PREVIC
Superintendência Nacional de Previdência Complementar

PROCESSO Nº 44011.005386/2022-14

TERMO DE REFERÊNCIA

FIREWALL DO TIPO "NEXT-GENERATION FIREWALL" (NGFW)

HISTÓRICO DE REVISÕES			
Data	**Versão**	**Descrição**	**Autor**
01/09/2022	1.0	Criação do documento.	Alexandre Crusca Pozzetti
06/09/2022	1.1	Levantamento de informações e requisitos para a contratação	Wendel Martinez Carvalho
23/09/2022	1.2	Edição e inclusão das informações referentes à contratação	Alexandre Crusca Pozzetti
29/09/2022	1.3	Atualização e Revisão de requisitos	Alexandre Crusca Pozzetti
14/10/2022	1.4	Atualização dos valores máximos da contratação após propostas e análise crítica	Alexandre Crusca Pozzetti
27/10/2022	1.5	Alterações para atendimento do Parecer Técnico da Procuradoria Federal junto a Previc	Alexandre Crusca Pozzetti

Observações:

1- Conforme mandamento posto no art. 29 da IN nº 05, de 2017, o modelo deste Termo de Referência está atualizado de acordo com o documento encontrado no sítio eletrônico da AGU (ultima atualização julho/2021);
2 - Este documento segue estritamente a ordem dos itens do modelo da AGU até o Subitem 19.
3 - Todos os Subitens posteriores foram inseridos para dar maior detalhamento da necessidade de contratação desta Autarquia Federal.

1. **DO OBJETO**

1.1. 1.1. Aquisição de equipamentos Firewall do tipo "Next-Generation Firewall" (NGFW), contemplando serviço de instalação, configuração, repasse de conhecimento, suporte e garantia, conforme condições, quantidades e exigências estabelecidas neste instrumento:

1.2. **BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO**

1.2.1. O objeto deste Termo de Referência envolve bens e serviços especializados em Tecnologia, Comunicação e Segurança da Informação, aderentes às especificações técnicas estabelecidas neste Termo de Referência.

GRUPO ÚNICO – SOLUÇÃO DE SEGURANÇA DE REDE COM FIREWALL DE ÚLTIMA GERAÇÃO (NGFW)

Grupo	Item	Descrição/Especificação	CATMAT	Unidade de Medida	Quantidade
Único	**1.1**	Firewall do tipo "Next-Generation Firewall" (NGFW), incluindo licenciamento de uso e garantia e suporte técnico de no mínimo 48 meses.	481646	Dispositivo	02
	1.2	Serviço de instalação e configuração da solução de Firewall NGFW.	26972	Serviço	01
	1.3	Treinamento oficial do Firewall.	20052	Serviço	01

1.2.2. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.

1.2.3. Os itens registrados em grupo único são constituídos por equipamentos, suprimentos, licenças e serviços integrados entre si, de forma a convergir para uma solução unificada. Assim sendo, o fornecimento parcelado desses itens individuais inviabilizaria a implantação da solução. Por este motivo, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 ("*I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas*").

1.2.4. A contratação para execução indireta de serviços será realizada pelo regime de "**Empreitada por Preço Unitário**", onde se contrata a execução de um serviço por preço certo de unidades determinadas (alínea "b" no inciso VIII do art. 6º da Lei n° 8.666/1993).

1.2.5. Considerando a natureza dos serviços e o disposto no parágrafo único do art. 25 da Instrução Normativa SGD/ME nº 01/2019, a licitação será realizada na **modalidade Pregão Eletrônico do tipo Menor Preço Global** por grupo.

1.2.6. O prazo de vigência da contratação é de 12 meses contados da publicação do instrumento de contrato, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

2. **JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO**

2.1. A Justificativa e o objetivo da contratação encontram-se pormenorizadas em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência (Documento SEI nº 0498489).

3. **DESCRIÇÃO DA SOLUÇÃO**

3.1. A descrição da solução como um todo, encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência (Documento SEI nº 0498489).

4. **CLASSIFICAÇÃO DOS BENS COMUNS**

4.1. Trata-se de aquisição de bem comum, a ser contratada mediante licitação, na modalidade pregão, em sua forma eletrônica.

4.2. Os objetos a serem contratados enquadram-se na classificação de bens comuns, nos termos do parágrafo único, do art. 1°, da Lei 10.520, de 2002, c/c item II do art. 3º do Decreto nº 10.024/2019. Além disso, todos possuem padrões de desempenho e qualidade objetivamente definidos por meio de especificações usuais praticadas no mercado, conforme § 2º do artigo 12 do Decreto nº 7.174, de 12 de maio de 2010;

5. **CRITÉRIOS DE SUSTENTABILIDADE**

5.1. A Contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 3º da Lei nº 8.666/93 e com o art. 6º da Instrução Normativa/SLTI/MPOG nº 01, de 19 de janeiro de 2010.

5.2. Aplicar as normas técnicas da Associação Brasileira de Normas Técnicas – **ABNT NBR**, referente ao uso de materiais atóxicos, biodegradáveis e recicláveis, quando aplicável ao objeto desta contratação.

5.3. A empresa contratada deve estar aderente, no que couber, à Lei nº 12.187/09 (Política Nacional sobre Mudança do Clima), a Lei nº 12.305/10 (Política Nacional de Resíduos Sólidos), especialmente seu art. 7º, inc. XI, o Decreto nº 7.404/10 (arts. 5 a 7), a Instrução Normativa SLTI/MP nº 01/10 (Critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional), a Instrução Normativa SLTI/MP n.º 02/2014 (Aquisição ou locação de máquinas e aparelhos consumidores de energia pela Administração Pública Federal direta, autárquica e fundacional, e uso da Etiqueta Nacional de Conservação de Energia [ENCE] nos projetos e respectivas edificações públicas federais novas ou que recebam retrofit.

5.4. Somente poderão ser utilizados na execução dos serviços bens de informática e/ou automação que possuam a certificação de que trata a Portaria INMETRO nº 170, de 2012 ou que possuam comprovada segurança, compatibilidade eletromagnética e eficiência energética equivalente.

5.5. Somente poderão ser utilizados na execução dos serviços bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenilpolibromados (PBDEs).”

5.6. De acordo com a IN/SEGES 1/2010, art. 5º, a presente contratação está de acordo com o "Guia Nacional de Licitações Sustentáveis”, editado pela CGU/AGU.

6. **ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO**

6.1. A CONTRATADA deverá, em no máximo 30 (trinta) dias corridos, contados a partir do recebimento da nota de empenho e/ou da assinatura do contrato, apresentar o Projeto Executivo contendo detalhamento da proposta técnica e o plano de implantação dos equipamentos. Para tal, a CONTRATADA deverá se familiarizar com a infraestrutura da CONTRATANTE e prever no projeto a melhor forma de instalação.

6.2. A entrega dos equipamentos deverá ocorrer no prazo máximo de 60 (sessenta) dias, contados do recebimento pela CONTRATADA da assinatura do contrato ou da respectiva nota de empenho.

6.2.1. Eventual necessidade de prorrogação do prazo supracitado deverá ser devidamente justificado e requisitado com no mínimo 10 (dez) dias antes do fim do prazo do subitem anterior.

6.3. A entrega se dará em remessa *única*, no seguinte endereço: Setor Comercial Norte Q 6, Shopping ID, Torre A, 3º Andar - Asa Norte, Brasília - DF.

6.4. Os bens serão recebidos provisoriamente no prazo de 10 (dez) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

6.5. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

6.6. Os bens serão recebidos definitivamente no prazo de 10 (dez) dias, contados da devida instalação e configuração dos equipamentos;

6.6.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

6.7. Deverá ser entregue junto com os equipamentos, ou disponibilizados por meio digital, os certificados de garantia dos equipamentos.

6.8. A validade da garantia dos equipamentos adquiridos será verificada junto ao fabricante dos equipamentos;

6.9. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7. **OBRIGAÇÕES DA CONTRATANTE**

7.1. São obrigações da Contratante:

7.1.1. receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

7.1.2. verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

7.1.3. comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

7.1.4. acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

7.1.5. efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

7.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

8. **OBRIGAÇÕES DA CONTRATADA**

8.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

8.1.1. efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: *marca, fabricante, modelo, procedência e prazo de garantia ou validade;*

8.1.1.1. O *objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;*

8.1.2. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

8.1.3. substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

8.1.4. comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

8.1.5. manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

8.1.6. indicar preposto para representá-la durante a execução do contrato.

8.1.7. promover a destinação final ambientalmente adequada, sempre que a legislação assim o exigir, como nos casos de pneus, pilhas e baterias, etc....

8.2. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;

9. DA SUBCONTRATAÇÃO

9.1. É vedada a subcontratação total ou parcial do objeto.

9.2. O suporte técnico do fabricante não caracteriza subcontratação.

10. DA ALTERAÇÃO SUBJETIVA

10.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

11. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

11.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

11.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

11.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

12. DO PAGAMENTO

12.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado, conforme disposto artigo 40, XIV, “a”, da Lei 8.666, de 1993.

12.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

12.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

12.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

12.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

12.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

12.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

12.6. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

12.7. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

12.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

12.9. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

12.10. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

12.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

12.11.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

12.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

12.12.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

12.13. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

12.14. EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I= (TX)	I=	(6 / 100)	I = 0,00016438
		365	TIX = Percentual da taxa anual = 6%

13. **DO REAJUSTE**

13.1. Por se tratar de contratação de equipamentos e serviços de instalação de repasse de conhecimento, não haverá prorrogação contratual e reajuste aplicável a esta contratação.

14. **DA GARANTIA DE EXECUÇÃO**

14.1. *O adjudicatário, no prazo de 15 (quinze dias) após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a 5%* (cinco por cento) *do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.*

14.2. *Caberá ao contratado optar por uma das seguintes modalidades de garantia:*

14.2.1. *caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;*

14.2.2. *seguro-garantia;*

14.2.3. *fiança bancária.*

14.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.

14.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

14.5. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 15 (quinze) dias úteis, contados da data em que for notificada.

14.6. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

14.7. A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente. (artigo 56, §4º da Lei nº 8666/93).

15. **DA GARANTIA CONTRATUAL DOS BENS**

15.1. *O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 57 (cinquenta e sete) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto, tendo em vista que tratam-se de equipamentos de alto custo e alta complexidade tecnológica, além de serem imprescindíveis para a manutenção das atividades da CONTRATANTE;*

15.1.1. *A garantia total dos bens deve ser de, no mínimo, 60 (sessenta) meses.*

15.2. *A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.*

15.3. *A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.*

15.4. *Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.*

15.5. *As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.*

15.6. *Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 05 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.*

15.7. *O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante.*

15.8. *Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.*

15.9. *Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da Contratada o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.*

15.10. *O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.*

15.11. *A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.*

16. **DAS SANÇÕES ADMINISTRATIVAS**

16.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

a) Falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas na contratação;

b) Ensejar o retardamento da execução do objeto;

c) Falhar ou fraudar na execução do contrato;

d) Comportar-se de modo inidôneo;

e) Cometer fraude fiscal;

16.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

16.2.1. Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

16.2.2. multa moratória de 0,33% (zero vírgula trinta e três por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

16.2.3. multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

16.2.4. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

16.2.5. impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

16.2.6. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

16.3. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

16.3.1. As sanções previstas nos subitens 16.2.1, 16.2.4, 16.2.5 e 16.2.6 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando -a dos pagamentos a serem efetuados.

16.3.2. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

16.3.2.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

16.3.2.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

16.3.2.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

16.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

16.5. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

16.5.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada p ela autoridade competente.

16.6. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

16.7. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.8. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

16.9. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

16.10. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

16.11. As penalidades serão obrigatoriamente registradas no SICAF.

17. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

17.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

17.2. Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor estão previstos no edital.

17.3. Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de serviços em características e quantidades compatíveis com a presente licitação, mediante apresentação de um ou mais ATESTADO(S) DE CAPACIDADE TÉCNICA que deverão comprovar o fornecimento de, no mínimo, 50% (cinquenta por cento) do volume estimado de equipamentos com características compatíveis com o objeto da presente pretensão contratual, incluindo garantia e assistência técnica, podendo considerar contratos já executados e/ou em execução.

17.4. A comprovação de capacidade técnica será realizada individualmente para cada item.

17.5. Para cada item, a(s) Licitante(s) deverá(ão) apresentar:

17.5.1. a) atestado(s) que se refiram a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior devendo ser comprovado por meio do contrato;

17.5.2. b. atestado(s) que se refiram a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

17.6. A licitante deve disponibilizar, quando solicitado. todas as informações necessárias à comprovação de legitimidade do(s) atestado(s) apresentado(s) fornecendo, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foram prestados os serviços.

17.7. *Os critérios de aceitabilidade de preços serão:*

17.8. *Valor Global por Grupo:*

17.8.1. *Grupo I:* **R$ 1.205.000,00**

17.8.2. O critério de julgamento da proposta é o menor preço global, por Grupo.

17.9. As regras de desempate entre propostas são as discriminadas no edital.

18. **DA ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS**

18.1. O valor máximo aceito pela Administração para essa contratação é de R$ 1.205.000,00 (um milhão duzentos e cinco mil reais) . Os valores foram calculados levando em consideração os preços MÁXIMOS aceitos no grupo único, conforme tabela abaixo:

GRUPO	ITEM	DESCRIÇÃO DOS EQUIPAMENTOS	QUANTIDADE	VALOR TOTAL (R$)
Único	**1.1**	Firewall do tipo "Next-Generation Firewall" (NGFW), incluindo licenciamento de uso e garantia e suporte técnico de no mínimo 48 meses.	02	**1.205.000,00**
	1.2	Serviço de instalação e configuração da solução de Firewall NGFW.	01	
	1.3	Treinamento oficial do Firewall.	01	

18.2. **Análise Crítica dos Preços.**

18.2.1. Em conformidade com Acórdão 1108/2007 do Tribunal de Conta da União, quanto à análise crítica da pesquisa de preços, informamos que todos os editais/ARP´s foram objeto de análise pela equipe de planejamento da contratação, tratando-se de equipamentos similares ao demandado pela Autarquia.

18.2.2. Foi também realizado pesquisa junto ao site "painel de preços", do Governo Federal, bem como foram encontradas contratações públicas de outros entes federativos, todos compiladas nos expedientes SEI nº 0498427e nº 0498434.

18.2.3. A fim de atender os requisitos dispostos na Instrução Normativa nº 73, de 5 de agosto de 2020 (§ 3° do art. 6°) acerca de pesquisa de mercado, seguem informações abaixo:

I - identificação do agente responsável pela cotação: **Alexandre Crusca Pozzetti e Nilton Ricardo Guimaraes S. Cunha**

II - caracterização das fontes consultadas: Painel de Preços, Editais Federais Homologados e de outros entes públicos (SEI nº 0498434);

III - série de preços coletados: Vide Planilha de Cotações, justificativa e analise crítica (SEI nº 0498430);

IV - método matemático aplicado para a definição do valor estimado: Menor preço.

V - justificativas para a metodologia utilizada, em especial para a desconsideração de valores inexequíveis, inconsistentes e excessivamente elevados, se aplicável: a metodologia utilizada teve o intuito de adequar o preço a ser estimado à nossa realidade, pois a maioria dos parâmetros são oriundos de contratações com quantitativo superior ao demandado pela Previc. Assim, considerando que a economia de escala pode reduzir os valores quando a compra se refere a muitos equipamentos, julgamos prudente não considerarmos o menor preço encontrado como critério de estimativa, a fim de não frustrar o certame.

19. **DOS RECURSOS ORÇAMENTÁRIOS**

19.1. *As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:*

19.1.1. Programa de Trabalho: 09.122.0032.2000.0001

19.1.2. Natureza da Despesa Firewall: 44.90.52.43

19.1.3. Plano de Trabalho Resumido (PTRES): 204627

19.1.4. Plano Orçamentário: 0002

19.1.5. Fonte: 0174

20. **ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO INSTITUCIONAIS**

20.1. A presente proposta de contratação está alinhada com o Planejamento Institucional e visa contribuir para o alcance do objetivo elencado no atual Plano Estratégico da Previc.

20.2. Segundo o Planejamento Estratégico da Previc, publicado na Portaria nº 266, de 17 de junho de 2020, em sua perspectiva de eficiência administrativa, é um objetivo do Ministério: "*Objetivo N1 - Intensificar uso de tecnologia nos processos de trabalho e de supervisão*.

20.3. Este Termo de Referência também está alinhado com o Plano Diretor de Tecnologia da Informação - PDTI 2020 - 2022, assim como possui registro no Plano Anual de Contratações 2022.

20.4. Segue abaixo a tabela de alinhamento estratégico:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**OBJETIVOS ESTRATÉGICOS**
N1	Intensificar uso de tecnologia nos processos de trabalho e de supervisão.
ALINHAMENTO AO PDTIC 2020-2022	
ID	**Item do PDTIC**
N88	Contratação de equipamento para proteção de dados (Firewall)
ALINHAMENTO AO PAC 2022	

Item	Descrição
	Contratação de equipamento para proteção de dados (Firewall)

Tabela: Alinhamentos de planejamento institucionais

21. **ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

REQUISITOS TÉCNICOS GERAIS

21.1. **GRUPO Único - ITEM 1.1 -** ***Firewall do tipo Next-Generation (NGFW)***

21.1.1. Quantidade: 02 (dois) dispositivos.

21.1.2. Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), formada por dois dispositivos físicos (appliances) interconectados e operando em modo de alta disponibilidade, com recursos de virtualização de sistemas, filtragem de pacotes, filtro de URL (web-filtering) com controle de transmissão de dados e de acesso à internet, controle de aplicação, controle por meio de identificação de usuários, controle de uso de largura de banda (QoS), SD-WAN; recursos de VPN (site-to-site e client-to-site) em tecnologia IPSec e SSL, sistema de prevenção de intrusão (IPS) e prevenção contra ameaças de vírus, spywares e malwares, incluindo os de tipo “Zero Day”.

21.1.3. Caso o modelo de licenciamento da solução ofertada seja do tipo “modular”, os seguintes módulos da solução deverão estar devidamente licenciados para uso imediato, assim que concluída a etapa de instalação e configuração da solução, conforme especificações contidas no Item 02 deste grupo:

21.1.3.1. Segurança avançada de Firewall;

21.1.3.2. Virtualização de sistemas;

21.1.3.3. VPN;

21.1.3.4. Filtro de conteúdo web (URL Filtering);

21.1.3.5. Quality of Service (QoS);

21.1.3.6. Controle avançado de aplicações;

21.1.3.7. Controle de identificação de usuários, com integração obrigatória ao sistema de controle de diretórios da PREVIC- *Microsoft Active Directory* (LDAP);

21.1.4. Os módulos de integração de redes SD-WAN e de proteção contra ameaças de vírus, malwares e spywares não deverão ser imediatamente licenciados, visto que a PREVIC não pretende utilizá-los de imediato, seja por conta de sua configuração atual de rede WAN, seja pela existência no ambiente de ferramentas que já cumprem essa função e que ainda possuem contrato vigente de garantia e suporte técnico.

21.1.5. Conjunto de dispositivo físico (appliance) de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), sistema operacional embarcado no dispositivo e software para sua gestão e monitoramento, permitindo o controle granular das políticas de segurança de rede, atuando além da camada 2 a 4 do modelo OSI, ou seja, além da filtragem por endereços MAC e endereços e portas TCP/IP, permitindo a configuração de políticas de segurança também por aplicações, incluindo seu conteúdo, usuários e tipos de tráfego de rede, recursos tipicamente executados em camada 7.

