

COORD.GERAL DE RECURSOS LOGÍSTICOS

Estudo Técnico Preliminar 9/2025**1. Informações Básicas**

Número do processo: 50000.026167/2024-54

2. Descrição da necessidade

2.1. Nos últimos anos, o Ministério dos Transportes (MT) modernizou a infraestrutura de tecnologia da informação, adquirindo soluções de TIC que contribuíram para garantir a continuidade e disponibilidade dos sistemas, serviços e aplicações, além de entregar camada de segurança na proteção de dados e no acesso aos principais serviços disponibilizados na internet.

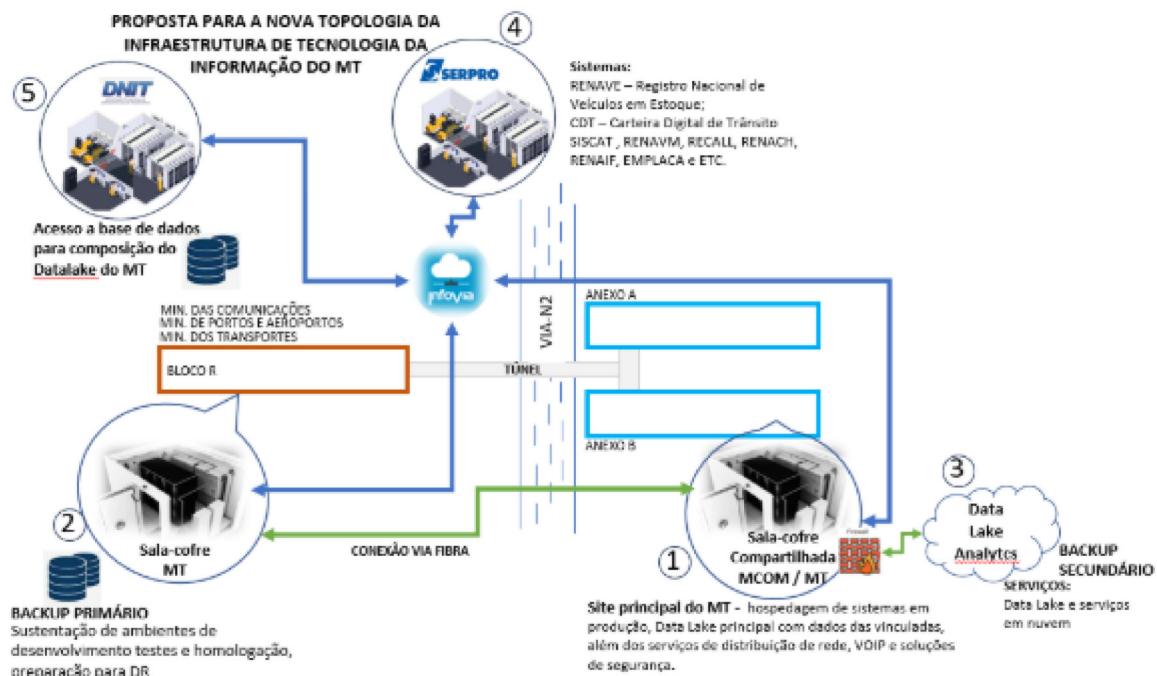
2.2. Para desempenhar suas atribuições institucionais, é necessário que o apoio tecnológico às atividades do MT disponha de uma infraestrutura tecnológica que tenha capacidade de suportar os diversos sistemas e atividades, finalísticas e administrativas, necessárias ao bom desempenho de suas competências legais, bem como de uma estrutura de comunicação eficiente e segura, de modo a permitir a proteção de dados sensíveis da organização e a disponibilidade dos sistemas e serviços hospedados no datacenter da instituição.

2.3. Neste contexto, como forma de minimizar possíveis perdas de dados decorrentes de falhas graves nas citadas Soluções de TIC, como por exemplo dano permanente, causado por desgaste, etc., uma opção seria a extensão de garantia como forma de otimizar todo o investimento já realizado e garantir o suporte adequado, possibilidade a ser explorada no presente estudo.

2.4. Características do Ambiente do Datacenter e da infraestrutura de tecnologia da informação do MT

2.4.1. Conforme consta registrado na Nota Técnica 4 (SEI 9160542) autuada no processo 50000.036460/2024-20, e conforme apresentado na reunião do Comitê de Governança Digital e Segurança da Informação, a nova infraestrutura de tecnologia da informação do MT passará a ser composta da seguinte topologia:

2.4.1.1. Datacenter do MT como Backup e adotando uso compartilhado do Datacenter do Ministério das Comunicações como site principal, mantendo SERPRO, Data Lake Local e serviços em nuvem conforme ilustração a seguir:



I. Sala-Cofre Compartilhada (MCOM/MT): De propriedade do Ministério das Comunicações (MCOM), localizada no prédio anexo ao edifício sede do MT, por meio do uso compartilhado entre as Pastas, a sala passa a ser o site principal do Ministério dos Transportes, proporcionando hospedagem dos sistemas de produção, Data Lake principal, alimentado por dados próprios e de outros órgãos (como SERPRO e DNIT), além de serviços de rede, VOIP e soluções de segurança. Como é um ambiente compartilhado entre MCOM e MT, aproveita-se a infraestrutura já existente e robusta, otimizando investimentos e espaço.

II. Sala-Cofre do Ministério dos Transportes (backup MCOM/MT): Atua como repositório de backup primário para o MT e backup secundário para o MCOM. Sustenta ambientes de desenvolvimento, testes, homologação e preparação para recuperação de desastres (DR). Possui conexão dedicada (via fibra) com a sala-cofre compartilhada, garantindo redundância e segurança na transmissão de dados.

III. Data Lake e Serviços em Nuvem (Backup Secundário): Além do Data Lake principal hospedado no site compartilhado, há utilização de serviços em nuvem para backup secundário, aumentando a resiliência e a disponibilidade dos dados. O Data Lake Analytics pode ser executado na nuvem, permitindo análise de dados em larga escala, sem sobrecarregar a infraestrutura física.

IV. Conexão com o SERPRO: Sistemas críticos, como RENAVE (Registro Nacional de Veículos em Estoque), CDT (Carteira Digital de Trânsito) e outros (SISCAT, RENAVAM, RENACH, RENAIF, EMPLACA, etc.), são mantidos no SERPRO e os dados são acessados por meio da Infovia, garantindo integração segura e confiável. A Infovia provê conectividade redundante e de alta capacidade entre os órgãos, viabilizando o tráfego de dados sensíveis do ponto de vista de serviços públicos.

V. Integração com DNIT: acesso à base de dados do DNIT (Departamento Nacional de Infraestrutura de Transportes) complementa o Data Lake do MT, incorporando dados relevantes para gestão e análise no contexto do transporte. Isso enriquece as informações disponíveis para tomada de decisão, permitindo análises mais completas e integradas.

2.4.2. Verifica-se então que a solução de NG-FIREWALL deverá ser capaz de atender, não só a demanda atual, mas também deverá ser compatível com a necessidade da implementação da nova infraestrutura de tecnologia da informação do Ministério dos Transportes.

2.4.3. A necessidade desta contratação encontra-se alinhada ao Mapa Estratégico Institucional, à Estratégia Brasileira de Governo Digital, ao Plano Diretor de Tecnologia da Informação e Comunicação e ao Plano de Contratações Anual, conforme apresentado nos quadros a seguir:

PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL - PEI (2024-2027)

Fonte: <https://www.gov.br/transportes/pt-br/assuntos/portal-da-estrategia/planejamento-estrategico-2024-2027/planejamento-estrategia>

Eixo	Objetivos Estratégicos
DADOS	7: Implementar estratégias de dados para posicionar o Ministério dos Transportes como indutor de soluções que otimizem a comunicação com a sociedade e a produtividade do Brasil.
DESENVOLVIMENTO INSTITUCIONAL	6: Desenvolver capacidade institucional do Ministério dos Transportes com foco em excelência e produtividade para atendimento dos desafios prioritários;
GOVERNANÇA COLABORATIVA	8: Fortalecer a governança colaborativa com governo e sociedade para garantir a efetividade das políticas públicas.

Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2024-2026

Fonte: Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC — Ministério dos Transportes (<https://www.gov.br/transportes/pt-br/assuntos/governanca/governanca-de-tic-1/plano-diretor-de-tecnologia-da-informacao-e-comunicacao-pdtic/>)

OBJETIVO ESTRATÉGICO DE TI (OTI)	AÇÕES (AC)
OTI4 - Atualizar Parque Tecnológico	AC4.3.1.1 - Atualização da infraestrutura de Tecnologia da Informação e Comunicação.
OTI6 - Promover a Segurança da Informação	AC6.1.1.3 - Desenvolver e Implementar a Política de Controle de Acesso; C6.1.1.4 - Desenvolver e Implementar a Política de Gestão de Registro (Logs) de Auditoria;

ALINHAMENTO AO PAC - TIC – 2025

Fonte: Portal Nacional de Contratações Públicas (<https://pncp.gov.br/app/pca/37115342000167/2025>)

Item	Identificador da Contratação	Descrição
156	390004-45/2025	Solução de NG-FIREWALL - Aquisição de solução de segurança de redes composta de firewall

2.4.4. Com essa aquisição pretende-se garantir:

- a) Preservação da integridade e da confidencialidade dos dados dos usuários dos sistemas e serviços do Ministério dos Transportes, incluindo servidores, colaboradores e cidadãos, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018); e
- b) Autenticação e rastreabilidade das informações de acesso aos sistemas e redes do Ministério dos Transportes pelo período mínimo de 01 ano, de acordo com o Marco Civil da Internet (Lei nº 12.965/2014).

2.4.5. Por este motivo, torna-se imprescindível, pelos critérios de eficiência e economicidade, manter tal solução atualizada, com novo processo licitatório.

2.5. Motivação/Justificativa

2.5.1. A informação constitui-se como um dos principais ativos das organizações e instituições públicas, sendo elemento essencial para a tomada de decisões em todos os níveis e fator determinante para a gestão governamental. Nesse contexto, impõe-se aos gestores o dever de adotar medidas que assegurem a proteção e a integridade dessas informações.

2.5.2. A Tecnologia da Informação e Comunicação (TIC), no âmbito da Administração Pública Federal, consolidou-se como elemento fundamental para o funcionamento e a formulação de estratégias das organizações públicas. Com vistas à utilização eficaz da informação, a TIC sustenta práticas e objetivos organizacionais voltados à melhoria da gestão dos recursos públicos e à elevação da qualidade dos serviços prestados à sociedade.

2.5.3. Observa-se, de forma crescente, a dependência das instituições em relação às informações, as quais se vinculam diretamente à TIC, especialmente no que tange a serviços, sistemas e infraestruturas. Como consequência dessa transformação e da crescente dependência tecnológica, verifica-se não apenas o aumento do número de ativos a serem gerenciados, mas também a ampliação da relevância do monitoramento desses recursos, com o objetivo de detectar falhas e assegurar a segurança da informação e a continuidade dos serviços.

2.5.4. A redução do tempo de resposta a incidentes configura-se como um dos principais objetivos do monitoramento da segurança, uma vez que a indisponibilidade de serviços impacta diretamente as atividades finalísticas, os resultados institucionais e, por conseguinte, a satisfação dos usuários.

2.5.5. Nesse cenário, o conceito de defesa em camadas assume papel central, haja vista a impossibilidade de se garantir a neutralização integral de ataques cibernéticos. É plausível admitir que, em determinado momento, agentes maliciosos possam obter acesso a sistemas críticos, com potencial para causar danos significativos. Diante disso, torna-se imprescindível que a organização esteja apta a detectar e responder, de forma célere e eficaz, a ataques que não tenham sido bloqueados pelas camadas de proteção existentes.

2.5.6. Destaca-se, nesse sentido, a importância da correta configuração das regras de firewall, com o propósito de permitir exclusivamente o tráfego autorizado e bloquear atividades maliciosas ou indesejadas, assegurando, assim, a disponibilidade e a integridade dos serviços prestados.

2.5.7. Conforme a literatura especializada, o firewall é definido como um sistema de segurança de redes de computadores que restringe o tráfego de dados entre a internet e uma rede privada. Tal dispositivo, seja físico ou virtual, atua por meio do bloqueio ou da liberação seletiva de pacotes de dados, prevenindo ataques cibernéticos, controlando acessos a redes e aplicativos e gerenciando dispositivos móveis. A adoção de firewalls com regras de acesso bem definidas e o investimento em segurança de rede são medidas fundamentais para a proteção das informações institucionais.

2.5.8. Na prática, o firewall é um sistema configurado por administradores, que estabelece regras de liberação ou bloqueio de tráfego entre redes. Tais regras devem observar, rigorosamente, o princípio do privilégio mínimo, a fim de evitar acessos indevidos a sistemas e redes.

2.5.9. Dessa forma, a contratação ora proposta visa não apenas aprimorar os processos de identificação e tratamento de ameaças à segurança cibernética, como também fortalecer a governança e a gestão de TIC, especialmente nos aspectos relacionados à segurança da informação e à prevenção de incidentes.

