TERMO DE REFERÊNCIA

PAE 2023/835789

PAE 4.0 E-2024/2096228

DO OBJETO

Registro de Preços para futura e eventual contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, conforme quantidades e exigências estabelecidas neste Termo de Referência, para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, de acordo com as especificações e quantitativos previstos neste Termo.

Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, com a forma de fornecimento por demanda.

DA JUSTIFICATIVA

A Defensoria Pública do Estado do Pará – DPE/PA tem como meta estratégica na Tecnologia da Informação e Comunicação - TIC a disponibilização de ferramentas tecnológicas que garantam o adequado funcionamento do ambiente tecnológico e que colaborem com a melhoria da produtividade dos seus usuários. Portanto, assim como os outros poderes que compõem a estrutura de Estado, a DPE/PA necessita de proteção e segurança sobre o conteúdo armazenado

e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

Os seguintes fatores motivaram essa contratação:

• Reforço da segurança cibernética das unidades da Defensoria Pública do Pará;
• Aumento da quantidade de ataques maliciosos às aplicações oferecidas pela DPE;
• Aumento nos sistemas informatizados;

Os seguintes resultados são esperados:

• Disponibilidade de sistemas e aplicações da DPE (Solar, Intranet, Sistema de Diária, etc);
• Reforço da estrutura de Segurança da Informação, principalmente em virtude do aumento massivo de ataques cibernéticos a órgãos governamentais.
• Minimizar o risco de continuidade do negócio por ataques à infraestrutura de TI.
• Melhorar o nível de segurança de dados da Defensoria Pública do Estado do Pará;
• Controlar os usuários que entram na rede corporativa;
• Controlar o acesso aos aplicativos e recursos que os usuários pretendem acessar;
• Permitir que contratados, parceiros e convidados entrem na rede conforme necessário, mas restrinja seu acesso;
• Segmentar funcionários em grupos com base em sua função de trabalho e crie políticas de acesso baseadas em função;
• Proteger contra ataques cibernéticos implementando sistemas e controles que detectam atividades incomuns ou suspeitas;
• Automatizar a resposta a incidentes;
• Gerar relatórios e insights sobre tentativas de acesso em toda a instituição;

• Reduzir a proliferação de dispositivos nas unidades de todo estado combinando firewalls, switches e pontos de acesso wi-fi em uma única solução, permitindo o gerenciamento integrado de serviços de rede.

• Consolidar a identificação, autenticação, autorização, detecção e resposta dos incidentes de segurança.

Diversos fatores impulsionaram essa consolidação, como a busca por redução de custos, aumento da produtividade, melhora da mobilidade, flexibilidade e escalabilidade. Os benefícios da integração são numerosos, incluindo eficiência na gestão da infraestrutura e dos processos, agilidade na comunicação entre colaboradores, flexibilidade para se adaptar às necessidades da instituição!ão e segurança contra ataques cibernéticos. Apesar dos desafios, as tendências para o futuro da gestão de redes são promissoras, com a integração da inteligência artificial, migração para a nuvem e integração de dispositivos da Internet das Coisas (IoT) à plataforma de comunicação. Exemplos de soluções convergentes que já estão disponíveis no mercado e que hoje utilizamos na Defensoria, como o Google Workspace, para atender às nossas necessidades.

No cenário atual, caracterizado por ameaças cibernéticas em constante evolução e pela necessidade de uma infraestrutura de TI ágil e eficiente, a consolidação das tecnologias de conectividade de rede corporativa emerge como uma necessidade imperativa. Esta iniciativa visa integrar redes wireless, controle de admissão à rede e soluções robustas de segurança cibernética em uma única plataforma. Para a DPE-PA, tal consolidação é estratégica, garantindo não apenas a eficiência operacional, mas também a segurança e a confiabilidade de sua infraestrutura de rede.

A base para esta justificativa reside em três premissas fundamentais: a necessidade de uma conectividade de rede ininterrupta, a demanda por uma infraestrutura robusta e flexível e a importância primordial da segurança cibernética. No contexto da DPE-PA, uma organização que depende criticamente de seus sistemas de TI para a prestação de serviços jurídicos essenciais, estas premissas são inegociáveis.