21.1.6. O Firewall NGFW deve ser do tipo “rackmount”, permitindo sua instalação em racks de Datacenter no padrão 19 polegadas, devendo consumir um espaço no rack de no máximo 2U por dispositivo.

21.1.7. Não serão aceitos equipamentos servidores (“rack servers”) e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux para usuários finais, adaptados para funcionar como “appliance” físico. Ou seja, a solução como um todo de ser fabricada pelo mesmo fornecedor, tanto em seus componentes físicos de hardware quando seus softwares embarcados principais.

21.1.8. O software que executa a função de console de administração e monitoramento da solução poderá ser fornecido à parte, para instalação em máquinas físicas ou virtuais, não necessitando ser obrigatoriamente embarcado no appliance físico. Nestes casos, este módulo da solução deverá ser compatível com o ambiente de virtualização da PREVIC – Microsoft Hyper-V 2016 em modo clusterizado, devendo ser instalado em sistema operacional Windows Server (versão 2016 ou superior) ou Linux (distribuições com suporte e atualização vigentes na data de instalação).

21.1.9. Tanto o dispositivo físico (“appliance”) quanto seus softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site da fabricante da solução como item “end-of-life”, “end-of-sale” ou outros status que denotem que a solução se encontra em processo de descontinuidade pelo seu fabricante.

21.1.10. Todas as funcionalidades da solução Firewall NGFW deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo após o fim do contrato de suporte técnico e garantia do fabricante, e mesmo que não subsista mais o direito de receber atualizações por descontinuidade da solução por parte da fabricante. Inclui todos os recursos típicos do Firewall NGFW, como filtro URL, IDS/IPS, controle por identificação de usuários, controle de aplicações, VPN (IPSec e SSL), QoS, de-criptografia SSL e SSH, DHCP services (server, client e relay), NAT, VLAN e protocolos de roteamento dinâmico.

21.1.11. **Alimentação de energia**

21.1.11.1. O dispositivo deve possuir tecnologia de alimentação redundante de energia, com no mínimo 02 (duas) fontes do tipo “hot-swap”, bivolts (100-240 VAC – 50/60 Hz), com possibilidade de serem alimentadas em corrente contínua, com carga entre 48 e 60 VDC. Cada fonte de alimentação deve ser capaz de sozinha suprir todo o equipamento em sua completa atividade.

21.1.11.2. Cada fonte deve ser acompanhada por seu respectivo cabo de alimentação (power chord), padrão 3 pinos NBR 14.136, com comprimento mínimo de 2,5 m (dois metros e meio).

21.1.12. **Memória interna e armazenamento**

21.1.12.1. Para armazenamento de seu sistema operacional, arquivos de configuração e logs, o dispositivo deverá possuir, no mínimo, 01 (uma) unidade de armazenamento de alta performance, do tipo “Solid State Drive” (SSD), com capacidade mínima de armazenamento de 230 GB (duzentos e trinta gigabytes).

21.1.12.2. A unidade de armazenamento SSD deve ser do tipo externamente removível, com trava física de remoção, e estar acessível facilmente seja pela parte frontal, seja pela parte traseira do Firewall NGFW.

21.1.12.3. Não serão aceitos equipamentos com unidades internas de armazenamento que necessitem de abertura total de sua carcaça, ou sua retirada da rack para sua remoção ou substituição.

21.1.13. **Interfaces de conexão de rede**

21.1.13.1. Possuir, no mínimo, as seguintes interfaces de conexão:

21.1.13.1.1. 04 (quatro) interfaces de rede 10 Gbps, padrão SFP+, compatíveis com transceivers padrão SFP de 1 Gbps.

21.1.13.1.2. 04 (quatro) interfaces de rede 1 Gbps, padrão SFP, distintas das 04 interfaces SFP+ anteriormente exigidas.

21.1.13.1.3. 12 (doze) interfaces de rede Ethernet, padrão RJ-45, podendo transferir dados em padrão Ethernet (10 mpbs), Fast Ethernet (100 mpbs), e Gigabit Ethernet (1 Gbps), duplex e auto negociáveis.

21.1.13.1.4. 02 (duas) duas interfaces dedicadas exclusivamente para configuração de alta disponibilidade entre os 02 (dois) Firewalls, sendo que pelo menos uma das interfaces deve operar em velocidade mínima de 10 Gbps. Caso utilize interface de padrão proprietário da fabricante, cada porta deste tipo de vir acompanhada com o respectivo cabo de interconexão, de modo a permitir a conexão dos dois firewalls, que estarão instalados sequencialmente em um rack, com distância máxima entre eles de 2U. Caso trabalhe em padrão SFP/SFP+, cada interface deverá vir acompanhada de seu respectivo transceiver devidamente ativado.

21.1.13.1.5. 02 (duas) interfaces de gerenciamento, padrão Ethernet 10/100/1000 RJ-45, sendo que pelo menos uma delas seja para gerenciamento direto via console, ou seja, com conexão direta do dispositivo a um computador ou dispositivo similar em modo terminal, e outra seja para gerenciamento remoto via interface gráfica.

21.1.13.1.6. 01 (uma) porta USB padrão (1.0 ou superior), para conexão direta de flash drives com função de instalação e inicialização do sistema operacional do NGFW (“bootstrap”), sem necessidade de conexão ativa à internet.

21.1.13.1.7. 01 (uma) porta Micro-USB para acesso de console no modo terminal.

21.1.13.2. *Transceivers para conexão dos firewalls NGFW ao ambiente de rede da PREVIC:*

21.1.13.3. Deverá ser fornecido no mínimo os seguintes transceivers, todos do tipo bidirecional “short range”, devidamente ativos e licenciados para funcionamento:

21.1.13.3.1. 8 (oito) módulos transceivers 10GE SFP+ (quatro para cada Firewall NGFW);

21.1.13.3.2. 8 (oito) módulos transceivers 1G SFP (quatro para cada Firewall NGFW);

21.1.13.4. Além destes transceivers, deverão ser fornecidos transceivers adicionais para interfaces de redundância e alta disponibilidade, caso necessários, na quantidade suficiente para configurar a solução em modo “alta disponibilidade”.

21.1.14. **Performance de rede**

21.1.14.1. Todas as taxas de performance constantes a seguir deverão ser comprovadas por meio de publicação oficial de domínio público da fabricante, como Manuais de Operação ou “Datasheets”, facilmente encontrados no sítio da fabricante. Não serão aceitos documentos elaborados por terceiros, ou publicações de sítios do tipo “resenha de produto”;

21.1.14.2. Taxas mínimas de throughput aceitas, considerando-se transferências de dados em aplicações web com tráfego no protocolo HTTP ou em um conjunto de protocolos usualmente utilizados para aplicações desta natureza, utilizando-se de pacotes de tamanho máximo do protocolo TCP/IP (64 KB), em cenário de simulação de tráfego real (“real-world traffic band”), com os recursos de auditoria ativados (logs) e sem a utilização de recursos de aceleração de pacotes abaixo da camada de aplicação do modelo TCP/IP:

21.1.14.2.1. Firewall NGFW com 4,4 Gbps para transferências de dados em aplicações web (http/https), com pacotes de tamanho máximo no protocolo TCP (64 KB);

21.1.14.2.2. 2,3 Gbps para transferências de dados em aplicações web (http/https), com todas as funções de prevenção de ameaças ativadas (antivírus, antimalware, anti-spyware, segurança de DNS, IPS, bloqueio de arquivos etc.);

21.1.14.2.3. 2,5 Gbps para conexões de VPN em aplicações web (http) usando o protocolo IPSec;

21.1.14.3. Suportar pelo menos 1.000.000 (um milhão) de sessões simultâneas;

21.1.14.4. Ser capaz de suportar pelo menos 45.000 (quarenta e cinco mil) novas sessões por segundo, considerando-se para tal novas requisições HTTP de pelo menos 1 byte de tamanho.

21.1.15. **Alta Disponibilidade e balanceamento de carga:**

21.1.15.1. Permitir a configuração dos dois appliances em modo de alta disponibilidade, com suporte mínimo aos seguintes modos de configuração: Ativo-Ativo, Ativo-Passivo e Clusterizado;

21.1.15.2. A alternância entre os dispositivos configurados em modo de alta disponibilidade deve se dar no mínimo pelos seguintes parâmetros de detecção de anomalia:

21.1.15.2.1. Falha de funcionamento do dispositivo;

21.1.15.2.2. Falha de link, seja por falha no tráfego em rotas (path monitoring) quanto por falha no tráfego das suas interfaces (interface monitoring);

21.1.15.3. Deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deverá estar comunicável através da rota. Caso haja falha na comunicação o firewall deverá ter a capacidade de usar rota alternativa para restabelecer a comunicação;

21.1.15.4. Operando em modo de alta disponibilidade, os dispositivos deverão, no mínimo, sincronizar as seguintes informações entre si:

21.1.15.4.1. Sessões;

21.1.15.4.2. Certificados digitais;

21.1.15.4.3. Informações registradas em sua Forwarding information base (FIB);

21.1.15.4.4. Configurações registradas em suas políticas de Firewall, incluindo em seus objetos de rede;

21.1.15.4.5. Possuir administração através de linha de comando através de SSH versão 2 e através de interface Web.

21.1.15.4.6. Políticas de QoS e de VPN;

21.1.15.4.7. Configurações de NAT;

21.1.16. **Virtualização de sistemas:**

21.1.16.1. A solução deve permitir à virtualização lógica de Firewall, ou seja, em um único appliance físico ser possível criar Firewalls NGFW virtualizados;

21.1.16.2. Entende-se como NGFW virtual um conjunto de interfaces físicas e lógicas, que permite a criação e a administração segregada de routers, VLAN's, conexões virtuais e zonas de segurança, com suas próprias regras de acesso administrativo, políticas de segurança, objetos, profiles, filtros e certificados; permitindo assim uma segmentação administrativa que facilita o gerenciamento das políticas de segurança de rede, além de ganhos de escalabilidade sem a necessidade de se adquirir novos appliances físicos para exercer a simples função de segregação de regras de segurança dentro do mesmo domínio de rede;

21.1.16.3. Cada instância virtual deverá suportar, portanto, as mesmas funcionalidades de proteção NGFW oferecidas pelo appliance físico: Firewall, IPS, URL-Filtering, VPN, DNS Security, Threat Prevention (Antivírus, Anti-malware, Anti-Spyware), Controle de Aplicações, QoS, NAT, etc;

21.1.16.4. Cada appliance físico deve possuir um sistema de virtualização lógica que permita a criação de pelo menos 5 instâncias virtuais de Firewall NGFW, sendo que inicialmente cada Firewall NGFW deverá ser licenciado para oferecer a criação de pelo menos 01 (uma) instância virtual, ou seja, uma instância virtual licenciada para cada appliance físico ofertado.

21.1.17. **Segmentação e endereçamento de rede:**

21.1.17.1. Cada dispositivo Firewall NGFW, seja o appliance físico ou sua instância virtualizada, deve permitir as seguintes configurações mínimas de segmentação e endereçamento de rede:

21.1.17.1.1. Ao menos 50 (cinquenta) zonas de segurança;

21.1.17.1.2. Ao menos 10 (dez) roteadores virtuais;

21.1.17.1.3. Permitir a criação de sub-interfaces lógicas Ethernet;

21.1.17.1.4. Suportar a criação de pelo menos 4000 (quatro mil) VLANs (802.1q tags) por dispositivo e por interface;

21.1.17.2. Suportar agregação de links por meio de implementação 802.3ad Link Aggregation e Link Aggregation Control Protocol (LACP);

21.1.17.3. Permitir configuração de balanceamento de link através de, no mínimo, as seguintes opções:

21.1.17.3.1. Por políticas aplicadas a usuário ou grupos de usuários do LDAP/Active Directory;

21.1.17.3.2. Por políticas configuradas por aplicação e porta de destino;

21.1.17.4. Permitir a configuração de interfaces nos seguintes modos:

21.1.17.4.1. Sniffer": Monitoramento e análise de tráfego por espelhamento de porta local (SPAN) ou remota (RSPAN);

21.1.17.4.2. Layer 2 switching, com ou sem utilização de VLAN's;

21.1.17.4.3. Layer 3 routing;

21.1.17.4.4. Modo transparente ou "virtual wire" (interconexão de portas do Firewall NGFW);

21.1.17.4.5. Agrupamento de interfaces (IEEE 802.1AX link aggregation);

21.1.17.4.6. Misto: Mais de um modo de configuração de interface no mesmo appliance físico ou virtual;

21.1.17.5. Permitir o roteamento ou encaminhamento de pacotes baseado em políticas (PBF - Policy Based Forwarding);

21.1.17.6. Implementar recursos de Network Address Translation (NAT) em redes IPv4 e IPv6, incluindo implementação em rede híbrida (NAT64), com suporte mínimo aos seguintes recursos:

21.1.17.6.1. NAT de Origem e de NAT de Destino, configurados isolada ou simultaneamente;

21.1.17.6.2. NAT estático do tipo "One-to-One", bidirecional "One-to-One" e "Many-to-Many";

21.1.17.6.3. NAT dinâmico do tipo "Many-to-One" e "Many-to-Many";

21.1.17.6.4. NAT Overload com tradução de endereço de porta (PAT);

21.1.17.6.5. NAT para interfaces conectadas virtualmente (Virtual Wire), com implementações mínimas de NAT Estático, NAT de Origem e NAT de Destino;

21.1.18. **Serviços adicionais de rede:**

21.1.18.1. Deverá suportar objetos e regras IPV6, com suporte mínimo as seguintes funcionalidades em IPv6: NAT64 ou Dual stack IPv4/IPv6, identificação de usuários a partir do LDAP, incluindo Active Directory, Captive Portal, IPv6 over IPv4 IPSec, OSPFv3; NDP (Neighbor Discovery Protocol); regras de proteção contra DoS (Denial of Service), de-criptografia SSL e SSH, PBF (Policy Based Forwarding), SLAAC (address auto configuration), QoS, DHCPv6 Relay, IPSec, VPN SSL, SNMP, NTP, SYSLOG, DNS, Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicações;

21.1.18.2. Implementar o protocolo DHCP (Dynamic Host Configuration Protocol), podendo atuar como cliente, servidor ou relay do serviço de DHCP;

21.1.18.3. Deverá suportar objetos e regras multicast;

21.1.18.4. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces Layer 3;

21.1.18.5. Deverá suportar o uso da solução em implementações de rede SD-WAN, com utilização de rotas dinâmicas, assim como por meio de seleção de rotas por parâmetros de performance, com suporte mínimo a seleção de rotas por latência, "jitter" e índice de perda de pacotes.

21.1.19. **Quality of Service (QoS):**

21.1.19.1. A solução deve permitir o controle de tráfego por meio de políticas de QoS, ou seja, por meio de controle de uso de largura de banda, de taxa de transferência (throughput), latência e "jitter";

21.1.19.2. Permitir a marcação, inclusive por aplicação, de pacotes DiffServ;

21.1.19.3. Permitir QoS direcionado a interfaces agregadas;

21.1.19.4. Monitorar o uso de banda no tráfego das aplicações, tanto por sessões realizadas quanto por tráfego (bytes transitados);

21.1.19.5. Além de configuração de QoS por interface, a solução deve também permitir, no mínimo, a administração de configurações de QoS por meio de:

21.1.19.5.1. Perfis de QoS (Profiles);

21.1.19.5.2. Políticas de QoS (Policies);

21.1.20. ***Perfis de QoS (Profiles):***

21.1.20.1. Os perfis de QoS devem permitir a definição de valores por classes de QoS típicas, tendo suporte mínimo às seguintes classes QoS:

21.1.20.1.1. Fila de prioridade, com no mínimo 3 valores de prioridade distintos equivalentes às prioridades “baixa, média e alta”;

21.1.20.1.2. Banda garantida, com valores numéricos equivalentes à largura reservada de banda, usualmente registradas em “mbps”;

21.1.20.1.3. Banda máxima, com valores numéricos equivalentes à velocidade máxima reservada de banda, usualmente registradas em “mbps”;

21.1.20.2. Deve permitir a consulta em tempo real de estatísticas das classes QoS definidas na solução;

21.1.20.3. Quando o Firewall NGFW for configurado em modo de virtualização de sistemas, a solução deve permitir a configuração de políticas e perfis de QoS distintos por instância virtual de Firewall;

21.1.21. ***Políticas de QoS (Policies):***

21.1.21.1. Permitir a otimização do consumo de largura de banda por, no mínimo, os seguintes parâmetros de configuração:

21.1.21.1.1. Origem e destino do tráfego, permitindo no mínimo o registro por zona, rede/sub-rede e endereço IP;

21.1.21.1.2. Serviço (Protocolo/porta de acesso);

21.1.21.1.3. Categoria de endereços de URL, incluindo URL’s personalizadas;

21.1.21.1.4. Usuário e grupos de usuários, incluindo por meio de usuários oriundos de controlador de diretório LDAP, em especial por meio do Microsoft Active Directory;

21.1.22. **Recursos adicionais de segurança de rede Firewall:**

21.1.22.1. Permitir a segregação da rede por meio de zonas de segurança (“Firewall Zones”);

21.1.22.2. Proteção contra “spoofing” de endereço IP;

21.1.22.3. Bloqueio de sessões TCP que tentem burlar o padrão de “three-way handshake” do protocolo (“split handshake attacks”);

21.1.22.4. Bloqueio de conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o “three-way handshake”;

21.1.22.5. Bloqueio de tráfego por filtragem de dados, para bloqueio de certas categorias de arquivos, com suporte mínimo aos seguintes tipos de arquivos: exe, bat, cab, dll, pif e reg;

21.1.22.6. Além dos tipos de arquivos citados no item anterior, deve permitir a filtragem baseada em parâmetros customizados pelo administrador da solução, com suporte mínimo a filtragens por extensão de arquivo e por assinatura;

21.1.22.7. Realizar filtragem de arquivos mesmo quando inseridos dentro de um arquivo compactado.

21.1.22.8. **Virtual Private Network - VPN:**

21.1.22.9. A solução deve permitir a criação de túneis virtuais criptografados para acesso a recursos da rede interna da PREVIC por meio de uma rede pública, como a Internet;

21.1.22.10. Suportar pelo menos dois modos de configuração:

21.1.22.10.1. VPN site-to-site, permitindo a criação de túneis entre a rede interna da PREVIC e sítios remotos ou redes locais de outras localidades e órgãos;

21.1.22.10.2. VPN client-to-site, permitindo a conexão individual de usuários à rede interna da PREVIC por meio de dispositivos como computadores, notebooks e smartphones;

21.1.22.11. Para a configuração de VPN site-to-site, a solução deve permitir a criação de túneis mesmo quando a outra ponta utilizar uma solução de segurança Firewall distinta da fornecida, sendo compatível no mínimo com as seguintes soluções de Firewall:

21.1.22.11.1. Palo Alto Networks;

21.1.22.11.2. Fortinet;

21.1.22.11.3. CheckPoint;

21.1.22.11.4. Cisco Systems;

21.1.22.11.5. Juniper Networks;

21.1.22.11.6. SonicWall;

21.1.22.12. Suportar a implementação de VPN por, no mínimo, os seguintes protocolos:

21.1.22.12.1. Security Socket Layer – SSL;

21.1.22.12.2. IP Security Protocol – IPSec;

21.1.22.13. Deverá estar licenciada para suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;

21.1.22.14. Deverá estar licenciada para suportar, no mínimo 1.000 (mil) túneis de VPN IPSEC simultâneos;

21.1.23. **VPN SSL:**

21.1.23.1. O usuário poderá realizar a conexão à rede interna da PREVIC por meio de uma aplicação cliente instalada no sistema operacional do equipamento, ou por meio de interface web por meio de autenticação segura, ou seja, as funcionalidades de VPN SSL deverão ser atendidas com ou sem o uso de um software instalado localmente no dispositivo do usuário (software “agente”);

