Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 50500.026666/2022-49

2. Descrição da necessidade

2.1. A atualização e expansão da solução de inspeção de pacotes de dados é necessária pois tem como objetivo garantir a disponibilidade dos serviços de TI através da aquisição de solução de segurança para prevenir de ataques; evitar que usuários não autorizados acessem serviços ou sistemas e controlar as ações realizadas na rede da ANTT; e prover linha de redundância para o enlace do Backbone principal.

2.2. Os equipamentos da solução de inspeção de pacotes de dados consistem em um dispositivo de rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software.

2.3. Esta solução controla todas as comunicações que passam de uma rede a outra e, em função do que sejam, permite ou denega seu passo. Para permitir ou denegar uma comunicação, a solução examina o tipo de serviço ao qual corresponde, que podem ser a sítios do tipo Portais (Terra, UOL, IG, por exemplo), correio eletrônico, dentre outros.

2.4. A solução de inspeção de pacotes de dados também é um grande aliado no combate a vírus e cavalos de Troia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados. Em redes corporativas, como a da ANTT, torna-se possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo rastrear e descobrir quais usuários as efetuaram.

2.5. Atualmente esse serviço é mantido por solução adquirida por meio do Contrato Administrativo nº 034/2017, cuja validade encerrar-se-á em 15 de dezembro de 2022.

3. Área requisitante

Área Requisitante	Responsável
Gerência de Infraestrutura Tecnológica	Victor Hugo Gouveia de Lucena Lima

4. Necessidades de Negócio

4.1. A pretensa contratação encontra-se alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação da ANTT - PDTIC 2021-2024, ao Planejamento Estratégico Institucional - PEI, de acordo com o Mapa Estratégico da ANTT 2020-2030, e ao Plano Anual de Contratações - PAC 2022, conforme tabela abaixo:

Planejamento Estratégico ANTT - 2020-2030	
ID	**Objetivo Estratégico**
OPG4	Potencializar a capacidade de inovação e absorção de tecnologias de forma estruturada
PR2	Aprimorar a disponibilidade, a qualidade e a integração das informações internas e externas

Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC	
Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2021-2024	
ID	**NECESSIDADE**
N7	Propor a modernização das tecnologias utilizadas nos sistemas de informação com uso de mecanismos inovadores
N10	Aperfeiçoar os mecanismos e ambientes para assegurar alta disponibilidade e evolução tecnológica

ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
-	Definir padrões de qualidade com vistas a aprimorar a aquisição ou desenvolvimento das soluções	-	Implementar soluções com uso de inteligência artificial
-	Executar os serviços de gestão e manutenção de infraestrutura: dados em nuvem, site redundante, rede de dados, banco de dados, segurança	-	Garantir disponibilidade das aplicações: 99%

Alinhamento ao Plano Anual de Contratações - PAC		
Item no PAC	**Descrição**	**Aprovação**
2.7	Solução de Inspeção de Pacotes de Dados, incluindo o fornecimento de equipamentos e softwares integrados em forma de *appliance* e/ou quando especificado; serviços de instalação e configuração, suporte técnico e garantia, serviços de operação assistida e demais serviços associados	Aprovado na Revisão do Planejamento Anual de Contratações - PAC 2022, nos termos da Deliberação nº 297/2022.

4.2. A Agência Nacional de Transporte Terrestres - ANTT, criada pela Lei nº 10.233, de 5 de junho de 2001, integrante da administração federal indireta, submetidas ao regime autárquico especial e vinculada ao Ministério dos Transporte, tem como missão e visão de futuro:

“Missão: Assegurar aos usuários adequada infraestrutura e prestação de serviços de transporte terrestre, com transparência e regulação efetiva, proporcionando melhoria contínua dos serviços.”

“Visão de Futuro: Ser reconhecida pela sociedade como uma Agência inovadora, com autonomia decisória, transparente e efetiva na sua atuação no setor de transportes terrestres.”

4.3. A ANTT diante de sua missão e visão de futuro e de seus Objetivos Estratégicos, pelo qual busca promover a melhoria contínua da operação e serviços de transportes terrestres tem como competências:

> *A concessão de ferrovias, rodovias e transporte ferroviário associado à exploração da infraestrutura;*
>
> *A permissão de transporte coletivo regular de passageiros pelos meios rodoviário e ferroviário não associados à exploração da infraestrutura;*
>
> *A autorização de transporte de passageiros por empresa de turismo e sob regime de fretamento, transporte internacional de cargas, transporte multimodal e terminais.*

4.4. O Planejamento Estratégico da ANTT, elaborado para o ciclo de 2020-2030, traça objetivos estratégicos relacionados aos recursos de TIC. A Tecnologia da Informação e Comunicação compreende uma série de soluções e serviços computacionais que atendem aos diversos níveis de decisão da ANTT, tendo papel primordial na construção da regulação e na fiscalização dos serviços de transportes terrestres, em alinhamento com a Missão Institucional e buscando agregar valor para que se possa alcançar a Visão Estratégica para 2030.

4.5. O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2021-2024 busca unir as ações executivas ao planejamento estratégico, contribuindo para o atingimento dos objetivos desejados. Uma dessas ações é continuar promovendo a cultura de Segurança da Informação e Comunicação, com base na Política de Segurança da Informação e Comunicações (PoSIC), para mitigar os riscos que comprometem a Disponibilidade, Integridade, Confidencialidade e Autenticidade das Informações.

4.6. Neste sentido, a Superintendência de Tecnologia da Informação - SUTEC necessita renovar as licenças de uso existentes dos appliances de Firewall Check Point que expiram ao final deste ano de 2022 e adquirir solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI. Portanto, pretende-se dar continuidade ao serviço de proteção de perímetro da rede corporativa da ANTT, atingir melhoria na capacidade do órgão em responder de forma rápida e adequada a incidentes de segurança que possam vir a ocorrer, além de aprimorar a disponibilidade, a qualidade e a integração das informações internas e externas da ANTT.

4.7. A SUTEC, diante desse cenário, propõe a contratação da renovação das licenças de uso de software dos appliances de Firewall Check Point e a aquisição de solução de segurança integrada à solução de rede definida por software (SDN) Cisco Application Centric Infrastructure (ACI), incluindo garantia, atualização de software e suporte técnico.

5. Necessidades Tecnológicas

5.1. O objeto da pretendida contratação é uma Solução de Tecnologia da Informação e Comunicação (TIC), que visa manter os sistemas e serviços de TI disponíveis de forma

estruturada e segura, proporcionando a melhoria contínua dos serviços prestados à sociedade pela ANTT.

5.2. A solução de Inspeção de Pacotes de Dados constitui um elemento crítico para a disponibilidade, confiabilidade, segurança e desempenho de todos os serviços acessíveis pela rede da ANTT. Destaca-se que essa solução é responsável por mitigar os riscos de ataques ao ambiente computacional, protegendo dados, informações e ativos de rede contra invasões ou infecções causadas por falhas de configuração, ação de códigos maliciosos, malware, spyware, exploração de vulnerabilidades, atividades maliciosas, como participar de botnets, phishing, programas de códigos maliciosos, sequestro de dados, uso indevido dos recursos, executar varreduras na rede (scan), executar ações maliciosas e bloquear ataques de distribuídos de negação de serviços (DDoS).

