada por e-mail, sem prejuízo da aplicação das sanções previstas na Lei, Decreto e no Código de Defesa do Consumidor.

4.4. A CONTRATADA deverá garantir o pleno funcionamento do objeto durante toda a vigência contratual.

CLÁUSULA QUINTA - SLA

5.1. Durante o período de garantia da solução, a CONTRATADA deverá disponibilizar suporte técnico para atendimento de incidentes, dúvidas operacionais e correção de falhas relacionadas ao hardware e software fornecidos.

5.2. O suporte técnico deverá ser disponibilizado por meio de sistema de abertura de chamados, portal eletrônico, correio eletrônico ou telefone.

5.3. Os chamados serão classificados conforme o grau de criticidade do incidente, conforme definido abaixo.

5.4. O descumprimento do SLA ensejará na aplicação de penalidade contratual.

5.5. **Criticidade Alta (Severidade 1), situações em que houver:**

5.5.1. Indisponibilidade do equipamento NGFW ou das funcionalidades de segurança e SD-WAN da solução;

5.5.2. Interrupção de comunicação entre unidades críticas;

5.5.3. Falha grave que impeça a operação da solução.

5.5.4. SLA aplicável:

5.5.4.1. Tempo máximo de resposta: até 4 (quatro) horas úteis

5.5.4.2. Tempo máximo para solução ou mitigação: até 24 (vinte e quatro) horas úteis.

5.6. **Criticidade Média (Severidade 2), situações em que houver:**

5.6.1. Degradação de desempenho da solução;

5.6.2. Falha parcial em funcionalidades da solução;

5.6.3. Problemas que não impeçam totalmente a operação da rede.

5.6.4. SLA aplicável:

5.6.4.1. Tempo máximo de resposta: até 8 (oito) horas úteis

5.6.4.2. Tempo máximo para solução: até 48 (quarenta e oito) horas úteis

5.7. **Criticidade Baixa (Severidade 3), situações relacionadas a:**

5.7.1. Dúvidas operacionais;

5.7.2. Ajustes de configuração;

5.7.3. Solicitações de informação ou suporte técnico.

5.7.4. SLA aplicável:

5.7.4.1. Tempo máximo de resposta: até 24 (vinte e quatro) horas úteis;

5.7.4.2. Tempo máximo para solução: até 5 (cinco) dias úteis.

5.8. **Substituição de Hardware**

5.8.1. Caso seja identificado defeito em equipamento fornecido na solução, a CONTRATADA deverá providenciar:

5.8.1.1. diagnóstico técnico do equipamento;

5.8.1.2. reparo ou substituição.

5.8.2. O prazo máximo para substituição de equipamento defeituoso será de até 10 (dez) dias corridos, contados da abertura do chamado.

CLÁUSULA SEXTA - DO PRAZO DE VIGÊNCIA

6.1. O prazo de vigência deste Contrato será de XX (xxxxxxxxx) meses, sem prejuízo da garantia, contados da data da assinatura.

6.2. Respeitados os limites da Lei nº 14.133/2021, o presente Contrato poderá ser prorrogado, por acordo entre as partes, desde que a medida seja vantajosa para a CONTRATANTE.

CLÁUSULA SÉTIMA - DA EXECUÇÃO DO OBJETO

7.1. A CONTRATADA deverá fornecer o objeto do Contrato, atendendo ao disposto a seguir.

7.1.1. **Licenciamento**

7.1.1.1. O software e hardware deverão ser fornecidos, em sua versão mais atual, disponibilizadas no mercado, pelo fabricante. Se necessário a CONTRATADA deverá executar a configuração inicial do hardware para compatibilização inicial com o software.

7.1.1.2. A CONTRATADA deverá disponibilizar token ou arquivo de ativação da licença da solução contratada por meio eletrônico (link para download) sem ônus para a CONTRATANTE.

7.1.1.3. O objeto deverá ser entregue, conforme Especificação Técnica detalhada no Anexo I deste Contrato.

7.1.1.4. A CONTRATADA deverá fornecer um treinamento online para 06 (seis) pessoas, em tempo real ou no modo gravado no idioma português, com carga horária mínima de 24 (vinte e quatro) horas/aula. O treinamento deverá receber dos alunos avaliação média mínima de 60% (sessenta por cento) relativos aos itens: conteúdo programático, material didático (apostila, vídeos, etc.), didática do instrutor, conhecimento técnico do instrutor. Caso a avaliação do treinamento seja inferior a 60% (sessenta por cento), o treinamento deverá ser aplicado novamente para os mesmos alunos.

7.1.2. **Hardware e demais componentes da solução**

7.1.2.1. A CONTRATADA deverá fornecer equipamentos de segurança de rede do tipo Next Generation Firewall (NGFW) com suporte a funcionalidades de SD-WAN, incluindo todos os componentes necessários para o pleno funcionamento da solução.

7.1.2.2. Os equipamentos fornecidos deverão ser novos, sem uso anterior, em linha normal de fabricação pelo fabricante e acompanhados de todos os acessórios necessários à sua instalação, configuração e operação.

7.1.2.3. Os dispositivos deverão ser compatíveis com a plataforma de gerenciamento centralizado da solução SD-WAN fornecida, garantindo integração completa entre hardware e software.

7.1.2.4. A CONTRATADA deverá realizar a configuração inicial dos equipamentos, incluindo sua integração com a plataforma de gerenciamento da solução, quando necessário para o correto funcionamento da infraestrutura.

7.1.2.5. Deverão fazer parte do fornecimento todos os componentes necessários à instalação e operação dos equipamentos, incluindo cabos, fontes de alimentação, módulos de interface, kits de montagem em rack e demais acessórios requeridos.

7.1.2.6. Os equipamentos deverão ser entregues acompanhados da documentação técnica necessária para sua operação e administração, preferencialmente em idioma português ou inglês.

7.1.2.7. A CONTRATADA deverá garantir a compatibilidade dos equipamentos fornecidos com os padrões e protocolos de rede amplamente adotados no mercado, permitindo sua integração com a infraestrutura existente da CONTRATANTE.

CLÁUSULA OITAVA - DO PRAZO DE EXECUÇÃO

8.1. O prazo máximo para disponibilização do objeto contratado é de até 60 (sessenta) dias corridos, contados a partir do recebimento pela CONTRATADA da Nota de Empenho, devidamente assinada pela CONTRATANTE.

8.2. A solução deverá ser entregue mediante Nota Fiscal de Venda, de acordo com as especificações técnicas do Anexo I deste Contrato e do Termo de Referência.

CLÁUSULA NONA - DO LOCAL DE ENTREGA/EXECUÇÃO

9.1. Em caso de entrega física, o objeto deverá ser entregue no endereço a ser fornecido pela CONTRATANTE, dentro da região metropolitana de Belo Horizonte.

9.2. Entregas eletrônicas deverão ser realizadas no e-mail fornecido pela CONTRATANTE.

9.3. É necessário realizar aviso de entrega, com antecedência de 48 (quarenta e oito) horas, agendando data e horário, por meio do telefone ou email fornecidos pela CONTRATANTE.

CLÁUSULA DÉCIMA - DO PREÇO

10.1. Pelo objeto contratado, a CONTRATANTE pagará à CONTRATADA o valor total de R$ xxxxxxxxx (xxxxxxxxxxxxxxxxxxxxxxxxxxx), conforme tabela abaixo:

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
X	Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	x	R$	R$
Valor Global				R$

10.2. Estão consideradas no preço previsto no 10.1. todas as despesas diretas e indiretas decorrentes da execução contratual, inclusive tributos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA DÉCIMA PRIMEIRA – DA FORMA DE PAGAMENTO

11.1. O pagamento será realizado em até 30 (trinta) dias corridos contados do adimplemento da obrigação.

11.1.1. Considera-se adimplida a obrigação a entrega do objeto com seu aceite definitivo pela CONTRATANTE.

11.2. Os itens deverão ser entregues mediante apresentação de Nota Fiscal, de acordo com as especificações deste Contrato e do Anexo I deste Contrato e do Termo de Referência.

11.3. No preço apresentado deverá estar incluído todos os custos tais como impostos, taxas e quaisquer outros que se fizerem necessários para o perfeito cumprimento do objeto deste termo.

11.4. A CONTRATADA deverá entregar a Nota Fiscal Eletrônica e fazer constar, no mínimo, o número do Processo Administrativo, do instrumento contratual e da Nota de Empenho, descrição dos itens e período da licença, preço unitário e o valor total da Nota, dados bancários, além de todas as informações exigidas pela legislação vigente.

11.5. A Nota Fiscal Eletrônica, deverá, obrigatoriamente, vir acompanhada de comprovação da regularidade fiscal, por meio de consulta ao cadastro no SUCAF.

11.6. No caso de haver retenção, a CONTRATADA discriminará individualmente na Nota Fiscal, o percentual e o valor do(s) tributo(s) a ser(em) retido(s).

11.7. A Nota Fiscal Eletrônica deverá ser encaminhada para o endereço eletrônico da CONTRATANTE acompanhada do arquivo no formato .xml.

11.8. Caso a CONTRATADA seja enquadrada no sistema de pagamento de impostos SIMPLES, na condição de microempresa ou empresa de pequeno porte, deverá apresentar, no pagamento, à CONTRATANTE, declaração, na forma do Anexo I da Instrução Normativa RFB nº 459, de 17 de outubro de 2004 - SRF, em duas vias, assinadas pelo seu representante legal.

11.9. Não sendo observadas as condições dos itens acima, o atraso no pagamento será imputado à CONTRATADA, não decorrendo disso quaisquer ônus para a CONTRATANTE.

11.10. Os pagamentos a serem efetuados em favor da CONTRATADA estarão sujeitos, quando couber, à retenção na fonte dos tributos previstos em lei.

11.11. A CONTRATADA deverá observar, quando da emissão da Nota Fiscal, a natureza do objeto e as tributações inerentes a ele.

11.12. Considerando que a CONTRATANTE não é contribuinte do ICMS, quando se tratar de Nota Fiscal emitida por estabelecimento fora do estado de Minas Gerais, o fornecedor da mercadoria/produto deverá utilizar no campo CFOP da Nota Fiscal os códigos 6.107 ou 6.108, conforme cada caso.

CLÁUSULA DÉCIMA SEGUNDA – DA DOTAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da contratação estão programadas na seguinte dotação orçamentária: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE

13.1. O Contrato poderá ser reajustado nos termos da legislação vigente.

13.2. Somente poderão ser reajustados os preços quando observado o interregno mínimo de 12 (doze) meses contados a partir do orçamento estimado da contratação ou da

concessão do último reajuste, tendo como indexador o IPCA (Índice Nacional de Preços ao Consumidor Amplo) do IBGE (Instituto Brasileiro de Geografia e Estatística) ou outro índice que vier substituí-lo, acumulado nos últimos 12 (doze) meses.

13.3. O reajuste somente será avaliado pela CONTRATANTE mediante solicitação expressa da CONTRATADA.

13.3.1. O reajuste supramencionado somente será pago a partir da data da referida solicitação.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA CONTRATUAL

14.1. A CONTRATADA obriga-se a apresentar garantia à CONTRATANTE, no valor de 5% (cinco por cento) do valor total do Contrato, conforme determina a Lei Federal 14.133/2021 e o Decreto 19.552/2026, podendo optar por:

14.1.1. Caução em dinheiro;

14.1.2. Seguro garantia;

14.1.3. Fiança bancária.

14.2. O recolhimento da garantia deverá ser prévio à assinatura do Contrato, nos termos da legislação aplicável à espécie.

14.3 A garantia contratual deverá ser mantida enquanto viger o Contrato.

14.4. Em se tratando de garantia prestada através de caução em dinheiro, ela deverá ser recolhida em conta corrente a ser informada pela CONTRATANTE no momento da assinatura do Contrato.

14.5. A Apólice de Seguro deverá ser emitida por Instituição autorizada pela SUSEP a operar no mercado securitário e deverá prever expressamente:

14.5.1. Responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas à CONTRATADA.

14.6. A Carta de Fiança deverá ser emitida por Instituição financeira autorizada pelo Banco Central do Brasil - BACEN para funcionar no Brasil, prevendo expressamente:

14.6.1. Renúncia expressa, pelo fiador, ao benefício de ordem disposto no artigo 827 do Código Civil.

14.7. Se a garantia for utilizada em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis contados da data em que for notificada pela CONTRATANTE.

14.8. Em caso de alteração do valor contratual, prorrogação do prazo de vigência, utilização total ou parcial da garantia pela CONTRATANTE, ou em situações outras que impliquem em perda ou insuficiência da garantia, a CONTRATADA deverá providenciar a complementação ou substituição da garantia prestada no prazo determinado pela CONTRATANTE, observadas as condições originais para aceitação da garantia estipuladas nesta Cláusula.

14.9. A garantia prestada pela CONTRATADA será liberada ou restituída após a execução e cumprimento integral do presente Contrato, nos termos da Lei 14.133/2021 e do Decreto 19.552/2026.

14.10. A garantia na modalidade caução em dinheiro será atualizada monetariamente pelo índice da caderneta de poupança quando da sua restituição, não contemplando remuneração *pro rata die*.

CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

15.1. Compete à CONTRATADA:

15.1.1. Manter, durante a vigência do Contrato, todas as condições exigidas quando da contratação, comprovando-as sempre que solicitado pela CONTRATANTE;

15.1.2. Comunicar a imposição de penalidade que acarrete o impedimento de contratar com a CONTRATANTE, bem como a eventual perda dos pressupostos para a participação de licitação, nos termos da Lei 14.133/2021;

15.1.3. Cumprir as obrigações dentro dos prazos assinalados;

15.1.4. Responder pela qualidade e execução do objeto, observando as normas éticas e técnicas aplicáveis;

15.1.5. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto deste Contrato em que se verificarem vícios, defeitos ou incorreções;

15.1.6. Apresentar as informações solicitadas e os documentos comprobatórios do adequado cumprimento das obrigações;

15.1.7. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pela CONTRATANTE, relacionados ao objeto;

15.1.8. Reparar todos os danos e prejuízos causados à CONTRATANTE ou a terceiros, não restando excluída ou reduzida esta responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por parte da CONTRATANTE;

15.1.9. Não infringir quaisquer direitos autorais, patentes ou registros, inclusive marcas, know-how ou trade-secrets, durante a execução do objeto contratado, sendo responsável pelos prejuízos, inclusive honorários de advogado, custas e despesas decorrentes de qualquer medida ou processo judicial ou administrativo iniciado em face da CONTRATANTE, por acusação da espécie;

15.1.10. Garantir como "segredos comerciais e confidenciais" quaisquer informações, dados, processos, fórmulas, utilizando-os apenas para as finalidades

previstas neste contrato, não podendo revelá-los ou facilitar sua revelação a terceiros;

15.1.11. Responsabilizar-se pelo cumprimento dos requisitos definidos pela Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no que se refere ao tratamento de dados pessoais, à proteção dos direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural, bem como ao cumprimento no disposto na RESOLUÇÃO CD/ANPD Nº 19, de 23 de agosto de 2024;

15.1.12. Permitir acompanhamento e fiscalização da execução do objeto contratual pelo Fiscal;

15.1.13. Fornecer o suporte e apoio técnico para instalação, configuração e operação da solução SD-WAN, identificando falhas ou inconsistência, incluindo ainda o esclarecimento de dúvidas, de forma a garantir o funcionamento da solução;

15.1.14. Garantir assistência técnica e atualização contínua, conforme especificado no Anexo I deste Contrato e do Termo de Referência;

15.1.15. Designar 01 (um) preposto como responsável pelo Contrato para participar de eventuais reuniões e ser o interlocutor da CONTRATADA, zelando pelo fiel cumprimento das obrigações previstas neste Instrumento;

15.1.16. Entregar a solução com todos os acessórios necessários para uso imediato.

CLÁUSULA DÉCIMA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

16.1. Compete à CONTRATANTE:

16.1.1. Fiscalizar e avaliar a execução do contrato, por meio do Fiscal designado;

16.1.2. Realizar o recebimento do objeto, quando ele estiver conforme;

16.1.3. Realizar os pagamentos devidos à CONTRATADA, nas condições estabelecidas neste Contrato;

16.1.4. Exigir da CONTRATADA o cumprimento do objeto nas idênticas condições assumidas quando da celebração do Contrato;

16.1.5. Solicitar, acompanhar, fiscalizar, exercer controle, administração e gestão do Contrato assinado com a CONTRATADA para o cumprimento do objeto contratado;

16.1.6. Notificar a CONTRATADA, por escrito, fixando-lhe prazo para corrigir defeitos ou irregularidades ocorridas no recebimento do(s) item(ns) adquirido(s), sob pena de aplicação das penalidades previstas em Contrato.

CLÁUSULA DÉCIMA SÉTIMA - DAS DISPOSIÇÕES LEGAIS

17.1. Este Contrato é regulado pelas suas cláusulas, pela Lei 14.133/2021 e Decretos Municipais 11.245/2003 e 18.096/2022.

CLÁUSULA DÉCIMA OITAVA – DA DOCUMENTAÇÃO INTEGRANTE

18.1. Constituem partes integrantes do presente Contrato a proposta apresentada pela CONTRATADA, o edital da licitação Pregão Eletrônico xxxxx/xxxx e seus anexos, independentemente de transcrição, nos termos da Lei Federal 14.133/2021.

18.2. Em caso de divergência ou contradição entre as disposições dos documentos mencionados no 18.1 e as deste Contrato, prevalecerão as regras contidas no edital da licitação.

CLÁUSULA DÉCIMA NONA – DA SUBCONTRATAÇÃO

19.1. É vedado à CONTRATADA subcontratar as obrigações assumidas neste Contrato.

CLÁUSULA VIGÉSIMA – DA GESTÃO E FISCALIZAÇÃO

20.1. O Fiscal e Gestor do contrato serão designados oportunamente, mediante Portaria.

20.1. Todo o objeto será acompanhado pelo Fiscal do Contrato, que será responsável por verificar e fazer cumprir a execução do Objeto de acordo com as exigências contratuais, especificações, normas técnicas, instruções técnicas e padrões de qualidade, desde o início até o recebimento definitivo, podendo, inclusive, questionar detalhes de execução ou executados, materiais em utilização ou já utilizados, sujeitando-os a análise e aprovação.

