MINISTÉRIO DA DEFESA - MD
SECRETARIA-GERAL - SG
SECRETARIA DE ORÇAMENTO E ORGANIZAÇÃO INSTITUCIONAL - SEORI
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DETIC

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.
O presente ETP tem por objetivo levantar os elementos necessários e suficientes à avaliação e escolha da opção mais vantajosa para eventual aquisição de equipamentos e sistemas de segurança de TI para as redes de dados da Administração Central do Ministério da Defesa (ACMD), decorrente das necessidades apresentadas nos Documentos de Oficialização da Demanda (DOD), bem como demostrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

As redes de dados da Administração Central do Ministério da Defesa (ACMD) são compostas pela rede administrativa, mantida pela Secretaria Geral (SG) e pela Rede Operacional de Defesa (ROD), mantida pelo Estado-Maior Conjunto das Forças Armadas (EMCFA).

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS – (IN. 01/2019, art. 11, Inciso I).

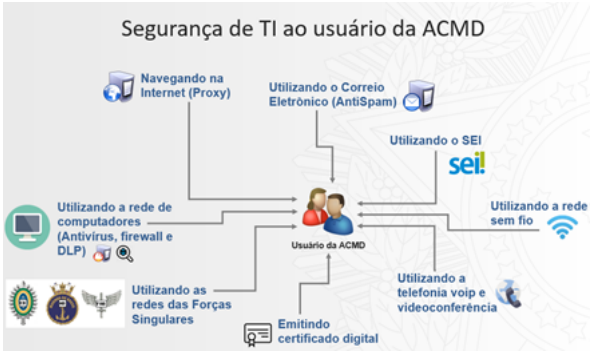
1.1 - Identificação das necessidades de negócio

Área de negócio: Secretaria Geral

O Departamento de Tecnologia da Informação e Comunicação (DETIC) tem como uma de suas atribuições, a de disponibilizar e gerir os recursos de Tecnologia da Informação e Comunicação (TIC) que sustentam as atividades do negócio da ACMD. Para tanto, faz-se necessário analisar as necessidades de soluções de TIC, com vistas ao desenvolvimento ou à contratação de tais soluções.

Compete ao Núcleo de Segurança da Informação e Comunicações (NUSIC), do DETIC, planejar, implantar, administrar e manter os ativos de segurança de Tecnologia da Informação (TI) e comunicação no âmbito da administração central do Ministério da Defesa.

Atualmente, o NUSIC mantém em funcionamento diversas ferramentas e soluções de segurança de TI, que englobam equipamentos (*hardwares*) e sistemas (*softwares*), e que, trabalhando em conjunto, garantem níveis de segurança aceitáveis aos usuários da rede administrativa da ACMD no desenvolvimento de suas atividades laborais. Algumas dessas atividades estão demonstradas na figura abaixo:



As ferramentas e os equipamentos de segurança, responsáveis atualmente pelas proteções aos usuários da rede administrativa da ACMD, estão suportados por contratos em fase final de vigência e, portanto, faz-se necessária a manutenção de sistemas e equipamentos que permitam garantir a segurança de TI da rede administrativa da ACMD, em conformidade com os normativos vigentes, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD) e às normas do Gabinete de Segurança da Informação da Presidência da República.

Nesse sentido, para a continuidade e modernização das soluções de segurança existentes, são relacionadas as seguintes necessidades de negócio a serem atendidas:

- a proteção das estações de trabalho;
- o monitoramento e a proteção do sistema de arquivos;
- a proteção e o controle da Internet disponibilizada aos usuários;
- a proteção do trâmite de mensagens do Correio Eletrônico corporativo;
- a proteção das redes internas e redes parceiras;
- a proteção da rede sem fio;
- a proteção do sistema de telefonia;
- a proteção dos portais (defesa.gov.br);
- a proteção dos sistemas corporativos;
- a possibilidade de realizar varreduras de vulnerabilidades; e
- a possibilidade de realizar auditorias e verificações de conformidade.

Área de negócio: EMCFA

O Sistema Militar de Comando e Controle (SISMC²) é o conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais ao C², visando atender ao Preparo e ao Emprego das Forças Armadas (FA). Abrange os Sistemas Militares de C² das FA, bem como outros sob a responsabilidade do Ministério da Defesa (MD).

Tem por finalidade fornecer os recursos de C² necessários ao funcionamento da Estrutura Militar de Defesa, a fim de atender às necessidades decorrentes do Preparo e do Emprego das FA, devendo possuir a capacidade de interagir com organizações nacionais ou internacionais, militares ou civis.

No âmbito do SISMC², a atividade de C² é desenvolvida por meio de Centros de Comando e Controle (CC²), que deverão estar interconectados entre si por meio de rede de dados segregada e segura, permitindo a necessária comunicação de dados operacionais militares entre os níveis estratégico, operacional e tático.

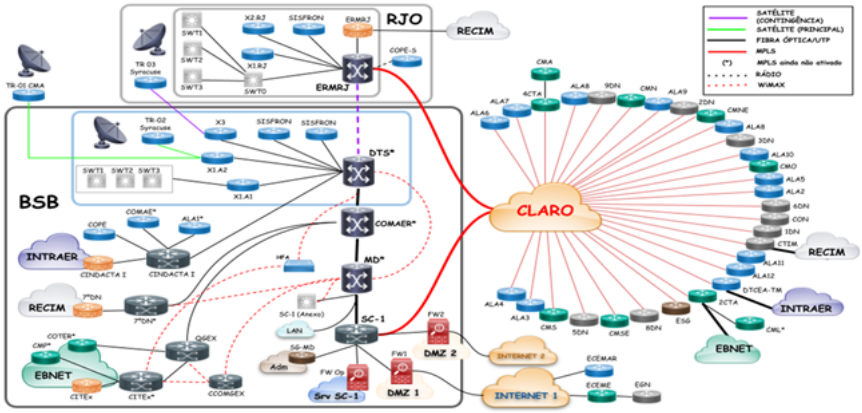
Os principais serviços e sistemas hospedados no Centro de Comando e Controle do MD (CC²MD) são: a) **acesso à ROD**; b) voz sobre IP (VoIP); c) Correio Eletrônico Operacional; d) Serviço de Transferência de Arquivos (FTP); e) Rede Privada Virtual (VPN); f) acesso às redes internas de comunicações e de dados das FA; g) acesso seguro à Internet; h) Sistema de Videoconferência; e i) sistemas de apoio à decisão.

No que concerne à Rede Operacional de Defesa (ROD), esta é a principal fornecedora dos enlaces de comunicações de dados militares operacionais, que compõe o SISMC². Está estruturada como uma *Wide Area Network* (WAN), com conectividade segregada (restrita, segura e controlada) e diversificada, por meio de um segmento terrestre e um segmento satelital, das redes de dados das Forças Armadas (RECIM 102, EBNET e INTRAER) e da Internet.

A ROD foi desenvolvida para prover os diversos serviços e sistemas hospedados no CC²MD em apoio às operações conjuntas e singulares de interesse do MD. Esses serviços asseguram um fluxo de informações em tempo real entre os CC² do SISMC², permitindo a interoperabilidade destes centros, principalmente nos níveis estratégico e operacional.

A manutenção do funcionamento seguro e contínuo das capacidades de comando e controle sob responsabilidade do MD é fundamental para a garantia da soberania nacional. Neste contexto, a segurança da informação, no âmbito do SISMC², deve empregar as melhores práticas de segurança.

A figura abaixo representa a capilaridade e os requisitos tecnológicos da ROD ao atendimento das demandas operacionais, de forma a manter elevados níveis de disponibilidade e segurança no âmbito do SISMC²:



De forma ampla e geral, as necessidades das duas áreas de negócio do MD podem ser resumidas em:

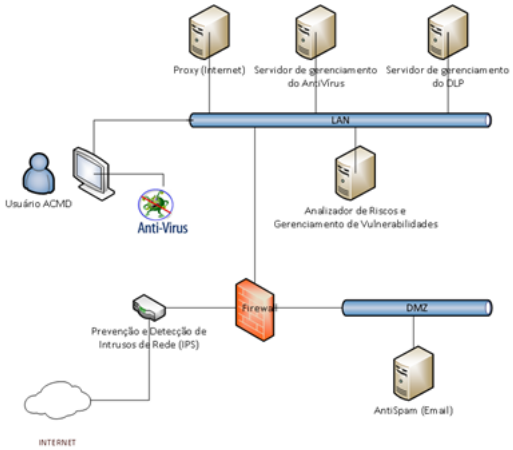
1. Manter níveis aceitáveis de disponibilidade, integridade, confidencialidade e integridade das informações do MD;
2. Garantir a segurança adequada para o tratamento das informações, dos serviços e dos sistemas suportados pelas equipes do DETIC e da ROD;
3. Reduzir o número de incidentes relacionados à segurança das redes de dados da ACMD; e
4. Garantir a continuidade do negócio, de modo que serviços essenciais não sejam interrompidos.

1.2 - Identificação das necessidades tecnológicas

Para o atendimento às necessidades de negócio listadas no item anterior, as seguintes soluções tecnológicas são indispensáveis:

1. Proteção de endpoints do tipo Anti Malware (item 5.4.3 da POSIC/MD);
2. Prevenção de perda de dados do tipo DLP (item 5.4.1 da POSIC/MD);
3. Filtragem e proteção de navegação Web do tipo Proxy (item 5.11.1 da POSIC/MD e item 8.1, alínea b, da NC03/POSIC/MD);
4. Detecção e prevenção de intrusão de rede do tipo IDS/IPS (itens 5.4.3 e 5.9.1 da POSIC/MD);
5. Filtragem e proteção de e-mails do tipo AntiSpam (item 5.10.1 da POSIC/MD e item 4.4.1, alínea f, da NC04/POSIC/MD);
6. Detecção e gerenciamento de vulnerabilidades (item 5.6.1 da POSIC/MD); e
7. Segurança de rede do tipo Firewall (itens 5.4.3 e 5.9.1 da POSIC/MD e item 8.1, alínea b, da NC03/POSIC/MD).

A figura abaixo demonstra os requisitos tecnológicos necessários ao atendimento das demandas do negócio, implementados de forma conjugada e complementar:



1.3 - Demais requisitos necessários e suficientes à escolha da solução de TIC

a. Para cada uma das necessidades tecnológicas elencadas, são necessárias: a previsão de manutenção (preventiva, corretiva e evolutiva), de suporte técnico, de garantia (quando envolver equipamento) e de repasse de conhecimento.
b. Para a manutenção dos níveis de segurança já implementados nas redes de dados da ACMD, as soluções a serem adquiridas e implementadas devem ter a sua capacidade e efetividade **iguais ou superiores às atuais**, ou seja, os requisitos técnicos serão baseados nas soluções que estão atualmente em funcionamento.
c. As soluções de número 1 (Proteção de endpoints do tipo Anti Malware), 2 (Prevenção de perda de dados do tipo DLP), 3 (Filtragem e proteção de navegação Web do tipo Proxy) e 4 (Detecção e prevenção de intrusão de rede do tipo IDS/IPS) devem ser do mesmo fabricante ou desenvolvedor. Dessa forma, convém ainda que o suporte dos serviços relacionados à essas soluções sejam realizadas pela mesma equipe, que possua o domínio técnico e a responsabilidade por toda a solução. Justificativas:

    1. Necessidade de compatibilidade entre as soluções;
    2. Necessidade de gerenciamento unificado;
    3. Necessidade de operação integrada;
    4. Necessidade de compartilhamento de informações de reputação, onde um artefato ou endereço malicioso possa ser comunicado e bloqueado em todas as soluções, de forma automática;
    5. Necessidade da manutenção da topologia atual, que tem demonstrado efetividade nas proteções aos usuários relacionadas à essas soluções.

d. Para a manutenção da disponibilidade dos serviços de Internet, do envio e recebimento de e-mails e das proteções das redes da ACMD, as soluções de número 3 (Filtragem e proteção de navegação Web do tipo Proxy), 5 (Filtragem e proteção de e-mails do tipo AntiSpam), 7 (Segurança de rede do tipo Firewall) e 4 (Detecção e prevenção de intrusão de rede do tipo IDS/IPS) devem ser implementadas de forma redundante, com equipamentos/sistemas a serem instalados em centros de processamento de dados distintos.
e. A equipe técnica do NUSIC e da ROD deverá ser capacitada para operar todas as soluções tecnológicas como forma de garantir a devida independência tecnológica com relação ao fornecedor da solução.
f. Ao adquirir-se as soluções pretendidas, busca-se o melhor atendimento às necessidades do órgão com a melhor eficiência possível, portanto, para as atividades de manutenção e suporte técnico serão permitidos, quando possível, o atendimento na modalidade remota.
g. Todas as soluções deverão ser instaladas nos centros de processamento de dados do MD ou nos locais indicados pela equipe do NUSIC e da ROD.
h. As soluções a serem adquiridas devem permitir a instalação em ambientes tecnológicos distintos, uma vez que serão utilizadas em redes segregadas e operadas de forma independente pelas equipes do NUSIC e da ROD.

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS - (IN. 01/2019, Art. 14)

Grupo	Item	Descrição do bem ou serviço	Quantidade
1	1	Licença de uso de software/programa de proteção de endpoints do tipo Anti-Malware com validade de 36 (trinta e seis) meses.	2350 licenças
	2	Licença de uso de software/programa de prevenção de perda de dados do tipo DLP com validade de 36 (trinta e seis) meses.	2350 licenças
	3	Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway com validade de 36 (trinta e seis) meses.	2350 licenças
	4	Equipamento de detecção e prevenção de intrusão de rede do tipo IDS/IPS com licenciamento e garantia de 36 (trinta e seis) meses.	2 equipamentos
	5	Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure Email Gateway com validade de 36 (trinta e seis) meses.	2350 licenças
	6	Licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades com validade de 36 (trinta e seis) meses.	2200 licenças
	7	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo I).	4 equipamentos
	8	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo II).	3 equipamentos

Tabela I

a. As quantidades acima definidas foram estabelecidas **considerando as soluções atualmente contratadas**, instaladas e operando na rede administrativa do Ministério da Defesa bem como na Rede Operacional de Defesa, justificadas da seguinte forma:

Justificativas do DETIC (Área de negócio: Secretaria Geral)

Grupo	Item	Descrição do bem ou serviço	Quantidade	Justificativas
1	1	Licença de uso de software/programa de	2100 licenças	

		proteção de endpoints do tipo Anti-Malware com validade de 36 (trinta e seis) meses.	DETIC	Quantidade de ativos na rede administrativa da ACMD, atualmente suportados pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), com o acréscimo de 100 unidades para o atendimento à Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658). As evidências da quantidade atual de ativos da rede administrativa da ACMD estão presentes no arquivo "01 - Quantitativo_ativos_DETIC.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	2	Licença de uso de software/programa de prevenção de perda de dados do tipo DLP com validade de 36 (trinta e seis) meses.	2100 licenças DETIC	Quantidade de ativos na rede administrativa da ACMD, atualmente suportados pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), com o acréscimo de 100 unidades para o atendimento à Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658). As evidências da quantidade atual de ativos da rede administrativa da ACMD estão presentes no arquivo "01 - Quantitativo_ativos_DETIC.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	3	Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway com validade de 36 (trinta e seis) meses.	2100 licenças DETIC	Quantidade de ativos na rede administrativa da ACMD, atualmente suportados pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), com o acréscimo de 100 unidades para o atendimento à Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658). As evidências da quantidade atual de ativos da rede administrativa da ACMD estão presentes no arquivo "01 - Quantitativo_ativos_DETIC.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	4	Equipamento de detecção e prevenção de intrusão de rede do tipo IDS/IPS com licenciamento e garantia de 36 (trinta e seis) meses.	2 equipamentos DETIC	Quantidade de equipamentos IDS/IPS, atualmente suportados pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), a serem substituídos nos dois ambientes de processamento de dados da rede administrativa da ACMD, visando a alta disponibilidade. A substituição ocorre em virtude tanto do término da garantia contratual, quanto da descontinuidade do suporte do equipamento atualmente utilizado, qual seja o McAfee M-3050. De acordo com informações do fabricante, disponíveis em https://kc.mcafee.com/corporate/index?page=content&id=KB87925&locale=en_US, os equipamentos dessa série chegaram em *End of Life* e *End of Support* no dia 31 de dezembro de 2021. As justificativas técnicas acerca dos novos equipamentos desejados estão presentes nos arquivos "04 - Excesso_Carga_IPS_2021-2022.xlsx" e "05 - Throughput_IPS.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	5	Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure Email Gateway com validade de 36 (trinta e seis) meses.	2100 licenças DETIC	Quantidade de licenças atualmente suportadas pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), com o acréscimo de 100 unidades para o atendimento da Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658). As evidências da quantidade atual de ativos da rede administrativa da ACMD estão presentes no arquivo "01 - Quantitativo_ativos_DETIC.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	6	Licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades com validade de 36 (trinta e seis) meses.	2200 licenças DETIC	Quantidade de ativos na rede administrativa da ACMD, atualmente suportados pelo Contrato nº 013-DEPTI-COLIC/2017-MD (0641397), com o acréscimo de 100 unidades para o atendimento à Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658), e com o acréscimo de 100 unidades para possibilitar a realização de varreduras nos demais ativos de rede e sistemas web (defesa.gov.br) gerenciados pelo DETIC. As evidências dos quantitativos requeridos estão presentes nos arquivos "01 - Quantitativo_ativos_DETIC.PNG" e "03 - Sistemas web externos (defesa.gov.br).txt" (5177658). Os sistemas e ativos internos não foram listados por questões de segurança. As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	7	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo I).	4 equipamentos DETIC	Quantidade de equipamentos Firewall, atualmente suportados pelo Contrato nº 020-DEPTI-COLIC/2017-MD (0744910), a serem substituídos nos dois ambientes de processamento de dados da rede administrativa da ACMD, visando a alta disponibilidade. Englobam os seguimentos interno (2 unidades) e externo (2 unidades) da rede administrativa da ACMD. Para os 02 equipamentos do seguimento interno, não há necessidade de alterações nas especificações técnicas, ou seja, elas foram baseadas nos equipamentos que estão em funcionamento na rede administrativa da ACMD. Já para os 02 equipamentos do seguimento externo, existe a necessidade de se obter um equipamento mais robusto, que possua velocidade de operação superior ao atual. Essa necessidade justifica-se no apoio de infraestrutura de TIC que o DETIC está prestando à Escola Superior de Defesa (ESD), conforme disponível no anexo (5177658), em virtude das implementações do novo sistema de backup, que tem demandado uma quantidade alta de *throughput* no momento em que os Jobs são executados e, finalmente, em virtude da crescente demanda pelo trabalho remoto, suportado por esses equipamentos. As justificativas técnicas acerca dos novos equipamentos desejados estão presentes nos arquivos "06 - Excesso_Carga_Firewalls_Externos_2021.PNG", "07 - Excesso_Carga_Firewalls_Externos_2022.PNG" e "08 - Throughput_Firewalls_Externos.PNG" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	8	-	-	-

Tabela II

Justificativas da ROD (Área de negócio: EMCFA)				
Grupo	Item	Descrição do bem ou serviço	Quantidade	Justificativas
1	1	Licença de uso de software/programa de proteção de endpoints do tipo Anti-Malware com validade de 36 (trinta e seis) meses.	250 licenças ROD	Quantidade de ativos na rede de dados da ROD, atualmente suportados pelo Termo Aditivo nº 024-DETIC CONTRAT/2020 (2370372). As evidências da quantidade atual de ativos da ROD estão presentes no arquivo "01 - Quantitativo_ROD.jpeg" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	2	Licença de uso de software/programa de	250 licenças ROD	

		prevenção de perda de dados do tipo DLP com validade de 36 (trinta e seis) meses.		Quantidade de ativos na rede de dados da ROD, atualmente suportados pelo Termo Aditivo nº 024-DETIC CONTRAT/2020 (2370372). As evidências da quantidade atual de ativos da ROD estão presentes no arquivo "01 - Quantitativo_ROD.jpeg" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	3	Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway com validade de 36 (trinta e seis) meses.	250 licenças ROD	Quantidade de ativos na rede de dados da ROD, atualmente suportados pelo Termo Aditivo nº 024-DETIC CONTRAT/2020 (2370372). As evidências da quantidade atual de ativos da ROD estão presentes no arquivo "01 - Quantitativo_ROD.jpeg" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	4	-	-	-
	5	Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure Email Gateway com validade de 36 (trinta e seis) meses.	250 licenças ROD	Quantidade de licenças atualmente suportadas pelo Termo Aditivo nº 024-DETIC CONTRAT/2020 (2370372). As evidências da quantidade atual de ativos da ROD estão presentes no arquivo "01 - Quantitativo_ROD.jpeg" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.
	6	-	-	-
	7	-	-	-
	8	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo II).	3 equipamentos ROD	O SISMC² fornece os recursos de C² necessários ao funcionamento da Estrutura Militar de Defesa (Etta Mi D) com a finalidade de atender as necessidades decorrentes do Preparo e Emprego das FA devendo possuir a capacidade de interagir com organizações nacionais ou internacionais, militares ou civis, externas à Etta Mi D. Por definição, um sistema como o SISMC² não possui requisitos que permitam definir claramente o final do seu processo de desenvolvimento, uma vez que o advento de novas tecnologias e o amadurecimento da doutrina introduzem novos requisitos, tornando o SISMC² um Sistema de Sistemas (SdS) em constante aprimoramento. Neste sentido, a Rede Operacional de Defesa (ROD) é uma das principais fornecedoras de serviços de comunicações de dados militares operacionais que compõe o SISMC², e que necessita assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que por ela trafegam. Para garantir a segurança da ROD, é imperativo priorizar as ações voltadas para a segurança da informação e comunicações, por meio de projeto de implantação de ferramentas de segurança, entre as quais, destaca-se a instalação de segurança de rede do tipo Firewall. Diante das especificidades da ROD, que necessita garantir alta disponibilidade de sua infraestrutura, almeja-se a utilização de equipamentos que suportem, entre outros, os seguintes serviços: • Manter o ambiente computacional da ROD seguro no que se diz respeito a ameaças virtuais; • Proteção contra negação de serviço (DoS); • Estabelecer controle baseado em políticas específicas para aplicações e usuários. As justificativas técnicas acerca dos equipamentos desejados estão presentes no arquivo "02 - Throughput_Firewalls_ROD.png" (5177658). As Especificações Técnicas referentes à esse item, constam no **APÊNDICE I** deste ETP.

Tabela III

b. Em observância ao que trata o art. 9 da Instrução Normativa nº 01, de 19 de janeiro de 2010, disponível em http://www.comprasnet.gov.br/legislacao/legislacaoDetalhe.asp?ctdCod=295, os equipamentos que estão em produção nas redes de dados da ACMD, a serem substituídos, serão disponibilizados em lista para publicação no fórum eletrônico de divulgação de materiais ociosos para doação a outros órgãos e entidades da Administração Pública ou serão doados a organizações militares vinculadas ao MD.

3 – ANÁLISE DE SOLUÇÕES

a. **Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:**

Os demais Órgãos ou entidades da Administração pública federal igualmente possuem necessidades de manter dispositivos e sistemas que permitam garantir a segurança de seus ativos de TI, uma vez que tal atividade reveste-se de importância para a manutenção de níveis aceitáveis de disponibilidade, integridade, confidencialidade e integridade de suas informações.

Dessa forma, foram observados nos levantamentos de preços realizados por meio de consulta ao Painel de preços (https://paineldeprecos.planejamento.gov.br/), soluções semelhantes em outros órgãos e entidades da Administração Pública. Nesse levantamento, foram identificadas soluções de segurança da informação, baseadas em diversas tecnologias. No entanto, as topologias e arquiteturas adotados em cada órgão são configurados às suas necessidades, bem como às características de seus sistemas e ativos de TI, o que faz com que cada qual, incluindo-se as redes da ACMD, possuam características e requisitos únicos e particulares.

b. **Alternativas do mercado:**

As soluções levantadas baseiam-se em soluções de código livre, gratuitas, e soluções de mercado compostas por: aquisição de equipamentos, licenças, contratação de suporte e repasse de conhecimento ou a contratação das soluções na forma de serviço.

c. **Existência de software público brasileiro**:

Foi realizada uma pesquisa no site (https://softwarepublico.gov.br), contudo não foi identificada nenhuma solução que atenda aos requisitos técnicos necessários.

d. **As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis:**

Não se aplica.

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

Não será necessária, tendo em vista a rede administrativa da ACMD bem como a Rede Operacional de Defesa já disporem de infraestrutura adequada para a implantação das soluções requeridas. Vale ressaltar que essas soluções já estão implementadas em ambas as estruturas de TI, e o que se pretende nessa contratação, é aquisição de novos licenciamentos e equipamentos bem como os respectivos suportes técnicos devido à impossibilidade de renovação dos atuais contratos.

f. **Possibilidade de aquisição na forma de bens ou contratação como serviço:**

A solução composta por equipamentos, licenças, suporte técnico e repasse de conhecimento, conforme detalhado na Tabela I do Item 2, poderá ser contratada na forma de aquisição dos bens ou fornecida na forma de serviço, com pagamentos mensais durante a vigência contratual.

Para essas duas possibilidades, os equipamentos devem ser instalados e configurados nas dependências do MD, especificamente nos centros de processamento de dados do DETIC e da ROD.

g. **Os diferentes modelos de prestação do serviço**:

Conforme item anterior, ou seja, aquisição dos bens ou contratação das soluções como serviço.

h. **Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes:**

As soluções levantadas possuem especificações, composição e características de bens e serviços diferentes entre si, conforme item Tabela I do item 2.

i. **A ampliação ou substituição da solução implantada**.

As soluções levantadas visam a aquisição de novos licenciamentos, a substituição dos equipamentos implantados com ampliação das capacidades de hardware, bem como a cobertura contratual de suporte técnico e repasse de conhecimento.

O presente Estudo Técnico Preliminar visa analisar solução para substituição de outra já implementada na rede administrativa da ACMD e na ROD, dessa forma as soluções a serem adquiridas e implementadas devem ter a sua capacidade e efetividade **iguais ou superiores às atuais**, ou seja, os requisitos técnicos serão baseados nas soluções que estão atualmente em funcionamento.

j. **As diferentes métricas de prestação do serviço e de pagamento.**

As diferentes métricas de prestação de serviço e pagamento levantadas são:

- Contratação das licenças com prazo/validade estabelecidos e pagamento único;
- Aquisição dos equipamentos com licenciamento/garantia estabelecidos e pagamento único; e
- Contratação das soluções na forma de serviço com pagamentos mensais durante a vigência contratual.

3.1 - Identificação das Soluções – (IN. 01/2019, art 11, inciso II, alínea "a" ao "i")

Item	Descrição da solução (ou cenário)
S-01	Utilização de Software Livre.
S-02	Utilização de Solução Própria.
S-03	Aquisição dos equipamentos e licenças.
S-04	Contratação das soluções na forma de serviço.

Tabela IV

3.2 – Análise Comparativo de Soluções - (IN. 01/2019, art 11, inciso III, caput)

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	S-01		X	-
	S-02		X	-
	S-03	X		-
	S-04	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	S-01		X	-
	S-02		X	-
	S-03		X	-
	S-04		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	S-01		X	-
	S-02		X	-
	S-03		X	-
	S-04		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	S-01		X	-
	S-02		X	-
	S-03	X		-
	S-04	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	S-01			X
	S-02			X

Requisito	Solução	Sim	Não	Não se Aplica
	S-03			X
	S-04			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	S-01			X
	S-02			X
	S-03			X
	S-04			X

Tabela V

Para o preenchimento dos requisitos acima, foram consideradas todas as 7 necessidades de negócio, de forma unificada.

Solução 01 – Software livre.

- Descrição:

  Software Livre é conceituado como qualquer programa de computador que pode ser usado, copiado, estudado, modificado e redistribuído sem nenhum tipo de restrição. Assim, além da sua utilização não estar vinculada ao pagamento de direitos autorais, a principal característica do Software Livre está na distribuição com o código fonte aberto, dando permissão a qualquer usuário de modificá-lo e adaptá-lo às suas necessidades individuais.

- Análise:

  Ao analisar a solução S-01 (utilização de diversas ferramentas open-source para suportar as necessidades do negócio) percebe-se que embora para este cenário o custo envolvido seja mínimo, visto que empregaria ferramentas gratuitas, o tempo que seria gasto para a pesquisa, desenvolvimento, implementação e integração de todas as ferramentas necessárias, inviabilizaria a adoção deste cenário. Cabe informar que o DETIC e a ROD não possuem profissionais com as qualificações requeridas para a implementação e integração dos softwares necessários ao atendimento das demandas listadas no item I deste Estudo. Outra questão importante é que nem todas as funcionalidades necessárias são providas por ferramentas open-source: muitas dessas ferramentas possuem versões gratuitas, com funcionalidades limitadas, e versões completas, com modelos de negócio enquadrados na Solução 03 desse ETP. Por fim, existe também a preocupação com códigos maliciosos que podem ser inseridos nessas ferramentas, de forma intencional, criando brechas para a invasão desses sistemas e também para a execução de código remoto, conforme reportagem de 12 de maio de 2022, disponível em https://canaltech.com.br/seguranca/pesquisadores-detectam-backdoors-criticas-em-repositorios-open-source-216243/.