21.1.23.2. Permitir autenticação de usuário via LDAP, incluindo Microsoft Active Directory, RADIUS, OTP (“One Time Password”), via certificado digital e em base de usuários local;

21.1.23.3. Permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;

21.1.23.4. Permitir atribuição de endereço IP nos clientes remotos de VPN, assim como a atribuição de IP fixos aos usuários remotos de VPN;

21.1.23.5. Permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada, baseada em usuário ou grupo de usuário LDAP/Active Directory;

21.1.23.6. Permitir atribuição de DNS nos clientes remotos de VPN;

21.1.23.7. Permitir que, assim que conectado à VPN, todo o tráfego do usuário remoto seja direcionado para dentro do túnel VPN, impedindo comunicação direta com dispositivos locais e direcionamento de tráfego para soluções de proxy locais;

21.1.23.8. Suportar proxy ARP e uso de interfaces PPPoE;

21.1.23.9. A solução deverá verificar se o cliente que está realizando a conexão é o mesmo para o qual o certificado digital foi inicialmente emitido. Caso a solução identifique alguma anomalia ou não conformidade com o Certificado e o dispositivo associado, o acesso VPN deverá ser imediatamente bloqueado;

21.1.23.10. Deverá manter uma conexão segura com o portal VPN durante toda a sessão;

21.1.23.11. Permitir a associação dos clientes remotos de VPN com políticas de controle de aplicações, IPS, antivírus/antimalware e filtro de URL;

21.1.23.12. O cliente remoto deverá ter a opção de escolher manualmente o Gateway de VPN, ou configurar a seleção do Gateway de forma automática. Quando optar pela seleção automática de Gateway, o agente deverá escolher a melhor rota entre os Gateways disponíveis com base no menor tempo de resposta;

21.1.23.13. Quando utilizada a opção de conexão via aplicação cliente (agente), deve atender aos seguintes requisitos adicionais:

21.1.23.14. Ao estabelecer a conexão SSL, o agente deve se comunicar com o portal de VPN da solução Firewall NGFW para coleta e configuração dos parâmetros de segurança associados ao usuário por meio de políticas de segurança;

21.1.23.15. Permitir o estabelecimento de conexão VPN SSL por, no mínimo, as seguintes formas:

21.1.23.15.1. Antes do usuário autenticar-se (inicialização automática no sistema operacional);

21.1.23.15.2. Após o usuário autenticar-se;

21.1.23.15.3. Sob demanda do usuário;

21.1.23.16. O software cliente deve ser compatível com, no mínimo, os seguintes sistemas operacionais:

21.1.23.16.1. Microsoft Windows, versão igual ou superior a 8.1, plataforma 32 ou 64 bits;

21.1.23.16.2. Linux, com suporte mínimo a distribuições baseadas em RedHat e Debian, com ou sem interface gráfica instalada;

21.1.23.16.3. MacOS, versão igual ou superior a 10.15;

21.1.23.16.4. Sistemas operacionais para smartphones, com suporte mínimo a iOS e Android, por meio de download e instalação pelas respectivas plataformas de distribuição de Apps (Apple Store; Google Store);

21.1.24. **VPN IPSec:**

21.1.24.1. Deverá suportar a implementação de VPN IPSec com uso de diferentes algoritmos de autenticação e encriptação, com suporte mínimo aos seguintes algoritmos:

21.1.24.1.1. Data Encryption Standard (DES) de 56 bits;

21.1.24.1.2. Triple Data Encryption Standard (3DES) de 112 bits;

21.1.24.1.3. Advanced Encryption Standard (AES), com suporte mínimo a Cipher Block Chaining (CBC) de 128, 192 ou 256 bits, Counter with CBC-MAC (CCM) de 128 bits e Galois/Counter Mode (GCM) de 128 ou 256 bits;

21.1.24.1.4. MD5;

21.1.24.1.5. SHA-1, SHA-256, SHA-384 e SHA-512;

21.1.24.1.6. Diffie-Hellman Group 1, Group 2, Group 5; Group 14; Group 19 e Group 20;

21.1.24.1.7. Internet Key Exchange (IKEv1 e v2);

21.1.24.2. Permitir a criação de VPN IPSec site-to-site tanto em modo padrão, com um único túnel VPN conectando-se a um único site remoto, quanto em modo “multisites”, com conexão VPN simultânea a dois ou mais sites remotos;

21.1.24.3. Permitir a criação de VPN IPSec site-to-site nas seguintes implementações mínimas:

21.1.24.3.1. Roteamento estático;

21.1.24.3.2. Roteamento dinâmico via protocolo Open Shortest Path First (OSPF);

21.1.24.3.3. Roteamento estático e dinâmico (em conjunto);

21.1.24.4. Permitir o monitoramento de falhas de conexão em túneis IPSec, incluindo em seu Gateway IKE e em sua interface, com suporte a ações automáticas em caso de falha em um dos peers de VPN, identificadas por meio de parâmetros configuráveis de threshold de resposta, com no mínimo o suporte às seguintes ações automáticas:

21.1.24.4.1. Aguardar a recuperação do túnel até um determinado tempo;

21.1.24.4.2. Rotear o tráfego para um caminho alternativo, desabilitando o túnel que não estiver respondendo.

21.1.24.4.3. **Políticas de segurança:**

21.1.24.5. Deve permitir a configuração de parâmetros de segurança de rede por meio de políticas (“Policies”), que podem ser configuradas por meio de diversos parâmetros e atributos;

21.1.24.6. Cada política deve ter um “label” identificador único, permitindo o uso de um nome com até pelo menos 60 (sessenta) caracteres alfanuméricos;

21.1.24.7. Além do “label” identificador, deve conter um ou mais campos de informações complementares adicionais, que auxiliam na identificação da política e de suas principais características, contendo no mínimo a possibilidade de usar um campo do tipo “descrição”, com tamanho de até pelo menos 1024 (mil e vinte e quatro) caracteres;

21.1.24.8. Possuir um campo específico para registro de “palavra-chave” ou “tag-words”, que possa ser utilizada para filtragem rápida e identificação das políticas de segurança;

21.1.24.9. Deve permitir a configuração do tipo de ação a ser realizada pelo Firewall, tendo no mínimo as seguintes opções de ação:

21.1.24.9.1. Permitir o tráfego (“Allow” ou “Release”);

21.1.24.9.2. Negar o tráfego (“Deny” ou “Block”);

21.1.24.9.3. Descartar o pacote TCP (“Drop”), sem negação explícita do tráfego;

21.1.24.9.4. Reiniciar o tráfego (“Reset”), no mínimo permitindo o reset no lado cliente, no lado servidor ou em ambos;

21.1.24.10. Cada política deve permitir a configuração personalizada de recursos como nível de auditoria (logging) e parâmetros de Quality of Service (QoS);

21.1.24.11. Cada política deve permitir a sua ativação e desativação baseada em um calendário de operação (“schedules”);

21.1.24.12. Cada política deve permitir sua classificação quanto às zonas de segurança estabelecidas, permitindo no mínimo a seguinte classificação:

21.1.24.12.1. Política do tipo “global”: As regras deste tipo de política podem ser utilizadas por quaisquer das zonas de segurança especificadas, tanto para tráfego interno (“interzone traffic”) quanto para tráfego entre zonas distintas (zonas de origem e de destino do tráfego);

21.1.24.12.2. Política do tipo “Interna”: Suas regras só se aplicam ao tráfego que transita dentro das zonas especificadas como sendo “zona de origem”;

21.1.24.12.3. Política do tipo “Externa”: Suas regras só se aplicam ao tráfego que transita entre as zonas de origem e de destino, porém não entre o tráfego interno de cada zona;

21.1.24.13. Deve permitir a configuração de parâmetros de “Zona de Origem” e “Zona de Destino”, permitindo inclusive apontar como Zona de Destino um endereço NAT, e permitindo também apontar mais de uma zona como sendo de origem ou destino da política de segurança;

21.1.24.14. Deve permitir estabelecer a origem e o destino do tráfego por outros parâmetros além de zonas de segurança, tendo suporte mínimo aos seguintes parâmetros de origem e destino:

21.1.24.14.1. Por número IP;

21.1.24.14.2. Por hostname e domínio (FQDN);

21.1.24.14.3. Por sub-rede;

21.1.24.14.4. Por grupos previamente criados na solução Firewall NGFW;

21.1.24.14.5. Por país ou região geográfica;

21.1.24.15. Deve permitir a seleção do serviço de Camada 4 ao qual a política se aplica, podendo o campo ser configurado tanto por meio da definição explícita do número da porta UDP ou TCP, quanto por meio da seleção de categorias de serviço disponibilizadas pelo sistema operacional do Firewall NGFW (i.e.: HTTP; DNS; FTP; etc.);

21.1.24.16. Deve permitir estabelecer a qual usuário, ou grupo de usuários, a política de segurança se aplica, permitindo a integração da identificação desses usuários por meio de controlador de domínio externo LDAP, como o Microsoft Active Directory;

21.1.24.17. Deve permitir a configuração da aplicação para a qual a política será aplicada, por meio de recurso avançado de controle de aplicações, recurso específico descrito mais detalhadamente no "Controle avançado de aplicações" deste Termo de Referência;

21.1.24.18. Deve permitir a configuração de categoria de URL para a qual as regras da política de segurança serão aplicadas;

21.1.24.19. Deve possuir no mínimo um campo para associação da política a perfis de segurança previamente cadastrados, que facilitam a aplicação de políticas de controle de acesso e prevenção de vazamento de dados;

21.1.25. **Políticas de segurança baseadas em objetos dinâmicos:**

21.1.26. Além da configuração de parâmetros estáticos nas políticas de segurança, a solução deve permitir a criação de objetos dinâmicos, permitindo uma configuração mais flexível das políticas de segurança;

21.1.27. Entende-se por objetos dinâmicos o agrupamento de informações identificadas unicamente dentro da solução, que podem ser utilizados como parâmetros de configuração das políticas de segurança, e que permitam a inclusão e a exclusão automática de seus elementos internos, baseada em parâmetros configuráveis pelo administrador da solução;

21.1.28. Os objetos dinâmicos devem permitir o agrupamento mínimo dos seguintes itens de configuração:

21.1.28.0.1. Endereços IP (IPv4 e IPv6);

21.1.28.0.2. Agrupamento de endereços IP (IPv4 e IPv6), como ranges de IP ou sub-redes (VLAN’s);

21.1.28.0.3. Lista dinâmica de endereços IP;

21.1.28.0.4. Hostnames, domínios e URL’s (FQDN);

21.1.28.0.5. Região do planeta, permitindo no mínimo a seleção por país ou por coordenada (latitude e longitude);

21.1.28.0.6. Usuários e grupos de usuários, tanto de uma lista interna da solução quanto de uma fonte externa de consulta, como LDAP e Active Directory;

21.1.28.0.7. Aplicações e grupo de aplicações, com possibilidade de criação de filtros dinâmicos com base em atributos de aplicação, tais como “categoria”, “plataforma tecnológica” etc;

21.1.28.0.8. Serviços e grupos de serviço, por meio de parâmetros de Camada 4, como protocolo TCP/UDP e porta de acesso;

21.1.29. **Consulta à bases externas para criação de objetos dinâmicos**

21.1.29.1. Permitir a criação de objetos dinâmicos com base em informações obtidas em consultas a fontes externas de endereços IP, domínios, URLs e soluções de administração de usuários e grupos de usuários;

21.1.29.2. Deverá permitir a autenticação segura através de certificado digital a essas fontes externas de informação;

21.1.29.3. Deverá permitir consultar e criar exceções para informações oriundas de listas externas a partir da interface de gerência do próprio Firewall NGFW;

21.1.30. **Controle avançado de aplicações:**

21.1.30.1. Capacidade de identificar aplicações sem depender unicamente do conjunto formado por parâmetros básicos de configuração de rede, como porta, protocolo e método de encriptação, utilizando-se de outros mecanismos de identificação, como por meio de análise comportamental e de contexto de utilização da aplicação, permitindo tanto a liberação quanto o bloqueio do tráfego da aplicação sem a necessidade de se realizar este procedimento por meio de mudanças nas configurações de porta e protocolo de comunicação;

21.1.30.2. A identificação da aplicação deverá se dar por múltiplos mecanismos, não somente por um único mecanismo isolado;

21.1.30.3. Deve ser capaz de reconhecer aplicações em tráfego sob o protocolo IPv6;

21.1.30.4. Permitir a configuração de limite de banda (QoS) usada por aplicações, baseado no IP de origem, tanto de download quanto de upload;

21.1.30.5. Permitir que o controle de portas seja aplicado para todas as aplicações;

21.1.30.6. Quando da identificação de tentativa de uso de uma aplicação bloqueada, a solução deve permitir a ativação de mensagem de alerta ao usuário final;

21.1.30.7. Deve possuir uma sólida base de assinaturas de aplicações, com registro de propriedades únicas da aplicação, que deverá ser periodicamente atualizada de forma automática durante todo o período de licenciamento da solução;

21.1.30.8. Deve inspecionar o payload de pacote de dados e detectar assinaturas de aplicações, verificando se a aplicação está utilizando seus parâmetros padrões de configuração, como porta e protocolo de comunicação;

21.1.30.9. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações;

21.1.30.10. Capacidade de decodificação de protocolos conhecidos, com o objetivo de detectar aplicações encapsuladas dentro do protocolo originalmente identificado, validando se o tráfego encapsulado corresponde com sua especificação. A decodificação de protocolo também deverá identificar funcionalidades específicas dentro de uma aplicação, além de detectar arquivos e outros conteúdos que deverão ser inspecionados de acordo as regras de segurança implementadas;

21.1.30.11. Capacidade de identificar o uso de táticas evasivas que visam mascarar o comportamento e o tráfego de dados de uma aplicação por meio de uso de técnicas avançadas como NAT-T e “pinholes” em protocolos como FTP e SIP;

21.1.30.12. Capacidade de identificar o uso de táticas evasivas que visam mascarar o comportamento e o tráfego de dados de uma aplicação por meio de técnicas de análise heurística e comportamental;

21.1.30.13. Além do controle sobre aplicações conhecidas, a solução deverá possuir mecanismos de controle sobre aplicações desconhecidas ou personalizadas;

21.1.30.14. Permitir a criação de assinaturas personalizadas para aplicações proprietárias, sem necessidade de interferência ou validação externa por parte da fabricante da solução Firewall NGFW, permitindo também aos administradores da solução que façam uma solicitação ao fabricante para inclusão dessas aplicações na base de assinaturas de aplicações;

21.1.30.15. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, regras de contexto (sessões ou transações), posição no payload dos pacotes TCP/UDP e uso de decoders para pelo menos os seguintes protocolos: HTTP, FTP, SMB, SMTP, Telnet, SSH, MSSQL, IMAP, IMAP, MS-RPC, RTSP e File body;

21.1.30.16. Permitir a criação de grupos de aplicações, estáticos ou dinâmicos;

21.1.30.17. Para grupos de aplicações do tipo dinâmico, a inclusão e exclusão dinâmica da aplicação no grupo deverá ser realizada por meio de características das aplicações, configuráveis pelo operador da solução, sendo exigido no mínimo a configuração por meio dos seguintes parâmetros:

21.1.30.17.1. Nível de risco;

21.1.30.17.2. Categoria e subcategoria;

21.1.30.17.3. Tecnologia utilizada na aplicação (se é “cliente-servidor”, aplicação web, protocolo de rede utilizado etc.);

21.1.30.17.4. Características típicas de uso de malware ou uso de técnicas evasivas, tais como uso excessivo de banda, transferência intensiva ou constante de arquivos, etc;

21.1.30.18. A interface gráfica de configuração das regras de controle avançado de aplicações deverá permitir a aplicação de filtros na tabela de regras de segurança, permitindo a identificação de anomalias ou falhas na configuração das regras de segurança, tais como:

21.1.30.18.1. Regras de segurança, ou aplicações que foram incluídas dentro de regras de segurança, em que não houve passagem de tráfego nos últimos dias ou semanas, com range de alcance de pelo menos 90 dias antecessores à data de pesquisa;

21.1.30.18.2. Regras que permitem a passagem de tráfego baseado em porta/protocolo, e não por regras avançadas de identificação de aplicação, permitindo filtrar quais aplicações estão trafegando, e o respectivo volume trafegado por cada a aplicação por, pelo menos, os últimos 30 dias antecessores à data da pesquisa;

21.1.31. **Controle por meio de identificação de usuários:**

21.1.31.1. Permitir a utilização de políticas de segurança baseadas em usuários e grupos de usuários, com visibilidade e controle de quem está usando os recursos de rede, incluindo aplicações;

21.1.31.2. Quanto a soluções externas de autenticação de usuários, a função de controle por meio de identificação de usuários deve ter compatibilidade mínima com as seguintes tecnologias ou protocolos de autenticação: Controladores de domínio Active Directory com nível funcional acima da versão 2012 R2; LDAP; Kerberos e RADIUS;

21.1.31.3. Também deve ser possível realizar autenticação em soluções de rede sem fio, através de “Captive Portal”, além de autenticação em base local de usuário, alocada na própria solução Firewall NGFW;

21.1.31.4. Quanto à integração com o serviço de controlador de domínio presente no ambiente da PREVIC – Microsoft Active Directory, a solução deve permitir o aproveitamento da sua estrutura de grupos de usuários para associação às políticas de segurança;

21.1.31.5. Permitir a criação de grupos customizados de usuários no Firewall NGFW, baseado em atributos coletados do LDAP/Active Directory;

21.1.31.6. Permitir a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, em especial em servidores Microsoft Windows via *Microsoft Terminal Server*;

21.1.31.7. Permitir que se configure, sem necessidade de instalação de software cliente, um “Captive Portal” com autenticação (usuário e senha), para controle do acesso à internet realizado de dentro da rede PREVIC, em equipamentos que não estejam registrados no controlador de domínio, como por exemplo, usuários com dispositivos móveis que se conectarem à rede sem fio da PREVIC;

21.1.31.8. Permitir configuração de políticas de segurança por meio de identificação de usuários através de leitura de campo em HTTP do tipo “x-forwarded-for” (XFF). Ao se configurar este tipo de recurso, a solução deve registrar nos logs do Firewall NGFW o endereço IP, bem como o usuário de rede responsável pelo acesso;

21.1.32. **Filtro de conteúdo web (URL Filtering):**

21.1.32.1. Solução que permita o controle e monitoramento do acesso a sítios de internet por parte dos usuários clientes da rede PREVIC;

21.1.32.2. Deve funcionar de forma integrada às demais funcionalidades da solução Firewall NGFW, incluindo a de controle avançado de aplicações e, em especial, ao controle por meio de identificação de usuários, descrita no subitem **21.2** deste Termo de Referência, permitindo a integração de base de controle de usuários externas, como LDAP/Active Directory, E-Directory, assim como através de base de repositório de usuários local da solução;

21.1.32.3. Quando da integração com controle de diretório de usuários externo, os logs de acesso aos sites coletados pela solução devem registrar a identificação do usuário de rede, permitindo a consulta integrada dos acessos entre o repositório externo de usuários e os logs da solução Firewall NGFW;

21.1.32.4. Capacidade de criação de políticas de filtro de conteúdo web baseadas em diferentes parâmetros, com suporte mínimo aos seguintes itens de parametrização:

21.1.32.4.1. Usuários e grupo de usuários;

21.1.32.4.2. Zona de segurança;

21.1.32.4.3. Rede e sub-redes;

21.1.32.4.4. Endereços IP;

21.1.32.4.5. Por URL;

21.1.32.4.6. Categoria de URL;

21.1.32.5. Possuir o recurso de configuração de período de execução da política, permitindo estabelecer dias e faixas de horários específicas em que a política de filtragem de URL esteja habilitada ou desabilitada no ambiente;

21.1.32.6. A página de bloqueio padrão da solução deve ser customizada, permitindo, por exemplo, a inserção do logotipo da PREVIC e registro de instruções para abertura de chamados para eventual liberação de site bloqueado;

21.1.32.7. Possuir funcionalidade “anti-phishing” integrada ao filtro de conteúdo web, permitindo o bloqueio de acesso a sites caso o usuário tente fazer o envio de suas credenciais em sites classificados como “phishing” pela solução;

21.1.32.8. Analisar se no navegador do usuário está ativa a função de busca segura (“safe search”) e, caso não esteja habilitada, realizar o bloqueio de acesso aos sites buscadores, como Google, Bing, etc. Na página de bloqueio, deverá permitir inserir instruções ao usuário sobre como habilitar a função de busca segura em seu navegador ou sistema operacional;

21.1.32.9. O mecanismo validador de URL deve prioritariamente consultar uma base de URLs local, armazenada no disco rígido do appliance físico, optando pela consulta online (“cloud”) quando a base local estiver desatualizada, inabilitada ou a URL consultada não possuir registro na base local do appliance;

21.1.32.10. Permitir a liberação de URLs bloqueadas (“white list”), incluindo a exclusão do bloqueio por categoria de URL;

21.1.32.11. Permitir a exibição de página de alerta para acesso a sites listados em “blacklists” de URLs, mas que não estejam explicitamente bloqueados pelo filtro URL da solução, possibilitando que o usuário acesse um site potencialmente arriscado clicando num botão do tipo "Continuar" ou “Avançar”;

21.1.32.12. Permitir a concessão provisória de acesso a determinados sites que estiverem bloqueados, através de aplicação de um nível adicional de segurança, por meio de autenticação por senha adicional concedida pela equipe de suporte técnico, por exemplo;

21.1.32.13. Permitir salvar nos logs de acesso informações de cabeçalho HTTP, com suporte mínimo aos seguintes campos: UserAgent, Referer, e X-Forwarded-For (XFF);

21.1.32.14. Permitir a classificação de nível de risco de URLs, com suporte mínimo a três níveis de risco aplicáveis, equivalentes aos riscos de nível “baixo”, “médio” e “alto”;

21.1.32.15. A categorização de sites deve permitir a associação da URL a mais de uma única categoria, assim como o uso de caracteres coringas (“Wildcards”);

21.1.32.16. Permitir a criação de categorias de URLs customizadas;

21.1.32.17. Permitir o uso de listas dinâmicas de categorias de URLs, incluindo listas dinâmicas externas;

21.1.32.18. Ao categorizar um site, a análise da filtragem de URL não deve se limitar apenas ao nível de diretório, realizando a análise em toda a extensão da URL registrada;

21.1.32.19. Permitir a criação e o uso de categorias de exceção, ou seja, categorias que permitem a aplicação de regras de exceção para, por exemplo, liberar o acesso a determinado site enquadrado em categoria bloqueada por uma determinada política de filtragem de URL (“override policy”);

21.1.32.20. As categorias de URL, incluindo as categorias customizadas, devem podem ser reaproveitadas em outros módulos da solução Firewall NGFW, permitindo, por exemplo, que se crie uma política de QoS que se aplique a uma determinada categoria de URL;

21.1.33. **Segurança em tráfego criptografado:**

21.1.33.1. Quanto à segurança em tráfego criptografado, a solução deve permitir, no mínimo:

21.1.33.2. O controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e de saída (Outbound);

21.1.33.3. O “offload” de certificado em inspeção de conexões SSL de entrada (Inbound);

21.1.33.4. De-criptografar o tráfego Inbound e Outbound em conexões negociadas com TLS v 1.3 ou superior;

21.1.33.5. Inspeção e de-criptografia de SSH com base em políticas de segurança;

21.1.33.6. A de-criptografia de SSH deverá possibilitar a identificação e o bloqueio de tráfego, caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança;

21.1.33.7. De-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

21.1.33.8. Deverá permitir o espelhamento de tráfego de-criptografado (SSL e TLS) para análise por meio de soluções externas de segurança, como por exemplo, soluções de análise forense de rede, ferramentas de auditoria, Data Loss Prevention, etc.

21.1.34. **Proteção contra ameaças:**

21.1.34.1. Trata-se de um conjunto de ferramentas para prevenção e proteção contra ameaças, integradas ao Firewall, com recursos mínimos de:

21.1.34.1.1. Antivírus e antimalware;

21.1.34.1.2. Anti-spyware;

21.1.34.1.3. Sistema de prevenção de intrusão (IPS);

21.1.34.2. Capacidade para identificação e bloqueio de ameaças típicas, como vírus, trojans, spywares, ransomwares e demais tipos de malwares;

21.1.34.3. Permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

21.1.34.4. Permitir ativar ou desativar as assinaturas, incluindo a opção de habilitá-las apenas em modo de monitoramento;

21.1.34.5. Quando a solução de Firewall NGFW for implementada em regime de alta disponibilidade em modo ativo/passivo, ela deverá sincronizar automaticamente as assinaturas de IPS, Antivírus/Anti-Spyware entre os dispositivos;

21.1.34.6. Permitir configurar as ações a serem tomadas pela solução quando uma ameaça for detectada, com suporte mínimo as seguintes ações:

21.1.34.6.1. Permitir a ameaça;

21.1.34.6.2. Permitir a ameaça com geração obrigatória de logs;

21.1.34.6.3. Bloquear a ameaça;

21.1.34.6.4. Bloquear o endereço IP do atacante por um intervalo de tempo específico;

21.1.34.6.5. Enviar TCP-Reset ao atacante;

21.1.34.7. Permitir criar exceções por IP de origem ou de destino, assim como exceções por assinatura;

21.1.34.8. Permitir a criação de diferentes políticas com suporte mínimo aos seguintes parâmetros de configuração, podendo ser configurados em conjunto:

21.1.34.8.1. Zona de segurança;

21.1.34.8.2. Endereço de origem;

21.1.34.8.3. Endereço de destino;

21.1.34.8.4. Serviço (protocolo/porta);

21.1.34.8.5. Usuários e Grupo de usuários;

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

21.1.34.10. Proteção contra vírus em conteúdo HTML e Javascript, software espião (spyware) e worms;

21.1.34.11. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos;

21.1.34.12. Detectar e prevenir ameaças em tráfegos HTTP/2;

21.1.34.13. Permitir o bloqueio por tipo de arquivos, tais como .src; .bat; .exe;

21.1.34.14. Rastreamento de vírus em arquivos PDF e em arquivos comprimidos com algoritmo deflate (i.e.: .zip; .gzip);

21.1.34.15. Possuir o recurso de bloqueio de vulnerabilidades, incluindo bloqueio de vulnerabilidade em softwares conhecidos (exploit);

21.1.34.16. Possuir o recurso de identificação e bloqueio de comunicação com “botnets”;

21.1.34.17. Possuir recurso de proteção contra ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

21.1.34.18. Possuir recurso de proteção contra ataques de negação de serviços (DoS), incluindo o uso de assinaturas específicas para a mitigação de ataques desta natureza;

21.1.34.19. Possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6) previamente definidos;

21.1.34.20. Ser capaz de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain generation algorithm - DGA), com registro em logs de, no mínimo, as seguintes informações:

21.1.34.20.1. Domínio identificado;

21.1.34.20.2. ID de assinatura de detecção;

21.1.34.20.3. Login do usuário logado na estação/servidor que originou o tráfego;

21.1.34.20.4. Aplicação e porta de destino;

21.1.34.20.5. IP de origem e de destino;

21.1.34.20.6. Horário da detecção (timestamp);

21.1.34.20.7. Grau de severidade atribuída pela solução;

21.1.34.20.8. Ação tomada pela solução;

21.1.34.21. Possuir sistema de análise automática para detecção e bloqueio de encapsulamento de DNS com finalidade de roubo de dados ou comunicação de comando e controle, com suporte mínimo a detecção por:

21.1.34.21.1. Padrão de consulta;

21.1.34.21.2. Taxa de consultas;

21.1.34.21.3. Análise estatística de frequência de domínios (n-grama);

21.1.34.21.4. Entropia;

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

21.1.34.23. Possibilitar a criação de assinaturas customizadas, sem a necessidade de codificação, ou seja, por meio da própria interface gráfica da solução;

21.1.34.24. Permitir o uso de operadores de negação na criação de assinaturas customizadas de IPS e anti-malware/spyware, permitindo a criação de exceções de varredura e detecção;

21.1.34.25. Realizar inspeção de IPS baseado em diferentes modalidades de análise, com suporte mínimo à:

21.1.34.25.1. IP Defragmentation;

21.1.34.25.2. Bloqueio de pacotes malformados;

21.1.34.25.3. Remontagem de pacotes de TCP;

21.1.34.25.4. Detecção de anomalias de protocolo;

21.1.34.25.5. Decodificação de protocolo;

21.1.34.25.6. Padrões de estado de conexões;

21.1.34.25.7. Análise heurística;

21.1.34.26. Suportar técnicas de prevenção para pacotes TCP/IP, permitindo configurar ações como “drop” e “Tcp-reset” (Cliente, Servidor e ambos);

21.1.34.27. Suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;

21.1.34.28. Permitir que, na captura de pacotes por assinaturas de IPS e Antispyware, seja definido o número de pacotes a serem capturados, com possibilidade de seleção de, no mínimo, 50 pacotes;

21.1.34.29. Suportar referência cruzada com CVE;

21.1.34.30. Possuir recursos para impedir ataques de flood de tráfego de rede, tais como Synflood, ICMPflood, UDPflood, etc;

21.1.34.31. Ser capaz de detectar e bloquear a origem de port scans, com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento, como Zabbix e Grafana;

21.1.34.32. Deverá registrar na console de monitoramento da solução informações básicas sobre ameaças identificadas, com no mínimo os seguintes campos de informação:

21.1.34.32.1. O nome da assinatura ou do ataque;

21.1.34.32.2. Aplicação;

21.1.34.32.3. Usuário;

21.1.34.32.4. Origem e o destino da comunicação

21.1.34.32.5. Ação tomada pela solução;

21.1.35. **Detecção e tratamento para malwares desconhecidos (“zero day”):**

21.1.35.1. Ser capaz de detectar e analisar malwares desconhecidos, ou seja, que não estejam na base de registro de assinaturas da solução, utilizando-se para tal de recursos avançados, como o uso de “Sandbox” para isolamento e tratamento da ameaça;

21.1.35.2. Monitorar os arquivos trafegados na internet em protocolos como HTTP; HTTPs, FTP e SMTP;

21.1.35.3. Monitorar os arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e Layer3;

21.1.35.4. Ser capaz de detectar e analisar arquivos suspeitos em ambiente Sandbox simulando, o mínimo, os sistemas operacionais Windows, versão 8 ou superior;

21.1.35.5. Realizar o envio automático de arquivos trafegados na rede PREVIC para análise Sandbox, onde o arquivo será executado e simulado em ambiente controlado;

21.1.35.6. Permitir o envio para análise em Sandbox de malwares bloqueados pelo antivírus da solução;

21.1.35.7. A seleção dos arquivos para envio para análise deverá se dar por meio políticas granulares de segurança, considerando-se parâmetros típicos da solução Firewall NGFW, como endereço IP de origem/destino, usuário/grupo de usuários, aplicação, protocolo/porta, URL e categoria de URL, tipo de arquivo;

21.1.35.8. Diferenciar os arquivos analisados em pelo menos três categorias:

21.1.35.8.1. Malicioso;

21.1.35.8.2. Não malicioso;

21.1.35.8.3. Não maliciosos, mas com características indesejáveis;

21.1.35.9. Entende-se como “não maliciosos, mas com características indesejáveis”; softwares que causem problemas de performance em dispositivos, tais como lentidão na execução do sistema operacional, ou que alterem parâmetros de sistema, como alterações no registro do Windows;

21.1.35.10. Suportar a análise Sandbox de arquivos executáveis, DLLs, compactados (.zip, .rar, .7-zip etc.) e criptografados em tráfego SSL;

21.1.35.11. Suportar a análise Sandbox de arquivos do pacote Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class), e arquivos do sistema operacional Android;

21.1.35.12. Capacidade de análise de links em Sandbox, com registro posterior na base de filtro de URL da solução, caso o link analisado em Sandbox for classificado em categorias maliciosas, como “phishing”;

21.1.35.13. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API;

21.1.35.14. Permitir exportar, a partir da própria console de gerenciamento da solução, o resultado das análises de malwares do tipo “Zero Day” em arquivo tabulado, como .txt; .csv ou .pdf;

21.1.36. **Autenticação de usuários**

21.1.36.1. Permitir a autenticação de usuários tanto por meio de unidade autenticadora interna quanto por meio de soluções de autenticação externa à solução Firewall NGFW;

21.1.36.2. A autenticação local da solução deve permitir a organização das contas de acesso por meio de grupos e níveis de acesso, além de permitir a configuração de complexidade de senhas e sua data de expiração;

21.1.36.3. Quanto a soluções externas de autenticação de usuários, a solução deve ter compatibilidade mínima com as seguintes tecnologias ou protocolos de autenticação:

21.1.36.4. Controladores de domínio Active Directory com nível funcional acima da versão 2012 R2;

21.1.36.4.1. LDAP;

21.1.36.4.2. Kerberos;

21.1.36.4.3. RADIUS e TACACS+;

21.1.36.5. Permitir a integração com soluções de autenticação de usuários com múltiplos fatores de autenticação (“Multi-Factor Authentication”) e com soluções do tipo “single sign-on” (SSO) e “single logout” (SLO);

21.1.36.6. Permitir a integração com aplicações que se utilizam de solução de provisão de identidade por meio da linguagem de marcação Security Assertion Markup Language (SAML);

21.1.36.7. Deverá permitir autenticação centralizada, tanto da rede cabeada como da rede sem fio, utilizando-se da base LDAP existente;

21.1.37. **Monitoramento por LED’s indicadores**

21.1.37.1. O appliance físico deve possuir LED's indicadores de status em sua parte frontal, permitindo a verificação in loco dos seguintes parâmetros básicos:

21.1.37.1.1. *Status de energização*: com no mínimo a informação de que o equipamento está ligado (energizado) ou não (Power on/off)

21.1.37.1.2. *Status operacional*: Com no mínimo a indicação de dois status: O dispositivo está pronto para uso e o dispositivo está em processo de inicialização;

21.1.37.1.3. *Temperatura*: Com no mínimo a informação de que o appliance está sob condições de temperatura normal ou está operando em condições anormais de temperatura;

21.1.37.1.4. *Falha de componentes*: Pelo menos um LED indicador que deve ser acionado quando um ou mais dos principais componentes de hardware estão com falha de funcionamento. Os componentes mínimos que deverão ser monitorados por este LED são: Fontes de alimentação de energia; disco rígido; módulo de ventoinhas de refrigeração (Fans) e modo de alta disponibilidade com falha;

21.1.37.1.5. *Alta Disponibilidade*: Pelo menos um LED que monitore o status e o papel do *appliance* quando ele faz parte de uma solução configurada em modo de alta disponibilidade, exibindo no mínimo os seguintes indicadores: Modo ativo; Modo passivo; sem alta disponibilidade ativada;

21.1.37.2. Cada interface de rede, seja Ethernet ou SFP/SFP+, também deve possuir seu respectivo LED indicador de atividade, exibindo no mínimo as seguintes informações:

21.1.37.2.1. *LED ligado: interface conectada a um link de rede;*

21.1.37.2.2. *LEDs piscando intermitentemente: Indica atividade de tráfego na respectiva interface;*

21.1.37.3. Devem também estar disponíveis LED's indicadores de status para, no mínimo, os seguintes componentes, podendo ser disponibilizados na parte traseira do dispositivo:

21.1.37.4. *Fontes de alimentação: LED's indicando no mínimo os seguintes status:*

21.1.37.4.1. Não há alimentação de energia ou há sobrecarga/subcarga;

21.1.37.4.2. A voltagem de input está operando dentro da margem esperada;

21.1.37.4.3. A voltagem de input está operando abaixo ou acima da margem esperada;

21.1.37.4.4. A saída de energia da fonte está operando normalmente;

21.1.37.4.5. A fonte está operando em modo standby (para fonte redundante);

21.1.37.4.6. A fonte de energia está com problemas para alimentar o dispositivo;

21.1.37.5. *Ventoinhas de refrigeração: LED deve indicar se as ventoinhas estão operando normalmente ou se há falhas de funcionamento*;

21.1.38. **Gerenciamento Remoto da solução:**

21.1.38.1. A solução deve ser fornecida com software de gerenciamento remoto via interface gráfica, com capacidade para gerenciar os dois appliances físicos adquiridos neste processo, que estarão configurados em modo de alta disponibilidade, além de permitir a configuração e gerenciamento de suas instâncias virtuais;

21.1.38.2. A ferramenta de gerenciamento remoto deve ser fornecida com a integralidade de suas funções habilitadas, sem necessidade de aquisição posterior de licenças de software adicionais;

21.1.38.3. O gerenciamento remoto da solução de ser acessível via autenticação de usuário, com suporte mínimo a:

21.1.38.3.1. Autenticação local com SSL;

21.1.38.3.2. Autenticação local com SSH;

21.1.38.3.3. Autenticação externa via LDAP, em especial por integração com Active Directory;

21.1.38.3.4. Autenticação externa via Kerberos; TACACS+ e RADIUS;

21.1.38.3.5. Autenticação externa via serviço de múltiplo fator de autenticação, incluindo aplicações que se utilizam de provedor de identidade SAML;

21.1.38.4. Deve permitir a configuração de múltiplos perfis de acesso para administração da solução, segregados por papéis, com suporte mínimo equivalentes aos seguintes papéis:

21.1.38.4.1. Administrador Total: Função de "super usuário", possui acesso total às funcionalidades da solução, incluindo a função de gestão de acesso a usuários;

21.1.38.4.2. Administrador de Instância: Pode gerenciar todas as funcionalidades de uma instância física ou virtual de NGFW, mas não tem permissão para gerenciar a solução NGFW como um todo;

21.1.38.4.3. Monitoramento: Acesso restrito para os módulos de visualização e monitoramento da solução, não tendo permissão para editar configurações e políticas;

21.1.38.4.4. Monitoramento Granular: Similar ao perfil anterior, possuindo acesso somente aos módulos que o administrador selecionar;

21.1.38.4.5. Operação: Permite editar as configurações dos diversos módulos e políticas de segurança;

21.1.38.4.6. Operação Granular: Similar ao perfil anterior, possuindo acesso de edição somente aos módulos que o administrador selecionar;

21.1.38.4.7. Gestor de Acesso: Perfil a quem é dada a permissão de conceder, modificar e revogar o acesso a outros usuários da solução;

21.1.38.5. Deverá permitir o acesso concorrente de diversos usuários, incluindo usuários com papel de administrador e operador, que poderão realizar edições de configurações e políticas simultaneamente. Caso haja mais de uma mudança de configuração sendo realizada ao mesmo tempo, o usuário com perfil de administração poderá selecionar qual modificação será aplicada;

