Anexo D - Atestado de Conformidade para Pagamento da Nota Fiscal - Contratação de Serviços (continuados sem mão de obra residente, concessionárias de serviços públicos, locação de imóveis, serviços sob demanda e outros contratos)

LIQUIDAÇÃO DA NOTA FISCAL	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DE EXECUÇÃO DO SERVIÇO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. NA LIQUIDAÇÃO MENSAL DA NOTA FISCAL:			
1.1 O Fiscal de Contrato atestou a conformidade na prestação dos serviços (Caso afirmativo informar o número do marcador do referido documento do respectivo PROAD)			
1.2 Valor da Nota Fiscal corresponde ao valor contratual mensal			
1.3 Verificar se o CNPJ da contratada contido na Nota Fiscal é o mesmo que consta da Nota de Empenho			
1.4 Período da prestação de serviços está correto (sempre corresponde ao mês anterior ao da fatura)			
2. VALIDADE DAS CERTIDÕES NEGATIVAS:			
2.1 Certidão Negativa de Débitos Trabalhistas			
2.2 GRF (FGTS)			
2.3 Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União			
2.4 Certidão Negativa de Débitos Salariais			
2.5 Prova de Regularidade com a Fazenda Estadual			
2.6 Prova de Regularidade com a Fazenda Municipal			

Em _____/_____/_____.

_____

Fiscal administrativo do contrato
(informar nome)

Anexo E - Atestado de Conformidade para Pagamento da Nota Fiscal - Aquisições de bens

LIQUIDAÇÃO DA NOTA FISCAL	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DE EXECUÇÃO DO SERVIÇO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. NA LIQUIDAÇÃO MENSAL DA NOTA FISCAL:			
1.1 Houve recebimento provisório e definitivo da comissão de recebimento ou conforme especificado em contrato			
1.2 Valor da Nota Fiscal corresponde ao valor da nota de empenho			
1.3 Verificar se o CNPJ da contratada contido na Nota Fiscal é o mesmo que consta da Nota de Empenho			
1.4 Data de entrega da mercadoria de acordo com o edital ou contrato.			
2. VALIDADE DAS CERTIDÕES NEGATIVAS:			
2.1 Certidão negativa de débitos trabalhistas			
2.2 GRF (FGTS)			
2.3 Certidão conjunta de débitos relativos aos Tributos Federais e Dívida Ativa			
2.4 Prova de regularidade com a Fazenda Estadual			
2.5 Prova de regularidade com a Fazenda Municipal			

Em _____/_____/______.

____
Fiscal administrativo do contrato
(informar nome)

Anexo F - Termo de Encerramento de Contrato - Serviços (serviços sob demanda; serviços de prestação mensal e continuada (sem mão de obra residente); concessionárias de Serviço Público; locação de imóveis; outros contratos.

TERMO DE ENCERRAMENTO DE CONTRATO	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DA VIGÊNCIA DO CONTRATO:	
GESTOR DO CONTRATO:	

Item	SIM	NÃO	Não se aplica
1. A contratada atendeu e cumpriu as obrigações contratuais durante a sua vigência?			
2. Existe alguma pendência na prestação dos serviços, durante a vigência contratual? (Caso afirmativo relatar no item 6)			
3. Foi relatado ao gestor do contrato alguma pendência ou falta em que a contratada tenha incorrido durante a vigência do contrato? (Caso afirmativo relatar no item 6)			
4. Ocorreu alguma aplicação de penalidade à empresa contratada no período contratual? (Caso afirmativo relatar no item 6)			
5. Na avaliação de desempenho, caso previsto no contrato, a contratada atingiu os limites previstos? (Caso negativo relatar no item 6)			
6. Pendências contratuais:			
7. Outras observações:			
8. Atesto que não há pendências relativas à execução do objeto contratado. A empresa contratada prestou os serviços durante a vigência contratual em estrita observância às determinações, forma e condições previstas no contrato.			

Em _____/_____/_____.

_____
Gestor do contrato
(informar nome/carimbo)

Anexo G - Termo Final de Conformidade – Contratos de serviços continuados (sem mão-de-obra residente, concessionárias de serviços públicos, locação de imóveis e outros contratos continuados)

TERMO FINAL DE CONFORMIDADE	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DA VIGÊNCIA DO CONTRATO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. Existe alguma pendência na validade das certidões negativas? (Caso afirmativo relatar no item 4)			
2. Existem pendências relativas à apresentação da documentação obrigatória da mão-de-obra diretamente envolvida na execução dos serviços? (Caso afirmativo relatar no item 4)			
3. Pendências de Certidões Negativas:			
4. Pendências relativas à documentação obrigatória da mão de obra envolvida:			
5. Atesto que não há pendências relativas à documentação das obrigações trabalhistas e demais obrigações referentes as condições de habilitação e qualificação exigidas, nos termos do inciso XVI, do art. 92, da Lei nº 14.133/2021			
6. Observações:			

Em _____/_____/_____.

_____
Fiscal administrativo do contrato
(informar nome/carimbo)

Anexo H - "Termo de Confidencialidade e de Responsabilidade"

Eu, (nome do profissional contratado), Inscrito no Cadastro de Pessoa Física(CPF) número (número do CPF do profissional), denominado PROFISSIONAL CONTRATADO da empresa (nome da empresa contratada),CNPJ (CNPJ da empresa contratada), denominada EMPREGADORA,declaro estar ciente das disposições abaixo, com as quais concordo plenamente.

O PROFISSIONAL CONTRATADO compromete-se a manter no mais absoluto sigilo e confidencialidade todas as informações do Tribunal Regional do Trabalho da 12ª Região, que, por qualquer meio, direta ou indiretamente,tomar conhecimento em razão dos serviços ora contratados.

O PROFISSIONAL CONTRATADO poderá ter acesso e conhecimento de informações e dados disponíveis do Tribunal Regional do Trabalho da 12ª Região, incluindo informações relativas aos servidores e magistrados,processos administrativos e judiciais, atividades de pesquisa, engenharia e desenvolvimento, tecnologia, pesquisa e métodos de processamento de dados, listas de usuários dos sistemas, dados sobre andamento processual,fornecedores, produtos, processos, listas de autores e réus em ações trabalhistas, informações financeiras, organizacionais, entre outros, devendo manter todas as informações em sigilo absoluto.

O PROFISSIONAL CONTRATADO tem ciência de que o tratamento dos dados a que poderá ter acesso, na forma como é descrito no art. 5º da Lei nº13.709/2018 – LGPD, será realizado exclusivamente nos limites e finalidades previstos no presente contrato. Declaro estar ciente de que, pela inobservância do acima exposto, poderei responder civil, penal e administrativamente, nos termos da lei.

ANDERSON BASTOS 28/08/2025 18:21
ALEX WAGNER ZOLET 28/08/2025 18:34
PAULO SELEME CORREA 28/08/2025 18:49

Anexo I - Especificações Técnicas para Solução de Next Generation Firewall - NGFW - Atualizado em 28/8/2025

Inicialmente, apresenta-se na tabela A1 a lista de produtos previstos para aquisição como solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall

Tabela A1 - Produtos a serem adquiridos

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Unidade (1)**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Cluster
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo IV - Pagamento em parcela única, antecipada.**	Cluster

7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo V - Pagamento em parcela única, antecipada.**	Cluster
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença/ Cluster
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Licença/ Cluster
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VI**	Equip.
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VII**	Equip.
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Equip.
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) na modalidade Software como serviço e Treinamento		
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Usuário
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Aluno
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) **- Tipo I e Tipo IV**	Serviço/ Cluster
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) **- Tipo II e Tipo V**	Serviço/ Cluster
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) **- Tipo III**	Serviço/ Cluster
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de	Serviço/ Equip.

	proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	

(1) Ver definição de cluster abaixo.

Definições importantes:

Cluster: conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Garantia de funcionamento: todos os serviços e atividades necessários para manter a solução em perfeito estado de funcionamento e que não envolvam operação ou configuração, tais como: manutenção corretiva, substituição de peças e componentes, substituição de equipamentos, atualizações de versões de *hardware* e *software*, revisões e/ou distribuições (*releases*) e correções (*patches*) dos programas (*softwares, firmwares, drivers*), etc. Deve incluir ainda o acesso, por meio da Internet, de base de documentos e conhecimentos mantida pela fabricante da solução, contemplando seus manuais de instalação. (responsabilidade do fabricante)

Atualização de assinaturas de proteção: acesso e meios para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa, etc. (responsabilidade do fabricante)

Suporte técnico: todos os serviços e atividades necessários à detecção de problemas de configuração e diagnóstico acerca de vícios e problemas dos produtos a fim de proporcionar o uso adequado e otimizado da solução, incluindo o esclarecimento de dúvidas,sugestão de melhores práticas e orientação técnica da Equipe Técnica do contratante.

A tabela A2 apresenta um compêndio dos prazos previstos na contratação.