20.2. O Fiscal deverá analisar e decidir sobre proposições da CONTRATADA que visem melhorar a execução, recomendar aplicação de advertências, multas ou outras penalidades no contrato.

20.3. O Fiscal realizará a validação do objeto executado aceitos/aprovados e tomará todas as providências e ações necessárias ao bom andamento da execução do Objeto, submetendo todos os questionamentos/comunicando ao Gestor do Contrato, em tempo hábil, qualquer ocorrência que requeira tomada de decisões ou providências que ultrapassem o seu âmbito de competência.

CLÁUSULA VIGÉSIMA PRIMEIRA - DAS ALTERAÇÕES CONTRATUAIS

21.1. Desde que não altere a natureza do objeto contratado ou descumpra o dever de licitar, o presente Contrato poderá ser alterado, por acordo entre as partes, para melhor adaptar suas previsões ao interesse da CONTRATANTE, nos termos e limites da Lei

Federal 14.133/2021.

21.2. As alterações contratuais serão formalizadas por meio de Termo Aditivo e Termo de Apostila, quando admitido.

CLÁUSULA VIGÉSIMA SEGUNDA– DA CESSÃO DO CONTRATO

22.1. O presente Contrato não poderá ser cedido ou utilizado sob qualquer hipótese como título de circulação comercial, caução, cessão de crédito e/ou documento exequível a ser apresentado contra a CONTRATANTE por terceiros.

22.2. Fica vedado à CONTRATADA transferir ou ceder, a qualquer título, os direitos e obrigações assumidos neste Contrato.

CLÁUSULA VIGÉSIMA TERCEIRA – DA PROTEÇÃO E TRANSMISSÃO DE INFORMAÇÃO, DADOS PESSOAIS E/OU BASE DE DADOS

23.1. Aplicar-se-á a este instrumento a Lei Geral de Proteção de Dados Pessoais - LGPD.

23.2. A CONTRATADA obriga-se ao dever de proteção, confidencialidade e sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso, inclusive em razão de licenciamento ou da operação dos programas/sistemas, nos termos da Lei 13.709/2018, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no presente instrumento contratual.

23.3. A CONTRATADA obriga-se a implementar medidas técnicas e administrativas suficientes visando a segurança, a proteção, à confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento não previstos.

23.4. A CONTRATADA deve assegurar-se de que todos os seus colaboradores, consultores e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo.

23.5. A CONTRATADA não poderá utilizar-se de informação, dados pessoais e/ou base de dados a que tenha acesso, para fins distintos ao cumprimento do objeto deste instrumento contratual.

23.6. A CONTRATADA não poderá disponibilizar e/ou transmitir a terceiros, sem prévia autorização escrita, informação, dados pessoais e/ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.

23.7. A CONTRATADA obriga-se a fornecer informação, dados pessoais e/ou base de dados estritamente necessários caso quando da transmissão autorizada a terceiros durante o cumprimento do objeto descrito neste instrumento contratual.

23.8. A CONTRATADA fica obrigada a devolver todos os documentos, registros e cópias que contenham informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual no prazo de 30 (trinta) dias corridos, contados da data da ocorrência de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas.

23.9. A CONTRATADA não será permitida deter cópias ou backups, informações, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.

23.10. A CONTRATADA deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja necessidade de realizar seu tratamento.

23.11. A CONTRATADA deverá notificar, imediatamente, a CONTRATANTE no caso de vazamento, perda parcial ou total de informação, dados pessoais e/ou base de dados.

23.12. A notificação não eximirá a CONTRATADA das obrigações e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.

23.13. A CONTRATADA que descumprir nos termos da Lei 13.709/2018 suas alterações e regulamentações posteriores, durante ou após a execução do objeto descrito no presente instrumento contratual fica obrigado a assumir total responsabilidade e ao ressarcimento por todo e qualquer dano e/ou prejuízo sofrido, incluindo sanções aplicadas pela autoridade competente.

23.14. A CONTRATADA fica obrigada a manter preposto para comunicação com a CONTRATANTE para os assuntos pertinentes à Lei 13.709/2018 suas alterações e regulamentações posteriores.

23.15. O dever de sigilo e confidencialidade, e as demais obrigações descritas na presente cláusula, permanecerão em vigor após a extinção das relações entre a CONTRATADA e a CONTRATANTE, bem como, entre a CONTRATADA e os seus colaboradores, subcontratados, consultores e/ou prestadores de serviços sob pena das sanções previstas na Lei 13.709/2018, suas alterações e regulamentações posteriores, salvo decisão judicial contrária.

23.16. O não cumprimento de quaisquer das obrigações descritas nesta cláusula sujeitará a CONTRATADA a processo administrativo para apuração de responsabilidade e, consequente, sanção, sem prejuízo de outras.

CLÁUSULA VIGÉSIMA QUARTA – DO SIGILO E DA CONFIDENCIALIDADE

24.1. As partes se obrigam ao dever de proteção, confidencialidade e sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso, inclusive em razão

de licenciamento ou da operação dos programas/sistemas, nos termos da Lei 13.709/2018, suas alterações e regulamentações posteriores, bem como, a Política de Privacidade e Proteção de Dados da CONTRATANTE, veiculada por meio da instrução normativa disponível em: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

CLÁUSULA VIGÉSIMA QUINTA - DA FRAUDE E CORRUPÇÃO

25.1. As partes interessadas se obrigam a cumprir e a fazer cumprir as normas contra fraude e corrupção na qual estão asseguradas medidas adequadas para proteção do interesse público.

25.2. Para a participação neste instrumento contratual, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste Contrato, ou de outra forma que não relacionada a este instrumento, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

25.3. A ocorrência de qualquer das hipóteses acima elencadas será denunciada à Controladoria Geral do Município - CTGM, para adoção das medidas cabíveis, nos termos do Decreto Municipal 16.954/2018.

CLÁUSULA VIGÉSIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

26.1. No caso de eventuais infrações cometidas ou de inadimplemento contratual, serão aplicadas as sanções previstas na Lei Federal 14.133/2021, Decretos Municipais 16.954/2018, 16.538/2016, 17.317/2020 e 18.096/2022.

CLÁUSULA VIGÉSIMA SÉTIMA – DA EXTINÇÃO E DA RESCISÃO DO CONTRATO

27.1. O presente Contrato extinguir-se-á ao seu término, sem necessidade de qualquer notificação ou interpelação ou judicial ou extrajudicial, podendo, no entanto, ser rescindido a qualquer tempo.

27.2. O presente contrato poderá ser rescindido nas hipóteses previstas na legislação, desde que formalmente motivado nos autos do processo, assegurado o contraditório e a ampla defesa, bem como nas hipóteses de a CONTRATADA:

27.2.1. Infringir quaisquer das cláusulas ou condições do presente contrato;

27.2.2. Entrar em regime de falência, dissolver-se ou extinguir-se;

27.2.3. Transferir ou ceder o presente contrato a terceiros, no todo ou em parte;

27.2.4. Recusar-se a receber qualquer ordem ou instrução para melhor execução

deste contrato, insistindo em fazê-lo com imperícia ou desleixo;

27.2.5. Deixar de comprovar o regular cumprimento de suas obrigações trabalhistas, tributárias e sociais;

27.2.6. Ser declarada inidônea e/ou suspensa e/ou impedida do direito de licitar ou contratar com a Administração Municipal;

27.2.7. Subcontratar, ceder ou transferir, total ou parcialmente o objeto contratado, exceto na hipótese de serviço secundário que não integre a essência do objeto, desde que expressamente autorizada pelo CONTRATANTE, mantida em qualquer caso a integral responsabilidade da CONTRATADA;

27.2.8. Associar-se com outrem, bem como realizar fusão, cisão, incorporação ou integralização de capital, salvo com expressa autorização do CONTRATANTE.

27.3. A rescisão do contrato poderá ser:

27.3.1. Determinada por ato unilateral e escrito da Administração, nos casos enumerados no subitem anterior;

27.3.2. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a CONTRATANTE;

27.3.3 Judicial, nos termos da legislação.

27.4. Este contrato poderá ser rescindido por ato unilateral do CONTRATANTE, devidamente justificado, quando o interesse público assim o exigir, sem indenização à CONTRATADA, a não ser em caso de dano efetivo disso resultante.

CLÁUSULA VIGÉSIMA OITAVA – DOS CASOS OMISSOS

28.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei Federal 14.133/2021 e demais normas aplicáveis.

CLÁUSULA VIGÉSIMA NONA – DAS DISPOSIÇÕES GERAIS

29.1. A tolerância da CONTRATANTE com qualquer atraso ou inadimplência por parte da CONTRATADA, não importará de forma alguma em alteração ou novação da obrigação.

29.2. A CONTRATADA autoriza a CONTRATANTE a descontar o valor correspondente aos referidos danos ou prejuízos diretamente das faturas pertinentes aos pagamentos que lhe forem devidos, independentemente de qualquer procedimento judicial ou extrajudicial, assegurada a prévia defesa.

29.3. A ausência ou omissão da fiscalização da CONTRATANTE não eximirá a CONTRATADA das responsabilidades previstas neste Contrato.

29.4. Todas as alterações que se fizerem necessárias serão registradas por intermédio de lavratura de Termo Aditivo ou Termo de Apostila, quando couber.

29.5. Os direitos decorrentes deste Contrato, não poderão em hipótese alguma, ser

negociados com instituições financeiras, não se responsabilizando a CONTRATANTE por quaisquer consequências oriundas de tais transações, respondendo, ainda, o Fornecedor por perdas e danos.

CLÁUSULA TRIGÉSIMA - DA PUBLICAÇÃO

30.1. A publicação do extrato do presente contrato no Diário Oficial do Município – DOM correrá por conta e ônus da CONTRATANTE.

30.2. A CONTRATADA fica ciente de que ocorrerá a publicação de todos os documentos apresentados durante o processo licitatório e instrumentos jurídicos celebrados, que serão publicados em Portal de Transparência com acesso livre, para fins de cumprimento da Lei de Acesso à Informação.

CLÁUSULA TRIGÉSIMA PRIMEIRA – DO FORO

31.1. É competente o foro de Belo Horizonte/MG para a solução de eventuais litígios decorrentes deste contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

E por estarem justos e contratados, firmam o presente instrumento em 02 (duas) vias de igual teor e forma.

Belo Horizonte, de de 202X.

Xxxxxxxxxxx	Xxxxxxxxxxxxxxxx
CONTRATANTE	CONTRATADA

ANEXO I - ESPECIFICAÇÃO TÉCNICA

1. SOLUÇÃO NGFW COM FUNCIONALIDADES SD-WAN TIPO 1 PARA DATA CENTER, COM SERVIÇO DE INSTALAÇÃO, SUPORTE, TREINAMENTO E GARANTIA DE 60 MESES.

1.1. CARACTERÍSTICAS GERAIS – NGFW DATA CENTER:

1.1.1. A solução deve possuir capacidade de gerenciamento inteligente de múltiplos links WAN (internet, MPLS, banda larga) com seleção dinâmica e automática baseada em desempenho, latência, perda de pacotes, jitter, disponibilidade, carga e tipo de aplicação. A solução deve permitir políticas de roteamento por aplicação, garantindo que o tráfego crítico utilize sempre o melhor caminho disponível, com suporte a endereçamentos estáticos e dinâmicos. Todas as funcionalidades de SD-WAN, incluindo orquestração, monitoramento, análise e controle, devem funcionar de forma completamente autônoma, sem necessidade de contratação de serviços adicionais em nuvem ou dependência de controladores externos, garantindo soberania dos dados e independência operacional com gerenciamento on-premises completo.

1.1.2. O sistema deve realizar monitoramento contínuo e em tempo real da qualidade dos links WAN, incluindo medição de latência, jitter, perda de pacotes e banda disponível, por meio de métodos ativos (probes sintéticas) e passivos (análise do tráfego real). A solução deve ser capaz de medir o status de saúde do link com base em métricas de desempenho e thresholds configuráveis, que servirão como fatores de decisão nas regras de SD-WAN. Os resultados de desempenho devem ser apresentados em formato gráfico através da interface de gerenciamento, permitindo análise em tempo real e histórica com identificação proativa de degradação de performance. A solução deve oferecer visibilidade completa do consumo de banda por aplicação, incluindo identificação de aplicações por assinatura (não apenas por porta), com métricas de performance por tipo de tráfego e capacidade de priorização dinâmica.

1.1.3. O equipamento deve realizar comutação automática e transparente do tráfego entre os links disponíveis baseado em regras definidas pelo usuário, incluindo contadores de latência, perda de pacotes,

disponibilidade e carga. O failover deve ocorrer em milissegundos para aplicações críticas, sem interrupção de sessões estabelecidas. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a qualidade do link é modificada.

1.1.4. A solução deve suportar a criação e gerenciamento de no mínimo 2000 regras que combinem comportamento de tráfego e segurança, permitindo políticas granulares por:

- Aplicação (com reconhecimento por assinatura, independente de porta e protocolo);
- Usuário e grupos do Active Directory/LDAP;
- Origem e destino;
- Horário;
- Qualidade do link (baseada em latência, jitter, perda de pacotes e largura de banda).

1.1.4.1. As regras devem ser processadas sem degradação significativa de performance, suportando integração com funcionalidades de firewall, VPN, NAT, IPS, Antivírus e Filtro Web.

1.1.5. A solução deverá suportar, no mínimo, os seguintes métodos de roteamento SD-WAN:

- Manual: prioridades atribuídas manualmente às interfaces;
- Melhor Qualidade: priorização baseada na qualidade do link (latência, jitter, perda, banda);
- Menor Custo: priorização baseada no custo atribuído à interface, considerando qualidade do link;
- Balanceamento de Carga: distribuição do tráfego entre interfaces disponíveis com base em algoritmos de balanceamento e qualidade do link.

1.1.5.1. Deve suportar roteamento dinâmico BGP com IPv6 e permitir a configuração de políticas de QoS em protocolos e aplicações de camada 7, associadas percentualmente à largura de banda da interface SD-WAN.

1.1.6. A solução deve possuir mecanismos de correção de perda de pacotes em tempo real para otimizar o desempenho e a confiabilidade de links WAN e túneis VPN, especialmente para aplicações sensíveis a perdas (áudio, VoIP, videoconferência). Estes mecanismos devem incluir: Correção de Erro Antecipada (Forward

Error Correction - FEC), com capacidade de ajuste dinâmico da relação entre pacotes base e redundantes com base nas condições do link em tempo real e métricas de SLA; Mecanismos de mitigação de perdas que possam ser ativados seletivamente por aplicação ou política, baseados em thresholds de perda de pacotes configuráveis.

1.1.6.1. Os recursos devem ser compatíveis com as topologias hub-spoke e full-mesh, e aplicáveis a aplicações específicas para otimizar o uso de recursos de banda e processamento.

1.1.7. A solução deve suportar múltiplos métodos de health check para monitorar a disponibilidade e qualidade dos links WAN e servidores de destino, permitindo a tomada de decisão em políticas de SD-WAN e balanceamento de carga. Os métodos devem incluir, no mínimo:

- Ping (ICMP) para verificação básica de conectividade;
- Verificações em camada 4 (TCP/UDP) em portas configuráveis;
- Verificações em camada 7 (HTTP/HTTPS) com validação de resposta.

1.1.7.1. A solução deve suportar health check ativo (probes sintéticas criadas pelo administrador) e passivo (utilizando o próprio tráfego do usuário para inferir condições dos links).

1.1.8. A solução deve ser capaz de prover arquitetura onde, em comunicação Data Center (DC) x Unidades Remotas (UR) com link comprometido entre UR-A e DC possa ser utilizado o circuito entre UR-B e DC para que UR-A alcance o DC.

1.1.8.1. Deve ser capaz de criar VPN "Full-Mesh" dinâmica, com túneis entre pontas remotas criados sob demanda e encerrados quando o tráfego cessar, evitando escoamento via hub. A configuração VPN IPSEC deve oferecer suporte para DH Group 14 e 15.

1.1.9. A solução deve fornecer reconhecimento default em camada 7 de, pelo menos, 2000 aplicações largamente utilizadas em contextos de SaaS, nuvem e multimídia (ex: Vimeo, YouTube, Facebook). O reconhecimento deve ser realizado independente de porta e protocolo, inspecionando o payload do pacote, totalmente segregado da camada 4. Deve contar com banco de dados interno

onde seja possível atrelar uma aplicação a um IP/range de IPs de destino.

1.1.10. A solução deve suportar múltiplas instâncias de tabelas de roteamento VRF (Virtual Routing and Forwarding) para segmentar tráfego L3 de forma lógica dentro do mesmo appliance, garantindo que pacotes sejam encaminhados apenas entre interfaces pertencentes ao mesmo VRF. Deve ser possível associar interfaces físicas, subinterfaces e interfaces virtuais (incluindo VLANs e túneis VPN) a VRFs específicas de forma determinística, com rotas, políticas e encaminhamento totalmente separados por VRF.

1.1.11. A solução deve suportar rotas estáticas e protocolos de roteamento dinâmico (BGP e OSPF) em instâncias VRF distintas, incluindo capacidade de configurar múltiplos processos por VRF para cenários multi-tenant ou separação de roteamento. As VRFs devem interoperar com funcionalidades de VPN, NAT, inspeção de segurança, políticas de firewall e SD-WAN, preservando isolamento quando requerido e permitindo exceções controladas para roteamento entre VRFs apenas mediante regras explícitas de trânsito ou rotas compartilhadas.

1.1.12. A solução deve ter capacidade de coletar telemetria, tabelas de rota, sessões ativas e logs com capacidade de segregação por domínio lógico (VRF, tenant, ou instância de roteamento), para suporte a troubleshooting, auditoria e integração com sistemas de monitoramento centralizados.

1.1.13. A solução deve permitir a criação de endereços IPs virtuais e balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais. Deve suportar balanceamento para os serviços HTTP, HTTPS, TCP e UDP, com os seguintes métodos:

- Endereço IP de origem ou Static;
- Round Robin;
- Weighted;
- First Alive e HTTP host;
- Least Session;
- Least RTT.

1.1.14. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID, e suportar SSL/TLS offloading para descarregamento do processamento criptográfico dos servidores.

1.1.15. A solução deve ter capacidade de identificar, através de health checks, quais servidores reais estão ativos em configurações de balanceamento de carga, removendo automaticamente o tráfego dos servidores indisponíveis. Deve permitir health checks periódicos, no mínimo, via:

- ICMP (ping) para verificação básica;
- TCP em portas configuráveis;
- HTTP/HTTPS com validação de código de resposta ou conteúdo específico.