Solução 02 – Solução própria

- Descrição:

  Solução desenvolvida pela própria organização, sem a necessidade de uma aquisição.

- Análise:

  Esta solução apresenta-se como inviável, devido à falta de pessoal especializado e às dificuldades de se desenvolver sistemas dessa complexidade com recursos humanos e materiais próprios. Ainda que fosse possível, não haveria a possibilidade de integração com as soluções atualmente utilizadas no MD, devido à complexidade desses sistemas.

  Vale reforçar que sistemas e ferramentas de segurança de TI são extremamente complexos e o MD não possui profissionais dedicados ao desenvolvimento dessas soluções no tempo requerido.

Solução 03 – Aquisição dos equipamentos e licenças.

- Descrição:

  No mercado existem diversas soluções que atendem aos requisitos técnicos necessários. Seguem abaixo as soluções identificadas e que atendem aos requisitos demandados:

Necessidade de negócio	Soluções disponíveis	Descrição
Proteção de endpoints	Sistemas de Antivírus / Anti-malware	Sistemas que objetivam detectar, proteger e remover softwares maliciosos nos ativos de TI em que são insta configurados. Normalmente agem de forma preventiva, detectando ameaças antes mesmo que elas sejam ins mas também são capazes de remediar os problemas após a infecção.
Prevenção de perda de dados	Sistemas de Data Loss Prevention	Sistemas que objetivam detectar e prevenir vazamentos de dados, exfiltração de dados ou a destruição de da organização. O termo DLP se refere tanto a ações contra a perda de dados (evento no qual os dados são defi organização) como ações contra vazamentos de dados (transferência indevida de dados para fora da fronteir
Filtragem e proteção de navegação Web	Sistemas de proxy ou Secure Web Gateway	Sistemas que atuam como um gateway pelo qual todo o tráfego de Internet passa. É utilizado para proteger na Web por meio da filtragem de URL, detecção e filtragem de código malicioso e controles de aplicativos. para detectar ou evitar que dados confidenciais saiam da organização.
Detecção e prevenção de intrusão de rede	Equipamentos ou sistemas do tipo IDS/IPS	Sistemas ou equipamentos destinados a monitorar e examinar o tráfego de rede em busca de eventos que po segurança dessa rede. Por meio do IPS é possível automatizar a proteção da rede contra acessos não autoriz de vulnerabilidades e outros tipos de ataques cibernéticos.
Filtragem e proteção de e-mails	Sistemas de Anti-spam ou Secure E-mail Gateway	Sistemas que atuam como um gateway pelo qual todos os e-mails de entrada e saída passam. É utilizado par tais como spam, ataques de phishing, malware ou conteúdo fraudulento. Pode ser utilizado também para det confidenciais saiam da organização.
Detecção e gerenciamento de vulnerabilidades	Sistemas de análise de vulnerabilidades	Ferramentas ou sistemas automatizados que permitem que as organizações verifiquem se suas redes, seus si falhas de segurança que possam expô-los a ameaças e possíveis ataques cibernéticos.
Segurança de rede	Equipamentos ou sistemas do tipo Firewall	Sistemas ou equipamentos destinados a evitar acesso não autorizado a uma determinada rede, ou a conjunto Podem ser implementados em hardware ou software, ou em ambos. Cada mensagem que entra ou sai da red examina a fim de determinar se atende ou não os critérios de segurança especificados.

Tabela VI

- Análise:

  Esta solução apresenta-se como viável para o órgão e possui algumas vantagens e desvantagens, listadas a seguir:

  Vantagens:

  - Atualização tecnológica completa das soluções de segurança em produção na rede da ACMD;
  - Equipamentos e licenças de propriedade do órgão: não há o risco de descontinuidade dos serviços caso haja interrupção do contrato ou a falência da empresa contratada;
  - Requer uma quantidade reduzida de homem-hora no processo de gestão e fiscalização contratual, gerando economicidade ao órgão.

Desvantagem:

- Desembolso do valor total a ser adquirido no ato da contratação.

Solução 04 – Contratação das soluções na forma de serviço.

- Descrição:

  Existe também a possibilidade da contratação de todas as soluções, na forma de serviço, onde as licenças e os equipamentos são alocados no órgão para utilização local, ou em nuvem, durante o período de vigência contratual.

- Análise:

  Assim como a Solução 03, essa solução também se apresenta como viável para o órgão e possui algumas vantagens e desvantagens, listadas a seguir:

  Vantagens:

  - Atualização tecnológica completa das soluções de segurança em produção na rede da ACMD;
  - Desembolsos mensais durante o período contratual.

  Desvantagens:

  - Solução de alto risco pois os equipamentos e as licenças são de propriedade da empresa o que requer uma estratégia de mitigação de perdas de dados e continuidade dos serviços caso haja interrupção do contrato ou da prestação de serviço.
  - Requer uma grande quantidade de homem-hora no processo de gestão e fiscalização contratual para a realização das análises, dos atestes e dos pagamentos mensais.

4 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS - (IN. 01/2019, art 11, § 1º)

As soluções S-01 e S-02 são consideradas inviáveis, tendo em vista os motivos expostos em suas respectivas análises.

5 – ANÁLISE COMPARATIVA DE CUSTOS (TCO) – (IN. 01/2019, art. inciso III, alínea “a”)

Para as soluções técnica e funcionalmente viáveis, quais sejam as soluções 03 e 04, foram realizados os comparativos dos custos totais de propriedade, a seguir:

5.1 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE - (IN. 01/2019, art. 11, inciso III, letra “b”)

Foram realizadas pesquisas de preços visando a estimativa de custos para a solução 03 (aquisição dos equipamentos e licenças) e para a solução 04 (contratação das soluções na forma de serviço). Para a solução 03, foram encontrados alguns contratos similares com a APF que contemplam as soluções objeto desse ETP, contudo, por conterem quantitativos e prazos distintos, foram considerados os valores unitários e os prazos de 12 meses e 36 meses.

De forma adicional, foram realizadas consultas à empresas do ramo, solicitando estimativa de custos para as soluções demandadas. Todos os valores levantados para a solução 03 foram consolidados nas tabelas VII e VIII, conforme abaixo:

Pesquisa de preços – valores unitários obtidos para a Solução 03 com **validade de 12 meses**					
Solução	ORÇAMENTO 1 (Fasthelp)	ORÇAMENTO 2 (Vtechti)	ORÇAMENTO 3 (Layer)	CONSULTA (PAINEL/BANCO DE PREÇOS)	
Proteção de endpoints	R$ 59,18	R$ 64,50	R$ 72,36	R$ 30,00 (UASG 10001)	R$ 31,50 (UASG 828624)
Prevenção de perda de dados	R$ 38,79	R$ 43,06	R$ 55,42		
Filtragem e proteção de navegação Web	R$ 62,40	R$ 62,90	R$ 71,62		
Detecção e prevenção de intrusão de rede	R$ 786.495,42	R$ 845.968,95	R$ 953.462,36		
Filtragem e proteção de e-mails	R$ 83,20	R$ 92,35	R$ 132,48	R$ 136.04 (UASG 323028)	
Detecção e gerenciamento de vulnerabilidades	R$ 160,68	R$ 192,82	R$ 163,99		
Segurança de rede - firewall (Tipo I)	R$ 228.800,00	R$ 260.956,80	R$ 282.456,89		
Segurança de rede - firewall (Tipo II)	R$ 156.000,00	R$ 186.602,00	R$ 195.362,44	R$ 176.542,00 (UASG 926092)	R$ 378.800,00 (UASG 926137)

Tabela VII

Pesquisa de preços – valores unitários obtidos para a Solução 03 com **validade de 36 meses**						
Solução	ORÇAMENTO 1 (Fasthelp)	ORÇAMENTO 2 (Vtechti)	ORÇAMENTO 3 (Layer)	CONSULTA (PAINEL/BANCO DE PREÇOS		
Proteção de endpoints	R$ 177,53	R$ 195,67	R$ 216,48	R$ 129,50 (UASG 257003)	R$ 160,00 (UASG 936001)	R$
Prevenção de perda de dados	R$ 116,38	R$ 126,85	R$ 143,52	R$ 128,00 (UASG 926137)		
Filtragem e proteção de navegação Web	R$ 124,80	R$ 136,44	R$ 142,99	R$ 234,95 (UASG 892453)		
Detecção e prevenção de intrusão de rede	R$ 1.364.539,07	R$ 1.426.887,07	R$ 1.403.564,48			
Filtragem e proteção de e-mails	R$ 208,00	R$ 249,60	R$ 302,45	R$ 472,63 (UASG 926137)		
Detecção e gerenciamento de vulnerabilidades	R$ 433,84	R$ 529,28	R$ 612,74	R$ 371,63 (UASG 926002)		

Segurança de rede - firewall (Tipo I)	R$ 478.400,00	R$ 520.624,00	R$ 624.152,89	R$ 461.890,00 (UASG 925302)	R$ 474.692,00 (UASG 399003)	R$
Segurança de rede - firewall (Tipo II)	R$ 275.600,00	R$ 301.744,56	R$ 334.625,15	R$ 252.000,00 (UASG 158718)		

Tabela VIII

A estimativa de custo realizada para a solução 03, utilizou como parâmetro o menor dos valores obtidos de cada item. Segue abaixo o resultado final da estimativa realizada tanto para 12 meses, quanto para 36 meses:

Pesquisa de preços – valores obtidos para a Solução 03							
Validade de 12 meses				**Validade de 36 meses**			
SOLUÇÃO	QUANTIDADE	VALOR UNITARIO	VALOR TOTAL	SOLUÇÃO	QUANTIDADE	VALOR UNITARIO	VALOR
Proteção de Endpoints	2350	R$ 30,00	R$ 70.500,00	Proteção de Endpoints	2350	R$ 129,50	R$ 30
Proteção DLP	2350	R$ 38,79	R$ 91.156,50	Proteção DLP	2350	R$ 116,38	R$ 27
Proteção Secure Web Gateway	2350	R$ 62,40	R$ 146.640,00	Proteção Secure Web Gateway	2350	R$ 124,80	R$ 29
Equipamento IDS/IPS	2	R$ 786.495,42	R$ 1.572.990,84	Equipamento IDS/IPS	2	R$ 1.364.539,07	R$ 2.72
Proteção Secure Email Gateway	2350	R$ 83,20	R$ 195.520,00	Proteção Secure Email Gateway	2350	R$ 208,00	R$ 48
Analisador de Vulnerabilidades	2200	R$ 160,68	R$ 353.496,00	Analisador de Vulnerabilidades	2200	R$ 371,63	R$ 81
Equipamento Firewall (Tipo I)	4	R$ 228.800,00	R$ 915.200,00	Equipamento Firewall (Tipo I)	4	R$ 461.890,00	R$ 1.84
Equipamento Firewall (Tipo II)	3	R$ 156.000,00	R$ 468.000,00	Equipamento Firewall (Tipo II)	3	R$ 252.000,00	R$ 75
TOTAL			**R$ 3.813.503,34**				**R$ 7.51**

Tabela IX

Todos os levantamentos foram realizados por meio de consultas ao sistema banco de preços (https://www.bancodeprecos.com.br), ao sistema painel de preços (https://paineldeprecos.planejamento.gov.br) e complementados por meio de cotações junto à empresas especializadas. Os resultados das pesquisas estão disponíveis no documento SEI (5177658).

Com relação à solução 04, não foi possível obter nos sistemas consultados, contratos semelhantes que contemplassem todas as soluções ofertadas na forma de serviços. Portanto, para a estimativa de custos dessa solução, foram realizadas consultas por e-mail com algumas empresas do ramo, onde foi solicitada uma estimativa de preços baseada nas necessidades do MD, conforme documento SEI (5177658). O resultado obtido foi o seguinte:

Pesquisa de preços – valores obtidos para a Solução 04			
Solução	ORÇAMENTO 1 (FastHelp)	ORÇAMENTO 2 (Vtechti)	ORÇAMENTO 3 (Layer)
Serviço de Proteção de endpoints (AntiMalware)	R$ 22,50	R$ 20,59	R$ 28,85
Serviço de Prevenção de perda de dados (DLP)	R$ 33,28	R$ 33,03	R$ 42,16
Serviço de Filtragem e proteção de navegação Web (Proxy)	R$ 23,11	R$ 19,42	R$ 26,59
Serviço de Detecção e prevenção de intrusão de rede (IDS/IPS)	R$ 49.000,00	R$ 26.270,00	R$ 41.542,49
Serviço de Filtragem e proteção de e-mails (AntiSpam)	R$ 17,91	R$ 18,45	R$ 22,47
Serviço de Detecção e gerenciamento de vulnerabilidades	R$ 18,14	R$ 16,16	R$ 5,12
Serviço de Segurança de rede (Firewall Tipo I)	R$ 37.500,00	R$ 39.328,03	R$ 52.496,59
Serviço de Segurança de rede (Firewall Tipo II)	R$ 23.333,33	R$ 30.590,00	R$ 31.265,32

Tabela X

Na estimativa de custo realizada para a solução 04, utilizou-se como parâmetro o menor dos valores unitários mensais obtidos de cada item, conforme tabela abaixo:

Pesquisa de preços – valores obtidos para a Solução 04			
Solução	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL
Serviço de Proteção de endpoints (AntiMalware)	2350	R$ 20,59	R$ 48.386,50
Serviço de Prevenção de perda de dados (DLP)	2350	R$ 33,03	R$ 77.620,50
Serviço de Filtragem e proteção de navegação Web (Proxy)	2350	R$ 19,42	R$ 45.637,00
Serviço de Detecção e prevenção de intrusão de rede (IDS/IPS)	2	R$ 26.270,00	R$ 52.540,00
Serviço de Filtragem e proteção de e-mails (AntiSpam)	2350	R$ 17,91	R$ 42.088,50
Serviço de Detecção e gerenciamento de vulnerabilidades	2200	R$ 5,12	R$ 11.264,00
Serviço de Segurança de rede (Firewall Tipo I)	4	R$ 37.500,00	R$ 150.000,00
Serviço de Segurança de rede (Firewall Tipo II)	3	R$ 23.333,33	R$ 69.999,99
TOTAL MENSAL			**R$ 497.536,49**
TOTAL ANUAL			**R$ 5.970.437,88**

Tabela XI

5.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO) – (IN. 01/2019, art. 11, inciso III, alínea "a")

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
S-03 (12 meses)	R$ 3.813.503,34	R$ 3.813.503,34	R$ 3.813.503,34	**R$ 11.440.510,0**
S-03 (36 meses)	R$ 7.510.122,14	R$ 0	R$ 0	**R$ 7.510.122,14**
S-04	R$ 5.970.437,88	R$ 5.970.437,88	R$ 5.970.437,88	**R$ 17.911.313,64**

Tabela XII

Para a Solução 03, com validade de 12 meses, o custo total de propriedade após 36 meses (3 anos) de contrato é de **R$ 11.440.510,00**.

Para a Solução 03, com validade de 36 meses, o custo total de propriedade após 36 meses (3 anos) é de **R$ 7.510.122,14**.

Para a Solução 04, o custo total de propriedade após 36 meses (3 anos) de contrato é de **R$ 17.911.313,64**.

6 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA – (IN. 01/2019, art. 14)

Aquisição de soluções de segurança de TI, compostas por licenças de uso de softwares/programas de proteção de endpoints (anti-malware), Data Loss Prevention (DLP), Secure Web Gateway (web proxy), Secure Email Gateway (anti-spam), detecção e gerenciamento de vulnerabilidades, equipamentos IDS/IPS e equipamentos Firewall, conforme condições, quantidades e exigências estabelecidas no instrumento convocatório e seus anexos.

6.1 – Parcelamento da Solução de TIC Escolhida (IN. 01/2019, art. 12, §2º, inciso I)

Em que pese as soluções de segurança de TI demandadas serem autônomas, ou seja, uma solução não afeta tecnicamente a outra, as soluções que contém os itens 01, 02, 03 e 04 devem funcionar de forma integrada, conforme as justificativas técnicas fornecidas no Item 1.3, alínea "c" deste ETP. Pelo exposto elas devem ser agrupadas e adquiridas pelo mesmo fornecedor. Além das justificativas fornecidas no Item 1.3, alínea "c", deste ETP, existem outras motivações para o agrupamento, conforme abaixo:

- Funcionamento harmônico, com compatibilidade e garantia de interligação entre todos os equipamentos e os sistemas elencados no grupo;
- Fornecedor único, responsável pela viabilidade da integração e garantia de harmonia e operacionalidade de todo o conjunto de itens adquiridos; e
- Economicidade, pois o MD ganha em capacidade de gestão do contrato, com instrumentos de cobrança efetiva e com procedimentos padronizados de suporte técnico durante o período de licenciamento e garantia, propiciando agilidade na identificação e resolução dos problemas advindos de falhas ou outros eventos que estejam relacionados ao grupo 01, que funcionarão interligados.

Cabe destacar que seria oneroso para a Administração gerenciar vários fornecedores e prestadores de serviço em múltiplos contratos para essas soluções que deverão funcionar de forma coordenada e integrada. Tal situação, certamente, iria gerar casos em que o suporte técnico continuado para a CONTRATANTE seria provido por empresas distintas e traria uma complexidade que fugiria ao objetivo da contratação, podendo inclusive comprometer o funcionamento conjunto das soluções de segurança.

Em função de não haver exigência técnica de integração para as demais soluções, os itens 05, 06, 07 e 08 não foram agrupados.

6.2 – Bens e Serviços que compõem a solução

Após a análise das soluções, recomenda-se como solução que melhor atende aos requisitos apresentados no presente estudo, com economicidade, eficiência e eficácia a **Solução 03**, qual seja, a aquisição de soluções de mercado compostas pelos seguintes itens:

Grupo	Item	Descrição do bem ou serviço	Quantidade
1	1	Licença de uso de software/programa de proteção de endpoints do tipo Anti-Malware com validade de 36 (trinta e seis) meses.	2350 licenças
	2	Licença de uso de software/programa de prevenção de perda de dados do tipo DLP com validade de 36 (trinta e seis) meses.	2350 licenças
	3	Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway com validade de 36 (trinta e seis) meses.	2350 licenças
	4	Equipamento de detecção e prevenção de intrusão de rede do tipo IDS/IPS com licenciamento e garantia de 36 (trinta e seis) meses.	2 equipamentos
	5	Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure Email Gateway com validade de 36 (trinta e seis) meses.	2350 licenças
	6	Licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades com validade de 36 (trinta e seis) meses.	2200 licenças
	7	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo I).	4 equipamentos
	8	Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo II).	3 equipamentos

Tabela XIII

Observação:

a. As soluções do grupo 1 bem como as soluções dos itens 5 e 6 deverão ser adquiridas após a data de validade do TERMO ADITIVO Nº 025-DETIC-CONTRAT/2021 (3923102), qual seja, 21/8/2022.
b. As soluções dos itens 7 e 8 deverão ser adquiridas após a data de validade do TERMO ADITIVO Nº 044-DETIC-CONTRAT/2021 (4218796), qual seja, 08/11/2022.

7 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO - (IN. 01/2019, art. 20)

Com base no Cálculo Total de Propriedade (TCO) e nas pesquisas de mercado realizadas, verificou-se que a solução escolhida apresentou um custo total estimado de **R$ 7.510.122,14** (sete milhões e quinhentos e dez mil cento e vinte e dois reais e quatorze centavos), conforme a Tabela XII do item 5.2.

Segue abaixo a estimativa de custo total da contratação distribuída por área de negócio:

Estimativa do custo total da contratação							
Demanda DETIC				**Demanda ROD**			
SOLUÇÃO	QUANTIDADE	VALOR UNITARIO	VALOR TOTAL	SOLUÇÃO	QUANTIDADE	VALOR UNITARIO	VALOR
Proteção de Endpoints	2100	R$ 129,50	R$ 271.950,00	Proteção de Endpoints	250	R$ 129,50	R$ 32
Proteção DLP	2100	R$ 116,38	R$ 244.398,00	Proteção DLP	250	R$ 116,38	R$ 29
Proteção Secure Web Gateway	2100	R$ 124,80	R$ 262.080,00	Proteção Secure Web Gateway	250	R$ 124,80	R$ 31
Equipamento IDS/IPS	2	R$ 1.364.539,07	R$ 2.729.078,14	Equipamento IDS/IPS	-	-	
Proteção Secure Email Gateway	2100	R$ 208,00	R$ 436.800,00	Proteção Secure Email Gateway	250	R$ 208,00	R$ 52
Analisador de Vulnerabilidades	2200	R$ 371,63	R$ 817.586,00	Analisador de Vulnerabilidades	-	-	
Equipamento Firewall (Tipo I)	4	R$ 461.890,00	R$ 1.847.560,00	Equipamento Firewall (Tipo I)	-	-	
Equipamento Firewall (Tipo II)	-	-	-	Equipamento Firewall (Tipo II)	3	R$ 252.000,00	R$ 75
TOTAL POR ÁREA			**R$ 6.609.452,14**				**R$ 900.**
TOTAL GERAL							**R$ 7.51**

Tabela XIV

8 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO - (IN. 01/2019, art. 11, inciso v)

A Equipe de Planejamento da Contratação declara o presente estudo técnico preliminar viável do ponto de vista técnico, negocial e econômico, desde que sejam adotadas as premissas e conclusões descritas neste documento conforme preconizado na IN nº 01/2019 – Secretaria de Governo Digital/Ministério da Economia.

8.1 – Justificativa Solução Escolhida - (IN. 01/2019, art. 11, inciso v)

A solução escolhida foi a que melhor atende às necessidades de negócio, tecnológicas e os demais requisitos necessários e suficientes à escolha da solução de TIC, previstos no item 01 deste ETP.

Cabe destacar que a solução escolhida foi a que apresentou o menor custo total estimado para o MD, conforme indicado na Tabela XII.

Outro ponto relevante a ser destacado é que as desvantagens relativas à Solução 04, listadas no item 3.2 deste ETP, são muito relevantes e tiveram peso no processo de escolha pela Solução 03 (36 meses).

Conclui-se, portanto, que a opção mais adequada para prover as soluções requeridas, mitigando os riscos operacionais de continuidade dos serviços, de proteção dos dados organizacionais e com economicidade, é a **Solução 03 com validade de 36 meses.**

8.2 – Benefícios a serem alcançados com a aquisição (IN. 01/2019, art. 11, inciso v)

Espera-se alcançar os seguintes benefícios, com a contratação:

Benefícios da contratação.		
ID	**Benefícios**	**Eficácia/ Eficiência/ Efetividade/ Economicidade**
1	Identificar e registrar tráfegos e atividades suspeitas, bem como realizar os devidos bloqueios.	Eficácia
2	Identificar vulnerabilidades em aplicações e ativos das redes de dados da ACMD.	Eficácia
3	Reduzir do número de incidentes relacionados à segurança das redes de dados da ACMD.	Efetividade

Benefícios da contratação.		
ID	**Benefícios**	**Eficácia/ Eficiência/ Efetividade/ Economicidade**
4	Manter níveis aceitáveis de disponibilidade, integridade, confidencialidade e integridade das informações da ACMD.	Eficácia
5	Aprimorar as tecnologias de segurança de TI utilizadas nas redes de dados da ACMD.	Efetividade
6	Garantir a continuidade dos negócios da ACMD por meio de melhorias, apoio técnico e manutenções das soluções a serem adquiridas.	Eficácia
7	Manter as soluções com suporte e garantia dos fabricantes com por no mínimo 36 meses.	Economicidade
8	Manter a integração das infraestruturas, dados e sistemas das redes que compõe a ACMD bem como de suas redes parceiras.	Eficiência/Economicidade

Tabela XV

9 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria DEADI/SEORI/SG-MD N° 2209 de 18 de abril de 2022.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ **EDMAR DA SILVA BRAGA JÚNIOR** **SIAPE/CPF:** ***.963.811-**	_____ **DANIEL DE SOUZA SANTOS** **SIAPE/CPF:** 1803164/***.631.381-**
_____ **CF (T) MARCELLO DA SILVA FIGUEIREDO** **SIAPE/CPF:** ***.226.897-**	_____ **ANTONIO GAETANI DE SOUSA SANTOS** **SIAPE/CPF:** ***.283.901-**

10 – APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC
_____ **JEFERSON DENIS CRUZ DE MEDEIROS** Contra-Almirante Diretor **SIAPE/CPF:** ***.645.537-**

APÊNDICE I

ESPECIFICAÇÕES TÉCNICAS

CARACTERÍSTICAS COMUNS A TODOS OS ITENS

- As soluções do grupo 01, itens 01 (Proteção de endpoints do tipo Anti-Malware), 02 (Prevenção de perda de dados do tipo DLP), 03 (Filtragem e proteção de navegação Web do tipo Secure Web Gateway) e 04 (Detecção e prevenção de intrusão de rede IDS/IPS) devem ser do mesmo fabricante ou desenvolvedor;
- Devem ser entregues e instalados nos endereços fornecidos pelo Ministério da Defesa;
- Deve ser realizado o repasse de conhecimento da operação dos ativos durante a instalação, conforme os requisitos do item 4.2 - Requisitos de Capacitação, do Termo de Referência;
- O repasse de conhecimento deverá contemplar a operação e a administração de todos os itens; e
- Deve ser elaborada e entregue ao Ministério da Defesa toda a documentação da instalação, configuração e migração, com todas as informações relevantes para a administração e gerência dos ativos, bem como a topologia e diagramas da rede, após a implantação de todos os itens;

- Deverá ser entregue comprovação ponto a ponto de atendimento das características técnicas da solução aos requisitos exigidos neste Termo de Referência por meio da transcrição de trecho do documento oficial do fabricante que comprove expressamente o atendimento das funcionalidades, informando:
  - Qual é o documento;
  - Onde encontrar o documento;
  - Qual a página do documento; e
  - Qual o parágrafo do documento.

ITEM 01 - LICENÇA DE USO DE SOFTWARE/PROGRAMA DE PROTEÇÃO DE ENDPOINTS DO TIPO ANTI-MALWARE

1. **Características Gerais da Solução**
   - A solução deve ser integrada e do mesmo fabricante da plataforma de DLP, IDS/IPS e Secure Web Gateway;
   - A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
   - A solução deve permitir a instalação em ambientes tecnológicos distintos, uma vez que será utilizada em redes segregadas e operada de forma independente pelas equipes de TI da CONTRATANTE;
   - Os sistemas utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão; e
   - Deve possuir serviço de Suporte Técnico e garantia de atualização durante o período da assinatura contratada.
2. **A solução deve contemplar as seguintes funcionalidades básicas, descritas a seguir:**
   - Deve possuir suporte às arquiteturas 32-bits e 64-bits.
   - Deve suportar as seguintes plataformas clientes:
     - Windows 10;
     - Windows 8.1;
     - Windows 8;
     - Windows 7;
     - Windows Server 2016;
     - Windows Server 2012;
     - Windows Server 2008 R2;
     - Amazon Linux;
     - Red Hat Enterprise Linux;
     - Suse Linux Enterprise;
     - Oracle Linux;
     - CentOS;
     - Ubuntu;
     - Debian;
     - Fedora.
   - Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:
     - AWS;
     - Azure;
     - Citrix XenApp;
     - Citrix XenDesktop;
     - Citrix XenServer;
     - Microsoft Hyper-V 2012 R2;
     - Vmware ESXi;
     - Vmware Player;
     - Vmware vShpere;
     - Vmware Workstation.
   - A proteção deverá ser realizada por softwares específicos que atendam a funcionalidades descritas neste Termo de Referência e deverá conter um agente de gerenciamento independente dos softwares de proteção, permitindo que componentes sejam adicionados ou removidos conforme às necessidades dos administradores;
   - O conjunto de softwares de proteção e agente de gerenciamento deverão ser fornecidos pelo mesmo fabricante;
   - O software de proteção deve compreender as seguintes funcionalidades:
     - Prevenção de ameaças;
     - Firewall e prevenção contra intrusão;
     - Controle Web;
     - Prevenção adaptável contra ameaças;
   - Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
     - Relatórios;
     - Dashboards;
     - Políticas;
     - Configuração;
     - Instalação/Desinstalação;
   - O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente;
   - O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante;
   - A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise contextual, não baseada somente em assinaturas de detecção;
   - A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;
   - A solução deverá realizar verificações periódicas no ambiente para alertar o fabricante de potenciais problemas ocasionados pela atualização de vacina;
   - A solução deve conter módulo capaz de proteger contra redes de BOT, negação de serviço, executáveis não confiáveis e conexões web maliciosas;

- A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar); e
- A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre soluções de fabricantes terceiros (Exemplo: Checkpoint, Fortinet, Avecto, TrapX, Fireeye, NMAP, Cisco, IBM), compartilhando as informações para melhor mitigar novas ameaças. Este módulo deve estar público para o desenvolvimento da comunidade via Github.