Tabela A2 - Prazos da contratação

Item	Descrição da Atividade	Prazo
Itens 1, 2, 3, 4,e 5	Início do Serviço de garantia e atualização de assinaturas de proteção e suporte técnico	Até 10 dias após a comunicação da assinatura do contrato.
Itens 6 e 7	Entrega dos Equipamentos	Até 60 dias corridos contados da comunicação da assinatura do contrato.
	Reunião de Alinhamento Inicial	Em até 15 dias da comunicação da assinatura do contrato.
	Entrega do Plano de Trabalho (Cronograma e Escopo)	Em até 15 dias da reunião de alinhamento inicial.
	Análise do Plano de Trabalho	Em até 10 dias da entrega do Plano de Trabalho.
	Versão final do Plano de Trabalho	Em até 5 dias da resposta do TRT12 sobre a análise do Plano de Trabalho.
	Conclusão da Instalação	Até 90 dias da comunicação da assinatura do contrato.
	Início da Garantia e Suporte	Inicia com o recebimento definitivo do equipamento.
Item 8	Cursos disponíveis para as contratantes	Até 30 dias corridos após a comunicação da assinatura do contrato.
Itens 9 e 10	Fornecimento/Habilitação do serviço	Até 15 dias da solicitação da contratante.
Itens 11, 12 e 13	Entrega dos Equipamentos	De 1 a 20 equipamentos: Até 45 dias contados da comunicação da assinatura do contrato.
		Mais de 20 equipamentos: Até 90 dias contados da comunicação da assinatura do contrato.
	Reunião de Alinhamento Inicial	Em até 15 dias da comunicação da assinatura do contrato.
	Entrega do Plano de Trabalho (Cronograma e Escopo)	Em até 10 dias da reunião de alinhamento inicial.
	Análise do Plano de Trabalho	Em até 5 dias da entrega do Plano de Trabalho.
	Versão final do Plano de Trabalho	Em até 5 dias da resposta do TRT12 sobre a análise do Plano de Trabalho.
	Conclusão da Instalação	De 1 a 20 equipamentos: Até 60 dias da comunicação da assinatura do contrato.
		Mais de 20 equipamentos: Até 90 dias da

		comunicação da assinatura do contrato.
	Início da Garantia e Suporte	Inicia com o recebimento definitivo do equipamento.
Item 14	Disponível, para uso, integrada com a base de identificação de usuários do contratante	Até 60 dias da comunicação da assinatura do contrato.
Item 15	Cursos disponíveis para as contratantes	Até 30 dias corridos após a comunicação da assinatura do contrato.
Itens 16, 17, 18 e 19	Início do serviço	Equipamentos já instalados: Em até 15 dias da comunicação da assinatura do contrato.
		Equipamentos novos: com o recebimento definitivo dos equipamentos.

Antes de iniciar a descrição dos requisitos detalhados para a solução, como a solução de NG Firewall e SASE são complexos, implicam em risco de interrupção da prestação jurisdicional e ainda, em caso de substituição de fornecedor, é necessário obter nova quantidade profissionais terceiros e dos Tribunais para assegurar a continuidade da prestação, a EPC entende que, independente dos demais requisitos, o prazo de vigência de 60 meses é o mais adequado. Este período propiciará uma segurança para as equipes de TIC dos Tribunais, e também permitirá que as empresas amortizem seus investimentos em profissionais qualificados, garantindo maior concorrência, como também preços mais vantajosos considerando os custos de mobilização e desmobilização. Esse prazo também garante que a prestação jurisdicional não sofrerá pela troca de solução de Firewall, no mínimo, por 5 anos.

1. Requisitos para a Solução de NGFW - Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento

Esta seção trata de especificações para os equipamentos que compõem a Solução de alta disponibilidade de Next Generation Firewall, licenças e periféricos necessários para o seu pleno funcionamento nos ambientes *on premises* dos Órgãos públicos participantes.

Como o Firewall é uma solução que identifica e protege, em tempo real, Redes e dispositivos dos contratantes, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente.

O Grupo I foi definido em itens que englobam a renovação do serviço de garantia, atualização de assinaturas de proteção e suporte técnico para os equipamentos que já estão em uso nos tribunais participantes (itens de 1 a 5). Trata também da aquisição de novos equipamentos de NGFW vinculada a contratação conjunta do serviço de garantia, atualização de assinaturas de proteção (itens 6 e 7). O item 8 refere-se a aquisição de treinamento para capacitar os servidores que vão instalar, configurar e operar a solução.

1.1. Especificação dos Equipamentos do Grupo I itens 1 a 5 - dos Tipos I, II e III

Os equipamentos Tipos I, II e III são os equipamentos que foram dimensionados pelo fabricante Checkpoint para substituir os equipamentos que já estavam em operação nos tribunais que participaram da contratação de extensão de garantia Processos Administrativos 3928/2023 e 9665/2023 e que tiveram seus equipamentos antigos declarados como *end-of-life end-of-support* durante a vigência do contrato.

O Equipamento Tipo I é o modelo Quantum 16200 Plus do fabricante Checkpoint.

O Equipamento Tipo II corresponde aos modelos Quantum Force 9700/9800 Plus do fabricante Checkpoint.

O Equipamento Tipo III corresponde aos modelos Quantum 6700/9200 Plus do fabricante Checkpoint.

No caso de troca de equipamentos os novos equipamentos devem ter capacidade idêntica ou superior ao antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior, bem como as especificações do item 1.4 deste Anexo.

O TRT12 ainda não fez a substituição do equipamento antigo 23500. Para este regional a contratação do Item 2 - Serviço de garantia e atualização de assinaturas de proteção e suporte técnico comporta também o fornecimento e

instalação do cluster de equipamentos 9800 Plus em sua capacidade máxima de memória e processamento.

1.2. Grupo I Item 6 do Edital - Aquisição de Cluster de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo IV - Pagamento em parcela única, antecipada.

Cada equipamento que compõe o cluster da solução Next Generation Firewall do Tipo IV deverá atender às seguintes especificações.

1.2.1. Throughput de NGFW mínimo esperado de, no mínimo, 45 Gbps (cinquenta Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas;

1.2.2. Throughput de Threat Prevention de, no mínimo, 35 Gbps (trinta e cinco Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados;

1.2.3. Número de conexões simultâneas de, no mínimo, 7.000.000 (sete milhões);

1.2.4. Número de novas conexões por segundo de, no mínimo, 350.000 (trezentos e cinquenta mil);

1.2.5. Deve suportar VPN IPSec *client-to-site* para no mínimo 6.000 usuários simultâneos;

1.2.6. Mínimo de 2 (dois) Discos Rígidos com capacidade, mínima, por disco de 480 GB (Gigabytes), tipo CFAST/SSD/M.2, operando em redundância, por appliance;

1.2.7. Mínimo de 4 (quatro) Interfaces QSFP28(100Gb)/QSFP+(40Gb) por appliance;

1.2.8. Mínimo de 16 (dezesseis) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance;

1.2.9. Mínimo de 4 (quatro) portas 40Gb preenchidas com respectivo transceiver QSFP+, e adicionalmente, 16 (dezesseis) portas SFP+ 10Gb preenchidas com transceivers SFP+ 10GB-SR, para conexão via cabos de fibra óptica.

1.2.10. Devem ser fornecidos cordões ópticos de, no mínimo, 15m nas mesmas quantidades e compatíveis com os transceivers especificados no item anterior.

Observação: As taxas de transferência (*throughput*) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

1.3. Grupo I Item 7 do Edital - Aquisição de Cluster de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo V - Pagamento em parcela única, antecipada.

Cada equipamento que compõe o cluster da solução Next Generation Firewall do Tipo V deverá atender às seguintes especificações.

1.3.1. Throughput de NGFW mínimo esperado de, no mínimo, 21 Gbps (vinte e um Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas.

1.3.2. Throughput de Threat Prevention de, no mínimo, 20 Gbps (vinte Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados.

1.3.3. Número de conexões simultâneas de, no mínimo, 3.000.000 (três milhões).

1.3.4. Número de novas conexões por segundo de, no mínimo, 240.000 (duzentos e quarenta mil).

1.3.5. Deve suportar VPN IPSec *client-to-site* para no mínimo 3.500 usuários simultâneos.

1.3.6. Mínimo de 2 (dois) Discos Rígidos com capacidade mínima, por disco, de 480 GB (Gigabytes), tipo CFAST/SSD/M.2, operando em redundância, por appliance.

1.3.7. Mínimo de 2 (duas) Interfaces QSFP28(100Gb)/QSFP+(40Gb) por appliance.

1.3.8. Mínimo de 8 (oito) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance.

1.3.9. Mínimo de 4 (quatro) Interfaces UTP 1Gb (Gigabit), tipo RJ-45 por appliance.

1.3.10. Mínimo de 2 (duas) portas 40Gb preenchidas com respectivo transceiver QSFP+, e adicionalmente, 8 (oito) portas SFP+ 10Gb sendo 6 portas preenchidas com transceivers SFP+ 10GB-SR e duas portas preenchidas com 10GB-LR, para conexão via cabos de fibra óptica.

1.3.11. Devem ser fornecidos cordões ópticos de, no mínimo, 15m nas mesmas quantidades e compatíveis com os transceivers especificados no item anterior.

Observação: As taxas de transferência (throughput) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

1.4. Características comuns para os equipamentos que compõem cada Cluster dos Itens 1 a 7 do Grupo I, Tipos I, II, III, IV e V

Os equipamentos que compõem os Clusters dos Itens 1 a 7, do Grupo I, da contratação, deverão ser do mesmo fabricante (Checkpoint), conforme justificativa constante no ETP.

Para os itens 6 e 7 o prazo de entrega é de 60 dias contados da comunicação da assinatura do contrato. Para equipamentos que entrem em *end-of-life*, *end-of-support* e/ou *end-of-sale* o prazo de entrega será de 60 dias a partir da solicitação da contratante.

A seguir serão especificadas as características comuns para os equipamentos referentes ao Grupo I, itens 1 a 7[1] do Edital e Termo de Referência da presente contratação.