A consolidação visa abordar várias necessidades cruciais. Primeiramente, reduzir a complexidade e o custo de gerenciamento de múltiplas redes, uma vez que a diversidade de soluções fragmentadas pode aumentar os riscos operacionais e os custos. Além disso, busca-se melhorar a performance da rede, aumentando a velocidade, confiabilidade e disponibilidade - fatores que são diretamente proporcionais à capacidade da DPE-PA de responder de maneira

eficiente às necessidades de seus usuários. A segurança aprimorada, através de medidas robustas de proteção e controle de acesso granular, é outra necessidade vital, permitindo o acesso seguro à rede e alinhando-se às melhores práticas de segurança da informação.

Os benefícios de tal consolidação são abrangentes. Primeiramente, observa-se uma redução significativa de custos relacionados à aquisição, manutenção e gerenciamento da infraestrutura de rede. A melhoria na performance da rede não só aumenta a produtividade como também garante maior agilidade nos processos operacionais. A segurança da rede é consideravelmente reforçada, protegendo a organização contra-ataques cibernéticos e acesso não autorizado. Além disso, a maior flexibilidade permite uma fácil expansão e adaptação da rede às necessidades em constante mudança da organização, enquanto o gerenciamento simplificado facilita a administração e o controle centralizado.

Propõe-se a consolidação das tecnologias de conectividade de rede corporativa em uma única plataforma, que abranja tanto a rede cabeada quanto a rede sem fio, o controle de admissão à rede, e soluções robustas de segurança cibernética. Esta plataforma escalável, adaptando-se ao crescimento da organização e às novas demandas de conectividade. A segurança avançada e a conformidade com os padrões de segurança da informação são imperativos, assim como a gestão centralizada, que simplifica a administração e o controle da rede.

A consolidação das tecnologias de conectividade de rede corporativa representa um investimento estratégico crucial para a DPE-PA. Essa iniciativa não só garante a eficiência, segurança e confiabilidade da infraestrutura de rede, mas também traz benefícios tangíveis como a redução de custos, aumento da produtividade, segurança reforçada e maior flexibilidade. A implementação de uma plataforma consolidada posiciona a DPE-PA como uma organização ágil e resiliente, pronta para enfrentar os desafios tecnológicos atuais e futuros ao considerar a justificativa para a consolidação de tecnologias de conectividade de rede corporativa na Defensoria Pública do Estado do Pará (DPE-PA).

A argumentação abordada anteriormente é fortalecida e ampliada pela integração e simplificação de gestão, pela segurança aprimorada, pela resiliência e confiabilidade, pela eficiência operacional e redução de custos, e pela adaptação às evoluções das necessidades de negócios. Além disso, aspectos como compatibilidade e interoperabilidade, atualizações e manutenção simplificadas, redução de silos operacionais, análise de dados aprimorada, resposta a incidentes acelerada, conformidade regulatória facilitada, e a melhoria na experiência do usuário ressaltam a importância estratégica desta consolidação.

No âmbito técnico, a consolidação permite abordar desafios como desempenho e escalabilidade, essenciais para atender às demandas atuais e futuras da DPE-PA. Garantir a confiabilidade e a segurança em um cenário de ameaças cibernéticas em evolução é crucial para proteger os dados sensíveis e as operações da instituição. Além disso, o gerenciamento e provisionamento eficientes facilitam a administração da rede, otimizando recursos e antecipando problemas. A integração e interoperabilidade com sistemas de TI existentes e novas tecnologias asseguram a flexibilidade e proteção do investimento em infraestrutura.

A escolha de soluções que se alinham com objetivos de sustentabilidade reflete o compromisso da DPE-PA com práticas responsáveis, um aspecto cada vez mais relevante no cenário atual.

Historicamente, a jornada tecnológica transitou por diversas fases, iniciando-se em uma era de simplicidade, onde as redes eram fundamentadas em cabos físicos e topologias básicas, a conectividade era limitada e a segurança focava em medidas periféricas. Esta fase foi seguida por um período de complexidade caracterizado pela adoção de IP, virtualização, e um crescimento exponencial tanto em dispositivos conectados quanto em ameaças de segurança, culminando na era atual de convergência. Neste estágio, tecnologias como Software Defined Networking (SDN), automação, nuvem híbrida, e 5G tornaram-se preponderantes, enquanto a segurança evoluiu para incorporar estratégias como Zero Trust e micro segmentação, amplamente apoiadas pela análise de comportamento e capacidades preditivas da IA.