2.5.10. Por fim, a implementação da solução delineada neste Estudo revela-se essencial para que este Ministério possa evoluir em suas capacidades de proteção contra-ataques cibernéticos, promovendo maior resiliência institucional e continuidade dos serviços públicos.

3. Área requisitante

Área Requisitante	Responsável
COINT - Coordenação de Infraestrutura Tecnológica	Henrique Alcântara Veloso Mota

4. Necessidades de Negócio

1	Segurança da rede corporativa;
2	Firewall;
3	IPS (Intrusion Prevention System) - Sistema de Prevenção contra Intrusos;
4	Antivírus para inspeção de tráfego dentro de um firewall
5	Proteção contra todo o espectro de ameaças baseadas em e-mail

5. Necessidades Tecnológicas

1	Conexão segura entre redes externas e a rede;
2	Controlar acesso a conteúdo internos e externos;
3	Priorização do uso da banda de internet para segmentos críticos;
4	Filtro de Conteúdo Web;
5	QoS (Quality of Service) - Qualidade de Serviço.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

1	Controle de Aplicações;
2	Transferência de conhecimento
3	Garantia e suporte.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. O Ministério dos Transportes - MT possui implantada atualmente uma Solução de Segurança de redes que teve o término de seu Contrato de Serviços de Suporte e Garantia de funcionamento da Solução em janeiro de 2025.

7.2. A Solução de Segurança encontra-se ativa, mas a ausência de suporte e garantia para a solução Appliance UTM FortiGate pode acarretar diversas limitações e riscos, especialmente a este Ministério, que possui ambiente corporativo que depende de segurança de rede robusta, sendo assim os principais pontos a considerar:

7.2.1. Riscos de Segurança

7.2.1.1. Sem suporte, atualizações de firmware e assinaturas de segurança (como antivírus, IPS, web filtering) podem não estar disponíveis, deixando o sistema vulnerável a novas ameaças.

7.2.1.2. Falta de correções para vulnerabilidades conhecidas, o que pode ser explorado por atacantes.

7.2.2. Falta de Assistência Técnica

7.2.2.1. Em caso de falhas ou mau funcionamento, não há suporte oficial da Fortinet para diagnóstico ou substituição de hardware.

7.2.2.2. Dificuldade em resolver problemas complexos sem acesso a engenheiros certificados ou suporte especializado.

7.2.3. Impacto na Performance

7.2.3.1. Sem atualizações, o desempenho pode ser comprometido, especialmente se os recursos UTM (como inspeção SSL, antivírus, controle de aplicações) estiverem ativados, pois exigem alto uso de CPU e memória

7.2.4. Conformidade e Auditoria

7.2.4.1. Empresas que precisam seguir normas como LGPD, ISO 27001 ou PCI-DSS podem ter problemas de conformidade ao utilizar equipamentos sem garantia de funcionamento ou suporte.

7.3. Não obstante, um dos maiores desafios é o de uniformizar e agregar valor a esse ativo, acrescentando eficiência, maximizando a utilização das ferramentas e, neste sentido, otimizando recursos humanos e viabilizando assim melhoria nos investimentos e nos recursos aplicados.

7.4. A estrutura existente advém dos investimentos efetuados, especificamente nos anos de 2018/2020, quando a solução de segurança de rede foi contratada.

7.5. Naquela oportunidade, o Ministério do Planejamento, Desenvolvimento e Gestão atendendo o interesse dos órgãos do Sistema de Administração de Recurso de Tecnologia da Informação – SISF, elaborou um Estudo Técnico de Planejamento, consignado em suas justificativas, no sentido de realizar a contratação mediante a deflagração do Pregão Eletrônico para Registro de Preços nº 5/2017 – UASG 201.057.

7.6. O planejamento desta contratação foi impulsionado pelas experiências bem-sucedidas em aquisições conjuntas de Ativos de Redes. Isso levou a equipe da CGINF/DESIN/STI a gerenciar o projeto de aquisição compartilhada da solução de segurança de redes. Para tanto, foi instituído um Grupo de Trabalho Técnico, formalizado pela Portaria nº 03 de 21 de janeiro de 2016.

7.7. Em conformidade com a Instrução Normativa STI/MP nº 04, de 11 de setembro de 2014, tanto o processo de Planejamento da Contratação quanto a elaboração do Edital do certame, incluindo as especificações técnicas, foram conduzidos pela Equipe de Planejamento da Contratação (EPC). Esta equipe foi composta por representantes do DESIN/STI, do referido Grupo de Trabalho Técnico e da Central de Compras e Contratações – SEGES/MP.

7.8. Nesse contexto, o MP ficou responsável pela distribuição e veiculação oficial do instrumento convocatório. Adicionalmente, durante o processo licitatório, o apoio ao pregoeiro foi prestado pelo Grupo de Trabalho, por meio de esclarecimentos e respostas a questionamentos e impugnações que eventualmente surgiram.

7.9. O Pregão Eletrônico para Registro de Preços nº 5/2017, propôs a contratação da solução de segurança de rede com a seguinte configuração de seu objeto:

DO OBJETO - 1.1. O objeto da presente licitação é o registro de preços, para eventual aquisição, de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluindo todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades dos contratantes. 1.2. A licitação será dividida em Grupos/Lotes, formados por 7 (sete) itens cada Grupo/Lote, conforme tabela constante do Anexo B – Especificações Técnicas (Relação dos Grupos/Lotes) do Termo de Referência, facultando-se à licitante a participação em quantos Grupos/Lotes forem de seu interesse, devendo oferecer proposta para todos os itens que o compõem.

7.10. Destacamos cada item do Grupo/Lote que esse Ministério aderiu, conforme abaixo:

Item	Item da ARP	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quant. Adesão MT	Métrica ou Unidade
1	22	Firewall multifuncional Tipo 4	150100	2	Unidade
2	23	Conjunto de funcionalidades IPS/IDS do FW Tipo 4	150100	2	Unidade
3	24	Conjunto de funcionalidades antivírus e anti-malware do FW Tipo 4	150100	2	Unidade
4	25	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 4	150100	2	Unidade
5	26	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 4	150100	2	Unidade
6	27	Treinamento oficial até 5 pessoas do FW Tipo 4	3840	1	Treinamento
8	28	Solução de gerência centralizada do FW Tipo 4	150100	2	Unidade

7.11 O Ministério dos Transportes (MT) está ciente da Consulta Pública nº 9/2025, aberta pela Central de Compras do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), que visa subsidiar o planejamento de uma contratação centralizada de solução de segurança de rede multifuncional do tipo Firewall de Próxima Geração (NGFW). No entanto, a solução de segurança de rede do MT encontra-se sem contrato de suporte e garantia de funcionamento desde janeiro de 2025. Diante dos riscos de segurança e das possíveis limitações e vulnerabilidades decorrentes da ausência de suporte e atualizações, o Ministério não pode aguardar a conclusão de todo o processo de licitação centralizada, que demandaria tempo considerável. A urgência em restabelecer o suporte e a garantia da solução atual é premente para mitigar os riscos operacionais e de segurança da informação.

8. Levantamento de soluções

8.1. Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas

8.1.1. MPMT (UASG 926625 / PE 101/2021): Aquisição de solução fortinet de firewall de aplicação, endpoint remoto, incluindo licenciamento, suporte e garantia para 36 meses;

8.1.2. INPI (UASG 183038 / PE 2/2021): Contratação de empresa especializada para prestação de suporte técnico, manutenção, garantia e licenciamento de solução de segurança de redes e gerenciamento unificado de ameaças (firewall/utm) fortinet composta por dois equipamentos fortigate 1000d e para suporte técnico, manutenção, garantia e licenciamento de ferramenta de concentração de logs e e geração de relatórios fortianalyzer virtual appliance faz-vmgb25, por 36 (trinta e seis) meses;

8.1.3. JUSTICA FEDERAL DE 1°. INSTANCIA - PR (UASG 90018 / PE 77/2022): Registro de Preços de pacotes de serviço Fortinet FortiCare, visando à manutenção dos equipamentos de SD-WAN da Justiça Federal da 4ª Região (JF4R), incluindo suporte técnico especializado com garantia não inferior a 48 meses;

8.1.4. UFBA (UASG 153038 /PE 15/2023): Aquisição de ativos de segurança de rede do tipo Next Generation Firewall (NGFW), com SD-WAN integrada, instalação e suporte técnico, com garantia de 60 (sessenta meses).

8.1.5. Em observância ao disposto no **art. 10 do Decreto nº 11.462/2023**, o qual determina que, antes da instauração de novo processo licitatório, os órgãos e entidades da Administração Pública devem consultar as Intenções de Registro de Preços (IRPs) vigentes e deliberar quanto à conveniência de participação ou adesão, procedeu-se à análise das atas de registro de preços disponíveis no Portal Nacional de Contratações Públicas (PNCP), relativas à aquisição de soluções de firewall de nova geração (NGFW) e correlatos.

8.1.6. Após exame detalhado de 25 atas vigentes, observou-se que:

8.1.6.1 Apenas a ata do Ministério da Cultura - MinC apresenta aderência jurídica e técnica à demanda do Ministério dos Transportes, atendendo aos requisitos do Decreto e podendo ser consideradas como referências válidas de mercado e Aderente usada em um Cenário no TCO, não demonstrou-se vantajosa.

8.1.6.2 Nove órgãos mantiveram o mesmo fabricante adotado na solução de referência (Fortinet, Palo Alto ou Check Point), demonstrando tendência de padronização tecnológica no segmento de segurança de rede;

8.1.6.3 Todavia, a maioria das atas apresenta limitações de porte, vedação expressa à adesão, ou pertencem a outra esfera de poder, o que inviabiliza a participação direta ou o uso como base de preço.

8.1.7. Dessa forma, a equipe técnica cumpre integralmente a exigência do Decreto, anexando aos autos esta manifestação conclusiva sobre as IRPs analisadas, a qual demonstra que, não havendo atas plenamente compatíveis e vantajosas, justifica-se a realização de processo licitatório próprio, observando-se o princípio da eficiência e a economicidade da contratação.

Nº	Órgão / Entidade	Id PNCP	Fabricante / Solução	Esfera / Poder	Vedação de adesão	Compatibilidade ETP	Situação jurídica	Resultado final

1	TST / TRT12	00509968000148-1-003200/2025-000001	Check Point Quantum NGFW + SD-WAN + SASE (60 m)	Judiciário Fed.	Vedada (Cláusula 6ª)	Equivalente em porte, fabricante diferente	Outra esfera / vedação	Não aderente – referência técnica apenas
2	ANM	29406625000130-1-000078/2025-000001	Fortinet FG-901G (UTP 60 m)	Executivo Fed.	Vedada	Comparável (maior conexões, menor throughput)	Vedação	Não aderente – comparativo técnico apenas
3	Ministério das Comunicações	37753638000103-1-000042/2025-000001	Atualização firewall existente	Executivo Fed.	—	Incompatível	Parcial	Não aderente
4	FUNARTE	26963660000161-1-000061/2025-000001	NGFW genérico	Executivo Fed.	Vedada	Incompatível	Vedação	Não aderente
5	JF – ES	00508903000188-1-002765/2024-000002	Palo Alto PA-5220 (renovação 12 m)	Judiciário Fed.	Restrita (JF)	Incompatível (modelo inferior / renovação)	Outra esfera	Não aderente
6	CODEVASF	SRP 90141/2024	Palo Alto PA-3220 (renovação 36 m)	Executivo Fed.	Permitida	Incompatível (fabricante ≠ Fortinet, porte menor)	Mesma esfera	Não aderente
7	UFMS	15461510000133-1-000020/2025-000001	Sophos (cluster)	Executivo Fed.	Vedada	Incompatível	Vedação	Não aderente
8	Ministério da Cultura	01264142000129-1-000012/2023-000002	NGFW + Gerência	Executivo Fed.	Permitida	Compatível	Mesma esfera	Aderente – usado na pesquisa de preço
9	IFTM	10695891000100-1-000157/2024-000001	FortiGate (renovação)	Executivo Fed.	—	Incompatível (menor porte)	Parcial	Não aderente
10	AGU	26994558000123-1-000004/2025-000001	Fortinet (porte ≈ FG-1000F)	Executivo Fed.	Vedada	Parcial	Vedação	Não aderente
11	JF – AL	00508903000188-1-003125/2024-000001	Firewall pequeno porte	Judiciário	—	Incompatível	Outra esfera	Não aderente
12	EBSERH (HU-UFJF)	15126437000143-1-003192/2024-000006	Fortinet FG-201F (UTP 36 m)	Emp. Pública Fed.	Regime Lei 13.303	Menor porte	Regime distinto	Não aderente
13	UFS	13031547000104-1-000002/2024-000001	Palo Alto PA-1410 /460/450	Executivo Fed.	Permite adesão	Menor porte	Mesma esfera	Não aderente
14	UFLA	22078679000174-1-000070/2024-000001	Licenciamento firewall	Executivo Fed.	—	Incompatível	Parcial	Não aderente
15	JF – MA (1)	00508903000188-1-002779/2024-000002	Serviço NGFW + SD-WAN (link)	Judiciário Fed.	Vedada	Objeto diverso	Outra esfera	Não aderente
16	JF – MA (2)	00508903000188-1-002779/2024-000001	Fortinet FG-201F (UTP 60 m)	Judiciário Fed.	Vedada	Menor porte	Outra esfera	Não aderente
17–21	EBSERH (HU-UFJF)	15126437000143-1-003192/2024-000005 a 000001	TIC geral	Emp. Pública Fed.	—	Incompatível	Parcial	Não aderente
22	TRF-3	0059949362000176-1-000100/2024-000001	Check Point SG19100 PLUS (60 m)	Judiciário Fed.	Permite adesão	Equivalente em porte, sem SD-WAN nativa	Outra esfera	Não aderente – comparativo técnico apenas
23	JF – ES (2)	00508903000188-1-002765/2024-000001	Palo Alto PA-5220 (renovação 12 m)	Judiciário Fed.	Restrita (JF)	Incompatível (renovação / outra marca)	Outra esfera	Não aderente
24	IF Sudeste MG	10723648000140-1-000141/2024-000001	Fortinet FG-201F (UTP 60 m)	Executivo Fed.	Vedada	Menor porte	Vedação	Não aderente
25	UFV	25944455000196-1-000098/2024-000001	Fortinet FG-121G (UTP 60 m)	Executivo Fed.	Vedada	Menor porte	Vedação	Não aderente

8.2. As alternativas do mercado

8.2.1. Segundo pesquisas do Gartner, empresa de consultoria e pesquisa sobre tendências tecnológicas, 3/4 dos ataques procuram explorar vulnerabilidades ao nível da aplicação. Essa abordagem significa que o hacker, ao descobrir uma falha em uma aplicação, pode explorar a situação para extração de dados de maneira lenta e de difícil detecção em um sistema ou banco de dados.