1.4.1. O *hardware* para cada equipamento appliance que compõem o cluster deve constar as seguintes características:

a) Deve ser apropriado para o uso em ambiente tropical, com umidade relativa entre 10 e 85% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C;
b) O fluxo do ar refrigerado deve ser recebido pela parte dianteira e dispensado na parte traseira do equipamento;
c) Possuir 2 (duas) fontes de alimentação independentes, redundantes e com capacidade de substituição sem desligar o equipamento (*hot-swappable*), com alimentação nominal de 100~120VAC e 210~230VAC, frequência de funcionamento de 50 ou 60Hz, ou ainda com ajuste automático de tensão e frequência (*auto-ranging*), por appliance;
d) Deverá vir acompanhado de cabos de alimentação para todas as fontes, com, no mínimo, 1,80m, com plugue tripolar 2P+T no padrão ABNT NBR 14136;
e) Deverá vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (rack) padrão EIA-310 com largura de 19” (dezenove polegadas);
f) Possuir no mínimo 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI);
g) Possuir, no mínimo, 1 (uma) interface *out-of-band* dedicada para gerenciamento com capacidade compatível com o tipo do equipamento, I, II e III;

[1] As presentes especificações se aplicarão também caso os equipamentos que estejam abrangidos pelo serviço de suporte e garantia (Itens 1 a 7) precisem ser substituídos.

h) Possuir, no mínimo, 1 (uma) interface para o sincronismo de estados da solução de alta disponibilidade;
i) A interface de sincronismo não precisa, necessariamente, estar rotulada para a finalidade de sincronismo do recurso de alta disponibilidade, sendo aceitável qualquer interface do equipamento. A capacidade da interface deve ser compatível com cada tipo do equipamento, I, II e III;
j) Os equipamentos devem ser fornecidos em sua capacidade máxima de processamento e memória;
k) Possuir, no máximo, 4Us de altura;
l) Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;
m) Possuir certificação de conformidade sustentável de acordo com os padrões EPA (Enviromental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances), WEEE (Waste Electrical and Electronic Equipment) ou EMI Certifications FCC part 15, CE, EN55022, EN55024;
n) Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;
o) Deve informar, no painel de gerência do equipamento, a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede, podendo ser mostrado também no sistema de gerência centralizado, e;
p) Deve informar, no painel de gerência do equipamento, o número de conexões simultâneas e de novas conexões por segundo do equipamento, podendo ser mostrado também no sistema de gerência centralizado.

1.4.2. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale*.

1.4.3. Cada equipamento (appliance) deve oferecer, no mínimo, as seguintes funcionalidades:

a) Suportar os protocolos IPv4 e IPv6;
b) Suportar, no mínimo, 1.024 VLANs no padrão IEEE802.1q;

c) Suportar agregação de links no padrão IEEE802.3ad;
d) Suportar o protocolo DHCP;
e) Suportar o protocolo NTP;
f) Suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e IPv6;
g) Suportar os protocolos RIP, OSPF v2, OSPF v3, BGP v4 (RFC 4271) e BGP v6;
h) Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;
i) Suportar os protocolos SNMP v2c e SNMP v3;
j) Possuir Management Information Base (MIB) própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;
k) Suportar Policy Based Routing (PBR), ou Policy Based Forwarding (PBF), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
l) Suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), camada 2 de rede (*layer*-2), camada 3 de rede (*layer*-3), e suas combinações;
m) Permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS;
n) Possuir funcionalidades de Backup/Restore de sua configuração e políticas de segurança;
o) Permitir o agendamento automático dos Backups, podendo ser realizado pela solução de gerenciamento;
p) Armazenar os Backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP, e;
q) Criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

1.4.4. Funcionalidades de identificação de usuários da solução (appliance):

a) Promover a integração com serviços de diretório LDAP, via serviço de diretórios OpenLDAP e Active Directory, baseados em caracteres da língua

portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos e ameaças;

b) Deve identificar de forma transparente os usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS, e ainda, para LDAP será admissível o uso de agentes nas estações de trabalho e servidores;

c) Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS e proxies internos;

d) Será permitido que a solução de gerenciamento centralizado possua um "appliance virtual" específico para atendimento às necessidades de identificação e autenticação de usuários;

e) Possuir portal de autenticação (*Captive Portal*) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory, servidores RADIUS;

f) O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;

g) Permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;

h) Registrar a identificação do usuário em todos os logs de eventos de acesso e de ameaças gerados pelo equipamento;

i) Registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (*batches*) ou processos de correlação após a ocorrência do evento em questão, e;

j) Deve estar licenciado e permitir a identificação e autenticação de pelo menos 10.000 (dez mil) usuários simultâneos.

1.4.5. Funcionalidades de Firewall por equipamento (appliance)

a) Não deve possuir restrições ao número de máquinas ou usuários protegidos;

b) Suportar a implementação tanto em modo transparente (*layer*-2) quanto em modo gateway (*layer*-3);

c) Suportar inspeção Stateful de tráfegos IPv4 e IPv6;
d) Suportar controle de acesso para pelo menos 90 serviços e protocolos pré-definidos;
e) Suportar os protocolos para transmissão de áudio e vídeo H.323, SIP e MGCP;
f) Suportar os protocolos de Streaming com compressão RTCP, RTMP, RTSP e RTP;
g) Implementar mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT, dependendo da origem, destino ou porta);
h) Permitir transição entre endereços de redes IPv4 e IPv6, permitindo a comunicação entre dispositivos que usam esses protocolos diferentes, por meio de NAT N46 (que permite IPv4 acessar IPv6) e NAT64 (que permite IPv6 acessar IPv4).
i) Permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;
j) Implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*), tanto para IPv4 quanto para IPv6;
k) Implementar mecanismo de captura de pacotes;
l) Identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
m) Suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;
n) Suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período, e suas combinações;
o) Deve ser possível a aplicação de novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas, salvo as conexões atingidas pelas regras alteradas, e;
p) Possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: Endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, status dos flags

"ACK", "SYN" e "FIN" ou sinalizar nos logs que o *Three-way-handshake* não foi concluído com sucesso, ação sobre o pacote (permitido ou negado).

q) A solução deve ser capaz de exportar dados de fluxo de tráfego (flows) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP *Flow Information Export*) ou sFlow ou Netflow;

1.4.6. Funcionalidades de geolocalização por equipamento (*appliance*):

a) Identificar os países de origem e destino de todas as conexões estabelecidas com a Internet através do equipamento;
b) Suportar a atualização automática das listas de geolocalização;
c) Aplicar as atualizações sem perda das conexões ativas;
d) Armazenar as listas de geolocalização no próprio equipamento;
e) Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo também o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;
f) Possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças;

1.4.7. Funcionalidades de controle de acesso à Internet por equipamento (appliance)

a) Prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações, independente de porta e protocolo, e da classificação de URLs;
b) Identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;
c) Identificar se as aplicações estão utilizando sua porta default;
d) Identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;
e) Identificar aplicações criptografadas usando SSL/TLS;
f) Identificar um mínimo de 5.000 (cinco mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, instant messaging, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;

g) Deve ser capaz de identificar, pelo menos, as seguintes aplicações: Torrent, TOR, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger ou Facebook Chat, Google+, Google Chat, Tinder, Instagram, Twitter (X), Linkedin, Dropbox, Google Drive, One Drive, Logmein, TeamViewer, MSRDP, VNC, Ultrasurf, Webex, Zoom;

h) Permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante;

i) Suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações;

j) Permitir aplicar as atualizações sem perda das conexões ativas e das assinaturas customizadas;

k) Armazenar preferencialmente a base de assinaturas no próprio equipamento, aceitando-se também na solução de gerenciamento centralizado;

l) Classificar as aplicações em categorias, tecnologia e fator de risco;

m) Identificar os usuários que estão utilizando as aplicações, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

n) Permitir o bloqueio de aplicações que não estejam utilizando suas portas default;

o) Suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

p) Permitir a utilização ou bloqueio individualizado das aplicações, para determinados usuários ou grupo de usuários;

q) Permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;

r) Permitir o controle de uso de banda de *download* ou *upload* utilizada pelas aplicações (*traffic shaping*) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. Os controles descritos poderão ser aplicados individualmente ou combinados, conforme a necessidade da contratante;

s) Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categorias;

t) Possuir, no mínimo, 60 categorias de URLs, incluindo, mas não se limitando, às seguintes categorias ou suas semelhantes[2]: *adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming média, violence, weapons*;

u) Permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada;

v) Permitir a criação de categorias/listas customizadas;

w) Permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas;

x) Suportar a atualização automática das listas de categorias, e aplicação das atualizações sem perda das conexões ativas e das URLs customizadas;

y) Armazenar as listas de categorias no próprio equipamento ou na solução de gerenciamento centralizado;

z) Deve identificar os usuários que estão acessando as páginas web na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

aa) Suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser implementadas individualmente ou combinados, conforme a necessidade da contratante;

bb) Alertar o usuário quando uma URL for bloqueada por meio da página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;

cc) Permitir o bloqueio e continuação da navegação web (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão “Continuar” ou a inclusão de usuário e senha, para possibilitar o usuário continuar acessando o site), e;

[2] O nome das categorias está em língua inglesa porque trata-se de uma prática comum entre os fabricantes de solução Firewall.

dd) Registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado;

1.4.8. Funcionalidades de prevenção de ameaças por equipamento (appliance):

a) Possuir, no mínimo, funcionalidades de IPS, Antivírus, Anti-Bot, Anti-Malware e Anti-Spyware;
b) Possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque;
c) Possuir proteção contra ataques de negação de serviço DoS e DDoS;
d) Possuir assinaturas para bloqueio de ataques “buffer overflow”;
e) Possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de “troubleshooting” e análise forense;
f) Deve ser capaz de inspecionar tráfego criptografado usando protocolo SSL/TLS;
g) Deve ser capaz de inspecionar integralmente todos os pacotes de dados, sem prejuízo na performance do equipamento, para a seção 1.1 de acordo com os datasheets dos equipamentos já em operação e até os limites indicados nas seções 1.2 e 1.3;
h) Possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (*Common Vulnerabilities and Exposures*);
i) Possibilitar a criação de assinaturas customizadas;
j) Identificar os usuários relacionados aos eventos de IPS na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
k) Possibilitar a criação de políticas de segurança que emitam alertas, sem realizar bloqueios, ao detectar a ocorrência de um ataque específico, identificando sua origem ou destino com base em um endereço IP ou rede CIDR específicos;
l) Permitir a criação de políticas de segurança capazes de bloquear ataques específicos por meio de ações como DROP (descarte) e/ou RESET