1.2. ESPECIFICAÇÕES DE HARDWARE – NGFW DATA CENTER

1.2.1. 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. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

1.2.2. Deve possuir, pelo menos, 04 (quatro) interfaces SFP28 GE, 04 (quatro) interfaces SFP+ 10GE, todas interfaces com seus respectivos transceptores ópticos [SR] do próprio fabricante.

1.2.3. Deverá ser entregue também a seguinte quantidade de transceptores ópticos [LR]:

- **02 Transceivers:**
  - Protocol Standard: 25GBase-LR, 10GBase-LR
  - IEEE Standard: 802.3cc
  - Module Type: SFP28
  - Data Link Rate for Ethernet: 25.78 Gbps
  - Transmission Range: 10 km
  - Media: SM (Single-Mode)
  - Connector Type: Duplex LC
- **02 Transceivers:**
  - Protocol Standard: 10GBase-LR

- IEEE Standard: 802.3ae
- Module Type: SFP+
- Data Link Rate for Ethernet: 10 Gbps
- Transmission Range: 10 km
- Media: SM (Single-Mode)
- Connector Type: Duplex LC

1.2.4. O equipamento deve possuir no mínimo 14 (quatorze) portas Ethernet de 1 Gigabit com conector RJ45 (cobre), para conectividade com equipamentos locais, servidores, switches de acesso e segmentos LAN.

1.2.5. Deve possuir porta de gerenciamento dedicada e exclusiva (out-of-band) com conector RJ45, isolada do tráfego de produção, permitindo acesso administrativo seguro mesmo em caso de falhas na configuração de rede ou comprometimento de segurança das interfaces de dados.

1.2.6. Deve dispor de porta console para acesso direto ao equipamento através de USB, RJ45 ou DB9 (RS232), esta interface é essencial para configuração inicial, troubleshooting e recuperação de desastres quando o acesso via rede não está disponível.

1.2.7. O equipamento deve possuir capacidade de Captive Portal integrado, permitindo autenticação de usuários via página web antes de liberar acesso à internet. Deve suportar múltiplos métodos de autenticação incluindo login/senha local, integração com Active Directory/LDAP, RADIUS, autenticação por redes sociais e customização completa da página de login com logotipo e mensagens da organização. Esta funcionalidade é essencial para controle de usuários, aplicação de políticas granulares por usuário/grupo e auditoria de acesso.

1.2.8. A solução deve implementar backup automático e programável de configurações através da interface web de gerenciamento, incluindo versionamento, agendamento de backups periódicos, armazenamento local e remoto (FTP/SFTP/SCP), notificações por e-mail e capacidade de restore rápido com rollback para versões anteriores.

1.2.9. Deve possuir obrigatoriamente sistema de armazenamento interno dedicado composto por, no mínimo, 02 (duas) unidades de disco do tipo SSD (Solid State Drive), operando nativamente em

configuração de espelhamento (RAID 1) para garantir a integridade, redundância e alta disponibilidade dos dados em caso de falha física de uma das unidades. O armazenamento local deve ser utilizado pelo sistema operacional para as seguintes finalidades:

- Autonomia Forense e Auditoria Local: Garantir a persistência de registros de tráfego e capturas completas de pacotes (PCAP) diretamente no hardware por um período mínimo de 07 (sete) dias, assegurando a visibilidade para investigação de incidentes mesmo após reinicializações do sistema ou interrupções de conectividade
- Resiliência e Buffering de Logs: Atuar como buffer de contingência para armazenamento temporário de registros de eventos e estatísticas, garantindo que nenhum dado de conformidade (compliance) seja perdido caso a plataforma de análise centralizada esteja temporariamente inacessível.
- Performance de Inspeção Profunda: Suportar o banco de dados local para técnicas de detecção baseadas em impressão digital de documentos (DLP) e otimização de tráfego, permitindo a tomada de decisão de segurança em alta velocidade sem dependência de consultas constantes a bases de dados externas.

1.3. CAPACIDADE E PERFORMANCE – NGFW DATA CENTER

1.3.1. Taxa de transferência com IPS (Intrusion Prevention System) habilitado deve ser de no mínimo 40 Gbps, garantindo inspeção profunda de pacotes sem gargalos de performance mesmo em cenários de tráfego intenso.

1.3.2. A taxa de transferência com todas as funcionalidades NGFW ativas (firewall, application control, IPS, antivírus) deve ser de no mínimo 30 Gbps, assegurando proteção abrangente sem degradação significativa de desempenho.

1.3.3. A capacidade de processamento de Threat Prevention (IPS, antivírus, anti-spyware) ativa deve ser de no mínimo 28 Gbps.

1.3.4. A solução deve apresentar capacidade de processamento em camada 3 para tráfego IPv4/IPv6 com diferentes perfis de pacotes, garantindo performance wire-speed em cenários heterogêneos. A solução deve sustentar, no mínimo, 150 Gbps para pacotes de 1518

bytes, 150 Gbps para pacotes de 512 bytes e 140 Gbps para pacotes de 64 bytes, além de 100 milhões de pacotes por segundo (Mpps) com pacotes de 64 bytes em cenário stateful full-duplex, conforme metodologia RFC 2544 ou RFC 9411. A latência interna para pacotes de 64 bytes não deverá exceder 8 microssegundos sob carga nominal. Este desempenho deve ser mantido de forma determinística mesmo com a aplicação simultânea de políticas de firewall e inspeção de tráfego, sem comprometimento da estabilidade operacional ou degradação da capacidade de gerenciamento do equipamento.

1.3.5. A solução deve suportar no mínimo 14,5 milhões de sessões TCP simultâneas, garantindo capacidade para grandes volumes de usuários e aplicações concorrentes sem limitações artificiais impostas por licenciamento.

1.3.6. A solução deve suportar no mínimo 695.000 novas conexões TCP por segundo, garantindo capacidade para ambientes web, APIs e aplicações com alta frequência e volume de abertura de conexões, sem limitações artificiais impostas por licenciamento.

1.3.7. A solução deve suportar no mínimo 28.000 políticas de firewall, permitindo segmentação granular e controles detalhados sem impacto em performance ou limitações artificiais impostas por licenciamento.

1.4. FUNCIONALIDADES DE REDE – NGFW DATA CENTER

1.4.1. A solução deve possuir suporte completo e nativo aos protocolos IPv4 e IPv6 em todas as funcionalidades, incluindo roteamento, firewall, NAT, DHCP, VPN e monitoramento. Deve suportar dual-stack e mecanismos de transição IPv4/IPv6, como NAT64 e NAT46, garantindo interoperabilidade em ambientes heterogêneos.

1.4.2. A solução deve implementar protocolos avançados de roteamento, incluindo:

- Roteamento estático e dinâmico com OSPF (para roteamento interno), BGPv4 (para roteamento externo com múltiplos uplinks) e ISIS
- Policy Based Routing (PBR) para desvios de tráfego baseados em políticas
- VRF (Virtual Routing and Forwarding) para segmentação lógica de redes com tabelas de roteamento independentes

- VRRP (Virtual Router Redundancy Protocol) para redundância de gateway
- MPLS para redes corporativas avançadas
- VXLAN para overlay networks e virtualização de rede
- Roteamento e forwarding multicast com protocolos PIM-SM e PIM-DM

1.4.2.1. As VRFs devem interoperar com funcionalidades de VPN, NAT, inspeção de segurança, políticas de firewall e SD-WAN, preservando isolamento quando requerido e permitindo exceções controladas para roteamento entre VRFs apenas mediante regras explícitas.

1.4.3. A solução deve suportar o padrão IEEE 802.1Q com capacidade para configurar no mínimo 4094 VLANs simultaneamente, permitindo ampla segmentação de rede e isolamento de tráfego. Deve permitir a criação de VLANs nativamente e operar nos modos bridge (transparente), router, proxy explícito, sniffer e/ou VLAN-tagged. Deve suportar LACP (IEEE 802.3ad) para agregação de múltiplas interfaces físicas em um único link lógico, aumentando a banda disponível e provendo redundância de enlaces. Em modo transparente, deve funcionar sem alterar o endereço MAC do tráfego, permitindo filtro de pacotes em camada 2 e forwarding para protocolos não IP.

1.4.4. A solução deve suportar tradução de endereços estáticos (NAT 1:1, muitos:1, NAT64, NAT46) e dinâmicos (PAT, muitos:1). Deve incluir funcionalidades de STUN, Full Cone NAT, permitir filtro de pacotes com e sem NAT, e possibilitar abertura dinâmica de portas para serviços que requerem portas dinâmicas (session-helpers ou ALGs). Deve suportar DHCP Cliente, Servidor e Relay para IPv4 e IPv6 (DHCPv6), com funcionalidades avançadas como:

- Múltiplos pools de endereços
- Reservas por endereço MAC
- Opções customizadas
- DNS dinâmico (DDNS)
- Relay DHCP para segmentos remotos

1.4.5. A solução deve possuir implementação robusta de QoS (Quality of Service) permitindo:

- Classificação de tráfego por múltiplos critérios: aplicação, IP de origem/destino, porta, protocolo, DSCP, VLAN, usuário/grupo
- Marcação de pacotes com modificação de valores DSCP para DiffServ
- Priorização de tráfego com suporte a ToS (Type of Service)
- Limitação de banda (rate limiting) e garantia de banda mínima para aplicações críticas
- Criação de filas de prioridade e gerenciamento de congestionamento

1.4.5.1. Deve permitir definir banda máxima e banda garantida por:

- Usuário ou grupo de usuários (integrado a Active Directory/LDAP)
- Endereço IP (origem/destino)
- Sub-rede (origem/destino)
- Protocolo
- Aplicação (incluindo peer-to-peer, streaming, chat, VoIP, Web)

1.4.5.2. A definição de banda deve ser possível tanto por valor absoluto quanto por percentual.

1.4.6. A solução deve suportar alta disponibilidade (HA) nos modos ativo-passivo e ativo-ativo com divisão de carga, mantendo todas as licenças de software habilitadas sem perda de conexões. Deve suportar VRRP para redundância de gateway e possuir funcionalidade de balanceamento e contingência de links de internet.

1.4.7. A solução deve oferecer:

- Ferramenta de diagnóstico do tipo tcpdump ou similar para captura e análise de tráfego
- Porta de comunicação serial ou USB para acesso local protegido por usuário/senha
- Suporte a sFlow para monitoramento de tráfego
- Comunicação criptografada entre estação de gerência e appliance (interface gráfica e CLI)

1.4.7.1. SNMP: Implementação completa dos protocolos SNMP versões 1, 2c e 3 para integração com sistemas de monitoramento e gerenciamento de rede, com suporte a

MIBs padrão e específicas do fabricante. SNMPv3 deve incluir autenticação e criptografia.

1.4.7.2. APIs e Automação:

- Exposição de APIs RESTful completas e documentadas para orquestração e automação (políticas de segurança, objetos de rede, logs, operações de manutenção)
- Suporte a execução automatizada de playbooks baseados em eventos (isolamento de endpoint, alteração de políticas, bloqueio de rede)
- Integração direta com plataformas SOAR via webhook e API
- Recursos de automação para operações diárias: execução de scripts, envio de e-mails, notificações via Teams, agendamentos, resposta a eventos de rede/segurança

1.4.8. A solução deve oferecer autenticação de usuários em base local e integração com servidores:

- RADIUS (autenticação, autorização e accounting)
- TACACS+ (com suporte a autorização por comando e accounting detalhado)
- LDAP e Microsoft Active Directory (reconhecimento de contas e grupos)

1.4.8.1. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Active Directory/LDAP, permitindo criação de regras baseadas em usuário e grupo. Deve suportar:

- Autenticação de dois fatores com integração a tokens
- Single-sign-on via Active Directory, RADIUS e SAML
- Autenticação para tráfego HTTP, HTTPS, FTP e Telnet
- IP/MAC binding para controle de endereços internos e prevenção de IP spoofing

1.4.9. A solução deve suportar certificados digitais X.509, SCEP (Simple Certificate Enrollment Protocol), CSR (Certificate Signing Request) e OCSP (Online Certificate Status Protocol), garantindo autenticação segura e comunicação criptografada.

1.4.10. Deve possuir mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações como: dcerpc, DNS (TCP/UDP), FTP, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, SCCP, TFTP e TNS. Deve suportar aplicações multimídia (H.323, SIP) e técnicas de detecção de programas peer-to-peer e mensagens instantâneas.

1.4.11. A solução deve possuir tecnologia de firewall stateful, mecanismo de anti-spoofing e permitir:

- Criação de serviços por porta ou conjunto de portas (TCP, UDP, ICMP, IP)
- Agrupamento de serviços para facilitar administração
- Criação de regras definidas pelo usuário
- Objetos e agrupamentos de objetos (usuários, redes, FQDN, protocolos, serviços)

1.4.11.1. Deve permitir controle de acesso por:

- Endereço IP de origem/destino
- Sub-rede
- Domínio (ex: gov.br, org.br)
- Períodos do dia e dia da semana
- Usuário e grupo de usuários
- Tipo de dispositivo
- Protocolo e aplicação

1.4.12. A solução deve possuir conectores com nuvens públicas (AWS, Microsoft Azure, GCP, OCI) e privadas (Kubernetes, VMware, OpenStack, Cisco ACI, Nutanix). Modificações nas clouds devem refletir automaticamente nos objetos do firewall, evitando reconfiguração manual de regras. Deve possuir integração com threat feeds para sincronismo de listas externas de IPs, MACs, domínios e hashes de malwares.

1.4.13. A solução deve suportar monitoramento em tempo real das configurações aplicadas, identificando vulnerabilidades, sugerindo boas práticas para melhoria do hardening e performance, atribuindo nota à configuração. Deve informar itens aprovados/reprovados nas validações e, para cada critério, detalhar elementos envolvidos, configuração sob validação, resultado, severidade e regra de compliance aplicável.

1.4.14. A solução deve possuir recurso para detecção de dispositivos IoT por métodos passivos (inspeção de tráfego, fingerprinting de protocolos), identificando MAC Address, IP, SO, hostname e login.

Deve buscar informações em base local e, se necessário, na nuvem do fabricante sobre vulnerabilidades associadas. Deve classificar perfil comportamental e score de risco por dispositivo baseado em anomalias de tráfego, destinos incomuns, tentativas de conexão externas e mudanças repentinas de padrão, com detecções configuráveis por perfil de risco.

1.5. FUNCIONALIDADES DE SEGURANÇA AVANÇADA – NGFW DATA CENTER

1.5.1. A solução de IPS deve estar orientada à proteção de redes, integrada nativamente à plataforma de segurança (não módulo externo), permitindo funcionamento em modo transparente, sniffer e router. Deve suportar verificação de tráfego em tempo real via aceleração de hardware e possuir capacidade de remontagem de pacotes para identificação de ataques, garantindo inspeção inline que não cause degradação significativa de performance.

1.5.2. A solução deve possuir base de assinaturas de IPS com, pelo menos, 15.000 (quinze mil) ameaças conhecidas, cobrindo exploits, buffer overflows, SQL injection, cross-site scripting, command injection, denial of service, scanning/reconnaissance, entre outras técnicas de ataque. As assinaturas devem ser atualizadas automaticamente várias vezes ao dia. Deve permitir a criação de padrões de ataque manualmente, assinaturas personalizadas via interface gráfica, e uso de operadores de negação na criação de assinaturas customizadas para permitir exceções com granularidade.

1.5.3. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão. 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 e zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS.

1.5.4. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, como por exemplo agrupar todas as

assinaturas relacionadas a web-server para proteção específica de Servidores Web, facilitando a gestão e aplicação de políticas.

1.5.5. A solução deve possuir:

- Capacidade de análise de tráfego para detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep
- Mecanismos de detecção/proteção de ataques
- Reconhecimento de padrões
- Análise de protocolos
- Detecção de anomalias
- Filtros de ataques por anomalias
- Filtros de anomalias de tráfego estatístico (flooding, scan, source e destination session limit)
- Filtros de anomalias de protocolos
- Reconhecimento de ataques de DoS, reconnaissance, exploits e evasion
- Verificação de ataque na camada de aplicação

1.5.6. A solução deve possuir proteção contra

- Ataques de RPC (Remote Procedure Call)
- Ataques Windows ou NetBios
- Ataques SMTP, IMAP, Sendmail e POP
- Ataques DNS (Domain Name System)
- Ataques a FTP, SSH, Telnet e rlogin
- Ataques ICMP (Internet Control Message Protocol)c

1.5.7. A solução deve:

- Mitigar os efeitos dos ataques de negação de serviços
- Ser imune e capaz de impedir ataques básicos como Syn flood, ICMP flood e UDP flood
- Detectar e bloquear a origem de portscans
- Bloquear ataques efetuados por worms conhecidos
- Possuir assinaturas específicas para mitigação de ataques DoS e DDoS
- Possuir assinaturas para bloqueio de ataques de buffer overflow
- Incluir proteção contra ataques de negação de serviços
- Permitir o bloqueio de vulnerabilidades e exploits conhecidos
- Identificar e bloquear comunicação com botnets

- Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos

1.5.7.1. Deve incluir proteção contra ataques nos layers 3, 4 e 7 do modelo OSI, com recursos como rate limiting por IP/subnet, blacklisting automático de atacantes e desafio CAPTCHA para validação de origem legítima.

1.5.8. A solução deve possuir as seguintes estratégias de bloqueio: pass, drop e reset. Deve ter capacidade de resposta/logs ativa a ataques, prover terminação de sessões via TCP resets e gerar logs de sessões.

1.5.9. Deve possuir recurso que coloque momentaneamente novas assinaturas em modo "monitor" apenas (detecção passiva), gerando alertas detalhados sobre atividades suspeitas sem bloqueio automático, evitando falsos positivos. Esse tempo deve permitir customização e, após o período configurado, a assinatura deve mudar para modo bloqueio automaticamente. O modo IDS deve permitir análise forense e resposta coordenada, operando em conjunto com o IPS.