8.2.2. Há no mercado diversas soluções corporativas de segurança de firewall. Por essa razão, um referencial de mercado amplamente utilizado, não apenas pela Administração Pública Federal, mas também por empresas privadas, mundialmente, é a análise independente do Gartner.

8.2.3. Anualmente são publicados relatórios comparando as principais soluções do mercado em determinados nichos da tecnologia da informação. Em cada um desses relatórios, fabricantes são avaliados e posicionados em um gráfico (chamado de quadrante mágico) em que são pesados “habilidade de execução” e “completude de visão”. Isso representa uma visão do nível de maturidade e posicionamento no mercado das soluções disponíveis.

8.2.4. O quadrante é uma representação gráfica do mercado tecnológico por um determinado período e define forças dentro de um segmento empresarial, fazendo com que fiquem nítidas as qualidades e possíveis falhas das empresas mais significativas da área de tecnologia, conforme imagem abaixo:



8.2.5. Apesar disso, a empresa não endossa nenhum fornecedor, produto ou serviço retratado. Seu objetivo final é funcionar exclusivamente como uma ferramenta de pesquisa para embasar decisões a partir de necessidades específicas de cada negócio. Ele é dividido da seguinte forma:

8.2.5.1. Líderes (Leaders): aqui são colocadas as empresas tecnologicamente mais avançadas. São aquelas que ditam as regras dentro do seu segmento por ter uma melhor visão de mercado e capacidade de levar adiante as suas promessas;

8.2.5.2. Desafiadores (Challengers): são empresas que estão logo atrás dos líderes. São companhias com capacidade de execução plena. Entretanto, apenas possuem uma parcela do mercado;

8.2.5.3. Visionários (Visionaries): nesse ponto temos as empresas mais fortes em pesquisa e desenvolvimento, verdadeiras visionárias. No entanto, muitas vezes não possuem a tecnologia – ou simplesmente não são capazes – para executar o que é prometido; e

8.2.5.4. Concorrentes de Nicho (Niche Palyers): as empresas desse quadrante são aquelas que focam em determinadas características de um mercado. Basta imaginar uma empresa automobilística focada apenas em carros 4×4 para trilheiras. Ela se diferencia de uma fabricante de carro comum.

8.2.6. Para esta, o levantamento de alternativas do mercado foi utilizado como premissa o Quadrante da Gartner os fornecedores “Leaders”.

8.2.7 Vale ressaltar que os fabricantes líderes de mercado foram consultados por meio de revenda e em seus próprios sites para análise aprofundada de produtos e valores, com o intuito de embasar tal contratação.

8.2.8. O atual fornecedor encontra-se nos fabricantes líderes, sendo benéfico para manutenção da qualidade dos serviços oferecidos manter o nível em relação a solução já adquirida.

8.3. Resumo Comparativo dos Líderes de Mercado

Recurso	FortiGate FG-1000F	Palo Alto PA-5450	Check Point 26000
Firewall Throughput	80 Gbps	120 Gbps	64 Gbps
Threat Protection	11 Gbps	60 Gbps	24 Gbps
SSL Inspection	10 Gbps	50 Gbps	20 Gbps
VDOMs / Virtualização	250	N/D	N/D
Integração SD-WAN / SASE	Sim	Sim	Parcial
Inteligência Artificial	FortiGuard AI	ML integrado	Infinity AI

8.3.1. Fortinet FortiGate FG-1000F

- **Throughput (Firewall):** até 80 Gbps
- **Threat Protection Throughput:** ~11 Gbps
- **SSL Inspection:** ~10 Gbps
- **Interfaces:** 40x GE RJ45, 16x 10GE SFP+, 4x 40GE QSFP+
- **Virtual Domains (VDOMs):** até 250
- **Recursos-chave:**
 - ASIC FortiSPU para desempenho otimizado
 - Integração nativa com SD-WAN, ZTNA e SASE
 - FortiGuard AI para inteligência de ameaças
 - Alta densidade de portas e baixa latência

8.3.2. Palo Alto Networks PA-5450 (concorrente direto)

- **Throughput (Firewall):** até 120 Gbps
- **Threat Prevention:** ~60 Gbps

- **SSL Decryption:** ~50 Gbps
- **Interfaces:** Modular (até 100G)
- **Recursos-chave:**
 - Machine Learning integrado para prevenção de ameaças zero-day
 - Integração com Cortex XDR e Prisma Access
 - Excelente visibilidade de aplicações e usuários

8.3.3. Check Point Quantum 26000

- **Throughput (Firewall):** até 64 Gbps
- **Threat Prevention:** ~24 Gbps
- **SSL Inspection:** ~20 Gbps
- **Interfaces:** Modular (1G/10G/40G)
- **Recursos-chave:**
 - Infinity Threat Prevention com IA
 - Gerenciamento centralizado com SmartConsole
 - Alta escalabilidade com clustering

8.4. A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações

8.4.1. Não se identificaram softwares de governo ou livres equivalentes no Catálogo instituído pela Portaria STI/MP nº 46/2016 que atendam ao objeto, uma vez que a presente contratação trata da modernização de solução de segurança de rede (NG-Firewall) baseada em *appliances* e licenciamento proprietário, inexistindo alternativa catalogada aplicável.

8.5. As políticas, os modelos e os padrões de governo

8.5.1. Padrões de Interoperabilidade de Governo Eletrônico - ePing: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.5.2. Modelo de Acessibilidade em Governo Eletrônico - eMag: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.5.3. Padrões Web em Governo Eletrônico - ePwg: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.5.4. Padrões de Design System de governo: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.5.5. Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.5.6. Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil: Não se aplica por se tratar de renovação de extensão de garantia, solução específica.

8.6. As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc.)

8.6.1. Para utilização do objeto não será necessária qualquer adequação do ambiente por se tratar de equipamentos em pleno uso por este Ministério, salvo demanda muito particular e além da previsibilidade.

8.7. Os diferentes modelos de prestação do serviço

8.7.1. Contratar fabricante, ou revenda autorizada, para prestar serviços de extensão de garantia e suporte técnico e de renovação de garantia de licenciamento, com direito de atualização.

8.8. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes

8.8.1. Contratação de serviços de suporte e extensão de garantia para o appliance FortiGate, da fabricante Fortinet.

8.8.2. Contratação de serviços de renovação de garantia de licenciamento FortiGate e FortiAnalyzer da fabricante Fortinet.

Id	Descrição da solução (ou cenário)
1	Aquisição de nova Solução de Segurança de Redes por meio de Licitação (Pregão Eletrônico)
2	Modernização da Solução de Segurança de Redes existente , incluindo renovação do suporte técnico, extensão da garantia e direito de atualização de versões do licenciamento.
3	Utilizar <i>software</i> livre distribuído gratuitamente

9. Análise comparativa de soluções

9.1. Análise Comparativa dos Cenários de Solução de Segurança de Rede por Requisitos

Requisitos		Cenários		
		ID 1: Aquisição de nova Solução de Segurança de Redes por meio de Licitação (Pregão Eletrônico)	ID 2: Modernização da Solução de Segurança de Redes existente , incluindo renovação do suporte técnico, extensão da garantia e direito de atualização de versões do licenciamento.	ID 3 Utilizar <i>software</i> livre distribuído gratuitamente
Negócio	Alta Disponibilidade e tolerância a falhas	Atende	Atende	Não atende
	Suporte e garantia	Atende	Atende	Não atende
	Requisitos Legais	Atende	Atende	Atende
	Grau de dependência Orçamentária	Não atende	Atende	Atende
	Alta Disponibilidade e tolerância a falhas	Atende	Atende	Não atende
	Suporte e garantia	Atende	Atende	Não atende

Tecnológico	Impacto na troca de solução	Não atende	Atende	Não atende
	Necessidade de ajuste na Infraestrutura	Não atende	Atende	Não atende
	Impacto no processo de trabalho para utilização mais eficiente da solução	Não atende	Atende	Não atende
	Maturidade do mercado no fornecimento da solução	Atende	Atende	Não atende
	Necessidade de Capacitação da Equipe de Operações	Não atende	Atende	Não atende

9.2. Demais requisitos necessários e suficientes à escolha da solução de TIC

Critério / Cenário	1. Aquisição via Licitação (Pregão Eletrônico)	2. Modernização da Solução Existente	3. Utilização de Software Livre
Custo Inicial	Alto (compra de nova solução + serviços)	Moderado (renovação de suporte e licenças)	Baixo ou nulo
Custo de Manutenção	Incluso em contrato, mas pode ser elevado a longo prazo	Geralmente mais previsível e negociável	Pode ser alto (necessidade de equipe especializada interna)
Tempo de Implantação	Médio a longo (processo licitatório + implantação)	Curto (continuidade da solução atual)	Variável (depende da expertise interna)
Suporte Técnico	Garantido por contrato com SLA	Mantido com renovação de contrato	Limitado à comunidade ou equipe interna
Atualizações e Segurança	Garantidas por contrato e fabricante	Garantidas durante vigência do suporte	Dependem da comunidade e da equipe interna
Conformidade com Normas e Auditorias	Alta (soluções comerciais geralmente certificadas)	Alta (se a solução atual já for certificada)	Baixa a média (pode exigir justificativas e documentação adicional)
Flexibilidade e Customização	Limitada (soluções comerciais são mais fechadas)	Limitada (dependente do fornecedor)	Alta (código aberto permite customizações)
Dependência de Fornecedor	Alta	Alta	Baixa (autonomia da equipe interna)

Risco Operacional	Baixo (soluções testadas e com suporte)	Baixo a médio (depende da estabilidade da solução atual)	Alto (exige equipe capacitada e gestão rigorosa)
Escalabilidade e Integração com Outras Soluções	Alta (soluções comerciais geralmente têm APIs e suporte a integrações)	Média a alta (dependendo da solução atual)	Variável (depende da solução escolhida e da capacidade técnica da equipe)
Visibilidade e Monitoramento	Alta (dashboards, relatórios e alertas integrados)	Mantida (se já existente)	Variável (pode exigir ferramentas adicionais de monitoramento)

9.2.1 Confronto com os modelos da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Modelo previsto na Portaria 5.950/2023	Descrição legal	Há correspondência no ETP ?	Conclusão
IaaS – Infraestrutura como Serviço	Recursos computacionais (servidores, armazenamento, rede) providos em nuvem pública.	Não - o ETP trata de appliances físicos próprios do órgão.	Não aplicável
PaaS – Plataforma como Serviço	Ambientes de desenvolvimento e hospedagem de aplicações.	Não há camada de desenvolvimento ou provisionamento de plataformas.	Não aplicável
SaaS – Software como Serviço	Softwares entregues via internet, sob subscrição.	Parcial — há subscrição de licenças e atualizações, mas vinculadas a hardware local (on-prem). Não se trata de SaaS hospedado em nuvem.	Não aplicável como SaaS típico
Serviços de migração, suporte e integração em nuvem	Atividades correlatas a ambientes cloud.	Não há migração nem hospedagem em nuvem contratada.	Não aplicável

9.2.1.1 Quanto à aplicabilidade da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, verifica-se que o objeto deste Estudo Técnico Preliminar - modernização e renovação da solução de segurança de redes do tipo Next Generation Firewall (NGFW), baseada em appliances físicos e licenças vinculadas à infraestrutura local (on-premise) - não se enquadra nas tipologias de software ou de serviços de computação em nuvem (SaaS, PaaS ou IaaS) tratadas pela referida Portaria.