(reinicialização da conexão), com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

m) Permitir a criação de exceções ou exclusões para a inspeção de uma determinada assinatura ou grupo de assinaturas, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

n) Registrar todos os eventos de IPS, incluindo o usuário identificado;

o) Identificar e bloquear a comunicação com botnets;

p) Bloquear *malwares* e *spywares*;

q) Inspecionar e bloquear vírus, ao menos, nos seguintes tipos de tráfego: FTP, HTTP, HTTPS e SMTP;

r) Suportar proteção contra vírus em conteúdo HTML e javascript, *software* espião (*spyware*) e *worms*;

s) Suportar a inspeção de vírus em arquivos comprimidos utilizando algoritmo deflate, como o padrão zip, gzip, entre outros;

t) Suportar bloqueio de *download* de pelo menos 50 tipos de arquivos como, arquivos tipo Executáveis, PDF, DLLs, Arquivos de Código, MSI, doc, xls, ppt, entre outros;

u) Suportar a atualização automática das bases de assinaturas para prevenção de ameaças;

v) Suportar aplicação das atualizações de prevenção de ameaças sem reinicialização do equipamento e nem perda das conexões ativas que não sejam afetadas pelas atualizações;

w) Armazenar as bases de assinaturas de prevenção de ameaças no próprio equipamento ou na solução de gerenciamento centralizado;

x) Identificar os usuários relacionados aos eventos de bloqueio relacionados a prevenção de ameaças na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

y) Permitir a criação de políticas de segurança que gerem alertas, sem realizar bloqueios, ao detectar a ocorrência de uma ameaça específica, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

z) Permitir a criação de políticas de segurança que bloqueiem a ocorrência de ameaças específicas com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos, e;

aa) Suportar notificações e alertas sobre ameaças via e-mail, SNMP traps e log de pacotes;

1.4.9. Características de QoS por equipamento (*appliance*):

a) Permitir o controle de tráfego com base nas aplicações com, no mínimo as ações: permitir, negar, agendar o uso, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou cada usuário;
b) Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp);
c) Suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e RTP;
d) Suportar a marcação de pacotes DiffServ;
e) Permitir o monitoramento do uso da priorização de tráfego que as aplicações fazem por bytes, sessões e por usuário.

1.4.10. Características de inspeção SSL/TLS por equipamento (*appliance*):

a) Identificar, descriptografar e analisar o tráfego SSL e TLS 1.2/1.3 tanto em conexões de entrada (*Inbound*) quanto de saída (*Outbound*);
b) Deve permitir a descriptografia da área útil do pacote de dados (*payload*) para fins de controle de acesso à Internet e proteção contra ameaças, e;
c) Permitir a diferenciação de conexões pessoais (Bancos, *Shopping*, etc.) e conexões não pessoais por meio de classificação automática.

1.4.11. Características de VPN por equipamento (*appliance*):

a) Deve disponibilizar **licenciamento** para VPN *site-to-site*, sem limite do número de usuários simultâneos e sem limite do uso de túneis;
b) Suportar VPN *site-to-site* em topologias *Full Meshed* (todos os *gateways* possuem links específicos para todos os demais *gateways*) e também Estrela (*gateways* satélites se comunicam somente com um único *gateway* central);
c) Suportar, pelo menos, criptografias AES-128, AES-256;

d) Suportar integridade de dados com SHA-1 e SHA-256;
e) Suportar o protocolo IKE, fases I e II;
f) Suportar os algoritmos RSA e pelo menos 4 dos grupos Diffie-Hellman groups 1, 2, 5, 14, 15, 16, 17, 18;
g) Suportar NAT-T (NAT Transversal);
h) Deve possuir cliente próprio para instalação nos dispositivos fixos e móveis dos usuários, sem custo adicional e sem limite do número de usuários, e;
i) O cliente de VPN *client-to-site* deve ser compatível, ou suportar, o cliente nativo de pelo menos os seguintes Sistemas Operacionais: Windows 10 e Windows 11, Apple IOS versão 15 ou superior, Android versão 14 ou superior, Mac OS e Linux.
j) Deve permitir conexão VPN *client-to-site* de forma *Clientless*, com autenticação via *browser*, para fechar a VPN através de um portal TLS;
k) Deve suportar atribuição de endereço IP e de DNS dos clientes remotos de VPN;
l) Suportar Autenticação em Dois Fatores (2FA) para todos os usuários de VPN, sendo uma autenticação via usuário e senha, validados por bases LDAP com uso de serviço de diretórios OpenLdap, Active Directory, e base de usuários interna do appliance. Já o segundo fator pode ser Token gerado por e-mail (obrigatoriamente) e também protocolo TOTP e Certificado digital, admite-se ainda que o segundo fator seja implementado com ferramenta de terceiros;
m) Em relação ao certificado digital do item anterior, deverá ser compatível com: certificado emitido por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, e certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
n) O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*single-sign-on*) aos usuários, integrando-se, no mínimo, com as ferramentas de Windows *login* da empresa Microsoft;
o) Permitir criação de políticas para usuários e grupos para tráfego de VPN *client-to-site*;
p) Integrar com serviços diretórios LDAP, via OpenLDAP e Active Directory, para a autenticação de usuários de VPN e também definição de regras de acesso;

q) Permitir a definição de condições específicas para autorizar o acesso remoto às redes internas via VPN *client-to-site*, garantindo maior segurança e controle. Entre essas condições, é necessário, no mínimo, suportar a verificação das versões dos Sistemas Operacionais dos dispositivos dos usuários, a exigência de um software antivírus instalado, ativo e com as definições atualizadas, e a validação das últimas atualizações "KBs" da Microsoft para ambientes Windows. Além disso, o sistema deve permitir a criação de uma lista de equipamentos autorizados, utilizando filtros como MAC-Address ou Hostname, e incluir restrições adicionais baseadas em registros do sistema (*registry*) do Windows. As condições descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

r) Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12[3];

s) Suportar a leitura e verificação de CRLs (*certification revogation lists*), e;

t) Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL/TLS.

1.4.12. Funcionalidades de Prevenção de Perda de Dados (*Data Loss Prevention*)

a) Evitar vazamento de informações em meio digital (*Data Loss Prevention* - DLP), atuando de maneira preventiva por meio do monitoramento de mensagens e arquivos transitados, e;

b) Caso seja identificado algum conteúdo que não deve ser transitado, a solução deve alertar o usuário que este conteúdo é sensível, ou mesmo bloquear o tráfego associado, baseado em filtros de conteúdo definidos pelo contratante.

1.4.13. Características da alta disponibilidade:

[3] O PKCS #12 faz parte da família de padrões chamados Public-Key Cryptography Standards (PKCS) publicados pela RSA Laboratories. Esse padrão de criptografia define um formato de arquivo para armazenar muitos objetos de criptografia como um único arquivo. E tal arquivo é usado para agrupar uma chave privada com seu certificado X.509 ou todos os membros de uma cadeia de confiança.

a) Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo, com sincronismo de estados integrado;
b) Suportar o balanceamento de carga interno na arquitetura ativo/ativo, disponibilizando a capacidade agregada dos dois equipamentos no cluster;
c) Suportar, no mínimo, 2 equipamentos por cluster. No caso de uso de três equipamentos será permitido que um permaneça em *stand by*;
d) Deve sincronizar entre os nós do Cluster todas as configurações recursos necessários para que a solução mantenha o funcionamento pleno em caso de falha de um dos equipamentos, como conexões e sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs, entre outros.
e) Monitorar a falha dos links de comunicação e entre os nós do cluster;
f) Identificar e transferir automaticamente a operação do sistema (procedimento de *failover*) sempre que ocorrer: Falha de um cluster (quando existirem mais de um cluster instalado no contratante), transferindo a carga para o outro em data center distinto. Falha de um dos membros do cluster. Falha de qualquer componente ou processo crítico de um dos membros do cluster. Falha de um dos links de comunicação monitorados, e;
g) Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e interrupções no tráfego.

1.4.14. Funcionalidades para tratamento de ameaças desconhecidas (Zero-Day)

a) Deve contemplar ferramenta compatível com conceito de Sandboxing para prevenção de ataques *zero-day*;
b) Prevenção de ataques por meio do bloqueio efetivo de *malwares* desconhecidos (Dia Zero), oriundos da comunicação Web (HTTP e HTTPS), FTP, SMTP e IMAP/POP3 durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente;
c) O envio de conteúdo para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

d) A funcionalidade de Sandbox deverá ser implementada em nuvem, appliance físico ou em ambiente virtual.
e) Caso a solução de Sandbox seja disponibilizada em ambiente virtual, é de responsabilidade da contratada providenciar servidores e softwares necessários para o funcionamento da ferramenta.
f) Deve ser capaz de enviar para análise, no mínimo, arquivos tipo Executável, PDF, DLLs, Arquivos de Código e MSI;
g) Suportar a análise de arquivos maliciosos em ambiente emulado e controlado com, no mínimo, os sistemas operacionais Windows 10 ou superior, Mac OS X ou superior;
h) Ser capaz de inspecionar e prevenir *malwares* desconhecidos em tráfego criptografado SSL/TLS;
i) Manter a performance sem degradação, independentemente das funcionalidades ativadas. (Ex.: AntiMalware, IPS, URL Filtering, e demais);
j) Geração de relatórios decorrentes das análises de links em Sandbox em caso de identificação de *malwares* e sites hospedeiros de exploits;
k) Deve ser capaz de classificar sites falsos, e atualizar a base do filtro URL da solução, e;
l) Deve prover análise em tempo real de páginas maliciosas e dessa forma, permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução.