1.5.10. A solução deve possuir métodos de notificação de detecção de ataques, incluindo:

- Alarmes na console de administração
- Alertas via correio eletrônico
- Monitoração do comportamento do appliance mediante SNMP (versões 1, 2c e 3), com capacidade de enviar traps quando ocorrer um evento relevante para a correta operação da rede

1.5.11. A solução deve possuir capacidade de proteção inline e em tempo real contra ameaças desconhecidas (zero-day) e malwares de última geração através de motores de Inteligência Artificial (AI) e Machine Learning (ML) integrados nativamente ao sistema operacional do equipamento. Esta proteção deve operar localmente no hardware (on-premises), sem dependência obrigatória de nuvens externas para a tomada de decisão inicial, garantindo vereditos em frações de segundo (sub-second) para a identificação e bloqueio de artefatos maliciosos antes que estes penetrem na rede interna. A solução deve suportar análise heurística avançada e

modelos de ML para tráfego criptografado e fluxos de arquivos, permitindo a detecção autônoma de ameaças nunca antes vistas, gerando registros detalhados para auditoria e tomada de decisão do analista.

1.5.12. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado (sandboxing) para análise comportamental aprofundada. A solução de sandbox deve permitir a retenção inline do arquivo, ou seja, o usuário não o receberá enquanto ele não for analisado e definido como "limpo". A análise deve incluir técnicas de heurística e machine learning, com geração de relatórios detalhados sobre o comportamento dos artefatos.

1.5.13. A solução deve suportar a captura de pacotes (PCAP) por assinatura de IPS ou regra de firewall. 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.

1.5.14. A solução deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

- Nome da assinatura ou do ataque
- Aplicação
- Usuário
- Origem da comunicação
- Destino da comunicação
- Ação tomada pelo dispositivo

1.5.14.1. Os eventos devem identificar o país de onde partiu a ameaça (geolocalização).

1.5.15. A solução deve permitir aplicação de políticas baseadas em geolocalização de endereços IP de origem e destino, incluindo bloqueio ou liberação de tráfego de/para países específicos, útil para reduzir superfície de ataque bloqueando regiões de alto risco. Deve suportar ações granulares: bloquear acesso de países específicos a determinados serviços, permitir apenas países autorizados para acesso administrativo, entre outras políticas customizáveis.

1.5.16. A solução deve permitir o bloqueio de vírus e spywares em tempo real através de scanning de arquivos em, pelo menos, os seguintes

protocolos: HTTP e HTTPS, FTP, SMB, SMTP, POP3, IMAP. Deve utilizar múltiplas engenharias de detecção, incluindo análise heurística e comportamental, com suporte a scanning de arquivos compactados e criptografados (quando possível).

1.5.17. A solução deve oferecer bloqueio de domínios maliciosos via DNS, com integração a feeds de inteligência de ameaças, interceptando queries DNS e bloqueando resoluções de domínios associados a malware, phishing, botnet C&C, sites de ransomware, proxies anônimos e TOR exit nodes, de forma transparente aos usuários e aplicações. A proteção deve ser aplicada de forma automática e dinâmica.

1.5.18. A solução deve suportar Dynamic DNS (DDNS) permitindo atualização automática de registros DNS quando endereços IP públicos mudam, essencial para links de internet dinâmicos, com suporte aos principais provedores de DDNS do mercado e configuração de múltiplos domínios.

1.5.19. A solução deve possuir proteção em tempo real contra URLs maliciosas e phishing através de categorização dinâmica e análise de reputação. Deve bloquear acesso a sites comprovadamente maliciosos, páginas de phishing bancário, sites de distribuição de malware e destinos utilizados em campanhas de ataques direcionados, com suporte a listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra). A base de categorias deve conter no mínimo 60 categorias e 60 milhões de sites classificados.

1.5.20. A solução deve permitir identificação e controle granular de milhares de aplicações através de assinatura profunda (não apenas porta/protocolo), reconhecendo aplicações criptografadas, tuneladas e que utilizam portas não padrão. Deve permitir controles por aplicação: bloquear, permitir, limitar banda, aplicar QoS, registrar logs, entre outros. Cobertura mínima de 3.000 aplicações identificáveis, com pelo menos 20 categorias de classificação.

1.5.21. A solução deve possuir integração com threat feeds para sincronismo de listas externas de IPs, MACs, domínios e hashes de malwares, com atualização automática e frequente, garantindo bloqueio proativo contra ameaças emergentes.

1.5.22. A solução deve possuir capacidade de inspeção de tráfego criptografado SSL/TLS através de técnicas de descriptografia controlada, permitindo inspeção e re-criptografia de tráfego HTTPS, garantindo que malware, ataques e vazamento de dados não se escondam sob criptografia. Deve suportar listas de exceção para sites bancários, de saúde e outros que não devem ser inspecionados, com compatibilidade para TLS 1.2 e 1.3.

1.6. DLP (Segurança de dados) – NGFW DATA CENTER

1.6.1. O equipamento deve possuir funcionalidade de **DLP** (Data Loss Prevention) para prevenir vazamento de dados sensíveis através de múltiplos protocolos (HTTP, HTTPS, FTP, SMTP, etc.). Deve suportar detecção baseada em: padrões de expressões regulares (CPF, cartão de crédito, etc.), fingerprinting de documentos, palavras-chave customizadas e marcadores de classificação de dados. Deve permitir ações como: bloquear transmissão, alertar, quarentenar, aplicar watermark, etc.

1.6.2. O motor de detecção DLP deve operar de forma integrada e simultânea com múltiplas técnicas de identificação:

- Padrões predefinidos: bases de dados atualizadas para documentos nacionais (CPF, CNPJ, RG, passaporte), credenciais de acesso e cartões de pagamento (crédito/débito)
- Expressões regulares customizáveis: criação de padrões específicos para cada ambiente
- Bibliotecas de palavras-chave: dicionários com suporte a múltiplos idiomas
- Reconhecimento de etiquetas de sensibilidade (Sensitivity Labels): integração com ecossistemas de classificação de dados, como Microsoft Purview, para identificação baseada em metadados e classificação nativa de documentos
- Fingerprinting de documentos: identificação por impressão digital (hash) de documentos exatos, com capacidade de criação e atualização automatizada de bases de fingerprinting através de varredura programada em servidores de arquivos externos via protocolo de rede (SMB/CIFS, NFS)

- Assinaturas contextuais e por conteúdo: análise baseada em contexto para redução de falsos positivos

1.6.3. A solução deve oferecer inspeção de tráfego criptografado SSL/TLS com controles granulares para aplicação de políticas DLP em conexões HTTPS, garantindo que dados sensíveis não sejam exfiltrados através de canais seguros. Deve permitir:

- Exceções por domínio: lista de sites bancários, de saúde e outros que não devem ser inspecionados por requisitos de privacidade ou conformidade
- Mascaramento de dados: ocultação parcial de informações sensíveis em logs e alertas
- Controle por categoria: aplicar inspeção seletiva baseada em categorias de URL ou reputação de destino
- Compatibilidade com TLS 1.2 e 1.3

1.6.4. A solução deve integrar-se a serviços de inteligência de ameaças e catálogos centralizados de assinaturas/padrões para receber atualizações automáticas e frequentes de:

- Novos tipos de dados sensíveis
- Padrões de detecção atualizados
- Regras DLP recomendadas
- Indicadores de comprometimento (IOCs) relacionados a vazamento de dados

1.6.4.1. A integração deve garantir que a proteção DLP permaneça efetiva contra novas formas de exfiltração e ameaças emergentes, sem necessidade de intervenção manual constante.

1.7. IoT/OT – NGFW DATA CENTER

1.7.1. Identificação automática e passiva de dispositivos IoT na rede através de análise de tráfego, fingerprinting e machine learning. Deve classificar dispositivos por tipo (câmeras IP, sensores, smart TVs, impressoras, etc.), fabricante e modelo, permitindo aplicação de políticas específicas de segmentação e controle para dispositivos IoT que geralmente possuem vulnerabilidades.

1.7.1.1. Proteção específica para ambientes de Tecnologia Operacional (OT) e sistemas industriais (SCADA, ICS). Deve incluir: identificação de protocolos industriais (Modbus,

DNP3, OPC, etc.), detecção de anomalias em comunicações OT, segmentação entre redes IT e OT, proteção contra ataques direcionados a ambientes industriais e visibilidade específica para ativos OT.

1.8. FILTRO DE CONTEÚDO WEB – NGFW DATA CENTER

1.8.1. A solução deve possuir solução de filtro de conteúdo Web integrado à solução de segurança, com suporte a Proxy Explícito e Transparente, devendo implementar roteamento WCCP e ICAP ou mecanismos equivalentes que permitam a integração com proxies externos, sistemas de cache, soluções de descarregamento de tráfego e inspeção avançada de conteúdo, garantindo a mesma funcionalidade e performance. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web. Deve filtrar o conteúdo baseado em categorias em tempo real, permitindo a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

1.8.2. A solução deve possuir, pelo menos, 60 (sessenta) categorias para classificação de sites Web, com base mínima contendo 60.000.000 (sessenta milhões) de sites internet Web já registrados e classificados. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP, permitindo a reclassificação de sites Web por ambos os critérios. Deve possuir a funcionalidade de cota de tempo e banda consumida por categoria.

1.8.3. A solução deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web:Proxy anônimo; Webmail;Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras; Inteligência artificial; Criptomoedas.

1.8.4. A solução deve permitir:

- Criação de categorias personalizadas;
- Criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
- Criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, por endereço IP de origem e por sub-rede de origem;
- Recurso do tipo "safe search" ou similar em sites de buscas, filtrando o resultado de pesquisas efetuadas em tais sites que apresentem conteúdo nocivo.

1.8.5. A solução deve prover mecanismo de aceite ou aviso ao usuário (podendo ser customizável, aceitando idioma português), a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado, incluindo a capacidade de exibir páginas de bloqueio customizáveis, termos de aceite, avisos de conformidade ou políticas de uso aceitável, garantindo que o usuário seja informado e, quando necessário, confirme o entendimento antes de prosseguir. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.

1.8.6. A solução deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, permitindo a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

1.8.7. A solução deve permitir:

- Filtragem de conteúdo do tráfego WEB de URLs conhecidas em applets Java, cookies e activeX;
- Bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
- Bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
- Bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.

1.8.8. A solução deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.

1.9. LICENCIAMENTO - NGFW DATA CENTER

1.9.1. Deve possuir e estar licenciado durante a vigência da garantia de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, SD-WAN, Traffic Shapping e QoS, Filtro de Conteúdo Web, retenção inline de malwares desconhecidos, Inline CASB, Detecção e descoberta de vulnerabilidades de dispositivos IoT, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de

Aplicações, Prevenção de Perda de Dados (DLP) e Avaliação de Risco e Compliance (hardening).

1.9.2. O licenciamento da solução deve incluir todas as funcionalidades de segurança e SD-WAN especificadas neste documento, sem qualquer limitação artificial imposta por licenciamento quanto a número de VLANs, políticas de firewall, regras de SD-WAN, túneis VPN, sessões simultâneas ou quaisquer outros recursos de software do equipamento, ressalvadas as limitações físicas inerentes à capacidade do hardware adquirido, as quais deverão estar claramente especificadas na ficha técnica do modelo ofertado.

1.9.3. A empresa licitante deverá provisionar junto aos contratos de "Garantia" e "Suporte do Fabricante", junto ao fabricante da solução ofertada, garantia técnica total pelo fabricante da Solução pelo período mínimo de 60 (sessenta) meses, incluindo suporte técnico em regime de atendimento de 24x7 (vinte e quatro horas, sete dias por semana), contados a partir da data de emissão do atestado de recebimento definitivo dos bens e materiais (hardwares, softwares e licenciamentos) pela CONTRATANTE. Deverá possuir atendimento, com retorno rápido para questões críticas, em até 30 minutos, e para questões não críticas em até 4 horas úteis, por especialistas cibernéticos do próprio fabricante da Solução ofertada.

1.9.4. Para os serviços de suporte e assistência técnica para serviços de trocas ou reparo de peças (referentes aos componentes de hardwares), estes devem possuir prazo de solução no dia útil subsequente com atendimento em, no máximo 48h (quarenta e oito horas), a partir do recebimento do item de troca ou reparo, enviado pelo seu fabricante correlacionado.

1.9.5. **SUPORTE 24X7**

1.9.5.1. A CONTRATADA deve fornecer ou garantir suporte técnico 24 horas por dia, 7 dias por semana, 365 dias por ano, diretamente do fabricante ou através de parceiro autorizado com SLA garantido. O suporte deve incluir: abertura de chamados por telefone, e-mail e portal web, atendimento preferencialmente em português, acesso a base de conhecimento, downloads de firmware e documentação.

1.9.6. **ATUALIZAÇÃO E CORREÇÃO DE VULNERABILIDADES POR PATCHES**

1.9.6.1. O fabricante deve disponibilizar atualizações de firmware/software e patches de segurança de forma regular e responsiva. As atualizações devem poder ser aplicadas SEM perda de configurações e COM equipamento em produção (quando possível aplicação com baixo impacto). Deve incluir atualizações de: assinaturas de IPS, antivírus, categorização de URLs, feeds de inteligência de ameaças, firmware do sistema operacional e correções de CVEs.

1.9.7. **SLA DE CORREÇÃO DE PATCHES BEM DEFINIDO PELO FABRICANTE**

1.9.7.1. O fabricante deve publicar e manter uma política formal e pública de SLA para lançamento de patches de correção de vulnerabilidades de segurança e falhas do produto. Esta política deve definir prazos máximos de resposta baseados na criticidade da vulnerabilidade (crítica, alta, média, baixa) de acordo com padrões como CVSS. A política deve estar disponível publicamente no site do fabricante e ser vinculante contratualmente.

1.9.8. O prazo mínimo de garantia para os equipamentos e licenças é de 60 (sessenta) meses a partir da data de aceite definitivo, incluindo:

- Garantia de hardware contra defeitos de fabricação;
- Suporte técnico 24x7 durante todo o período;
- Atualizações de firmware e patches de segurança;
- Atualizações de assinaturas (IPS, antivírus, URL filtering, etc.);
- Substituição de hardware defeituoso sem custo adicional;
    - RMA (Return Merchandise Authorization) com prazo máximo conforme SLA do fabricante.

1.10. GERENCIAMENTO CENTRALIZADO

1.10.1. A solução de gerenciamento centralizado e monitoramento deverá ser completamente on-premises, sem dependência obrigatória de serviços em nuvem ou controladores externos pagos para seu funcionamento contínuo, garantindo soberania dos dados e independência operacional. A solução poderá ser ofertada em formato de appliance físico (hardware do próprio fabricante) ou appliance virtual, conforme conveniência da contratante.

1.10.2. A solução deve permitir, a partir de uma única console centralizada:

- Configuração e administração de políticas: criação e gerenciamento de políticas de Firewall, Controle de Aplicação, IPS (Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL, NAT, QoS e SD-WAN para todos os dispositivos gerenciados
- Provisionamento de VPN: criação e monitoramento de comunidades VPN (IPsec e SSL) com visualização geográfica dos túneis em mapa
- Templates de configuração: criação de templates padronizados para DNS, SNMP, configurações de log, administração e outras definições recorrentes
- Objetos centralizados: criação e gestão unificada de objetos (redes, serviços, usuários, FQDNs) para reutilização em múltiplos dispositivos
- Visibilidade consolidada: dashboards com visibilidade das verificações de saúde dos links, desempenho de aplicações, utilização de largura de banda e conformidade com SLAs definidos

1.10.3. A solução deve suportar, sem custo adicional, o conceito de multi-tenancy, permitindo a gestão de ambientes independentes (clientes, departamentos, filiais) de forma isolada uns dos outros a partir da mesma solução, com administradores e políticas específicas por tenant.

1.10.4. Deve suportar autenticação de administradores em base local e de modo remoto por meio de:

- RADIUS (autenticação, autorização e accounting)
- LDAP / Microsoft Active Directory
- TACACS+ (com autorização por comando)
- PKI / certificados digitais

1.10.4.1. Deverá permitir a definição de perfis de acesso granulares com permissões como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações específicas, entre outras.

1.10.5. A solução deve oferecer mecanismos de governança e controle de alterações, incluindo:

- Bloqueio de edição concorrente: garantia de integridade das configurações através de bloqueio quando dois ou mais administradores acessarem o mesmo ativo simultaneamente
- Workflow de aprovações: definição de cadeia de aprovação para alterações antes da aplicação em produção
- Identificação visual: uso de palavras-chave ou cores para facilitar identificação de regras
- Localização de objetos: capacidade de localizar em quais regras um objeto (ex: computador, serviço) está sendo utilizado
- Numeração de regras: atribuição sequencial automática para regras de firewall, NAT e QoS

1.10.5.1. Agendamento e expiração: criação de regras que fiquem ativas apenas em horários definidos ou com data de expiração programada

1.10.6. A solução deve possuir mecanismos robustos de backup e recuperação:

- Backup automático: realização de backups das configurações de todos os dispositivos gerenciados, com agendamento configurável (dia e hora)
- Exportação de backups: transferência de arquivos de backup para servidores externos via FTP, SCP ou SFTP
- Rollback: capacidade de retornar para a última configuração salva ou para versões anteriores
- Comparação de configurações: visualização e comparação entre configurações atuais e versões anteriores, destacando alterações realizadas
- Backup da própria solução: sistema de backup/restauração de todas as configurações da solução de gerenciamento

1.10.7. A solução deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos gerenciados, de forma centralizada e automatizada, incluindo:

- Atualizações de firmware dos firewalls
- Atualizações de assinaturas de segurança (IPS, AV, URL)
- Validação prévia e agendamento das atualizações

1.10.8. A solução deve expor APIs RESTful completas e documentadas para permitir:

- Integração com portais personalizados
- Automação de provisionamento e configuração de objetos e políticas de segurança
- Orquestração com ferramentas externas (Ansible, Terraform, etc.)
- Consulta e extração de dados para sistemas de ticketing e CMDB

1.10.9. A solução deve incluir ferramenta para gerenciar centralmente as licenças de todos os appliances controlados, permitindo ao administrador:

- Visualizar status de licenciamento de cada dispositivo
- Renovar e atualizar licenças de forma centralizada
- Receber alertas sobre expiração próxima de licenças

1.10.10. A solução deve oferecer ferramentas de diagnóstico de rede diretamente na interface de gerenciamento, incluindo:

- Ping e traceroute para IPv4 e IPv6
- Captura de pacotes (PCAP) para análise aprofundada
- Testes de conectividade para validação de políticas e regras

1.10.11. A interface de gerenciamento deve ser acessível via web (HTTP/HTTPS) com dashboard intuitivo, gráficos em tempo real e configuração completa de todos os recursos. Deve também suportar acesso via SSH para configuração avançada via CLI e automação através de scripts. A interface web deve ser responsiva, suportando acesso em todos os web browsers. A interface deve ser moderna, intuitiva e não requerer treinamento extensivo para operações básicas, incluindo:

- Wizards para configurações comuns
- Validação de configurações antes de aplicar
- Preview de mudanças
- Sistema de help context-sensitive
- Documentação integrada

1.10.12. A solução deve possuir capacidade de coleta centralizada de logs de segurança, tráfego e eventos de todos os dispositivos gerenciados, permitindo:

- Exportação via Syslog ou Rsyslog para sistemas externos de SIEM, correlação e análise

- Tipos de logs: tentativas de acesso, bloqueios, ameaças detectadas, mudanças de configuração, VPN, autenticação, etc.
- Múltiplos destinos: suporte a envio simultâneo para diferentes coletores
- Formatação customizável: adequação aos formatos exigidos pelos sistemas de destino.