3. **Proteção de Ameaças para Windows**

- **Prevenção de exploração:**

  - Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo);
  - Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos;
  - Deve ser possível ativar/desativar a prevenção de execução de dados do Windows;
  - Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
  - Deve conter assinatura de ataques com conteúdo atualizável periodicamente;
  - Deve permitir aos administradores a criação de assinaturas personalizadas para controle de pastas, registro, processos, serviços;
  - Deve permitir o bloqueio de ameaças através de ataques de rede;
  - Deve permitir o monitoramento de ataques de Buffer Overflow em processos e aplicações específicas;
  - Deve ser possível incluir exclusões por: Processo, Nome, Caminho do Arquivo, Hash MD5. E Em Módulo chamador: Nome, Caminho, Hash MD5, Signatário Digital e Proteção de acesso.

- **Proteção de acesso:**

  Deve fornecer regras de proteção nativamente, ou seja, definidas pelo fabricante da solução, no mínimo, para:

  - Acesso remoto a pastas locais;
  - Alteração políticas de direitos dos usuários;
  - Alterar os registros de extensão dos arquivos;
  - Criação de novos arquivos na pasta Arquivo de Programas;
  - Criação de novos executáveis na pasta Windows;
  - Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;
  - Criar ou Modificar remotamente arquivos ou pastas;
  - Desativar o editor de registro e o gerenciador de tarefas;
  - Executar arquivos das pastas do usuário;
  - Execução de scripts pelo host de script do Windows;
  - Instalar objetos de ajuda a navegação ou extensões de shell;
  - Instalar novos CLSIDs, APPIDs e TYPELIBs;
  - Modificar configurações de rede;
  - Modificar configurações do Internet Explorer;
  - Modificar processos principais do Windows;
  - Navegadores iniciando programas da pasta de downloads;
  - Registrar programas para execução automática;

  As regras especificadas devem permitir o seu:

  - Bloqueio, ou
  - Informação, ou
  - Bloqueio e Informação;

  Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:

  - Processos;
    - Nome do processo;
    - Hash MD5;
    - Assinatura Digital;
    - Usuário.
  - Arquivos, com as seguintes ações:
    - Criação;
    - Deletar;
    - Executar;
    - Alteração de permissão;
    - Leitura;
    - Renomear;
    - Escrever.
  - Chave de Registro, com as seguintes ações:
    - Escrever;
    - Criar;
    - Deletar;
    - Ler;
    - Enumerar;
    - Carregar;
    - Substituir;
    - Restaurar;
    - Alterar permissão.
  - Valor de Registro, com as seguintes ações:
    - Ler;
    - Criar;
    - Deletar.
  - Processos, com as seguintes ações:
    - Qualquer acesso;
    - Criar thread;
    - Modificar;
    - Terminar;
    - Executar.
  - Serviços, com as seguintes ações:
    - Iniciar;
    - Interromper;

        - Pausar;
        - Continuar;
        - Criar;
        - Remover;
    - Habilitar perfil de hardware;
    - Desabilitar perfil de hardware;
    - Alterar modo de inicialização;
    - Alterar informação de logon;
    - Deve permitir a criação de exclusões.

- **Varredura ao acessar:**

    - A Varredura deve ser passível de habilitação/desativação por opção do administrador;
    - Deve iniciar a proteção durante a inicialização do sistema operacional;
    - Deve ser capaz de realizar análise no setor de boot;
    - O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
    - Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;
    - Deve possibilitar ao administrador a análise de instaladores confiáveis;
    - Deve realizar análise durante cópia entre pastas locais;
    - A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
    - Deve permitir a configuração do nível de agressividade da análise entre:
        - Muito Baixo;
        - Baixo;
        - Médio;
        - Alto;
        - Muito alto.
    - Deve conter integração com a funcionalidade AMSI (Antimalware Scan Interface) da Microsoft;
    - Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
    - Deve realizar varredura quando o processo:
        - Ler o disco;
        - Gravar no disco;
        - Deixar a solução de proteção decidir;
    - Deve possibilitar análise em:
        - Unidades de Rede;
        - Arquivos abertos para backup;
        - Arquivos compactados, por exemplo .jar;
        - Arquivos codificados (MIME).
    - Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
    - Deve permitir a criação de perfis de varredura baseado em uma lista de processos;
    - Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
        - Limpar o arquivo;
        - Excluir o arquivo;
        - Negar acesso ao arquivo;
    - Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
        - Limpar o arquivo;
        - Excluir o arquivo;
        - Permitir acesso ao arquivo;
        - Negar acesso ao arquivo.
    - Deve possibilitar ao administrador a gestão de uma lista de exclusões;
    - Deve possuir módulo capaz de interceptar scripts destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;
    - Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;
    - Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

- **Varredura sob demanda:**

    - Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.
    - Deve permitir a criação de repetição da tarefa.
    - Deve permitir definir a hora da execução da tarefa de análise;
    - Deve permitir a criação da tarefa de varredura de com agendamento aleatório;
    - Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional;
    - Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
        - Memória para rootkits;
        - Processos em execução;
        - Arquivos registrados;
        - Meu computador;
        - Todas as unidades locais;
        - Todas as unidades fixas;
        - Todas as unidades removíveis;
        - Todas as unidades mapeadas;
        - Pasta inicial;
        - Pasta de perfil do usuário;
        - Pasta Windows;
        - Pasta de arquivos de programas;
        - Pasta temporária;
        - Lixeira;
        - Arquivo ou pasta especificada pelo administrador;
        - Setor de inicialização (boot);
        - Arquivos compactados;
        - Arquivos MIME.
    - Deve possuir opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
    - Deve possuir áreas de exclusão que não deverão ser varridas;
    - Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada para a detecção de ameaças desconhecidas;
    - Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
        - Limpar o arquivo;
        - Excluir o arquivo;
        - Negar acesso ao arquivo.

- Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
  - Limpar o arquivo;
  - Excluir o arquivo;
  - Permitir acesso ao arquivo;
  - Negar acesso ao arquivo.
- Para minimizar o impacto ao usuário, a solução deve permitir:
  - Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
  - Iniciar a varredura apenas quando o sistema estiver ocioso;
  - Permitir ao usuário retomar varreduras pausadas;
  - Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede.

4. **Proteção de Ameaças para Linux**

- Deve permitir a atualização automática das vacinas de detecção;
- Deve detectar ameaças usando métodos de acesso e de varredura sob demanda;
- Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas;
- Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações:
  - Limpar o arquivo;
  - Deletar o arquivo;
  - Negar acesso ao arquivo.
- Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos;
- Deve permitir a opção de manter a configuração de exclusão realizada no agente, não sendo sobrescrita pela política principal;
- Deve permitir a gestão do agente local por meio de linha de comando;
- Ao configurar a análise ao acessar, deve permitir:
  - Quando analisar (exemplo: ao ler o arquivo);
  - O que analisar (exemplo: todos os arquivos);
  - Analise de arquivos compressos;
  - Analise de volumes de rede;
  - Analise de programas não desejados.
- Ao configurar a analise sob demanda, deve permitir:
  - Analise de arquivos compressos;
  - Analise de PUP;
  - Analise de macros desconhecidos;
  - Analise de programas desconhecidos;
  - Caminhos da análise (path);
  - Analise de pastas e subpastas;
  - Analise de macros;
  - Exclusão de paths, pastas e tipos de arquivos;
  - Uso de cache;
  - Ação Primária e Secundária.
- Deve possuir quarentena local para armazenar ameaças desconhecidas;
- Deve possuir ação para mover artefatos maliciosos para a área de quarentena;
- Deve usar heurística para detectar arquivos potencialmente maliciosos;
- Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo;

5. **Proteção de Rede**

O módulo de Firewall de Host deve incluir as seguintes capacidades:

- Deve permitir a ativação/desativação do módulo de Firewall através da console;
- Deve ser capaz de prevenir intrusões e proteger os nós gerenciados garantindo cobertura contra ataques dia zero;
- Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;
- Deve possuir assinaturas de proteção para:
  - Arquivos;
  - Chave de Registro;
  - Processos;
  - Serviços.
- Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;
- Deve ser possível bloquear trafego bridge;
- Deve ser possível bloquear contra falsificação de IP (IP Spoofing);
- O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
- Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;
- Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:
  - Nome;
  - Nome do arquivo ou Caminho;
  - Hash MD5;
  - Assinador digital.
- Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;
- As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.
- Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;

- Deve permitir inspeção do protocolo FTP;
- Deve ser possível bloquear trafego de protocolos não suportados;
- O módulo de Firewall deve vir com um conjunto de regras previamente criadas pelo próprio fabricante.
- O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
    - Ação
        - Bloquear;
        - Permitir.
    - Direção
        - Ambas;
        - Entrada;
        - Saída.
    - Protocolo
        - Qualquer protocolo;
        - Protocolo IP;
        - Ipv4;
        - Ipv6;
        - Protocolo Não-IP.
    - Tipo de Conexão
        - Rede Sem Fio;
        - Rede cabeada;
        - Rede Virtual.
    - Especificação da Rede
        - Endereço IP;
        - Subnet;
        - Range;
        - FQDN.
    - Protocolo de Transporte
        - Todos;
        - ICMP;
        - ICMPv6;
        - TCP;
        - UDP;
        - STP;
        - GRE;
        - IGMP;
        - IPSEC AH;
        - IPSEC ESP;
        - Ipv6 in Ipv4;
        - ISIS over Ipv4;
        - L2TP.
    - Agendamento
        - Dias da Semana;
        - Hora Inicio;
        - Hora Fim;
        - Aplicações.
- Deve possuir as seguintes proteções:
    - Generic Buffer Overflow Protection;
    - Suspicious caller and caller validation;
    - Exploit Prevention;
    - Data Execution Protection;
    - Generic Privilege Escalation Protection.
- Deve possuir modulo de proteção contra intrusão por meio da rede;
- O módulo de proteção contra intrusos deve possuir regras já pré-definidas pelo fabricante;
- Deve permitir a criação customizada de regras de proteção, para no mínimo:
    - Buffer Overflow;
    - Uso Ilegal de API;
    - Arquivos;
    - Serviços;
    - Registro
    - Processos;
- Ao bloquear um determinado atacante pelo módulo de proteção de rede, deve ser possível indicar um tempo mínimo no qual a máquina atacante não poderá se comunicar com a atacada;
- Deve permitir a indicação de assinaturas e endereços IP que não deverão ser levadas em consideração pelo mecanismo de análise;
- Deverá possuir, no mínimo, as seguintes assinaturas:
    - Proteção contra intrusão
        - TCP Port Scan;
        - UDP Port Scan;
        - Proteção contra vulnerabilidades SMB;
        - Proteção contra brute force;
    - Serviços
        - IIS Envelope;
        - IIS Shielding;
        - MSSQL;

        - Event Log;
        - Remote Access;
        - Netmon;
        - Remote Command;
        - RunAs;
    - Registro:
        - Drive usb inserido;
    - Processos:
        - Double File Extension;
    - Buffer Overflow:
        - Exchange;
        - IIS;
        - Services.exe;
        - SVCHOST.exe
        - Generic Buffer Overflow;
        - Generic Privilege Escalation;
        - Windows Explorer;
        - WinHLP32.
    - Uso Ilegal de API
        - Mimikatz;
        - MS Agent;
        - Microsoft XML Core;
        - Microsoft WMITools;
        - MSDTC RPC Vulnerability;
        - PowerShell Command Restriction;
        - Print Spooler Load Library Vulnerability;
        - Fileless Threat;
        - Firefox Ilegal URL Quotes;
        - Google Desktop Javascript Injection;
        - Hidden Powershell.
- Deve fornecer proteção para aplicações, constando na lista fornecida pelo fabricante, no mínimo:
    - Adobe Acrobat;
    - Adobe Flash Player;
    - Adobe Flash Player Plugin
    - Apple iTunes;
    - Apple Safari;
    - CoolPDFReader;
    - Cscript;
    - Firefox;
    - Google Chrome;
    - Foxit Reader;
    - Java Platform;
    - Microsoft Edge;
    - Microsoft Internet Explorer;
    - Microsoft Outlook;
    - Microsoft Visual C++;
    - Microsoft Windows Explorer;
    - Microsoft Windows Powershell;
    - Microsoft Windows Win32 Runtime;
    - Mozilla;
    - OpenOffice;
    - Registry Editor;
    - VLC Media Player.

6. **Proteção Web**

O modulo de Controle Web deve possuir as seguintes funcionalidades:

- Deve permitir o bloqueio de browsers não suportados, dentre eles:
    - Opera;
    - Safari for Windows;
    - Netscape;
    - Maxthon;
    - Flock;
    - Avant Browser;
    - Deepnet Explorer;
    - PhaseOut.
- Deve permitir o controle de browsers suportados, dentre eles:
    - Chrome;
    - Firefox;
    - Internet Explorer.
- Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.
- Deve possuir, no mínimo, as seguintes categorias:
    - Browser Exploits;
    - Download Maliciosos;
    - Sites Maliciosos;
    - Phishing;
    - Pornografia;
    - Hacking/Computer Crime;
    - Spyware/Adware/Keyloggers;

- Anonymizer;
- Anonymizer Utilities;
- Alcohol;
- Blogs/Wiki;
- Business;
- Chat;
- Content Server;
- Dating;
- Dating/Social Networking;
- Digital Postcards;
- Discrimination;
- Drugs;
- Education;
- Entertainment;
- Extreme;
- Fashion;
- Finance;
- For Kids;
- Forum;
- Gambling;
- Game/Cartoon Violence;
- Games;
- General News;
- Government/Military;
- Gruesome Content;
- Health;
- Historical Revisionism;
- History;
- Humor/Comics;
- Illegal UK;
- Incidental Nudity;
- Information Security;
- Instant Messaging;
- Interactive Web Applications;
- Internet Radio/TV;
- Internet Services;
- Job Search;
- Major Global Religions;
- Marketing/Merchandising;
- Media Downloads;
- Media Sharing;
- Messaging;
- Mobile Phone;
- Moderated;
- Motor Vehicles;
- Non-Profit/Advocacy/NGO;
- Nudity;
- Online Shopping;
- P2P/File Sharing;
- Parked Domain;
- Personal Network Storage;
- Personal Pages;
- Pharmacy;
- Politics/Opinion;
- Portal Sites;
- Potential Criminal Activities;
- Potential Illegal Software;
- Potentially Unwanted Programs;
- Profanity;
- Professional Networking;
- Provocative Attire;
- Public Information;
- Real Estate;
- Recreation/Hobbies;
- Religion/Ideology;
- Remote Access;
- Residential IP Addresses;
- Resource Sharing;
- Restaurants;
- School Cheating Information;
- Search Engines;
- Sexual Materials;
- Shareware/Freeware;
- Social Networking;
- Software/Hardware;
- Spam URLs;
- Sports;
- Stock Trading;
- Streaming Media;
- Technical Information;
- Technical/Business Forums;
- Text Translators;
- Text/Spoken Only;
- Tobacco;
- Travel;
- Uncategorized;
- Usenet News;

  - Violence;
  - Visual Search Engine;
  - Weapons;
  - Web Ads;
  - Web Mail;
  - Web Meetings;
  - Web Phone.
- Deve ser possível bloquear um site conforme a sua classificação:
  - Vermelho: Alto Risco.
  - Amarelo: Médio Risco.
  - Cinza: Não categorizado.
- Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
- Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;
- Deve permitir a varredura de arquivos baixados da internet;
- Deve ser possível excluir endereços IP da análise;
- Deve permitir a busca segura para buscadores, dentre eles:
  - Google;
  - Yahoo
  - Bing;
  - Ask;
- Deve bloquear links que direcionem para sites com alto risco.
- Deve permitir a customização das mensagens apresentadas para o usuário;

7. **Proteção de Aplicações**

- O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas;
- Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes;
- Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;
- Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante que deverá informar um nível de confidência (Bom, Mau ou Não Classificado);
- Deve ser possível criar uma imagem base para a criação de uma política geral;
- Capacidade de trabalhar no modo adaptativo, ou seja, criando regras automaticamente assim que novas aplicações instaladas ou executadas na máquina;
- A solução deverá permitir a realização de varreduras sob demanda em máquinas para executar a blindagem de aplicativos;
- Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:
  - Desabilitado: proteção desativada;
  - Monitoramento: Monitora toda a atividade da Estação de Trabalho;
  - Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;
- Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1);
- A solução deve suportar as seguintes modalidades de proteção:
  - Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impedidas de serem executadas.
  - Application Blocking / Blacklisting: criação de uma lista de aplicações não autorizadas que não podem ser executadas.
  - Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.
- Deve suportar a criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.
- Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação.
- Seve suportar os mecanismos de proteção:
  - Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc.) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.
  - Memory Protection: permite proteção contra ataques e exploração de vulnerabilidades para os programas em Whitelist.
- Deve suportar a criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:
  - Binário: binário específico identificado através de seu nome ou de algoritmo de verificação SHA-1.
  - Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).
  - Trusted Installer: software instalado por um programa instalador específico, identificações por seu algoritmo de verificação, independentemente de sua origem.
  - Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.
  - Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.
  - Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.
  - Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.
- Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%);
- Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES%);
- Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;
- Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:
  - Critical Address Space Protection;
  - NX - No eXecute (mp-nx);
  - Virtual Address Space Randomization;
  - Mp-vasr-rebase;

  - Mp-vasr-randomization;
  - Mp-vasr-relocation;
  - Mp-vasr-reloc;
  - Forced DLL Relocation.
- Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho;
- Permitir o bloqueio de aplicações e os processos que a aplicação interage;
- Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;
- Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos podem ser executados;

8. **Módulo de Gerência**

- A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;
- Não serão aceitas soluções que possuam mais de uma console de gestão;
- Deve suportar a instalação nos seguintes sistemas operacionais:
  - Microsoft Windows Server 2012;
  - Microsoft Windows Server 2016;
  - Microsoft Windows Server 2019.
- Deve suportar Ipv4 e Ipv6;
- Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
  - Vmware ESX;
  - Citrix Xen Server;
  - Microsoft Hyper-V;
  - Nutanix.
- Deve possuir suporte a base de dados:
  - SQL Server 2012 ou superior.
- Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;
- A console deve ser acessível por meio dos principais browsers disponíveis no mercado (Exemplo: Google Chrome, Mozilla Firefox) por meio de conexão segura (Https);
- Deve ser possível segregar a instalação da solução em:
  - Servidor Console Central;
  - Servidor Base de Dados;
  - Servidor de Interação com os Agentes;
  - Agentes Distribuidores de Vacina.

9. **Capacidades da Gerência**

- Deve possuir um menu que possibilite ao administrador visualizar as funcionalidades de:
  - Gerência de Relatórios;
  - Gerência de Sistemas;
  - Gerência de Políticas e configurações dos produtos listados neste termo de referência;
  - Gerência de Softwares;
  - Gerência de Automação;
  - Gerência de Usuários;
  - Gerência de Configuração;
- Deve apresentar aos administradores as páginas de Menu acessadas mais recentes;
- Deve possibilitar ao administrador a visibilidade do ambiente por meio de Dashboards existentes na solução;
- Deve permitir ao administrador a criação, edição, importação e exportação de dashboards.
- Ao criar um dashboard, o administrador deve escolher entre mantê-lo Privado, Público ou Compartilhado;
- Deve permitir a criação de novos dashboards utilizando:
  - Informação de Gerência de Sistemas;
  - Informação de Eventos;
  - Informação de Gestão de Políticas;
  - Informação de Sistemas Detectados;
  - Informação do módulo Endpoint Security;
  - Informação de estatística do agente;
  - Informação de log.
- Durante a criação de um novo dashboard, a ferramenta deverá permitir a escolha de:
  - Tipo de Informação;
  - Tipo de Gráfico;
  - Tipo de dados que serão apresentados;
  - Tipo de Filtros.
- A solução deve apresentar a query SQL realizada para a apresentação de um dashboard;
- Deve permitir a exportação dos dados apresentados em um dashboard contendo apenas um sumário executivo ou o sumário mais a coleta completa;
- Deve permitir exportar o dashboard nos formatos CSV, XML, HTML e PDF;
- Deve permitir ao administrador a criação de relatórios, por meio de uma ferramenta integrada a console de administração, permitindo a customização do formato do relatório;
- Deve possibilitar ao administrador o uso de queries já criadas para a construção de relatórios;

- Deve possuir painel gráfico específico para o monitoramento dos eventos de:
  - Regras de Firewall;
  - Log de evento de ameaças;
  - Eventos de prevenção de exploração;
  - Evento da solução de aprendizado de máquina;
- Deve permitir a instalação dos Módulos da Solução a partir de um único servidor;
- A solução deverá permitir a instalação do agente de maneira facilitada, dentre elas:
  - Criação de uma URL com o instalador;
  - Criação de um pacote de instalação;
  - Integração por meio do Active Directory;
  - Resposta automática ao detectar uma nova máquina sem agente da solução;
- Ao instalar o novo agente, o mesmo deve ser redirecionado, de maneira automática, ao grupo pertencente.
- A criação de grupos deve ser customizada ou por meio de integração com serviços de diretório (Exemplo: Active Directory);
- A ordenação de cliente deve obedecer a regras pré-estabelecidas pelo administrador da solução, sendo no mínimo:
  - Endereço IP;
  - Marcação;
- A ordenação por meio do uso do Endereçamento IP, deve permitir o uso de um único endereço, um range IPV4/IPV6 e subnet;
- A ordenação por meio do uso de Marcadores, deve ser possível por meio da seleção de propriedades, dentre elas:
  - Tipo de CPU;
  - Nome DNS;
  - Memória Livre;
  - Se é um Laptop;
  - Endereço MAC;
  - Descrição do Sistema;
  - Plataforma do Sistema Operacional;
  - Tipo do Sistema Operacional;
  - Versão do Sistema Operacional;
- Para cada grupo, deve ser possível indicar a herança de política da raiz ou quebrar a herança e definir novos parâmetros;
- Deve permitir a visualização de tarefas especificadas para cada grupo;
- Deve permitir a visualização das políticas aplicadas para cada grupo;
- Para permitir a descoberta de máquinas sem agente, a solução deverá trabalhar com agentes sensores que identificam máquinas sem agente;
- Ao identificar uma máquina sem agente, a solução deve permitir a criação de resposta automatizada, permitindo que a instalação seja feita de maneira silenciosa para o usuário e não assistida pelo administrador da solução;
- Deve permitir a adição manual de sistemas não gerenciados, permitindo a posterior instalação do agente;
- Permitir a alteração das políticas do Módulos da Solução nos clientes de maneira remota;
- Deve permitir a alteração das políticas em um único agente;
- Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança;
- Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;
- Deve possibilitar a configuração de melhor seleção do repositório por meio de:
  - Menor tempo de ping;
  - Distância de subnet;
- Deve permitir a criação de uma lista de repositórios que os clientes deverão buscar por ordem de prioridade;
- Deve permitir a criação de um grupo de teste para a aplicação da vacina antes de espalhar para os demais agentes do ambiente, este processo deve ser automático;
- A solução deve permitir o uso de repositórios distribuídos para a distribuição de softwares, vacinas e atualizações e patches;
- Os repositórios distribuídos devem estar sincronizados com o repositório central;
- Em caso de indisponibilidade do repositório central, deve ser possível a configuração de um repositório backup no qual os repositórios irão em busca de atualizações;
- A adição de um novo repositório deve obedecer aos seguintes parâmetros:
  - Tipo;
  - HTTP;
  - FTP;
  - UNC;
  - Servidor Remoto;
  - Credenciais;
  - Atualizações;
- Deve permitir a criação de agentes locais com privilégios de distribuição de atualizações;
- Deve possuir funcionalidade “lazy caching”, ou seja, fazer o download do repositório principal, apenas quando solicitado por algum outro agente;
- A solução deverá permitir a instalação de agentes de replicação adicionais, responsáveis pela comunicação entre agente servidor, possibilitando a entrega de políticas e atualizações da solução;
- Deve permitir a instalação de agentes de replicação na DMZ;
- Deve possibilitar ao administrador a visualização das características básicas de hardware das máquinas, dentre elas:
  - Informações de CPU;
  - Informações de Memória;
  - Informação de Disco;
  - Nome DNS;
  - Nome do Domínio;
  - Endereço IP;
  - Informações do Sistema Operacional;
  - Time Zone;

- Usuário Logado;
- Se é VDI;

- Deve permitir a criação de propriedades customizadas, a exemplo informar o modelo da placa de vídeo em uma propriedade customizada;
- Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
- Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;
- Deve permitir a criação de políticas customizadas;
- Deve apresentar ao administrador um histórico de alteração de política para cada um dos módulos da solução, incluindo:
  - Data;
  - Usuário;
  - Comentário;
  - Versão do produto;
- Deve criar regras de aplicação de política automatizada com base na estação de trabalho ou no usuário;
- Para a política baseada em usuários, deve ser possível criar, no mínimo, políticas diferenciadas para os módulos de Firewall de host e Filtro Web;
- Deve permitir a criação de resposta automatizada ao detectar evento de ameaça, ou de cliente ou de servidor;
- Dentre as ações de resposta automatizada, deve ser possível:
  - Encaminhar uma Trap SNMP com o nome da ameaça, Severidade e a ação tomada;
  - Executar um comando do sistema;
  - Encaminhar um e-mail;
  - Uma tarefa do servidor;
  - Executar um comando externo;
- Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
- Forçar a configuração determinada no servidor para os clientes;
- Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente;
- A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura;
- Geração de relatórios que contenham as seguintes informações:
  - Máquinas com a lista de definições de vírus desatualizada;
  - Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
  - Os vírus que mais foram detectados;
  - As máquinas que mais sofreram infecções em um determinado período;
  - Os usuários que mais sofreram infecções em um determinado período;
- Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);
- Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;
- Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
  - Cobertura da proteção de Navegação Segura;
  - Relatório dos últimos 30 dias da detecção de códigos maliciosos;
  - Top 10 Computadores com Infecções;
  - Top 10 Computadores com Sites bloqueados pela política;
  - Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
  - Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;
- Deve gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota;
- Deve suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
- Deve ter a capacidade de gerar registros/logs para auditoria;
- A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

10. **Proteção Adaptativa de Ameaças (ATP + EDR)**

- O módulo de inteligência contra ameaças deve conter o mecanismo de confinamento dinâmico de aplicações.
- A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com característica maliciosa (Exemplo: Ransomware);
- A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
- Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;
- Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;
- Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas;
- Deve ser possível a classificação de cada aplicativo de maneira manual e até mesmo sua reclassificação através da console de administração central;
- Dentre os comportamentos maliciosos, deve ser capaz de:
  - Bloquear acesso local a partir de cookies;
  - Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;
  - Criação de arquivos em qualquer local de rede;
  - Criação de novos CLSIDs, APPIDs e TYPELIBs;
  - Criação de threads em outro processo;
  - Bloquear a desativação de executáveis críticos do sistema operacional;
  - Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;
  - Gravação e Leitura na memória de outro processo;
  - Bloqueio de Modificação da política de firewall do windows;
  - Bloqueio de Modificação da pasta de tarefas do Windows;
  - Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;
  - Bloqueio de Modificação de arquivos executáveis portáteis;
  - Bloqueio de Modificação de bit de atributo oculto;
  - Bloqueio de Modificação de bit de atributo somente leitura;
  - Bloqueio de Modificação de entradas de registro de DLL AppInit;
  - Bloqueio de Modificação de locais do registro de inicialização;
  - Bloqueio de Modificação de pastas de dados de usuários;

- Bloqueio de Modificação do local do Registro de Serviços;
- Bloqueio de Suspensão de um processo;
- Bloqueio de Término de outro processo;

- Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra;
- Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada;
- O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca visto pela solução;
- Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;
- A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

Módulo de Análise Avançada

- Deve permitir que o mecanismo trabalhe apenas em modo de observação;
- Deve permitir a análise de processos iniciados em drives mapeados de rede;
- Deve ser capaz de trabalhar com técnicas de análise matemática para identificação de ameaças sem a necessidade de assinaturas;
- Deve permitir a operação:
  - Apenas no cliente;
  - No cliente e integrada com a Nuvem do fabricante;
- Ao selecionar a análise apenas no cliente, deve ser possível indicar a sensibilidade do motor de análise;
- Deve permitir a seleção do melhor modo de operação da solução, variando entre:
  - Modo Balanceado;
  - Modo Produtividade;
  - Modo Segurança;
- Deve ativar o módulo de confinamento dinâmico, de maneira automática, caso uma ameaça atinja um determinado nível de criticidade a ser indicado pelo administrador da solução;

Reputação local de ameaças

- O módulo de reputação local deve manter uma base de dados com todos os executáveis detectados no ambiente.
- Para cada executável, deverão ser apresentadas as reputações:
  - Local;
  - Centro de Inteligência do Fabricante;
  - Analisador Dia Zero;
  - Filtro de Conteúdo Web.
- Deve permitir uma visualização analítica sobre cada arquivo detectado no ambiente, com no mínimo as seguintes informações:
  - Data do último acesso;
  - Tamanho do arquivo;
  - Se está listado no Adicionar/Remover programas do Windows;
  - Data de compilação;
  - Registrado como serviço;
  - Registrado para executar automaticamente;
  - Mais de 6 meses de idade;
  - Idade foi falsificada;
  - Executado a partir do cmd.exe.
- Deve ser capaz de informar a URL de origem do arquivo e sua reputação;
- Deve permitir integração com base global de vírus – VirusTotal – para comparação e se o arquivo sob análise já foi detectado por outro fabricante de segurança, permitindo que esta informação seja utilizada para a indicação de que o artefato é malicioso ou não;
- Deve permitir o rastreamento da execução do arquivo malicioso pelo ambiente informando qual foi a sua primeira execução e sua última;
- Deve permitir a identificação da estação de trabalho e do usuário associado a mesma;
- O módulo deve permitir automatização de contramedidas a partir de soluções do mesmo fabricante e de fabricantes terceiros;

Módulo de Resposta

- Deve ser capaz de implementar visibilidade dos dados gerados pelo Endpoint, como por exemplo:
  - Processos;
  - Fluxos de comunicação de rede;
  - Arquivos;
  - Perfil de Usuários;
  - Registro do Windows;
  - Atualizações Instalados;
  - Grupos Locais;
  - Informação do Host.
- Deve ser capaz de permitir a criação de coletores customizados para a coleta das informações desejadas;
- Deve permitir a configuração de gatilhos que resultarão em uma reação ou contramedida frente ao dado coletado;
- Deve ser capaz de implementar ações nos sistemas classificados como comprometidos;
- Deve permitir a execução de scripts nas linguagens:
  - Comandos do Sistema Operacional;
  - PowerShell;
  - Bash;
  - Python;
  - Visual Basic.
- Deve vir com políticas de monitoramento previamente configuradas pelo fabricante da solução;
- Deve ser capaz de executar busca por padrões nas estações clientes em tempo real;

- O campo de busca deve ser intuitivo e sugerir campos de informação durante a inserção de informações (auto completar);
- Deve ser capaz de salvar buscas realizadas previamente;
- Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca:
  - Endereço IP Local;
  - Hash do processo em execução;
  - ID do processo;
  - Status da transação TCP;
  - Número da porta que originou o pacote de rede;
  - Nome do arquivo;
  - Última data de gravação do arquivo;
  - Data de Criação do arquivo;
  - Data de deleção do arquivo;
  - Versão do Sistema Operacional;
  - Nome do Grupo de usuários;
  - Se o grupo é local;
  - SID do grupo;
  - MAC de origem;
  - MAC de destino;
  - FLAGS TCP (ACK, SYN, RST e FIN);
  - Número de transação TCP;
  - Kernel Time;
  - User Time;
  - Comando que iniciou o processo;
  - Quantidade de RAM utilizada pelo processo;
  - Quantidade de Threads criadas pelo processo;
  - MD5 do processo;
  - SHA-1 do processo;
  - Valor da chave de registro;
  - Caminho da chave de registro.
- A resposta a uma determinada condição deverá ser executada como um serviço não interativo;

11. **Proteção para Dispositivos Móveis**

- A solução detectar ameaças e vulnerabilidades em dispositivos Apple iOS e Google Android;
- Deve ser compatível com sistemas operacionais Android 5 ou superior e iOS 8 ou superior;
- As capacidades de proteção devem funcionar mesmo se o dispositivo não estiver on-line;
- Deve identificar ameaças e ataques atuais ou iminentes, mesmo que nunca tenham sido vistos antes, através de capacidade de autoaprendizagem.
- Sua proteção em tempo real deve detectar phishings por meio de links perigosos encontrados em mensagens de texto, aplicativos de mídias sociais e e-mails.