1.4.15. Administração e Gerência centralizada da solução de Next Generation Firewall.

1.4.15.1. A solução centralizada deverá gerenciar, de forma integrada, todos os equipamentos dos Grupos I e II que terão a renovação de garantia estendida ou que o órgão vier a adquirir, em qualquer combinação e quantidade dentro dos limites registrados.

1.4.15.2. A solução de gerenciamento centralizado deverá ser composta por, pelo menos, 1 (um) “appliance virtual” – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (*Distributed Management Task Force*), ou sistema operacional desenvolvido pelo próprio fabricante da solução de

gerenciamento que possa ser instalado e executado em ambiente virtual.

1.4.15.3. Será instalada em ambiente de virtualização e *hardware* de propriedade do contratante.

1.4.15.4. A Licença de Software para administração / gerência deve estar disponível, para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

1.4.15.5. A solução de gerência terá atualização e suporte pelo período de 60 meses a contar do seu recebimento definitivo. Deverá permitir sua utilização por tempo indeterminado, em sua última versão disponível na data do encerramento do período de 60 meses.

1.4.15.6. A solução de gerência deverá ser separada dos *gateways* de segurança, que irão gerenciar políticas de segurança de todos os *Firewalls* e funcionalidades solicitadas neste documento.

1.4.15.7. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

1.4.15.8. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos gerenciados via plataforma de segurança.

1.4.15.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

1.4.15.10. Suportar acesso via SSH para gerência, via cliente do próprio fabricante ou WEB (HTTPS).

1.4.15.11. O gerenciamento deve permitir/possuir monitoramento de logs, ferramentas de investigação de logs e acesso concorrente de administradores via contas diferentes.

1.4.15.12. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comando

1.4.15.13. A solução deve suportar a criação de regras com agendamento personalizado, permitindo configurar datas e horários de início e término para o uso de cada regra.

1.4.15.14. Suportar backup das configurações e reversão (*rollback)* de configuração, pelo menos, para a última configuração salva.

1.4.15.15. Suportar validação de regras antes da aplicação.

1.4.15.16. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras já existentes (*shadowing*).

1.4.15.17. Permitir a visualização dos logs em tempo real de uma regra específica, diretamente na mesma tela de configuração da regra selecionada, garantindo uma experiência integrada e facilitando o monitoramento e a análise imediata do tráfego associado.

1.4.15.18. Possibilitar a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo.

1.4.15.19. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

1.4.15.20. Permitir a criação de certificados digitais para autenticação de usuários.

1.4.15.21. Geração de relatórios de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança. Deve permitir apresentar eventos em um

único portal (*dashboard*). Também devem existir relatórios e telas de apresentação onde sejam apresentados os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, *Anti-Malware* e *Sandboxing*).

1.4.15.22. Permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.4.15.23. Permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0.

1.4.15.24. Permitir que os administradores consigam revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.4.15.25. Permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

1.4.15.26. Registrar logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

1.4.15.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados.

1.4.15.28. Permitir a criação de relatórios personalizados.

1.4.15.29. Permitir criar relatórios com o resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais *hosts* por número de ameaças identificadas, atividades de usuários específicos e grupos de usuários do AD/LDAP. Os relatórios de usuários e grupos devem incluir as aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e *Anti-Malware*) de rede vinculadas a este tráfego.

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, *Anti-Malware*), e URLs que passaram pela solução.

1.4.15.30. Possibilitar exportação dos logs em formatos CSV ou TXT.

1.4.15.31. Aplicar separadamente proteções relacionadas a ameaças e regras de acesso.

1.4.15.32. Para evitar erros na alteração de políticas, a solução deve combinar configuração de políticas e análise de logs em um único painel.

1.4.15.33. O visualizador de log deve ter um recurso de pesquisa.

1.4.15.34. Possibilitar a geração de relatórios de eventos no formato PDF ou HTML.

1.4.15.35. Possibilitar rotação do log.

1.4.15.36. O gerenciamento centralizado deverá ser entregue como appliance virtual em formato compatível/homologado com tecnologia VMWare ESXi.

1.4.15.37. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes físicos (*on premises*), virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI).

1.4.15.38. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações por meio de RestAPI.

1.4.15.39. Consolidar logs e relatórios de todos os dispositivos administrados pela gerência integrada.

1.4.15.40. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

1.4.15.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real.

1.4.15.42. Nas opções de Drill-Down deve ser possível identificar os acessos específicos de cada usuário.

1.4.15.43. Permitir que os relatórios possam ser salvos, enviados por e-mail e impressos.

1.4.15.44. Deve permitir a criação de filtros na visualização on-line dos relatórios com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

1.4.15.45. Permitir visualização via painel de gerência on-line da quantidade de tráfego utilizado de aplicações e navegação para permitir análise avançada de incidentes.

1.4.15.46. Gerar relatório dos eventos de ataque de forma completamente visual, contendo, no mínimo, gráficos de consumo de banda utilizado pelos ataques e quantidade de eventos de segurança gerados e também eventos de segurança protegidos.

1.4.15.47. Permitir a integração com servidores de autenticação por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS.

1.4.15.48. Criar certificados digitais para acesso dos usuários VPN.

1.4.15.49. Criar certificados digitais para VPNs *Site-to-Site*.

1.4.15.50. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplada a sua maior capacidade ou a capacidade de criação de certificados deve ser ilimitada.

1.4.15.51. Permitir criação de políticas de acesso de usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP e Microsoft Active Directory, de forma que os usuários sejam reconhecidos de forma transparente.

1.4.15.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças classificadas por origens e destinos do tráfego de dados.

1.4.15.53. Possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado, permitindo a procura correlacionada de logs em uma única tela, como por exemplo: pesquisar logs de Antivírus e navegação web simultaneamente na mesma consulta (*query* de pesquisa).

1.4.15.54. O relatório das emulações (*sandboxing*) deve conter deve conter um dos seguintes conjuntos de informações:

a) Print screen dos arquivos emulados, todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações individualizado para cada SO emulado, ou;
b) Tipo do arquivo, tamanho do arquivo, nome do arquivo, hash do arquivo, usuário que o recebeu, o veredito (um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema).

1.4.15.55. Possibilitar a procura por IPs e redes, de forma que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

1.4.15.56. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.4.15.57. Capacidade de personalização de gráficos com os dados dos logs, como barra, linha e tabela;

1.4.15.58. Permitir a criação de painéis (*dashboards*) customizados para visualização do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.4.15.59. Possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema e dos componentes gerenciados por ele, contendo, no mínimo, licenças ativas, utilização de memória, utilização de discos e uso de CPUs;

1.4.15.60. Ser capaz de correlacionar eventos de todas as suas fontes de log em tempo real;

1.4.15.61. Fornecer conteúdo de correlação de eventos pré-definido organizado por categoria;

1.4.15.62. Monitorar alterações, análise e otimização de regras de políticas de segurança;

1.4.15.63. Possibilitar a verificação de regras de acesso por meio de uma consulta de origem, destino e serviço, a solução também deve apresentar se o tráfego está permitido, bloqueado ou parcialmente permitido/bloqueado, demonstrando os dispositivos no caminho, roteamento e interfaces;

1.4.15.64. Deve apresentar relatórios de otimização de regras e objetos, no mínimo, contendo as seguintes informações:

a) Regras não usadas;
b) Regras cobertas
c) Consolidar regras
d) Regras desabilitadas
e) Regras temporárias (definição de data e hora de funcionamento)
f) Regras mais usadas;

g) Última vez que uma regra foi usada;
h) Objetos duplicados;
i) Objetos vazios, e;
j) Serviços duplicados.

1.4.15.65. Permitir a monitoração de itens de configuração do sistema operacional dos dispositivos gerenciados;

1.4.15.66. Enviar alertas configuráveis sobre regras a expirar;

1.4.15.67. Emitir alertas em caso de alterações de configuração que não estão em conformidade com os padrões e políticas corporativas vigentes;

1.4.15.68. Realizar a comparação das configurações de um mesmo ou entre diferentes dispositivos;

1.4.15.69. Permitir o agendamento para a geração de relatórios dos dispositivos gerenciados;

1.4.15.70. Ser capaz de fornecer lista de usuários de VPN dos dispositivos gerenciados, no mínimo, baseados nos seguintes critérios:

a) Data de criação;
b) Grupos de usuários;
c) Métodos de autenticação dos usuários, e
d) Data de expiração dos usuários.

1.4.15.71. A comunicação entre a solução e os dispositivos de segurança gerenciados deve ser autenticada e criptografada;

1.4.15.72. Capacidade de comparar a base de regras do firewall com baselines padrão de mercado e fornecer um relatório de conformidade com o padrão utilizado na comparação;

1.4.15.73. Capacidade de migrar as regras e políticas dos dispositivos instalados nos contratantes para dispositivos substitutos, mesmo que de modelo e fabricante diferentes, utilizando a gerência ou ferramenta de terceiros.

1.4.15.74. Qualquer alteração na configuração dos dispositivos deve ser identificada automaticamente contendo as seguintes informações:

a) Qual foi a alteração;
b) Quem efetuou a alteração;
c) A data e hora da alteração;
d) Cada alteração nos dispositivos, deve ser identificado, no mínimo:
e) Alterações nas Regras (Criação, Remoção, Modificação);
f) Alteração nos Objetos de Redes e Serviços;
g) Alterações de Rotas ou Interfaces, e;
h) Visibilidade de toda alteração de configuração nos dispositivos.