1.10.13. A solução deve gerar alertas automáticos baseados em eventos predefinidos, utilizando:

- E-mail para notificação de administradores
- SNMP traps para integração com sistemas de monitoramento
- Syslog para envio de eventos a sistemas SIEM

1.10.14. A solução deve suportar a exportação de dados de fluxo de rede através de protocolos padrão (Netflow v5/v9, IPFIX, sFlow) para ambientes IPv4 e IPv6, permitindo integração com ferramentas de análise de tráfego, capacity planning e detecção de anomalias. Deve suportar sampling configurável e exportação para múltiplos coletores simultaneamente.

1.10.15. A solução deve estar dimensionada e licenciada para gerenciar no mínimo 10 (dez) Firewalls de Próxima Geração (NGFW), considerando os modelos ofertados neste processo. O licenciamento deverá cobrir toda a vigência da garantia de 60 (sessenta) meses, incluindo:

- Suporte técnico do fabricante
- Atualizações de software

1.10.15.1. Atualizações automáticas das bases de dados de todas as funcionalidades (IPS, Antivírus, Filtro Web, etc.) durante todo o período contratual

1.10.16. A solução deve possuir um assistente integrado ao painel de operações, baseado em inteligência artificial generativa, que auxilie nas seguintes atividades:

- Configuração do ambiente e implementação de funcionalidades (VPN, SD-WAN, políticas de segurança)
- Investigação e troubleshooting de problemas no ambiente gerenciado
- Execução de comandos em linguagem natural para facilitar a operação diária

- Criação automatizada de scripts de configuração

1.10.16.1. A solução deverá disponibilizar um volume mínimo de 3.000.000 (três milhões) de tokens para consumo do motor de linguagem natural, considerando que o assistente deve operar de forma on-premises. Caso a solução de gerenciamento não possua assistente de IA nativo, será permitida a composição com soluções e plataformas de IA generativa complementares, desde que devidamente licenciadas, integradas, operacionais e atendendo plenamente aos requisitos técnicos exigidos neste item

1.11. MONITORAMENTO E LOGS

1.11.1. A solução de centralização de logs, monitoramento e relatórios deverá ser ofertada em formato de appliance físico (hardware do próprio fabricante) ou appliance virtual, conforme conveniência da contratante. Não deverá haver limitações artificiais quanto ao número de vCPUs, expansão de memória RAM ou capacidade de armazenamento, respeitando apenas os limites físicos do hardware subjacente.

1.11.2. A solução deverá suportar acesso via SSH e WEB (HTTPS) para gerenciamento, com comunicação e autenticação criptografada (usuário e senha) tanto na interface gráfica (GUI) quanto via linha de comando. Deverá permitir:

• Acesso simultâneo à administração

• Criação de pelo menos 2 perfis distintos (administração e monitoramento)

• Ativação/desativação por interface das permissões de acesso HTTP, HTTPS e SSH

• Autenticação de usuários via LDAP, RADIUS e TACACS+

• Suporte a SAML para autenticação do usuário administrador

• Compatibilidade com autenticação de dois fatores (token) para administradores

• Aplicação de políticas de senha (tamanho mínimo, caracteres permitidos)

1.11.3. Deverá permitir a virtualização do gerenciamento, onde cada administrador só tem acesso aos dispositivos e instâncias autorizados. Deverá permitir a criação de um administrador geral

com acesso a todas as instâncias, Definição de perfis de acesso com permissões granulares:

- Acesso de gravação
- Acesso de leitura
- Criação de novos usuários
- Alterações nas configurações gerais
- Definição do espaço que cada instância de virtualização pode usar para armazenamento de log

1.11.4. Os logs gerados pelos dispositivos gerenciados deverão ser centralizados na plataforma, devendo também ser possível o envio para:

- Servidor Syslog externo ou similar
- Servidor FTP/SFTP externo

1.11.4.1. A solução deverá permitir:

- Exportação de logs no formato CSV
- Encaminhamento de logs nos formatos syslog e CEF (Common Event Format)
- Download de arquivos de log da plataforma para uso externo
- Visualização em tempo real dos logs recebidos
- Exibição centralizada de logs de um ou mais dispositivos, com uso de filtros para facilitar pesquisas

1.11.4.2. Deverá suportar SNMP versões 2 e 3 para integração com sistemas de monitoramento.

1.11.5. A solução deverá possuir capacidade de geração de relatórios, permitindo os seguintes formatos de saída: HTML, CSV, XML e PDF. Tipos de relatórios predefinidos (obrigatórios):

- Conformidade com PCI DSS
- Uso de aplicações SaaS
- Prevenção de perda de dados (DLP)
- VPN
- IPS (Intrusion Prevention System)
- Análise de segurança do usuário
- Análise de ameaças cibernéticas
- Resumo diário de eventos e incidentes
- Tráfego DNS

- Top 10 aplicações mais utilizadas
- Top 10 sites mais acessados
- Uso de mídias sociais
- Cyberbullying e auto-mutilação

1.11.5.1. Deverá possuir relatórios de análise de postura e conformidade associados, no mínimo, às normas PCI, CIS e SOC2, contendo:

- Vulnerabilidade
- Categoria
- Recomendações
- Score
- Dispositivo afetado
- Políticas de Compliance

1.11.5.2. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando:

1.11.6. A solução deverá permitir:

- Importação e exportação de relatórios
- Duplicação de relatórios existentes para edição posterior
- Personalização da capa dos relatórios
- Personalização de gráficos: barras, linhas, tabelas
- Definição do design: inclusão de gráficos, texto, imagens, alinhamento, quebras de página, fontes, cores
- Especificação do idioma dos relatórios
- Personalização de qualquer relatório pré-estabelecido pelo administrador
- Criação de consultas SQL ou similares nos bancos de dados de logs para uso em gráficos e tabelas

1.11.6.1. Deverá possuir ferramenta para análise de desempenho na geração de relatórios, permitindo detectar e corrigir problemas.

1.11.7. A solução deverá permitir:

- Geração e envio automático de relatórios periódicos
- Programação conforme calendário definido pelo administrador
- Envio por e-mail para destinatários específicos
- Envio automático para servidor SFTP ou FTP externo

1.11.8. Deverá gerar alertas automáticos baseados em eventos especiais em logs e gravidade do evento, utilizando: E-mail, SNMP traps,

Syslog. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal.

1.11.9. A solução deve permitir a correlação de eventos, provendo painéis diversos e possibilitando a criação de novas telas para visualizar recursos de rede e segurança. Deve suportar operadores lógicos como: AND, FOLLOWED_BY, AND_NOT. Deve permitir que os Incidentes detectados sejam visualizados através de todas as categorias definidas pela Matrix Enterprise do MITRE ATT&CK.

1.11.10. Através da análise de tráfego de rede IP, web (URL) e domínios visitados, a solução deve suportar:

- Monitoramento de computadores potencialmente comprometidos ou usuários com uso de rede suspeito
- Atribuição de pontuações de risco (baixo, médio, alto) definindo os vereditos dos níveis de comprometimento
- Análise detalhada dos computadores comprometidos, exibindo detalhes das ameaças detectadas
- Recebimento de relatórios de surtos de ameaças globais, alertando automaticamente os administradores e criando regras para resposta eficaz a incidentes causados por essas ameaças

1.11.11. A solução deve suportar recursos de automação (playbooks) para, possam tomar ações automáticas visando mitigar riscos. Triggers para os playbooks: Horário, sob demanda, Incidente, Evento específico. Ações disponíveis para os playbooks: Criação de incidentes baseados em IOCs identificados na rede

1.11.12. A solução deverá exibir graficamente em tempo real:

- Taxa de geração de logs para cada dispositivo gerenciado
- Quantidade de logs enviados por dispositivo
- Informações do sistema: licenças, memória, disco rígido, uso de CPU, taxa de log por segundo, total de logs diários, alertas do sistema

1.11.12.1. Deverá permitir:

- Visualização em tempo real dos logs recebidos
- Mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real

- Geração de relatórios de tráfego em tempo real nos formatos: mapa geográfico, gráfico de bolhas e gráficos convencionais

1.11.12.2. Deverá gerar logs de auditoria com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.

1.11.13. A solução deverá possuir capacidade para receber pelo menos 100 GB de logs diários, com atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses. Deverá possuir licenciamento do serviço de Indicadores de Comprometimento (IoC) do mesmo fabricante, com capacidade para receber pelo menos 100 GB de logs diários. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses, com mecanismos de apagamento automático para logs antigos.

1.11.14. A solução deve possuir um assistente integrado ao painel de operações, baseado em inteligência artificial generativa (Assistente de IA), que auxilie na: Investigação de incidentes; Resposta a incidentes; Caça de ameaças (Threat Hunting). Requisitos do Assistente de IA:

- Disponibilizar volume mínimo de 3.000.000 (três milhões) de tokens para consumo do motor de linguagem natural, quando o modelo de cobrança ou consumo for baseado em tokens. Caso o licenciamento seja diferente do especificado, deverá ser fornecido algo próximo ao solicitado; permitir que administradores utilizem comandos em linguagem natural para facilitar a execução de tarefas; Capacidade de interpretar eventos de segurança, gerar resumos detalhados, identificar potenciais impactos e fornecer recomendações de remediação; Capacidade de fornecer respostas contextualizadas com base nos dados coletados pela solução.

1.11.14.1. Caso a solução não possua assistente de IA nativo, será permitida a composição com soluções e plataformas de IA generativa complementares, desde que devidamente licenciadas, integradas, operacionais e atendendo plenamente aos requisitos técnicos exigidos neste item.

1.12. EXPERIÊNCIA DIGITAL (DEM)

1.12.1. A plataforma deve utilizar uma rede globalmente distribuída de probes (Pontos de Presença - PoPs) para monitorar servidores e serviços publicamente acessíveis, avaliando uptime, desempenho e transações sintéticas. A solução deve incluir um coletor virtual ou uma opção de appliance físico, que resida atrás da solução de segurança cibernética distribuída NGFW, para monitoramento seguro e aprofundado de servidores e dispositivos na rede privada. Deve ser possível instalar um agente em sistemas operacionais Windows, Mac e Linux para coletar a saúde essencial do sistema operacional e métricas de desempenho de aplicações, alertando quando os limites são violados. A instalação do agente deve suportar scripts de instalação rápida ou manual e parâmetros configuráveis, incluindo a ativação de Monitoramento de Experiência Digital (DEM).

1.12.2. A plataforma deve oferecer suporte para monitoramento de:

- Servidores e dispositivos de rede;
- Ambientes de Virtualização (VMware);
- Ambientes de Nuvem (AWS, Azure, Google Cloud Platform);
- Kubernetes.

1.12.2.1. Monitoramento da carga de trabalho em nuvem (cloud workloads):

- A solução deverá fornecer uma visão centralizada de todas as aplicações e recursos em data centers locais e provedores de nuvem líderes (AWS, Azure, Google Cloud);
- Detectar e monitorar automaticamente recursos recém-adicionados (dynamic workload discovery) sem intervenção manual;
- Oferecer monitoramento granular de desempenho e utilização de recursos para otimização de alocação.

1.12.3. Monitorar proativamente métricas de desempenho como latência, jitter e perda de pacotes para garantir experiências de usuário fluida. Fornecer visibilidade detalhada do desempenho de aplicações da perspectiva de usuários individuais (agentes instaláveis em Windows e Mac). A solução deverá simular interações reais do

usuário (Synthetic Transaction Monitoring) para identificar problemas proativamente. Isso deve incluir suporte para transações sintéticas de navegador e JavaScript, executadas tanto de dentro quanto de fora da rede local. Fornecer uma visão abrangente dos gargalos de desempenho em redes públicas e privadas (Network path analysis ou Upstream Path health Monitoring).

1.12.4. A solução deve quebrar os silos de monitoramento, integrando DEM e monitoramento de infraestrutura de TI em uma plataforma unificada que atua como uma fonte única de métricas de desempenho da rede. Suporte a plugins de aplicação para monitoramento de tecnologias específicas (e.g., Active Directory, Apache Kafka, Apache Webserver, Cassandra, MySQL, MSSQL, Oracle, PostgreSQL, Redis, Prometheus, IIS, VMware, NetFlow, SNMP). A plataforma deve oferecer visibilidade profunda nos links membros de SD-WAN, suportando a configuração de monitoramento sintético de aplicação SD-WAN e análise de caminho em tempo real para ajuste proativo da rede.

1.12.5. A solução deverá ter a capacidade de correlacionar incidentes de sistema (por exemplo, alta CPU com tempos de resposta de aplicação falhando) antes de gerar um alerta para o cliente, reduzindo o "ruído" e minimizando o MTTR (Tempo Médio de Reparo). Suporte a Linhas do Tempo de Alerta (Alert Timelines) configuráveis para caminhos de escalonamento automatizados e extensíveis. Alertas devem ser configuráveis com base em Acordos de Nível de Serviço (SLAs) predefinidos. A solução deverá suportar a supressão de alertas de incidentes resolvidos e a configuração de agendamentos de manutenção. Automação e Resposta.

1.12.5.1. A solução deve fornecer recursos de contramedidas que permitam respostas programáticas imediatas a incidentes, incluindo ações investigativas e corretivas, tanto para ambientes Linux quanto Windows;

1.12.5.2. Suporte a Automação de Playbooks Personalizados e fluxos de trabalho de Política de Monitoramento.

1.12.6. A plataforma deve suportar integrações para notificação e gerenciamento de incidentes, incluindo e-mail, SMS, e integração com plataformas como ServiceNow, Slack, Microsoft Teams, PagerDuty, OpsGenie, Webhooks, Jira e Zendesk/Salesforce.

1.12.7. A plataforma deve incluir um construtor de dashboards de arrastar e soltar (drag and drop builder) para exibir e visualizar fluxos de dados, com opções de formatação, seleção de dados, filtragem e agregação de dados. A solução deverá oferecer uma ampla gama de widgets prontos para uso (por exemplo, contador de incidentes ativos, gráfico de linha avançado, mapa geográfico, heatmap e gráfico de topologia). Permitir a criação de visualizações e o salvamento de visualizações em Mapas de Topologia. O uso de tags deve ser suportado para segmentar e categorizar a infraestrutura, permitindo a exibição dinâmica de infraestrutura e métricas por tag. Possibilitar a definição do nível de acesso ao dashboard (Disponível para todos, limitado por tag, apenas para mim). A plataforma deve suportar a definição de escopo no nível do dashboard (Dashboard-level scoping) por tags ou por atributos-chave.

1.12.8. A solução deve oferecer a capacidade de gerar relatórios e páginas de status públicas, suportando a exportação de Relatórios de Métricas por longos períodos. Fornecer acesso REST API para integrações e uso (incluindo chaves API e limites de taxa).

1.12.9. Suporte a Single Sign-On (SSO) utilizando SAML + ADFS 3.0, Okta, e Azure Active Directory/Google Workplace. A plataforma deve também suportar stripping de dados sensíveis e funções de segurança de acesso do usuário.

1.12.10. A plataforma deverá empregar técnicas para correlacionar automaticamente eventos, métricas de desempenho e logs, fornecendo ao administrador a provável Causa-Raiz e o caminho crítico de impacto, visando acelerar o Tempo Médio de Resolução (MTTR).

1.12.11. A plataforma deverá disponibilizar dashboards, relatórios e políticas de monitoramento de saúde e desempenho prontos para uso para as 10 tecnologias mais críticas, permitindo a ativação do monitoramento em menos de 30 minutos por recurso. A solução deve incluir uma retenção de dados de no mínimo 12 meses.

1.13. LICENCIAMENTO EXPERIÊNCIA DIGITAL (DEM)

1.13.1. A Solução de Monitoramento de Experiência Digital (DEM) deverá ser agnóstica de plataforma, permitindo a visibilidade de ponta a ponta sobre a experiência digital de usuários e aplicações,

coletando métricas de desempenho em endpoints, redes, SD-WAN e serviços em nuvem para observar, correlacionar e automatizar respostas a problemas de disponibilidade e latência. A solução deverá estar devidamente licenciada durante a vigência da garantia de 60 (sessenta) meses, permitindo garantia, com suporte 24X7 e atualizações ao software, atualizações automáticas das bases de dados de todas as suas funcionalidades durante a vigência do contrato. Deverá permitir o monitoramento de pelo menos:

- 100 (cem) dispositivos/servidores de rede;
- 100 (cem) dispositivos de usuários finais.

1.13.1.1. A solução proposta deve suportar o monitoramento de infraestruturas públicas e privadas, utilizando uma abordagem de três dimensões (observar, correlacionar e responder) de monitoramento para correlacionar diferentes tipos de eventos e incidentes.

2. SOLUÇÃO NGFW COM FUNCIONALIDADE SD-WAN TIPO 2 PARA BRANCH OFFICE (PRÉDIOS REMOTOS DE MENOR PORTE), COM SERVIÇO DE INSTALAÇÃO, SUPORTE, TREINAMENTO E GARANTIA DE 60 MESES.