ITEM 02 - LICENÇA DE USO DE SOFTWARE/PROGRAMA DE PREVENÇÃO DE PERDA DE DADOS DO TIPO DLP

1. **Características Gerais da Solução**

- A solução deve ser integrada e do mesmo fabricante da plataforma de Proteção de Endpoints, IDS/IPS e Secure Web Gateway.
- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- A solução deve permitir a instalação em ambientes tecnológicos distintos, uma vez que será utilizada em redes segregadas e operada de forma independente pelas equipes de TI da CONTRATANTE;
- O sistema utilizado deve possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão; e
- Deve possuir serviço de Suporte Técnico e garantia de atualização durante o período da assinatura contratada.

2. **A solução deve contemplar as seguintes funcionalidades básicas, descritas a seguir:**

- Devem ser fornecidas licenças de uso da solução de Data Loss Prevention (DLP) para prover a descoberta, monitoração e proteção de dados confidenciais, onde quer que sejam armazenados ou usados.
- O CONTRATADO deve entregar todas as licenças de software necessárias, atendendo durante toda a vigência do contrato as especificações recomendadas pelo fabricante, considerando o cenário de utilização de todo o volume de licenças previsto no edital;
- Todos os componentes de software requeridos para atender às funcionalidades exigidas no Edital devem ser fornecidos, inclusive licenças de Bancos de Dados, caso sejam necessárias;
- Deve permitir a instalação de agente de backup e exportação das configurações vigentes para total recuperação em caso de desastre;
- A solução deve oferecer cobertura abrangente de dados confidenciais em sistemas de armazenamento, redes e endpoints;
- Todos os componentes que fazem parte da solução deverão estar integrados com suporte para os seguintes sistemas operacionais: Windows 7, Windows 8 ou 8.1, Windows 10, Windows Server 2016, Windows Server 2019 e versões superiores.

3. **Console de gerenciamento**

- Deve ter administração centralizada por console único de gerenciamento;
- As configurações de todos os módulos de detecção e criação de relatórios deverão ser realizadas através da mesma console;
- O gerenciamento da solução deve ser baseado em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação criptografada (HTTPS/TLS, versão 1.2 ou superior). Também será aceita a instalação de aplicação cliente (console de gerência) nas estações dos analistas responsáveis pela gestão da solução;
- O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, em um dos sistemas operacionais:
  - Microsoft Windows Server; e

- Red Hat Enterprise Linux;

- Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado;
- Deve possuir integração com Active Directory, para autenticação de usuários da solução;
- Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação;
- Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;
- Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;
- Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;
- Deve permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);
- Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;
- Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;
- Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados;
- Deve possuir logs detalhados de auditoria de alterações de políticas;
- Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;
- Deve ter suporte a servidores com hardware x86 e sistema operacional Windows ou Linux, não requerendo a utilização de appliance;

4. **Implementação e gerenciamento do agente**

- O agente deve ser suportado no mínimo nos seguintes Sistemas Operacionais:
  - Windows 7 SP1;
  - Windows 8 ou 8.1;
  - Windows 10 ou superior;
  - Windows Server 2016;
  - Windows Server 2019 e versões superiores;
  - Apple MAC OS X 10.15.0 e versões superiores.
- A gerência da solução deverá ser responsável pela Distribuição (Deploy), Instalação, Gerenciamento e Desinstalação do Agente nas estações, bem como deverá executar inventário das máquinas nas quais estão com agentes instalados, esse inventário deverá coletar informações cruciais para o uso ideal do agente de DLP na estação do usuário; o Essa instalação poderá ser remota de forma silenciosa e sem a intervenção do usuário;
- Um único agente deve executar todas as funções, inclusive a verificação de terminais e a monitoração e bloqueio de dados que saem do terminal;
- A soluçaõ deve integrar-se com os drivers do sistema operacional Windows em várias aplicações para garantir a estabilidade, interoperabilidade e segurança.;
- As atualizações dos agentes devem ser enviadas diretamente pela console de gerenciamento;

5. **Segurança do agente**

- As comunicações entre o agente e o servidor devem ser criptografadas e autenticadas;
- Deve permitir a opção de solicitação de senha para desinstalar o agente;
- Deve ter a capacidade de monitorar e bloquear tentativas de cópia de conteúdo confidencial para, no mínimo, os seguintes dispositivos (a ferramenta deve ser capaz de liberar a gravação ou somente leitura):
  - Drives USB;
  - CD/DVD;
  - SD e Compact flash cards.
- Deve ser integrável com ferramentas de criptografia, a fim de criptografar apenas o conteúdo confidencial enviado para um dispositivo USB ou e-mail;
- Deve monitorar tentativas de cópia de conteúdo confidencial para o disco rígido e para compartilhamento na rede;
- Deve exibir alerta "pop-up" na tela do usuário em caso de violação de política;
- O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial;
- Deve permitir monitorar e bloquear transmissão FTP;
- Deve, para um grupo pré-determinado de usuários, permitir o envio de informação confidencial, apresentando um “pop-up” de alerta quanto a criticidade da informação e solicitando confirmação da ação, a qual deve ser logada na console central;
- A solução deverá utilizar banco de dados relacional SQL Server ou Oracle. Todas as licenças para uso do banco de dados devem ser fornecidas;
- A solução deve permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
- A solução deve ter capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
- A solução deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção;
- A solução deve possuir módulos de detecção distintos, licenciados de forma independente, gerenciados por console único, para:
  - Localizar dados confidenciais armazenados em servidores de arquivos, intranet e bancos de dados;
  - Localizar dados confidenciais armazenados em desktops e laptops;
  - Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP, capturando tráfego em modo promíscuo;
- A solução deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações sensíveis detectadas;
- A solução deve possuir, no mínimo, 60 modelos de políticas preexistentes produzidas, suportadas e atualizadas pelo fabricante da solução ou pelo CONTRATADO, que incluem palavras-chave e padrões de dados, para no mínimo, as principais normas internacionais HIPAA, Cobit, ISO 27002, PCI, SOX e GDPR/LGPD.
- Toda política criada na solução deve ser única, compatível e válida para aplicação em qualquer um dos módulos (agente, monitor de rede, scanner de dado armazenado);
- A solução deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:
  - Conteúdo detectado em arquivos e tráfego de rede (protocolos);
  - Remetente e destinatário de correio;
  - Tipo real (baseado em cabeçalho, não extensão),
  - Nome e tamanho do arquivo;

- Protocolo de comunicação utilizado;

- A solução deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
  - Compactados (ZIP, RAR, GZ, LHA, HQX, JAR);
  - CAD (DWG, DXF, VSD, DGN);
  - Planilhas (XLS, XLSX, 123, SXC, ODS);
  - Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
  - Apresentações (PPT, PPTX, SXI, SXP, ODP);
  - Outros (PDF, MDB);
- A solução deverá ter a capacidade de detectar e bloquear incidentes de tentativa de vazamento de informação confidencial, fornecendo detalhes dos arquivos oriundos dos incidentes na console da solução, com informações de contexto (hora, classificação, regras, propriedades, entre outros);
- A solução deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo;
- A solução deve possuir recursos avançados de inspeção de conteúdo, incluindo OCR;
- A solução deve ter a capacidade de indexar através de impressão digital (hash) para dados estruturados e não estruturados;
- A solução deve ter a capacidade de normalizar todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);
- A solução deve possuir capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
- Deve permitir a criação de dicionários de dados baseados em palavras-chave, frases e expressões regulares para serem usados nas regras de DLP;
- A solução deve ter a capacidade nativa de detectar uma grande variedade de padrões de dados que representam dados confidenciais (por exemplo, CPFs, depósitos, dados da tarja magnética, IBAN);
- A solução deve ter a capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, EUA, União Europeia, e Brasil;
- A solução deve permitir detectar faixas de números válidos para determinados tipos de dados, tal como, no mínimo, número de cartão de crédito válido;
- A solução deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails;
- A solução deve ter a capacidade de bloquear a captura de tela (print screen) integral, ou seja, mesmo que seja de uma janela NÃO ativa no momento da captura;
- A solução deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem;
- A solução deve suportar a verificação de arquivos compactados recursivos (exemplo zip dentro de zip);
- A solução deve identificar conteúdo armazenado em colunas específicas de planilhas eletrônicas e em bancos de dados;
- A solução deve ser capaz de gerar incidentes para detecção se parte do conteúdo for copiado;
- A solução deve, em um determinado incidente, permitir a verificação por assunto, remetente, destinatário, nome de arquivo, proprietário do arquivo, nome de usuário e política;
- A solução deve exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo;
- A solução deve permitir ocultar certos dados, como informações de identidade do remetente, durante a visualização do Incidente na tela do Console, dependendo do nível de acesso dado ao operador da ferramenta, para no mínimo, os seguintes tópicos:
  - Endereço de e-mail;
  - Nome de usuário;
  - Proprietário do arquivo;
- A solução deve permitir destacar na tela do incidente os dados confidenciais detectados;
- A solução deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo;
- A solução deve possuir mecanismo de envio de notificações personalizáveis através de e-mail, como casos de violação de política;
- A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações;
- A solução deve ser permitir notificar automaticamente o remetente e o gerente ou superior hierárquico do usuário envolvido no incidente;
- A solução deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:
  - Bloqueio de mensagem;
  - Quarentena de arquivo;
  - Notificação ao usuário;
  - Bloqueio do acesso web;
  - Bloqueio de cópia e impressão;
- A solução deve permitir armazenar a mensagem e o arquivo original que gerou o incidente;
- A solução deve verificar existência de conteúdo confidencial em file systems para no mínimo CIFS, NFS, SMB e NTFS;
- A solução deve permitir a análise dos file systems sem a necessidade de agentes nos servidores de origem;
- A solução deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP;

6. **Classificação da informação**

- A solução deve possibilitar classificar tanto a informação recém-criada, como as já existentes;
- A solução deve ter a capacidade de, automaticamente, classificar arquivos, para no mínimo:
  - Word, Excel, PowerPoint e Project Microsoft Office;
  - Open Office;
  - PDF;
  - ZIP;
  - MSG, TIF e EML files;
  - JPEG;
  - HTML.
- A solução deve ter a capacidade de permitir ao usuário realizar a classificação da informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas;
- A solução deve possibilitar a customização de graus de sigilo/categorias para a classificação da informação pelo usuário de acordo com a política de classificação da instituição;

- A solução deve ter integração para classificação da informação pelo usuário, para no mínimo:
  - Word, Excel, PowerPoint e Project Microsoft Office;
  - Open Office;
  - PDF;
  - ZIP;
  - MSG, TIF e EML files;
  - JPEG;
  - HTML.

7. **Proteção de Dispositivos não autorizados**

- A solução deve ser instalada em computadores com Sistemas Operacionais Windows e OS X/macOS;
- A solução deverá permitir o bloqueio total do dispositivo ou apenas o monitoramento;
- Deve permitir o controle dos seguintes dispositivos:
  - Dispositivos de Armazenamento Removíveis;
  - Dispositivos Bluetooth;
  - MP3 Players;
  - Dispositivos Plug and Play
- Deve controlar quais dados podem ser copiados para mídias removíveis;
- Deve permitir o bloqueio da execução de aplicativos a partir de dispositivos removíveis, podendo criar exceções ao bloqueio;
- Deve permitir a proteção de drives USB, smartphones e dispositivos Bluetooth;
- Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;
- A solução deve permitir a proteção de dispositivos móveis com base em:
  - Classe do Dispositivo: Agrupamento de dispositivos com as mesmas características e possibilidade de gerenciamento do mesmo;
  - Definição do Dispositivo: Identifica e agrupa dispositivos conforme propriedades comuns;
  - Regras: Controlam o comportamento do dispositivo;
- Deve permitir a configuração dos dispositivos nos modos:
- Bloqueio, ou;
- Somente Leitura;
- Para a família Windows, deve permitir a classificação dos dispositivos em 3 categorias:
  - Gerenciado;
  - Não gerenciado;
  - Em Lista Branca.
- Deve permitir o agrupamento de dispositivos por meio de propriedades comuns, como por exemplo: VendorID, ProductID, Device Class;
- Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:
  - Tipo de BUS;
  - Classe do Dispositivo (Device Class);
  - ID do fabricante (Vendor ID);
  - ID do produto (Product ID).
- Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:
  - Tipo de BUS;
  - Se o sistema de arquivo é passível de escrita;
  - Se o sistema de arquivo é somente leitura;
  - Tipo de Sistema de Arquivo;
  - Nome do Sistema de Arquivo;
  - Número de Série do Sistema de Arquivo.
- Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive);
- Deve possuir as seguintes classes de dispositivos de maneira nativa:
  - Bateria;
  - Biometria;
  - Bluetooth;
  - Drives de CD/DVD;
  - Decoders;
  - Adaptadores de vídeo;
  - Disco Fixo;
  - Controladoras de Disquete;
  - Drives de Disquete;
  - GPS;
  - Infravermelho;
  - IEEE 1394;
  - Mouse;
  - Modem;
  - Fax;
  - Adaptadores de Rede;
  - PCMCIA.
- Deve possuir os seguintes modelos:
  - Dispositivos Apple;
  - Dispositivos BlueTooth;
  - Drives CD/DVD;
  - Dispositivos de armazenamento removível;
  - Leitor de cartão SD.
  - Dispositivos Windows Portable;
  - Dispositivos Plug-n-Play USB.

- Deve ser possível criar modelos customizados para, no mínimo:
  - Disco Fixo;
  - Dispositivo Plug-n-Play;
  - Dispositivo de Armazenamento Removível.
- Deve ser possível criar classe de dispositivos customizados utilizando o GUID (Globally Unique Identifier) do dispositivo;
- Ao identificar um novo dispositivo conectado no computador cliente, cujo hardware for desconhecido, a solução deve emitir um alerta no console centralizada indicando uma nova classe de dispositivo encontrada;
- Deve permitir atrelar um Usuário ou Todos os usuários a um dispositivo específico por meio do seu GUID;
- Deve permitir, no console centralizada, a criação dos seguintes controles:
  - Regra para controle de Dispositivo Citrix XenApp;
  - Regra para controle de Disco Rígido Fixo;
  - Regra para dispositivos Plug-n-Play;
  - Regra para dispositivos de armazenamento removível;
  - Regra de acesso de arquivos a dispositivos de armazenamento removível;
  - Regra de Dispositivo TrueCrypt.
- Para cada regra, deve ser possível aplicar para:
  - Qualquer usuário (All);
  - Pertencer a um determinado grupo;
  - Pertencer a todos os grupos;
  - Usuário local ou usuário não-LDAP.
- Durante a definição da regra, deve permitir a escolha da identificação do objeto LDAP, para, no mínimo:
  - SID do Objeto;
  - Nome do Objeto;
  - Domínio\Nome do Objeto.
- Para cada regra deve ser possível configurar exclusões para, no mínimo:
  - Usuários;
  - Dispositivos.
- Para cada regra deve ser possível configurar a severidade entre, no mínimo:
  - Informação;
  - Atenção;
  - Menor;
  - Maior;
  - Crítico.
- Para cada regra, a solução deve permitir a configuração de reações distintas entre:
  - Computador conectado à rede corporativa;
  - Computador desconectado da rede corporativa.
- Deve possuir capacidade de controlar (Bloquear) o acesso a determinadas extensões ou arquivos TrueType a dispositivos de armazenamento removíveis;
- A solução deve permitir que se desabilite uma regra dentre o conjunto de regras.

8. **Relatórios**

- A solução deve permitir a emissão de relatório de incidentes e tendências por empresa, departamento e usuário, utilizando o LDAP (MS Active Directory) corporativo;
- A solução deve permitir agrupar, filtrar e classificar relatórios;
- A solução deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
  - Timestamp;
  - Tamanho e data do arquivo;
  - Endereço IP de origem e destino;
  - Histórico de incidentes e detalhes;
  - Remetente e destinatário;
- A solução deve permitir exportar relatórios para formato PDF, HTML, XML ou CSV;
- A solução deve ter capacidade de enviar relatórios por e-mail via agendamento (datas específicas e periodicamente);
- A solução deve apresentar um painel de controle para visualização dos relatórios;
- A solução deve ter a capacidade para configurar, salvar relatórios e painéis de controle personalizados por usuário;
- A solução deve ter opção de publicar relatórios salvos para todos os usuários ou mantê-los como relatórios pessoais.;
- A solução deve permitir gerar relatórios resumidos por níveis, agrupados, sumarizados e com capacidade de detalhamento;

ITEM 03 - LICENÇA DE USO DE SOFTWARE/PROGRAMA DE FILTRAGEM E PROTEÇÃO DE NAVEGAÇÃO WEB DO TIPO SECURE WEB GATEWAY

1. **Características Gerais da Solução**

- A solução deve ser integrada e do mesmo fabricante da plataforma de Proteção de Endpoints, DLP, e IDS/IPS.
- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- A solução deve permitir a instalação em ambientes tecnológicos distintos, uma vez que será utilizada em redes segregadas e operada de forma independente pelas equipes de TI da CONTRATANTE;
- O sistema utilizado deve possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão; e
- Deve possuir serviço de Suporte Técnico e garantia de atualização durante o período da assinatura contratada.

2. **A solução deverá ser especializada para o tratamento de filtragem de conteúdo Web para, no mínimo, as seguintes funcionalidades:**

- Filtro de URL´s baseado em lista;
- Filtro de acesso web baseado em categorias do site acessado;
- Filtro de ameaças digitais (malware);
- Filtro de tipo de arquivo (media filtering);
- Filtro de aplicações web;
- Controle de utilização de banda;
- Gerenciamento de quota por tempo ou volume;
- Manipulação de código HTML da página web;
- Autenticação de usuários para navegação;
- Filtro de arquivos;
- A solução deverá implementar filtros ao tráfego HTTP, mesmo que o tráfego esteja criptografado em SSL 3.0 ou TLS nas versões 1.0, 1.1 e 1.2;
- O gerenciamento da solução de regras e configurações da solução de filtro de conteúdo deve ser realizado no próprio equipamento ou máquina virtual, não sendo necessária a instalação de servidores ou equipamentos adicionais para este fim;
- A funcionalidade de proxy deve ser nativa e integrada ao equipamento ofertado tanto para HTTP como para HTTPS;
- A solução proposta deverá implantar a funcionalidade de filtro dos protocolos HTTP, HTTPS e FTP;
- A solução deverá suportar redirecionamento para filtragem através do protocolo WCCP (Web Cache Communication Protocol);
- Deverá suportar os seguintes modos de operação:
  - Modo Proxy explícito;
  - Modo Proxy em Alta Disponibilidade (Não deve existir a dependência de equipamentos externos para utilização de alta disponibilidade);
  - Modo roteador transparente, com recebimento de roteamento explícito;
  - Modo transparente em linha, capaz de realizar filtro interconectado entre dois equipamentos de rede;
- Deve suportar a operação como servidor ICAP;
- Deve suportar a operação como cliente ICAP;
- Deverá permitir que os modos de proxy explícito e roteador transparente possam ser utilizados simultaneamente;
- Caso a solução não possibilite o funcionamento em modo simultâneo nos dois modos indicados no item anterior, o fornecedor deverá entregar dois ambientes de modo a satisfazer este requisito;
- Ao ser configurado em modo transparente em linha o equipamento deverá efetuar a monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 (Layer-2) do modelo OSI (Open System Interconnection), ou seja, a interface de monitoração e proteção não requer endereço IP configurado;
- A configuração das placas de rede da solução ofertada deve suportar endereços IPv4 e endereços IPv6;
- Em ambas configurações de IPv4 e IPv6 deve ser possível a configuração de MTU;
- A solução deve permitir a configuração manual e/ou automática de horário através de servidores NTP a serem configurados na solução;
- Deve possuir função de CACHE nativa na solução sem necessidades de produtos terceiros ou utilização de outros equipamentos para a realização desta função;
- Deve suportar FTP sobre HTTP nos modos ativo/passivo;
- Deve possibilitar a configuração das portas utilizadas para o serviço de proxy;
- Deve possuir a capacidade de restringir as portas utilizadas para o comando HTTP CONNECT;
- Deve permitir segregação de interfaces de rede com conectividade para funções específicas para, no mínimo, as seguintes funções:
  - Conectividade de clientes para o equipamento de filtro de conteúdo;
  - Conectividade do equipamento de filtro de conteúdo com a Internet;
  - Conectividade dos clientes quando na rede interna;
  - Conectividade dos clientes quando na rede externa.
- Deve ser capaz de criar lista de destinos que serão excessões às regras de filtro de conteúdo e políticas baseadas, no mínimo, em:
  - Endereço IP;
  - CIDR (Classless Inter-Domain Routing);
  - Domínio;
  - Hostname completo ou parte;
- Deverá atuar como proxy transparente através do redirecionamento de conexões utilizando WCCP;
- Deve possuir integração com serviços de diretório LDAP e domínios Active Directory para auditoria e autenticação sem a necessidade de instalação de agentes ou plugins em estação de trabalho ou servidor;
- A solução deverá ser capaz de criar e hospedar arquivos PAC (Proxy Auto-configuration);
- A solução deverá ser capaz de hospedar arquivos WPAD.DAT;
- A solução deverá ser capaz de analisar requisições HTTP e FTP independente da porta TCP utilizada;
- A solução deve oferecer customização para arquivos de log de acesso, registrando em log, no mínimo, os seguintes itens:
  - Usuário;
  - Grupo de usuário;
  - Categoria do site acessado;
  - URL;
  - Porta da URL;
  - Data;
  - Horário;
  - Texto fixo personalizado;
  - Endereço IP de origem e destino;
- Deverá suportar IP Spoofing para implementação em modo transparente;
- A solução deve suportar instalação em ambiente virtualizado com os seguintes hypervisors:
  - VMWare ESXi;

- Hyper-V;
- A solução deve suportar a instalação em instância Amazon EC2;

3. **Características de software - filtragem e reputação de sites**

- A base de URLs deve ser atualizada automaticamente via Internet, por meio de uma base proprietária do fornecedor que suporte os serviços descritos neste termo e os equipamentos listados;
- A base de URLs deve manter o conhecimento de pelo menos 105 (cento e cinco) categorias pré-definidas e no mínimo 20 (vinte) milhões de domínios de URL's cadastradas;
- O fabricante deverá prover métodos de consulta em tempo real das categorias de um determinado site, bem como permitir que os administradores consultem a categoria diretamente através do equipamento de filtro de conteúdo;
- Deve possibilitar a criação de no mínimo 500 (quinhentas) categorias extras customizadas (definidas pelo usuário);
- A ferramenta deve ser capaz de realizar controle de banda para download/upload;
- A solução deve ser capaz de controlar utilização mínima e máxima de banda para determinados tipos de tráfego;
- O controle de banda deve ser granular, ou seja, podendo ser aplicado com restrições aos seguintes parâmetros:
  - Grupo de usuários;
  - Horário;
  - Categoria do Site.
- Deve ser possível enviar para o fabricante da solução as URLs não cadastradas na base de dados para análise e inclusão na base de categorias.
- Deve permitir a criação de filtros URLs baseado em políticas de tempo, tais como dias da semana e range de horário, ou seja, alguns sites só poderão ser acessados fora do horário de expediente.
- Deverá ser capaz de criar ações diferentes para as URL´s em políticas por tempo.
- Deve ser capaz de realizar a detecção de URLs frente a composição dos seguintes itens:
  - URL;
  - Host;
  - Domínio;
  - Protocolo;
  - Caminho da URL.
- Deverá possuir modelo de notificação padrão aos usuários através de páginas de bloqueio;
- Deverá permitir customização das páginas de notificações existentes e a criação de novas páginas de resposta podendo personalizar, no mínimo:
  - Fonte utilizada;
  - Imagens;
  - Mensagem;
  - Cores e logo;
  - Inclusão de hyperlinks;
  - Nome da política que ocasionou o bloqueio;
  - System name e IP do cliente.
- A solução deverá detectar, monitorar e interceptar o acesso feito às páginas abertas dentro de servidores remotos, como:
  - Servidores de tradução;
  - Proxies anônimos.
- As transações que forem detectadas deverão estar de acordo com as políticas estabelecidas pela empresa, onde o conteúdo não permitido que for acessado sob este mecanismo deverá ser bloqueado e o conteúdo dentro de políticas que permitem o acesso deverão ser permitidos;
- Deve possuir, no mínimo, as seguintes categorias URL:
  - Sites de conteúdos maliciosos;
  - Site de bate-papo (chat) e fóruns on-line;
  - Sites de Anonymizers;
  - Sites com utilitários para Anonymizing;
  - Browser Exploits;
  - Sites de Encontros (Dating);
  - Sites de Discriminação;
  - Sites sobre Drogas;
  - Sites sobre Apostas;
  - Sites sobre conteúdo agressivo (Gruesome Content);
  - Site com downloads maliciosos;
  - Site com download de media;
  - Sites de compartilhamento de medias;
  - Instant Messaging;
  - P2P/File Sharing;
  - Sites para armazenamento de dados pessoais (Personal Network Storage);
  - Sites sobre Potenciais Atividades Criminais;
  - Sites sobre Potenciais Crimes de Hacking/Computer Crime;
  - Sites sobre Potenciais Softwares Ilegais;
  - PUPS;
  - Endereços de IP Residencial;
  - Shareware/Freeware;
  - Spyware/Adware/Keyloggers;
  - Web Mail.
- Deve possuir um sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino, utilizando dados de uma rede mundial de monitoração de tráfego web e de e-mail para definir a reputação dos servidores de destino com cobertura global;
- Permitir ações diferenciadas de acordo com cada reputação obtida, como bloquear, permitir ou verificar detalhadamente os objetos de cada acesso;
- O produto deve ser capaz de realizar controle de aplicações web aplicando políticas por:
  - Aplicações;
  - Usuários;
  - Grupos de risco de aplicação.
- O filtro de aplicação deve permitir configurar permissão de acesso de somente leitura para aplicações específicas;

- Deve possuir capacidade de classificação de conteúdo dinâmico, aplicando categorização aos websites que eventualmente ainda não estejam categorizados pelos serviços de nuvem do fabricante ou localmente;
- Deve possuir serviço de inteligência do fabricante da solução, nativo ao produto, para informação de URLs de alto risco, médio risco e baixo risco;
- Ao detectar uma URL de alto risco ou médio risco o equipamento deve emitir uma notificação ao usuário oferecendo a opção de prosseguir caso o risco seja aceitável;
- O equipamento deve ser capaz de extrair conteúdo HTLM e permitir que valores de tags e elementos possam ser removidos ou alterados;
- Deve ser capaz de efetuar bloqueios e controle de Web 2.0, como por exemplo:
  - Liberar apenas canais específicos do Youtube;
  - Bloqueio de determinados canais do Youtube;
  - Bloqueio de vídeos do YouTube por palavras chave;
  - Bloqueio do Chat do facebook;
  - Bloqueio da Criação de Eventos do facebook;
  - Bloqueio de carregamento de vídeos e fotos para o Facebook.