A IA, nesta sinfonia tecnológica, atua como o maestro, orquestrando uma harmonização entre a otimização da infraestrutura de rede, a personalização da conectividade e a prevenção proativa de ameaças de segurança. Por meio da automação, análise de dados e aprendizado contínuo, a IA permite que redes se ajustem dinamicamente, personalizem a experiência do usuário em dispositivos e plataformas, e identifica ameaças em potencial antes mesmo que se concretizem, garantindo uma proteção mais robusta e adaptável.

A implementação prática dessa convergência se manifesta através de monitoramento em tempo real, resposta automatizada a incidentes e proteção contra ataques direcionados, demonstrando a capacidade da IA de aprender com o passado para proteger o futuro. Contudo, apesar das oportunidades significativas como aumento de eficiência, segurança aprimorada e experiências de usuário enriquecidas, existem desafios notáveis. A integração de tecnologias emergentes, o gerenciamento eficaz de grandes volumes de dados e o desenvolvimento de competências especializadas em IA representam obstáculos significativos.

Em estudo recente, do renomado Gartner Group, veiculou relatório de janeiro deste ano, 2024, consolidou a abordagem de conectividade cabeada a redes sem fio com detecção de intrusos, abordando aspectos de segurança na infraestrutura de conectividade, escalabilidade, autenticação integrada e telemetria para otimização da rede, assim como a integração e o monitoramento do comportamento das ações de usuários, e aspectos relevantes de inteligência artificial, com visibilidade e gerenciamento de desempenho. Neste viés, apresento o quadrante mágico de fornecedores, onde nomeiam os líderes, no quadrante superior à direita.

https://www.gartner.com/en/documents/5253763

Conclui-se, portanto, que a convergência de infraestrutura de rede, conectividade e segurança da informação, sob a regência da inteligência artificial, não é meramente uma tendência, mas uma evolução inevitável no domínio tecnológico. Esta progressão não apenas habilita organizações a enfrentar desafios futuros com maior resiliência, mas também pavimenta o caminho para uma era de inovações sem precedentes, onde a segurança e a eficiência coexistem em perfeita harmonia.

Esses aspectos sublinham a importância de uma abordagem consolidada nas contratações, na qual a seleção de um fornecedor único capaz de entregar uma solução integrada e holística se

apresenta como a estratégia mais eficaz. Além de mitigar os riscos de incompatibilidade, segurança e gestão, essa abordagem unificada minimiza as chances de desvios nos prazos de entrega e as incertezas relacionadas à seleção dos fornecedores, assegurando uma implementação mais fluida e coordenada das tecnologias necessárias.

Para a Defensoria Pública do Estado do Pará, é imperativo considerar esses fatores ao planejar suas contratações, optando por soluções que promovam a integração, eficiência e resiliência operacional. Uma estratégia de contratação bem delineada, focada na simplificação e na segurança, é fundamental para garantir a continuidade e a qualidade dos serviços oferecidos à população, alinhando-se aos objetivos estratégicos e operacionais da DPE-PA.

Na era contemporânea da tecnologia, observa-se uma tendência inevitável rumo à convergência de infraestrutura de rede, conectividade e segurança da informação, uma transformação amplamente impulsionada pelos avanços em inteligência artificial (IA). Esta metamorfose tecnológica, relembrança da evolução musical de simples melodias para complexas sinfonias, reflete uma resposta versátil aos crescentes desafios de segurança cibernética e à crescente influência da IA sobre o cenário tecnológico.

Em suma, a consolidação das tecnologias de conectividade de rede corporativa é um passo estratégico fundamental para a DPE-PA, promovendo uma gestão mais eficiente, segurança reforçada, e capacidade de adaptar-se às exigências futuras. A implementação de uma infraestrutura unificada traz benefícios tangíveis em termos de redução de custos, aumento da produtividade, e maior flexibilidade, alinhando a organização com as melhores práticas e tendências do mercado. Essa iniciativa posiciona a DPE-PA como uma entidade líder em inovação e eficiência operacional, pronta para enfrentar os desafios do cenário tecnológico dinâmico e garantir a prestação de serviços jurídicos de alta qualidade.