2.1. CARACTERÍSTICAS GERAIS – NGFW PRÉDIOS REMOTOS DE MENOR PORTE:

2.1.1. A solução deve possuir capacidade de gerenciamento inteligente de múltiplos links WAN (internet, MPLS, banda larga) com seleção dinâmica e automática baseada em desempenho, latência, perda de pacotes, jitter, disponibilidade, carga e tipo de aplicação. A solução deve permitir políticas de roteamento por aplicação, garantindo que o tráfego crítico utilize sempre o melhor caminho disponível, com suporte a endereçamentos estáticos e dinâmicos. Todas as funcionalidades de SD-WAN, incluindo orquestração, monitoramento, análise e controle, devem funcionar de forma completamente autônoma, sem necessidade de contratação de serviços adicionais em nuvem ou dependência de controladores externos, garantindo soberania dos dados e independência operacional com gerenciamento on-premises completo.

2.1.2. O sistema deve realizar monitoramento contínuo e em tempo real da qualidade dos links WAN, incluindo medição de latência, jitter, perda de pacotes e banda disponível, por meio de métodos ativos (probes sintéticas) e passivos (análise do tráfego real) . A solução

deve ser capaz de medir o status de saúde do link com base em métricas de desempenho e thresholds configuráveis, que servirão como fatores de decisão nas regras de SD-WAN. Os resultados de desempenho devem ser apresentados em formato gráfico através da interface de gerenciamento, permitindo análise em tempo real e histórica com identificação proativa de degradação de performance. A solução deve oferecer visibilidade completa do consumo de banda por aplicação, incluindo identificação de aplicações por assinatura (não apenas por porta), com métricas de performance por tipo de tráfego e capacidade de priorização dinâmica.

2.1.3. O equipamento deve realizar comutação automática e transparente do tráfego entre os links disponíveis baseado em regras definidas pelo usuário, incluindo contadores de latência, perda de pacotes, disponibilidade e carga. O failover deve ocorrer em milissegundos para aplicações críticas, sem interrupção de sessões estabelecidas.

2.1.3.1. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a qualidade do link é modificada.

2.1.4. A solução deve suportar a criação e gerenciamento de no mínimo 2000 regras que combinem comportamento de tráfego e segurança, permitindo políticas granulares por:

- Aplicação (com reconhecimento por assinatura, independente de porta e protocolo);
- Usuário e grupos do Active Directory/LDAP;
- Origem e destino;
- Horário;
- Qualidade do link (baseada em latência, jitter, perda de pacotes e largura de banda).

2.1.4.1. As regras devem ser processadas sem degradação significativa de performance, suportando integração com funcionalidades de firewall, VPN, NAT, IPS, Antivírus e Filtro Web.

2.1.5. A solução deverá suportar, no mínimo, os seguintes métodos de roteamento SD-WAN:

- Manual: prioridades atribuídas manualmente às interfaces;
- Melhor Qualidade: priorização baseada na qualidade do link (latência, jitter, perda, banda);

- Menor Custo: priorização baseada no custo atribuído à interface, considerando qualidade do link;
- Balanceamento de Carga: distribuição do tráfego entre interfaces disponíveis com base em algoritmos de balanceamento e qualidade do link.

2.1.5.1. Deve suportar roteamento dinâmico BGP com IPv6 e permitir a configuração de políticas de QoS em protocolos e aplicações de camada 7, associadas percentualmente à largura de banda da interface SD-WAN.

2.1.6. A solução deve possuir mecanismos de correção de perda de pacotes em tempo real para otimizar o desempenho e a confiabilidade de links WAN e túneis VPN, especialmente para aplicações sensíveis a perdas (áudio, VoIP, videoconferência). Estes mecanismos devem incluir: Correção de Erro Antecipada (Forward Error Correction - FEC), com capacidade de ajuste dinâmico da relação entre pacotes base e redundantes com base nas condições do link em tempo real e métricas de SLA; Mecanismos de mitigação de perdas que possam ser ativados seletivamente por aplicação ou política, baseados em thresholds de perda de pacotes configuráveis.

2.1.6.1. Os recursos devem ser compatíveis com as topologias hub-spoke e full-mesh, e aplicáveis a aplicações específicas para otimizar o uso de recursos de banda e processamento.

2.1.7. A solução deve suportar múltiplos métodos de health check para monitorar a disponibilidade e qualidade dos links WAN e servidores de destino, permitindo a tomada de decisão em políticas de SD-WAN e balanceamento de carga. Os métodos devem incluir, no mínimo:

- Ping (ICMP) para verificação básica de conectividade;
- Verificações em camada 4 (TCP/UDP) em portas configuráveis;
- Verificações em camada 7 (HTTP/HTTPS) com validação de resposta.

2.1.7.1. A solução deve suportar health check ativo (probes sintéticas criadas pelo administrador) e passivo (utilizando o próprio tráfego do usuário para inferir condições dos links).

2.1.8. A solução deve ser capaz de prover arquitetura onde, em comunicação Data Center (DC) x Unidades Remotas (UR) com link

comprometido entre UR-A e DC possa ser utilizado o circuito entre UR-B e DC para que UR-A alcance o DC.

2.1.8.1. Deve ser capaz de criar VPN "Full-Mesh" dinâmica, com túneis entre pontas remotas criados sob demanda e encerrados quando o tráfego cessar, evitando escoamento via hub. A configuração VPN IPSEC deve oferecer suporte para DH Group 14 e 15.

2.1.9. A solução deve fornecer reconhecimento default em camada 7 de, pelo menos, 2000 aplicações largamente utilizadas em contextos de SaaS, nuvem e multimídia (ex: Vimeo, YouTube, Facebook). O reconhecimento deve ser realizado independente de porta e protocolo, inspecionando o payload do pacote, totalmente segregado da camada 4. Deve contar com banco de dados interno onde seja possível atrelar uma aplicação a um IP/range de IPs de destino.

2.1.10. A solução deve suportar múltiplas instâncias de tabelas de roteamento VRF (Virtual Routing and Forwarding) para segmentar tráfego L3 de forma lógica dentro do mesmo appliance, garantindo que pacotes sejam encaminhados apenas entre interfaces pertencentes ao mesmo VRF. Deve ser possível associar interfaces físicas, subinterfaces e interfaces virtuais (incluindo VLANs e túneis VPN) a VRFs específicas de forma determinística, com rotas, políticas e encaminhamento totalmente separados por VRF.

2.1.11. A solução deve suportar rotas estáticas e protocolos de roteamento dinâmico (BGP e OSPF) em instâncias VRF distintas, incluindo capacidade de configurar múltiplos processos por VRF para cenários multi-tenant ou separação de roteamento. As VRFs devem interoperar com funcionalidades de VPN, NAT, inspeção de segurança, políticas de firewall e SD-WAN, preservando isolamento quando requerido e permitindo exceções controladas para roteamento entre VRFs apenas mediante regras explícitas de trânsito ou rotas compartilhadas.

2.1.12. A solução deve ter capacidade de coletar telemetria, tabelas de rota, sessões ativas e logs com capacidade de segregação por domínio lógico (VRF, tenant, ou instância de roteamento), para suporte a troubleshooting, auditoria e integração com sistemas de monitoramento centralizados.

2.1.13. A solução deve permitir a criação de endereços IPs virtuais e balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais. Deve suportar balanceamento para os serviços HTTP, HTTPS, TCP e UDP, com os seguintes métodos:

- Endereço IP de origem ou Static;
- Round Robin;
- Weighted;
- First Alive e HTTP host;
- Least Session;
- Least RTT.

2.1.14. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID, e suportar SSL/TLS offloading para descarregamento do processamento criptográfico dos servidores.

2.1.15. A solução deve ter capacidade de identificar, através de health checks, quais servidores reais estão ativos em configurações de balanceamento de carga, removendo automaticamente o tráfego dos servidores indisponíveis. Deve permitir health checks periódicos, no mínimo, via:

- ICMP (ping) para verificação básica;
- TCP em portas configuráveis;
- HTTP/HTTPS com validação de código de resposta ou conteúdo específico.

2.2. ESPECIFICAÇÕES DE HARDWARE – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.2.1. 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. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

2.2.2. Deve possuir, pelo menos, 08 (oito) interfaces Ethernet de 1Gbps com conector RJ45 (cobre), para conectividade com equipamentos locais, servidores, switches de acesso e segmentos LAN.

2.2.3. Deve dispor de porta console para acesso direto ao equipamento através de USB, RJ45 ou DB9 (RS232), esta interface é essencial para configuração inicial, troubleshooting e recuperação de desastres quando o acesso via rede não está disponível.

2.2.4. O equipamento deve possuir capacidade de Captive Portal integrado, permitindo autenticação de usuários via página web antes de liberar acesso à internet. Deve suportar múltiplos métodos de autenticação incluindo login/senha local, integração com Active Directory/LDAP, RADIUS, autenticação por redes sociais e customização completa da página de login com logotipo e mensagens da organização. Esta funcionalidade é essencial para controle de usuários, aplicação de políticas granulares por usuário/grupo e auditoria de acesso.

2.2.5. A solução deve implementar backup automático e programável de configurações através da interface web de gerenciamento, incluindo versionamento, agendamento de backups periódicos, armazenamento local e remoto (FTP/SFTP/SCP), notificações por e-mail e capacidade de restore rápido com rollback para versões anteriores.

2.3. CAPACIDADE E PERFORMANCE – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.3.1. Taxa de transferência com IPS (Intrusion Prevention System) habilitado deve ser de no mínimo 1,2 Gbps, garantindo inspeção profunda de pacotes sem gargalos de performance mesmo em cenários de tráfego intenso.

2.3.2. A taxa de transferência com todas as funcionalidades NGFW ativas (firewall, application control, IPS, antivírus) deve ser de no mínimo 950 Mbps, assegurando proteção abrangente sem degradação significativa de desempenho.

2.3.3. A capacidade de processamento de Threat Prevention (IPS, antivírus, anti-spyware) ativa deve ser de no mínimo 750 Mbps.

2.3.4. A solução deve apresentar capacidade de processamento em camada 3 para tráfego IPv4/IPv6 com diferentes perfis de pacotes,

garantindo performance adequada para ambientes de filiais e médias empresas. A solução deve sustentar, no mínimo, 8 Gbps para pacotes de 1518 bytes, 8 Gbps para pacotes de 512 bytes e throughput com pacotes de 64 bytes compatível com os requisitos de desempenho da rede, além de capacidade de processamento de pacotes por segundo (Mpps) compatível com os limites de novas sessões por segundo e sessões simultâneas exigidos neste documento, conforme metodologia RFC 2544 ou RFC 9411. A latência interna para pacotes de 64 bytes não deverá exceder 5 microssegundos sob carga nominal.

2.3.5. A solução deve suportar no mínimo 585.000 sessões TCP simultâneas, garantindo capacidade para médios volumes de usuários e aplicações concorrentes sem limitações artificiais impostas por licenciamento.

2.3.6. A solução deve suportar no mínimo 28.000 novas conexões TCP por segundo, garantindo capacidade para ambientes web, APIs e aplicações com média frequência de abertura de conexões, sem limitações artificiais impostas por licenciamento.

2.3.7. A solução deve suportar no mínimo 3.500 políticas de firewall, permitindo segmentação granular e controles detalhados sem impacto em performance ou limitações artificiais impostas por licenciamento.

2.4. FUNCIONALIDADES DE REDE – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.4.1. A solução deve possuir suporte completo e nativo aos protocolos IPv4 e IPv6 em todas as funcionalidades, incluindo roteamento, firewall, NAT, DHCP, VPN e monitoramento. Deve suportar dual-stack e mecanismos de transição IPv4/IPv6, como NAT64 e NAT46, garantindo interoperabilidade em ambientes heterogêneos.

2.4.2. A solução deve implementar protocolos avançados de roteamento, incluindo:

- Roteamento estático e dinâmico com OSPF (para roteamento interno), BGPv4 (para roteamento externo com múltiplos uplinks) e ISIS
- Policy Based Routing (PBR) para desvios de tráfego baseados em políticas

- VRF (Virtual Routing and Forwarding) para segmentação lógica de redes com tabelas de roteamento independentes
- VRRP (Virtual Router Redundancy Protocol) para redundância de gateway
- MPLS para redes corporativas avançadas
- VXLAN para overlay networks e virtualização de rede
- Roteamento e forwarding multicast com protocolos PIM-SM e PIM-DM

2.4.2.1. As VRFs devem interoperar com funcionalidades de VPN, NAT, inspeção de segurança, políticas de firewall e SD-WAN, preservando isolamento quando requerido e permitindo exceções controladas para roteamento entre VRFs apenas mediante regras explícitas.

2.4.3. A solução deve suportar o padrão IEEE 802.1Q com capacidade para configurar no mínimo 4094 VLANs simultaneamente, permitindo ampla segmentação de rede e isolamento de tráfego. Deve permitir a criação de VLANs nativamente e operar nos modos bridge (transparente), router, proxy explícito, sniffer e/ou VLAN-tagged. Deve suportar LACP (IEEE 802.3ad) para agregação de múltiplas interfaces físicas em um único link lógico, aumentando a banda disponível e provendo redundância de enlaces. Em modo transparente, deve funcionar sem alterar o endereço MAC do tráfego, permitindo filtro de pacotes em camada 2 e forwarding para protocolos não IP.

2.4.4. A solução deve suportar tradução de endereços estáticos (NAT 1:1, muitos:1, NAT64, NAT46) e dinâmicos (PAT, muitos:1). Deve incluir funcionalidades de STUN, Full Cone NAT, permitir filtro de pacotes com e sem NAT, e possibilitar abertura dinâmica de portas para serviços que requerem portas dinâmicas (session-helpers ou ALGs). Deve suportar DHCP Cliente, Servidor e Relay para IPv4 e IPv6 (DHCPv6), com funcionalidades avançadas como:

- Múltiplos pools de endereços
- Reservas por endereço MAC
- Opções customizadas
- DNS dinâmico (DDNS)
- Relay DHCP para segmentos remotos

2.4.5. A solução deve possuir implementação robusta de QoS (Quality of Service) permitindo:

- Classificação de tráfego por múltiplos critérios: aplicação, IP de origem/destino, porta, protocolo, DSCP, VLAN, usuário/grupo
- Marcação de pacotes com modificação de valores DSCP para DiffServ
- Priorização de tráfego com suporte a ToS (Type of Service)
- Limitação de banda (rate limiting) e garantia de banda mínima para aplicações críticas
- Criação de filas de prioridade e gerenciamento de congestionamento

2.4.5.1. Deve permitir definir banda máxima e banda garantida por

- Usuário ou grupo de usuários (integrado a Active Directory/LDAP)
- Endereço IP (origem/destino)
- Sub-rede (origem/destino)
- Protocolo
- Aplicação (incluindo peer-to-peer, streaming, chat, VoIP, Web)

2.4.5.2. A definição de banda deve ser possível tanto por valor absoluto quanto por percentual.

2.4.6. A solução deve suportar alta disponibilidade (HA) nos modos ativo-passivo e ativo-ativo com divisão de carga, mantendo todas as licenças de software habilitadas sem perda de conexões. Deve suportar VRRP para redundância de gateway e possuir funcionalidade de balanceamento e contingência de links de internet.

2.4.7. A solução deve oferecer:

- Ferramenta de diagnóstico do tipo tcpdump ou similar para captura e análise de tráfego
- Porta de comunicação serial ou USB para acesso local protegido por usuário/senha
- Suporte a sFlow para monitoramento de tráfego
- Comunicação criptografada entre estação de gerência e appliance (interface gráfica e CLI)

2.4.7.1. SNMP: Implementação completa dos protocolos SNMP versões 1, 2c e 3 para integração com sistemas de

monitoramento e gerenciamento de rede, com suporte a MIBs padrão e específicas do fabricante. SNMPv3 deve incluir autenticação e criptografia.

2.4.7.2. APIs e Automação:

- Exposição de APIs RESTful completas e documentadas para orquestração e automação (políticas de segurança, objetos de rede, logs, operações de manutenção)
- Suporte a execução automatizada de playbooks baseados em eventos (isolamento de endpoint, alteração de políticas, bloqueio de rede)
- Integração direta com plataformas SOAR via webhook e API
- Recursos de automação para operações diárias: execução de scripts, envio de e-mails, notificações via Teams, agendamentos, resposta a eventos de rede/segurança

2.4.8. A solução deve oferecer autenticação de usuários em base local e integração com servidores:

- RADIUS (autenticação, autorização e accounting)
- TACACS+ (com suporte a autorização por comando e accounting detalhado)
- LDAP e Microsoft Active Directory (reconhecimento de contas e grupos)

2.4.8.1. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Active Directory/LDAP, permitindo criação de regras baseadas em usuário e grupo. Deve suportar:

- Autenticação de dois fatores com integração a tokens
- Single-sign-on via Active Directory, RADIUS e SAML
- Autenticação para tráfego HTTP, HTTPS, FTP e Telnet
- IP/MAC binding para controle de endereços internos e prevenção de IP spoofing

2.4.9. A solução deve suportar certificados digitais X.509, SCEP (Simple Certificate Enrollment Protocol), CSR (Certificate Signing Request) e OCSP (Online Certificate Status Protocol), garantindo autenticação segura e comunicação criptografada.

2.4.10. Deve possuir mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações como: dcerpc, DNS (TCP/UDP), FTP, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, SCCP, TFTP e TNS. Deve suportar aplicações multimídia (H.323, SIP) e técnicas de detecção de programas peer-to-peer e mensagens instantâneas.

2.4.11. A solução deve possuir tecnologia de firewall stateful, mecanismo de anti-spoofing e permitir:

- Criação de serviços por porta ou conjunto de portas (TCP, UDP, ICMP, IP)
- Agrupamento de serviços para facilitar administração
- Criação de regras definidas pelo usuário
- Objetos e agrupamentos de objetos (usuários, redes, FQDN, protocolos, serviços)

2.4.11.1. Deve permitir controle de acesso por:

- Endereço IP de origem/destino
- Sub-rede
- Domínio (ex: gov.br, org.br)
- Períodos do dia e dia da semana
- Usuário e grupo de usuários
- Tipo de dispositivo
- Protocolo e aplicação

2.4.12. A solução deve possuir conectores com nuvens públicas (AWS, Microsoft Azure, GCP, OCI) e privadas (Kubernetes, VMware, OpenStack, Cisco ACI, Nutanix). Modificações nas clouds devem refletir automaticamente nos objetos do firewall, evitando reconfiguração manual de regras. Deve possuir integração com threat feeds para sincronismo de listas externas de IPs, MACs, domínios e hashes de malwares.