4. **Autenticação**

- Autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha para o usuário;
- Autenticação segura de clientes, ou seja, os dados de autenticação trocados entre o servidor de diretórios e o proxy estejam criptografados, tanto para LDAP como para NTLM;
- Autenticação baseada em LDAP;
- Utilização de um NTLM-Agent, sendo um agente externo instalado em um sistema baseado em Windows para aplicação do método de autenticação NTLM;
- Banco de dados de usuários em uma base na própria solução;
- Através de servidores LDAP;
- Através de servidores Novell eDirectory;
- Através de servidores RADIUS;
- Através de servidores Kerberos;
- Através de servidores de autenticação externo;
- A autenticação deve possuir compatibilidade com todos os métodos abaixo descritos:
  - Básica (Basic Authentication) utilizando tecnica de POPUP;
  - NTLM over Proxy;
  - Kerberos over HTTP;
  - SAML v2.
- Autenticação (login, senha e domínio) para usuários que estejam utilizando sistemas operacionais diferentes do Windows (Linux, por exemplo), validando estes usuários no serviço de diretórios Microsoft Active Directory;
- Autenticação de usuários e estações de trabalho sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho e/ou servidor;
- Total integração com o Microsoft Active Directory para autenticação de usuários e reconhecimento de grupos de domínio, sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos nas estações de trabalho dos usuários ou nos servidores;

5. **Criação de regras**

- A solução ofertada deve possuir mecanismo de criação de regras a partir de lógica booleana permitindo flexibilidade e otimização a partir de parâmetros pré-definidos;
- A solução deve permitir a criação de regras standalone e conjuntos de regras de forma independente;
- A solução deve permitir a criação de conjunto de regras baseados em critérios para que seja válida;
- Estes critérios devem ser aplicados para requisições e respostas HTTP(S) e FTP, além de objetos incluídos no corpo da resposta ou requisição;
- O produto deve possuir pelo menos 400 propriedades baseadas em características do acesso HTTP(S) para identificar, no mínimo:
  - Caminho da URL acessada;
  - Endereço IP de destino;
  - Protocolo utilizado;
  - Cabeçalho Referer;
  - Tipo do conteúdo baseado no cabeçalho Content-Type;
  - Tamanho do objeto, em contexto de arquivo, enviado através de pagínas web;
  - Domínio da URL acessada;
- Aplicação do conjunto de regras deve se basear em todas as propriedades e permitir a criação de lógica booleana entre estas propriedades e seus valores para decisão de habilitação ou não desse conjunto de regras;
- O equipamento deve ser capaz de realizar as seguintes ações no caso de satisfazer um critério de regra:
  - Bloquear;
  - Permitir;
  - Remover conteúdo;
  - Redirecionar o acesso;
- Cada propriedade deverá ser comparada a um valor através de operadores (igual, diferente, pertence a lista, não pertence a lista, maior que, maior que ou igual, menor que, ou menor que ou igual) para ser considerada válida ou não e com isso tomar a decisão se a regra é aplicável àquele acesso web;
- Dentro das regras deve ser possível combinar várias características do acesso utilizando propriedades através de operadores lógicos “OU” e “E” (AND, OR), não havendo limitação de quantas características possam ser incluídas em uma única regra;
- Após validação desta regra o produto deve tomar as seguintes ações:
  - Autenticar;
  - Bloquear;
  - Continuar;
  - Redirecionar;
  - Remover;

- Parar analise do ciclo;
- Parar análise do conjunto de regras;

- A solução deve permitir o uso de listas nas regras utilizando a mesma lógica booleana acima explicadas:
  - Categorias;
  - Autoridades Certificadoras;
  - Hosts e certificados confiáveis;
  - Endereços IP;
  - Intervalos de endereço IP;
  - Usuários locais;
  - Tipo de mídia;
  - Números;
  - Expressões Regulares (utilizando REGEX e/ou GLOB);
- A solução deve possuir mecanismo de DLP para web nativo, sem necessidade de licença adicional;
- A solução deve ser capaz de integrar-se a ferramenta de DLP de rede através de ICAP com suporte a REQMOD E RESPMOD;
- A ferramenta deve ser capaz de bloquear o envio de documentos para web baseado em extensão ou tipo de documento;

6. Inspeção de canais criptografados (HTTPS)

- Deve permitir a inspeção de canais cifrados (HTTPS);
- A abertura do tráfego HTTPS deve ocorrer no mesmo equipamento de filtro de conteúdo, não sendo necessário equipamentos terceiros;
- Deve permitir que a criptografia seja removida e entregue a um equipamento terceiro para análise através de ICAP;
- Deve ser capaz de realizar três funções básicas, dentre elas:
  - Tratamento do método CONNECT, isto é, terminar a negociação TLS com clientes e abrir um túnel de comunicação com host de destino;
  - Verificação de certificados do site de destino;
  - Abertura do tráfego para inspeção de conteúdo.
- Deve permitir a isenção de inspeção em, no mínimo, nas seguintes ocasiões:
  - Categoria eximida pelos administradores;
  - Site web eximido pelos administradores;
  - Conexão utilizando certificados de cliente.
- Deve permitir a troca do certificado raiz utilizado para inspeção de tráfego HTTPS;
- Deve permitir a inspeção do certificado do site de destino, mesmo quando a solução for instalada em modo transparente;
- Deve realizar a validação dos certificados para, no mínimo:
  - Certificados expirados;
  - Auto assinados;
  - Cadeia muito longa;
  - Desconhecidos;
  - Expirados;
  - Não confiáveis.
- A partir desta validação, deve ser possível utilizar a predisposição em regras para posterior bloqueio sob condições não autorizadas, sendo possível utilizar uma das condições acima ou todas ao mesmo tempo;
- Deve permitir a criação de lista branca para certificados que não deverão ser inspecionados;

7. **Características do módulo AntiMalware**

- A solução deverá possuir um módulo de análise de malwares desenvolvido pelo fabricante da solução, não sendo aceitos OEMs;
- A solução deve oferecer a opção de no mínimo dois mecanismos de antivírus rodando simultaneamente possibilitando uma camada adicional de filtragem;
- Se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, SNMP e E-mail;
- Deve realizar a análise de comportamento (emulação) das páginas que serão acessadas;
- Identificar e bloquear aplicações Java Scripts maliciosas;
- Identificar e bloquear aplicações Java applets maliciosas;
- Identificar e bloquear aplicações Java applications maliciosas;
- Identificar e bloquear aplicações ActiveX maliciosas;
- Identificar e bloquear aplicações Flash ActionScripts;
- Identificar e bloquear aplicações executáveis Windows maliciosas;
- Identificar e bloquear scripts Visual Basic maliciosos;
- Identificar e bloquear aplicações potencialmente não desejadas;
- Deve possuir tecnologia de análise em nuvem para arquivos suspeitos. Esta tecnologia deve se basear no envio do hash do arquivo/código para o centro de inteligência do fabricante a fim do mesmo validar se o arquivo é malicioso ou não e prover o bloqueio/controle sem a necessidade de vacina instalada na solução ofertada;
- Possuir filtros de análise de comportamento para proteção pró-ativa contra ataques de dia zero com bloqueio de tráfego web em tempo real sem a necessidade de possuir uma assinatura;
- A varredura deverá ser feita sequencialmente no sistema, sem o uso de protocolos de comunicação entre as ferramentas, como por exemplo o protocolo ICAP;
- A solução deve possibilitar bloquear todos os comportamentos/técnicas abaixo descritas:
  - Data theft: Backdoor;
  - Data theft: Keylogger;
  - Data theft: Password stealer;
  - System compromise: Code execution exploit;
  - System compromise: Browser exploit;
  - System compromise: Trojan;

- Stealth activity: Rootkit;
- Viral Replication: Network worm;
- Viral Replication: File infector virus;
- System compromise: Trojan downloader;
- System compromise: Trojan dropper;
- System compromise: Trojan proxy;
- Web threats: Infected website;
- Stealth activity: Code injection;
- Detection evasion: Obfuscated code;
- Detection evasion: Packed code;
- Potentially unwanted: Ad-/Spyware;
- Potentially unwanted: Adware;
- Data theft: Spyware;
- Potentially unwanted: Dialer;
- Web threats: Vulnerable ActiveX controls;
- Potentially unwanted: Suspicious activity;
- Web threats: Cross-site scripting;
- Potentially unwanted: Deceptive behavior;
- Potentially unwanted: Redirector;
- Potentially unwanted: Direct kernel communication;
- Potentially unwanted: Privacy violation.

8. **Cache**

- Deve possuir capacidade de armazenar objetos para otimizar a entrega a solicitação dos clientes;
- Deve ser possível controlar as URL's que serão armazenadas em cache;
- Deve permitir o controle dos arquivos que deverão ser armazenados em cache;
- Deve permitir o controle do tamanho dos arquivos armazenados em cache;
- Deve permitir cache de sites utilizando o protocolo HTTPS;

9. **Casos de uso**

- Deve permitir o controle granular de Facebook, para no mínimo:
  - Controle do applet de mensagens;
  - Controle de posts;
  - Controle de eventos.
- Deve permitir o controle granular do Youtube, para no mínimo:
  - Controle por canal;
  - Controle por uploader;
  - Controle por palavra chave;
  - Controle por categorização do YouTube;
- Deve permitir o controle granular do Wikipedia, para no mínimo:
  - Bloqueio do frame de edição.
- Deve permitir a criptografia de arquivos que são enviados para armazenamento em nuvem (Dropbox, Google Drive, One Drive);
- Ao criptografar um arquivo o mesmo só poderá ser descriptografado após passagem pela solução de Filtragem Web;
- Este módulo deverá ser nativo da solução e não requerer nenhum equipamento externo;
- Deve ser capaz de bloquear páginas por país de origem (Geolocalização);
- Deve permitir a criação de portais de alerta, antes de um usuário acessar uma determinada categoria de URL, deve-se apresentar um portal informando uma mensagem a ser definida pelo administrador da solução;
- Deve ser capaz de bloquear aplicações web categorizadas como indesejadas pelo administrador, dentre elas:
  - Voice over IP (Exemplo: Google Voice);
  - Tunel (Exemplo: Tor e UltraSurf);
  - Redes Sociais (Exemplo: Facebook, Google Hangout, Google Plus, Twitter);
  - Webmail (Exemplo: Hotmail, Yahoo);
  - FileShare (Exemplo: Box.net, BitTorrent, Filestube, Gnutella);
  - IM (Exemplo: Skype).
- Deve utilizar a reputação do Centro de Inteligência do fabricante para determinar, de maneira automática, aplicações de médio e alto risco e o posterior uso da predisposição para criação de regras de bloqueio;
- Detectar e bloquear "user agent" não autorizados;
- Deve permitir a criação de regras para não permitir que aplicações web e URL's realizem o comando POST (apenas leitura);
- Deve permitir o uso de dicionário para controle de fuga de dados (DLP);

10. **Módulo de Gestão**

- A gestão do produto deve estar embarcada no próprio equipamento ou Máquina Virtual, sem a necessidade de servidores externos;
- A gerência deve ser via Interface Web;
- Deve possuir capacidade de aceitar comandos via linha de comando (SSH);
- Possuir MIB própria para verificação das informações de utilização via SNMP;
- Possibilitar o envio de alertas administrativos utilizando e-mails e traps SNMP.;
- Possibilitar a criação de políticas de acesso a interface de gerenciamento baseada em endereço IP e range de IP's que podem acessar o sistema;
- Deverá possuir pelo menos sete perfis de usuários de acesso;
- Deverá permitir a criação de perfis de acesso customizado;
- A solução deverá permitir autenticação externa, para autenticar os usuários ao logar na gerência da solução através dos seguintes métodos de autenticação:

  - Através de servidores NTLM;
  - Banco de dados de usuários em uma base na própria solução;
  - Através de servidores LDAP;
  - Através de servidores Novell eDirectory;
  - Através de servidores RADIUS;
  - Através de servidores Kerberos;
- Deve possuir integração com a solução de proteção de endpoints;
- Deve prover as seguintes informações para relatórios:
  - Quantidade de Requisições/Segundo;
  - Alertas;
  - Erros;
  - Informações sobre a Engine de Analise de Malware;
  - Versão do Filtro URL;
- Relatórios pré-configurados com as seguintes informações:
  - Sumário Executivo de Acessos;
  - Sumário de Acessos a URL's;
  - Sumário das Categorias Acessadas;
  - Sumário dos Malwares Acessados;
  - Sumário do Sistema;
  - Utilização de Rede (Volume de Tráfego);
  - Utilização do Sistema;
  - Status do Update;
  - Sumário Web;
  - Tráfego por protocolo;
  - Requests por protocolo;
  - Volume de Tráfego;
  - Bytes transferidos por domínio;
  - Bytes transferidos por IP de origem;
  - Bytes transferidos por IP de destino;
  - Estatísticas de uso de CACHE;
  - Estatísticas do Filtro URL;
- Deve possuir capacidade de realizar a captura de sessão de usuário e identificar possiveis problemas na aplicação de uma regra em específico;
- Deve suportar o envio de informações de log para uma solução de SIEM do mesmo fabricante;
- Deve suportar captura de pacotes para mitigação de problemas de conexão (tcpdump);
- Deve permitir a realização de backup e restauração da configuração a partir da própria console de gerência;
- Deve possuir log de auditoria de todas as ações realizadas na console com, no mínimo, as seguintes informações:
  - Data e hora;
  - Usuário;
  - Ação;
  - IP origem;
  - Detalhes da ação;
- Deve permitir a configuração de Network Bonding através da console;
- Deve suportar a configuração de Source-based routing pela console;
- Deve permitir a configuração da quantidade de threads a ser utilizada para a análise de malware;
- Deve permitir informar ao usuário a tela de progresso da análise de um arquivo;
- Deve ser possível configurar o tempo máximo de retenção de logs e a sua auto exclusão após um tamanho pré-definido;
- Deve permitir a analise de navegação de um determinado endereço IP pela console em tempo real, de forma a permitir o administrador toda a visibilidade;
- Deve permitir o uso de múltiplas portas para o serviço de proxy, exemplo:
  - Porta 9090 para conexões com destino porta 80;
  - Porta 8080 para conexões com destino porta 443.
- Deve possuir capacidade de atuar como um proxy para conexões socks;
- Deve permitir a configuração de timeouts para:
  - Tempo máximo para conexões iniciais;
  - Tempo máximo para timeout de conexão;
  - Timeout para conexões de cliente;
  - Tempo máximo para conexões HTTP não utilizadas;
  - Timeout UDP.
- Deve permitir a configuração do valor máximo de conexões de clientes para um determinado appliance ou máquina virtual;
- Deve permitir, no mínimo, os seguintes comandos através de interface REST (Representational State Transfer):
  - Gerenciar listas;
  - Realizar backup;
  - Fazer download de arquivos de log;

11. **Módulo de Relatórios**

- A solução apresentada deverá possuir um mecanismo para geração de relatórios e logs;
- Serão aceitos módulos de relatórios que rodem fora do equipamento de filtro de conteúdo (out-of-box), desde que sejam do mesmo fabricante;
- Deve possuir ferramenta para análise de tráfego interativo, visando identificar o resultado das regras aplicadas, facilitando a metodologia de análise de problemas;
- Deve permitir que informações possam ser obtidas através de API;
- Deve permitir que os relatórios possam ser enviados por email;
- Deve permitir que a execução de relatórios seja agendada;

- O módulo de relatório deverá se adequar aos padrões de mercado, com suporte completo de instalação a no mínimo os seguintes sistemas operacionais e bases de dados:
  - Windows 2012 Server;
  - Windows 2016 Server;
  - Windows 2019 Server;
  - Microsoft SQL Server 2012 ou superior.
- Deverá permitir a criação dos relatórios nos formatos:
  - HTML;
  - PDF;
  - CSV.
- Deverá possuir no mínimo 30 relatórios pré-definidos, permitindo ao administrador configurar novos relatórios;
- Deve permitir a configuração de condições de determinados campos para o armazenamento em log;
- Deve suportar o envio de informações para syslog;
- Permitir personalização de relatórios para que possa ser possível a customização de, no mínimo, os seguintes itens:
  - Apresentação gráfico em fatias;
  - Apresentação de gráfico em barras;
  - Apresentação de gráfico bolha;
  - Apresentação de gráfico em linhas;
  - Apresentação de tabela;
  - Seleção de colunas que devem ser apresentadas.
- Permitir a utilização de campos da solução para filtragem de resultados, incluindo:
  - Site;
  - URL;
  - Categoria;
  - Usuário;
  - Grupo do usuário;
  - Data e Hora;
  - Aplicação Web;
  - Browser utilizado;
  - Se o conteúdo estava em cache.
- Permitir de forma opcional a criação de contas na ferramenta de relatório com restrição ao acesso a partes especifica dos dados com todos os filtros abaixo:
  - Usuários individuais;
  - Grupos de usuários;
  - Intervalos de endereço de IP de origem;
- Permitir atribuir colunas predefinidas, excluir colunas ou renomear colunas dos arquivos de log nos arquivos existentes. Isso deverá ser feito a partir de um assistente de customização de logs;
- Deverá prover uma interface de monitoramento (dashboard), apresentando a atividade de acesso web, incluindo:
  - Categorias;
  - Sites maliciosos - tentativas de acesso;
  - Sites acessados;
  - Usuários com maior incidência por endereço IP;
  - Usuários com maior incidência de acessos que envolvam malware;
  - Detecção de Malware por Site;
  - Utilização Web por reputação;
  - Consumo de banda de saída do tráfego;
  - Categorias com maior incidência de acesso por consumo de banda;
  - Aplicações web com maior incidência de acesso por consumo de banda;
  - Usuários com maior incidência de acesso por consumo de banda;
  - Comportamento da utilização Web.

ITEM 04 - EQUIPAMENTO DE DETECÇÃO E PREVENÇÃO DE INTRUSÃO DE REDE IDS/IPS

1. **Características de Gerais da Solução**

- A solução deve ser integrada e do mesmo fabricante da plataforma de Proteção de Endpoints, DLP, e Secure Web Gateway;
- Os equipamentos devem ser novos e de primeiro uso;
- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- O fornecedor deverá realizar também a instalação lógica migrando as configurações dos equipamentos de rede em produção para os novos ativos fornecidos;
- Os produtos utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão; e
- Deve possuir serviço de Suporte Técnico e garantia durante o período contratado.

2. **Características de Hardware**

- O equipamento deve ser baseado em Appliance com suporte a montagem em rack (bastidor) de 19” (dezenove polegadas), com utilização de no máximo 2-RU (duas unidades de bastidor) de altura;
- O equipamento deve ser baseado em arquitetura específica e desenvolvido, tanto software quanto hardware, para a funcionalidade única, exclusiva e específica de Next Generation Intrusion Prevention System, conforme documentos do Gartner, que é um referencial de mercado quanto ao posicionamento de tecnologias e possui requisitos para classificação de “Next Generation Network Intrusion Prevention, não sendo aceito um equipamento de uso geral e/ou multifuncional (UTM – Unified Threat Management/NGFW – Next Generation Firewall), tal como: Chassi servidor (Server Chassis), estação de trabalho (Desktop) e/ou equipamento blade;

- O equipamento deve ser baseado em armazenamento do tipo SSD (Solid State Disk) de no mínimo 240 GB, não sendo permitido utilização de armazenamento do tipo HDD (Hard Disk Drive);
- O equipamento deve permitir a entrada de ar frio pela frente e liberação de ar pela parte traseira;
- O equipamento deve suportar fonte de energia com chaveamento de voltagem automático;
- O equipamento deve suportar capacidade de operação em 100V à 240V (50/60Hz);
- O equipamento deve suportar redundância de fonte de energia substituível do tipo “hot-swappable”;
- O equipamento deve possuir, no mínimo, a seguinte capacidade instalada:
  - Porta console serial dedicada;
  - Dois módulos para expansão de interfaces;
  - Porta de gerência dedicada;
  - Duas portas USB.
- O equipamento deve possuir, no mínimo, 8 (oito) interfaces embutidas com velocidade de 10/100/1000 Mbps;
- Deve possuir ainda, no mínimo, 2 (duas) interfaces embutidas de fibra com velocidade de 1/10 GigE SFP+;
- Quando instalado em modo “inline” em caso de falha de hardware as 8 (oito) interfaces deverão permitir o fluxo normal do tráfego pelo equipamento de maneira nativa, ou seja, sem a necessidade de adição de módulos externos (deve possui fail-open interno);
- O equipamento deve suportar a expansão de interfaces, através de módulos, para a quantidade máxima de 18 (dezoito) SFP+ – Velocidade 10 Gbps;
- Deve possuir porta de resposta dedicada, sem contabilizar das 8 interfaces embutidas, para caso o equipamento seja instalado em modo SPAN;
- O equipamento deve possuir capacidade de processamento de 3 Gbps de tráfego agregado, considerando tráfego SSL de entrada utilizando chaves de tamanho 1.024 bits (128-bit ARC4);
- O equipamento deve suportar taxa de, no mínimo 4.000.000 (cinco milhões) conexões concorrentes e taxa de, no mínimo 200.000 (duzentas mil) novas conexões TCP por segundo;
- O equipamento deve suportar a taxa de, no mínimo, 115.000 (cento e vinte oito mil) novas conexões HTTP;

3. **Características do Modos de Operação**

- O equipamento deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando no modo de operação em linha (Inline Mode);
- O equipamento deve suportar os seguintes modos de operação:
  - SPAN Port (IDS);
  - TAP Mode;
  - In-line Fail-Closed;
  - In-line Fail-Open.
- O equipamento deve suportar, de forma simultânea e em interfaces distintas, os modos: SPAN (IDS Mode) e Inline (IPS Mode);
- O equipamento deve suportar monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 (Layer-2) do modelo OSI (Open System Interconnection), isto é, não ser necessário a configuração de endereço IP e existência de endereço MAC na porta de monitoração;
- O equipamento deve suportar instalação Inline Mode sem bloqueio para ataques, isto é, quando instalado em Inline Mode o equipamento pode ser configurado para não bloquear ataques específicos ou todos os ataques, apenas alertando-os;
- Quando instalado em Modo In-line o equipamento deve suportar:
  - Deve ser capaz de normalizar o tráfego;
  - Deve ser capaz de processar os pacotes em velocidades wire speed;
  - Deve ser capaz de priorizar tráfego;
- O equipamento deve suportar inspeção total do tráfego em ambiente com roteamento assimétrico e links agregados;
- O equipamento deve permitir a configuração de grupos de interface, ou seja, permitir que diferentes interfaces sejam configuradas para combinar o tráfego a ser processado tornando-as uma única interface lógica de estado e análise de intrusão;
- O equipamento deve suportar, em suas interfaces, a segmentação pelos seguintes tipos de tráfego:
  - Interface Dedicada;
  - VLAN;
  - Bridge VLAN;
  - CIDR.
- Deve permitir e estar licenciado para a virtualização, ou seja, deve ser capaz de segmentar tráfego diverso em uma única interface através da criação de interfaces virtuais;
- Deve permitir e estar licenciado para um total de 1.000 instâncias virtuais;
- O equipamento deve suportar instalação em modo de operação de alta-disponibilidade, utilizando apenas 1 (uma) interface de sincronismo “heartbeat”;
- O equipamento deve suportar configuração flexível de “inline-forward” (Layer-2) para tráfego que ultrapasse a análise de tráfego agregado (“over-subscription”) suportado pelo equipamento;
- O equipamento deve suportar os 3 modelos abaixo de alta-disponibililidade:
  - Ativo/Passivo: Quando dois sensores são instalados em segmentos de rede os quais configurados como um primário em modo ativo e um secundário em modo “standby”, sendo que o tráfego fluirá por apenas um caminho por vez;
  - Ativo/Ativo: Quando dois sensores são instalados em segmentos de rede os quais ambos os caminhos são ativos, sendo que o tráfego fluirá por ambos;
  - Stacked: Quando dois sensores são instalados em modo Ativo/Ativo em um único segmento de rede ativo;
- Quando configurado em alta disponibilidade, os equipamentos devem ser Stateful Fail-over, ou seja, utilizando-se dois equipamentos conectados entre si, mantendo os estados das sessões, em um ambiente configurado com roteamento simétrico;
- Quando configurado em alta disponibilidade os equipamentos devem manter os estados das sessões, em um ambiente configurado com roteamento assimétrico (ambos os links de comunicação ativos). Os equipamentos podem operar em modo ativo/ativo ou ativo/passivo;
- Quando configurado em alta disponibilidade, os equipamentos devem ser capazes de trabalhar no modo Stateful-Fail Open, ou seja, deve manter os estados das sessões, em um ambiente configurado com roteamento simétrico ou roteamento assimétrico. Os equipamentos podem operar em modo ativo/ativo ou ativo/passivo;
- Quando configurado em modo Stacked, os equipamentos devem possuir métodos para a não duplicação dos alertas, como por exemplo caso o evento ocorra ao mesmo tempo em ambos os equipamentos, o que possuir o maior número serial será o responsável pelo envio dos alertas para a console;

4. **Características de Detecção de Ataques**

- O equipamento deve suportar análise e decodificação de, no mínimo, 150 (cento e cinquenta) protocolos de rede, entre a camada 2 (Layer-2) e camada 7 (Layer-7) do modelo OSI (Open System Interconnection), para no mínimo: ARP, BOOTP, DCCP, DHCP, DNS, EIGRP, FINGER, FTP, HTTP, HTTPS, ICMP (versão 4 e versão 6), IMAP, IP (versão 4 e versão 6), LDAP, NetBIOS, NFS, POP3, RADIUS, SMTP, SNMP, SSH, RPC, TCP, TELNET, TFTP e UDP;
- O equipamento deve suportar identificação de ataques para protocolos de rede independente das portas de comunicação utilizadas, de forma automática, para no mínimo os protocolos: DCERPC, DNS, FTP, HTTP, IMAP, IRC, POP3, PORTMAPPER, SIP, SMTP, SNMP, SUNRPC e UPNP;
- O equipamento deve suportar tanto análise Stateful Inspection, mantendo o estado das sessões monitoradas, quanto Stateless Inspection;
- O equipamento deve suportar análise de tráfego na direção servidor-cliente, isto é, ataques originados externamente e direcionados à clientes e/ou usuários internos (“Client-side Attacks” ou “Drive-by Attacks”);
- O equipamento deve suportar inspeção de tráfego codificado em Base64, respostas HTTP em pedaços (chunked);
- O equipamento deve suportar a análise de respostas HTTP comprimidas (gzip);
- O equipamento deve suportar a reconstrução de pacotes SMB para impedir evasão de detecção;
- O equipamento deve suportar a análise do cabeçalho X-Forwarded-For para identificar o endereço IP original de um ataque detectado;
- Deve ser capaz de detectar comunicação C&C através das seguintes técnicas:
  - Detectores de callback e descoberta de callback por meio de heurística;
  - Deve permitir configurar a sensibilidade da heurística aplicada;
  - DNS Sinkholing;
  - FastFlux agents;
  - Domain Generation Algorithm.
- Deve ser capaz de criar uma reputação por endpoint, utilizando combinações de endereço IP e porta, e posteriormente utilizar esta reputação para o auxílio no bloqueio a ataques;
- Um mesmo endereço ip pode ter mais de uma reputação, dependendo da porta em uso;
- O equipamento deve suportar mecanismo de criação de perfis de dispositivos, possibilitando a identificação de sistemas operacionais (OS fingerprinting) destes dispositivos de forma passiva (apenas com caracteristicas do trafego), isto é, o equipamento deve suportar tecnologias de criação de perfis de dispositivos, através da análise passiva do tráfego para DHCP, HTTP e pacotes TCP;
- O equipamento deve suportar detecção e bloqueio de ataques direcionados à servidores de aplicação WEB (WEB Application), através de tecnologia heurística, isto é, detecção heurística e bloqueio de ataques SQL Injection;
- Deve ser permitido criar a configuração por path específico;
- Deve ser permitida a personalização de texto da requisição HTTP considerado malicioso;
- O equipamento deve suportar proteção contra negação de serviço direcionado a servidores Web, permitindo:
  - Direção do Tráfego;
  - Quantidade máxima de conexões simultâneas para todos os servidores Web;
  - Possuir proteção contra “Slow-Connection”;
  - Limitar a quantidade de conexões por path;
  - Permitir a detecção do User Agent;
  - Limitar os paths que deverão ser protegidos;
- O equipamento deve suportar obtenção de informações detalhadas sobre ataques de no mínimo:
  - Reputação de arquivo (File Reputation);
  - Reputação de endereço IP (IP Reputation);
  - Reputação de aplicação e protocolo (Application and Protocol Reputation);
  - Localização geográfica (país) tanto do endereço IP de origem quanto de destino.
- O equipamento deve suportar algoritmo de pontuação para relevância de um ataque, baseado no Common Platform Enumeration (CPE), permitindo distinguir quando um ataque for bem-sucedido ou quando um ataque falhar;
- O equipamento deve suportar análise do nível de relevância de um ataque, permitindo uma demonstração de no mínimo 5 (cinco) faixas de relevância, tais como: muito baixa, baixa, média, alta e muito alta;
- O equipamento deve suportar criação de políticas de Firewall para controle de aplicativos, possuindo no mínimo 1.000 (mil) identificações de aplicativos e protocolos (App. ID), permitindo criação de regras de acesso para aplicativos comuns, tais como: Facebook, Yahoo! Instant Messenger e Gmail, entre outros;
- O equipamento deve suportar detecção e bloqueio de shellcodes, utilizando-se tecnologia patenteada, permitindo que instruções de computador sejam examinadas – para a presença de uma instrução de chamada do sistema – e revisadas – para a presença de um conjunto de instruções de “decoder” (descodificador);
- O equipamento deve suportar as categorias de ataques e tipos de ameaças, conforme padrões de mercado e definidos por entidades independentes (Common Weakness Enumeration e Common Attack Pattern Enumeration and Classification), para no mínimo: CAPEC-10, CAPEC-100, CAPEC-112, CAPEC-119, CAPEC-123, CAPEC-14, CAPEC-16, CAPEC-49, CWE-119, CWE-120, CWE-121, CWE-122, CWE-129, CWE-131, CWE-20, CWE-200, CWE-205, CWE-227, CWE-264, CWE-307, CWE-400, CWE-436, CWE-506, CWE-507, CWE-509, CWE-512, CWE-514, CWE-553, CWE-680, CWE-770, CWE-78, CWE-805, CWE-806, CWE-88, CWE-89 e CWE-94;
- Suportar detecção e bloqueio de ataques do tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS) de forma nativa, para no mínimo:
  - Assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1996-26, CA-1997-28, CA-1998-13, CVE-1999-0015, CVE-1999-0016, CVE-1999-0128, CVE-1999-0153, CVE-1999-0258, CVE-1999-0345, CVE-1999-0969, CVE-2000-0305, CVE-2004-0230, CVE-2004-0790, CVE-2005-0688 e CVE-2005-0048;
  - Assinaturas para detecção e bloqueio de atividades de agentes (zumbis) DDoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1999-17, CA-2000-01, CVE-2000-0138, IN-99-07, IN-2000-01 e IN-2000-05;
  - Detecção e bloqueio baseado em modo aprendizagem (learning mode), através de anomalias estatísticas (statistical anomalies) e desequilíbrio de volume de tráfego, que permite utilização de perfil de tráfego tanto de longo quanto de curto prazo, para flood (volume) DoS Attacks, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1996-21, CA-1996-01, CA-1998-01 e CVE-2002-1712;
  - Detecção e bloqueio baseados em SYN Cookie (SYN Proxy), que permita utilização de uma “secret key” juntamente ao ISN (Initial Sequence Number) – nos pacotes de resposta TCP (SYN+ACK) às requisições de conexão TCP (SYN) – como parte integrante do processo de “3-way handshake”.
- O equipamento deve suportar políticas de Firewall camada 3 (Layer 3), que permitam no mínimo:

- Filtros de origem e destino por: país (Geo-localização), nome (DNS), endereço IPv4, bloco de endereços IPv4, rede ou grupo de redes;
- Filtros de aplicação: aplicação, grupo de aplicações, porta de comunicação customizada, serviço ou grupo de serviços;
- Filtro de tempo efetivo (temporizador): período de tempo finito, período de tempo recorrente ou grupo de períodos de tempo recorrente;
- Filtro de resposta: bloqueio (drop) e negação (deny), tanto para stateful quanto para stateless, e ignorar;
- Filtro de Autenticação: solicitar autenticação do usuário por meio de integração com o Active Directory para posterior liberação do tráfego caso a credencial seja válida;

- O equipamento deve suportar limite de conexões, que permite definição de valores “threshold” para limitar o número de conexões que podem ser estabelecidas de/para uma máquina, através de no mínimo:
  - Protocolos;
  - Reputação;
  - Geo-localização;
  - Conexões ativas ou taxa de conexão.
- O equipamento deve suportar proteção de servidores DNS (Domain Name Service) contra ataques – com ou sem a presença de endereços IP forjados (IP Spoofing) – e que permita utilizar-se apenas do protocolo TCP para resolução de nomes (name lookup/resolve), não permitindo a utilização do protocolo UDP para esta finalidade;
- O equipamento deve suportar detecção e bloqueio de tráfego de aplicações Instant Messenger e P2P (Peer-to-Peer), para no mínimo: AOL Instant Messenger, Ares, Azureus, Bearshare, Bittorrent, Blubster, DirectConnect, eDonkey, eMule, Enppy, ICQ, FileNara, Gnucleus, Gnutella, Grokster, Groove, JAP Anonymizer, Kazaa, Limewire, Morpheus, MSN Messenger, Mutella, MyNapster, Mxie, OpenLITO, Overnet, Phex, Piolet, RockItNet, Shareaza, Skype, SoulSeek, Swapper, Xolox, WinMX e Yahoo! Messenger;
- O equipamento deve suportar detecção e bloqueio de ataques através de túneis IPv6, para no mínimo: IPv4 in IPv4, IPv4 in IPv6, IPv6 in IPv4 e IPv6 in IPv6;
- Deve possuir, de maneira nativa, perfis de proteção, para no mínimo:
  - DMZ;
  - Servidor DNS;
  - Servidor de Arquivos;
  - Firewall Interno;
  - Segmento de Rede Interno;
  - Servidor Linux;
  - Servidor de E-mail;
  - Firewall Externo;
  - Servidor Solaris;
  - Servidor Unix;
  - Servidor Web;
  - Servidor Windows e Solaris;
  - Servidores Windows e Unix;
  - Família Windows;
  - Servidores Windows;
  - Servidores Linux .
- Deve permitir a customização de perfis de ataque de forma a melhor atender a necessidade conforme parâmetros desejados pelo administrador da solução.
- A customização do perfil de ataque deve oferecer suporte a, no mínimo, os seguintes sistemas operacionais:
  - Windows 2008, 2012 2016 e 2019;
  - BSD, OpenBSD, FreeBSD e NetBSD;
  - Linux;
  - AIX;
  - iOS e Android;
  - MacOS
- Deve ser possível criar regra para ignorar o tráfego que nativamente ativa uma resposta do IPS, fazendo com que tal condição não gere alerta ou bloqueio por parte do equipamento de proteção;

5. **Características da Análise de Tráfego Criptografado**

- O atendimento técnico a este item se restringe aos equipamentos de Classe 5, 6 e 7;
- O equipamento deve suportar um throughput exclusivo de tráfego criptografado de, no mínimo, 1.5 Gbps utilizando chaves de tamanho 1.024 bits (128-bit ARC4);
- Para o tráfego 100% criptografado, deve suportar, no mínimo 22.000 (vinte e duas mil) conexões por segundo;
- O equipamento deve suportar análise de tráfego criptografado HTTPS (Hyper Transfer Protocol Secure), não sendo permitido utilização de equipamento externo, conforme abaixo:
  - Análise de conexões seguras que utilizem SSL (Secure Sockets Layer) e TLS (Transport Layer Security), para no mínimo: SSL versão 2, SSL versão 3, TLS versão 1.0, TLS versão 1.1 e TLS versão 1.2;
  - Análise de tráfego para comunicação(ões) “inbound” estabelecida(s) com servidores WEB, para no mínimo: Microsoft Internet Information Server (IIS), Apache e IBM WebSphere;
- O equipamento deve permitir importação de no mínimo 1024 (mil e vinte e quatro) certificados em formato PKCS #12 (extensões ".pkcs12", ".p12" ou ".pfx"), com chave(s) privada(s) RSA de 1024-bit e 2048-bit;
- O equipamento deve suportar algoritmos de chaves simétricas, para no mínimo: RC4, DES, 3DES e AES;
- O equipamento deve suportar a inspeção de tráfego no sentido inbound e outbound;
- O equipamento deve suportar funções de “hashing”, para no mínimo: MD5 e SHA-1;

6. **Características de Respostas à Ataques**

- O equipamento deve suportar TCP Reset;
- O equipamento deve suportar ICMP Host Unreachable;
- O equipamento deve suportar bloqueio (drop) de pacotes;
- O equipamento deve suportar aplicação, extensão e remoção de quarentena (IPS Quarantine) sob demanda;
- O equipamento deve suportar captura de pacotes para análise de evidências em formato LIBPCAP(Library for Packet Capture);
- O equipamento deve suportar envio de SNMP para as versões:

- SNMPv2c;
- SNMPv3.

- O equipamento deve suportar envio de e-mail;

7. **Características de Detecção de Ameaças (Malwares) Avançadas**

- O equipamento deve ser capaz de inspecionar, no mínimo, os seguintes protocolos em busca de artefatos maliciosos:
  - HTTP;
  - FTP;
  - SMTP.
- Deve suportar a análise de artefatos com tamanho de até 25 Megabytes;
- Deve suportar a emulação de artefatos maliciosos em memória, não requerendo para tal equipamentos adicionais, permitindo que tal funcionalidade seja executada no próprio equipamento proposto;
- O equipamento deve suportar a análise de até 4094 arquivos de maneira simultânea;
- O mecanismo de análise, presente no equipamento proposto, deve ser capaz de analisar as seguintes categorias de arquivos:
  - Executáveis;
  - Arquivos Office;
  - PDF;
  - Java;
  - Flash;
- A solução deve permitir que o artefato malicioso seja salvo e gerenciado pela console de gestão centralizada do equipamento;
- O equipamento deve suportar tecnologias de detecção e bloqueio de códigos maliciosos e ameaças (malwares), para no mínimo:
  - Mecanismo de lista local de arquivos confiáveis (lista branca), os quais não precisarão ser analisados por serem notoriamente confiáveis;
  - Mecanismo de lista com valores “MD5 Hash” de arquivos que sejam códigos maliciosos e ameaças (malwares) conhecidas e armazenado em uma base de dados local (lista negra).
- Deve ser capaz de informar os arquivos executáveis por conexão dos executaveis que geram tráfego na rede;
- Deve ser capaz de monitorar a saída do tráfego de rede;
- Deverá ser capaz de gerar um conjunto de informações (metadados) de conexões realizadas, como por exemplo:
  - Endereço origem e destino;
  - Protocolo;
  - Porta de origem e destino;
  - Nome do executável;
  - Local no qual o arquivo está armazenado;
  - Nome do executável no disco;
  - Reputação de arquivos executáveis;
  - Pontuação do centro de inteligência do fabricante;
  - Valor MD5;
  - Nome do assinador;
  - Descrição do arquivo.
- O equipamento deve possuir mecanismo de detecção de códigos maliciosos e ameaças (malwares) globais baseado em nuvem e permitindo o uso de reputação de arquivos;
- O equipamento deve possuir mecanismo de detecção de códigos malicioso e ameaças (malwares) em arquivos PDF e Flash, permitindo no mínimo:
  - Extração e análise heurística de JavaScript malicioso em arquivos PDF;
  - Capacidade de análise de arquivos PDF, mesmo quando criptografados;
  - Suporte a formato de arquivos XDP;
  - Suporte a objetos e arquivos embutido em arquivos PDF, tais como: arquivos PDF, arquivos Flash (.cws, .fws, or .zws), arquivos Portable Executable (PE) ou arquivos Microsoft Office.
- O equipamento deve suportar integração nativa com solução de análise de malwares dia zero em sandbox, seja na nuvem ou appliance on-premise, desde que seja do mesmo fabricante.

8. **Console de Gestão Centralizada**

- A solução de gerência deve permitir gerenciamento centralizado do(s) equipamento(s):
  - Equipamento de Proteção Contra Ataques de Rede;
  - Equipamento de Análise de Comportamento de Rede.
- A solução de gerência deve ser fornecida em software ou hardware, para a funcionalidade única, exclusiva e específica de gerenciamento do(s) sensor NGIPS(s), não sendo permitido que o(s) sensor NGIPS(s) operem como solução de gerência;
- A solução de gerência, caso disponibilizada em hardware, deve suportar no mínimo 2 (duas) fontes de energia internas, para Corrente Alterna ou Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz);
- A solução de gerência em hardware deve possuir capacidade de armazenamento do tipo redundante (RAID – Redundant Array of Independent Drives);
- A solução de gerência em hardware deve possuir ao menos 1 (uma) interface 1GigE (Gigabit Ethernet), para cabeamentos Cobre (100Base-TX ou 1000Base-T), onde a interface pode ser fixa ou pode ser fornecida com o respectivo transmissor-receptor, o qual deve ser considerado no momento da elaboração da proposta e, se necessário, fornecido juntamente com o equipamento;
- A solução de gerência deve considerar uma instalação em alta-disponibilidade no modo ativo/passivo, onde:
  - Uma das gerências deve ser primária (ativa);
  - Uma das gerências deve ser secundária (passiva).
- Em caso de falha da gerência primária (ativa), automaticamente a secundária (passiva) deve assumir o gerenciamento centralizado do(s) equipamento(s);
- As configurações devem ser sincronizadas em tempo real entre a gerência primária (ativa) e a gerência secundário (passiva);
- A solução de gerência deve possuir políticas baseadas em assinaturas recomendadas pelo fabricante para bloqueio, as quais são baseadas nas recomendações provenientes de equipe de pesquisa do fabricante.
- A solução de gerência deve suportar console do tipo “Agent-less”, isto é, não há necessidade de instalação de software de console de gerenciamento, sendo necessário compatibilidade com os principais navegadores do mercado, incluindo: Microsoft Internet Explorer, Mozilla Firefox e Google

Chrome;

- A solução de gerência deve suportar atualização de software e firmware do(s) equipamento(s), de forma remota e centralizada, conforme abaixo:
  - Online: automática e/ou manual de conteúdo de segurança e produto através da Internet, podendo ser realizada sem interferência do usuário;
  - Offline: automática e/ou manual de conteúdo de segurança e produto através de pacotes de atualização importados pela gerência, sem conexão com a Internet.
- A solução de gerência deve suportar aplicação de políticas e regras, de forma remota e centralizada, sem afetar a detecção e bloqueio, isto é, o(s) equipamento(s) gerenciado(s) não perderá(ão) capacidade de detecção e bloqueio durante o processo de aplicação de políticas e regras;
- A solução de gerência deve suportar comunicação criptografada com o(s) equipamento(s) de proteção de rede com certificados SHA256;
- A solução de gerência deve permitir envio de registros de eventos através de integração com servidor SYSLOGD.
- A solução de gerência deve suportar integração, através de SNMPv2c ou SNMPv3, com solução de Sistema de Gerenciamento de Rede (NMS – Network Management System), onde deve ser fornecido o(s) respectivo(s) arquivo(s) MIB;
- A solução de gerência deve permitir sincronismo de horário do(s) equipamento(s) através de integração com servidor NTP (Network Time Protocol);
- A console de gerência do IPS deve suportar a informação das, no mínimo, seguintes informações do endpoint afetado pelo evento:
  - Sistema Operacional;
  - Últimos 10 eventos detectados na solução de IPS de Host;
  - Últimos 10 eventos detectados na solução de Antivírus.
- Deve apresentar o executável na estação de rede que gerou um fluxo suspeito;
- Deve ser capaz de apresentar todos os executáveis que geram tráfego de rede em uma estação de trabalho para:
  - Executáveis Responsáveis por tráfego de Saída;
  - Executáveis Responsáveis por tráfego de Entrada.
- A solução de gerência deve suportar operação e armazenamento com Sistema Gerenciador de Banco de Dados Relacional (SGBDR – Relational Database Management System ou RDBMS) que utilize linguagem de pesquisa declarativa SQL (Structured Query Language);
- A solução de gerência deve suportar arquivamento (backup) dos eventos gerados pelo(s) equipamento(s), conforme abaixo:
  - Manual: arquivamento (backup) dos eventos sob-demanda, sendo realizado de forma manual pelo administrador.
  - Automático: arquivamento (backup) dos eventos de forma agendada e automática, sendo previamente configurado pelo administrador.
- A solução de gerência deve permitir tarefas tanto de arquivamento (backup) quanto de restauração (restore) de sua base de dados.
- A solução de gerência deve ser capaz de armazenar 30.000.000 (trinta milhões) de eventos em Sistema Gerenciador de Banco de Dados Relacional (SGBDR – Relational Database Management System ou RDBMS), permitindo uma retenção de até 6 (seis) meses.
- A solução de gerência deve suportar administração, configuração e manutenção de contas de acesso de usuários e administradores através de autenticação:
  - LOCAL: usuários e administradores cadastrados na gerência, permitindo definir políticas de composição de senhas;
  - LDAP: usuários e administradores importados e integrados com o Windows AD (Active Directory);
  - RADIUS: usuários e administradores importados e integrados com servidor RADIUS;
- A solução de gerência deve suportar atribuição de perfis para usuário e administradores, para no mínimo:
  - Administrador;
  - Super usuário;
  - Revisor (Somente leitura).
- A solução de gerência deve permitir monitoração dos recursos alocados do(s) equipamento(s), para no mínimo:
  - Utilização de processamento do(s) equipamento(s);
  - Taxa de transferência do(s) equipamento(s);
  - Taxa de transferência da(s) interface(s) do(s) equipamento(s).
- A solução de gerência deve suportar notificação de falhas de sistema, permitindo envio de informação sobre falha de sistema, conforme abaixo:
  - Através de integração com servidor SYSLOGD;
  - Através de integração com servidor SNMP;
  - Através de integração dom servidor SMTP.
- A solução de gerência deve possuir capacidade de geração de relatórios, não sendo permitido utilização de solução de terceiros ou externa;
- A solução de gerência deve ser capaz de gerar relatórios, de forma remota e centralizada, para os eventos e alertas do(s) equipamento(s), conforme abaixo:
  - Manual: geração de relatórios sob-demanda, sendo realizada de forma manual pelo administrador;
  - Automático: geração de relatórios de forma agendada e automática, sendo previamente configurada pelo administrador.
- A solução de gerência deve permitir exportar relatórios para arquivos HTML e PDF;
- A solução de gerência deve possuir relatórios pré-definidos, para no mínimo:
  - Resumo executivo.
  - Resumo de reputação da origem do ataque.
  - Resumo de reputação do destino do ataque.
  - Ataques de reconhecimento.
  - Análise de tendências.
  - Os 10 (dez) ataques mais detectados.
  - As 10 (dez) ameaças (malwares) mais detectados.
  - As 10 (dez) origens que mais atacaram.
  - Os 10 (dez) destinos que mais foram atacados.
- A solução de gerência deve suportar a execução de relatórios customizados pelo administrador;
- A solução deve permitir o uso de API’s para integração com fabricantes terceiros;
- A solução deve utilizar protocolo open para o intercâmbio de informação de ameaças entre fabricantes terceiros;
- A integração deve permitir que através de um único ponto a informação classificada como ameaça seja replicada para mais de um produto, de maneira automática;
- A integração deve permitir que exista comunicação de consulta com bases abertas de informação de ameaça, a exemplo VirusTotal;

ITEM 05 - LICENÇA DE USO DE SOFTWARE/PROGRAMA DE FILTRAGEM E PROTEÇÃO DE E-MAILS DO TIPO SECURE E-MAIL GATEWAY

1. **Características de Gerais da Solução**

- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- A solução deve permitir a instalação em ambientes tecnológicos distintos, uma vez que será utilizada em redes segregadas e operada de forma independente pelas equipes de TI da CONTRATANTE;
- O sistema utilizado deve possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão; e
- Deve possuir serviço de Suporte Técnico e garantia de atualização durante o período da assinatura contratada.

2. **Requisitos de Arquitetura Tecnológica - Da Plataforma**

- A solução deve possuir controle de caixas postais e fluxo de análise de mensagens/dia ilimitadas, de acordo com os recursos de hardware disponíveis;
- Deve ser uma solução MTA (Mail Transfer Agent) completa com suporte ao protocolo SMTP, que controla o envio e o recebimento de todas as mensagens da empresa, com registro de logs das atividades do MTA;
- A solução deve ser proprietária e a subscrição licenciada para utilização de todos os módulos que compõe a solução para 2350 caixas postais;
- Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, spyware, worms, trojans, spam, phishing, e-mail marketing e conteúdos indesejados;
- Deve possuir módulos de DLP, Criptografia, APT e Archiving compondo a solução;
- Deve permitir alta disponibilidade das funções de filtragem, garantindo que o serviço de correio nunca pare por falha da solução;
- A solução deverá ser implantada em appliance virtual, sendo compativel com os principais sistemas de virtualização do mercado, entre eles:
  - VMWare;
  - Microsoft Hyper-V;
  - Nutanix.

3. **Requisitos de Arquitetura Tecnológica - Pontos Gerais**

- A licença de uso por subscrição do software deve possuir 36 (trinta e seis) meses de atualização do fabricante, compreendendo os seguintes módulos:
  - Atualização das assinaturas de segurança disponibilizadas automaticamente como por exemplo: assinaturas de vírus, malwares e outras ameaças, serviços de reputação de websites, IPs e assinaturas de Websites e aplicativos web;
  - Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante, bem como atualizações de recursos e melhorias dentro da mesma versão;
  - Acesso a base de inteligência global do fabricante para análise online de ameaças;
- Deve analisar as mensagens, no mínimo, por meio dos seguintes métodos:
  - Proteção dinâmica por reputação;
  - Assinaturas de spam;
  - Filtros de Vírus.
- A verificação de vírus, além da técnica tradicional (por assinatura), também deve ser feito através de BigData do fabricante, bem como utilização de método Fuzzy Hash ou Similar para detecção de similaridades e detecção de possível variante de malware;
- Deve possuir dois módulos de antivírus, sendo um do próprio fabricante, já devidamente licenciado para uso simultâneo;
- Deve possuir filtros de anexos;
- Deve possuir filtros de phishing;
- Deve realizar análise heurística;
- Deve realizar análise do cabeçalho, corpo e anexo das mensagens;
- Deve realizar o e-mail bounce;
- Deve possuir dicionários pré-definidos e customizados com palavras e expressões regulares;
- Já deve vir com dicionários pré-estabelecidos, para posterior utilização, tais como:
  - Número de cartão de crédito;
  - CNPJ;
  - RG e CPF.
- Deve possuir mecanismo de backup e recuperação da configuração da solução;
- Deve possuir capacidade de envio de backup via FTP e SFTP, sendo configurado diretamente na interface gráfica da solução (sem necessidade de qualquer configuração em linha de comando);
- Os manuais necessários à instalação e administração da solução, devem constar no seguinte idioma: Português do Brasil ou Inglês;
- A interface de administração do sistema deve ter suporte a no mínimo um dos seguintes idiomas:
  - Português do Brasil;
  - Inglês.
- A interface de quarentena do usuário deve suportar o idioma Português do Brasil;
- Deve possuir banco de dados relacional para armazenamento dos registros de acesso, logs de sistema e configurações. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante. Não serão aceitas soluções baseadas em armazenamento de Logs em formato Texto;
- Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino;
- Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;
- Ter a capacidade de processar o tráfego de entrada e de saída de mensagens no mesmo appliance, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido;
- A solução deve ser capaz de efetuar a saída de e-mails indicando um IP específico para a saída de mensagens, isto é, possuir a capacidade de redirecionar as mensagens de saída por IP’s diferentes para cada domínio cadastrado no appliance se o administrador assim desejar;

- A solução deve permitir criação de regras por:
  - Grupos de usuários;
  - Domínios;
  - Range de IP;
  - IP/Rede;
  - Remetentes específicos;
  - Destinatários específicos;
  - Grupos de LDAP.
- A solução deve tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;
- Deve ter a possibilidade de permitir relay autenticado para clientes externos da corporação;
- Deve possuir ferramenta de auditoria de e-mail, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”;
- A console de gerenciamento deve acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:
  - Administração centralizada de todas as regras e filtros integrantes da solução;
  - Status da versão das assinaturas do antivírus em uso;
  - Controle de acesso de usuários, com diferentes privilégios de configuração;
  - Criação de relatórios, gráficos e estatisticas, com suporte a múltiplos domínios;
  - Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.
- Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;
- Deve ser capaz de utilizar os protocolos de transferência de arquivos SCP e FTP;
- Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF;
- Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:
  - Conteúdo do anexo;
  - Mime-Type do anexo;
  - Extensão do anexo;
  - Nome completo do anexo;
  - Nome parcial do anexo;
  - Expressão regular;
  - Tamanho do anexo;
  - Anexos compactados com senha;
  - Quantidade de níveis de compactação no mesmo anexo.
- Deve possuir um sistema de Disaster e Recover ao qual é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente;
- Possuir a função de abertura de relay automático para empresas que usam Microsoft Office 365, sem necessidade de cadastro de IP´s ou DNS da Microsoft para abertura de relay;
- Deve possuir sistema de diagnóstico via interface WEB, com no mínimo a execução dos seguintes testes:
  - Teste de Conectividade TCP – Informando o Host e a Porta a serem testados;
  - Teste de Conectividade ICMP – Informando o Host a ser testado;
  - Teste de DNS – Informando o Host ou o Domínio a serem testados;
  - Teste de Envio de E-mail;
  - Teste de Lookup de E-mail via LDAP;
  - Teste de Conectividade com o fabricante (para isso, testa-se as portas necessárias de comunicação junto ao fabricante);
  - Teste de TRACEROUTE;
  - Teste de DNS Reverso;
  - Teste de SPF, para checar se tem registro para um determinado domínio;
  - Teste de DKIM, para checar se tem registro para um domínio;
  - Teste de DMARC, para checar se tem registro para um domínio;
  - Teste de portas de Saída utilizadas pelo sistema.
- Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:
  - Serviço de antivírus;
  - Serviço de MTA;
  - Serviço de Banco de Dados;
  - Serviço de SMNP.
- Deve permitir a instalação de agentes/plug-ins (tanto no appliance de gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, com no mínimo:
  - Zabbix;
  - Nagios.

4. **Da Alta Disponibilidade**

- A solução deve suportar Cluster de Alta Disponibilidade na forma de Cluster Ativo-Ativo ou Load Balance através do registro MX e/ou sistemas de balanceamento proprietário, assegurando as funções de filtragem que o serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução;
- Deve permitir a configuração em Cluster com appliances fisicos ou virtualizados em DataCenters distintos;
- O cluster deve poder ser formado por appliances fisicos e appliaces virtuais de forma mista;
- Administração centralizada de múltiplos nós de filtragem em uma única interface web, independente se estiver em modo cluster de alta disponibilidade ou load balance de forma que o gerenciamento e a replicação de políticas do cluster também seja feita de forma centralizada;
- A administração de todo cluster deve ser feita através de um único IP de destino, não sendo permitido a gestão de regras de forma descentralizada;
- Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único Virtual IP;

5. **Do Gerenciamento**

- O acesso à interface de administração deve possuir diferentes níveis de permissionamento, de forma granular, permitindo que sejam configurados perfis diferentes, por endereços de e-mail e domínio permitidos;

- O sistema deve permitir criar usuário do tipo Auditor que tenha permissão de visualizar através da interface web os e-mails que forem colocados para auditoria, sendo possível definir quais endereços de e-mails ou domínios ele poderá auditar;
- O sistema deve possuir ainda, no mínimo, os perfis pré-definidos:
  - Administrador: Com acesso total às configurações da solução;
  - Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;
  - Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;
  - Operador: Com acesso à administração da quarentena e gerenciamento da "Black e White List";
  - Usuário: Possui a capacidade de administrar sua "Black e White List", individualmente, bem como sua área de quarentena individual.
- Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:
  - E-mails;
  - Domínios;
  - IP's;
  - Range de IP;
  - Expressão Regular;
  - Usuários;
  - Listas de distribuição;
  - Grupos de LDAP.

6. **Alertas e Logs da Solução**

- A solução deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso;
- A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável;
- Possuir registro de log de TODAS as ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso para obtenção do mesmo, não sendo necessário acionamento da fabricante da solução;
- Possuir mecanismo de alerta por e-mail quando houver nova atualização do sistema e sobre o status do processo de atualizações;
- Deve possuir capacidade de envio dos logs de um nó específico ou de todo o cluster para um servidor de syslog ou de SIEM. Também deve ser possível selecionar os logs a serem enviados, no mínimo, para as opções abaixo:
  - Emergency;
  - Alert;
  - Critical;
  - Error;
  - Warning;
  - Notice;
  - Informational;
  - Debug.
- Deve ser possível enviar alertas por e-mail e por snmp caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio dos alertas devem ser, no mínimo:
  - Espaço em disco;
  - Filas de e-mail;
  - Memória;
  - Processador;
  - Serviço de Filtragem;
  - Atualização do sistema de segurança;
  - Antivirus e Anti-spam;
  - Ponto de acesso indisponível.