1.4.15.75. O sistema deve realizar validação contínua das políticas e controles de segurança por meio de simulações em ambiente real; Deve possuir suporte de integração com plataformas de SIEM, permitindo análise e correlação de eventos em tempo real;

1.4.15.76. Possuir uma biblioteca de ameaças atualizada diariamente, contendo, no mínimo, 15.000 técnicas de táticas e procedimentos (TTPs) e 3.000 tipos de ameaças, incluindo *exploits* de vulnerabilidades e ataques APTs;

1.4.15.77. Possibilitar geração de relatórios personalizados que evidenciem mudanças na postura de segurança ao longo do tempo, incluindo recomendações específicas para mitigações baseadas no fornecedor e no cenário da ameaça;

1.4.15.78. Compatibilidade com ferramentas de segurança de rede, incluindo integração com plataformas de mercado para gestão de segurança;

1.14.16. Licenciamento das funcionalidades especificadas no Edital para os equipamentos (appliances)

Todas as funcionalidades descritas para a solução de Next Generation Firewall devem estar devidamente licenciadas e disponíveis para uso durante todo o período do contrato. Sendo elas, *Application Control*, identificação de usuários, *firewall*, geolocalização, navegação internet e inspeção de tráfego SSL/TLS, IPS, VPN, ameaças *zero-day, sandboxing, logging*, gerência centralizada, SD-WAN (caso contratada via Itens 10 e 11 deste Edital) e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.14.17. Instalação do Cluster Grupo I itens 1 a 7

Os novos equipamentos adquiridos ou os equipamentos a serem substituídos por estarem em *end-of-support* deverão ser instalados seguindo o planejamento definido nesta subseção.

1.14.17.1. Requisitos Gerais da Instalação

1.14.17.1.1. Caberá à contratada todo o processo de planejamento, a instalação, a configuração, os testes, a migração e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos, como switchs, roteadores, equipamentos servidores, entre outros.

1.14.17.1.2. O processo de instalação, configuração, testes e migração deve acontecer em até 90 dias corridos após a comunicação da assinatura do contrato no caso de aquisição de novos equipamentos. Nos casos onde for decretado *end-of-support* para equipamentos dentro do prazo de vigência do contrato de garantia, o processo de instalação, configuração, testes e migração do equipamento a ser substituído deve ter como marco inicial a notificação da empresa sobre a necessidade de troca dos equipamentos.

1.14.17.1.3. A atividade de janela para efetiva entrada em produção do novo equipamento da solução de Firewall deverá ser agendada pelo contratante.

1.4.17.1.4. A contratada deverá realizar uma avaliação preliminar do ambiente de TI da contratante, incluindo uma análise da infraestrutura atual, para identificar quaisquer pré-requisitos ou necessidades de adaptação antes da implementação.

1.4.17.1.5. A Instalação terá quatro marcos: Reunião de Alinhamento Inicial; Entrega do Plano de Trabalho; Execução da instalação, migração e testes; Efetiva entrada em produção do novo equipamento.

1.4.17.1.6. A contratada é responsável pela instalação completa e configuração dos equipamentos e *software*, garantindo que estes estejam operacionais e otimizados para o ambiente da contratante.

1.4.17.1.7. A contratada deverá manter um canal de comunicação com a contratante durante a instalação/migração.

1.4.17.2. Requisitos de Instalação/migração

1.4.17.2.1. A instalação/migração não deve interromper as operações diárias da contratante sem agendamentos prévios e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

1.4.17.2.2. Eventuais necessidades de interrupção devem ser autorizadas e agendadas com a Administração do Órgão, com possibilidade de serem realizadas em finais de semana.

1.4.17.2.3. A instalação/migração envolverá as seguintes atividades:

a) Reunião de Alinhamento Inicial:
   i) A reunião de alinhamento inicial deverá ocorrer em até 15 dias da comunicação da assinatura do contrato.
   ii) Neste momento, a contratante deverá informar se a contratada deverá realizar a migração das configurações de solução de Firewall já instaladas, ou se prefere instalar uma configuração totalmente nova.

b) Entrega do Plano de Trabalho (Cronograma e Escopo):

i) O Plano de Trabalho deverá contemplar ao menos: Declaração de Escopo, Matriz RACI, Cronograma (datas da Instalação Física e Lógica e Efetiva entrada em produção do novo equipamento), Recursos Humanos, procedimentos e testes a serem realizados no final da instalação

ii) O documento em PDF deverá ser enviado para o Gestor e o Fiscal Técnico em até 15 dias da reunião de alinhamento inicial.

iii) A contratante terá 10 dias para analisar o documento, realizando, por e-mail, as solicitações que entender cabíveis.

iv) Sendo necessárias alterações a contratada terá 5 dias para apresentar, também por e-mail, a versão final.

c) Execução da instalação, migração e testes:

i) Esta etapa terá início após a entrega dos equipamentos e deverá ser concluída em até 90 dias da comunicação da assinatura do contrato.

ii) A contratada deverá disponibilizar o acompanhamento "on site" durante a instalação de, pelo menos, um especialista, certificado pelo fabricante do equipamento, para ser responsável pela execução da instalação, migração e testes, pelo tempo necessário, com, no mínimo, 40 horas de trabalho (sem contar a uma hora diária de almoço), sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h;

iii) Caso a instalação não seja concluída no período citado no item anterior, deverá haver um especialista técnico, em esquema de atendimento remoto, sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h, que poderá ser acionado via telefone celular, até o recebimento definitivo do serviço de instalação.

iv) A instalação física compreende a fixação, conexão de cabos de energia e lógicos de forma a possibilitar o funcionamento da solução de Cluster nas dependências do contratante

v) Todas as conexões elétricas e lógicas utilizadas deverão ter seus cabos (rede, óticos e/ou elétricos) identificados (etiquetagem), sendo a

contratada responsável pelo fornecimento e impressão das etiquetas e materiais necessários para a organização, como presilhas, velcros, entre outros.

vi) A instalação lógica se inicia com a preparação dos equipamentos com sua última versão estável com seus patches (releases) mais recentes instalados. Não serão aceitas funcionalidades que estejam executando em builds não-estáveis (alpha, beta etc.) ou modificações personalizadas diretamente em código.

vii) Quando solicitado pela contratante na reunião de alinhamento, a instalação compreenderá a migração das configurações e regras existentes no ambiente atual do contratante, suportado por um cluster de firewalls que pode ser de fabricante distinto da solução ofertada, assim como as demais configurações de segurança e disponibilidade.

viii) Transferência das configurações da solução atual para o novo equipamento, além de criação de novas regras e políticas que se mostrarem necessárias. Preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo, em uma rede virtual (VLAN) distinta do ambiente produtivo para que não haja influência na operação;

ix) Validação dos dados criados nos novos equipamentos comparando-os com os dados dos equipamentos legados, garantindo a integridade das configurações;

x) Configuração lógica do equipamento para comunicação deste com a rede de dados da contratante.

xi) Realização dos testes especificados no item 1.4.17.2.4.

xii) Ao final da etapa de Execução da instalação, migração e testes, deverá ser enviado, para o e-mail do Gestor e do fiscal técnico, o Arquivo de configurações dos novos equipamentos.

d) Efetiva Entrada em Produção do Novo Equipamento:

i) Esta data deverá ser alinhada e autorizada pelo Gestor do contrato.

1.4.17.2.4. Testes

No intuito de validar o funcionamento das configurações realizadas, incluindo migração, devem ser realizados, no mínimo, os seguintes testes:

a) Deverá ser feito, no mínimo, dois tipos de acesso a partir da rede interna para a rede Servidores e para a rede DMZ.
   i) Acesso 1: utilizando protocolo https e sendo liberado o acesso, e;
   ii) Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ é liberado para a rede servidores;

b) Deverá ser feito um tipo de acesso externo com origem em um cliente VPN com destino a rede servidores.

c) Deverá ser exibido na console de gerência os registros que demonstrem:
   i) O horário da aplicação das últimas políticas;
   ii) A mudança realizada para bloqueio do Facebook;
   iii) O horário da mudança, e;
   iv) O administrador que realizou a mudança;

d) Deve ser desligada a PDU do nó ativo;
   i) Verificar se o nó passivo assumiu as operações com RTO[4]=0 (zero);
   ii) Ligar o appliance do nó ativo, e;
   iii) O nó ativo deverá assumir o controle das operações.

1.5. Características comuns para - Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - Grupo I Itens 1 a 7 (Equipamentos Tipo I, II, III, IV e V)

Entende-se apropriado apresentar um único conjunto de especificações para os serviços de garantia do Grupo itens 1 a 7, porque a única alteração entre estes itens é a capacidade do produto em que o serviço será aplicado.

[4] RTO (Recovery Time Objective) é a sigla em inglês para Objetivo de Tempo de Recuperação. É uma métrica que define o tempo máximo que um sistema pode ficar inativo após uma interrupção

Cada unidade do serviço atenderá um cluster de equipamentos.

Assim, para os Firewalls dos Tipos I, II e III (Itens 1 a 5) que terão a assinatura por 60 meses adicionais e os Tipos IV e V (itens 6 e 7) cuja contratação do serviço de garantia por 60 meses está vinculada a aquisição dos novos equipamentos, a contratada deve oferecer, no mínimo, os serviços de garantia e atualização conforme segue.

1.5.1. Os serviços de assistência técnica “on-site”, realizados pela contratada ou autorizados pela mesma mediante declaração expressa, deverão ser prestados nos municípios das sedes dos Tribunais, nas Capitais e suas respectivas regiões metropolitanas.