9.2.2. Quanto às Portarias SGD/MGI nº 1.070/2023 e nº 750/2023, verifica-se que ambas não se aplicam à presente contratação, uma vez que o objeto não se refere nem a serviços de operação de infraestrutura e atendimento a usuários de TIC, nem a serviços de desenvolvimento, manutenção ou sustentação de software.

9.2.3. O ETP nº 9/2025 versa sobre a modernização de solução de segurança de redes (NG-Firewall), de natureza infraestrutural e especializada, devendo, portanto, observar as disposições gerais da **IN SGD/ME nº 94 /2022** e da Lei nº 14.133/2021.

9.2.4. **Quanto à verificação de correspondência com o Catálogo de Soluções de TIC,** conforme o § 6º do art. 9º da IN SGD/ME nº 94/2022, verifica-se que a solução de segurança de redes (NG-Firewall) descrita neste estudo não possui item equivalente nos Catálogos de Soluções Padronizadas publicados pelo Órgão Central do SISP, não se aplica a obrigatoriedade de adoção das condições padronizadas.

9.3. Cenários

9.3.1. Cenário 1: Aquisição via Licitação (Pregão Eletrônico)

9.3.1.1. Vantagens:

9.3.1.1.1. Utilização de equipamentos novos, modernos e atualizados, de primeiro uso;

9.3.1.1.2. Possibilidade de exigir garantia e suporte técnico por 60 meses, assim como foi definido na última contratação.

9.3.1.2. Desvantagens:

9.3.1.1.1. Não aproveitamento da Solução já existente do Ministério.

9.3.1.1.2. Preço estimado para a contratação substancialmente mais elevado;

9.3.1.1.3. Possível impacto na infraestrutura caso a empresa vencedora forneça Solução diferente da utilizada atualmente;

9.3.1.1.4. Possibilidade de paralisar a equipe técnica para ser capacitada em administrar e gerenciar nova Solução;

9.3.2. Cenário 2: Modernização da Solução Existente

9.3.2.1. Vantagens:

9.3.2.1.1. Não haverá custos de adaptação ou de migração do ambiente atual; ;

9.3.2.1.2. Não haverá descontinuidade dos serviços, aplicações e dos equipamentos servidores;

9.3.2.1.3. Valor da contratação ser mais vantajoso para o Ministério;

9.3.2.1.4. Não haverá necessidade de paralisar a equipe técnica para ser capacitada na Solução.

9.3.2.2. Desvantagens:

9.3.2.2.1. Possível limitação do tempo de extensão da garantia.

9.3.3. Cenário 3: Utilização de Software Livre

9.3.3.1. Vantagens:

9.3.3.1.1. Oferece **autonomia e economia**.

9.3.3.2. Desvantagens:

9.3.3.2.1. Haverá custos de adaptação ou de migração do ambiente atual;

9.3.3.2.2. Haverá necessidade de paralisar a equipe técnica para ser capacitada na Solução;

9.4. Resumo Estratégico:

9.4.1. **Cenário 1** é ideal para organizações que buscam **renovação tecnológica completa**, com **garantia de suporte e conformidade**, mas exige **maior investimento e tempo**.

9.4.2. **Cenário 2** é mais econômico e ágil, mantendo a continuidade operacional, desde que a solução atual ainda atenda aos requisitos técnicos e de segurança.

9.4.3. **Cenário 3** oferece **autonomia e economia**, mas exige **alta maturidade da equipe técnica**, além de **maior risco operacional e esforço de manutenção**.

10. Registro de soluções consideradas inviáveis

10.1. Utilizar software livre distribuído gratuitamente

10.1.1. A terceira Alternativa de Solução de TIC, vislumbrada para atender a necessidade do MT, seria a utilização de *software* livre de distribuição gratuita, a qual seria composta por *hardwares* tipo servidor, virtual ou físico, e *softwares* livres com funcionalidade de *Firewall* instalados, adicionado a demais softwares acessórios para suportar as necessidades de Segurança da Informação atualmente em uso na Solução proprietária Fortinet implantada no Ministério dos Transportes.

10.1.2. Atualmente, é possível encontrar no mercado diversas Soluções de *Firewall* gratuitas que oferecem funcionalidades como VPN, NAT, chaves RSA e monitoramento de tráfego, identificação de tipos de vírus, controles de acessos, ferramentas de privacidade e prioridade e proteção de ataques de rede ou tentativas de invasão de PCs, dentre outras existentes.

10.1.3. No entanto, alguns empecilhos à utilização de *Firewalls* gratuitos estão relacionados à interface ruim e difícil de ser compreendida, a disponibilidade de funções para atender à todas as demandas da organização, a inexistência de garantias de que todas as funções que ele diz oferecer estarem de fato disponíveis, a falta de atualizações de correção e proteção contínua e, principalmente, a dificuldade de encontrar serviços de suporte técnico confiável junto a fornecedores de mercado.

10.1.4. Desta forma, em pesquisa realizada nas diversas comunidades de *softwares* livres, foram encontrados os seguintes *softwares* que possivelmente comportaria as funcionalidades de *Firewall* com funções necessárias ao atendimento da demanda do MT, quais sejam, *pfsense* com *Squid*, *snort* e *HAVP*.

10.1.5. Mesmo atuando em diversos seguimentos de uma solução de segurança de rede, as citadas ferramentas não trabalham de forma integrada e gerenciada como ocorre na Solução atual do Ministério dos Transportes, além de não realizar diversas funcionalidades essenciais ao negócio deste Ministério.

10.1.6. Ademais, ferramentas livres, em sua origem, não possuem serviços de atendimento de suporte técnico a solução, nem controle de atualizações homologadas por fabricante, o que impactaria consideravelmente os níveis de serviços necessários ao negócio do MT e traria riscos de indisponibilidade prolongada, erros desconhecidos, defasagem de atualização de base de segurança, e, conseqüentemente, a diminuição no nível de segurança da rede do Órgão.

10.1.7. Por fim, como a equipe técnica não detém o domínio técnico das ferramentas mencionadas (ou similares), seria necessário contratar serviço de projeto, implantação, operação da solução e repasse de conhecimento, além de ser aconselhável realizar contrato de serviço de suporte técnico continuado para a Solução, visando dirimir os riscos de indisponibilidade dela. Além disso, para o cenário atual, não haveria aproveitamento dos custos realizado nos anos anteriores, uma vez que os *softwares* livres substituiriam toda a Solução atual do Ministério dos Transportes que ficaria sem serviço de garantia, suporte técnico e atualização após término da vigência do Contrato atual.

10.1.8. Os *softwares* livres citados não possuem custos de licenciamentos, ou seja, não existe um valor a ser pago anualmente para que se continue recebendo as atualizações de segurança e de correção sobre o *software* utilizado, mas existem custos acessórios com a manutenção de equipe técnica especializada nos referidos *softwares*, maior grau de esforço em administração e operacionalização, capacitação de equipe, dentre outros. Há que ressaltar o aumento do risco de indisponibilidade da solução devido a inexistência de suporte técnico do fabricante, além de haver nível de serviço para atendimento, então, o custo de propriedade relacionado a essa Alternativa 3 de Solução torna-se incerto, não podendo ser estimado para a realização de comparativo com as demais Soluções.

11. Análise comparativa de custos (TCO)

11.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

11.1.1. Considerando o disposto no **art. 18, inciso II, da Instrução Normativa SGD/ME nº 94/2022**, que orienta que o Estudo Técnico Preliminar deve apresentar a análise comparativa de soluções de TIC com base nas necessidades do órgão e nos resultados pretendidos, este ETP delimita que o **Item 1 – Firewall de Próxima Geração (NGFW)** constitui o **núcleo funcional da solução de segurança perimetral** e, portanto, é o **elemento central para definição dos cenários comparativos e da viabilidade da contratação**.

11.1.2. Os demais componentes previstos — tais como **licenciamento unificado (UTP), gerência centralizada, suporte técnico, implantação e capacitação** — possuem **natureza acessória**, integrando-se funcionalmente ao firewall, mas **não configuram objetos autônomos** ou independentes. Esses itens são **inerentes à operacionalização do equipamento principal**, compondo o conjunto mínimo necessário para garantir a efetividade, a segurança e a rastreabilidade das políticas de rede, sem impacto direto na escolha do modelo tecnológico.

11.1.3. Assim, para efeito de **avaliação dos cenários apresentados no ETP (nova aquisição, modernização ou software livre)**, a análise comparativa deve concentrar-se no **componente central (Item 1 – Firewall)**, pois é ele quem define:

- o **nível de desempenho e proteção da rede**,
- a **capacidade de processamento e inspeção de tráfego**,
- a **compatibilidade com a arquitetura de segurança existente**, e
- o **custo total de propriedade (TCO)** do investimento.

11.1.4. Os itens acessórios (licenças, serviços e suporte) possuem **características homogêneas entre os fabricantes** e não alteram significativamente o resultado da comparação entre cenários — seu papel é garantir a **sustentação operacional** da solução escolhida.

11.1.5. Portanto, para **efeito de escolha de cenários**, a decisão técnica considera **exclusivamente o desempenho, porte e custo do Item 1 (Firewall)**, reconhecendo os demais elementos como **inerentes à execução contratual e dependentes da seleção do equipamento principal**. Essa abordagem assegura objetividade, transparência e aderência às boas práticas de planejamento da contratação de TIC, evitando sobreposição de custos e mantendo o foco na **solução-fim** que é a **proteção de rede perimetral de alto desempenho**.

				Parâmetro II - SISTEMAS OFICIAIS DO GOVERNO							
				PE Nº 09 /2023 MINC	PE Nº 90004 /2025 TCMPA	PE Nº 90004 /2024 DETRAN-DF	PE Nº 09 /2022 PRODAM				
ITEM	DESCRIÇÃO /ESPECIFICAÇÃO	Unidade de Medida	Qtd	Valor 60 meses	Valor 60 meses	Valor 60 meses	Valor 36 meses, realizado cálculo de proporção para 60 meses	Metodologia: Mediana (menos influenciada por valores muito altos ou muito baixos, a mediana pode ser adotada em casos onde os dados são apresentados de forma mais heterogênea e com um número pequeno de observações. Com o seu uso, entende-se que não é necessário usar metodologia complementar para descon sideração dos valores in exequíveis/excessivamente elevados)			

								Número de preços para o item	MEDIANA (unitária)	VALOR TOTAL - mediana x qtd	VALOR TOTAL ANUAL
1	Aquisição de nova Solução de Segurança de Redes e Sistema de Gerência Centralizada por meio de Licitação	Unidade	10	R\$ 1.771,741,00	R\$ 1.569,000,00	R\$ 1.778,990,00	R\$ 2.708,607,75	4	R\$ 1.775,365,50	R\$ 17.753,655.00	R\$ 17,753,655.00
											R\$ 17,753,655.00

				Parâmetro II - SISTEMAS OFICIAIS DO GOVERNO	Parâmetro IV - FORNECEDORES (Pedido de 03/11/2025)				Metodologia: Mediana (menos influenciada por valores muito altos ou muito baixos, a mediana pode ser adotada em casos onde os dados são apresentados de forma mais heterogênea e com um número pequeno de observações. Com o seu uso, entende-se que não é necessário usar metodologia complementar para desconsideração dos valores inexequíveis /excessivamente elevados)			
				PE Nº) 15 /2023 UFBA	TRTEC Informática Ltda	Alltech Soluções em Tecnologia Ltda.	MVC SECURITY CONSULTING LTDA	GLOBAL SEC. TECNOLOGIA & INFORMAÇÃO LTDA				
ITEM	DESCRIÇÃO /ESPECIFICAÇÃO	Unidade de Medida	Qtd	Valor 60 meses	Valor 60 meses	Valor 60 meses	Valor 36 meses, realizado cálculo de proporção para 60 meses					
									Número de preços para o item	MEDIANA (unitária)	VALOR TOTAL - mediana x qtd	VALOR TOTAL ANUAL
1	Modernização de Solução de Proteção de Rede Perimetral com direito a suporte e garantia por 60 meses Marca: Fortinet Modelo: FG-1000F	Unidade	10	R\$ 1.094,559.00	R\$ 1.499,000.00	R\$ 1.445,000.00	R\$ 1.592,458.71	R\$ 1.405,000.00	5	R\$ 1.445,000.00	R\$ 14,450,000.00	R\$ 14,450,000.00
												R\$ 14,450,000.00

11.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos					Total
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Cenário Viável 1	R\$ 3.914.169,38	R\$ -	R\$ -	R\$ -	R\$ -	R\$ 3.914.169,38
Cenário Viável 2	R\$ 2.816.960,12	R\$ -	R\$ -	R\$ -	R\$ -	R\$ 2.816.960,12

11.2.1. Encontra-se anexada aos autos no documento TCO - DETALHAMENTO (SEI n.º 10036539) a documentação de referencia e detalhada dos quadros acima.