5.3. Sendo assim, o software de uma solução de segurança necessita estar permanentemente atualizado, com as mais recentes versões dos mecanismos de defesa e as ferramentas mais atuais para proteção e gerenciamento de segurança das comunicações de rede. Além disso, o suporte técnico especializado fornecido por empresa certificada pelo fabricante CheckPoint se faz necessário para que as falhas, interrupções ou outros problemas de funcionamento sejam resolvidos com o menor tempo de resposta possível.

5.4. A solução de rede definida por software (SDN) Cisco ACI, adquirida no ano de 2019, por meio do Contrato nº 025/2019, é essencial para aumentar ainda mais a produtividade da TIC ao permitir que as equipes tenham uma plataforma comum com gerenciamento centralizado de ambientes físicos e virtuais da infraestrutura e monitoramento de integridade em tempo real. A arquitetura com base em políticas da solução, permite automatizar o provisionamento da infraestrutura de rede, dos serviços de aplicativos e das políticas de segurança com base em perfis de política predefinidos de forma muito mais simples e eficiente. Ademais, contribui para a redução de falhas planejadas e não planejadas, pois os problemas são identificados e resolvidos com mais rapidez. À medida que o tempo de paralisação diminui, os usuários e a equipe de TIC tornam-se mais produtivos. A solução de SDN torna as operações de TI mais eficientes, reduz a complexidade e os custos de infraestrutura de Data Center, oferece agilidade para disponibilizar aplicativos rapidamente e de modo seguro, além de minimizar o risco reduzindo o tempo de paralisação que pode afetar os serviços essenciais da ANTT.

5.5. Essa mudança de arquitetura na infraestrutura de rede com foco no provisionamento de aplicativos acarreta um grande aumento do tráfego lateral leste-oeste. Tradicionalmente, a segurança e a prevenção de ameaças têm se concentrado na proteção do perímetro ou do tráfego norte-sul, enquanto o tráfego leste-oeste entre aplicativos dentro do data center não é inspecionado como deveria ser. Nesse contexto, ameaças introduzidas no data center podem atravessar sem impedimentos, pois não passam pelo gateway de segurança. Por isso, a segurança deve ser abrangente, dinâmica e integrada com o data center definido por software Cisco ACI. Essa integração deve oferecer provisionamento de segurança automatizado juntamente com as proteções mais abrangentes. Os recursos de segurança integrados devem incluir: Firewall, IPS, controle de aplicativos, VPN IPsec, antivírus, anti-bot, extração e emulação de ameaças para proteções de Zero-Day. A solução deve ter gerenciamento centralizado com aplicação consistente de políticas de segurança e visibilidade total de ameaças no ambiente de data center físico e virtual da ANTT

5.6. Características essenciais da solução de segurança integrada ao Cisco Application Centric Infrastructure (ACI):

a) Inserção e orquestração dinâmica da proteção avançada contra ameaças com as mais altas taxas de captura de malware;

b) Microssegmentação operacionalmente viável para proteção do tráfego Leste-Oeste;

c) Políticas de segurança refinadas vinculadas a grupos de End Point da ACI (EPGs);

d) Conscientização do contexto do objeto ACI em logs de segurança e relatórios específicos do data center;

e) Marcar hosts infectados como meio de isolamento da rede (quarentena) ou remediação;

f) Fornecer rastreamento de incidentes e análise de ameaças para o tráfego do perímetro e do data center;

g) Gerenciamento de segurança unificado para controle e visibilidade em ambientes virtuais e físicos, incluindo suporte a multilocação;

h) Capacidade de usar o contexto de vários sistemas de gerenciamento de nuvem, como Cisco ACI, OpenStack e vCenter na mesma política de segurança;

i) Implantação rápida de políticas de segurança durante todo o ciclo de vida de implantação do aplicativo;

j) OPEX reduzido devido à implementação acelerada de aplicativos e segurança com maior eficiência no provisionamento de serviços e segmentação de segurança de rede.

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

6.1. Para o atendimento dessa demanda deve ser utilizada as tabelas abaixo como referência para renovação:

Item	Descrição	Modelo	QTD	Valor unitário
1.	Cluster com 2 appliances de Firewall NGTX Tipo 1	Check Point 15400 NGTX Appliance	2	340.000,00
2.	Cluster com 2 appliances de Firewall NGTX Tipo 2	Check Point 5800 NGTX Appliance	2	172.000,00
3.	Solução de Gerência Centralizada	Security Management Software	1	45.000,00

Tabela 2 – Descrição detalhada de cada Appliance

Item	Número de Série	Modelo	Patrimônio	Data de vencimento da licença

1.	LR201704000539	Check Point 15400 NGTX Appliance	5717205	14/02/2023
	LR201705006597	Check Point 15400 NGTX Appliance	5717204	14/02/2023
2.	1706BA4028	Check Point 5800 NGTX Appliance	5717207	14/02/2023
	1706BA3999	Check Point 5800 NGTX Appliance	5717206	14/02/2023
3.	-	Security Management Software	-	14/02/2023

Tabela 3 – End of Sale e End of Support dos modelos atuais:

Modelo	End of Sale	End of Support
Check Point 15400 NGTX Appliance	01/12/2020	01/12/2025
Check Point 5800 NGTX Appliance	01/12/2020	01/12/2025
Security Management Software	01/12/2018	01/12/2023

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Renovação das licenças de uso de software dos appliances de Firewall Check Point e aquisição de solução de segurança integrada à solução de rede definida por software (SDN) Cisco Application Centric Infrastructure (ACI), incluindo garantia, atualização de software e suporte técnico, nos termos da tabela abaixo:

Item	Descrição	Unidade de Medida	Quantidade
	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint		

1	15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2
2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2
3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1
4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4
5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1
6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1

8. Levantamento de soluções

8.1. A renovação de licenças para soluções de segurança da informação é comumente realizada na Administração Pública, sendo adotada por diversos órgãos. Trata-se de renovação da licença de uso do software com garantia e suporte técnico.

8.2. Neste caso, acrescenta-se ainda a contratação da solução de segurança integrada à solução de rede definida por software (SDN), para assegurar a proteção cibernética do Data Center na ANTT.