7. **Das Funcionalidades para o usuário final**

- Possuir interface web de administração segura HTTPS para que cada usuário final possa administrar suas opções pessoais e sua quarentena, sem que estas opções interfiram na filtragem dos demais usuários;
- A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo os seguintes idiomas:
  - Português do Brasil.
- O usuário final deve ser capaz de incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails;
- O usuário final deve ser capaz de visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que as mesmas sejam consideradas somente como "possível spam" ou "spam";
- O usuário final deve ser capaz de solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer, o qual não permita que o usuário final a libere;
- O usuário deverá ser capaz de selecionar qual o idioma utilizado sua interface, sendo no mínimo os seguintes idiomas:
  - Português do Brasil.

8. **Da Quarentena**

- Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio appliance, sem necessidade de nenhum hardware adicional;
- Deve possibilitar a gestão de quarentena pelos administrados de forma que o mesmo possa visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host destinatário, a mensagem original, tamanho da mensagem original e permitindo no mínimo as ações liberar e/ou excluir;
- Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;
- A interface deve permitir identificar quais Regras do Modulo de Anti-Spam foram ativadas e qual sua pontuação, afim de permitir ao administrador a elaboração de regras granulares;
- A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos;
- Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas no próprio appliance, seja ele virtual ou fisico.
- Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena;
- Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens;

- O sistema de quarentena de e-mails deve criptografar automaticamente as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails armazenados em quarentena, assim aumentando a confiabilidade e segurança da solução;
- Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, por exemplo: manter as mensagens das últimas 72 horas, dessa forma ao ultrapassar esse limite, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;
- O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo "indeterminado";
- Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena, por exemplo limitar uma quarentena a 100GB, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;
- O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela;
- Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

9. **Dos Usuários e Grupos**

- Possuir integração com serviço de diretórios LDAP, Microsoft Active Directory para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário ("Directory Harvest Attack");
- Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory;
- Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas;
- Permitir a utilização de mais de um servidor de LDAP ou Microsoft Active Directory ao mesmo tempo. Caso ocorra indisponibilidade do servidor primário a autenticação dos usuários deverá ocorrer normalmente no outro servidor configurado;
- Integração nativa com o Microsoft Exchange;
- Possibilitar a customização de regras e políticas por usuários ou grupos;
- A solução deverá permitir a configuração do intervalo de sincronismo com o serviço de diretório;
- Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de antivírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

10. **Dos Relatórios**

- Deve permitir a geração de relatórios de todos os appliances de um cluster de forma centralizada através de uma única interface web no console de gerenciamento;
- Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;
- Deve ser capaz de gerar relatórios por data ou por um intervalo de tempo específico;
- Deve ser possível configurar um período para a retenção dos dados utilizados para geração dos relatórios;
- Capacidade de criar relatórios contendo no mínimo as seguintes informações:
  - Sumário de mensagens;
  - Quantidade de mensagens processadas;
  - Relatório de Volume de Mensagens por Data;
  - Principais origens de spam por domínio, endereço de e-mail;
  - Principais destinos de spam por domínio, endereço de e-mail;
  - Principais origens de vírus;
  - Principais fontes de ataque;
  - Relatório de Top E-mail Relays;
  - Relatório de Top Remetentes por Quantidade;
  - Relatório de Top Remetentes por Volume;
  - Relatório de Top Destinatário por Quantidade;
  - Relatório de Top Destinatário por Volume
  - Estatisticas da quarentena;
  - Conexões completadas X bloqueadas;
  - Relatório de tráfego;
  - Principais destinatários de Spam;
  - Principais destinatários de e-mail;
  - Top Ataques por fraude de e-mail / tentativa de spoof.
- Permitir filtros de relatórios com definição de origem e destinos específico;
- Possuir relatórios estatisticos de conexões, ameaças, quarentena e SPAM;
- Deve apresentar estatisticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
- Os relatórios, no mínimo, devem poder ser filtrados por:
  - Período de tempo;
  - Ponto de Filtragem que o e-mail passou
  - De;
  - Para;
  - Qual a classificação que a mensagem atingiu, dentre eles no mínimo:
    - DLP;
    - Provável SPAM;
    - SPAM;
    - Vírus;
    - Conteúdo Bloqueado;
    - Whitelist;
    - Blacklist;
    - Tamanho Excedido;
    - Phishing.
  - Relatório para um único usuário ou Domínio.
  - Rastreamento das Mensagens.
- Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando);

- O rastreamento deve ser possível através de qualquer um dos seguintes campos:
  - ID da mensagem;
  - E-mail do Remente;
  - E-mail do Destinatário;
  - Domínio do Remetente;
  - Domínio do Destinatário;
  - Assunto da mensagem;
  - Nome do anexo;
  - Palavra contida no conteúdo do corpo da mensagem;
  - IP de Origem da mensagem;
  - Tamanho da mensagem;
  - Regra de SPAM;
  - Regra de DLP;
  - Se a mensagem foi entregue ou não;
  - Regras personalizadas aplicadas na mensagem;
  - Nome da ameaça encontrada.
- A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
  - Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando como filtro o assunto, o remetente, o destinatário, regra de bloqueio, conteúdo do corpo da mensagem, data, status, hora de entrega da mensagem, permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”;
  - O rastreamento deve ser a partir de uma única interface de gerenciamento independente de qual appliance filtrou a mensagem, não sendo aceito pesquisa via linha de comando;
  - O rastreamento deverá ter a opção de ser efetuado de todos os pontos de filtragem, sem a obrigatoriedade de separação de um único ponto de filtragem por vez;
  - Deve apresentar como resultado as seguintes informações:
    - Remetente da mensagem;
    - Destinatários da mensagem;
    - Servidor de origem;
    - Se foi armazenada em quarentena;
    - Se continha vírus;
    - A regra que atuou;
    - O servidor de origem;
    - O tamanho da mensagem;
    - Se foi entregue ou não;
    - Qual ponto de filtragem utilizado (qual appliance processou a mensagem).
  - No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue;
  - Se o e-mail tiver sido bloqueado por ser considerado spam ou possível spam, o log deve apresentar os filtros aplicados, bem como a pontuação apresentada por cada filtro e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador);
  - Deve ser capaz de visualizar a fila de e-mails em tempo real, bem como o sentido do e-mail na fila (se é fila de entrada ou saída), indicando total de e-mails na fila de saída, total de e-mails na fila de entrada e total de e-mails com erros na entrega;
  - Rastrear e-mails a partir de uma determinada ameaça;
  - Apresentar na interface gráfica as fontes de ataque e, através delas, apresentar quais e-mails foram recebidos, originários dessa fonte de ataque;

11. **Proteção Contra Ataques Direcionados**

- A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service);
- Ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com Suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS/ SSL, permitindo configurar domínios onde o TLS é mandatório;
- A solução deverá possuir a capacidade de executar as seguintes ações:
  - Limitar o número de conexões TCP permitidas através de um valor configurável;
  - Rejeitar a conexão SMTP que se caracterize como "flooding".
- Deve ser capaz de efetuar a filtragem do trafego de correio eletrônico bloqueando a entrada e saída de:
  - Vírus;
  - Spyware;
  - Worms;
  - Trojans;
  - Spam;
  - Phishing;
  - E-mail Marketing, ou qualquer outra forma de ameaça virtual.
- Deve possuir controle total da comunicação permitindo restringir:
  - IP reverso mal configurado;
  - Domínios inexistentes;
- Deve permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.
- Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador;
- Permitir criação de políticas customizadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;
- Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:
  - Aceitar;
  - Colocar em quarentena;
  - Inserir tag personalizada no assunto;
  - Marcar o cabeçalho.
- A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:
  - Alterar o assunto da mensagem;
  - Adicionar cabeçalhos para rastreamento;
  - Descartar a mensagem;

- Colocar em uma determinada área de quarentena definida pelo administrador.

- Deve permitir a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, inglês e espanhol;
- Deve permitir a criação de regras baseadas por país;
- Possuir a capacidade de criar filtros personalizados usando expressões regulares;
- Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;
- Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);
- Capacidade de limitar o número máximo de mensagens enviadas por remetente a cada hora, com opção de bloqueio automático do remetente, caso esse limite seja excedido;
- Permite criar regras customizáveis contra spammers, possibilitando um controle avançado em todo conteúdo do e-mail efetuando buscas por Expressões Regulares presentes em todo conteúdo do e-mail (SMTP HEADER, BODY, URL, ANEXOS), sendo possível criar regras compostas utilizando os operadores lógicos “E” e “OU”;
- O fabricante da solução deve possuir consulta de reputação de IP de remetentes de e-mail. Esta consulta deve retornar os dados do remetente, com informações referentes à:
  - IP reverso e localização;
  - Registro em blacklists mundiais;
  - Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.
- Capacidade de efetuar consultas externas ou internas na própria console da solução, para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de spams e phishings recebidos e outros tipos de ameaças;
- Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de e-mail;
- Deve possuir suporte ao bloqueio de conexões de e-mails nocivos durante o diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento do appliance, em especial baseado em lista local de bloqueio de conexão por: IP, e-mail, domínio, RBL’s e SPF;
- Deve permitir que o administrador do sistema cadastre novas RBL’s para serem utilizadas a nível de conexão SMTP;
- Deve ter capacidade de proteção a spoofing de e-mail (tanto Spoofing de e-mails na entrada – quando o hacker utiliza o domínio do órgão como remetente, como Spoofing de e-mails na saída – quando tem algum e-mail de saída que não esteja com o domínio do órgão como remetente);
- Possuir capacidade de criar cotas de envio e recebimento de e-mails em um prazo determinado de tempo, limitando o fluxo e prevenindo ataque do tipo DOS ou distribuição de spam através de um computador infectado na rede interna;
- Possuir mecanismo de “Spam Throttling” permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;
- Deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem;
- Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
- Possuir controle de “Outbreak”, penalizando o remetente por um tempo configurável pelo administrador ao detectar:
  - Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
  - Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
  - Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
- Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:
  - Fontes de ataques;
  - Ameaças encontradas.

12. **Da Proteção Contra Spam e Phishing**

- Possuir filtro de anti-spam para detecção de spams usando no mínimo as seguintes tecnologias:
  - FingerPrint: Filtro por assinatura de spam;
  - Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;
  - Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);
  - Análise de Imagens: Filtragem de spam em imagens;
  - Filtro de URL: Filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;
- Permitir ao administrador definir filtros por URL através de categorias, divididas por assunto, sendo possível definir uma pontuação. Categorias mínimas contidas na solução:
  - Conteúdo pornográfico;
  - Abuso infantil;
  - Redes sociais;
  - Racismo e ódio;
  - Pesquisa de empregos;
  - Streaming de áudio;
  - Streaming de vídeo;
  - Esportes;
  - Noticias;
  - Compras Online.
- Deve possuir tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;
- Deve possuir tecnologia capaz de avaliar um link "URL" recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivos (Tipo Zip, EXE, RAR, etc), na tentativa de enganar o usuário, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;
- Deve permitir que o administrador cadastre novas RBL’s a serem utilizadas a nível de cálculo de SPAM. O administrador deverá ter a autonomia para selecionar quais RBL’s serão utilizadas a nível de conexão SMTP e quais serão utilizadas a nível de cálculo de SPAM;
- Possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:
  - Recurso de Grey List;
  - Recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para “fail” e “soG fail”;
  - Recurso de checagem por DMARC;
  - Recurso de checagem por assinatura DKIM;

- Recurso de checagem de DNS Reverso;
- Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;
- Análise de reputação de IP;
- Reputação de Mensagens;
- Filtros de URL;
- Filtro de anti-phishing;
- Consulta de RBL´s (real-time blackhole list);
- Machine Learning.

- Deve permitir classificar a reputação de novas origens de spam com tecnologia de classificação dinâmica. O sistema de reputação deve utilizar dados de redes globais de monitoramento de tráfego web e de e-mail, não restringindo ao fluxo de mensagens do ambiente instalado;
- Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:
  - Origens das mensagens;
  - Destino das mensagens;
  - Domínios;
  - Endereços de e-mails;
  - Expressões regulares (dicionário de palavras);
  - Fluxo;
  - Quantidade de mensagens;
  - Tamanho de anexo;
  - Número máximo de destinatários em uma única mensagem;
  - Tipo de arquivos em anexo;
  - Extensões de arquivos em anexo, identificados por Mime-Type;
  - Anexos criptografados;
  - Anexos compactados;
  - Níveis de compactação dos arquivos anexos;
  - Quantidade de anexos na mensagem;
  - Conteúdo HTML no corpo da mensagem.
- Possuir mecanismo de análise de conteúdo HTML no corpo da mensagem, permitindo ao administrador desarmar as tags HTML possivelmente perigosas e bloquear as mensagens, possuindo no mínimo a identificação das seguintes Tags:
  - “<form>”;
  - “<script>”;
  - “<iframe>”.
- Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas Confiáveis e/ou Spams, permitindo ao administrador configurar nesses casos as seguintes ações:
  - Entregar direto o e-mail;
  - Colocar em quarentena;
  - Remover mensagem;
  - Auditar mensagem;
  - Encaminhar a mensagem;
  - Notificar o destinatário;
  - Adicionar header na mensagem;
  - Transformar HTML em texto simples.
- Possuir sistema de detecção de ataque de diretórios (DHA – Directory Harvest Attack), capaz de recusar novas conexões SMTP de uma fonte emissora, caso ela tenha enviado, em um período de tempo, mensagens a usuários inválidos/inexistentes no domínio;
- Deve permitir a criação de regras para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos da contratante, permitindo definir no mínimo: país de origem, endereço de domínio, IP do remetente; campo header da mensagem, conteúdo no corpo da mensagem e url contidas no e-mail;
- A solução deve permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório LDAP ou Microsoft Active Directory, que esteja integrado com a solução, administre suas próprias mensagens categorizadas como spam;
- Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory;
- Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o dialogo SMTP (tratar Non-Delivery Report Attack);
- Possuir proteção contra bounce e-mail attack através “Bounce Address Tag Verification”;
- Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas;
- Deve permitir que mensagens de Falso Negativo sejam reportadas através da interface gráfica para o laboratório de pesquisa do fabricante ou oferecer um caminho para que mensagens de Falso Negativo sejam reportadas diretamente ao laboratório do fabricante;
- Deve possuir mecanismo que permita a adição de Cabeçalho de identificação da classificação das mensagens como SPAM, a fim de integrar com sistemas de correio eletrônicos como, no mínimo:
  - Microsoft Exchange.

13. **Da Proteção Contra Vírus**

- Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente;
- Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail);
- Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores:
  - .rar;
  - .zip;
  - .tar;
  - .arj;
  - .cab;
  - .lha;
  - .exe;
  - .lzh;
  - .tgz;
  - gzip,
- A solução deve possuir, no mínimo, duas engines de antivírus e antimalware já integrados na solução sem custo adicional;
- Proteção contra Vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional:

- Dia-zero (zero-day);
- Vírus outbreak;
- Hora-zero (Zero-hour);
- Targeted Attack Protection;
- APT - advanced persistent threat.

- Tomar no mínimo as seguintes ações:
  - Descartar a mensagem;
  - Colocar em uma determinada área da quarentena definida pelo administrador.

14. **Das Notificações de Quarentena Individual do Usuário**

- A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (digest) em períodos de tempo pré-configuráveis por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste digest, dispensando a instalação de agentes e acesso a quarentena individual do usuário;
- Grupos diferentes de usuários devem poder receber a notificação em horários diferentes;
- O digest deve ser enviado em Língua portuguesa do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários;
- Deve ser possível a customização do digest com as seguintes características alteráveis:
  - E-mail de origem;
  - Título/Assunto do e-mail;
  - Mensagem do digest, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor;
  - Logomarca do digest;
- O digest deve permitir ao usuário final tomar no mínimo as ações de:
  - Liberar uma mensagem bloqueada;
  - Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens do mesmo já sejam barradas;
  - Marcar o remetente como confiável (whitelist), para que as futuras mensagens do mesmo não sejam pontuadas como spam;
  - Reportar o bloqueio indevido;
  - Solicitar envio de novo resumo;
  - Acessar sua área de quarentena.
- Deve permitir que o administrador escolha qual quarentena a ser incluída no digest do usuário final, por exemplo incluir no digest os e- mails quarentenados que foram considerados conteúdos maliciosos (VÍRUS);
- A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final selecionar, no mínimo:
  - Liberar e-mail;
  - Reportar Falso Positivo;
  - Incluir o remetente do e-mail em blacklist individual (do próprio usuário);
  - Incluir o remetente do e-mail em whitelist individual (do próprio usuário);
  - Visualizar o e-mail.

15. **Do Disclaimer**

- Deve ter a capacidade de incluir “disclaimers” nas mensagens enviadas;
- A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP ou Microsoft Active Directoy;
- A solução deverá suportar a configuração dos “disclaimers” em formato html e texto.

16. **Da Prevenção Roubo de Informações (DLP) e Conformidade**

- Deve possuir módulo DLP (Data Loss Prevention) do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;
- O módulo de DLP deve analisar todo conteúdo da mensagem a fim de garantir a confiabilidade das mensagens que saem da empresa, permitindo ao administrador configurar diversas ações a fim de restringir, controlar ou auditar as mensagens e informações sensíveis da empresa;
- Deve permitir criar regras de conformidade “Auditoria/Aderência” através de filtros avançados de análise da mensagem, permitindo identificar através de Dicionários (Conjunto de Palavras e Expressões Regulares) personalizados pelo administrador ou já existentes na ferramenta, dentre eles:
  - Identificação de CPF;
  - Número de cartão de crédito;
  - CNPJ.
  - As regras de conformidade podem ser criadas utilizando os termos dos dicionários definidos e que estejam nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:
    - Cabeçalho;
    - URL (contidas no e-mail);
    - Corpo do e-mail;
    - Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT.
- Permitir ao administrador criar regras de conformidade para arquivos criptografados, possibilitando ao administrador configurar a ação a ser tomada quando um anexo criptografado é identificado. A ferramenta deve ter no mínimo três algoritmos de detecção: Mecanismo Heurístico, Myme-Type e Extensão;
- Todos os itens do DLP devem permitir configurações através de regras que permitam ao administrador definir, no mínimo, as seguintes ações:
  - Entregar a mensagem;
  - Não entregar a mensagem;
  - Armazenar a mensagem para auditoria;
  - Notificar remetente e destinatário da mensagem;
  - Encaminhar a mensagem para outro destinatário.
- Todos os itens do DLP devem permitir configurações que permitam ao administrador criar regras complexas através de operadores lógicos “E” e “OU”;
- Deve permitir ao administrador gerar notificação (se assim desejar) ao remetente do e-mail, indicando que o e-mail enviado não condiz com as normas da empresa. Essa notificação poderá ser customizada de acordo com a necessidade do administrador.

17. **Da Criptografia de E-mail**

- Deve possuir módulo de criptografia do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;
- A criptografia deve atuar na saída de e-mails trabalhando de maneira transparente ao usuário final, sem a necessidade de plugins, agentes ou outro tipo de software, com uma interface para o destinatário das mensagens customizável pelo administrador;
- A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional;
- Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base no mínimo em:
  - Assunto;
  - Destinatário;
  - E-mail do Remetente;
  - Nome do Anexo.
- A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente;
- Deve impossibilitar o uso de Cache de Browser para acesso as mensagens criptografadas;
- Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada;
- Deve possibilitar ao administrador indicar se o destinatário poderá responder o e-mail;
- Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o e-mail.

18. **Da proteção Contra Ataques Dirigidos (TAP)**

- Deverá prover proteção contra ataques dirigidos tais como:
  - Spear-phishing;
  - Ataques Zero-Day;
  - Ameaças avançadas persistentes (APTs).
- Deve possuir técnica para construção de modelos estatisticos com Big Data;
- Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:
  - Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;
  - Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;
  - Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.
- Possuir, dentro da solução, um dashboard do módulo de Segurança contra-ataques dirigidos;
- O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:
  - Detecção - A análise de e-mail deve verificar variáveis em tempo real incluindo as propriedades da mensagem, bem como, o histórico de e-mail do destinatário para identificar anomalias que indiquem uma ameaça potencial;
  - Proteção - Deve assegurar que links para URLs suspeitas são dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto o serviço verifica se o destino é seguro;
  - Ação - Deve demonstrar aos administradores e gestores de segurança em tempo real e de forma interativa uma visão dos ataques sofridos e das ameaças que possam sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle online.
- Não será aceita solução baseada apenas em reputação de URL;
- A solução deve conter engine para detecção de Anomalias, não podendo se limitar a analise com definições baseadas em ataques já conhecidos;
- Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:
  - E-mail do Destinatário;
  - E-mail do Remetente;
  - Domínio de Origem;
  - Domínio de Destino;
  - IP/Rede;
  - Range de IP;
  - Expressão Regular;
  - Usuários;
  - Listas de distribuição;
  - Grupo de LDAP.
- A proteção de URL deverá reescrever os links do e-mail e a cada clique o sistema deverá analisar a URL e somente depois de passar por todos os testes, sendo constatado que não é malicioso, deve redirecionar para a URL original. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site deverá ser bloqueado para acesso;
- O sistema deverá ser capaz de varrer anexos, com no mínimo, tipos PDF, arquivos em Flash para payloads maliciosos e Microsoft office;
- Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para descartar e salvar uma cópia na quarentena;
- Deve possuir tecnologia SandBox local do mesmo fabricante ou em nuvem do próprio fabricante no Brasil, desde que esteja em conformidade com todas as regras da legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais);
- Deverá ser capaz de efetuar a verificação da reputação de anexos e caso a reputação do anexo não conste no banco de dados, a solução deverá ter a opção de enviar automaticamente o anexo para a nuvem do fabricante para análise em tempo real em sistema de SandBox do próprio fabricante, caso o administrador opte por este serviço. Este sistema de SandBox deve conter tecnologia de detecção usando “Analise Comportamental” do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas;
- A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita e os usuários que ignoraram através do Dashboard;
- A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP e URL's que comecem com “www” independente do protocolo;
- A solução deverá permitir que o administrador configure o sistema de proteção URL para que reescreva todas as mensagens que contiverem URL e envie ao sandbox para testes garantindo um alto nível de segurança;
- A solução deverá prover lista de exceções de URL para que não sejam reescritas;
- No Dashboard da solução deve ser possível:
  - Exibir o número de cliques em cada ameaça;
  - Exibir qual usuário clicou na URL detectada como ameaça;
  - Exibir informações atualizadas sobre as ameaças detectadas;
  - Exibir a classificação da mensagem;

- Exibir status atualizado e detalhado sobre as ameaça com no mínimo com as seguintes informações:
  - Clicado – Número de vezes que uma URL reescrita foi clicada por um usuário, inclusive se a mensagem for encaminhada para outro usuário e também for clicada;
  - Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso;
  - Permitida – Número de vezes que o modulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.
- Exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada;
- Filtrar uma URL em um campo de busca para analisar todas as ocorrências com aquela URL, bem como verificar o status atual dela e preview da página web;

- Possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta;
- Possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta;
- Possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta;
- Filtrar um IP em um campo de busca para analisar todas as ocorrências com aquele IP, bem como verificar o status atual dele e preview da página web;
- Disponibilizar sistema de coleta (report) de amostra do IP para análise da engenharia do fabricante;
- Ao administrador enviar uma amostra de um arquivo para análise e visualizar o retorno de todas as ocorrências encontradas para esse arquivo;
- A ferramenta de segurança contra ataques dirigidos, deve possuir o sistema colaborativo, ao qual o administrador poderá configurar que o usuário final possa indicar liberação e bloqueio de URL's, mesmo analisados pelo sistema e dessa forma reportando falsos positivos e falsos negativos. Deve prover também um Dashboard onde o Administrador poderá verificar todos reports enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo;
- Deve possuir módulo de CDR "Content Disarm and Reconstruction", que quando ativado irá remover conteúdos possivelmente perigosos, em no mínimo para os seguintes tipos:
  - JavaScript;
  - Links;
  - Executáveis;
  - VB Script.
- De dentro de documentos, em no mínimo para os seguintes tipos:
  - pdf;
  - doc;
  - docx;
  - ppt;
  - pptx;
  - xls;
  - xlsx.
- Deve possuir capacidade de ignorar reescrita de algumas URL's e não envio de arquivos para análise no SandBox do fabricante;
- O SandBox do fabricante deve ter a capacidade de analisar arquivos, mesmo que estejam inseridos em arquivos compactados, do tipo:
  - .swf;
  - .pdf;
  - .doc;
  - .xls;
  - .xlsx;
  - .ppt;
  - .ppt;
  - .pptx;
  - .rtf.
- Deve ter a opção de não fazer reescrita de URL's em casos de mensagens oriundas de determinados países, por exemplo: Mensagens oriundas da China, Austrália e Belize;
- Deve poder desativar a reescrita de URL's se a mensagem atingir uma pontuação mínima de SPAM definida pelo administrador;
- Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista de bloqueio (Blacklist) no sistema de detecção;
- Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista segura (Whitelist) no sistema de detecção.

19. **Do Sistema de Proteção a Fraude de E-mail**

- A solução deverá ter a capacidade de detectar domínios recém registrados (tempo considerado como recém adquirido deverá ser configurável pelo administrador) e indicar o que deve ser feito neste caso:
  - Pontuar;
  - Ignorar;
  - Bloquear.
- Deve possuir capacidade de detecção de Spoofing de e-mails externos, isto é, ter a capacidade de comparar o domínio do cabeçalho do e-mail (Header do E-mail/Envelope SMTP), com o domínio apresentado como remetente para o usuário final (Cabeçalho From) e indicar o que deve ser feito se forem diferentes:
  - Pontuar;
  - Ignorar;
  - Bloquear.
- O sistema deve possuir a opção de configurar regras para detectar e-mails que estejam utilizando ataques do tipo Look-A-Like Domain, isto é, detectar e-mails com domínios similares aos domínios utilizados pelo órgão;
- Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos tais como Google, Yahoo, Hotmail, etc, para serem usados em regras personalizadas de filtragem;
- Nativamente deve possuir sistema de detecção de e-mails externos (e-mails de entrada) que tentem utilizar o domínio da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

20. **Do Archiving e Auditoria de E-mail**

- O sistema deve permitir o armazenamento de cópia da mensagem original;

- O sistema deverá possuir uma interface de gerenciamento web via HTTPS, onde será possível administrar toda solução;
- Será permitido soluções de gerenciamento unificadas com a “Solução de Segurança para Serviço de E-mail” ou soluções de terceiros desde que devidamente licenciadas e passíveis de integração com a “Solução de Segurança para Serviço de E-mail” e com o sistema de correio Eletrônico Microsoft Exchange;
- O sistema deve permitir o armazenamento de todas as mensagens de entrada e de saída da rede de dados da contratante, bem como ter a capacidade de armazenar os e-mails internos trafegados dentro da empresa;
- Deve permitir a integração com sistema de correio Microsoft Exchange para o armazenamento dos e-mails trafegados no domínio interno da empresa. Esta integração pode ser feita através de uma conta especifica no Exchange usando o protocolo POP3 ou através do uso de conectores para o envio e recebimento das mensagens utilizando protocolo SMTP/TLS;
- A solução deve permitir integração com a “Solução de Segurança para Serviço de E-mail” através do protocolo SMTP/TLS para armazenamento das mensagens ou caso a solução seja do mesmo fabricante será permitido integração através de protocolo proprietário da solução;
- O sistema deve permitir que o administrador configure o tempo de armazenamento e o “rotacionamento” automático das mensagens utilizando pelo menos os seguintes critérios:
  - Por número de dias;
  - Por número de meses;
  - Por número de anos;
  - Por volume armazenamento de dados em MB/GB.
- O sistema deve ser dimensionado (hardware) para permitir o armazenamento de todas as mensagens por um período mínimo de 1 ano;
- A solução deve permitir o armazenamento das mensagens em disco Interno da solução e também possibilitar a integração com sistemas de armazenamentos externos para expansão, com pelo menos um dos seguintes tipos: HBA, Fibre Channel, ISCSI ou Storage Externo NAS.
- A solução deve permitir a realização de backup dos dados para um sistema de backup externo. Serão aceitas soluções que permitam exportar os dados para um compartilhamento externo ou que permitam a instalação de agente de backup;
- O sistema deve possuir console de administração possibilitando a consulta das mensagens armazenadas, efetuando busca por pelo menos os seguintes campos:
  - ID da mensagem;
  - IP de Origem da mensagem;
  - Assunto do e-mail;
  - De;
  - Para;
  - Palavras contidas no corpo da mensagem;
  - Nome de anexo;
  - Data;
  - Tamanho da mensagem;
  - Cabeçalhos da mensagem.
- O sistema deve permitir auditoria completa das mensagens incluindo a possibilidade do Download da mensagem original e/ou seus anexos;
- Deve ser possível criar usuários com permissões distintas a fim de limitar o acesso às informações, desta forma a solução deverá possuir no mínimo os seguintes perfis de acesso:
  - Permitir definir o domínio/e-mail que um usuário pode ter acesso;
  - Definir se o usuário deverá ou não ter acesso ao conteúdo da mensagem/anexos;
  - Permitir a criação de usuários para administração da ferramenta de forma granular, ou seja, definir quais áreas do sistema o usuário poderá ter acesso.
- Deve ser compativel com as principais normas de segurança da informação tais como: LGPD;
- Permitir auditoria completa das ações realizadas pelos administradores na interface Web com no mínimo o registro das seguintes ações: Login, Acesso a mensagem, Visualização e Download da Mensagem e Modificações de configurações de parâmetros da solução;
- Possibilitar o encaminhamento (envio) da Mensagem armazenada;
- Permitir integração com os Serviços de Diretórios para acesso a solução: Microsoft AD, LDAP.;
- Possibilidade de gerar relatórios dos e-mails armazenados com as seguintes opções:
  - Data;
  - Origem/Destino;
  - Domínio.
  - Qual a categoria a mensagem recebeu, dentre elas no mínimo:
  - DLP;
  - Provável SPAM;
  - SPAM;
  - Vírus;
  - Conteúdo Bloqueado;
  - Whitelist;
  - Blacklist;
  - Tamanho Excedido;
  - Phishing.
- Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail.