2.4.13. A solução deve suportar monitoramento em tempo real das configurações aplicadas, identificando vulnerabilidades, sugerindo boas práticas para melhoria do hardening e performance, atribuindo nota à configuração. Deve informar itens aprovados/reprovados nas validações e, para cada critério, detalhar elementos envolvidos, configuração sob validação, resultado, severidade e regra de compliance aplicável.

2.4.14. A solução deve possuir recurso para detecção de dispositivos IoT por métodos passivos (inspeção de tráfego, fingerprinting de protocolos), identificando MAC Address, IP, SO, hostname e login.

Deve buscar informações em base local e, se necessário, na nuvem do fabricante sobre vulnerabilidades associadas. Deve classificar perfil comportamental e score de risco por dispositivo baseado em anomalias de tráfego, destinos incomuns, tentativas de conexão externas e mudanças repentinas de padrão, com detecções configuráveis por perfil de risco.

2.5. FUNCIONALIDADES DE SEGURANÇA AVANÇADA – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.5.1. A solução de IPS deve estar orientada à proteção de redes, integrada nativamente à plataforma de segurança (não módulo externo), permitindo funcionamento em modo transparente, sniffer e router. Deve suportar verificação de tráfego em tempo real via aceleração de hardware e possuir capacidade de remontagem de pacotes para identificação de ataques, garantindo inspeção inline que não cause degradação significativa de performance.

2.5.2. A solução deve possuir base de assinaturas de IPS com, pelo menos, 15.000 (quinze mil) ameaças conhecidas, cobrindo exploits, buffer overflows, SQL injection, cross-site scripting, command injection, denial of service, scanning/reconnaissance, entre outras técnicas de ataque. As assinaturas devem ser atualizadas automaticamente várias vezes ao dia. Deve permitir a criação de padrões de ataque manualmente, assinaturas personalizadas via interface gráfica, e uso de operadores de negação na criação de assinaturas customizadas para permitir exceções com granularidade.

2.5.3. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão. 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 e zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS.

2.5.4. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, como por exemplo agrupar todas as assinaturas relacionadas a web-server para proteção específica de Servidores Web, facilitando a gestão e aplicação de políticas.

2.5.5. A solução deve possuir:

- Capacidade de análise de tráfego para detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep
- Mecanismos de detecção/proteção de ataques
- Reconhecimento de padrões
- Análise de protocolos
- Detecção de anomalias
- Filtros de ataques por anomalias
- Filtros de anomalias de tráfego estatístico (flooding, scan, source e destination session limit)
- Filtros de anomalias de protocolos
- Reconhecimento de ataques de DoS, reconnaissance, exploits e evasion
- Verificação de ataque na camada de aplicação

2.5.6. A solução deve possuir proteção contra:

- Ataques de RPC (Remote Procedure Call)
- Ataques Windows ou NetBios
- Ataques SMTP, IMAP, Sendmail e POP
- Ataques DNS (Domain Name System)
- Ataques a FTP, SSH, Telnet e rlogin
- Ataques ICMP (Internet Control Message Protocol)

2.5.7. A solução deve:

- Mitigar os efeitos dos ataques de negação de serviços
- Ser imune e capaz de impedir ataques básicos como Syn flood, ICMP flood e UDP flood
- Detectar e bloquear a origem de portscans
- Bloquear ataques efetuados por worms conhecidos
- Possuir assinaturas específicas para mitigação de ataques DoS e DDoS
- Possuir assinaturas para bloqueio de ataques de buffer overflow
- Incluir proteção contra ataques de negação de serviços
- Permitir o bloqueio de vulnerabilidades e exploits conhecidos
- Identificar e bloquear comunicação com botnets
- Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms

- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos

2.5.7.1. Deve incluir proteção contra ataques nos layers 3, 4 e 7 do modelo OSI, com recursos como rate limiting por IP/subnet, blacklisting automático de atacantes e desafio CAPTCHA para validação de origem legítima.

2.5.8. A solução deve possuir as seguintes estratégias de bloqueio: pass, drop e reset. Deve ter capacidade de resposta/logs ativa a ataques, prover terminação de sessões via TCP resets e gerar logs de sessões.

2.5.9. Deve possuir recurso que coloque momentaneamente novas assinaturas em modo "monitor" apenas (detecção passiva), gerando alertas detalhados sobre atividades suspeitas sem bloqueio automático, evitando falsos positivos. Esse tempo deve permitir customização e, após o período configurado, a assinatura deve mudar para modo bloqueio automaticamente. O modo IDS deve permitir análise forense e resposta coordenada, operando em conjunto com o IPS.

2.5.10. A solução deve possuir métodos de notificação de detecção de ataques, incluindo:

- Alarmes na console de administração
- Alertas via correio eletrônico
- Monitoração do comportamento do appliance mediante SNMP (versões 1, 2c e 3), com capacidade de enviar traps quando ocorrer um evento relevante para a correta operação da rede

2.5.11. A solução deve possuir capacidade de proteção inline e em tempo real contra ameaças desconhecidas (zero-day) e malwares de última geração através de motores de Inteligência Artificial (AI) e Machine Learning (ML) integrados nativamente ao sistema operacional do equipamento. Esta proteção deve operar localmente no hardware (on-premises), sem dependência obrigatória de nuvens externas para a tomada de decisão inicial, garantindo vereditos em frações de segundo (sub-second) para a identificação e bloqueio de artefatos maliciosos antes que estes penetrem na rede interna. A solução deve suportar análise heurística avançada e modelos de ML para tráfego criptografado e fluxos de arquivos, permitindo a detecção autônoma de ameaças nunca antes vistas,

gerando registros detalhados para auditoria e tomada de decisão do analista.

2.5.12. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado (sandboxing) para análise comportamental aprofundada. A solução de sandbox deve permitir a retenção inline do arquivo, ou seja, o usuário não o receberá enquanto ele não for analisado e definido como "limpo". A análise deve incluir técnicas de heurística e machine learning, com geração de relatórios detalhados sobre o comportamento dos artefatos.

2.5.13. A solução deve suportar a captura de pacotes (PCAP) por assinatura de IPS ou regra de firewall. 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.

2.5.14. A solução deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

- Nome da assinatura ou do ataque
- Aplicação
- Usuário
- Origem da comunicação
- Destino da comunicação
- Ação tomada pelo dispositivo

2.5.14.1. Os eventos devem identificar o país de onde partiu a ameaça (geolocalização).

2.5.15. A solução deve permitir aplicação de políticas baseadas em geolocalização de endereços IP de origem e destino, incluindo bloqueio ou liberação de tráfego de/para países específicos, útil para reduzir superfície de ataque bloqueando regiões de alto risco. Deve suportar ações granulares: bloquear acesso de países específicos a determinados serviços, permitir apenas países autorizados para acesso administrativo, entre outras políticas customizáveis.

2.5.16. A solução deve permitir o bloqueio de vírus e spywares em tempo real através de scanning de arquivos em, pelo menos, os seguintes protocolos: HTTP e HTTPS, FTP, SMB, SMTP, POP3, IMAP. Deve utilizar múltiplas engenharias de detecção, incluindo análise

heurística e comportamental, com suporte a scanning de arquivos compactados e criptografados (quando possível).

2.5.17. A solução deve oferecer bloqueio de domínios maliciosos via DNS, com integração a feeds de inteligência de ameaças, interceptando queries DNS e bloqueando resoluções de domínios associados a malware, phishing, botnet C&C, sites de ransomware, proxies anônimos e TOR exit nodes, de forma transparente aos usuários e aplicações. A proteção deve ser aplicada de forma automática e dinâmica.

2.5.18. A solução deve suportar Dynamic DNS (DDNS) permitindo atualização automática de registros DNS quando endereços IP públicos mudam, essencial para links de internet dinâmicos, com suporte aos principais provedores de DDNS do mercado e configuração de múltiplos domínios.

2.5.19. A solução deve possuir proteção em tempo real contra URLs maliciosas e phishing através de categorização dinâmica e análise de reputação. Deve bloquear acesso a sites comprovadamente maliciosos, páginas de phishing bancário, sites de distribuição de malware e destinos utilizados em campanhas de ataques direcionados, com suporte a listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra). A base de categorias deve conter no mínimo 60 categorias e 60 milhões de sites classificados.

2.5.20. A solução deve permitir identificação e controle granular de milhares de aplicações através de assinatura profunda (não apenas porta/protocolo), reconhecendo aplicações criptografadas, tuneladas e que utilizam portas não padrão. Deve permitir controles por aplicação: bloquear, permitir, limitar banda, aplicar QoS, registrar logs, entre outros. Cobertura mínima de 3.000 aplicações identificáveis, com pelo menos 20 categorias de classificação.

2.5.21. A solução deve possuir integração com threat feeds para sincronismo de listas externas de IPs, MACs, domínios e hashes de malwares, com atualização automática e frequente, garantindo bloqueio proativo contra ameaças emergentes.

2.5.22. A solução deve possuir capacidade de inspeção de tráfego criptografado SSL/TLS através de técnicas de descriptografia controlada, permitindo inspeção e re-criptografia de tráfego HTTPS,

garantindo que malware, ataques e vazamento de dados não se escondam sob criptografia. Deve suportar listas de exceção para sites bancários, de saúde e outros que não devem ser inspecionados, com compatibilidade para TLS 1.2 e 1.3.

2.6. FILTRO DE CONTEÚDO WEB – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.6.1. A solução deve possuir solução de filtro de conteúdo Web integrado à solução de segurança, com suporte a Proxy Explícito e Transparente, devendo implementar roteamento WCCP e ICAP ou mecanismos equivalentes que permitam a integração com proxies externos, sistemas de cache, soluções de descarregamento de tráfego e inspeção avançada de conteúdo, garantindo a mesma funcionalidade e performance. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web. Deve filtrar o conteúdo baseado em categorias em tempo real, permitindo a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

2.6.2. A solução deve possuir, pelo menos, 60 (sessenta) categorias para classificação de sites Web, com base mínima contendo 60.000.000 (sessenta milhões) de sites internet Web já registrados e classificados. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP, permitindo a reclassificação de sites Web por ambos os critérios. Deve possuir a funcionalidade de cota de tempo e banda consumida por categoria.

2.6.3. A solução deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web:Proxy anônimo; Webmail;Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras; Inteligência artificial; Criptomoedas.

2.6.4. A solução deve permitir:

- Criação de categorias personalizadas;
- Criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
- Criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, por endereço IP de origem e por sub-rede de origem;

- Recurso do tipo "safe search" ou similar em sites de buscas, filtrando o resultado de pesquisas efetuadas em tais sites que apresentem conteúdo nocivo.

2.6.5. A solução deve prover mecanismo de aceite ou aviso ao usuário (podendo ser customizável, aceitando idioma português), a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado, incluindo a capacidade de exibir páginas de bloqueio customizáveis, termos de aceite, avisos de conformidade ou políticas de uso aceitável, garantindo que o usuário seja informado e, quando necessário, confirme o entendimento antes de prosseguir. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.

2.6.6. A solução deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, permitindo a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

2.6.7. A solução deve permitir:

- Filtragem de conteúdo do tráfego WEB de URLs conhecidas em applets Java, cookies e activeX;
- Bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
- Bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
- Bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.

2.6.8. A solução deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.

2.7. LICENCIAMENTO – NGFW PRÉDIOS REMOTOS DE MENOR PORTE

2.7.1. Deve possuir e estar licenciado durante a vigência da garantia de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Segurança de Ameaças (IPS, Proteção Avançada contra Malware e

Controle de Conteúdo e Acesso (Filtragem de URL/DNS/Vídeo, Controle de Aplicativos).

2.7.2. O licenciamento da solução deve incluir todas as funcionalidades de segurança e SD-WAN especificadas neste documento, sem qualquer limitação artificial imposta por licenciamento quanto a número de VLANs, políticas de firewall, regras de SD-WAN, túneis VPN, sessões simultâneas ou quaisquer outros recursos de software do equipamento, ressalvadas as limitações físicas inerentes à capacidade do hardware adquirido, as quais deverão estar claramente especificadas na ficha técnica do modelo ofertado.

2.7.3. A empresa licitante deverá provisionar junto aos contratos de "Garantia" e "Suporte do Fabricante", junto ao fabricante da solução ofertada, garantia técnica total pelo fabricante da Solução pelo período mínimo de 60 (sessenta) meses, incluindo suporte técnico em regime de atendimento de 24x7 (vinte e quatro horas, sete dias por semana), contados a partir da data de emissão do atestado de recebimento definitivo dos bens e materiais (hardwares, softwares e licenciamentos) pela PRODABEL. Deverá possuir atendimento, com retorno rápido para questões críticas, em até 2 horas, e para questões não críticas no próximo dia útil, por especialistas do próprio fabricante da Solução ofertada.

2.7.4. Para os serviços de suporte e assistência técnica para serviços de trocas ou reparo de peças (referentes aos componentes de hardwares), estes devem possuir prazo de solução no dia útil subsequente com atendimento em, no máximo 48h (quarenta e oito horas), a partir do recebimento do item de troca ou reparo, enviado pelo seu fabricante correlacionado.

2.7.5. **SUPORTE 24X7**

2.7.5.1. A CONTRATADA deve fornecer ou garantir suporte técnico 24 horas por dia, 7 dias por semana, 365 dias por ano, diretamente do fabricante ou através de parceiro autorizado com SLA garantido. O suporte deve incluir: abertura de chamados por telefone, e-mail e portal web, atendimento preferencialmente em português, acesso a base de conhecimento, downloads de firmware e documentação.

2.7.6. **ATUALIZAÇÃO E CORREÇÃO DE VULNERABILIDADES POR PATCHES**

2.7.6.1. O fabricante deve disponibilizar atualizações de firmware/software e patches de segurança de forma regular e responsiva. As atualizações devem poder ser aplicadas SEM perda de configurações e COM equipamento em produção (quando possível aplicação com baixo impacto). Deve incluir atualizações de: assinaturas de IPS, antivírus, categorização de URLs, feeds de inteligência de ameaças, firmware do sistema operacional e correções de CVEs.

2.7.7. **SLA DE CORREÇÃO DE PATCHES BEM DEFINIDO PELO FABRICANTE**

2.7.7.1. O fabricante deve publicar e manter uma política formal e pública de SLA para lançamento de patches de correção de vulnerabilidades de segurança e falhas do produto. Esta política deve definir prazos máximos de resposta baseados na criticidade da vulnerabilidade (crítica, alta, média, baixa) de acordo com padrões como CVSS. A política deve estar disponível publicamente no site do fabricante e ser vinculante contratualmente.

2.7.8. O prazo mínimo de garantia para os equipamentos e licenças é de 60 (sessenta) meses a partir da data de aceite definitivo, incluindo:

- Garantia de hardware contra defeitos de fabricação;
- Suporte técnico 24x7 durante todo o período;
- Atualizações de firmware e patches de segurança
- Atualizações de assinaturas (IPS, antivírus, URL filtering, etc.);
- Substituição de hardware defeituoso sem custo adicional;
    - RMA (Return Merchandise Authorization) com prazo máximo conforme SLA do fabricante.

3. TREINAMENTO OFICIAL

3.1. A CONTRATADA deverá fornecer treinamento técnico especializado para a equipe da CONTRATANTE, com as seguintes características:

- Carga horária mínima: 24 horas.
- Modalidade: Online (Remoto).
- Conteúdo mínimo exigido:
    - Firewall de próxima geração: configuração de regras de filtragem, NAT, autenticação e perfis de segurança integrados para bloqueio de ameaças em tempo real.

SD-WAN: configuração de múltiplos links WAN, medição de qualidade (latência, jitter, perda), regras de direcionamento por desempenho, custo ou largura de banda, e integração com segurança inline.

- Gerenciamento centralizado: administração unificada de dispositivos, domínios isolados, pacotes de políticas compartilhadas (incluindo SD-WAN), provisionamento por modelos e implantação consistente. Controle de aplicações: identificação e gerenciamento de tráfego em camada 7, com direcionamento baseado em aplicação real, integrado ao SD-WAN.
- Monitoramento e análise: coleta central de logs e métricas (incluindo SD-WAN), relatórios, dashboards e visualização de desempenho e ameaças. Alta disponibilidade: redundância ativa-passiva/ativa-ativa e gerenciamento seguro de acessos e backups.

- Material didático: Preferencialmente em português.
- Certificado de conclusão: Para todos os participantes.
- Prazo de execução: Até 30 dias após a instalação e aceite dos equipamentos.
- Todos os encargos e ônus serão de responsabilidade da CONTRATADA.

3.2. O treinamento deverá ser ministrado seguindo estritamente a ementa oficial do fabricante da solução ofertada, sendo obrigatoriamente composto por módulos técnicos especializados que abranjam, de forma integral e aprofundada, os pilares de Segurança Avançada, SD-WAN, Gerenciamento Centralizado e Análise de Eventos (Logs).

3.3. A jornada de aprendizado deverá totalizar uma carga horária igual ou superior ao mínimo exigido, garantindo a transferência completa de conhecimento teórico e prático. O conteúdo deve capacitar a equipe técnica da CONTRATANTE na instalação, configuração, administração e diagnóstico, assegurando a autonomia operacional do ambiente.

4. PRESTAÇÃO DE SERVIÇO ESPECIALIZADO COM BANCO DE HORAS, INCLUINDO VERIFICAÇÃO DA SAÚDE DO AMBIENTE (LOGS, HARDWARE E LICENÇAS), INSTALAÇÃO E CONFIGURAÇÃO, ALÉM DE UMA GESTÃO DO CICLO DE VIDA (PATCHES E FIRMWARE).

4.1. Os serviços descritos neste, tratam de serviços técnicos junto a "Solução de Segurança" ofertada, os quais, terão suas demandas e atividades realizadas por profissional(is) designado(s) pela CONTRATADA, sendo ainda, permitidos ser apoiados ou realizados por especialista disponibilizado pelo fabricante da Solução, e deverão atender os seguintes critérios:

- Consultoria de Suporte para Especificação de Projetos;
- Suporte para Execução de Projetos;
- Operação Assistida e Documentação;
- Manutenções Preventivas;
- Manutenções Corretivas;
- Manutenções Evolutivas;
- Repasses tecnológicos (hand-on);
- Serviços Correlatos.