ID	Descrição da solução
1	**Solução 1 - Renovação das licenças de software dos appliances de Firewall Check Point com suporte técnico e aquisição de solução de segurança integrada à solução de rede definida por software (SDN): aproveitamento dos equipamentos de firewall atuais contratando apenas os serviços de suporte e garantia para as licenças de software e para os appliances atuais de firewall com adição da solução de segurança integrada para Cisco ACI da ANTT.**

2	**Solução 2 - Aquisição de novos appliances de Firewall NGFW com licenças de software e suporte técnico e aquisição de solução de segurança integrada à solução de rede definida por software (SDN): aquisição de novos appliances de firewall com serviços de suporte e garantia embutidos e adição da solução de segurança integrada para Cisco ACI da ANTT.**
3	**Solução 3 - Segurança como Serviço – SECaaS (Security as a Service): segurança como serviço é um modelo de negócios no qual um provedor de serviços integra seus serviços de segurança a uma infraestrutura corporativa por assinatura. Libera a equipe de segurança interna da ANTT e passa a gestão operacional da segurança para um provedor especializado.**

9. Análise comparativa de soluções

9.1. Com base nos resultados reportados no painel de preços e órgãos da Administração Pública, obteve os seguintes resultados:

PREGÃO	ÓRGÃO	UASG	Objeto
PE nº 01/2022	COMANDO DA MARINHA	740014	Aquisição de equipamentos a serem empregados nas Organizações Militares (OM) da Marinha do Brasil, para atender às necessidades da Diretoria de Comunicações e Tecnologia da Informação da Marinha, na qualidade de Diretoria Especializada (DE) responsável pelas atividades relativas às comunicações e à tecnologia da informação (TI) da Marinha do Brasil (MB).
			Aquisição, mediante Sistema de Registro de Preços, de solução para mitigação de ataques de negação de serviço (DoS

PE nº 02/2022	MEC	150002	/DDoS) e serviços agregados de implantação, instalação, configuração, operação assistida, garantia e suporte técnico dos equipamentos – de acordo com as especificações técnicas e condições previstas no Termo de Referência.
PE nº 78/2022	BRB	925008	Contratação de empresa especializada para renovação da infraestrutura de Firewalls do fabricante Check Point que o BRB possui, com módulos de expansão, treinamento e suporte especializado, conforme Edital e seus anexos.
PE nº 3/2022	Tribunal de Contas do Estado do Paraná	925457	Contratação de empresa especializada para prover renovação (prorrogação) de licenciamento e suporte técnico, bem como atualização tecnológica (aquisição de novas licenças e créditos para treinamentos junto ao fabricante) para solução de segurança da informação da Check Point composta por firewall e ferramenta de conexão remota, conforme estabelecido no Termo de

			Referência TR Anexo I do Edital.
PE nº 1326/2021	SERPRO	803080	Contratação de hardware, software e subscrição para atualização tecnológica de ambiente NGFW do SERPRO
PE nº 49/2021	Tribunal de Justiça do Estado de Mato Grosso	925007	Registro de Preço de Solução de Firewall Datacenter, através da aquisição de equipamentos e licenças com suporte técnico e garantia da fabricante, contemplando, inclusive, tais para os equipamentos e softwares legados que já fazem parte da solução deste PJMT - Account ID Check Point 8014345 - visando atender as políticas mínimas de segurança da informação que tangem este órgão, conforme especificações técnicas do Termo de Referência, e condições desse Edital e seus anexos
PE nº 34/2021	Tribunal Regional Eleitoral na Bahia	70013	Serviço de renovação de licenças de uso de firewall Check Point, com suporte técnico para os

			equipamentos e programas, bem como atualizações de versões
PE nº 6358/2021	Companhia Hidro Elétrica do São Francisco	910813	Fornecimento de Atualização de licenças dos softwares Check Point & Aquisição de Solução Zero Trust.
PE nº 15/2021	Tribunal Regional Eleitoral do Rio de Janeiro	70017	Aquisição de dois bancos de memória a serem instalados em dois firewalls, modelo 15.600, de fabricação da empresa Check Point Software Technologies Ltda, registrados com os códigos padronizados de identificação do fabricante (part number), incluindo a instalação e o suporte do contratada por 12 meses.
PE nº 13/2021	Tribunal Regional Eleitoral do Rio de Janeiro	70017	Aquisição de dois bancos de memória a serem instalados em dois firewalls, modelo 15.600, de fabricação da empresa Check Point Software Technologies Ltda, registrados com os códigos padronizados de identificação do fabricante (part number), incluindo a instalação e o suporte do contratada por 12 meses.

PE nº 53/2021	SECRETARIA DE ESTADO DE ECONOMIA DO DISTRITO FEDERAL	974002	Registro de Preços para a contratação de empresa especializada para Renovação e Expansão de Solução Integrada de Segurança de Redes composta de clusters de firewalls, com licenciamento, garana e suporte técnico por 36 (trinta e seis) meses para equipamentos novos e legado e treinamento, visando atender as necessidades da Subsecretaria de Tecnologia da Informação e Comunicação - SUTIC, da Secretaria de Estado de Economia do Distrito Federal, conforme condições e especificações constantes neste Termo de Referência e seus anexos.
PE nº 01/2022	INCRA-DF	373083	Aquisição de Solução de Renovação do Suporte e Garantia das Licenças de Software e dos Appliances de Firewall Checkpoint dos Incra, conforme quantitativos, especificações e condições descritas neste Termo de

			Referência (TR) e Anexos.
ATA SRP - PE nº 02/2021	CITEX/Comando do Exército	160091	Fornecimento de expansão tecnológica para solução de segurança de perímetro, instalada no 7º Centro de Telemática de Área (7º CTA), abrangendo o fornecimento de appliances next-generation firewall (NGFW), orquestrador, prestação de serviços de suporte técnico on-site e/ou remoto, manutenção corretiva e evolutiva com substituição de peças e/ou componentes e serviços técnicos especializados, pelo período de 12 (doze) meses.
PE nº 126/2021	BACEN- BANCO CENTRAL	179087	Serviço de atualização tecnológica da solução de proteção de rede com funcionalidades de reconhecimento de aplicações e prevenção de ameaças. O objeto compreende o hardware e software que compõe a solução, bem como licenças, garantia de hardware e software por 48 (quarenta e oito)

			meses, baseada em tecnologia Check Point, além dos serviços de instalação e repasse de conhecimento.
PE nº 61/2022	MPG - MINISTÉRIO PÚBLICO DO GOIÁS	https://intranet.mpgo.mp.br/sgoc/portal/processos/visualizar_documentos?id=14659	Contratação de serviço de suporte técnico e atualização do sistema de segurança da rede corporativa, pelo período de 21 (vinte e um) meses.
PE nº 2021007/Ata SRP 2022/12762	ETICE - EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ	943001 (https://www.etice.ce.gov.br/registro-de-preco-de-tic-rp-vigente-atas-protecao-de-rede-firewall/)	A presente Ata tem por objeto o Registro de preços para futuras e eventuais contratações de solução de proteção de redes incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, de acordo com as especificações e quantitativos previstos no Anexo I - Termo de Referência de Pregão

			Eletrônico nº 20210007-ETICE, que passa a fazer parte desta Ata, com as propostas de preços apresentadas pelos prestadores de serviços classificados em primeiro lugar, conforme consta nos autos do Processo nº 04358544/2021.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público?	Solução 1		X	
	Solução 2		X	
	Solução 3		X	

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução 1			X
	Solução 2			X
	Solução 3			X
Há necessidade de adequação do ambiente do órgão ou entidade?	Solução 1			X
	Solução 2			X
	Solução 3			X

10. Registro de soluções consideradas inviáveis

10.1. Conforme § 1º do art. 11, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

10.2. Assim sendo, as soluções 2 e 3 foram consideradas inviáveis, conforme justificativas abaixo:

10.2.1. A Solução 2, “Aquisição de novos appliances de Firewall NGFW com licenças de software e suporte técnico e aquisição de solução de segurança integrada à solução de rede definida por software (SDN)”, é considerada inviável por não haver reaproveitamento dos ativos de firewall atuais, recursos de hardware e de software que foram bastante onerosos, de implementação complexa e de difícil absorção de conhecimento do funcionamento. Ademais, os ativos ainda possuem condições de serem utilizados em sua plenitude, desde que mantido o licenciamento. Haverá necessidade de adequação do ambiente do órgão para substituir os novos equipamentos pelos atuais, bem como instalar, configurar e aprender a gerenciar os novos equipamentos. Logo, foi descartada ante ao exposto e motivos apresentados neste ETPC.