21.1.38.6. Deverá permitir o bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores da solução;

21.1.38.7. Aos usuários com papel de administrador da solução deve ser disponibilizada a consulta dos registros de acesso, onde ficarão armazenadas as informações básicas de acesso à solução, como identificação do usuário e data e hora do acesso, incluindo tentativas de acesso que apresentaram falha;

21.1.38.8. A ferramenta deve permitir o monitoramento, configuração e operação dos recursos oferecidos pelo equipamento, através de uma interface gráfica intuitiva;

21.1.38.9. Deverá ser possível acessar o equipamento e aplicar configurações durante momentos em que o tráfego for muito alto e a CPU e memória do equipamento estiverem sendo excessivamente utilizadas;

21.1.38.10. Deve informar em tempo real o status dos appliances físicos e instâncias virtuais, incluindo no mínimo os seguintes parâmetros:

21.1.38.10.1. Uso de CPU;

21.1.38.10.2. Status das interfaces de rede;

21.1.38.10.3. Status dos links monitorados para alta disponibilidade;

21.1.38.10.4. Número de sessões simultâneas;

21.1.38.11. A interface gráfica de gerenciamento deve ser preferencialmente do tipo “web GUI”, ou seja, acessível por meio de um navegador usual de internet (browser), sem a necessidade de instalação de software do tipo “stand alone”;

21.1.38.12. As funcionalidades devem ser organizadas e distribuídas em menus agregadores, facilitando assim a operação por meio de menus específicos segregados por assunto;

21.1.38.13. A ferramenta de gerenciamento remoto deve fornecer acesso a todas as funcionalidades especificadas neste Termo de Referência, por meio da criação e administração de todas as políticas suportáveis pelo Firewall NGFW, o que inclui as funcionalidades de:

21.1.38.13.1. Segurança avançada de Firewall;

21.1.38.13.2. Serviços adicionais de rede, como NAT, DHCP, roteamento de pacotes e Quality of Service (QoS) e SD-WAN;

21.1.38.13.3. Controle de aplicação;

21.1.38.13.4. Controle por meio de identificação dos usuários;

21.1.38.13.5. Filtro de URL;

21.1.38.13.6. VPN;

21.1.38.13.7. Virtualização de sistemas;

21.1.38.13.8. Proteção contra ameaças: Antivírus/Antimalware;

21.1.38.13.9. IPS;

21.1.38.14. A interface gráfica deve permitir a associação de palavras-chave e a segregação de cores para as regras aplicadas para suas políticas de segurança;

21.1.38.15. Deve permitir a validação prévia de configurações antes da sua aplicação; permitindo identificar erros antes de realizar a configuração da mudança de configurações, como por exemplo, informar uma rota inválida de destino;

21.1.38.16. A função de validação de regras antes de sua efetiva aplicação deve realizar uma análise de regras já configuradas na solução que entrem em conflito ou que sobreponham/sejam sobrepostas pela regra que está sendo salva;

21.1.38.17. Permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação à versão anterior;

21.1.38.18. Permitir salvar e exportar as configurações da solução, para fins de backup e restore;

21.1.38.19. Permitir o rollback de mudanças de configuração, suportando no mínimo o rollback para a última configuração salva;

21.1.38.20. Permitir também o rollback de atualizações de sistema operacional, suportando no mínimo o rollback para a última versão do sistema operacional instalada antes da última atualização;

21.1.38.21. Deverá possuir ferramenta de busca (“localizar”) global, permitindo consultas globais a diferentes objetos da solução, como: Nomes de aplicações, de usuários, de dispositivos, de zonas de segurança, de políticas e de ameaças; endereços e ranges de IPs; sub-redes; endereços URL; categorias de URL, palavras-chave; etc.;

21.1.38.22. Deve mostrar os status dos firewalls em alta disponibilidade;

21.1.38.23. Permitir configurar o envio de mensagens de alerta por parte da solução, via SNMP e via e-mail, permitindo assim o monitoramento do Firewall NGFW por meio de solução externa de monitoramento. Neste caso, deve permitir o envio de mensagens de alerta para no mínimo os seguintes parâmetros:

21.1.38.23.1. Falhas de hardware;

21.1.38.23.2. Uso excessivo de CPU e de memória interna (disco rígido);

21.1.38.23.3. Alertas de utilização máxima de recursos suportados pela solução. Este tipo de alerta deve ser enviado sempre que um determinado limite (threshold) for ultrapassado, como número de sessões concorrentes; número de usuários ou túneis de VPN concorrentes; etc.;

21.1.38.24. Permitir a coleta de estatísticas de todo o tráfego que passar por suas interfaces e funcionalidades de segurança, com coleta de informações básicas como endereço de origem/destino dos pacotes, data/horário e ação tomada pelo NGFW;

21.1.38.25. Permitir o monitoramento do tráfego por meio de ferramenta de coleta e exibição de logs, permitindo a aplicação de filtros, execução de função de busca (localizar) por mais de um valor de entrada, restringir a consulta por faixa de data e horário, além de permitir a exportação do resultado da pesquisa para formatos de dados estruturados, como arquivo .csv;

21.1.38.26. Permitir geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

21.1.38.27. Permitir o envio de logs para aplicações externas (syslogs) de forma granular, podendo-se selecionar quais campos serão exportados;

21.1.38.28. Possuir módulo de geração de relatórios ou dashboards personalizados, que permita exibir informações agregadas e correlacionadas de políticas, aplicações, grupos de usuário; ameaças, URLs, filtro de arquivos, e que possam ser utilizadas tanto para análise gerencial quanto para diagnóstico de problemas e resposta a incidentes;

21.1.38.29. Permitir a visualização sumarizada de todas as aplicações, ameaças, e URLs trafegadas;

21.1.38.30. Permitir a visualização rápida dos seguintes recursos agregados, pesquisável por range de data de pesquisa:

21.1.38.30.1. Principais aplicações, classificadas por utilização de largura de banda em tráfego de entrada e saída (inbound/outbound);

21.1.38.30.2. Principais aplicações, classificadas por taxa de transferência;

21.1.38.30.3. Principais hosts que apresentaram contaminações;

21.1.39. **Monitoramento e Auditoria:**

21.1.39.1. Implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos nesta rede, facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance deverão ser acessíveis via SNMP;

21.1.39.2. Permitir o gerenciamento de registros de logs tanto em sua base interna quanto em sistemas de monitoração externos (syslogs), simultaneamente;

21.1.39.3. Para o uso de sistemas externos de monitoramento (syslogs), deverá:

21.1.39.3.1. Suportar pelo menos 50 syslog senders por Firewall NGFW, físico ou virtualizado;

21.1.39.3.2. Permitir o envio de logs via protocolo UDP e SSL;

21.1.39.3.3. Possuir recursos de proteção contra *spoofing* de endereço IP;

21.1.39.4. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver SSL ou SSH;

21.1.40. **Acessórios adicionais:**

21.1.40.1. Além dos cabos de alimentação de energia, o equipamento deve ser acompanhado também dos seguintes acessórios obrigatórios:

21.1.40.2. Trilhos deslizantes e demais itens necessários para instalação em rack padrão 19 polegadas;

21.1.40.3. Cabos fibre channel com conectores LC/LC com no mínimo 5 (cinco) metros de comprimento, na mesma quantidade de transceivers SFP/SFP+ ofertados na solução, ou seja, no mínimo 16 (dezesseis) cabos;

21.1.40.4. Cabos e interfaces de interconexão entre os appliances físicos para configuração da solução em modo de "alta disponibilidade", considerando-se que os dois firewalls NGFW ficarão próximos um do outro na rack, com distância entre eles de até 02 (dois) U;

21.1.40.5. Todos os drivers, softwares e licenças necessários para o perfeito funcionamento de todos os componentes da solução;

21.1.40.6. Documentação com a especificação técnica dos equipamentos;

21.1.40.7. Manuais de instalação, operação e gerenciamento;

21.1.40.8. Todos os documentos e manuais deverão ser confeccionados preferencialmente em língua portuguesa e fornecidos no momento da entrega do equipamento por meio de mídia física ou digital.

21.2. **GRUPO Único - ITEM 02 - SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE FIREWALL NGFW**

21.2.1. **Resumo do Serviço:**

21.2.1.1. Refere-se ao serviço de instalação física e lógica dos dois Firewall especificados no Item 01 deste Grupo, "start-up" dos appliances físicos, sua configuração em modo de alta disponibilidade, configuração de seu sistema operacional, ativação de seus módulos e respectivas licenças de uso, configuração de regras de segurança baseadas tanto nas regras implementas na solução de Firewall utilizada hoje na PREVIC quanto em novas regras a serem especificadas neste item, assim como em regras acordadas posteriormente entre a equipe técnica da PREVIC e da LICITANTE, incluindo a migração dos clientes de VPN ativos na solução Firewall utilizada hoje no ambiente PREVIC para a nova solução Firewall NGFW, além da migração da solução atual de filtro de conteúdo Web Squid/LightSquid, para a solução de filtro de URL disponível pela nova solução de Firewall NGFW adquirida.

21.2.2. **Descrição da estrutura atual de rede e segurança da PREVIC**

21.2.2.1. Atualmente a rede LAN da sede da PREVIC, onde se localiza o Datacenter do órgão, se conecta a uma rede WAN formada com suas cinco representações regionais presentes no Rio de Janeiro-RJ, São Paulo-SP, Porto Alegre-RS, Belo Horizonte-MG e Recife-PE, através de uma solução WAN prestada pela Empresa de Tecnologia e Informações da Previdência - DATAPREV. Na prática, a rede da PREVIC é, na realidade, uma sub-rede da própria DATAPREV, com a sede e suas cinco representações regionais se conectando entre si por meio de circuitos MPLS/SD-WAN gerenciados pela DATAPREV;

21.2.2.2. Sendo uma sub-rede da DATAPREV, o serviço de segurança de perímetro de redes é também gerenciado pela mesma provedora de serviços. A conexão entre a rede LAN da sede da PREVIC e a rede DATAPREV é realizada através de um acesso à rede de dados de fibra óptica "INFOVIA", mantida em toda a Explanada dos Ministérios pela empresa SERPRO, com quem a DATAPREV possui um contrato de prestações de serviços de link de dados. Já suas representações regionais são LAN's integradas a redes da DATAPREV mantidas regionalmente, usualmente conectando-se por meio de circuitos originalmente utilizados pela rede do INSS;

21.2.2.3. A separação da sub-rede da PREVIC dentro da rede DATAPREV se dá por meio de segregações lógicas. As representações regionais são VLAN's das redes mantidas pela DATAPREV em suas respectivas localidades, já a rede da sede da PREVIC em Brasília-DF é uma sub-rede da rede DATAPREV-DF, segregação esta realizada por meio de uma instância virtual de Firewall NGFW dedicada integralmente à sub-rede PREVIC. A solução atualmente utilizada pela DATAPREV é um NGFW da fabricante Palo Alto, modelo PA-5250, com as seguintes licenças ativas: Threat Prevention; URL-Filtering e WildFire;

21.2.2.4. Em nosso ambiente interno não utilizamos as regras de Threat Prevention nem de URL-Filtering da solução da Palo Alto. Nestes casos utilizamos as seguintes soluções internas:

21.2.2.5. Threat Prevention: BitDefender GravityZone Ultra Suite;

21.2.2.6. URL-Filtering: Squid/LightSquid;

21.2.2.7. Por conta da pandemia de COVID-19 iniciada em 2020, a PREVIC implementou a política de trabalho remoto dentro de seu corpo funcional. Boa parte dos funcionários do órgão hoje trabalham em regime de "home office", utilizando-se de VPN SSL client-to-site para se conectar à rede interna da PREVIC. Para tal, utilizam-se de aplicativo cliente VPN "Palo Alto Global Protect". Os certificados digitais são gerados pela CA da solução NGFW Palo Alto gerenciada pela DATAPREV;

21.2.2.8. Para permitir o acesso de usuários externos a sistemas e serviços hospedados internamente em nossa rede, a PREVIC se utiliza de dois serviços hospedados em uma nuvem privada contratada também com a empresa DATAPREV. Nesta nuvem, implementa com a solução vCloud Suite da VMWare, estão hospedados os dois servidores de DNS Externo da PREVIC, além de um proxy reverso Nginx, que em conjunto fazem o redirecionamento das requisições oriundas da internet para a rede interna da PREVIC. A nuvem privada funciona, na prática, como uma DMZ, com um firewall virtual interno filtrando o tráfego oriundo da internet com destino a sistemas web e serviços hospedados na rede interna da PREVIC;

21.2.2.9. Adicionalmente, a PREVIC se utiliza de alguns serviços de nuvem da Microsoft Azure, em especial para funcionamento de seu serviço de mensageria (Microsoft Teams) e e-mail corporativo, este último implementado com Microsoft Exchange em modo híbrido, com as DAG hospedadas internamente, e o Edge e filtro antispam hospedados na nuvem da Microsoft Azure ("Exchange Online Protection").

FIGURA 1 - REDE LAN/WAN PREVIC

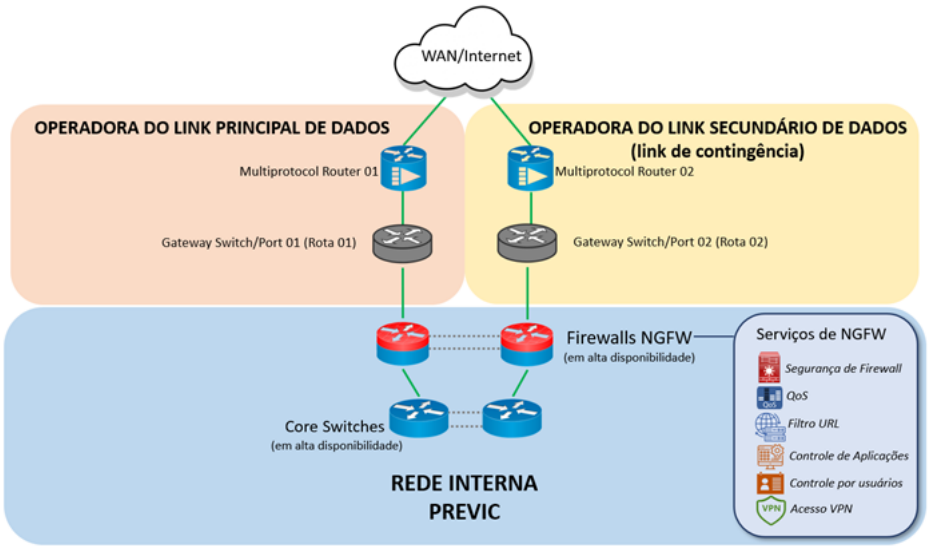


FIGURA 2 - INTEGRAÇÃO ENTRE REDE PREVIC SEDE E REDE DATAPREV

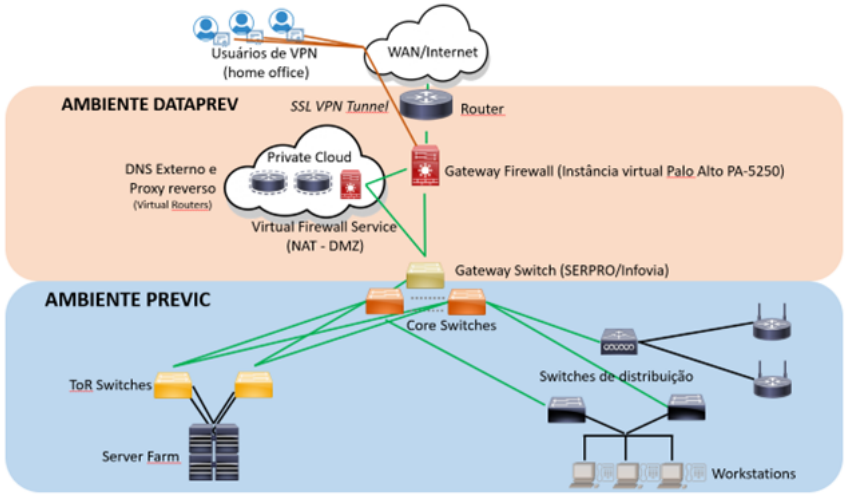
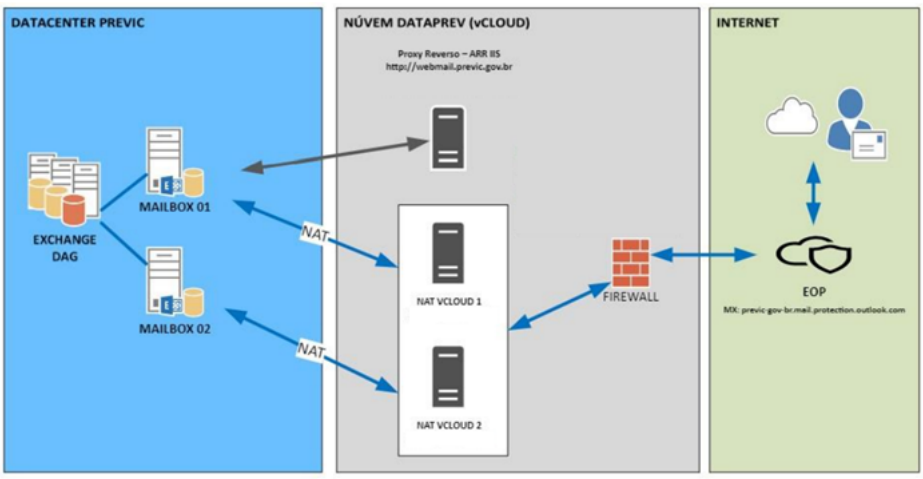


FIGURA 3 - ESTRUTURA EXCHANGE COM MICROSOFT EOP



21.2.3. **Projeto de mudança da estrutura de rede e segurança da PREVIC**

21.2.3.1. A PREVIC iniciou neste ano de 2022 um projeto de segregação total da empresa DATAPREV. Dentro do escopo deste projeto, decidiu-se por:

21.2.3.2. Concentrar serviços e sistemas corporativos em plataforma web, acessíveis por navegadores de internet e sem a necessidade de conexão permanente de suas representações regionais em uma rede WAN própria;

21.2.3.3. Para recursos que não podem ser disponibilizados em plataforma web acessível diretamente pela internet, como repositórios locais de arquivos (Fileserver, NFS), Intranet, bases de dados corporativas e sistemas cujo acesso seja estritamente interno por questões de segurança, o acesso será realizado via conexão individual de VPN (VPN Client);

21.2.3.4. Contratar uma solução de link de dados própria para a sua rede principal no edifício sede, onde fica hospedado o Datacenter do órgão, com previsão de utilização de dois links de dados dedicados e simétricos - Um link principal, com velocidade entre 150 e 200 mbps, e um link de backup secundário, com velocidade entre 100 e 150 mpbs, que entraria em operação somente quando o link principal não estivesse disponível;

21.2.3.5. Contratar link de dados convencionais para as cinco representações regionais, com velocidades de conexão variadas, de acordo com a necessidade de cada localidade;