	Estimativa de TCO ao longo dos anos					

Descrição da solução	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	Total
Cenário Viável 1	R\$ 14.450.000,00	R\$ -	R\$ -	R\$ -	R\$ -	R\$ 14.450.000,00
Cenário Viável 2	R\$ 17.753.655,00	R\$ -	R\$ -	R\$ -	R\$ -	R\$ 17.753.655,00

12. Descrição da solução de TIC a ser contratada

12.1. Justificativa para a Manutenção da Solução Tecnológica Atual

12.1.1. Considerando a existência de outros fornecedores posicionados como líderes no quadrante Gartner, a exemplo das empresas Palo Alto Networks e Check Point, a decisão pela continuidade da utilização da solução Fortinet fundamenta-se não apenas na familiaridade da equipe técnica com a referida plataforma, mas, sobretudo, em análise criteriosa dos desafios operacionais e dos custos envolvidos em eventual processo de migração.

12.1.2. A complexidade inerente a sistemas críticos, como os firewalls de próxima geração (NG-Firewall), transcende os aspectos de hardware e software, abrangendo integrações profundas com a infraestrutura de rede, sistemas de autenticação (Active Directory, LDAP), ferramentas de monitoramento, sistemas de gestão de incidentes e, no caso do Ministério dos Transportes, com ambientes externos, como os do SERPRO e do DNIT. A substituição da plataforma atual por solução de outro fabricante, ainda que tecnicamente viável, implicaria:

12.1.2.1. Custos Ocultos e Desproporcionais de Migração: Além do investimento necessário para aquisição da nova solução, seriam exigidos recursos significativos para reengenharia da rede, adaptação de políticas de segurança, reconfiguração de túneis VPN e reintegração com os sistemas dependentes. Tais custos, frequentemente subestimados, podem comprometer eventuais vantagens econômicas oriundas de novo licenciamento.

12.1.2.2. Risco Operacional e Tempo de Inatividade: A migração de um sistema de firewall é um processo de elevada complexidade e risco. Ainda que haja planejamento detalhado, permanece a possibilidade de interrupções prolongadas nos serviços essenciais, o que é inaceitável para a infraestrutura crítica do Ministério.

12.1.2.3. Curva de Aprendizado e Recapitação da Equipe Técnica: A equipe da Coordenação de Infraestrutura de Tecnologia da Informação (COINT) detém amplo conhecimento e experiência acumulados ao longo de cinco anos de operação com a plataforma Fortinet. A adoção de nova tecnologia demandaria capacitação integral da equipe, com custos adicionais de treinamento, redução temporária da produtividade e aumento da suscetibilidade a falhas operacionais.

12.1.2.4. Conformidade e Auditoria: A estabilidade e maturidade da solução atualmente em uso contribuem para o atendimento a normas regulatórias e exigências de auditoria. A adoção de nova plataforma poderia comprometer tais requisitos durante o período de transição.

12.1.3. Dessa forma, a decisão de manter e modernizar a solução Fortinet revela-se a alternativa mais racional e vantajosa sob a ótica do ciclo de vida do ativo, não configurando restrição à competitividade, mas sim medida de preservação da continuidade e da segurança dos serviços públicos prestados.

12.1.4. Ressalta-se que medida similar foi adotada no âmbito do Processo nº 50000.014343/2023-24, referente à contratação de serviços de renovação de garantia, suporte técnico, atualização de versões de software e suporte especializado para ativos de TIC, com o objetivo de mitigar riscos operacionais e preservar o investimento em capacitação técnica.

12.1.5. Ademais, a presente contratação encontra respaldo no art. 41, inciso I, alíneas “b” e “c”, da Lei nº 14.133, de 1º de abril de 2021, conforme transcrição a seguir:

Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá, excepcionalmente:

I – indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;

c) quando determinada marca ou modelo, comercializados por mais de um fornecedor, forem os únicos capazes de atender às necessidades do contratante.

12.2. Contratação por Sistema de Registro de Preços - SRP

12.2.1. Considerando a manifestação de interesse do Ministério das Portos e Aeroportos - MPOR e o arranjo colaborativo entre o Ministério dos Transportes - MT o e MPOR, será adotado o Sistema de Registro de Preços (SRP) para a realização do procedimento licitatório para a presente contratação.

12.2.2. Justificativa para a Adoção do SRP

12.2.2.1. A adoção do SRP se justifica pelos seguintes motivos:

12.2.2.1.1. Manifestação de Interesse do MPOR: manifestou interesse na presente contratação (SEI 9989941), o que demonstra a viabilidade da utilização do SRP para atender a demanda de ambos os Ministérios.

12.2.2.1.2. Adesão à Ata de Registro de Preços: **Não** será admitida a adesão à ata de registro de preços decorrente desta licitação.

12.2.2.1.2.1. O objeto desta contratação possui especificidades de mercado que limitam a capacidade produtiva/operacional dos potenciais fornecedores. A abertura para adesões não planejadas poderia comprometer a execução do contrato principal, gerando risco de inexecução ou atraso na entrega.

12.2.2.1.2.2. Eficiência Administrativa na Gestão da Ata: A gestão de adesões demanda estrutura administrativa robusta para análise de compatibilidade, controle de quantitativos e autorizações. Opta-se pela concentração de esforços na fiscalização da execução do contrato próprio, garantindo o princípio da eficiência.

12.2.2.1.3. Arranjo Colaborativo entre MT e MPOR: A Portaria MGI nº 43, de 31 de janeiro de 2023, estabelece um arranjo colaborativo entre o MT e MPOR, no qual o MT atua como Ministério provedor e será o órgão gerenciador do SRP, enquanto o MPOR atua como Ministério demandante e será o órgão participante do SRP. Essa parceria permite a otimização dos recursos públicos e a padronização dos processos de contratação.

12.2.2.2. O SRP oferece diversas vantagens, como:

12.2.2.2.1. Economia de Tempo e Recursos: o SRP permite a realização de um único processo licitatório para atender a demanda de diversos órgãos, reduzindo custos e agilizando os processos de contratação.

12.2.2.2.2. Padronização dos Preços contratados: o SRP garante a padronização dos preços dos bens ou serviços, beneficiando a Administração Pública e os fornecedores.

12.2.2.2.3. Desburocratização e Padronização: A adesão contribui para a padronização de bens e serviços adquiridos pela administração pública, promovendo uniformidade e controle.

12.2.2.2.4. Compatibilidade com o Objeto da ARP: O objeto da contratação pretendida é idêntico ou compatível com o registrado na ata, atendendo plenamente às necessidades do órgão aderente.

12.2.2.2.5. Economicidade: O preço registrado na ARP é mais vantajoso do que os praticados no mercado ou do que os obtidos em licitações anteriores. Redução de custos operacionais e administrativos com a condução de novo processo licitatório.

12.2.3. Amparo Legal

12.2.3.1. A adoção do SRP está amparada no art. 3º, III, do Decreto nº 11.462, de 31 de março de 2023, que define as diretrizes para o sistema de registro de preços na contratação de bens e serviços no âmbito da Administração Pública federal direta e regulamenta os artigos 82 a 86 da Lei nº 14.133, de 1º de abril de 2021.

“III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;”

12.2.4. Gerenciamento do SRP

12.2.4.1. O gerenciamento do Sistema de Registro de Preços (SRP) será realizado pelo Ministério dos Transportes - MT, conforme estabelecido no Decreto nº 11.462/2023.

12.2.4.2. A validade da Ata de Registro de Preços será de um ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

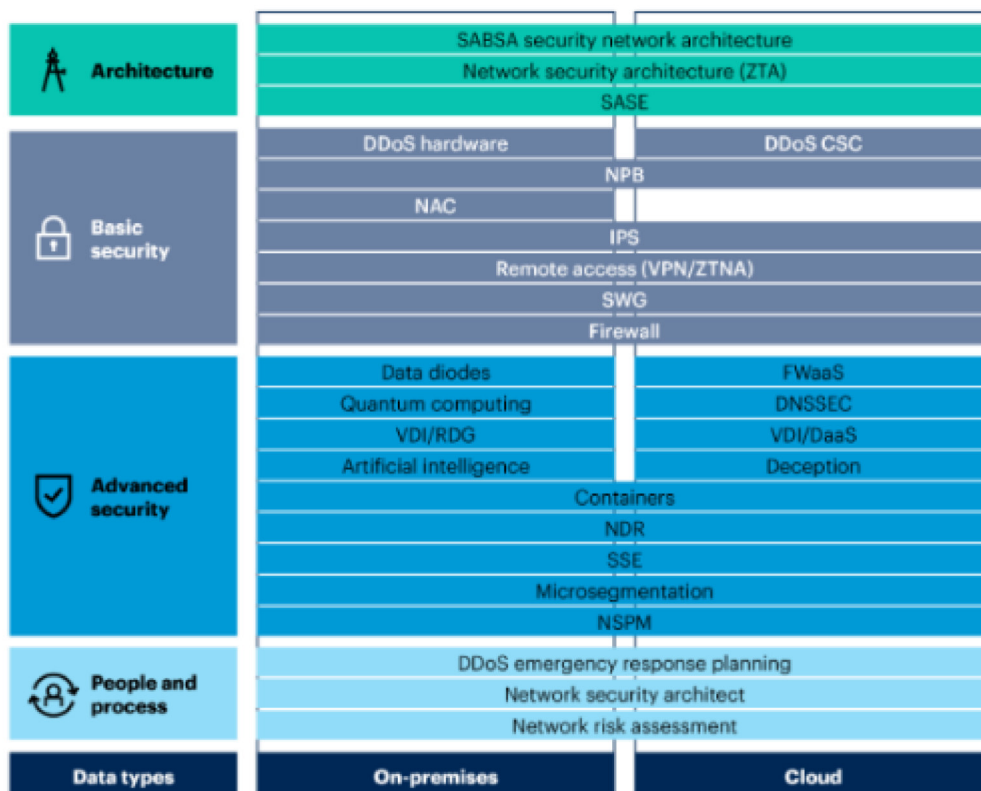
12.2.4.3. Diante do exposto, a adoção do SRP configura-se como a modalidade vantajosa para apresente contratação, as vantagens do SRP, o amparo legal e a estimativa da demanda. Acredita-se que essa modalidade de contratação permitirá a otimização dos recursos públicos, a padronização dos preços e a agilidade dos processos de compras, beneficiando ambas as Instituições.

12.2.5. Sendo assim o objeto da contratação será:

12.2.5.1. Registro de Preços para a eventual contratação de empresa especializada no fornecimento de Solução de Proteção de Rede Perimetral – Período de 60 meses, da empresa Fabricante Fortinet, incluída a Subscrição de todas as Licenças do Conjunto de Funcionalidades, serviços de implantação e transferência de tecnologia, garantia de atualização contínua do sistema operacional e suporte técnico de instalação durante o período de garantia.

12.2.5.2. Os itens que compõem esta solução levaram em consideração o Guia para Conceitos de Segurança de Rede da Gartner, minimamente com os requisitos básicos de segurança, necessários para uma segurança de rede eficaz.

Network Security Architecture



12.2.5.3. Justificando assim a inclusão das extensões de Conjunto de Funcionalidades de Controle de acesso com Proteção do acesso remoto à rede e - Gestão de ativos com detecção de dispositivos conectados à rede.

12.3. A pesquisa realizada e detalhada durante este Estudo permitiu concluir que serão suficientes e necessários os seguintes quantitativos:

12.3.1. MINISTÉRIO DOS TRANSPORTES

GRUPO	ITEM	PRODUTO/SERVIÇO	UNIDADE	QUANTIDADE
1	1	Solução de Proteção de Rede Perimetral – Período de 60 meses	UND	02
	2	Sistema de Gerência Centralizada – Período de 60 meses	UND	01
	3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	UND	100
	4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	UND	1500

12.3.2. MINISTÉRIO DE PORTOS E AEROPORTOS - MPOR

12.3.2.1. A estimativa do consumo definido pelo **MPOR** como órgão participante deverá, no prazo mínimo de oito dias úteis, anunciar a sua intenção pública no registro.

12.3.2.2. Observou-se que não foi registrada a participação do MPOR, conforme Tela Manifestações de Interesse - IRP 05/2025 (10246699).