10.2.2. A Solução 3, “Segurança como Serviço - SECaaS (Security as a Service)”, é considerada inviável, também por não haver reaproveitamento dos ativos de firewall atuais. Ademais, substituir todo o serviço e ignorar os atuais ativos de TIC que podem ter sua vida útil prorrogada, poderia ensejar em um investimento desnecessário, haja vista que a contratação completa do modelo SECaaS representaria uma imediata inutilização dos Appliances. Além disso, poderia resultar, em tese, riscos ao transferir por completo a gestão da segurança cibernética para terceiros que passariam a gerir os serviços sensíveis e essenciais ao órgão, bem como de parte da sua segurança da informação. Este modelo ainda não é muito comum na administração pública e acredita-se que não esteja maduro o suficiente para ampla adoção. Logo, foi descartada para o atual momento.

11. Análise comparativa de custos (TCO)

11.1. A análise comparativa de custos totais de propriedade, baseou-se em contratações similares no âmbito da Administração Pública, bem como em pesquisa ao mercado fornecedor da solução.

Lote	Item	Descrição	Unidde de Medida	Quantidade	REFERÊNCIAS													
					A PE Nº 3/2022 TC-PR		B PE Nº 34/2021 TRE-BA		C ATA SRP PE Nº 02/2021 CITEX-COMANDO DO EXÉRCITO		D		E		F		Valor Médio de Referência	
					Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2		-					280.159,75	560.319,50	331.000,00	662.000,00	389.653,06	779.306,12	333.604,27	667.208,54
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2		-					210.442,92	420.885,84	248.500,00	497.000,00	292.689,19	585.378,38	250.544,04	501.088,07
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1	43.273,74	43.273,74	75.000,00	75.000,00	157.800,00	157.800,00	78.946,44	78.946,44	93.220,00	93.220,00	109.800,46	109.800,46	80.048,13	80.048,13
	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4							122.395,78	489.583,12	144.500,00	578.000,00	170.231,16	680.924,62	145.708,98	582.835,91
	5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1							588.869,23	588.869,23	630.000,00	630.000,00	642.500,00	642.500,00	620.456,41	620.456,41
	6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1							310.984,29	310.984,29	398.000,00	398.000,00	402.900,00	402.900,00	370.628,10	370.628,10
VALOR TOTAL GLOBAL																		2.822.265,16

Descrição	Estimativa de TCO	

da solução	Ano 1	Ano 2	Ano 3	Total
Solução Viável 1	2.822.265,16	2.985.392,09	3.157.947,75	8.965.605,00

11.2. O custo total considerou o ICTI índice setembro/2022, no percentual de 5,78% - Fonte: https://www.ipea.gov.br/cartadeconjuntura/index.php/2022/11/indice-de-custo-da-tecnologia-da-informacao-icti-setembro-de-2022/.

12. Descrição da solução de TIC a ser contratada

12.1. O detalhamento técnico da solução encontra-se descrito no APÊNDICE “A”, deste Estudo Técnico.

13. Estimativa de custo total da contratação

Valor (R$): 2.822.265,16

13.1. O custo total da contratação resta estimado em **R$ 2.822.265,16** (dois milhões, oitocentos e vinte e dois mil duzentos e sessenta e cinco reais e dezesseis centavos), anual.

14. Justificativa técnica da escolha da solução

14.1. Do ponto de vista técnico o modelo de contração proporcionará gerenciamento centralizado e simplificado do tráfego de rede, garantindo maior eficiência; compatibilidade com a solução existente; aproveitamento do know-how adquirido pela equipe técnica, que se reflete em ganhos de produtividade e segurança.

15. Justificativa econômica da escolha da solução

15.1. Em relação aos aspectos econômicos o modelo de contratação proporcionará menores custos para a implantação, em virtude de compatibilidade das soluções; menores custos com a aquisição de licenças e suporte com produtos adicionais, que teriam de ser adquiridos para compor uma solução com fabricante diverso e preservação do investimento realizado na parametrização da solução.

16. Justificativa para o parcelamento ou não

16.1. Os itens do objeto deverão ser licitados e adjudicados por lote, considerando a indivisibilidade dos mesmos, pois a soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

16.2. O agrupamento de itens irá garantir a qualidade técnica da solução não prejudicando a competividade do certame, já que há várias empresas no mercado de fornecimento da solução na forma agrupada.

17. Benefícios a serem alcançados com a contratação

17.1. Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

a) Impedir o acesso não autorizado ao ambiente tecnológico da ANTT;

b) Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

c) Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

d) Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet;

e) Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, dentre outros;

f) Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas, controlando a banda de internet a fim de evitar abusos em sua utilização.

18. Providências a serem Adotadas

18.1. Trata-se de renovação das licenças de uso de software dos appliances de Firewall e aquisição de solução de segurança integrada à solução de rede definida por software (SDN), incluindo garantia, atualização de software e suporte técnico, para atender as necessidades da ANTT, ou seja, na forma de aquisição de bens. Dessa forma, não há necessidade de adequação do ambiente tecnológico. As atividades serão realizadas utilizando os recursos computacionais já disponíveis na Agência.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

Com base nas informações levantadas ao longo do estudo técnico preliminar, os integrantes requisitante e técnico, da equipe de planejamento, declaram que a contratação é viável, do ponto de vista técnico e econômico, sendo relevante e essencial para o desenvolvimento das atividades e trabalhos realizados pela Agência Nacional de Transportes Terrestres.

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019, da Secretaria de Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação.

20. Responsáveis

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019.

VICTOR HUGO GOUVEIA DE LUCENA LIMA

Integrante Técnico

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019.

JOÃO PROCÓPIO DO REGO NETO

Integrante Requisitante

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 - APÊNDICE A - Requisitos Técnicos da Solução Firewall_ETP_atualização.pdf (262.72 KB)

Anexo I - APÊNDICE A - Requisitos Técnicos da Solução Firewall_ETP_atualização.pdf

APÊNDICE "A"

REQUISITOS MÍNIMOS DA SOLUÇÃO

1. DESCRIÇÃO DOS REQUISITOS MÍNIMOS DA SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO

1.1. Contratação de expansão tecnológica para a solução de segurança de perímetro, abrangendo o fornecimento de equipamento, licenças e prestação de serviços de renovação de garantia e suporte técnico, para um período de 12 (doze) meses.