DESCRIÇÃO	CLASSIFICAÇÃO	CRITÉRIO
Consultoria de Suporte para Especificação de Projetos	Não Emergencial	Prestado somente em horário comercial.
Suporte para Execução de Projetos	Não Emergencial	Prestado somente em horário comercial.
Operação Assistida e Documentação	Não Emergencial	Prestado somente em horário comercial.
Manutenção preventiva	Não Emergencial	Parte de um plano pré-concebido ou agendado.
Manutenção corretiva	Emergencial	Intervenção para reestabelecimento de funcionalidades ou recursos normais que apresentem falha ou interrupção.
Manutenção evolutiva	Não Emergencial	Visa nova configuração ou adição de funcionalidades.
Repasses tecnológicos	Não Emergencial	Prestado somente em horário comercial.

TIPO	*CONSIDERAÇÕES*
EMERGENCIAL	*Um serviço será considerado emergencial quando houver impacto crítico ou risco iminente de paralisação de serviços de TIC e/ou processos de negócio, ou quando for identificada pela equipe técnica a necessidade de atuação imediata para evitar indisponibilidade, degradação severa ou falha relevante nos serviços das soluções ofertadas / contratadas.*

NÃO EMERGENCIAL	*Um serviço será considerado não emergencial quando sua execução não imediata não acarretar paralisações de serviços de TIC ou de processos de negócio do CONTRATANTE, ou mesmo quando a equipe técnica designada, o classificar como tal.*

4.2. **CONSULTORIA DE SUPORTE PARA ESPECIFICAÇÕES DE PROJETOS:**

4.2.1. A prestação dos serviços de consultoria de suporte para a especificação de projetos visa apoiar o Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE, na elaboração de planos de projeto de implantação de novos serviços junto a Solução, e integração a outras soluções de segurança estes já pré-existentes no ambiente de datacenter do mesmo;

4.2.2. A execução destes serviços deverá gerar subsídios para que o CONTRATANTE estabeleça planos de projetos visando a implantação dos objetivos pretendidos. Dentre os produtos/soluções a serem entregues a partir da prestação desta consultoria, citam-se: planos preliminares de projetos, detalhamento de escopo, especificação e dimensionamento de produtos e serviços, configurações, arquitetura de serviços, diagramas, estimativas de valores, restrições, prazos e demais variáveis pertinentes ao objetivo pretendido;

4.2.3. Este tipo de serviço será prestado somente em horário comercial, ou seja, em dia e hora útil (classificado, portanto, como NÃO EMERGENCIAL).

4.3. **SUPORTE PARA EXECUÇÃO DE PROJETOS:**

4.3.1. A prestação dos serviços de suporte para execução de projetos visa fornecer suporte operacional para o Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE, tendo como objetivo a execução de demanda e atividades, no que tange à implantação de projetos de novos serviços, projetos estes derivados dos serviços correlatos deste Item;

4.3.2. A utilização dos serviços de suporte para execução de projetos deverá estar vinculada a projetos que envolvam a implantação de algum novo serviço que envolva o atual ambiente segurado pela Solução, incluindo as integrações com outras Soluções de segurança, quando integráveis;

4.3.3. Este tipo de serviço será prestado somente em horário comercial, ou seja, em dia e hora útil (classificado, portanto, como NÃO EMERGENCIAL).

4.4. **OPERAÇÃO ASSISTIDA E DOCUMENTAÇÃO:**

4.4.1. A prestação dos serviços de operação assistida e documentação visa apoiar o "Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE, na execução temporária de rotinas operacionais, demanda ou atividades, visando a estabilização de novos serviços e soluções após processos de implantação, bem como, a geração de documentação;

4.4.2. Todos os serviços contratados por meio deste item, serão objeto de operação assistida, desde que o mesmo, seja voltado para as soluções ofertadas, assim como, suas possíveis integrações com outras soluções de segurança em produção no ambiente de datacenter do CONTRATANTE, e ainda:

- A operação assistida sempre será acompanhada por um profissional do "Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE, com o objetivo de absorção do conhecimento operacional para uso posterior.
- A documentação deverá conter minúcias de operação do serviço e eventualmente "As-Built" de configuração do objeto da operação assistida, visando criar condições para que o operador do "Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE, não necessite de reincidências dos serviços de operação assistida para o contexto em questão. Esta documentação será objeto de avaliação e aceite por parte do mesmo profissional supracitado, envolvido na operação assistida, o qual, constatará a suficiência da documentação para o desempenho das atividades;

4.4.3. Este tipo de serviço será prestado somente em horário comercial, ou seja, em dia e hora útil (classificado, portanto, como NÃO EMERGENCIAL).

4.5. **MANUTENÇÕES PREVENTIVAS, CORRETIVAS E EVOLUTIVAS:**

4.5.1. A prestação de serviços de manutenção, para este item de serviço, caracterizar-se-á segundo os seguintes critérios:

- MANUTENÇÃO PREVENTIVA: será realizada em serviço plenamente funcional, mas que eventualmente seja foco de recomendação de ajustes por parte do(s) fabricante(s) correlacionado(s), ou parte de um plano de manutenção preventiva pré-concebido ou agendado. Sempre será de característica NÃO EMERGENCIAL;
- MANUTENÇÃO CORRETIVA: será caracterizada pela intervenção do(s) profissional(is) designado(s) pela CONTRATADA para o reestabelecimento de funcionalidades ou recursos normais de serviços junto a Solução, que apresentem falha, ou mesmo interrupção em seu funcionamento. Sua característica será EMERGENCIAL, tendo em vista que quando acionada, para este item de serviço, não haverá comprometimento de níveis e prazos de serviços;
- MANUTENÇÃO EVOLUTIVA: será caracterizada pela prestação de serviços de manutenção eminentemente NÃO EMERGENCIAL, que visem nova configuração ou adição de funcionalidades e/ou recursos a determinado serviço de Defesa Cibernética, ou integrações com outras soluções de segurança em produção no ambiente de datacenter do CONTRATANTE, ou ainda, para própria Solução.

4.6. **REPASSES TECNOLÓGICOS (HAND-ON):**

4.6.1. Atividades de capacitação com foco prático, projetadas para transferir competências técnicas específicas para a equipe do cliente, garantindo autonomia na operação e manutenção do ambiente.

4.6.2. Este tipo de serviço será prestado somente em horário comercial, ou seja, em dia e hora útil (classificado, portanto, como NÃO EMERGENCIAL).

4.7. **SERVIÇOS CORRELATOS:**

4.7.1. Este item compreende atividades técnicas de sustentação e evolução da Solução contratada, limitadas aos seguintes escopos:

- Implantação e Ciclo de Vida: Instalação e configuração de componentes físicos ou virtuais, automação de backups, serviços de assessment e gestão de atualizações de firmware/patches (obrigatoriamente precedidos por análise de impacto e compatibilidade);
- Segurança Avançada: Readequação de políticas de firewall, ACLs, NAC (802.1x/MAC Auth) e perfis de segurança (IPS, WAF, Antivírus e Filtros de Web, DNS, Vídeo, E-mail e Arquivos);
- Redes e Conectividade: Gestão de VLANs, roteamento dinâmico (BGP/OSPF), QoS, planejamento de endereçamento IPv4/IPv6, geolocalização e configurações de WLAN/Captive Portal;
- SD-WAN e Disponibilidade: Configuração de zonas SD-WAN, malhas de túneis VPN (SSL/IPSec), topologias Hub-Spoke/Full-Mesh e clusters de Alta Disponibilidade (HA);
- Inteligência e Automação: Customização de dashboards de monitoração, alertas, relatórios técnicos e desenvolvimento de playbooks de automação para resposta a incidentes.

4.7.2. Para o acionamento destes serviços, a CONTRATANTE deverá detalhar a demanda evidenciando o alinhamento com o objeto, reservando-se à CONTRATADA o direito de recusar solicitações que extrapolem o escopo técnico previsto.

4.8. **FORMAS DE EXECUÇÃO:**

4.8.1. A prestação dos serviços de apoio, operação e manutenção será autorizada por meio de "Solicitações de Atendimento", pelo "Gestor do Contrato" indicado pelo CONTRATANTE, as quais deverão ser registradas e acompanhadas pelo mesmo "Sistema de Gestão de Chamados" disponibilizado pelo mesmo;

4.8.2. No ato do registro da "Solicitação de Atendimento", o CONTRATANTE, através do seu "Time de Segurança" e/ou "Níveis

N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo mesmo, deverá informar se o serviço será característica EMERGENCIAL ou NÃO EMERGENCIAL, conforme avaliação do profissional técnico responsável pela sua solicitação;

4.8.3. Os serviços EMERGENCIAIS, poderão ser prestados a qualquer momento, ou seja, em regime 24x7 (vinte e quatro horas por dia, os sete dias da semana), desde que acordado com a CONTRATADA, visando garantir a continuidade dos serviços de TIC ou de processos de negócio do CONTRATANTE;

4.8.4. Os demais serviços NÃO EMERGENCIAIS serão prestados em horário comercial, em regime 8x5 (oito horas por dia, os cinco dias úteis da semana), e ainda:

- As atividades programadas (NÃO EMERGENCIAIS), as quais, possam interferir negativamente no ambiente de datacenter do CONTRATANTE, provocando paralisações, deverão ser executadas preferencialmente fora do horário comercial, devendo a programação ser submetida à aprovação da equipe técnica designada do mesmo.
- Os prazos de atendimento poderão ser prorrogados, desde que aceitas pelo CONTRATANTE mediante justificativas apresentadas pela CONTRATADA, quando estas revelarem a necessidade de dilatação do prazo.

4.8.5. As "Solicitações de Atendimento" serão reguladas segundo as regras abaixo:

4.8.6. Deverá ser possível a abertura da "Solicitações de Atendimento", apenas via "Sistema de Gestão de Chamados" disponibilizado pelo próprio CONTRATANTE, podendo ser acionado, quando EMERGECIAL, por número de telefone e/ou e-mail. O detalhamento dos métodos segue abaixo:

- O registro via "Sistema de Gestão de Chamados" será a principal forma de abertura das "Solicitações de Atendimento" e de relacionamento técnico entre o CONTRATANTE e a CONTRATADA. A CONTRATADA, através do(s) seu(s) profissional(is) designado(s), deverão utilizar e interagir, realizando registros e

acompanhamento de todo o ciclo de atendimento, desde a solicitação até o encerramento do mesmo;

- A CONTRATADA disponibilizará atendimento, quando EMERGENCIAL, através de número de telefone e/ou e-mail, inclusive fora do horário comercial, de forma a garantir atendimento segundo os níveis e prazos dos serviços especificados neste Item. Devendo ser de sua responsabilidade registrar e gerenciar o atendimento telefônico e/ou por e-mail, de forma a permitir o acompanhamento de todo o ciclo de atendimento desde a sua solicitação até o seu encerramento.

4.8.7. Os serviços previstos neste item serão prestados, por padrão e de forma preferencial, na modalidade remota. O atendimento on-site (presencial) nas dependências da CONTRATANTE terá caráter opcional e excepcional, sendo realizado apenas quando expressamente solicitado pela equipe técnica da PRODABEL e desde que a natureza da atividade (ex: instalação física de hardware, trocas ou reparo de peças) exija a presença de um técnico no local.

4.8.8. Ao final do serviço será apresentado um relatório contendo escopo e prazo de realização do serviço, bem como, as ações tomadas para concluir o atendimento.

4.8.9. A CONTRATADA deverá encaminhar ao CONTRATANTE, um relatório técnico de execução de serviços, devendo constar deste relatório no mínimo as seguintes informações:

- Data/hora da solicitação;
- Nome do solicitante;
- Data/hora:minutos do início do atendimento;
- Descrição da solicitação;
- Descrição das atividades desempenhadas, de forma a permitir confronto entre o atendimento previsto e atendimento realizado;
- Data/hora:minutos de encerramento do atendimento;
- Quantidade efetiva de horas técnicas despendidas no atendimento, sendo este parâmetro a base do faturamento dos serviços, devendo ser obtido a partir da diferença entre "Data/hora:minutos do início do

atendimento" e "Data/hora:minutos de encerramento do atendimento", e ainda:

4.8.10. Não deverão ser contabilizadas horas consumidas com: preenchimento de relatório, deslocamentos, almoço, lanche ou qualquer outro procedimento não relacionado diretamente aos serviços. Nos casos em que houver a exigência de um suporte on-site, a quantidade efetiva de horas técnicas consumidas será contabilizada e abatida do banco de horas mensal apenas a partir do início da execução técnica no local (ex: instalação física de hardware, trocas ou reparo de peças). Conforme previsto no detalhamento deste item, não deverão ser contabilizadas nem abatidas do saldo de horas quaisquer despesas ou tempos relacionados a deslocamentos, transporte, estadias ou alimentação do profissional designado.

4.8.11. A quantidade efetiva de horas técnicas despendidas no atendimento será registrada horas:minutos.

4.8.12. Este relatório deverá ser encaminhado ao CONTRATANTE, de forma a servir de referência para a sua fiscalização;

4.8.13. Somente serão considerados válidos os serviços devidamente registrados no relatório acima citado e validados tecnicamente pelo "Time de Segurança" e/ou "Níveis N3" indicados pela equipe técnica designada, ou ainda, por prestadores de serviços disponibilizados pelo CONTRATANTE;

4.8.14. Ao final de cada mês, a CONTRATADA deverá apresentar um Relatório Mensal de Atividades consolidado, além dos relatórios individuais por chamado. Este documento deverá listar cronologicamente:

- As verificações de saúde do ambiente (logs, hardware e licenças);
- O status de conformidade das assinaturas de segurança e versões de firmware;
- A quantidade efetiva de horas técnicas consumidas, discriminando o início e fim de cada atendimento para fins de abatimento no banco de horas;
- O atesto de pleno funcionamento do objeto, servindo como base para a fiscalização e o pagamento mensal.

4.8.15. O banco de horas previsto para a prestação de serviço especializado possui ciclo de renovação mensal, dimensionado para garantir o

apoio técnico ao órgão. O saldo de horas não consumido dentro do mês de competência não será cumulativo, expirando automaticamente ao final do respectivo período, não podendo ser transportado para meses subsequentes ou utilizado como crédito para futuras demandas.

4.9. SOBRE OS SERVIÇOS DE INSTALAÇÃO

4.9.1. Observações para os Serviços específicos para instalação da solução. A CONTRATADA deverá estar apta a realizar a instalação física e a configuração lógica dos appliances de segurança de borda das Unidades Remotas, incluindo:

- Configuração e Sincronismo de Armazenamento: Configuração do sistema operacional e ativação do sistema de armazenamento interno composto por 02 (duas) unidades SSD operando em espelhamento (RAID 1), garantindo a integridade dos logs locais e dos dados de análise forense.
- Alta Disponibilidade (HA): Configuração de cluster em modo Ativo-Passivo ou Ativo-Ativo com sincronismo total de sessões, tabelas de roteamento e estados de segurança, garantindo a continuidade de serviços em caso de falha de hardware.
- Integração com Ecossistema de Gestão e Análise: Onboarding dos equipamentos na plataforma de orquestração centralizada e na plataforma de análise de eventos, permitindo a gerência via templates e a correlação de logs de segurança em tempo real.
- Agregação de Links e Performance: Configuração de agregação de interfaces (LACP) e interfaces de ultra-baixa latência (ULL) para interconexão com o core do datacenter em velocidades de 10Gbps ou 25Gbps.
- Orquestração de SD-WAN Hub: Configuração das interfaces de transporte (Underlays), criação da malha de túneis criptografados (Overlays) e definição de zonas SD-WAN para concentrar o tráfego das unidades remotas.
- Políticas de WAN Intelligence e SLA: Implementação de regras de inteligência de aplicação (Camada 7) e monitoramento de saúde de links (Performance SLA)

baseado em latência, jitter e perda de pacotes para garantir o tráfego de aplicações críticas.

- Segurança Avançada e Inspeção SSL: Configuração de perfis de Antivírus, Prevenção de Intrusão (IPS), Controle de Aplicações e inspeção profunda de tráfego criptografado (Deep SSL Inspection).
- Provisionamento Automatizado (Zero Touch Provisioning): Configuração do onboarding automatizado dos equipamentos junto à plataforma de orquestração central, garantindo que as unidades remotas recebam suas políticas e configurações de forma padronizada via Templates, sem necessidade de intervenção técnica local complexa.
- Configuração de Conectividade Híbrida (Underlays): Configuração e monitoramento de múltiplos links de transporte (ex: Banda Larga e MPLS), com suporte a endereçamento estático e dinâmico.
- Implementação de Túneis de Malha (Overlays): Criação automática de túneis criptografados seguros para comunicação com o Data Center (Hub-and-Spoke) e suporte à criação dinâmica de túneis entre unidades (Full-Mesh) para otimização de tráfego.
- Inteligência de Aplicação e SD-WAN: Configuração de regras para reconhecimento de aplicações em Camada 7 e direcionamento inteligente de tráfego baseado na saúde dos links e prioridades de negócio.
- Monitoramento de SLA e Saúde do Link: Configuração de medições ativas e passivas de latência, jitter e perda de pacotes para garantir a qualidade de aplicações críticas.
- Segurança Avançada de Borda: Implementação de políticas de firewall integradas com Prevenção de Intrusão (IPS), Antivírus, Filtro Web e inspeção profunda de tráfego criptografado nas filiais.
- Remediação de Links e Confiabilidade: Ativação de mecanismos de Correção de Erro Antecipada (FEC) e duplicação de pacotes para mitigar falhas em circuitos degradados e garantir a continuidade das sessões.
- Integração com Visibilidade e Telemetria: Habilitação do envio de logs e dados de telemetria para a plataforma de

análise central, permitindo o monitoramento da experiência digital do usuário final na filial.

- Testes de Aceite e Homologação: Validação da comutação automática de links (Failover), testes de performance WAN e verificação da conformidade das políticas de segurança.
- Documentação As-Built e Transferência de Conhecimento: Entrega de documentação técnica detalhada da unidade e repasse operacional para a equipe da CONTRATANTE, incluindo as instruções detalhadas de como abrir chamado técnico e utilizar o portal de suporte junto ao Fabricante.

4.9.2. A CONTRATADA deverá realizar a instalação física e a configuração lógica de todos os componentes que integram a solução, garantindo a interoperabilidade nativa entre as unidades de Datacenter e Unidades Remotas. A execução dos serviços deve observar o detalhamento técnico descrito nos itens específicos de cada solução.

4.9.3. Tempo estimado de execução: até 70 dias úteis.