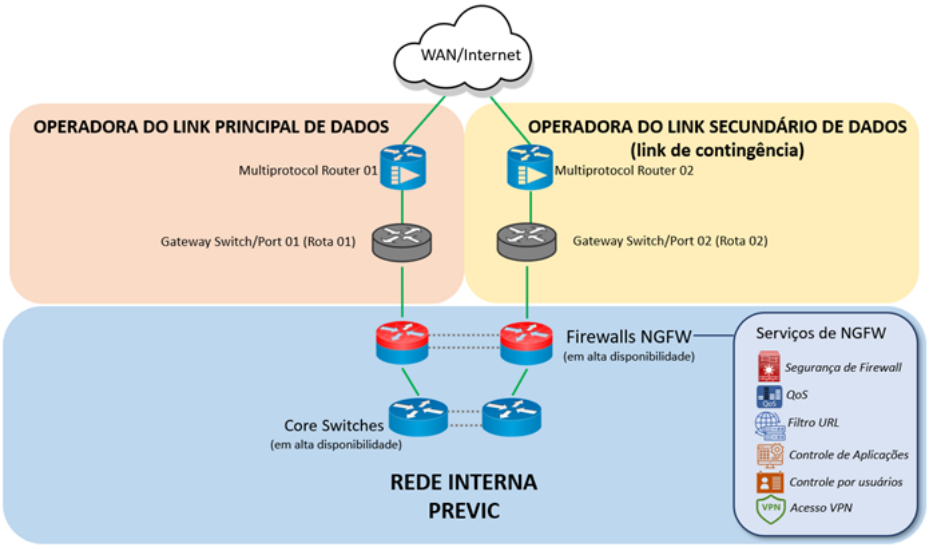
21.2.3.6. Contratar uma solução de segurança de redes que permita a migração de diversos recursos de segurança hoje providos pela empresa DATAPREV. Trata-se exatamente da presente contratação;

21.2.3.7. Com esta nova solução de segurança, substituir o Squid/LightSquid pela solução de URL-Filtering a ser ofertada em conjunto com a solução de Firewall NGFW, considerando-se que o filtro de conteúdo atual ter sérias limitações quanto à filtragem de conteúdo dinâmico, como o provido por aplicativos de smartphones e serviços de streaming;

21.2.3.8. Inicialmente não ativaremos o recurso de Threat Prevention da solução objeto desta aquisição, visto que a o BitDefender GravityZone foi adquirido recentemente pela autarquia, e ainda está sob garantia e suporte técnico da fabricante. Por este motivo não solicitamos a ativação desta licença de uso deste recurso no processo atual, solicitamos que o Firewall NGFW a ser fornecido possua todas as funcionalidades de Threat Prevention em sua arquitetura, sob possibilidade de posteriormente adquirirmos seu licenciamento em específico ao fim da vigência do contrato com a fornecedora da solução atual – BitDefender GravityZone;

21.2.3.9. Deste modo, a estrutura de redes da PREVIC passaria a ser completamente administrada pela própria autarquia, passando a ter uma estrutura diferente da atual:

Figura 4 - Nova Estrutura de rede PREVIC



21.2.3.10. Considerando-se o escopo da presente contratação, restrita à solução de segurança de rede, as ações a serem tomadas para a implementação desta mudança de estrutura de rede resumem-se a:

21.2.3.11. Instalar e configurar esta solução de segurança de rede, de modo a permitir que a rede da PREVIC se conecte à rede pública (internet) por dois links de dados distintos, um principal e outro para uso contingencial, de modo que, em caso de queda do link de dados principal, a solução roteie automaticamente o tráfego para o link de contingência;

21.2.3.12. Configurar os dois appliances em modo de alta disponibilidade, para que tenhamos dois equipamentos com configurações idênticas, conectados a interfaces e switches distintos de nossa rede interna, de modo que tanto o tráfego entre as redes internas da PREVIC quanto o tráfego entre a rede PREVIC e a Internet tenha mais de uma rota de trânsito de dados, não havendo pontos únicos de falha. Nesta nova estrutura, haveria redundância nos switches core, nos Firewall NGFW e nos links de dados para internet, reduzindo-se assim a probabilidade de quedas de conexão por ocorrência de falha em um determinado dispositivo, interface ou link de dados;

21.2.3.13. Reconfigurar as regras gerais de tráfego de rede, com novas rotas de saída (gateways), por conta dos novos links de dados, criação de zonas e de políticas de segurança para filtragem e controle de tráfego, e configuração de parâmetros de uso de banda de dados para qualidade de serviço (QoS);

21.2.3.14. Migrar e reconfigurar para a nova estrutura de rede, as regras de entrada e saída de tráfego de serviços e aplicações hospedadas em nosso ambiente interno;

21.2.3.15. Migrar os clientes de VPN ativos na estrutura atual para a nova estrutura;

21.2.3.16. Migrar o serviço de filtro de conteúdo web (proxy web) da solução atual – Squid/Light Squid, para a nova solução de filtro de URL;

21.2.3.17. Reconfigurar serviços de rede que serão afetados diretamente pela mudança da solução de segurança de redes, como solução de rede wi-fi interna, DNS interno e externo, DHCP, etc.

21.2.3.18. **Especificação técnica dos serviços:**

21.2.3.19. Após a entrega dos dois dispositivos Firewall NGFW (Lote 01 - Item 01), a empresa contratada deverá iniciar, num prazo máximo de até 30 (trinta) dias corridos, o serviço de instalação e configuração da solução;

21.2.3.20. Durante este prazo inicial de 30 dias corridos, a empresa contratada deverá realizar o planejamento da execução, com a confecção de um projeto de execução do serviço a ser prestado, contando com o apoio, no que couber, da equipe técnica da CGTI/DIRAD/PREVIC;

21.2.3.21. Nesta etapa inicial, a CONTRATADA deverá analisar a topologia e arquitetura da rede PREVIC, considerando todos os equipamentos e recursos de rede já existentes e instalados;

21.2.3.22. A CONTRATADA pode estender esta análise ao tráfego usualmente operado (inbound e outbound) de Internet, entre os switches core e os switches de acesso, rede wi-fi, acesso a sites remotos e serviços de rede externos como os hospedados em nuvens públicas e privadas. Para operacionalizar tal atividade, a CONTRATADA poderá solicitar à equipe técnica da PREVIC a configuração de uma ou mais interfaces de rede para espelhamento de tráfego ("sniffer"). Neste caso, a CONTRATADA deverá solicitar esta configuração com antecedência mínima de 03 (três) dias úteis, disponibilizando-se a detalhar qual tráfego deseja espelhar e o período total de análise;

21.2.3.23. Caso a empresa contratada entenda ser necessário o envolvimento das empresas provedoras dos links de dados para conexão à rede externa (internet), deverá ser solicitada reunião (virtual ou presencial) com antecedência mínima de 03 (três) dias úteis, para que a equipe da CGTI/DIRAD/PREVIC entre em contato com as empresas e consiga confirmar a disponibilidade para a realização da reunião;

21.2.3.24. O produto final de formalização desta etapa inicial será o "Projeto de Execução". Este documento deverá obrigatoriamente incluir:

21.2.3.24.1. A data de início e de término do serviço;

21.2.3.24.2. Cronograma completo de execução do serviço, constando as datas específicas e a descrição pormenorizada dos serviços a serem executados em cada etapa;

21.2.3.24.3. Pré-requisitos para a implantação, em conformidade com o ambiente computacional disponível na PREVIC;

21.2.3.24.4. Detalhamento das conexões e configurações físicas e lógicas necessárias para a execução do serviço;

21.2.3.24.5. Relação dos profissionais envolvidos, com fornecimento do nome completo e número do documento de identificação;

21.2.3.24.6. Prazo máximo de execução do serviço de instalação e configuração da solução: 60 (sessenta) dias corridos a partir da data do início do projeto;

21.2.3.25. A data de início do projeto não poderá ser superior a 10 (dez) dias úteis, a contar da data de envio do Projeto de Execução para avaliação da equipe técnica da CGTI/DIRAD/PREVIC;

21.2.3.26. O serviço de instalação e configuração só será iniciado após a aprovação do referido Projeto de Execução, que será avaliado pela PREVIC em até 10 (dez) dias corridos, a contar da data de recebimento do documento, período este em que o prazo máximo de execução do serviço, especificado no subitem **21.2.3.24.6** deste Termo de Referência, será interrompido;

21.2.3.27. Sendo o Projeto de Execução rejeitado pela PREVIC, o prazo máximo de instalação mencionado no parágrafo anterior será retomado. A empresa CONTRATADA deverá analisar a resposta enviada pela equipe técnica da CGTI/DIRAD/PREVIC e apresentar nova proposta em até 03 (três) dias corridos, a contar do recebimento da resposta de rejeição. Após o recebimento do novo Projeto de Execução, retoma-se a interrupção temporária do prazo de execução do serviço, conforme especificado no parágrafo anterior;

21.2.3.28. Sendo necessário, deverá ser solicitado, com antecedência mínima de 72 (setenta e duas) horas, o acesso à rede e ao ambiente corporativo de TI da PREVIC por parte de funcionários da empresa contratada, informando o motivo da concessão de acesso, a identificação do funcionário e o período de concessão das credenciais;

Descrição Completa do cronograma básico de execução:

Etapa	*Data Inicial*	*Prazo máximo*	*Responsável*	*Entrega Principal*
Planejamento do serviço e elaboração do Projeto de Execução	Data de entrega dos 02 Firewall NGFW	30 dias corridos	CONTRATADA	Projeto de Execução
Análise do Projeto de Execução	Data de entrega do Projeto de Execução por parte da CONTRATADA	10 dias corridos	CGTI/DIRAD/PREVIC	Manifestação quanto a aceitação ou rejeição do Projeto de Execução
Revisão do Projeto de Execução	A partir da data de manifestação da CGTI/DIRAD/PREVIC	3 dias corridos	CONTRATADA	Projeto de Execução revisado. (Etapa só será realizada caso a equipe da CGTI rejeite o Projeto de Execução apresentado pela CONTRATADA)
Instalação e Configuração da solução de segurança de rede NGFW	A partir da data de início registrada no Projeto de Execução, limitada a 10 dias úteis após a data de envio deste Plano para análise pela CGTI/DIRAD/PREVIC	60 dias corridos	CONTRATADA, com apoio da equipe técnica da CGTI/DIRAD/PREVIC	Solução NGFW configurada, testada e em operação no ambiente da PREVIC Relatório final de implantação da solução

21.2.3.29. A PREVIC irá disponibilizar, para instalação do equipamento, os seguintes itens de configuração e serviços de apoio:

21.2.3.29.1. Até 6 baias (6U) de espaço em uma rack de equipamentos padrão 19", sendo 4 baias para os appliances NGFW, e 2 baias para organização dos cabos de rede;

21.2.3.29.2. 04 (quatro) tomadas de energia padrão 3 pinos (NBR 14.136);

21.2.3.29.3. Portas Gigabit Ethernet e SFP/SFP+ para interconexão das interfaces de rede dos Firewalls NGFW e os switches de rede da PREVIC, na quantidade especificada no Projeto de Execução;

21.2.3.29.4. Cabos FTP Gigabit Ethernet Cat 6, conforme especificação técnica do subitem **21.4** deste Termo de Referência, na quantidade necessária para interconectar os switches de rede da PREVIC com as interfaces de rede dos Firewall NGFW;

21.2.3.29.5. Alocação de endereços IP e ranges de sub-rede, conforme orientação a ser repassada pela equipe técnica da contratada (pré-requisitos);

21.2.3.29.6. Apoio na execução de configurações adicionais de rede, em conjunto com a equipe técnica da empresa contratada; incluindo DNS Interno e Externo; NAT; endereçamento TCP/IP; serviço de DHCP; SMNP; criação ou alteração de grupos no Active Directory, e instalação de drivers nos servidores físicos ou virtuais;

21.2.4. O serviço de instalação e configuração da solução deverá ser realizado por técnicos certificados oficialmente pelo fabricante da solução ofertada, ou certificados por empresa oficialmente habilitada para realizar treinamentos da solução ofertada. A documentação comprobatória deverá ser anexada ao Projeto de Execução;

21.2.5. Todos os procedimentos de configuração de sistema deverão ser executados de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante da solução ofertada deverá disponibilizar ferramenta gratuita (ou incluir nos custos de serviço) para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

21.2.6. Eventuais mudanças de escopo e de requisitos do Projeto de Execução deverão ser devidamente formalizadas, sendo obrigatoriamente aprovadas pelo integrante técnico da presente contratação. Cada mudança deverá conter, no mínimo, as seguintes informações:

21.2.6.0.1. Data da alteração;

21.2.6.0.2. Descrição das mudanças;

21.2.6.0.3. Análise de Impacto/Análise de riscos da mudança;

21.2.6.0.4. Data de aprovação da mudança;

21.2.6.0.5. Comprovação da aprovação da mudança, por parte do integrante técnico;

21.2.7. O serviço de instalação e configuração deverá incluir necessariamente, as seguintes etapas e atividades, todas a serem executadas sob a supervisão da equipe técnica da CGTI/DIRAD/PREVIC:

DESEMBALAGEM DOS DOIS APPLIANCES FIREWALL NGFW;

21.2.8. **Inventario dos componentes dos dois appliances:**

21.2.8.1. Se neste processo for verificada a ausência de alguma peça ou componente, a empresa contratada deverá informar imediatamente à equipe técnica da CGTI/DIRAD/PREVIC, por meio de relatório assinado pelo técnico responsável pela instalação do equipamento. A partir da notificação o prazo de instalação do equipamento será suspenso, e a empresa contratada terá o prazo máximo de 48 (quarenta e oito) hora para expedição de pedido de envio do(s) componente(s) faltante(s), que deverá(ão) ser entregue(s) na sede da PREVIC dentro do prazo máximo de 120 (cento e vinte) horas, a contar da data e horário de solicitação junto à fabricante. A partir da recepção do(s) componente(s), a contratada terá o prazo máximo de 24 (horas) para reiniciar o serviço de instalação do equipamento, sendo a partir de então retomado o prazo máximo de finalização deste serviço.

21.2.9. **Instalação física:**

21.2.9.1. Esta etapa deverá incluir a integração de todas as peças, componentes e acessórios necessários para seu funcionamento, a colocação dos equipamentos na rack padrão 19" disponibilizada pela PREVIC, e a conexão física de todos os cabos (power cords, fibre channel e UTP), incluindo a instalação e ativação de transceivers e a interconexão de suas interfaces com as interfaces de rede dos switches da PREVIC e das operadoras de link de dados.

21.2.10. **Ligação inicial (start up):**

21.2.10.1. Após a instalação física deve-se efetuar a ligação inicial do equipamento e realizar todos os testes de verificação e de diagnóstico solicitados pelo manual do fabricante, com o objetivo de verificar se todos os componentes estão em perfeito funcionamento. Caso seja identificada nesta etapa alguma falha ou defeito no equipamento, a empresa contratada deverá tomar as mesmas medidas descritas no subitem **21.2.8** deste termo de referência (inventário de componentes);

21.2.11. **Configuração inicial (initial setup):**

21.2.11.1. Com o equipamento devidamente ligado e com seus componentes integralmente funcionais, deve-se realizar a configuração inicial da solução, de acordo com as recomendações estabelecidas pelo fabricante, incluindo atividades como:

21.2.11.1.1. Atribuição de endereço(s) IP(s) para gerenciamento remoto;

21.2.11.1.2. Configuração de hostnames e integração ao domínio da rede interna;

21.2.11.1.3. Configuração de data e hora e timezone;

21.2.11.1.4. Cadastramento dos usuários gerenciadores do equipamento;

21.2.11.1.5. Instalação e atualização do sistema operacional da solução, se necessário;

21.2.11.1.6. Atualização de drivers, firmwares e outros softwares acessórios necessários para o pleno funcionamento do equipamento;

21.2.11.1.7. Ativação de recursos básicos para início da configuração avançada da solução, incluindo licenças de software;

21.2.11.1.8. Ativação da console de gerenciamento remoto da solução.

21.2.12. **Configuração avançada:**

21.2.12.1. Com a configuração inicial concluída, deverá ser realizada a configuração avançada da solução, com o objetivo de torná-lo apto a executar as funções de segurança de redes, incluindo obrigatoriamente:

21.2.12.2. Interconexão dos dois Firewalls NGFW, e a configuração de ambos para operarem em modo de alta disponibilidade. A modalidade de configuração de alta disponibilidade (ativo/passivo, ativo/ativo ou clustering) deverá ser avaliada pela empresa contratada, considerando as particularidades da estrutura de redes da PREVIC e as funcionalidades da solução NGFW ofertada;

21.2.12.3. Conexão lógica da solução aos links de dados externos (internet) das operadoras, com criação de pelo menos uma zona pública de segurança para segregação do tráfego externo do tráfego interno da rede PREVIC;

21.2.12.4. Configuração da solução para monitoramento dos links de dados de internet, de modo a realizar o roteamento de tráfego caso o link operacional deixe de funcionar (falha no tráfego em rotas ou em interfaces);

21.2.12.5. Configuração das zonas internas de segurança, necessárias para segregação de tráfego interno na rede PREVIC, conforme descritas no Projeto de Execução;

21.2.12.6. Configuração de uma ou mais zonas de segurança neutras (Demilitarized Zone – DMZ), conforme descritas no Projeto de Execução, necessárias para permitir o tráfego entre a zona pública (internet) e as zonas internas, a serem utilizadas para o funcionamento de serviços como DNS Externo, Proxy Reverso e acesso VPN client-to-site;

21.2.12.7. Configuração de regras de segurança para controle do tráfego entre as zonas de segurança, migrando regras já aplicadas e configuradas na solução atual de segurança de perímetro de rede (Palo Alto PA-5250), adaptando regras que estejam configuradas apenas considerando as camadas 2 e 3 do modelo OSI, para regras abrangendo controle de aplicações (camada 7) e controle por identificação de usuários, e adicionando regras necessárias para o melhor funcionamento da nova estrutura de redes da PREVIC;

21.2.12.8. Configuração de políticas de segurança para melhor controle do tráfego entre as redes internas da PREVIC e entre a sua rede interna e a rede externa (internet), utilizando-se dos recursos avançados de um Firewall NGFW, como controle de aplicações e controle por identificação de usuários;

21.2.12.9. Migração da solução atual de filtro de conteúdo web Squid/Lightsquid para a solução de filtro de URL a ser ofertada dentro da solução Firewall NGFW, respeitando as regras de perfil de acesso estabelecidas atualmente por meio da Política de Acesso à Internet da PREVIC, Portaria nº 442/DICOL/PREVIC;

21.2.12.10. Migração da solução de VPN SSL client-to-site atualmente utilizada no ambiente PREVIC (Palo Alto PA-5250 + Global Protect Agent) para a nova solução de VPN a ser ofertada dentro da solução Firewall NGFW, incluindo a mudança de configuração de autenticação de usuários, hoje realizada via integração

do OpenLDAP da DATAPREV com a Certification Authority (CA) interna da Palo Alto PA-5250, para a integração entre CA interna da nova solução Firewall NGFW com o Active Directory/LDAP da PREVIC;

21.2.12.11. Configuração personalizada das regras de segurança para a nova solução de VPN. Atualmente a solução de VPN possui uma única política global. A nova solução deverá prover políticas de acesso diferenciadas por grupo de usuários VPN, com perfis de acesso diferentes aos recursos da rede interna;

21.2.12.12. Ativação de regras de controle de uso de banda de redes – QoS, incluindo regras orientadas à aplicações e recursos específicos, como módulo de reuniões e videochamadas do Microsoft Teams e streaming de áudio e de vídeo;

21.2.12.13. Configurar a nova solução para que não sobreponha ou inabilite os recursos de segurança já presentes e operacionais no ambiente PREVIC, como o antivírus/antimalware BitDefender GravityZone Ultra Suite e o filtro antispam Exchange Online Protection;

21.2.12.14. Realizar a integração necessária entre a nova solução Firewall NGFW e a controladora de Wi-Fi, de modo a permitir a conexão tanto de usuários da rede interna PREVIC quanto o uso da rede pública de Wi-Fi da autarquia para acesso limitado e temporário à internet;