Lote	Item	Descrição	Unidade de Medida	Quantidade
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1
	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4

	5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1
	6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1

2. <u>ITENS 1, 2 e 3</u>

2.1. FUNCIONALIDADE DE FIREWALL

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

2.1.1.1. 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.

2.1.2. Realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

2.1.3. Deve suportar os seguintes tipos de NAT:

2.1.3.1. 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.

2.1.4. Enviar logs para sistemas de monitoração externos, simultaneamente;

2.1.5. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

2.1.6. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

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

2.1.8. Deve suportar NAT64.

2.1.9. Suportar OSPF graceful restart.

2.1.10. Deve permitir a segregação entre o plano de dados de gerenciamento do plano de dados de rede.

2.1.11. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, WEB, alterações de política e comunicação SNMP.

2.1.12. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, inclusive com a capacidade de aplicação de filtros personalizados. A ferramenta deve ter a opção de gravar o tráfego capturado em arquivos do tipo CAP, PCAP ou equivalente.

2.1.13. 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).

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

2.2. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

2.2.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.

2.2.2. Controle de políticas por usuários, grupos de usuários, IPs e redes.

2.2.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2.

2.2.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.2.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

2.2.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.

2.2.5.2. Reconhecer pelo menos 2.800 (Duas mil e oitocentos) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

2.2.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não.

2.2.7. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

2.2.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo.

2.2.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.

2.2.10. Atualizar a base de assinaturas de aplicações automaticamente;

2.2.11. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

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

2.2.13. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística.

2.2.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

2.2.15. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

2.2.16. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

2.2.16.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.2.16.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes.

2.2.16.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local.

2.2.16.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.2.16.5. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário.

2.2.16.6. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs.

2.2.16.7. Suportar a criação de categorias de URLs customizadas.

2.2.16.8. Suportar a exclusão de URLs do bloqueio, por categoria.

2.2.16.9. Permitir a customização de página de bloqueio.

2.2.17. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede.

2.2.18. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários.

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

2.3. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

2.3.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

2.3.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.

2.3.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

2.3.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

2.3.5. Detectar e bloquear a origem de portscans.

2.3.6. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.

2.3.7. Possuir assinaturas para bloqueio de ataques de buffer overflow.

2.3.8. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, IMAP, SMB e FTP.

2.3.9. Suportar bloqueio de arquivos por tipo.

2.3.10. Identificar e bloquear comunicação com botnets.

2.3.11. Deve suportar referência cruzada com CVE.

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

2.3.13. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada.

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

2.3.15. Suportar rastreamento de vírus em arquivos pdf.

2.3.16. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.).

2.3.17. Possuir a capacidade de prevenção de ameaças não conhecidas.

2.3.18. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado.

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

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

2.3.21. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

2.3.22. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado.

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

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

2.3.25. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2010, 2013 e 2016.

2.3.26. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente.

2.3.27. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização.

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

2.3.29. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

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

2.3.31. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm.

2.3.32. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo.

2.3.33. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração: 4.33.1. Número de arquivos emulados.

2.3.34. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

2.3.34.1. Arquivos scaneados;

2.3.34.2. Arquivos maliciosos.

2.4. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

2.4.1. Suportar a criação de políticas de QoS por:

2.4.1.1. Endereço de origem, endereço de destino e por porta;

2.4.2. O QoS deve possibilitar a definição de classes por:

2.4.2.1. Banda garantida, banda máxima e fila de prioridade;

2.4.2.2. Disponibilizar estatísticas RealTime para classes de QoS;

2.5. FUNCIONALIDADES DE VPN

2.5.1. Suportar VPN Site-to-Site e Cliente-To-Site.

2.5.2. Suportar IPSec VPN.

2.5.3. Suportar SSL VPN.

2.5.4. A VPN IPSEc deve suportar:

2.5.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES-XCBC, AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI.

2.5.5. A VPN SSL deve suportar:

2.5.5.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

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

2.5.5.3. Deve ser capaz de informar se a senha do usuário da VPN SSL autenticado via Microsoft Active Directory está próxima a expirar.

2.5.5.4. Atribuição de endereço IP nos clientes remotos de VPN.

2.5.5.5. Atribuição de DNS nos clientes remotos de VPN.

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

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

2.5.5.8. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Windows 7 e Windows 8.

3. <u>ITEM 4</u>

3.1. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA

3.1.1. A solução de segurança deve operar como um serviço vinculado à solução de microssegmentação da Cisco (ACI).

3.1.2. A solução deve realizar a inspeção do tráfego em camadas L4 a L7.

3.1.3. A solução deve contemplar funcionalidades de controle de acesso e segurança como funcionalidades de firewall, controle de aplicações e filtragem de URL's, prevenção de ameaças (IPS, Antivírus, Anti-bot, Antimalware), suporte para conexões VPN IPSec de forma integrada e simultânea, além de proteção à nível de sandboxing fornecendo proteção contra ataques de dia zero.

3.1.4. A solução deve realizar a inspeção do tráfego lateral (Leste e Oeste) direcionado ao serviço de microssegmentação do Cisco ACI.

3.1.5. A solução deve realizar a inspeção do tráfego Norte e Sul direcionado ao serviço.

3.1.6. A solução deve estar completamente licenciada para 4 leafs conectados ao APIC.

3.1.7. A solução deve ser capaz de importar objetos criados na solução do Cisco ACI para a console de gerenciamento de segurança.

3.1.8. A política de segurança deve refletir objetos, como EPG (End Point Groups) importados do Cisco ACI, de forma automática, e permitir com que eles possam ser utilizados dentro da política de controle de acesso.

3.1.9. A solução de gateway de segurança e gerência centralizada deverão permitir serem instaladas em máquinas virtuais.

3.1.10. No caso de solução via software, em caso de perda do ambiente, deverá ser possível que a própria CONTRATANTE consiga reestabelecer o firewall em outra máquina sem a necessidade de acionar a CONTRATADA, mesmo que necessário validação do licenciamento. Se a solução

ofertada for Appliance, deverá ser disponibilizada duas caixas com licença de High Availability (H.A), sendo aceito, no mínimo a solução Ativo x Passivo.

3.1.11. Em caso de solução software, deverá ser devidamente compatível e homologado, com Cisco ACI nas versões: 5.x, 4.x ,3.1(2*), 3.1(1*), 3.0(2*), 3.0(1*).

3.1.12. Em caso de licenciamento por software, todos os recursos hardware necessários para o pleno funcionamento da solução será provido pela CONTRATANTE, no caso de Appliance este deve ser fornecido pela CONTRATADA.

3.1.13. A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte à criação de "pools" de gateways virtuais.

3.2. FUNCIONALIDADE DE FIREWALL

3.2.1. A solução deve consistir em funcionalidades de proteção de próxima geração.

3.2.2. 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.