12.3.3. MANIFESTAÇÕES DE INTERESSE - IRP 05/2025

GRUPO	UASG	ÓRGÃO	ITEM	QUANTITATIVO TOTAL ÓRGÃO PARTICIPANTE	ENDEREÇO
1	90026	SECRETARIA DO CONSELHO DA JUSTICA FEDERAL-CFJ	1	4	SCES, LOTE 09, TRECHO 03, POLO 08, BRASÍLIA/DF
			2	2	
	925942	TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ	1	2	AV. ALMIRANTE BARROSO, Belém/PA
			2	1	
			3	100	
			4	1500	
	29209	INFRA S.A.	1	2	SAUS QUADRA 1, BLOCO 'G', LOTES 3 E 5, BRASÍLIA/DF
			2	1	
			4	1050	

12.4. A solução de segurança de rede deve contemplar:

- I** - Firewall corporativo e multifuncional compatível com os modelos da empresa Fabricante Fortinet Inc.;
- II** - Subscrição das Licenças do Conjunto de Funcionalidades do Appliance, compatível com os modelos da empresa Fabricante Fortinet Inc.;
- III** - Gerenciamento centralizado, compatível com os modelos da empresa Fabricante Fortinet Inc.;
- IV** - Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede
- V** - Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede
- VI** - Serviços de implantação;
- VII** - Garantia de atualização contínua do sistema operacional e suporte técnico nos locais de instalação durante o período de garantia com repasse de conhecimento da solução; e
- VIII** - Garantia de funcionamento pelo período de 60 (sessenta) meses.

12.5. A solução de segurança de rede deve incluir, dentre outras, as seguintes funcionalidades:

- a)** alta disponibilidade;
- b)** anti-malware;

- c) anti-spyware;
- d) antivírus;
- e) anti-bot;
- f) filtro de conteúdo e filtro de URL;
- g) controle de aplicações;
- h) inspeção de pacotes;
- i) IPS/IDS;
- j) relatórios;
- k) inspeção SSL, VPNs e QoS;
- l) autenticação de usuários e antiDoS de rede.

12.6. Em observância as disposições contidas no art. 41, inciso I, alíneas “a” e “c” da Lei nº 14.133/2021, a solução de segurança de redes deve ser, obrigatoriamente, da marca e modelo da empresa Fabricante Fortinet Inc.

12.7. A solução de TIC consiste no fornecimento de soluções de tecnologias conforme especificação técnica pormenorizada no Anexo A – Caderno de Especificações Técnicas deste Estudo ou Termo de Referência.

13. Estimativa de custo total da contratação

Valor (R\$): 17.807.011,75

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	10	R\$ 14.450.000,00	R\$ 14.450.000,00
2	Sistema de Gerência Centralizada – Período de 60 meses	05	R\$ 1.785.975,00	R\$ 1.785.975,00
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	200	R\$ 421.505,00	R\$ 421.505,00
4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	4050	R\$ 1.149.531,75	R\$ 1.149.531,75
Total				R\$ 17.807.011,75

14. Justificativa técnica da escolha da solução

14.1. O sistema de firewall atua como um mecanismo de filtragem eletrônica, responsável por inspecionar o tráfego de dados na rede, identificando e controlando as operações de transmissão e recepção de informações que podem ser executadas em determinado momento.

14.2. A contratação de solução de segurança de rede, composta por firewall, consiste na adoção de uma plataforma de segurança da informação baseada em equipamentos dedicados (appliances), com o objetivo de proteger os ativos computacionais e informacionais da instituição. Nesse contexto, o funcionamento adequado do firewall configura-se como elemento essencial para a manutenção da eficiência e da eficácia dos serviços prestados.

14.3. A presente demanda evidencia a necessidade institucional de garantir a disponibilidade de uma solução de firewall composta por equipamentos atualizados, amparada por garantia do fabricante e por serviço de suporte técnico especializado, o qual poderá ser acionado em situações de falhas, dúvidas quanto à implementação ou sugestões de aprimoramento.

14.4. Considerando que malwares são constantemente desenvolvidos e disseminados na internet, torna-se imprescindível que as bases de dados da solução de firewall sejam atualizadas de forma contínua, em conformidade com as diretrizes do fabricante. Ademais, por se tratar de componente crítico da infraestrutura de rede, a solução representa investimento significativo, cuja preservação e prolongamento da vida útil são recomendáveis até que se verifique eventual obsolescência tecnológica.

14.5. Dessa forma, com vistas à manutenção do nível de segurança da rede institucional e à consequente garantia da disponibilidade dos serviços ofertados aos usuários internos e externos, revela-se necessária a modernização da solução de firewall atualmente em uso. Nesse sentido, conforme exposto na análise comparativa de soluções, conclui-se que a proposta apresentada no cenário 2 mostra-se como a alternativa mais adequada entre as opções viáveis.

14.6. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.6.1. A consolidação da demanda em grupo único item levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado vários fabricantes com capacidade de fornecer a solução de TIC na forma em que está apresentada neste Estudo.

14.6.2. Quanto à decisão pelo não parcelamento do objeto, a solução proposta é tecnicamente indivisível, pois integra equipamentos, licenças e serviços de suporte interdependentes que compõem uma infraestrutura única de segurança de rede. A fragmentação da contratação comprometeria a interoperabilidade, o desempenho e a garantia de funcionamento do conjunto, razão pela qual não se mostra viável a adjudicação por item isolado.

14.6.3. Nos termos dos §§ 1º e 2º do art. 82 da Lei nº 14.133/2021, a adoção do critério de julgamento de menor preço por grupo de itens será acompanhada da devida demonstração de vantagem técnica e econômica, bem como da indicação dos preços unitários máximos aceitáveis no edital, em conformidade com as diretrizes do Sistema de Registro de Preços.

15. Justificativa econômica da escolha da solução

15.1. Considera-se necessária a manutenção da solução atualmente em uso, em consonância com o ambiente tecnológico do Ministério dos Transportes, tendo em vista que a referida solução já se encontra implementada. Tal medida visa assegurar a plena compatibilidade e interoperabilidade com a infraestrutura existente, revelando-se, sob a ótica econômica, mais viável a continuidade da utilização dos equipamentos atuais do que a substituição integral do parque tecnológico, o que poderia acarretar impactos significativos na segurança das informações e dos sistemas institucionais.

15.2. Ademais, justifica-se a preservação do conhecimento técnico acumulado pela equipe da Coordenação de Infraestrutura Tecnológica - COINT, ao longo dos últimos cinco anos, o que representa a salvaguarda de investimentos já realizados em capacitação e experiência operacional, além de garantir a continuidade das atividades e a gestão centralizada dos recursos tecnológicos.

15.3. Ressalte-se, ainda, que a adoção da solução ora proposta poderá resultar em uma economia estimada de, no mínimo, **3.303.655,00 (três milhões, trezentos e três mil seiscentos e cinquenta e cinco reais)**, conforme demonstrado nas propostas analisadas para fins de estimativa de custos desta contratação.

15.4. Por fim, destaca-se que, após a realização do certame licitatório, na modalidade de Pregão Eletrônico, é possível que a economia mencionada seja ainda mais expressiva, em razão da competitividade inerente ao processo.

15.5. PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

15.5.1. Assim, por se tratar de uma solução integrada, em que a homogeneidade na qualidade de toda a solução é extremamente relevante, torna-se tecnicamente e economicamente inviável dividir ou parcelar o objeto, uma vez que uma única Contratada deverá ser responsável pelo fornecimento e instalação dos equipamentos e demais componentes, de modo a não prejudicar a execução operacional das atividades relacionadas ao objeto.

15.5.2. O fornecedor único torna-se o responsável pela integração de todos os componentes e pela manutenção da estabilidade e operacionalidade da solução. A Administração ganha em capacidade de gestão do contrato, com instrumentos de cobrança efetiva, fiscalização do contrato e procedimento padronizado de suporte técnico e garantia, propiciando agilidade na resolução dos problemas advindos de falhas encontradas na solução ou outros eventos relacionados ao objeto.

15.5.3. Diante de todo o exposto, fica assegurado o interesse público e justifica-se a adoção do julgamento da demanda tendo como critério o de Menor Preço por Grupo para o julgamento e classificação das propostas.

15.6 Quanto à vigência contratual plurianual, propõe-se o prazo de **60 (sessenta) meses**, em conformidade com o **art. 106, inciso I, da Lei nº 14.133/2021**, considerando que se trata de **bens e serviços de TIC de natureza infraestrutural e crítica**, cujos ciclos tecnológicos e contratuais são tipicamente plurianuais.

15.7. A duração proposta está alinhada às *Boas Práticas, Orientações e Vedações para Contratação de Ativos de TIC – Versão 4* (<https://www.gov.br/receitafederal/pt-br/aceso-a-informacao/licitacoes-e-contratos/licitacoes/rfb/unidades-federativas-uf/pr/srrf09/2024/pe-13-2023/anexos-etp/15-orientacoes-ativos-de-tic-v-4.pdf>), publicadas pela Secretaria

de Tecnologia da Informação (STI/MP), que em seu item **1.4.5.1** recomenda **vida útil mínima de cinco anos** para servidores de rede, equipamentos de armazenamento e segurança.

15.8. O prazo de 60 meses assegura **continuidade operacional, estabilidade de suporte técnico e economia de escala**, evitando custos administrativos e logísticos decorrentes de contratações fragmentadas e garantindo a **vantajosidade econômica** exigida pela legislação.

16. Benefícios a serem alcançados com a contratação

16.1. A aquisição da Solução TIC em estudo trará benefícios ao ambiente tecnológico interno, por meio da atualização do seu parque tecnológico, especialmente no que tange à Segurança da Informação deste MT, assim como os benefícios abaixo relacionados:

- Elevar o índice de disponibilidade das informações e serviços prestados por meio da rede corporativa e do sítio Web do MT;
- Continuar oferecendo Infraestrutura de Tecnologia da Informação adequada para que as áreas finalísticas do negócio do MT continuem operacionais;
- Suportar o crescente aumento de demanda por serviços de tecnologia da informação e, ao mesmo tempo, promover condições de melhoria na tomada de decisões estratégicas objetivando maior eficiência ao negócio, uma vez que as informações estratégicas estarão disponíveis;
- Contribuir para garantia de um nível adequado de disponibilidade, integridade e confidencialidade das informações produzidas, armazenadas e transmitidas por meio da Tecnologia da Informação;
- Manter atualizados os recursos de segurança da informação do MT, de forma a prover com rapidez, eficiência e eficácia plena capacidade de atender e suportar as necessidades de negócios.

17. Providências a serem Adotadas

17.1. Não há necessidade de adequação do ambiente, por se tratar de equipamentos em pleno uso pelo Ministério dos Transportes, salvo demanda muito particular e além da previsibilidade.

17.2. Gerenciar todas as fases do processo licitatório, desde a publicação até a homologação da ata de registro de preços.

17.3. Fornecer esclarecimentos e respostas a questionamentos e impugnações que surgirem durante o certame.

17.4. Assegurar que os serviços de extensão de garantia, suporte técnico, atualização contínua e transferência de tecnologia sejam executados conforme o contrato.

17.5. Monitorar os custos para garantir a economicidade e os benefícios esperados, conforme a análise de TCO.

17.6. Garantir que a transferência de conhecimento ocorra para a equipe da COINT, conforme previsto, a fim de manter a autonomia e a capacidade de gestão dos recursos tecnológicos.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1.1. O presente Estudo Técnico Preliminar - ETP, elaborado pelos Integrantes Técnico e Requisitante, em harmonia com a Instrução Normativa SGD /ME nº 94/2022, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante, bem como, observado os demais aspectos normativos, conclui pela viabilidade da contratação, sob os seguintes aspectos:

I - A solução possui especificações técnicas e padrões de desempenho e qualidade objetivamente definidos e usualmente utilizadas no mercado, consoante as exigências contidas no art. 2º, inciso XXXII da IN SGD/ME Nº 94 /2022;

II - Conforme levantamento dos diversos cenários, a solução é a única que atende as necessidades técnicas e econômicas da contratação;

III - A solução pode ser encontrada em, pelo menos, 6 (seis) Instituições Públicas, conforme pesquisa efetuada no site Compras.Gov e assentada no subitem 8.6 deste documento;

IV - A solução encontra-se amparada pelo instituto do art. 41, inciso I, alíneas “a” e “c” da Lei nº 14.133/2021; e

V - Mediante chamamento público, a ser efetuado com a publicação do Edital, para fins de realização da licitação, haverá manifesto interesse do mercado.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

JULIO CESAR FERREIRA DA SILVA

Integrante Técnico



Assinou eletronicamente em 19/11/2025 às 11:00:10.

HENRIQUE ALCANTARA VELOSO MOTA

Integrante Requisitante



Assinou eletronicamente em 19/11/2025 às 11:42:44.

DIOGO DA FONSECA TABALIPA

AUTORIDADE MÁXIMA DA ÁREA DE TIC



Assinou eletronicamente em 19/11/2025 às 19:32:38.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ANEXO A – CADERNO DE ESPECIFICAÇÕES TÉCNICAS_Modificado.pdf (330.5 KB)



MINISTÉRIO DOS TRANSPORTES
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO
COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO A – CADERNO DE ESPECIFICAÇÕES TÉCNICAS

1.1. Especificações técnicas

1.1.1. Item 1 Solução de Proteção de Rede Perimetral

1.1.1.1. A solução de segurança (NGFW) deve possuir a capacidade e as características abaixo:

1.1.1.1.1. Throughput de no mínimo, 15 (Quinze) Gbps, com as funcionalidades de Next Generation firewall(IPS e Application control habilitados simultaneamente), com padrão de tráfego empresarial ou similar.