21.2.12.15. Criação e concessão dos grupos de acesso para administração, operação e monitoramento da solução;

21.2.12.16. Ativação e calibragem das regras de monitoramento de tráfego, alertas, notificações, logging e auditoria;

21.2.12.17. Integração da nova solução Firewall NGFW às ferramentas de monitoramento de ativos de rede da PREVIC (Zabbix, Grafana e System Center);

21.2.12.18. Apoio na reconfiguração dos serviços de rede da PREVIC, em especial do serviço de DNS interno e externo, DHCP; proxy reverso, Veritas NetBackup, OKD/Kubernetes, Red Hat Openshift; Microsoft Office 365, em especial os recursos Microsoft Exchange, Microsoft Teams, Sharepoint e PowerBI; componentes de autenticação de usuários a sistemas, e demais recursos que venham a ser afetados pela implantação da nova solução de Firewall NGFW;

21.2.13. **Testes e homologação:**

21.2.13.1. Etapa a ser realizada em conjunto com a equipe técnica da CGTI/DIRAD/PREVIC, onde será realizada a validação das regras e configurações implementadas;

21.2.13.2. Os testes devem abranger todos os módulos ativados da solução, incluindo no mínimo as seguintes funcionalidades e recursos do ambiente:

21.2.13.2.1. Controle de tráfego intrazonas;

21.2.13.2.2. Controle de tráfego entre zonas distintas;

21.2.13.2.3. Filtro de URL: Validação mínima dos 3 perfis de acesso previstos pelas normas internas de segurança da PREVIC, além de teste de acesso à internet sem nenhum filtro aplicado;

21.2.13.2.4. Validação do tráfego das principais aplicações da PREVIC: Comunicação entre múltiplas camadas das aplicações principais da PREVIC, verificando se seus componentes estão processando os dados corretamente. Deve-se obrigatoriamente testar a comunicação entre as camadas de apresentação, de regras de negócio, persistência em bases de dados e autenticação externa de usuários;

21.2.13.2.5. Teste de execução de backup e restore de dados da rede interna via Veritas NetBackup, comprovando que a solução continua apta a realizar os procedimentos de backup e restore do ambiente;

21.2.13.2.6. Testes de envio e recebimento de e-mails por meio da solução Microsoft Exchange;

21.2.13.2.7. Teste de comunicação entre os componentes Microsoft 365 – Exchange on promises e EOP, Teams, Sharepoint e Office 365;

21.2.13.2.8. Teste de comunicação das soluções de container presentes no ambiente PREVIC: OKD/Docker e Red Hat Openshift, em especial a comunicação das aplicações e do orquestrador com os demais hosts da rede interna PREVIC e com o proxy reverso;

21.2.13.2.9. Teste de execução de rotinas de extração e transformação de dados (ETL/Data Warehouse) no SQL Server, incluindo sua comunicação com os servidores de geração de dashboards e relatórios (Integration Services e Power BI);

21.2.13.2.10. Teste de comunicação das ferramentas de monitoramento de ambiente – Zabbix, Grafana e System Center;

21.2.13.2.11. Teste de conexão via VPN client-to-site, com utilização de pelo menos um usuário para cada perfil de acesso VPN configurado, incluindo no mínimo 3 usuários acessando de outro Estado (Representações Regionais);

21.2.13.2.12. Teste de validação das regras de QoS configuradas;

21.2.13.2.13. Coleta e extração de dados de auditoria da solução de segurança de rede: Geração de relatórios ou dashboards, filtragem de informações e logging.

21.2.14. **Documentação Final**

21.2.14.1. O processo de implantação deverá ser devidamente documentado pela CONTRATADA ao longo de todo o período de execução. Ao fim do processo a CONTRATADA deverá apresentar um relatório com o detalhamento da implantação, contendo todas as etapas, histórico de mudanças, diagramas e detalhamento da estrutura da solução, procedimentos adotados, configurações efetuadas e resultado dos testes e homologação;

21.2.14.2. A entrega deste relatório é obrigatória, sendo este o principal artefato comprobatório de conclusão da execução do serviço, a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.

21.3. **GRUPO ÚNICO - ITEM 03 - TREINAMENTO OFICIAL DO FIREWALL NGFW**

21.3.1. Treinamento oficial sobre a solução de Firewall NGFW oferecida no Grupo Único deste Termo de Referência, a ser ministrada a funcionários da PREVIC, servidores ou terceirizados, que atuarão diretamente na administração e operação da solução após sua implementação;

21.3.2. Quantidade mínima: 03 (três) funcionários;

21.3.3. Treinamento oficial do fabricante com repasse de conhecimento específico sobre a solução instalada para, no mínimo, 03 (três) funcionários da PREVIC;

21.3.4. Duração mínima: 5 (cinco) dias ou 30 (trinta) horas semanais, a depender da modalidade de execução do treinamento, com duração diária máxima de 6 (seis) horas;

21.3.5. Início do treinamento: Em até 14 (quatorze) dias corridos, contados após a conclusão da instalação e configuração da solução e a ativação das licenças (subitem 21.2 - Grupo Único - Item 02). O prazo inicial poderá ser estendido, em caso de indisponibilidade de treinamento oficial no período, desde que a prorrogação seja previamente solicitada à CONTRATANTE, com antecedência mínima de 03 (três) dias úteis, antes da data prevista para início de sua execução;

21.3.6. O treinamento deverá ser ministrado em horário comercial, e deverá ser realizado pelo fabricante ou por uma empresa parceira devidamente certificada e autorizada pelo fabricante a ministrar treinamentos oficiais;

21.3.7. Modalidade: Preferencialmente na modalidade presencial, nas instalações do fabricante ou do parceiro autorizado, podendo também ser realizada na modalidade remota, em decorrência das restrições impostas pela pandemia de COVID-19;

21.3.8. O treinamento deverá oferecer material didático de apoio gratuito aos participantes, seja por meio de mídia física (livros, apostilas, etc.) ou digital (PDF). O material deverá ser cedido individualmente a cada participante, de modo que ele possa levar consigo e consultá-lo posteriormente;

21.3.9. Eventuais despesas de deslocamento, hospedagem e alimentação dos instrutores do curso serão de responsabilidade integral da CONTRATADA. Já as eventuais despesas de deslocamento, hospedagem e alimentação dos participantes do curso serão de responsabilidade integral da CONTRATANTE;

21.3.10. O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração e gerenciamento, além de tratamento de problemas típicos envolvendo a operação da solução;

21.3.11. O escopo básico do treinamento deverá conter:

21.3.11.1. Arquitetura da solução;

21.3.11.2. Configurações iniciais básicas;

21.3.11.3. Alta disponibilidade;

21.3.11.4. Controle de acesso dos administradores da solução;

21.3.11.5. Configuração de Interfaces;

21.3.11.6. Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT;

21.3.11.7. Controle por Identificação de Aplicações;

21.3.11.8. Controle por Identificação de Usuários, com conexão a fontes externas de autenticação;

21.3.11.9. Criação e gerenciamento de Filtro URL;

21.3.11.10. Decriptografia de tráfego;

21.3.11.11. Configurações de VPN (SSL e IPSec);

21.3.11.12. Monitoramento e Relatórios;

21.3.11.13. Logging e Auditoria;

21.3.12. Ao final do treinamento, deverá ser emitido certificado comprobatório da participação de cada funcionário da PREVIC. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.

21.4. **SUPRIMENTOS PARA INTERCONEXÃO DA SOLUÇÃO DE SEGURANÇA DE REDE AOS DISPOSITIVOS DA REDE PREVIC**

Descrição resumida:

21.4.1. Para atendimento ao subitem 21.2.3.29.4 deste Termo de Referência, deve ser oferecido o quanto baste de cabos de rede blindados e já montados (“Patch Cord”), categoria mínima Cat6, compatíveis com rede Gigabit Ethernet, padrão de blindagem mínima FTP (“Foiled Twisted Pair”), com um conector padrão RJ-45 em cada ponta do cabo montado, igualmente blindados, de cor externa vermelha, para uso na instalação física da solução descrita no Grupo Único deste Termo de Referência, conectando as interfaces Gigabit Ethernet dos dois Firewall NGFW às portas dos switches de rede do Datacenter da PREVIC;

21.4.2. Todos os cabos deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas;

21.4.3. Todos os cabos deverão ser entregues em remessa única;

21.4.4. Todas as especificações técnicas são as mesmas para o grupo, a única diferença entre os itens do grupo é o comprimento do cabo, sendo:

Especificações técnicas exigidas para todos os cabos:

21.4.5. Tipo de cabo: Cabo montado (“Patch Cord”);

21.4.6. Categoria mínima do cabo: Cat6 com filamentos de cobre puro, a serem utilizados em conexão de dispositivos de rede no padrão Gigabit Ethernet;

21.4.7. *Classe do cabo:* CMX resistente à chama, com cobertura protetora de PVC e isolação em polietileno;

21.4.8. *Diâmetro do cabo:* Entre 23 a 24 AWG;

21.4.9. *Blindagem do cabo:* Padrão mínimo aceitável é o FTP (“Foiled Twisted Pair”);

21.4.10. *Cor externa:* Vermelha;

21.4.11. *Configuração de pinagem:* Direta (“straight cable”);

21.4.12. *Conectores:* Cada patch cord deve possuir um conector do tipo RJ-45 em cada ponta (dois conectores por cabo). Os conectores também devem ser blindados, com revestimento externo de blindagem sendo feito de liga de metal leve, como alumínio;

21.4.13. *Capa protetora*: O cabo deve possuir capa protetora injetada para os conectores RJ-45 (“boot injetado”), evitando que a conexão entre o conector e o cabo fique exposta, trazendo ainda proteção adicional à haste de trava dos conectores RJ-45;

21.4.14. *Temperatura de operação:* Entre -10º a 60º Celsius;

21.4.15. *Garantia mínima:* 12 (doze) meses;

21.4.16. *Certificações e homologações mínimas:*

21.4.16.1. Certificação ANATEL;

21.4.16.2. ETL Verified;

21.4.16.3. Diretivas de preservação do meio ambiente: *Restriction of Hazardous Substances Directive (ROHS)*;

21.4.16.4. *Requisitos físicos e elétricos:* ANSI/TIA-568C.2 e ISO/IEC11801;

21.4.16.5. CMX: NBR 6244 / NBR 14705, IEC 60332 ou UL1581 (Vertical Tray Flame Test);

21.4.16.6. *Uso em redes de cabeamento estruturado:* NBR 14703 / NBR 14565;

REQUISITOS DE MANUTENÇÃO

Grupo Único - Solução de segurança de rede com Firewall de última geração (NGFW)

21.5. Os equipamentos e softwares adquiridos nesse processo deverão possuir garantia do fabricante ou de empresa autorizada pelo fabricante para prestação deste serviço no Brasil, com prazo mínimo de duração de 48 (quarenta e oito) meses, contados a partir do recebimento definitivo da solução, que se dará somente quando de sua completa instalação, configuração e início de operação;

21.6. Durante todo o prazo de vigência a garantia deverá incluir os serviços de manutenção preventiva e corretiva, cuja periodicidade de execução deverá se dar de acordo com as recomendações técnicas da fabricante da solução;

21.7. A manutenção preventiva deverá, no mínimo, incluir:

21.7.1. Atualização de todos os componentes de software da solução, incluindo patches de segurança, firmwares e versões de sistema operacional, seja para corrigir problemas identificados, seja para implementação de melhorias e acesso a novas funcionalidades;

21.7.2. Acesso e atualização de assinaturas de proteção, assim como às bases de dados mantidas pela fabricante, necessárias para o correto e pleno funcionamento da solução, tais como Black e White Lists, assinaturas do tipo "Zero Day", lista de aplicativos confiáveis, etc;

21.8. A manutenção corretiva deverá, no mínimo, incluir:

21.8.1. Reposição de peças, componentes e equipamentos que apresentarem defeito ou falha de funcionamento, abrangendo todos os itens que compõem a solução, incluindo seus acessórios, módulos de expansão, *transceivers* ou outros equipamentos fornecidos pela CONTRATADA para funcionamento da solução;

21.8.2. Em caso de defeitos de fabricação ou a necessidade de substituição hardware, a garantia deverá incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital. O envio da peça ou equipamento de reposição deverá ser realizado, no máximo, até o fim do próximo dia útil após a detecção da falha;

Serviço de Suporte Técnico

21.9. Durante todo o prazo de garantia, a PREVIC poderá solicitar o suporte técnico especializado da fabricante ou empresa oficialmente autorizada pela fabricante a prestar o serviço de suporte no Brasil, sem limitação de quantidade de chamados por período;

21.9.1. A solicitação de suporte técnico por parte da PREVIC se dará através de abertura de chamado, a ser realizado por, no mínimo, os seguintes meios de comunicação, disponibilizados sempre em idioma português (Brasil):

21.9.2. Ligação telefônica gratuita (0800);

21.9.3. Sistema web (website) com autenticação segura (mínimo usuário e senha de acesso);

21.9.4. E-mail corporativo (em caso de indisponibilidade dos meios anteriormente citados);

21.10. O suporte técnico deverá estar disponível na modalidade "24x7" (24 horas por dia, 7 dias por semana), tanto na modalidade remota quanto presencial (on-site);

21.11. O suporte deverá respeitar, no mínimo, os seguintes tempos de resposta para os níveis de severidade abaixo:

21.11.1. *Crítica*: Significa que a solução ficou inoperante ou ocorreu falha de grande impacto que fez com que a solução parasse de funcionar;

21.11.1.1. Para este nível de severidade o encaminhamento do chamado para atendimento deverá ser imediato, com tempo de resposta de resolução máxima de 60 (sessenta) minutos, a contar da recepção do chamado, sendo preferencialmente prestado na modalidade presencial (on-site). Nestes casos, considerar-se-á como resolução o retorno do funcionamento da solução, seja através de implementação de uma solução definitiva para o incidente, seja por meio de uma solução temporária para colocação emergencial da solução novamente em operação;

21.11.2. *Alta*: Incidentes que não causem a paralisação completa da solução, mas que causem dano moderado em seu funcionamento, tais como: Lentidão elevada, travamentos e interrupções recorrentes, inoperância parcial (alguma funcionalidade ou módulo da solução deixar de funcionar). Para este nível de severidade o tempo máximo de resposta deverá ser de até 02 (duas) horas, em horário comercial, a contar da recepção do chamado, sendo preferencialmente prestado na modalidade presencial (on-site). Nestes casos, considerar-se-á como resolução o restabelecimento do funcionamento normal da solução, seja através de implementação de uma solução definitiva para o incidente, seja por meio de uma solução temporária para colocação emergencial da solução novamente em operação normal;

21.11.3. *Média*: Incidentes que causem redução de performance da solução, tais como lentidão intermitente, erros e falhas em determinados módulos ou recursos e falha no funcionamento de políticas já implementadas; Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

21.11.4. *Baixa ou informativa*: Incidentes de baixo impacto, que não causem falhas ou redução de performance da solução, ou que afetem módulos ou funcionalidades que não sejam consideradas como essenciais para o funcionamento da solução, tais como ferramenta de geração de relatórios, acesso à dashboards, funções administrativas da solução (edição de grupos de administração, por exemplo). Inclui também chamados para esclarecimento de dúvidas sobre a configuração ou funcionamento da solução. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

REQUISITOS TEMPORAIS

Do Detalhamento da Metodologia de Execução/entregas

21.12. As despesas com transportadora e serviço de entrega, incluindo o transporte intra-predial, correrão totalmente por conta das empresas contratadas;

21.13. Eventuais danos ocorridos durante o transporte e entrega dos equipamentos não são de responsabilidade da PREVIC;

21.14. A entrega física de equipamentos, peças e suprimentos deve ser realizada em horário comercial, preferencialmente sob data previamente estabelecida ou informada pela CONTRATADA, no seguinte endereço:

Destinatário: PREVIC – Coordenação-Geral de Tecnologia da Informação

Endereço: Ed. Venâncio 3000, SCN Quadra 06 - Conjunto A - 3º andar - Asa Norte

CEP 70716-900 - Brasília-DF

21.15. A execução de serviços poderá ser realizada fora do horário comercial, quando necessária intervenção no ambiente tecnológica da PREVIC que possa causar indisponibilidade de serviços e sistemas de TI. Neste caso, a data e o horário de execução do serviço deverão ser previamente acordados com a CGTI/DIRAD/PREVIC;

21.16. Os suprimentos (cabos) necessários para a interconexão do equipamentos NGFW, por serem necessários para a interconexão entre a solução adquirida no "Grupo Único" e o ambiente de redes da PREVIC, precisam ser entregues antes do início da execução do serviço de instalação e configuração da Solução de segurança Firewall NGFW e, por este motivo, possuem prazo de entrega menor que o dos itens do "Grupo Único";

21.17. No caso dos equipamentos integrantes do Grupo Único, Item 01 – "Firewall NGFW", estes serão armazenados na CGTI/DIRAD/PREVIC assim que forem recebidos, e não serão desembalados por nenhum funcionário da PREVIC. A desembalagem deverá ser realizada pelo(s) profissional(is) indicado(s) para a execução do serviço de instalação destes equipamentos (Grupo Único – Item 02 – "Serviço de instalação e configuração da solução de Firewall NGFW");

21.18. A entrega dos itens se dará nos seguintes prazos:

Grupo Único - Item 01 –Firewall NGFW, incluindo licenciamento de uso e garantia e suporte técnico de no mínimo 48 meses:

21.19. Os dois dispositivos devem ser entregues simultaneamente, incluindo todos os seus acessórios e peças necessárias para sua correta instalação e configuração, em até 90 (noventa) dias corridos após a assinatura do contrato;

21.20. A ativação das licenças de uso e o início da vigência da garantia e suporte técnico deverá ser realizada durante a execução do serviço de instalação e configuração dos dois dispositivos. Deste modo, seu prazo máximo será o mesmo do Item 02.

Grupo Único - Item 02 - Serviço de instalação e configuração da solução de Firewall NGFW:

21.21. O serviço deverá ser prestado no prazo máximo de 90 (noventa) dias corridos, a contar da data de entrega do Item 01 – Firewall NGFW, sendo este prazo dividido em duas etapas:

21.21.1. *1ª Etapa*: A empresa contratada terá até 30 (quinze) dias corridos, a contar da data de entrega do item 01 – Firewall NGFW, para realizar o planejamento da execução do serviço;

21.21.2. *2ª Etapa*: Após a data de início efetivo da execução do serviço de instalação e configuração da solução, a empresa contratada terá até 60 (sessenta) dias corridos para concluir todas as atividades especificadas.

Grupo Único - Item 03 - Treinamento oficial do Firewall NGFW

21.22. O treinamento deverá ser iniciado em até 14 (quatorze) dias corridos, contados após a conclusão da instalação e configuração da solução e a ativação das licenças (*Item 02*).

21.23. O prazo inicial poderá ser estendido, em caso de indisponibilidade de treinamento oficial no período, desde que a prorrogação seja previamente solicitada à CONTRATANTE, com antecedência mínima de 03 (três) dias úteis, antes da data prevista para início de sua execução;

REQUISITOS DE EFICÁCIA ENERGÉTICA

21.24. Somente serão admitidas as ofertas caso cumpram com os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 170, de 2012 do INMETRO.

21.25. Somente serão admitidas as ofertas de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS(Restriction of Certain Hazardous Substances), tais comomercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)),cádmio (Cd), bifenil polibromados (PBBs), éteres difenilpolibromados (PBDEs).

REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

21.26. A CONTRATADA deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da CONTRATANTE;

21.27. A empresa CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação e Comunicações da PREVIC (Portaria PREVIC nº 204/2013), obrigando-se a manter o sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade da PREVIC aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificava;

21.28. Deverá a empresa CONTRATADA se abster de fornecer qualquer informação da contratante que possa beneficiar outrem ou prejudicar a imagem institucional da PREVIC;

21.29. Não será permitida a vinculação da instituição (isto inclui logomarcas, referências etc.) para fins de publicidade e propaganda;

21.30. Deverá ainda a empresa CONTRATADA pactuar com a PREVIC o compromisso de manutenção de sigilo e ciência das normas de segurança vigentes no órgão, responsabilizando-se por todos os seus colaboradores diretamente envolvidos na prestação dos serviços;

21.31. Não será permitido o uso dos recursos da PREVIC para fins próprios, particulares ou ilícitos. Inclui-se uso de serviço de telefonia, internet ou qualquer outro que venha a incidir gastos ou possibilitar vulnerabilidades, violência, incidentes de segurança física, incidentes de segurança da informação ou crimes, sob pena de responsabilidade civil e criminal;

21.32. Todo e qualquer incidente de segurança ou comportamento atípico que possa a vir a indicar sinais de violação de direitos deve ser comunicado imediatamente à CONTRATANTE.

21.33. A empresa CONTRATADA deverá emitir um "Termo de Sigilo e Responsabilidade", conforme modelo do ANEXO IV - Termo de Sigilo e Responsabilidade (SEI nº 0490870), se comprometendo a não divulgar quaisquer informações, sem a devida autorização prévia (Decreto nº 4.553, de 27 de dezembro de 2002).

REQUISITOS DE MANUTENÇÃO

Grupo Único - Solução de segurança de rede com Firewall de última geração (NGFW)

21.34. Os equipamentos e softwares adquiridos nesse processo deverão possuir garantia do fabricante ou de empresa autorizada pelo fabricante para prestação deste serviço no Brasil, com prazo mínimo de duração de 48 (quarenta e oito) meses, contados a partir do recebimento definitivo da solução, que se dará somente quando de sua completa instalação, configuração e início de operação;

21.35. Durante todo o prazo de vigência a garantia deverá incluir os serviços de manutenção preventiva e corretiva, cuja periodicidade de execução deverá se dar de acordo com as recomendações técnicas da fabricante da solução;

21.36. A manutenção preventiva deverá, no mínimo, incluir:

21.36.1. Atualização de todos os componentes de software da solução, incluindo patches de segurança, firmwares e versões de sistema operacional, seja para corrigir problemas identificados, seja para implementação de melhorias e acesso a novas funcionalidades;

21.36.2. Acesso e atualização de assinaturas de proteção, assim como às bases de dados mantidas pela fabricante, necessárias para o correto e pleno funcionamento da solução, tais como Black e White Lists, assinaturas do tipo "Zero Day", lista de aplicativos confiáveis, etc;

21.36.3. A manutenção corretiva deverá, no mínimo, incluir:

21.36.3.1. Reposição de peças, componentes e equipamentos que apresentarem defeito ou falha de funcionamento, abrangendo todos os itens que compõem a solução, incluindo seus acessórios, módulos de expansão, *transceivers* ou outros equipamentos fornecidos pela CONTRATADA para funcionamento da solução;

21.36.3.2. Em caso de defeitos de fabricação ou a necessidade de substituição hardware, a garantia deverá incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital. O envio da peça ou equipamento de reposição deverá ser realizado, no máximo, até o fim do próximo dia útil após a detecção da falha;

21.36.3.3.

Serviço de Suporte Técnico

21.37. Durante todo o prazo de garantia, a PREVIC poderá solicitar o suporte técnico especializado da fabricante ou empresa oficialmente autorizada pela fabricante a prestar o serviço de suporte no Brasil, sem limitação de quantidade de chamados por período;

21.38. A solicitação de suporte técnico por parte da PREVIC se dará através de abertura de chamado, a ser realizado por, no mínimo, os seguintes meios de comunicação, disponibilizados sempre em idioma português (Brasil):

21.38.1. Ligação telefônica gratuita (0800);

21.38.2. Sistema web (website) com autenticação segura (mínimo usuário e senha de acesso);

21.38.3. E-mail corporativo (em caso de indisponibilidade dos meios anteriormente citados);

21.39. O suporte técnico deverá estar disponível na modalidade "24x7" (24 horas por dia, 7 dias por semana), tanto na modalidade remota quanto presencial (on-site);

21.40. O suporte deverá respeitar, no mínimo, os seguintes tempos de resposta para os níveis de severidade abaixo:

21.40.1. *Crítica*: Significa que a solução ficou inoperante ou ocorreu falha de grande impacto que fez com que a solução parasse de funcionar;

21.40.1.1. Para este nível de severidade o encaminhamento do chamado para atendimento deverá ser imediato, com tempo de resposta de resolução máxima de 60 (sessenta) minutos, a contar da recepção do chamado, sendo preferencialmente prestado na modalidade presencial (on-site). Nestes casos, considerar-se-á como resolução o retorno do funcionamento da solução, seja através de implementação de uma solução definitiva para o incidente, seja por meio de uma solução temporária para colocação emergencial da solução novamente em operação;

21.40.2. *Alta*: Incidentes que não causem a paralisação completa da solução, mas que causem dano moderado em seu funcionamento, tais como: Lentidão elevada, travamentos e interrupções recorrentes, inoperância parcial (alguma funcionalidade ou módulo da solução deixar de funcionar). Para este nível de severidade o tempo máximo de resposta deverá ser de até 02 (duas) horas, em horário comercial, a contar da recepção do chamado, sendo preferencialmente prestado na modalidade presencial (on-site). Nestes casos, considerar-se-á como resolução o restabelecimento do funcionamento normal da solução, seja através de implementação de uma solução definitiva para o incidente, seja por meio de uma solução temporária para colocação emergencial da solução novamente em operação normal;

21.40.3. *Média*: Incidentes que causem redução de performance da solução, tais como lentidão intermitente, erros e falhas em determinados módulos ou recursos e falha no funcionamento de políticas já implementadas; Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

21.40.4. *Baixa ou informativa*: Incidentes de baixo impacto, que não causem falhas ou redução de performance da solução, ou que afetem módulos ou funcionalidades que não sejam consideradas como essenciais para o funcionamento da solução, tais como ferramenta de geração de relatórios, acesso à dashboards, funções administrativas da solução (edição de grupos de administração, por exemplo). Inclui também chamados para esclarecimento de dúvidas sobre a configuração ou funcionamento da solução. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

REQUISITOS DE NEGÓCIO

21.41. A solução auxiliará a PREVIC a preservar a integridade e a confidencialidade dos dados dos quais ela é custodiante, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com a Política de Segurança da Informação e Comunicações da PREVIC (Portaria nº 204/2013)

21.42. A solução deve permitir a rastreabilidade das informações de acesso dos usuários, e seu armazenamento para consulta futura, pelo período mínimo de 01 (um) ano, de acordo com o Marco Civil da Internet – Lei nº 12.965/2014;

21.43. A solução é considerada essencial para a proteção da infraestrutura de TI da autarquia, já que é através dela que a área de tecnologia conseguirá identificar e prevenir o uso ou acesso indevido a seus ativos de TI, e os dados neles armazenados, contribuindo assim para a redução de incidentes de segurança da informação, como por exemplo: vazamento de dados sigilosos ou de acesso restrito, acesso não autorizado a dispositivos e sistemas, acesso ou propagação indevida de conteúdo ilegal (i.e.: pornografia infantil, pirataria) e desvio de finalidade no uso dos ativos de TI da autarquia (i.e.: mineração de criptomoedas, uso dos links de Internet para download de conteúdo alheio às atividades da autarquia, ataques de negação de serviço - DDoS);

21.44. Com a crise pandêmica de COVID-19 iniciada em 2020, mostrou-se essencial para o prosseguimento das atividades de rotina de todas as empresas e órgãos públicos, a possibilidade de os funcionários acessarem remotamente recursos e sistemas hospedados na rede interna corporativa. A solução em questão provê mecanismos de acesso remoto à rede interna, através de clientes VPN e certificação digital, sendo essencial para o provimento deste tipo de recurso aos funcionários da PREVIC;

21.45. Melhorar o nível de qualidade e segurança dos serviços das aplicações internas da PREVIC, agregando funções e recursos que hoje não dispomos em nosso ambiente de redes.

REQUISITOS DE CAPACITAÇÃO

21.46. Considerando que a PREVIC atualmente não possui uma solução de segurança de Firewall NGFW em seu ambiente, não se dispõe hoje de profissionais, sejam servidores públicos ou funcionários terceirizados, com conhecimento técnico suficiente para manter a solução em operação. Por este motivo foi incluído no processo de aquisição o fornecimento de treinamento específico sobre o seu uso e operação, treinamento este que deverá ser conduzido pelo próprio fabricante ou por um representante oficialmente capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais. Os requisitos para este treinamento encontram-se detalhados na especificação técnica do item correspondente (Grupo Único – Item 03 "Treinamento oficial do Firewall NGFW").

REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

21.47. A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;

21.48. Todos os contatos relacionados ao gerenciamento de chamados, tanto para acionamento de garantia quanto para prestação de serviço de suporte técnico, deverão ser realizados em português brasileiro;

21.49. Quando da execução de serviços presenciais de suporte técnico no ambiente da PREVIC, os funcionários da CONTRATADA, ou prestadores de serviço indicados por ela, deverão apresentar identificação funcional prévia, para cadastramento e liberação de acesso; e ao realizar o serviço presencial,

deverão portar crachá identificador com foto;

21.50. Em conformidade com a IN SLTI/MPOG n. 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:

21.50.1. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

21.50.2. Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

21.50.3. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

21.50.4. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

REQUISITOS DE ARQUITETURA TECNOLÓGICA - ESPECIFICAÇÃO TÉCNICA

Compatibilidade com o Ambiente Tecnológico atual da Previc

21.51. A solução, em especial a integrante do Grupo Único – "Solução de segurança de rede com Firewall NGFW", deve ser compatível com o ambiente tecnológico da PREVIC, em especial com sua rede interna:

21.52. Rede LAN formada por:

21.52.1. Switches Core Gigabit Ethernet, com 2 portas 10G SFP+, fabricante Cisco, modelo WS-C2960XR-48TD-I;

21.52.2. Switches Top of Rack (ToR) Gigabit Ethernet, fabricante Cisco, modelos WS-C2960XR-24TS-I;

21.52.3. Switches de Acesso Gigabit Ethernet, fabricante Cisco, modelo SG500;

21.52.4. Access Points, fabricante Cisco, modelo Wireless Aironet 2802I (AIR-AP1852I-Z-K9-BR);

21.53. A conexão entre os switches Core e o roteador da operadora de link de dados (SERPRO – INFOVIA) se dá por meio de conexão de fibra óptica Gigabit, com cabos com conectores do tipo LC-LC. A PREVIC está com um projeto em andamento para substituição deste link de dados por outros dois links, conforme pode ser observado mais detalhadamente na especificação técnica do Item 03 do Grupo Único – Instalação e Configuração da Solução Firewall NGFW;

21.54. A solução atual de Firewall NGFW não é administrada diretamente pela PREVIC, e sim por sua contratada DATAPREV, a saber:

21.54.1. 01 (uma) instância virtual de Firewall NGFW, fabricante Palo Alto, modelo PA-5250, com as seguintes licenças ativas: Threat Prevention; URL-Filtering e WildFire. Os clientes da PREVIC utilizam-se de VPN client-to-site, com conexões SSL. Para tal, utilizam-se de aplicativo cliente VPN "Palo Alto Global Protect". Os certificados digitais são gerados pela CA da solução NGFW gerenciada pela DATAPREV;

21.54.2. Em nosso ambiente interno não utilizamos as regras de Threat Prevention nem de URL-Filtering da solução da Palo Alto. Nestes casos utilizamos as seguintes soluções internas:

21.54.2.1. *Threat Prevention*: BitDefender GravityZone Ultra Suite;

21.54.2.2. *URL-Filtering*: Squid/LightSquid;

21.55. Destas duas pretendemos com esta aquisição substituir o Squid/LightSquid pela solução de URL-Filtering a ser ofertada em conjunto com a solução de Firewall NGFW. Inicialmente não ativaremos o recurso de Threat Prevention da solução objeto desta aquisição, visto que a o BitDefender GravityZone foi adquirido recentemente pela autarquia, e ainda está sob garantia e suporte técnico da fabricante. Por este motivo não solicitamos a ativação desta licença de uso deste recurso no processo atual, solicitamos que o Firewall NGFW a ser fornecido possua todas as funcionalidades de *Threat Prevention* em sua arquitetura, sob possibilidade de posteriormente adquirirmos seu licenciamento em específico ao fim da vigência do contrato com a fornecedora da solução atual – BitDefender GravityZone.

REQUISITOS LEGAIS

21.56. Essa contratação está em conformidade com o Planejamento Estratégico, com o Plano Diretor de Tecnologia da Informação - PDTI da autarquia, com a Estratégia Geral de Tecnologia da Informação, com as disposições normativas da IN n°. 01/2019 - SEGES/ME e em conformidade com a Lei n°. 8.666/93;

21.57. Deverão ser cumpridas, no que couber, as exigências:

21.57.1. Do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;

21.57.2. Do art. 6º da Instrução Normativa MPOG n° 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços;

21.57.3. Da Portaria N° 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO;

21.57.4. Do Decreto nº 7.174/2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração Pública Federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

21.58. Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa n° 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão — SLTI/MPOG e no Decreto n° 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

21.58.1. Quanto à Lei nº 10.520/02, foi observada a instrução em seu art. 1º e Parágrafo único, o qual estabelece que para a aquisição de bens e serviços comuns, poderá ser adotada a licitação na modalidade de pregão. Ainda, em seu parágrafo único, detalha bens e serviços comuns como aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado;

21.58.2. Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa n° 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão — SLTI/MPOG e no Decreto n° 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

21.58.3. A participação no certame poderá ser exclusiva para a microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006.

22. **DAS PROPOSTA DE PREÇOS**

22.1. A proposta da licitante deverá conter a especificação clara e completa da prestação de serviços, obedecida a mesma ordem constante deste Termo de Referência, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento a ter mais de um resultado.

22.2. Não serão aceitas propostas contendo cópia das exigências deste Termo de Referência no lugar da especificação clara e inequívoca dos serviços a serem executados.

22.3. A licitante deverá apresentar planilha de preços, discriminando os valores total e unitário dos serviços contratados.

22.4. A proposta deverá conter declaração da licitante de que se encontra apta a prestar todos os serviços pertinentes ao ofertado e às regras de negócio envolvidas.

22.5. É obrigatório a utilização pelos licitantes do "Modelo de Proposta Comercial" editado pela CONTRATANTE, conforme documento SEI nº 0490871.

23. **DA RESCISÃO CONTRATUAL**

23.1. A inexecução total ou parcial do contrato poderá ensejar a sua rescisão, conforme o disposto nos artigos 77 a 80 da Lei n° 8.666/93;

23.2. Entende-se por inexecução total o não início da prestação dos serviços após 30 dias além do prazo definido;

23.3. Entende-se por inexecução parcial o atraso na prestação dos serviços dentro do prazo previsto;

23.4. Os casos de rescisão contratual serão formalmente motivados nos autos do procedimento, assegurado o contraditório e a ampla defesa;

23.5. A rescisão do contrato poderá ser:

23.5.0.1. Determinada por ato unilateral e escrito da CONTRATANTE nos casos enumerados nos incisos I a XII e XVII do artigo 78 da Lei n.° 8.666/93, mediante notificação por meio de ofício entregue diretamente ou por via postal, com prova de recebimento, sem prejuízo das penalidades previstas no contrato;

23.5.0.2. Amigável, por acordo entre as partes, mediante a assinatura de termo aditivo ao contrato, desde que haja conveniência para a PREVIC;

23.5.0.3. Judicial, nos termos da legislação em vigor.

23.6. A rescisão unilateral ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente;

23.7. Quando a rescisão ocorrer com base nos incisos XII a XVII do artigo 78 da Lei n° 8.666/93, sem que haja culpa da empresa contratada, ela será ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo direito a:

23.7.1. Devolução de garantia, se cabível;

23.7.2. Pagamentos devidos pela execução do contrato até a data da rescisão;

23.8. Pagamento do custo da desmobilização.

24. **DAS ALTERAÇÕES CONTRATUAIS**

24.1. Aceitar nas mesmas condições contratuais os acréscimos ou supressões que se fizerem no objeto do presente contrato, até 25% (vinte e cinco por cento) de seu valor inicial atualizado.

25. **DOS CRITÉRIOS DE HABILITAÇÃO DOS FORNECEDORES**

25.1. Declaração, sob as penalidades cabíveis, da inexistência de fatos impeditivos para a sua habilitação neste certame, na forma do § 2º, do art. 32 da Lei n° 8.666/93, Instrução Normativa-MARE-GM n° 05/95 e Decreto n° 3.722/2001;

25.2. Declaração de que a empresa não utiliza mão-de-obra direta ou indireta de menores, conforme contidas na Lei n° 9.854, de 27 de outubro de 1999, regulamentada pelo Decreto n° 4.358, de 05 de setembro de 2002;

25.3. Não deverá ser admitida a participação de pessoas jurídicas que estejam em uma ou mais das seguintes situações:

25.3.1. Processo de falência, recuperação judicial ou execução patrimonial;

25.3.2. Declaração de inidoneidade por qualquer órgão da Administração Pública Direta ou Indireta, Federal, Estadual ou Municipal, bem como as que estejam punidas com suspensão do direito de contratar ou licitar com a Administração;

25.3.3. Estar reunidas em consórcio ou ser controladoras coligadas ou subsidiárias entre si;

25.3.4. Ter em seu quadro funcional servidor de qualquer órgão ou entidade vinculada ao Ministério da Economia, na condição de sócio, dirigente, responsável técnico, administrador, empregado ou controlador.

26. **DA VISTORIA PARA A LICITAÇÃO**

26.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08:00 horas às 17:00. horas.

26.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

26.3. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

26.4. A vistoria deverá ser agendada pelo e-mail: **previc.sistemas@previc.gov.br**.

26.5. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

26.6. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

27. **ANEXOS**

27.1. ANEXO I - Planilha de Cotações, justificativa e analise crítica (SEI nº 0498430).

27.2. ANEXO II - Modelo de Termo de Recebimento Provisório (SEI nº 0490873);

27.3. ANEXO III - Modelo de Termo de Recebimento Definitivo (SEI nº 0490874);

27.4. ANEXO IV - Termo de Sigilo e Responsabilidade (SEI nº 0490870);

27.5. ANEXO V - Modelo de Proposta Comercial (SEI nº 0490871).

Documento assinado eletronicamente por **ALEXANDRE CRUSCA POZZETTI**, **Integrante Requisitante da Equipe de Planejamento da Contratação**, em 01/11/2022, às 16:44, conforme horário oficial de Brasília, com fundamento no §3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **WENDEL MARTINEZ CARVALHO**, **Fiscal de Contrato - Técnico**, em 01/11/2022, às 16:51, conforme horário oficial de Brasília, com fundamento no §3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **JAMES TAYLOR FARIA CHAVES**, **Coordenador(a)-Geral de Tecnologia da Informação**, em 01/11/2022, às 18:05, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 5º, inciso III, do Decreto nº 10.543, de 13 de novembro de 2020.
Nº de Série do Certificado: 143247065303282720208613527525431667620

A autenticidade deste documento pode ser conferida no site https://sei.previc.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0501778** e o código CRC **8B9B47D8**.

Previdência Complementar, desde 1977 protegendo o futuro de seus participantes.

Criado por alexandre.pozzetti, versão 9 por alexandre.pozzetti em 01/11/2022 16:43:46.