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

3.2.4. Realizar upgrade via SCP, SFTP e https via interface WEB.

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

3.2.6. 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.

3.2.7. Deve suportar os seguintes tipos de NAT:

3.2.8. 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.

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

3.2.10. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.

3.2.11. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

3.2.12. Enviar logs para sistemas de monitoração externos, simultaneamente.

3.2.13. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

3.2.14. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

3.2.15. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.2.16. Autenticação integrada via Kerberos.

3.2.17. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP;

3.2.18. As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.

3.2.19. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

3.2.20. A solução deve ter a capacidade de operar através de uma única instancia de Firewall 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).

3.2.21. Deverá suportar redundância e balanceamento de links, tendo capacidade mínima de 2 links de internet.

3.2.22. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

3.2.23. Deve permitir a configuração do tempo de checagem para cada um dos links.

3.3. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

3.3.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.

3.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes.

3.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.

3.3.4. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

3.3.4.2. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.3.4.3. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

3.3.4.4. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

3.3.4.5. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

3.3.5. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

3.3.6. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

3.3.7. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer);

3.3.8. Possuir mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador

da solução desejar bloquear apenas as subcategorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

3.3.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

3.3.10. Atualizar a base de assinaturas de aplicações automaticamente;

3.3.11. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

3.3.12. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.3.13. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

3.3.14. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

3.3.15. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.3.16. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

3.3.17. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

3.3.18. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.3.19. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

3.3.20. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

3.3.21. Suportar base ou cache de URLs local, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

3.3.22. Suportar a criação de categorias de URLs customizadas;

3.3.23. Suportar a exclusão de URLs do bloqueio, por categoria;

3.3.24. Permitir a customização de página de bloqueio;

3.3.25. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

3.3.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

3.3.27. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal).

3.4. FUNCIONALIDADE DE FILTRO DE DADOS

3.4.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

3.4.1.1. PCI - credit card numbers;

3.4.1.2. HIPAA - Medical Records Number – MRN;

3.4.1.3. International Bank Account Numbers – IBAN;

3.4.1.4. Source Code – JAVA;

3.4.1.5. U.S. Social Security Numbers - According to SSA;

3.4.1.6. Salary Survey Terms;

3.4.1.7. Viewer File – PDF;

3.4.1.8. Executable file;

3.4.1.9. Database file;

3.4.1.10. Document file;

3.4.1.11. Presentation file;

3.4.1.12. Spreadsheet file.

3.4.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

3.4.3. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

3.4.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

3.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

3.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

3.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.

3.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo.

3.5.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

3.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo.

3.5.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.5.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP

Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.5.6.2. Detectar e bloquear a origem de portscans;

3.5.6.3. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

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

3.5.6.5. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

3.5.6.6. Suportar bloqueio de arquivos por tipo;

3.5.6.7. Identificar e bloquear comunicação com botnets;

3.5.6.8. Deve suportar referência cruzada com CVE;

3.5.7. Em cada proteção de segurança, deve estar incluso informações como:

3.5.7.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

3.5.7.2. Severidade;

3.5.7.3. Tipo de ação a ser executada.

3.5.8. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

3.5.9. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

3.5.10. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

3.5.11. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

3.5.12. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.5.13. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

3.5.14. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

3.5.15. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

3.5.16. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente;

3.5.17. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

3.5.18. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

3.5.19. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados;

3.5.20. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

3.5.21. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

3.5.22. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

3.5.23. A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

3.5.24. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

3.5.25. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

3.5.26. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

3.5.27. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

3.5.28. A solução deve permitir a criação de White Lists baseado no MD5 do arquivo;

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

3.5.30. Suportar rastreamento de vírus em arquivos pdf;

3.5.31. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

3.5.32. Possuir a capacidade de prevenção de ameaças não conhecidas;

3.5.33. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada;

3.5.34. A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

3.5.35. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

3.5.36. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

3.5.38. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

3.5.39.

3.5.40. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede;

3.5.41. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

3.5.42. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

3.6. **FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO**

3.6.1. Suportar a criação de políticas de QoS por:

3.6.1.1. Endereço de origem, endereço de destino e por porta.

3.6.2. O QoS deve possibilitar a definição de classes por:

3.6.2.1. Banda garantida, banda máxima e fila de prioridade.

3.6.2.2. Disponibilizar estatísticas em tempo real para classes de QoS.

3.7. **FUNCIONALIDADES DE VPN**

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

3.7.2. Suportar IPSec VPN;

3.7.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

3.7.4. Suportar SSL VPN;

3.7.5. A solução de VPN Client-To-Site deve suportar e estar devidamente licenciada para 50 usuários simultâneos;

3.7.6. A VPN IPSEc deve suportar:

3.7.6.1. 3DES, Autenticação MD5, SHA-1 e SHA-2, Diffie-Hellman Group 1, Group 2, Group 5, Group 14 e Group 20, Algoritmo Internet Key Exchange (IKE) e IKE V2, AES 128 e 256 (Advanced Encryption Standard), SHA-256 e SHA-512 e Autenticação via certificado IKE PKI.

3.7.7. A VPN SSL deve suportar:

3.7.7.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

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

3.7.7.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

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

3.7.7.5. Atribuição de DNS nos clientes remotos de VPN;

3.7.7.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

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

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

3.7.7.9. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android.

3.7.8. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10, Windows 11 e MacOS X.

3.8. MÓDULO DE GERÊNCIA

3.8.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento.

3.8.2. A solução deverá ser gerenciada pelo mesmo sistema de gerenciamento das soluções de proteção de perímetro existente no órgão.

3.8.3. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, de, no mínimo 1 (um) mês.

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

3.8.5. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre.

3.8.6. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo.

3.8.7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

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

3.8.9. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).

3.8.10. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

3.8.11. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

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

3.8.13. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.

3.8.14. Suportar backup das configurações e rollback de configuração para a última configuração salva.

3.8.15. Suportar validação de regras antes da aplicação.

3.8.16. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

3.8.17. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada.

3.8.18. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre.

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

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

3.8.21. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).

3.8.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

3.8.23. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

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

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

3.8.26. Deve ser possível exportar os logs em CSV ou TXT.

3.8.27. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

3.8.28. Possibilitar rotação do log.

3.8.29. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

3.8.29.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego.

3.8.30. Deve permitir a criação de relatórios personalizados.

3.8.31. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5, 6 ou superior).

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

3.8.33. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações através de RestAPI.

3.8.34. Deve consolidar logs e relatórios de todos os dispositivos administrados.

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

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

3.8.37. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.

3.8.38. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo:

3.8.38.1. ISO 27001 e ISO 27002;

3.8.38.2. PCI-DSS;

3.8.38.3. NIST 800-41;

3.8.38.4. GDPR (base da norma LGPD).

3.8.39. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição irá seguir. Não sendo permitido licenciamento mensal “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.

3.8.40. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.

3.8.41. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior.

3.8.42. Permitir a customização do padrão regulatório da própria instituição.

3.8.43. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança.