1.1.1.1.2. Throughput de no mínimo, 12(Doze) Gbps, com as funcionalidades de Next Generation firewall, IPS, anti-malware e prevenção contra ameaças avançadas de dia-zero habilitadas e atuantes, conhecido como Threat Protection ou Threat Provention);

1.1.1.1.3. Throughput de no mínimo, 10 (Dez) Gbps, para inspeção de tráfego SSL, considerando pelo menos funcionalidade de IPS sobre tráfego HTTPS/WEB.

1.1.1.1.4. O Throughput é a quantidade de tráfego que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;

1.1.1.1.5. Suporte a, no mínimo, 7.500.000 (sete milhões e quinhentos mil) de conexões simultâneas;

1.1.1.1.6. Suporte a, no mínimo, 500.000 (quinhentos mil) novas conexões por segundo;

1.1.1.1.7. Armazenamento redundante de, no mínimo, de 480 GB SSD;

1.1.1.1.8. Deve possuir fontes de alimentação AC 100-240VAC redundantes e hot-swappable;

1.1.1.1.9. No mínimo, 8 (oito) interfaces de rede de GbE RJ-45;

1.1.1.1.10. No mínimo, 16 (Dezesseis) interfaces de rede de 1/10 Gbps SFP+/SFP acompanhado de seus respectivos Gbics do fabricante ofertado;

1.1.1.1.11. No mínimo, 4(Quatro) interfaces de rede de 25/10 SPF28/SFP+ slots acompanhado de seus respectivos Transceivers do fabricante ofertado;

1.1.1.1.12. No mínimo, 2(Duas) interfaces de rede de 40/100 Gbps QSFP+ slots acompanhado de seus respectivos Transceivers do fabricante ofertado;

1.1.1.1.13. No mínimo, 01 (uma) interface Gigabit dedicada para alta disponibilidade;

1.1.1.1.14. No mínimo, 01 (uma) interface Gigabit dedicada para Gerência;

1.1.1.1.15. 01 (uma) interface do tipo console ou similar;

1.1.1.1.16. Deverão ser licenciados para suportar, pelo menos, 1.000 (um mil) usuários de VPN de cliente.

1.1.1.1.17. VPN com capacidade de, pelo menos, 54 (cinquenta e quatro) Gbps de tráfego IPSec;

1.1.1.1.18. Suportar, no mínimo, 5 instâncias de firewall (cluster) e permitir a expansão, através de aquisição futura de licenças;

1.1.1.1.19. O Troughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.1.1.20. Todas as interfaces SFP+ fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores do tipo SR.

1.1.1.1.21. Não serão aceitos appliances virtualizados para os firewalls, somente equipamentos físicos.

1.1.1.2. Funcionalidades do Firewall:

1.1.1.2.1. As funcionalidades de firewall devem possuir a capacidade e as características abaixo:

1.1.1.2.2. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.1.2.3. Deve possibilitar a elaboração de políticas baseadas em geolocalização, permitindo o bloqueio de tráfego proveniente de determinado(s) país(es);

1.1.1.2.4. Deve permitir a exibição dos países de origem e destino nos registros de acesso;

1.1.1.2.5. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

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

1.1.1.2.7. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;

1.1.1.2.8. Deve ser possível realizar um espelhamento do tráfego de-criptografado;

1.1.1.2.9. Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;

1.1.1.2.10. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;

1.1.1.2.11. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.1.2.12. A plataforma deve ser otimizada para análise de conteúdo de aplicações em Camada 7 (Web Application Firewall);

1.1.1.2.13. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.1.2.14. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.1.2.15. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.1.1.3. Deve suportar os seguintes tipos de NAT e Roteamento:

1.1.1.3.1. NAT dinâmico (Many-to-1), NAT estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

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

1.1.1.3.3. Deve suportar atuar como proxy reverso para aplicações Web que utilizem protocolos HTTP e HTTPS;

1.1.1.3.4. Para IPv4, deve suportar roteamento estático e dinâmico (RIP V1, V2, OSPF e BGPv4) Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);

1.1.1.3.5. Deve suportar NAT64

1.1.1.3.6. Deverá suportar roteamento estático e dinâmico;

1.1.1.3.7. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, não sendo aceito soluções que fazem a gravação do tráfego para posterior abertura e análise, inclusive com a capacidade de aplicação de filtros personalizados;

1.1.1.3.8. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.1.1.3.9. Deve possuir sistema de monitoramento em tempo real do hardware via interface gráfica, interface Web HTTPS e linha de comando CLI;

1.1.1.3.10. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

1.1.1.3.11. Deverá suportar sFlow ou NetFlow;

1.1.1.3.12. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

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

1.1.1.3.14. Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.

1.1.1.4. Funcionalidades de Prevenção de Ataques:

1.1.1.4.1. Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

1.1.1.4.2. Deverá oferecer a capacidade de determinar políticas conforme o tempo, isto é, estabelecer normas para horários ou intervalos específicos (dia, mês, ano, dia da semana e hora);

1.1.1.4.3. A criação de políticas por agrupamentos de usuários, endereços IP, redes ou áreas de segurança deverá ser possível;

1.1.1.4.4. Deve ter a competência para criar políticas baseadas na visibilidade e controle de quem usa quais URLs, integrando com serviços de diretório, Active Directory e banco de dados local;

1.1.1.4.5. A identificação através do Active Directory deve habilitar SSO, de modo que os usuários não tenham que fazer login novamente na rede para passar pelo firewall;

1.1.1.4.6. Deve suportar a criação de políticas baseadas no controle por URL e categoria de URL;

1.1.1.4.7. Deve ter categorias de URLs pré-estabelecidas pelo fabricante que podem ser atualizadas a qualquer momento;

1.1.1.4.8. Deve ter no mínimo 50 categorias de URLs;

1.1.1.4.9. Deve contar com a função para excluir URLs do bloqueio;

1.1.1.4.10. Deverá permitir a personalização da página de bloqueio;

1.1.1.4.11. Deve possibilitar a limitação do acesso a canais específicos do YouTube, permitindo a configuração de uma lista de canais permitidos ou uma lista de canais bloqueados;

1.1.1.4.12. Deve impedir o acesso a conteúdo inadequado quando se utiliza a pesquisa em sites como Google, Bing e Yahoo, independentemente da opção Safe Search estar ativada no navegador do usuário;

1.1.1.4.13. Deve contar com recurso de prevenção contra phishing de credenciais, analisando quais estão sendo submetidas em sites externos, e ainda bloquear ou alertar o usuário;

1.1.1.4.14. Deve proporcionar a opção de estabelecer uma cota diária de uso web baseada em categoria, podendo estabelecer a cota com base, pelo menos, no tempo de uso e volume de tráfego;

1.1.1.4.15. Deverá ser possível bloquear tráfego HTTP POST, método usado para envio de informação a um website específico;

1.1.1.4.16. Deverá ser capaz de filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado;

1.1.1.4.17. Deve possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados mal-intencionados;

1.1.1.4.18. A filtragem de tráfego de vídeo com base na categoria e até mesmo no identificador de um canal do YouTube, por exemplo, deve ser possível;

1.1.1.4.19. Além de suportar Web Proxy explícito, deverá permitir Proxy Web transparente;

1.1.1.4.20. Deverá estar orientado à proteção de redes;

1.1.1.4.21. Deverá permitir funcionar em modo transparente, porta espelhada e gateway das redes protegidas.

1.1.1.4.22. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.

1.1.1.4.23. Deverá permitir a criação de padrões de ataque manualmente.

1.1.1.4.24. Deverá possuir integração à plataforma de segurança.

1.1.1.4.25. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques.

1.1.1.4.26. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.

1.1.1.4.27. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.

1.1.1.4.28. Deverá possuir análise de protocolos.

1.1.1.4.29. Deverá possuir detecção de anomalias.

1.1.1.4.30. Deverá possuir detecção de ataques de RPC (Remote Procedure Call).

1.1.1.4.31. Deverá possuir proteção contra-ataques de Windows ou NetBios.

1.1.1.4.32. Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

1.1.1.4.33. Deverá possuir proteção contra-ataques DNS (Domain Name System).

1.1.1.4.34. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.

1.1.1.4.35. Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).

1.1.1.4.36. Deverá possuir métodos de notificação de detecção de ataques.

1.1.1.4.37. Deverá possuir alarmes na console de administração.

1.1.1.4.38. Deverá possuir alertas via correio eletrônico.

1.1.1.4.39. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

1.1.1.4.40. Deverá ter a capacidade de resposta/logs ativa a ataques.

1.1.1.4.41. Deverá ter a capacidade de detectar e bloquear ameaças avançadas, como malware, ransomware e outras ameaças que os firewalls tradicionais podem não ser capazes de lidar. Isso é muitas vezes alcançado através da integração com outras tecnologias de segurança, como sistemas de prevenção de intrusões (IPS), proteção avançada contra malware (AMP) e sandboxing;

1.1.1.4.42. Deverá prover a terminação de sessões via TCP resets.

1.1.1.4.43. Deverá armazenar os logs de sessões.

1.1.1.4.44. Deverá mitigar os efeitos dos ataques de negação de serviços.

1.1.1.4.45. Deverá permitir a criação de assinaturas personalizadas.

1.1.1.4.46. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.

1.1.1.4.47. Deverá suportar verificação de ataque na camada de aplicação.

1.1.1.4.48. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware.

1.1.1.4.49. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

1.1.1.5. Funcionalidades de Controle de Qualidade do Serviço:

- 1.1.1.5.1. Suportar a criação de políticas de QoS por:
- 1.1.1.5.2. Endereço de origem, endereço de destino e por porta;
- 1.1.1.5.3. O QoS deve possibilitar a definição de classes por:
- 1.1.1.5.4. Banda garantida, banda máxima e fila de prioridade;
- 1.1.1.5.5. Disponibilizar estatísticas RealTime para classes de QoS;
- 1.1.1.5.6. Funcionalidades de VPN:
- 1.1.1.5.7. Suportar VPN Site-to-Site e Cliente-To-Site;
- 1.1.1.5.8. Suportar IPSEC VPN;
- 1.1.1.5.9. A VPN IPSEC deve suportar:
- 1.1.1.5.10. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.1.6. Suportar SSL VPN o qual deve:

- 1.1.1.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional (Windows e Linux) do equipamento ou por meio de interface WEB;
- 1.1.1.6.2. Permitir que o usuário realize conexão através de dispositivos mobile (Android e IOS) através de um cliente instalado do fabricante ofertado.
 - 1.1.1.6.2.1. Por questões de segurança, não serão aceitos cliente mobile de terceiros;
- 1.1.1.6.3. A funcionalidades de VPN de cliente devem ser atendidas com ou sem o uso de agente;

1.1.1.6.4. Deve ser capaz de informar se a senha do usuário da VPN de cliente autenticado via Microsoft Active Directory expirou e permitir que o usuário faça a troca da senha;

1.1.1.6.5. Atribuição de endereço IP nos clientes remotos de VPN;

1.1.1.6.6. Atribuição de DNS nos clientes remotos de VPN;

1.1.1.6.7. A solução ofertada deve suportar a tecnologia de VPN Dinâmica entre as filiais (ADVPN);

1.1.1.6.8. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.1.1.6.9. Suportar leitura e verificação de CRL (certificate revocation list);

1.1.1.6.10. O agente de VPN de cliente client-to-site deve ser compatível com pelo menos: Windows, Linux e Mac OS X.;

1.1.1.6.11. Deve suportar duplo fator de autenticação para a conexão VPN;

1.1.1.6.12. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN.

1.1.1.7. Suportar SD-WAN;

1.1.1.7.1. Não deve limitar número de links a serem balanceados.

1.1.1.7.2. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

1.1.1.7.3. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

1.1.1.7.3.1. Endereço IP de origem e/ou destino;

1.1.1.7.3.2. Subredes de origem e/ou destino;

1.1.1.7.3.3. Métricas de Jitter, latência e perda de pacotes por aplicação;

1.1.1.7.3.4. Status da porta de WAN primários (UP ou DOWN);

1.1.1.7.4. Deve reconhecer e respeitar no tráfego SD-Wan, para o teste de saúde dos links, o atributo DSCP "Differentiated Services Code Point", para aferição mais precisa conforme criticidade das aplicações.

1.1.1.7.5. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA.

1.1.1.7.6. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

1.1.1.7.7. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

1.1.1.7.8. O estabelecimento do túnel VPN entre os pontos de presença pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

1.1.1.7.9. Tratar o tráfego SD-Wan das aplicações críticas respeitando e aplicando as tags DSCPs das mesmas.

1.1.1.7.10. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW.

1.1.1.7.11. Permitir a monitoração dos links SD-Wan através de protocolos: ping, http, tcp-echo e udp-echo;

1.1.1.7.12. Permitir a monitoração dos links SD-Wan através do Protocolo IP nas versões 4 e 6;

1.1.1.7.13. Permitir a monitoração dos links SD-Wan combinando fatores de saúde podendo variar entre: tempo de checagem, número de checagens antes

de declarar o link como não operacional e número de checagens antes de declarar o link como operacional novamente;

1.1.1.7.14. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponíveis, que está orientado ao mesmo destino.