1.5.2. Todos os custos e encargos relacionados à execução dos serviços de garantia e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da contratada.

1.5.3. A contratada deverá prestar serviço de manutenção e suporte técnico ao longo da vigência do contrato destinado a:

a) Restabelecimento de serviços interrompidos ou degradados;
b) Solução de problemas de configuração e falhas técnicas nos serviços;
c) Esclarecimentos de dúvidas sobre configurações e utilização dos serviços, e;
d) Implementação de novas funcionalidades.

1.5.4. A garantia e serviço de assistência técnica do produto ofertados deverão ser do Fabricante.

1.5.5. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças, componentes e acessórios que se apresentem defeituosos de acordo com os manuais e normas técnicas específicas para os equipamentos. No caso do modelo do equipamento haver sido descontinuado, um similar será aceito, desde que possua as características técnicas iguais ou superiores às exigidas no Edital.

1.5.6. O serviço de garantia deverá abranger os defeitos de hardware e de software, através de manutenção preventiva ou corretiva, incluindo a substituição de peças, partes, componentes e acessórios, sem representar quaisquer ônus para o Tribunal.

1.5.7. Os equipamentos devem contar com garantia de funcionamento, atualização de assinaturas de proteção e assistência técnica do fabricante, além do suporte técnico local e remoto pela Contratada, 24x7 (vinte e quatro horas por dia, sete dias na semana), pelo prazo de 60 (sessenta) meses.

1.5.8. Todas as partes e peças deverão ser substituídas pelos serviços de garantia, através de funcionários habilitados e credenciados para tal. Não serão aceitos o envio de peças/equipamentos pelos Correios, para que haja substituição por parte do Contratante. O Contratante não se responsabiliza por quaisquer danos aos equipamentos, que possam vir a ocorrer caso seja utilizada a prática de postagem pelos Correios.

1.5.9. Toda e qualquer substituição de peças e componentes deverá ser acompanhada por funcionário designado pelo Contratante, que autorizará a substituição das peças e componentes, os quais deverão ser novos e originais.

1.5.10. Em caso de necessidade de nova instalação e/ou configuração os serviços deverão ser realizados pela Contratada ou pelo Fabricante, por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. Se necessário, a documentação original ou "as built" deverão ser atualizados pela contratada.

1.5.11. Os serviços de suporte que porventura implicarem na necessidade de desligamento de outros equipamentos, como servidores, storage, links, etc., deverão ser executados, preferencialmente, em horários fora do expediente, podendo inclusive ocorrer em finais de semana ou feriados, a critério do contratante.

1.5.12. A contratada deverá ter acesso completo aos Fóruns de Produtos do fabricante durante a vigência do contrato;

1.5.13. A contratada deverá ter acesso à base de conhecimento de suporte online do fabricante durante a vigência do contrato;

1.5.14. A contratada deverá ter cadastrado em portal do fabricante para *download* de *firmwares*, *patches* e *softwares* que fazem parte ou complementam a solução;

1.5.15. Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela contratada e os últimos níveis pelo fabricante.

1.5.16. Níveis de Gravidade dos chamados para definição de tempos de atendimento.

1.5.16.1. Gravidade 1

a) Um erro com impacto direto na segurança do produto;
b) Um erro isolado no software ou dispositivo em um ambiente de produção que torna o produto inoperante; por exemplo, impacto crítico no sistema, queda do sistema;
c) Um defeito relatado no produto em um ambiente de produção, que não pode ser razoavelmente contornado, em que haja uma condição de emergência que restrinja significativamente o uso, como por exemplo, PJe fora do ar por problemas de configuração do sistema Firewall;
d) Produto para de executar as funções de negócios necessárias, como interrupção no acesso à Internet via rede Interna; ou
e) Incapacidade de usar o equipamento ou qualquer outro impacto crítico na operação do Firewall que exija uma solução imediata.

1.5.16.2. Gravidade 2

a) Um erro isolado no software ou no equipamento que degrade substancialmente o desempenho dos sistemas de TIC que dependem dele,

por exemplo, Sistema PJe acessível mas com performance muito degradada, lento e/ou com funcionalidades limitadas devido problemas de Firewall;

b) Um defeito que restringe o uso de um ou mais recursos mas não chega a afetar completamente o uso do Firewall, ou;

c) A utilização de uma função importante não está disponível e as operações são gravemente impactadas; por exemplo, lentidão nos sistemas da rede interna acessados via Internet.

1.5.16.3. Gravidade 3

a) Um erro isolado no Firewall que causa apenas um impacto moderado no uso do produto; por exemplo, Demora no login de sistemas via Internet, demora em algumas operações específicas do PJe, intermitência entre lentidão e desempenho satisfatório;

b) Um defeito que restringe o uso de um ou mais recursos do produto licenciado mas pode ser facilmente contornado, como parada do funcionamento da navegação Internet via rede Interna com autenticação de usuário e senha, mas que pode funcionar normalmente se liberada a autenticação até o problema ser resolvido, ou;

c) Um erro que pode causar algumas restrições funcionais, mas não tem um impacto crítico ou severo nas operações, como parada no acesso a sites de compra on-line.

1.5.16.4. Tempos de atendimento

Os tempos de atendimento estão descritos na tabela TR3, conforme segue.

Tabela A3 - Tempos de atendimento o Serviço de atualização de garantia

Serviço	**Tempo e condições**
Regime do atendimento	24x7
Tempo de resposta comprometido para problemas de Gravidade 1 (1)	30 minutos
Tempo de resposta comprometido para	Gravidade 2 - 2 horas

problemas de Gravidade 2 e 3 (1)	Gravidade 3 - 4 horas
Remessa de equipamentos em caso de necessidade de troca (RMA)	Próximo voo de saída/entrega expressa (quando aplicável) ou remessa no mesmo dia útil (2)

(1) Entende-se cumpridos os 30 minutos de tempo de atendimento caso haja comunicação em tempo real (chat, telefone). (2) Equipamentos são enviados durante o horário comercial normal e podem chegar fora do horário comercial.

1.5.17. A Contratada deverá providenciar o deslocamento de peças ou equipamentos para substituição bem como seu retorno sem qualquer ônus à contratante.

1.5.18. Todas as peças ou componentes utilizados/substituídos nos reparos deverão ser originais do fabricante, sem uso anterior e possuir, no mínimo, o mesmo desempenho e as mesmas garantias daqueles originalmente fornecidos.

1.5.19. Em caso de novos equipamentos, os mesmos devem ser compatíveis com os demais ativos de data center de cada Órgão participante. Ficará a cargo da contratada a verificação de compatibilidade antes da efetivação da reposição. Caso o sistema ofertado não tenha sua compatibilidade verificada, o correto funcionamento de todas as funcionalidades do sistema ofertado será de inteira responsabilidade da contratada, que deverá empreender todos os esforços necessários para entregar o sistema em pleno funcionamento, sob pena de arcar com as multas contratuais relativas a quebra de contrato.

1.5.20. Caso o equipamento não possa ser reparado dentro do prazo previsto, deverá ser providenciada pela contratada a instalação, em caráter provisório, de equipamento equivalente ou de configuração superior até que seja sanado o defeito do equipamento em reparo.

1.5.21. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do contratante, o equipamento avariado poderá ser removido para o centro de atendimento da contratada. A contratada deverá fazer a justificativa por escrito relacionando os problemas apresentados que deverá ser apresentada ao setor competente do contratante que fará o aceite e providenciará a

autorização de saída do equipamento, desde que o mesmo seja substituído por outro equivalente ou de superior configuração, durante o período de reparo. O equipamento retirado para reparo deverá ser devolvido no prazo de 5 (cinco) dias úteis contados a partir da sua retirada.

1.5.22. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao contratante.

1.5.23. A contratada deverá substituir o equipamento já instalado, por um novo e de primeiro uso, no prazo máximo de 2 (dois) dias corridos, na hipótese do mesmo equipamento apresentar defeito por 2 (duas) ou mais vezes dentro de um período de 20 (vinte) dias corridos.

1.5.24. Caso os equipamentos cobertos pelo serviço de garantia, atualização de assinaturas de proteção e suporte técnico vierem a ser declarados pelo fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale* com essas datas terminando antes do período de vigência do contrato, os mesmos deverão ser substituídos pelos novos equipamentos indicados pelo fabricante em seu site, esses equipamentos devem ter capacidade idêntica ou superior ao equipamento antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior.

1.5.25. Os serviços dependentes de atualização pela Internet e cujas licenças serão vinculadas à vigência do contrato, são: controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), prevenção de perda de dados (data loss prevention) e postura dos endpoints, e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.5.26. O licenciamento deverá permitir a utilização da solução, por tempo indeterminado, em sua última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões.

1.5.27. Vigência e início do contrato

Para equipamentos já instalados a garantia deve iniciar em até 10 dias após a comunicação da assinatura do contrato. Para novos equipamentos os serviços de garantia e atualização terão vigência de 60 meses com início a partir da emissão do termo de recebimento definitivo da ativação de licenças vinculadas aos equipamentos Firewall Tipos I, II e III, IV e V (Grupo I Itens 1 a 7 do Edital).

1.6. Grupo I item 8 - Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall

1.6.1. O Treinamento fornecerá uma compreensão dos conceitos básicos e das habilidades necessárias para configurar minimamente um sistema de Firewall.

1.6.2. O curso de nível básico, item 8 deste Edital, abrangerá configurações de políticas de Segurança, gerenciamento e monitoramento de uma rede segura, atualizações e configurações de um gateway de segurança e implementação de uma rede virtual privada.