3.8.44. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados.

3.8.45. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual.

3.8.46. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança.

3.8.47. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.

3.8.48. Possuir alertas de políticas e os potenciais violações de conformidade.

3.8.49. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.

3.8.50. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real.

3.8.51. Permitir que os relatórios possam ser salvos, enviados e impressos.

3.8.52. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

3.8.53. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

3.8.54. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

3.8.55. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.8.56. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

3.8.57. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

3.8.58. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tantos gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

3.8.59. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

3.8.60. Criar certificados digitais para acesso dos usuários VPN;

3.8.61. Criar certificados digitais para VPNs Site-to-Site;

3.8.62. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

3.8.63. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

3.8.64. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição;

3.8.65. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma

única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

3.8.66. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

3.8.67. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes Pps e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

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

3.8.69. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

3.8.70. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

3.8.71. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

3.8.72. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

3.8.73. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

3.8.74. A solução deve ser capaz de personalizar e criar regras de correlação;

3.8.75. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

3.8.76. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

4. <u>ITENS 5 e 6</u>

4.1. REQUISITOS TÉCNICOS DA SOLUÇÃO DE PROTEÇÃO DE DDoS

4.1.1. REQUISITOS GERAIS

4.1.1.1. A solução DDoS deve ser um dispositivo dedicado e não uma função com licença em um Firewall, ou em um Balanceador.

4.1.1.2. Capacidade de mitigação: O sistema deve mitigar ataques DDoS ao menos a uma taxa mínima de 7.2 milhões de pacotes por segundo, sem bloquear ou afetar de maneira grave o tráfego legítimo. De igual forma, se exige uma capacidade mínima de mitigação em BW de 6Gbps e um desempenho de sessões concorrentes sob ataque ilimitado.

4.1.1.3. O sistema deve suportar mitigação de ataques SSL/TLS utilizando hardware dedicado, com Capacidade de tratar ao menos 20KCPS (RSA 2K).

4.1.1.4. O equipamento deve ter uma latência sob ataque menor ou igual a 60 microsegundos.

4.1.1.5. O sistema deve suportar mitigar ataques em IPv4 e IPv6.

4.1.1.6. O sistema, ao posicionar-se em linha, deverá ser completamente transparente, sem introduzir nenhuma alteração na rede. Adicionalmente, deve permitir habilitar “Interface grouping” ou “Interface tracking”, de tal forma que quando se desconecte uma porta, sua porta par também se desconecte, realizando assim a desconexão total do segmento que se está inspecionando de forma inline.

4.1.1.7. O sistema deve ter fontes redundantes e devem ser do tipo “hot-swap”.

4.1.2. CONECTIVIDADE E ÓTICAS

4.1.2.1. O equipamento deve contar com ao menos 2 portas com SFP+ para interconexão a 10Gbps futura.

4.1.2.2. O equipamento deve contar com proteção de ao menos 3 segmentos de cobre com bypass interno.

4.1.3. PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO (DDOS)

4.1.3.1. O sistema deve proteger contra inundação de anomalias de pacotes. Ao menos:

a) Unrecognized L2 Format;
b) Incorrect IPv4 Checksum;
c) Invalid IPv4 Header or Total Length;
d) Invalid IP Header or Total Length;
e) Inconsistent IPv6 Headers;
f) Invalid L4 Header Length;
g) TTL Equal to 0;
h) IPv6 Hop Limit Reached;
i) Unsupported L4 Protocol;

j) Invalid TCP Flags;
k) Source or Dest. Address same as Local Host;
l) Source Address same as Dest Address (Land Attack).

4.1.3.2. Protecão contra ataques DDoS em camada de rede. Ao menos:

a) TCP-SYN floods;
b) TCP ACK + fim Flood;
c) TCP-SYN + ACK floods;
d) TCP-RESET floods;
e) TCP fragments flood;
f) UDP Floods;
g) UDP Fragmented Floods;
h) ICMP Floods;
i) IGMP Floods.

4.1.3.3. Proteção de ataques DDoS em camada de aplicação. Incluindo ao menos:

a) Todo tipo de ataques de tipo reflection, independente do protocolo camada 7 utilizado;
b) Todo tipo de ataques de tipo Amplification, independente do protocolo camada 7 utilizado;
c) DNS Floods;
d) HTTP Floods;
e) Low and SLow.

4.1.3.4. O sistema deve ter proteção DDoS originada de trás de CDN ou proxies.

4.1.3.5. O sistema deve ter mecanismos de proteção para ataques de tipo dia zero e ataques conhecidos.

4.1.3.6. O sistema deve ter mecanismo de prevenção de falsos positivos DDoS através de desafios e respostas. Como mínimo:

a) Desafios e respostas para TCP;
b) Desafios e resposta HTTP: 302 Redirect, Java Script;
c) Desafios e resposta em DNS.

4.1.3.7. O sistema deve ter protecão TCP Out-of–State Flood Attack

4.1.3.8. O sistema deve ter proteção granular para limitar por PPS e Kbps o tráfego enviado um destino com certos parâmetros definidos.

4.1.3.9. O sistema deve ter proteção contra ferramentas conhecidas de DoS.

4.1.4. ANÁLISE DE COMPORTAMENTO

4.1.4.1. O sistema deve proporcionar detecção de ataques DoS/DDoS em tempo real, baseado em Análise de Comportamento ou estatístico. Não se admitem soluções baseadas em limites estáticos de nenhum tipo já que se busca reduzir a quantidade de falsos positivos que possam existir na rede.

4.1.4.2. O sistema deve prevenir falsos positivos na detecção causados por flash crowds ou aumentos de tráfego súbito, através da correlação de parâmetros que variem com a taxa de tráfego com aqueles parâmetros que não variam com a taxa de tráfego.

4.1.4.3. Em fase de Proteção, O sistema deve atuar de forma automática, mitigando o ataque sem intervenção humana.

4.1.4.4. O sistema não deve realizar mitigação através de rate limits. A mitigação do ataque deve ser cirúrgica, unicamente bloqueando o tráfego que corresponda ao ataque e deixando passar o tráfego legítimo, ainda que o endereço IP de origem seja o mesmo do atacante.

4.1.4.5. O sistema deve suportar proteção comportamental ou estatística contra o mal uso da aplicação ou da red o contra ataques de DoS e DDoS. A proteção comportamental deve resultar na criação de uma contra-medida em tempo real para a mitigação dos ataques de forma imediata.

4.1.4.6. O sistema deve ter proteção contra vetores de ataques previamente desconhecidos

4.1.4.7. O sistema deve proteger contra ataques DDoS de tipo Burst utilizando Análise de Comportamento e mitigação cirúrgica automática, em tempo real.

4.1.4.8. O sistema deve basear sua decisão de bloqueio na informação de excesso de tráfego contida em Burst prévios e deve ser capaz de readaptar-se em caso de que o vetor de ataques DDoS no Burst varíe.

4.1.4.9. O sistema deve detectar e bloquear Comportamentos anômalos próprios de scans de IP e portas à rede, com o fim de prevenir a enumeração de recursos da entidade.