ITEM 06- LICENÇA DE USO DE SOFTWARE/PROGRAMA DE DETECÇÃO E GERENCIAMENTO DE VULNERABILIDADES

1. **Características de Gerais da Solução**

- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- A solução deve permitir a instalação em ambientes tecnológicos distintos, uma vez que será utilizada em redes segregadas e operada de forma independente pelas equipes de TI da CONTRATANTE;
- A solução de gestão de vulnerabilidades é composta por softwares, aqui denominado de módulos, de gerenciamento centralizado e de varreduras que deverão ter a capacidade de realizar busca de vulnerabilidades, configurações incorretas e inconformidade dos ativos de rede, além da identificação de indícios e padrões de códigos maliciosos;

- A solução, de forma proativa e recorrente, deverá identificar possíveis vulnerabilidades de segurança da informação no ambiente com o fito de evitar que ataques cibernéticos obtenham sucesso na exploração de vulnerabilidades;
- Os sistemas utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão;
- Deve possuir serviço de Suporte Técnico e garantia de atualização durante o período da assinatura contratada;
- A solução deverá permitir a migração de licenças entre endereços IP distintos;
- Os produtos que compõem a solução deverão ter seu funcionamento restrito às suas funções, não podendo interferir ou causar lentidão no funcionamento das redes locais das unidades do CONTRATANTE.

2. **Requisitos técnicos para a gestão de vulnerabilidades**

- Deverá possuir um módulo de gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das demais funcionalidades da solução;
- O acesso ao módulo de gerenciamento deverá ser através de https (Secure Hypertext Transfer Protocol) e compatível, minimamente, com os navegadores Internet Explorer, Google Chrome e Mozilla Firefox;
- Deverá suportar múltiplos módulos de varredura (scanners) à procura de vulnerabilidade e exploits, sendo administrados pelo módulo de gerenciamento;
- Deverá ser capaz de escanear e gerenciar no mínimo 2350 ativos, podendo ser servidores, estações de trabalho, switches, roteadores, access points, impressoras, aplicações web etc;
- A solução deverá permitir hardening para impedir explorações no servidor;
- Ter a capacidade de efetuar a descoberta automática dos ativos que possuam endereço IP. Além da possibilidade do cadastramento manual dos ativos;
- A solução deverá permitir a administração e organização dos ativos com suporte a níveis hierárquicos ou tags;
- Possuir recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;
- As vulnerabilidades deverão ser apontadas em aplicações Web, Sistemas Gerenciadores de Banco de Dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
- Verificar vulnerabilidades em ambiente Windows para, no mínimo, detecção de hot fixes, service packs, registros, backdoors, trojans, malware, peer to peer, portas de serviço habilitadas e antivírus;
- Capacidade de selecionar e agrupar ativos encontrados, com possibilidade de inclusão por faixa de endereços IP;
- Capacidade de configuração de usuário e senha para a realização de varredura autenticada de sistemas operacionais e aplicações, sendo essas credenciais armazenadas de forma segura;
- Capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;
- Integração com a base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
- Definição de no mínimo três níveis de criticidade de vulnerabilidades;
- Deverá possuir base de conhecimento com assinaturas de vulnerabilidades com atualização, automática ou por agendamento, a partir do site do fabricante;
- Graduação de riscos, baseada em pontuação e priorizações, que permite medir o nível de riscos dos recursos e sistemas analisados, utilizando, no mínimo, os seguintes critérios:
  - CVSS Impact Score.
- Existência de códigos de exploração da vulnerabilidade encontrada (exploit);
- Existência de módulos de exploração da vulnerabilidade em frameworks automatizados, tais como: Metasploit, Core Impact, CANVAS;
- Apresentação de procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualização de software;
- Levantamento e classificação de ativos, baseado no número de vulnerabilidades encontradas;
- A solução deve ser capaz de identificar vulnerabilidades em aplicações web tais como cross-site scripting, SQL injection e outras vulnerabilidades associadas com o sistema;
- Deverá possuir API para automação de processos e integração com produtos de terceiros;
- Capacidade de envio de e-mail contendo notificações e alertas das vulnerabilidades encontradas;
- A solução deverá possuir mecanismo de proteção contra alteração e remoção indevida de registros e configurações;
- Possuir mecanismos de cópia de segurança (backup) e restauração (restore), contemplando, minimamente, as suas informações, configurações, políticas, usuários, credenciais e ativos.
- Capacidade de realização de varreduras simultâneas nos diversos ativos;
- As verificações em busca de vulnerabilidades deverão ser executadas a partir de um endereço IP ou de FQDN (Full Qualified Domain Name);
- A solução deverá possuir em sua base de vulnerabilidades, no mínimo, as seguintes informações: nome, descrição, CVSS score, referência (CVE, CWE, NVD, BID ou outra fonte), solução e link para o download da correção (se aplicável), contramedidas (se aplicável), e exploit (se aplicável);
- A solução deverá utilizar o padrão CVSS nas versões 2 e 3;
- Deverá ser possível realizar ajustes e alterações dos níveis de severidades das vulnerabilidades;
- A solução deve possuir um mecanismo de priorização das vulnerabilidades com análise dinâmica baseado em algoritmos de inteligência artificial;
- Capacidade de definir templates de configuração e agendamento de varreduras;
- Possuir configuração de agendamento para realização de varreduras automáticas;
- Permitir a execução manual de varreduras;
- Deverá possibilitar que uma varredura em execução seja interrompida;
- Permitir a configuração de intervalo de tempo para a execução da varredura;
- Permitir a configuração de timeout na execução de varredura;
- Caso uma varredura tenha sido interrompida por ter extrapolado o tempo de execução, deverá ser possível o seu reinício em outro momento a partir do ponto em que parou;

- Deverá ser possível o acompanhamento do andamento das varreduras através do módulo de gerenciamento;
- A solução deverá permitir a alteração do estado de criticidade das vulnerabilidades encontradas;
- A solução deverá permitir que uma determinada vulnerabilidade encontrada seja marcada como corrigida ou ignorada;
- Possuir a capacidade de identificação do uso de senha padrão de fabricantes de ativos;
- A solução deverá prover modelo de validação para controles técnicos da Norma ABNT NBR ISO 27002:2013 ou ISO/IEC 27002:2013;
- A solução deverá possuir compatibilidade com o padrão XCCDF (Extensible Configuration Checklist Description Format);
- A solução deverá realizar coleta automatizada para ativos tecnológicos, com compatibilidade com o padrão OVAL (Open Vulnerability and Assessment Language), na versão 5.11.1 ou superior;

3. **Requisitos de integração e monitoramento**

- A solução deverá permitir o gerenciamento dos dados através de pelo menos um dos seguintes métodos de interoperabilidade:
  - API (Application Programming Interface).
  - REST (Representational State Transfer).
- A solução deverá possuir capacidade de integração com o Microsoft Server Updade Services (WSUS);
- A solução deverá possuir capacidade de integração com o Microsoft System Center Configuration Managemente (SCCM);
- Suportar o protocolo SNMP (Simple Network Management Protocol), nas versões v2 ou v3;
- A solução deverá armazenar os logs localmente por período determinado e possuir funcionalidade que permita compartilhar os logs, em tempo real e/ou por agendamento, para um Syslog server com a finalidade de armazenamento a longo prazo;
- A solução deve possuir mecanismos de correlação de eventos observados em logs fornecidos de diferentes dispositivos de rede em conjunto com a monitoria passiva para detecção de comportamento malicioso e enriquecimento de resultados de varreduras;
- Deve ser capaz de correlacionar e normalizar os logs recebidos;
- A solução deve ser capaz de receber Logs de uma ampla variedade de fontes;
- Deve suportar coletar dados de eventos das seguintes fontes, no mínimo:
  - Windows Event Logs;
  - Logs de sistemas e aplicações das plataformas: Windows e Linux;
  - Tráfego TCP e UDP;
  - Encrypted Syslog.
- Deve suportar o monitoramento de arquivos para os seguintes sistemas operacionais:
  - Windows;
  - Debian;
  - CentOS;
  - Ubuntu.

4. **Requisitos de relatórios e painéis gerenciais (dashboards)**

- A solução deverá possuir painéis gerenciais (dashboards) prédefinidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- Deverá reportar eventos agrupados por sistema operacional, endereços IP, nome DNS, porta de serviços ou vulnerabilidades;
- A solução deverá ter a capacidade de emitir, minimamente, os seguintes relatórios:
  - Relatório de vulnerabilidades com os resultados encontrados nas varreduras;
  - Relatório de vulnerabilidades com comparativo ou diferencial entre varreduras;
  - Relatório do histórico de vulnerabilidades;
  - Relatório de vulnerabilidades por ativo e por período;
  - Relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CONTRATANTE em relação aos riscos de segurança da informação, contendo: hosts encontrados, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;
  - Relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos;
  - Relatório dos ativos monitorados, contendo informações sobre serviços e vulnerabilidades encontradas por ativo.
- Todos os relatórios deverão apresentar os níveis de severidade para as vulnerabilidades encontradas;
- A solução deverá permitir a exportação dos relatórios em pelo menos dois dos seguintes formatos: CSV, HTML, DOCX ou PDF;
- A solução deverá ter a capacidade de envio do relatório exportado por e-mail.

5. **Requisitos de criptografia**

- Todos os dados armazenados na solução e toda a comunicação de dados trafegada entre os módulos da solução deverão ser criptografados com o protocolo TLS, com certificado digital X.509 v3, para a autenticação do servidor da solução;
- A solução deverá ser capaz de importar certificados de Autoridade Certificadora (AC);
- Para a interface web, a solução deverá prover meios de habilitar e desabilitar as versões do protocolo TLS e dos cipher suites suportados, sendo que:
  - Deverá suportar a versão 1.2 do protocolo TLS ou superior.
  - Deverá permitir que, durante o handshake TLS, seja apresentado o certificado da entidade final e da AC intermediária para o cliente da conexão.

6. **Requisitos de controle de acesso**

- A solução deverá permitir acesso a suas funcionalidades somente a partir de endereços IP definidos e autorizados pelo CONTRATANTE;
- As permissões de acesso à solução deverão ser gerenciadas a partir do módulo de gerenciamento;
- Não deverá ter limite de usuários simultâneos;
- Para o provisionamento das autorizações de acesso dos usuários poderá ser utilizado recurso de cadastramento interno de usuários na solução ou poderá ser feita uma integração com o serviço de diretório Active Directory (AD) do CONTRATANTE;

- A solução deverá possibilitar o acesso multiusuário, com níveis de permissões distintas para administração de funcionalidades, acesso a logs e emissão de relatórios;
- A solução deverá possuir mecanismos de administração de permissões de acesso sobre suas funcionalidades, com a definição clara das hierarquias, papéis e atribuições dentro do contexto de negócio, permitindo a criação, edição e remoção de diferentes tipos de usuários, com diferentes níveis de autorização, permissões e visões;
- Deverá ser permitido a desativação manual de usuários;
- A solução deverá permitir que cada usuário pertença a mais de um perfil, acumulando suas permissões;
- A solução deverá permitir a parametrização da sua utilização e visualização de menus e respectivas informações de acordo com os perfis de acesso.

ITEM 07 - EQUIPAMENTO DE SEGURANÇA DE REDE FIREWALL (TIPO I)

1. **Características de Gerais da Solução**

- Os equipamentos devem ser novos e de primeiro uso;
- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- O fornecedor deverá realizar também a instalação lógica migrando as configurações dos equipamentos de rede em produção para os novos ativos fornecidos;
- Os produtos utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão.
- Deve possuir serviço de Suporte Técnico e garantia durante o período contratado;
- A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, identificação de usuários e controle granular de permissões;
- 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;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2. **Especificações básicas**

- Deve possuir desempenho (*throughput*) de, no mínimo, 4.3 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
- Deve possuir desempenho (*throughput*) de, no mínimo, 2.2 Gbps com todas as funcionalidades de segurança habilitadas simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- Deve possuir desempenho (*throughput*) de, no mínimo, 2.6 Gbps para VPN IPSec;
- Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;
- Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar);
- Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;
- Suporte a, no mínimo, 1.000.000 conexões simultâneas;
- Suporte a, no mínimo, 50.000 novas conexões por segundo;
- Fonte 120/240 AC ou DC, redundante e hot-swappble;
- Disco Solid State Drive (SSD) de, no mínimo, 240 GB;
- 12 (doze) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;
- 4 (quatro) interfaces de rede 10 Gbps SFP+;
- 2 (duas) interfaces de 1 Gbps dedicadas para alta disponibilidade;
- 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
- 1 (uma) interface do tipo console ou similar;
- Suporte a, no mínimo, 200 (trinta) zonas de segurança;
- Estar licenciada para ou suportar sem o uso de licença, 1.000 (mil) clientes de VPN SSL simultâneos;
- Estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 5 sistemas virtuais lógicos (Contextos) no firewall Físico;
- Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
- Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
- Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
- A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;
- Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

3. **Funcionalidades mínimas**

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

- Agregação de links 802.3ad e LACP;
- Policy based routing ou policy based forwarding;
- Roteamento multicast (PIM-SM);
- DHCP Relay;
- DHCP Server;
- Jumbo Frames;
- Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- Suportar sub-interfaces ethernet logicas;
- O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- Deve suportar os seguintes tipos de NAT:
  - Nat dinâmico (Many-to-1);
  - Nat dinâmico (Many-to-Many);
  - Nat estático (1-to-1);
  - NAT estático (Many-to-Many);
  - Nat estático bidirecional 1-to-1;
  - Tradução de porta (PAT);
  - NAT de Origem;
  - NAT de Destino;
  - Suportar NAT de Origem e NAT de Destino simultaneamente;
- Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
- Deve implementar o protocolo ECMP;
- Deve implementar balanceamento de link por hash do IP de origem;
- Deve implementar balanceamento de link por hash do IP de origem e destino;
- Deve implementar balanceamento de link através do método round-robin;
- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;
- Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
- Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
- Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
- Enviar log para sistemas de monitoração externos, simultaneamente;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- Proteção contra anti-spoofing;
- Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Suportar a OSPF graceful restart;
- Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;
- O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
- Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
  - Em modo transparente;
  - Em layer 3.
- A configuração em alta disponibilidade deve sincronizar:
  - Sessões;
  - Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
  - Certificados de-criptografados;
  - Associações de Segurança das VPNs;
  - Tabelas FIB.

- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4. **Controle por política de firewall**

- Deverá suportar controles por zona de segurança;
- Controles de políticas por porta e protocolo;
- Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
- Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e 1.3;
- Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- Controle de inspeção e de-criptografia de SSH por política;
- A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
- A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
- É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;
- Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
- Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
- QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;
- Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). Os fluxos mínimos de análise de regras legadas devem trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;

5. **Controle de aplicações**

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- Reconhecer pelo menos 1700 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;
- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
- Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;
- Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 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. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
- Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos apenas para alguns usuários;
- Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Atualizar a base de assinaturas de aplicações automaticamente;

- Reconhecer aplicações em IPv6;
- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- 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 Domain Controller, nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
  - HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
  - Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando na mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
  - Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
  - Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias.
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
- Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
  - Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc).
  - Nível de risco da aplicação.
  - Categoria e sub-categoria de aplicações.
  - Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc;
- Deve permitir a inserção de duplo fator de autenticação na política de segurança não limitando a VPN apenas no mínimo para certificados, One-Time-Password ou Token de Software;
- Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.

6. **Identificação dos usuários**

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
- Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 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);
- Suporte a autenticação Kerberos;
- Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;
- O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

7. **QOS**

- Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- Suportar a criação de políticas de QoS por:
  - Endereço de origem;
  - Endereço de destino;
  - Por usuário e grupo do LDAP/AD;
  - Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
  - Por porta.
- O QoS deve possibilitar a definição de classes por:
  - Banda Garantida;
  - Banda Máxima;
  - Fila de Prioridade.
- Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
- Disponibilizar estatísticas RealTime para classes de QoS;
- Deve suportar QOS (traffic-shapping), em interface agregadas;
- Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

8. **Filtro de dados**

- Permite a criação de filtros para arquivos e dados pré-definidos;
- Os arquivos devem ser identificados por extensão e assinaturas;
- Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
- Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;
- Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- Permitir listar o número de aplicações suportadas para controle de dados;
- Permitir listar o número de tipos de arquivos suportados para controle de dados.

9. **Geo-localização**

- Suportar a criação de politicas por Geo Localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

10. **VPN**

- Suportar VPN Site-to-Site e Cliente-To-Site;
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN IPSEc deve suportar:
  - 3DES;
  - Autenticação MD5 e SHA-1;
  - Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 e v2);
  - AES 128, 192 e 256 (Advanced Encryption Standard);
  - Autenticação via certificado IKE PKI.
- Deve possuir interoperabilidade com os seguintes fabricantes:
  - Cisco;
  - Checkpoint;
  - Juniper;
  - Palo Alto Networks;
  - Fortinet;
  - Sonic Wall.
- Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
- A VPN SSL deve suportar:
  - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
  - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
  - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
  - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
  - Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
  - Atribuição de DNS nos clientes remotos de VPN;
  - Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
  - A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
  - Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

- Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
- Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
- Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
- Dever permitir criar políticas de controle de aplicações para tráfego dos clientes remotos conectados na VPN SSL;
- A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
- Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- Suporta leitura e verificação de CRL (certificate revocation list);
- Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;
- Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
  - Antes do usuário autenticar na estação;
  - Após autenticação do usuário na estação;
  - Sob demanda do usuário;
- Deve Manter uma conexão segura com o portal durante a sessão;
- O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
- O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
- Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
- A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
- Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
- O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
- Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
- Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

11. **Console de gerência e monitoração**

- Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
- O gerenciamento deve permitir/possuir:
  - Criação e administração de políticas de firewall e controle de aplicação;
  - Monitoração de logs;
  - Ferramentas de investigação de logs;
  - Debugging;
  - Captura de pacotes;
  - Acesso concorrente de administradores.
- Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
- Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
- Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- Definição de perfis de acesso à console com permissões granulares como:
  - acesso de escrita;
  - acesso de leitura;
  - criação de usuários;
  - alteração de configurações.
- Autenticação integrada ao Microsoft Active Directory e servidor Radius;
- Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- Criação de regras que fiquem ativas em horário definido;
- Criação de regras com data de expiração;
- Backup das configurações e rollback de configuração para a última configuração salva;
- Suportar Rollback de Sistema Operacional para a ultima versão local;
- Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

- Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
- Deve suportar interface de configuração baseada no padrão Openconfig;
- Validação de regras antes da aplicação;
- Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc;
- É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação;
- Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada;
- É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas;
- Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
- Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Deve ter a capacidade de encaminhar todo tráfego seja ele criptografado ou não para uma cadeia de equipamentos de segurança tais como IPS, IDS e SIEM para inspeção. Esta funcionalidade pode ser entregue por ferramenta externa;
- Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- Deve prover relatórios com visão correlacionada de aplicações e ameaças para melhor diagnóstico e resposta a incidentes;
- Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, ameaças e tráfego bloqueado;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- Deve possuir relatórios de utilização dos recursos por aplicações, ameaças, etc;
- Prover uma visualização sumarizada de todas as aplicações e ameaças que passaram pela solução;
- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
- Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
- Deve ser possível exportar os logs em CSV;
- Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
- Rotação do log: deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
- Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
- Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
  - Situação do dispositivo e do cluster;
  - Principais aplicações;
  - Principais aplicações por risco;
  - Administradores autenticados na gerência da plataforma de segurança;
  - Número de sessões simultâneas;
  - Status das interfaces;
  - Uso de CPU;
- Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
  - Resumo gráfico de aplicações utilizadas;
  - Principais aplicações por utilização de largura de banda de entrada e saída;
  - 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 e ameaças de rede vinculadas a este tráfego;
- Deve permitir a criação de relatórios personalizados;
- Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
- Gerar alertas automáticos via:
  - Email;
  - SNMP;
  - Syslog.
- A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

ITEM 08 - EQUIPAMENTO DE SEGURANÇA DE REDE FIREWALL (TIPO II)

1. **Características de Gerais da Solução**

- Os equipamentos devem ser novos e de primeiro uso;
- A solução deverá ser instalada nas dependências (localmente) do Ministério da Defesa;
- O fornecedor deverá realizar também a instalação lógica migrando as configurações dos equipamentos de rede em produção para os novos ativos fornecidos;
- Os produtos utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a atualização de versão.
- Deve possuir serviço de Suporte Técnico e garantia durante o período contratado;
- A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, identificação de usuários e controle granular de permissões;
- 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;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2. **Especificações básicas**

- Deve possuir desempenho (*throughput*) de, no mínimo, 2 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
- Deve possuir desempenho (*throughput*) de, no mínimo, 1 Gbps com todas as funcionalidades de segurança habilitadas simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- Deve possuir desempenho (*throughput*) de, no mínimo, 1.8 Gbps para VPN IPSec;
- Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;
- Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar);
- Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;
- Suporte a, no mínimo, 190.000 conexões simultâneas;
- Suporte a, no mínimo, 13.000 novas conexões por segundo;
- Fonte 120/240 AC ou DC, redundante e hot-swappble;
- Disco Solid State Drive (SSD) de, no mínimo, 240 GB;
- 04 (quatro) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;
- 04 (quatro) interfaces de rede 10 Gbps SFP+;
- 2 (duas) interfaces de 1 Gbps dedicadas para alta disponibilidade;
- 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
- 1 (uma) interface do tipo console ou similar;
- Suporte a, no mínimo, 30 (trinta) zonas de segurança;
- Estar licenciada para ou suportar sem o uso de licença , 1.000 (mil) clientes de VPN SSL simultâneos;
- Estar licenciada para ou suportar sem o uso de licença, 1.000 (mil) túneis de VPN IPSEC simultâneos;
- Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
- Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
- Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
- A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;
- Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

3. **Funcionalidades mínimas**

- Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
- Agregação de links 802.3ad e LACP;
- Policy based routing ou policy based forwarding;
- Roteamento multicast (PIM-SM);
- DHCP Relay;
- DHCP Server;
- Jumbo Frames;
- Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- Suportar sub-interfaces ethernet logicas;
- O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

- Deve suportar os seguintes tipos de NAT:
- Nat dinâmico (Many-to-1);
- Nat dinâmico (Many-to-Many);
- Nat estático (1-to-1);
- NAT estático (Many-to-Many);

4. **Controle por política de firewall**

- Deverá suportar controles por zona de segurança;
- Controles de políticas por porta e protocolo;
- Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
- Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e 1.3;
- Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
- É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;
- Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
- Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
- QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;
- Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). Os fluxos mínimos de análise de regras legadas devem trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;

5. **Controle de aplicações**

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- Reconhecer pelo menos 1700 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;
- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
- Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;
- Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 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. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
- Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos apenas para alguns usuários;
- Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Reconhecer aplicações em IPv6;

- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- 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 Domain Controller, nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
  - HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
- Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando na mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
- Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
- Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
- Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
  - Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc).
  - Nível de risco da aplicação.
  - Categoria e sub-categoria de aplicações.
  - Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc;
- Deve permitir a inserção de duplo fator de autenticação na política de segurança não limitando a VPN apenas no mínimo para certificados, One-Time-Password ou Token de Software;
- Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.

6. **Identificação dos usuários**

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
- Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 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);
- Suporte a autenticação Kerberos;
- Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;
- O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

7. **QOS**

- Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- Suportar a criação de políticas de QoS por:
  - Endereço de origem;
  - Endereço de destino;
  - Por usuário e grupo do LDAP/AD;
  - Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
  - Por porta.
- O QoS deve possibilitar a definição de classes por:
  - Banda Garantida;
  - Banda Máxima;
  - Fila de Prioridade.
- Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
- Disponibilizar estatísticas RealTime para classes de QoS;
- Deve suportar QOS (traffic-shapping), em interface agregadas;
- Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

8. **Filtro de dados**

- Permite a criação de filtros para arquivos e dados pré-definidos;
- Os arquivos devem ser identificados por extensão e assinaturas;
- Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
- Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;
- Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- Permitir listar o número de aplicações suportadas para controle de dados;
- Permitir listar o número de tipos de arquivos suportados para controle de dados.

9. **Geo-localização**

- Suportar a criação de politicas por Geo Localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

10. **VPN**

- Suportar VPN Site-to-Site e Cliente-To-Site;
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN IPSEc deve suportar:
  - 3DES;
  - Autenticação MD5 e SHA-1;
  - Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 e v2);
  - AES 128, 192 e 256 (Advanced Encryption Standard);
  - Autenticação via certificado IKE PKI.
- Deve possuir interoperabilidade com os seguintes fabricantes:
  - Cisco;
  - Checkpoint;
  - Juniper;
  - Palo Alto Networks;
  - Fortinet;
  - Sonic Wall.
- Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
- A VPN SSL deve suportar:
  - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
  - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
  - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
  - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
  - Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
  - Atribuição de DNS nos clientes remotos de VPN;
  - Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
  - A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
  - Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

- Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
- Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
- Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
- Dever permitir criar políticas de controle de aplicações para tráfego dos clientes remotos conectados na VPN SSL;
- A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
- Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- Suporta leitura e verificação de CRL (certificate revocation list);
- Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
  - Antes do usuário autenticar na estação;
  - Após autenticação do usuário na estação;
  - Sob demanda do usuário;
- Deve Manter uma conexão segura com o portal durante a sessão;
- O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
- O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
- Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
- A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
- Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
- O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
- Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
- Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

11. **Console de gerência e monitoração**

- Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
- O gerenciamento deve permitir/possuir:
  - Criação e administração de políticas de firewall e controle de aplicação;
  - Monitoração de logs;
  - Ferramentas de investigação de logs;
  - Debugging;
  - Captura de pacotes;
  - Acesso concorrente de administradores.
- Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
- Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
- Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- Definição de perfis de acesso à console com permissões granulares como:
  - acesso de escrita;
  - acesso de leitura;
  - criação de usuários;
  - alteração de configurações.
- Autenticação integrada ao Microsoft Active Directory e servidor Radius;
- Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- Criação de regras que fiquem ativas em horário definido;
- Criação de regras com data de expiração;
- Backup das configurações e rollback de configuração para a última configuração salva;
- Suportar Rollback de Sistema Operacional para a ultima versão local;
- Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

- Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
- Deve suportar interface de configuração baseada no padrão Openconfig;
- Validação de regras antes da aplicação;
- Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc;
- É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação;
- Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada;
- É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas;
- Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
- Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Deve ter a capacidade de encaminhar todo tráfego seja ele criptografado ou não para uma cadeia de equipamentos de segurança tais como IPS, IDS e SIEM para inspeção. Esta funcionalidade pode ser entregue por ferramenta externa;
- Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- Deve prover relatórios com visão correlacionada de aplicações e ameaças para melhor diagnóstico e resposta a incidentes;
- Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças e tráfego bloqueado;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação e filtro de arquivos em uma única tela.
- Deve possuir relatórios de utilização dos recursos por aplicações, ameaças, etc;
- Prover uma visualização sumarizada de todas as aplicações e ameaças que passaram pela solução;
- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
- Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
- Deve ser possível exportar os logs em CSV;
- Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
- Rotação do log;
- Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
- Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
- Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
  - Situação do dispositivo e do cluster;
  - Principais aplicações;
  - Principais aplicações por risco;
  - Administradores autenticados na gerência da plataforma de segurança;
  - Número de sessões simultâneas;
  - Status das interfaces;
  - Uso de CPU;
- Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
  - Resumo gráfico de aplicações utilizadas;
  - Principais aplicações por utilização de largura de banda de entrada e saída;
  - 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 e ameaças de rede vinculadas a este tráfego;
- Deve permitir a criação de relatórios personalizados;
- Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
- Gerar alertas automáticos via:
  - Email;
  - SNMP;
  - Syslog.
- A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

Documento assinado eletronicamente por **Jeferson Denis Cruz de Medeiros**, **Diretor(a)**, em 17/08/2022, às 12:47, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

Documento assinado eletronicamente por **Daniel de Souza Santos**, **Coordenador(a)**, em 17/08/2022, às 13:27, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

Documento assinado eletronicamente por **Edmar da Silva Braga Junior**, **Assistente Técnico(a)**, em 17/08/2022, às 13:35, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

Documento assinado eletronicamente por **Marcello da Silva Figueiredo**, **Coordenador(a)**, em 17/08/2022, às 13:48, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

Documento assinado eletronicamente por **Antonio Gaetani de Sousa Santos**, **Supervisor(a)**, em 17/08/2022, às 15:30, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

A autenticidade do documento pode ser conferida no site https://sei.defesa.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, o código verificador **5445354** e o código CRC **A346AFF6**.