1.1.1.7.15. O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado, para permitir que aplicações sensíveis à perda de pacotes não sejam impactadas em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

1.1.1.8. Prevenção de Ameaças Avançadas (zero day)

1.1.1.8.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado, ou analisado dinamicamente com mecanismo de IA em ambiente controlado;

1.1.1.8.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

1.1.1.8.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW, após validação pelo ambiente Cloud de Sandbox.

1.1.2. Item 2 - Sistema de Gerência Centralizada

- 1.1.2.1.** Deve prover gestão centralizada dos equipamentos e ser necessariamente do mesmo fabricante do NGFW.
- 1.1.2.2.** Por console de gerência, entende-se as licenças de software necessárias para esta funcionalidade.
- 1.1.2.3.** Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi 6.7, Proxmox e Microsoft Hyper-V.
- 1.1.2.4.** Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
- 1.1.2.5.** Deverá possuir a capacidade de receber pelo menos 20 GB de logs diários.
- 1.1.2.6.** O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
- 1.1.2.7.** Permitir acesso concorrente de administradores.
- 1.1.2.8.** Deverá possuir autenticação de usuários para acesso à plataforma via LDAP e RADIUS.
- 1.1.2.9.** Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores.
- 1.1.2.10.** Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
- 1.1.2.11.** Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora.
- 1.1.2.12.** Deve registrar as ações efetuadas por quaisquer usuários.
- 1.1.2.13.** O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação.

- 1.1.2.14.** O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e AntiSpyware.
- 1.1.2.15.** O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL.
- 1.1.2.16.** Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
- 1.1.2.17.** O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall.
- 1.1.2.18.** A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
- 1.1.2.19.** A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.
- 1.1.2.20.** Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.
- 1.1.2.21.** Deverá possuir mecanismos de apagamento automático para logs antigos.
- 1.1.2.22.** Deverá permitir importação e exportação de relatórios.
- 1.1.2.23.** Deverá ter a capacidade de criar relatórios no formato HTML.
- 1.1.2.24.** Deverá ter a capacidade de criar relatórios em formato PDF.
- 1.1.2.25.** Deverá permitir exportar os logs no formato CSV.
- 1.1.2.26.** Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- 1.1.2.27.** Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- 1.1.2.28.** Suportar o padrão SAML para autenticação do usuário administrador.

- 1.1.2.29. Deverá estar licenciada para a quantidade de equipamentos a serem gerenciados.
- 1.1.2.30. Deverá Suportar até 20 GB de logs por dia;
- 1.1.2.31. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
- 1.1.2.32. Deverá integrar e gerenciar todos os ativos dos itens do objeto;
- 1.1.2.33. Deverá permitir instalar políticas pontualmente em seus gateways gerenciados, no gateway específico, não sendo aceito soluções com aplicações de políticas generalizadas para todo o parque gerenciado;
- 1.1.2.34. Deverá permitir instalar políticas "diferenciais", ou seja: apenas as alterações novas devem ser enviadas para os gateways selecionados, deixando inalterada a parte remanescente já configurada e em uso. Não sendo aceito soluções com aplicações de políticas generalizadas para todo o parque gerenciado.
- 1.1.2.35. Caso a Console de Operação da Solução de Gerenciamento Centralizado seja baseada em tecnologias descontinuadas, e.x Java, não será aceito, devendo ser fornecido método alternativo para garantia da integridade do Ambiente de Segurança e protegido.

1.1.3. Item 3 – Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede

- 1.1.3.1. A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;
- 1.1.3.2. A solução deve estar licenciada para um total de 100 (cem) usuários;
- 1.1.3.3. A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;

- 1.1.3.4.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;
- 1.1.3.5.** A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;
- 1.1.3.6.** Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;
- 1.1.3.7.** A solução deve ser escalável até 500 agentes;
- 1.1.3.8.** O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;
- 1.1.3.9.** Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits), Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022, Mac OS X: versões 13, 12, 11 e 10.15, Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;
- 1.1.3.10.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel;
- 1.1.3.11.** A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;
- 1.1.3.12.** Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;

- 1.1.3.13.** A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso;
- 1.1.3.14.** Deve ser possível revogar o certificado de um agente por meio da console central;
- 1.1.3.15.** O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;
- 1.1.3.16.** No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão;
- 1.1.3.17.** Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;
- 1.1.3.18.** A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;
- 1.1.3.19.** Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;
- 1.1.3.20.** Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;
- 1.1.3.21.** Deve ser possível exportar os logs diretamente a nível de agente;
- 1.1.3.22.** Deve ser possível exigir uma senha para desconectar o agente da console central;
- 1.1.3.23.** Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente;
- 1.1.3.24.** Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;

- 1.1.3.25.** Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos endpoints de acordo com o índice de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal;
- 1.1.3.26.** Deve ser possível configurar o agente para usar Proxy;
- 1.1.3.27.** O agente deve permitir a configuração local via XML (eXtensible Markup Language);
- 1.1.3.28.** Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;
- 1.1.3.29.** Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;
- 1.1.3.30.** Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;
- 1.1.3.31.** Deve ser possível especificar a validade do código de registro;
- 1.1.3.32.** A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa.
- 1.1.3.33.** Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net;
- 1.1.3.34.** A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;
- 1.1.3.35.** Deve ser possível agrupar agentes em grupos;
- 1.1.3.36.** Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;

- 1.1.3.37.** Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;
- 1.1.3.38.** A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;
- 1.1.3.39.** O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;
- 1.1.3.40.** Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;
- 1.1.3.41.** Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor.
- 1.1.3.42.** Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS;
- 1.1.3.43.** Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
- 1.1.3.44.** A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;

- 1.1.3.45.** Deve permitir criação de regras de conformidade que avaliem a postura do dispositivo e auxiliem o administrador no controle de acesso aos recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;
- 1.1.3.46.** As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;
- 1.1.3.47.** A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;
- 1.1.3.48.** Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;
- 1.1.3.49.** A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;
- 1.1.3.50.** Deve ser possível verificar quais endpoints estão associadas com cada tag;
- 1.1.3.51.** Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;
- 1.1.3.52.** Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;
- 1.1.3.53.** Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;

- 1.1.3.54.** Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;
- 1.1.3.55.** Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;
- 1.1.3.56.** A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;
- 1.1.3.57.** Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;
- 1.1.3.58.** Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;
- 1.1.3.59.** Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;
- 1.1.3.60.** Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;
- 1.1.3.61.** Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;
- 1.1.3.62.** O agente deve dispor de um sistema de notificação do tipo popup visando alertar o usuário;
- 1.1.3.63.** Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;
- 1.1.3.64.** Deve suportar a criação de várias versões de pacotes de instalação;
- 1.1.3.65.** As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade,

severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site

1.1.3.66. público do fabricante do software;

1.1.3.67. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;

1.1.3.68. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;

1.1.3.69. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;

1.1.3.70. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;

1.1.3.71. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;

1.1.3.72. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;

1.1.3.73. Deve ser possível determinar quando o filtro web entrará em ação no agente, se o mesmo deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;

1.1.3.74. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;

- 1.1.3.75.** O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução;

1.1.4. Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede

- 1.1.4.1.** Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
- 1.1.4.2.** Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do órgão;
- 1.1.4.3.** Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;
- 1.1.4.4.** A solução deve suportar capacidade de expansão para até 1500 endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;
- 1.1.4.5.** A solução deve estar licenciada para operação com, pelo menos, 1500 endpoints conectados simultaneamente;
- 1.1.4.6.** A solução deve ser entregue em alta disponibilidade;
- 1.1.4.7.** A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
- 1.1.4.8.** Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
- 1.1.4.9.** A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
- 1.1.4.10.** A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;

1.1.4.11. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

1.1.4.12. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

1.1.4.12.1. Consultas em DHCP Fingerprint;

1.1.4.12.2. Consultas via protocolos HTTP/HTTPS;

1.1.4.12.3. Consultas via protocolo SNMP;

1.1.4.12.4. Consultas via protocolo SSH;

1.1.4.12.5. Consultas via protocolo Telnet;

1.1.4.12.6. Consultas de portas TCP;

1.1.4.12.7. Consultas de portas UDP;

1.1.4.12.8. MAC OUI;

1.1.4.12.9. Consultas via protocolo WMI;

1.1.4.12.10. Protocolo ONVIF;

1.1.4.12.11. Protocolo NetFlow;

1.1.4.12.12. Base assinaturas pré-definidas;

1.1.4.13. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

1.1.4.13.1. Endereço MAC;

1.1.4.13.2. Endereço IP;

1.1.4.13.3. Sistema operacional;

1.1.4.13.4. Nome do host;

1.1.4.13.5. Horário de conexão;

1.1.4.13.6. Usuário conectado;

1.1.4.13.7. Localização.

1.1.4.14. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

1.1.4.14.1. Android;

1.1.4.14.2. Apple iOS para iPhone, iPod e iPad;

1.1.4.14.3. Chrome OS;

1.1.4.14.4. Linux;

1.1.4.14.5. MacOS X;

1.1.4.14.6. Windows 7, 8 e 10;

1.1.4.15. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;

1.1.4.16. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;

1.1.4.17. Deve permitir a recategorização periódica de dispositivos;

1.1.4.18. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;

1.1.4.19. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;

1.1.4.20. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;

1.1.4.21. A solução deve suportar RADIUS Change of Authorization;

1.1.4.22. A solução deve suportar MAC Address Bypass;

1.1.4.23. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

- 1.1.4.24.** A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;
- 1.1.4.25.** Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
- 1.1.4.26.** Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;
- 1.1.4.27.** A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;
- 1.1.4.28.** A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
- 1.1.4.29.** A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
- 1.1.4.30.** A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
- 1.1.4.31.** Deve permitir a definição de complexidade da senha dos usuários visitantes;
- 1.1.4.32.** Deve ser possível definir um período de validade para as contas de usuários visitantes;
- 1.1.4.33.** Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
- 1.1.4.34.** A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
- 1.1.4.35.** Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

- 1.1.4.36.** A solução deve vincular o login do visitante à máquina utilizada no acesso;
- 1.1.4.37.** Deve suportar a validação de credenciais:
- 1.1.4.37.1. Em base local interna à ferramenta;
 - 1.1.4.37.2. Em servidores RADIUS;
 - 1.1.4.37.3. Em servidores LDAP.
- 1.1.4.38.** A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
- 1.1.4.39.** A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
- 1.1.4.40.** Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;
- 1.1.4.41.** A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
- 1.1.4.42.** Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
- 1.1.4.43.** Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;
- 1.1.4.44.** Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;
- 1.1.4.45.** A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
- 1.1.4.46.** Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

1.1.4.47. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;

1.1.4.48. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;

1.1.4.49. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;

1.1.4.50. Se um dispositivo não passar os testes de conformidade, deve ser possível:

1.1.4.50.1. Não forçar a remediação;

1.1.4.50.2. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;

1.1.4.50.3. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

1.1.4.51. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

1.1.4.51.1. Windows 7;

1.1.4.51.2. Windows 8;

1.1.4.51.3. Windows 10;

1.1.4.51.4. MacOS;

1.1.4.51.5. Linux.

1.1.4.52. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

1.1.4.52.1. Presença de software de anti-vírus instalado e em execução;

1.1.4.52.2. Versão do sistema operacional;

1.1.4.52.3. Nome de domínio do Active Directory ao qual a estação Windows pertença;

1.1.4.52.4. Serviços em execução para estações Windows;

1.1.4.52.5. Informações sobre um determinado certificado digital em estações Windows;

1.1.4.52.6. Registros ou chaves de registro para estações Windows;

1.1.4.52.7. Processos em execução para estações Windows, Linux e MacOS;

1.1.4.52.8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;

1.1.4.52.9. Pacotes instalados em estações Linux e MacOS.

1.1.4.53. A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

1.1.4.54. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

1.1.4.55. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

1.1.4.55.1. Programas de gerenciamento e distribuição de software;

1.1.4.55.2. GPO do Active Directory;

1.1.4.55.3. Captive Portal;

1.1.4.56. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

1.1.4.57. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

- 1.1.4.58.** Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;
- 1.1.4.59.** A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;
- 1.1.4.60.** No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;
- 1.1.4.61.** A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;
- 1.1.4.62.** Deve suportar integração com soluções de patching;
- 1.1.4.63.** Deve suportar integração com soluções de análise de vulnerabilidades;
- 1.1.4.64.** A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
- 1.1.4.65.** A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;
- 1.1.4.66.** A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;
- 1.1.4.67.** A solução deve armazenar os eventos internamente e permitir que sejam exportados;
- 1.1.4.68.** A solução deve permitir a exportação dos eventos através de syslog;
- 1.1.4.69.** Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
- 1.1.4.70.** A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

- 1.1.4.71.** Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;
- 1.1.4.72.** Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;
- 1.1.4.73.** Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;
- 1.1.4.74.** Deve possibilitar o rastreamento de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;
- 1.1.4.75.** Caso o CONTRATANTE não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor incluí-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;
- 1.1.4.76.** Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, dispositivos registrados e rogues;