4.1.5. PROTEÇÃO DNS

4.1.5.1. O sistema deve suportar proteção DDoS DNS baseado em Análise de Comportamento de aplicação.

4.1.5.2. O sistema a nível de Análise de Comportamento ou estatístico DNS deve observar os seguintes parâmetros:

4.1.5.2.1. O sistema deve suportar um método de proteção de DNS mediante mecanismos de segurança positiva e negativa que permitam a proteção de ataques

4.1.5.2.2. O sistema deve suportar sistemas de proteção de DNS Challenge para limitar o tráfego malicioso mediante mecanismos de descarte de pacotes que reduzam os falsos positivos.

4.1.5.2.3. O sistema deve permitir crear listas brancas de subdomínios de forma manual ou automática.

4.1.5.3. A proteção de DNS deve ser completamente Stateless, Ingress-Only e não deve realizar contagens de NXDomains.

4.1.6. PROTEÇÃO SSL/TLS

4.1.6.1. A solução deve contar com hardware dedicado, o qual poderá ser interno ou externo, para o tratamento de tráfego SSL.

4.1.6.2. Proteção contra ataques DDoS Criptografados com SSL / TLS tanto na camada SSL como na camada HTTPS.

4.1.6.3. A solução deve poder autenticar sessões SSL com módulo de criptografia SSL para autenticar sessões legítimas e bloquear sessões de ataque criptografados por SSL.

4.1.6.4. A proteção SSL contra ataques de Negação de serviços, no deve cifrar/descifrar o tráfego quando não há ataque. A proteção só deve atuar em caso de ataque.

4.1.6.5. A proteção SSL deve funcionar em modo Ingress Only, sem necessidade de ver o tráfego que vem do servidor. Em outras palavras, a proteção deve ser Stateless.

4.1.6.6. O sistema deve habilitar flexibilidade com certificados wildcard de SSL, com o objeto de simplificar as operações e minimizar o número total de certificados administrados.

4.1.7. PERFIS DE GEOLOCALIZAÇÃO

4.1.7.1. A solução deve prover proteção de geolocalização que visualize os principais países atacantes de DDoS utilizando um mapa em tempo real.

4.1.7.2. A solução deve bloquear o tráfego de países específicos de imediato, com um clique de um botão na console de administração, utilizando um novo mapa de ataque dedicado, que apresente os principais países atacantes.

4.1.7.3. A solução de mitigação deve suportar dois modos de ativação de bloqueio: Sempre ativo e sob demanda.

4.1.7.4. A proteção deve admitir a configuração de listas de bloqueio/lista de permissões por objeto protegido, e que permita aos operadores da entidade a Capacidade de configurar rapidamente o bloqueio de país e as listas de permissões.

4.1.8. PROTEÇÃO CONTRA ATAQUES CONHECIDOS

4.1.8.1. A solução deve contar com um mecanismo de proteção de ataques DDoS lançados com ferramentas Conhecidas o que utilizem exploits conhecidos. Este mecanismo deve estar baseado em uma base de dados de assinaturas que contenha os parâmetros necessários para identificar estes ataques conhecidos.

4.1.8.2. As assinaturas devem ser atualizadas de forma automática através da internet durante a duração do suporte.

4.1.8.3. Ao ser a primeira linha de defesa, além de ataques DDoS Conhecidos deve proteger ao menos contra seguintes vulnerabilidades:

a) Web application vulnerabilities;
b) Mail server vulnerabilities;
c) FTP servers vulnerabilities;
d) DNS Vulnerabilities;
e) SQL Servers Vulnerabilities;
f) VoIP (SIP) vulnerabilities;
g) Buffer overflow.

4.1.9. REQUISITOS TÉCNICOS SISTEMA DE ADMINISTRAÇÃO CENTRALIZADA

4.1.9.1. O sistema deve suportar administração centralizada para toda A solução de DDoS.

4.1.9.2. O sistema deve ser tipo virtual appliance que permita instalar-se sobre Hyper-V ou VMware ESXi 5 ou superior na infraestrutura do cliente.

4.1.9.3. Deve-se incluir as licenças necessárias para poder ter Capacidade completa de realizar alterações e configurações da solução de mitigação de ataques.

4.1.9.4. O sistema deve suportar Web User interface para toda a configuração do dispositivo.

4.1.9.5. O sistema deve suportar um padrão industrial API para integração com aplicações personalizadas. A API deve ser oferecida sem custos.

4.1.9.6. A API deve estar completamente documentada.

4.1.9.7. A solução de administração deve prover a opção de personalizar "dashboards" por usuário, por política que mostrem informação em tempo real como: "top attacks view, traffic monitoring view, SLA reports (bandwidth consuming attack) view, etc".

4.1.9.8. O sistema deve suportar Acessos seguros HTTPS, SSH.

4.1.9.9. O sistema deve suportar o envio de eventos através de SYSLOG e SNMP.

4.1.9.10. O sistema deve suportar a configuração da solução através de scripts.

4.1.9.11. O sistema deve suportar RBAC para os administradores de múltiplos dispositivos.

4.1.9.12. O sistema deve suportar LDAP, RADIUS, TACACS e autenticação local.

4.1.9.13. O sistema deve suportar guardar toda a configuração em um servidor remoto.

4.1.9.14. O sistema deve suportar múltiplos administradores logados ao tempo na interface GUI.

4.1.9.15. O sistema deve suportar NTP.

4.1.9.16. O sistema deve gerar um alarme por cada alteração administrativa feita no dispositivo.

4.1.9.17. O sistema deve prover os MIBS completos.

4.1.9.18. O sistema deve suportar realização de backups por SCP, FTP, SFTP.

4.1.9.19. O sistema deve suportar ferramentas de diagnóstico como core dumps, arquivos de configuração, logs, etc.

4.1.9.20. O sistema deve suportar REST sobre HTTPS.

4.1.9.21. O sistema deve suportar a criação de scripts personalizados pela entidade que podem ser executados sobre múltiplos dispositivos ao mesmo tempo.

4.1.9.22. O sistema deve suportar relatórios históricos das soluções Anti DDoS.

4.1.9.23. Estes relatórios poderão ser programados e enviados de forma automática.

4.1.9.24. Deve contar com os seguintes protocolos para enviar os relatórios programados: via SFTP e SMTP.

4.1.9.25. Os seguintes são os formatos de relatórios que deve suportar o módulo de relatórios históricos: PDF, HTML, CSV, TEXT.

4.1.9.26. Deve contar com filtros granulares para personalizar o tipo e a informação nos relatórios.

4.1.9.27. Deve contar com relatórios out of the box, entre relatórios gerais de segurança e relatórios específicos da solução. Deve ter capacidade de gerar ao menos os seguintes relatórios:

a) Ataques por largura de banda;
b) Ataques por duração.
c) Ataques permitidos e negados;
d) Ataques críticos;
e) Relatórios de tipo TOP:
    a. Destinos;
    b. Origem;
    c. Aplicação.

---------- FIM DO APÊNDICE “A” ----------