1.6.3. O Treinamento deverá ser fornecido na forma de voucher[5] individual para treinamento oficial do fabricante;

1.6.4. A duração do treinamento deve ser de, no mínimo, 24 horas aula distribuídas em até 6 dias úteis, com um máximo de 8 horas aula por dia;

1.6.5. O treinamento e o material didático deverão ser em língua portuguesa;

1.6.6. O treinamento deverá ocorrer no período entre 8h00 e 18h00;

1.6.7. As turmas deverão ter até 15 alunos;

1.6.8. O treinamento deverá ser realizado de forma on-line e síncrona;

[5] Para o objeto definido nos itens 8 e 15 da presente contratação, o Voucher é um vale, ou valor em crédito, para realização de Treinamento Introdutório dentro de plataforma de educação à distância, que deve ser disponibilizado em turmas regulares dentro de um período específico de tempo, no caso, até 12 meses após a comunicação da assinatura do contrato.

1.6.9. Deverá ser fornecido certificado de conclusão do treinamento em até 10 dias após sua conclusão, contendo:

a) Nome do Aluno;
b) Nome do Curso;
c) Carga horária do Curso;
d) Data de início e fim do Curso;
e) Nome e assinatura do emissor, e;
f) Linguagem em Português do Brasil. Mesmos os certificados oficiais do fabricante.

1.6.10. As turmas para os cursos devem estar disponíveis para as contratantes em até 30 dias corridos após a comunicação da assinatura de cada contrato de aquisição de vouchers.

1.6.11. Devem haver turmas regulares até 12 meses depois da data da comunicação da assinatura de cada contrato.

1.6.12. A contratante deve ser comunicada mensalmente das turmas regulares e pode comunicar o uso do voucher do curso até, no mínimo, 15 dias antes do início da turma.

1.6.13. Conteúdo programático:

a) Introdução à tecnologia da Fabricante;
b) Gerenciamento de políticas de segurança;
c) Camadas de políticas;
d) Soluções e licenciamento da solução da fabricante;
e) Visibilidade do tráfego;
f) Conceitos básicos de VPN;
g) Gerenciando o acesso do usuário, e;
h) Implementação da tarefa do administrador.

2. Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall

Esta seção trata das especificações do Grupo II para aquisição dos equipamentos Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - itens 11, 12 e 13 (Equipamentos Tipo VI, VII e VIII). Trata também dos itens 9 e 10 sobre licenciamento de Serviço de *Software-Defined* WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV e dos itens 2 e 7 Firewalls Tipo II, V para o seu pleno funcionamento nos ambientes *on premises* dos Órgãos públicos participantes.

Como mesmo em proporções menores, a Solução dos itens 11, 12 e 13 da contratação funcionam também como Firewall, que, como já dito, é uma solução que identifica e protege, em tempo real, Redes e dispositivos dos contratantes, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente. Por esse motivo a aquisição dos Itens 11, 12 e 13, também deverão estarão vinculadas ao serviço de garantia, atualização de assinaturas de proteção e suporte técnico.

2.1. Item 11 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VI

O equipamento Next Generation Firewall do Tipo VI deverá atender às seguintes especificações:

2.1.1. Throughput de Threat Prevention de, no mínimo, 4 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente.

2.1.2. Suporte a, no mínimo, 600.000 (seiscentos mil) conexões simultâneas.

2.1.3. Suporte a, no mínimo, 28,000 (vinte e oito mil) conexões por segundo.

2.1.4. Throughput de, no mínimo, 2,4 Gbps para conexões VPN site-to-site.

2.1.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP;

2.1.6. Possuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP;

2.1.7. Possuir, pelo menos, 2 (duas) interfaces de rede 1/10Gbps SFP+;

2.2. Item 12 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VII

O equipamento Next Generation Firewall do Tipo VII - deverá atender às seguintes especificações:

2.2.1. Throughput de Threat Prevention de, no mínimo, 2Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente.

2.2.2. Suporte a, no mínimo, 400.000 (quatrocentos mil) conexões simultâneas.

2.2.3. Suporte a, no mínimo, 22.000 (vinte e dois mil) conexões por segundo.

2.2.4. Throughput de, no mínimo, 1.4 Gbps para conexões VPN site-to-site.

2.2.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP.

2.2.6. Possuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP.

2.3. Item 13 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VIII

O equipamento Next Generation Firewall do Tipo VIII deverá atender às seguintes especificações:

2.3.1. Throughput de Threat Prevention de, no mínimo, 650 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero), habilitados simultaneamente.

2.3.2. Suporte a, no mínimo, 200.000 (duzentos mil) conexões simultâneas.

2.3.3. Suporte a, no mínimo, 15.000 (quize mil) conexões por segundo.

2.3.4. Throughput de, no mínimo, 1,2 Gbps para conexões VPN site-to-site.

2.3.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP;

2.3.6. Possuir, pelo menos, 1 (uma) interfaces de rede 1Gbps SFP;

2.4. Características comuns para os Itens 11, 12 e 13 do Edital, Equipamentos de Next Generation Firewall - Tipos VI, VII e VIII

Os equipamentos dos grupos I e II deverão ser do mesmo fabricante dos equipamentos hoje em uso (Fabricante Checkpoint), conforme justificativa constante no ETP.

A seguir serão especificadas as características comuns para os equipamentos referentes aos itens 11 a 13 desta especificação técnica.

2.4.1. Acerca das especificações sobre Software-Defined WAN (SD-WAN), a solução

deverá atender, no mínimo, os seguintes requisitos:

a) A solução de SD-WAN deve ser parte da solução de segurança, com políticas comuns ao firewall principal, gerência e logs centralizados;
b) A solução deve permitir conexão entre as unidades e o TRT via túnel criptografado (VPN *site-to-site*), e;
c) A solução deve permitir ao usuário da unidade remoto acesso à Internet diretamente, sem passar pelo firewall principal (TRT), mas com as mesmas políticas de segurança, inspeção e filtro de conteúdo, de acordo com o seu perfil.

2.4.2. Características Gerais

2.4.2.1. Suportar autenticação para o serviço NTP.

2.4.2.2. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4 (RFC 4271).

2.4.2.3. Deve ser possível habilitar a interface LAN para encaminhar pacotes broadcast.

2.4.2.4. DHCP Relay

2.4.2.5. Possibilidade de definir por quais origens de rede são permitidas as conexões do administrador.

2.4.2.6. Os firewalls bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3.

2.4.2.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos.

2.4.2.8. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.4.2.9. A solução deve ser capaz de permitir ao usuário acesso à Internet via canal privado (VPN com site principal) ou diretamente (via link de Internet), de acordo com as políticas definidas por tipo de aplicação, com todas as inspeções, para serviços de, pelo menos, os seguintes provedores de serviço em nuvem: Microsoft Azure, Google Services, Amazon AWS, Zoom.

2.4.2.10. A solução deve suportar a configuração manual de novos serviços, monitorando continuamente, pelo menos, latência, jitter e perda de pacotes.

2.4.2.11. Deverá suportar, através de interfaces Ethernet, simultaneamente múltiplos acessos através de diferentes meios de transmissão, como MPLS, Internet Banda Larga, 5G/4G.

2.4.2.12. Deverá possibilitar o encaminhamento de tráfego para saídas de Internet distintas por aplicação, sejam elas locais ou remotas.

2.4.2.13. Deverá ser possível preservar as marcações de QoS no cabeçalho do pacote original para os pacotes transportados.

2.4.2.14. Deverá ser possível configurar o dispositivo SD-WAN em alta disponibilidade, com redundância de pelo menos dois dispositivos, trabalhando em modo ativo/standby.

2.4.2.15. A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante.

2.4.2.16. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de *software* livre.

2.4.2.17. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de *end-of-life, end-of-support* e/ou *end-of-sale*.

2.4.2.18. Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação,

cabos de alimentação, suportes, gavetas e braços, se necessário.

2.4.2.19. A solução deve ser capaz de exportar dados de fluxo de tráfego (*flows*) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP *Flow Information Export*) ou sFlow;

2.4.2.20. Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;

2.4.3. Funcionalidade de Prevenção de Ameaças

2.4.3.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.4.3.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.4.3.3. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL TCP, IKE aggressive Exchange;

2.4.3.4. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

2.4.3.5. Em cada proteção de segurança, devem estar incluídas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

2.4.3.6. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas

e customizadas;

2.4.3.7. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por, pelo menos. tipo de proteção, origem, destino, serviço e porta;

2.4.3.8. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

2.4.3.9. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela solução aberta;

2.4.3.10. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes;

2.4.3.11. A solução deve incluir ferramenta própria para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

2.4.3.12. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.4.3.13. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.4.3.14. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.4.3.15. A solução de IPS deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta.

2.4.3.16. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

a) Inspecionar tipos de arquivos conhecidos que contenham malware;
b) Inspecionar todos os tipos de arquivos, e;
c) Inspecionar tipos de arquivos de famílias específicas.

2.4.3.17. Deve bloquear acesso a URLs com malware.

2.4.3.18. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

2.4.4. Proteção Contra Ameaças Avançadas - *Zero Day*.

2.4.4.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT.

2.4.4.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo de comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via análise completa do arquivo no ambiente *sandbox*.

2.4.4.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL/TLS.

2.4.4.4. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas.

2.4.4.5. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado.

2.4.4.6. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, semanal e mensal, assim como o período de cada atualização.

2.4.4.7. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing virtualizado ou em nuvem. Não serão aceitas soluções em servidores ou software livre.

2.4.4.8. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança.

2.4.4.9. Toda análise poderá ser realizada na nuvem do próprio fabricante, sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais, desde que não seja solução de software livre.

2.4.4.10. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL/TLS.

2.4.4.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP.

2.4.4.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, outras extensões do pacote MS Office 365.

2.4.4.13. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

2.4.5. Filtro de Conteúdo Web

A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que