Portanto, em face das razões acima expostas, elaboramos o presente Termo de Referência, com o fim de instruir procedimento administrativo licitatório objetivando contratação de empresa para o fornecimento de solução de cibersegurança e gestão de rede para todas as unidades da Defensoria Pública do Estado do Pará.

DO MODELO DE CONTRATAÇÃO

Esse processo de contratação segue o modelo de contratação que contempla a definição dos procedimentos necessários e suficientes ao adequado fornecimento de Soluções de Tecnologia da Informação-TI, por lote único, envolvendo aquisição, instalação e manutenção.

DA JUSTIFICATIVA PARA LOTE ÚNICO

Os itens deste certame foram agrupados devido à sua necessidade de integração e sua interdependência, ou seja, a exigência de compatibilidade entre as partes e gestão integrada das entregas para garantir o seu funcionamento, dado que a sua implementação é bastante complexa.

Em contraponto, o parcelamento traz mais complexidade gerencial, e é um dos principais desafios trazidos pela separação das contratações. Quando uma entidade como o DPE-PA opta por dividir contratações em lotes distintos, enfrenta uma crescente complexidade operacional devido à necessidade de gerir múltiplos contratos com diferentes fornecedores. Este cenário demanda um aumento significativo dos recursos administrativos, além de elevar o risco de inconsistências e falhas na integração entre sistemas e soluções fornecidos por empresas distintas. Tais falhas de integração podem criar vulnerabilidades na segurança e gerar ineficiências operacionais, afetando diretamente a produtividade e a continuidade dos negócios.

A estratégia de dividir as contratações pode conduzir a custos ocultos que elevam o custo de propriedade ao longo do tempo. Esses custos adicionais, muitas vezes não antecipados, decorrem de despesas com integração, manutenção e suporte técnico. Esse aumento no do custo de propriedade pode diluir o retorno sobre o investimento, impactando negativamente os orçamentos destinados a outras iniciativas estratégicas da organização.

A segurança cibernética é outra área significativamente impactada pela fragmentação das contratações. A gestão de múltiplos fornecedores torna desafiador manter uma postura de segurança consistente e robusta, aumentando a superfície de ataque da organização e potencializando as vulnerabilidades. Este cenário complica a conformidade com normas e padrões de segurança, expondo a organização a riscos elevados de ataques cibernéticos e violações de dados.

A responsabilização e o suporte técnico também se tornam complexos em um cenário de contratações fragmentadas. A distribuição de responsabilidades entre diferentes fornecedores pode levar a dificuldades na resolução de problemas, uma vez que cada fornecedor pode tentar desviar a culpa para outro, complicando a identificação e correção de falhas. Esse cenário resulta em um tempo de resposta e resolução mais longo, aumentando o tempo de inatividade e prejudicando a experiência dos nossos usuários e serviços prestados.

A fragmentação das contratações pode criar barreiras à inovação e à escalabilidade. A dependência de múltiplos fornecedores pode restringir a capacidade da organização de adotar novas tecnologias e inovações, limitando sua flexibilidade e capacidade de resposta às mudanças do mercado. Essa limitação pode impedir o DPE-PA de explorar oportunidades estratégicas de crescimento e inovação.

Portanto, embora a separação das contratações em lotes distintos possa parecer vantajosa a princípio, as consideráveis desvantagens e riscos associados destacam a importância de optar por uma abordagem mais consolidada. Escolher um fornecedor único capaz de oferecer uma solução integrada é uma estratégia que pode mitigar esses riscos, proporcionando benefícios substanciais em termos de eficiência operacional, segurança e retorno sobre o investimento. Para o DPE-PA, adotar essa abordagem significa não apenas simplificar a gestão de suas contratações, mas também assegurar a resiliência, a segurança e a capacidade de inovação necessárias para atender às suas demandas operacionais e estratégicas.

Incorporando essa consideração adicional, a argumentação sobre a problemática da segmentação das contratações em lotes distintos pela Defensoria Pública do Estado do Pará (DPE-PA) ganha ainda mais peso. A subdivisão das contratações em lotes ou processos distintos não somente acarreta as desvantagens e riscos anteriormente mencionados, mas também introduz a complicação adicional relacionada aos prazos das contratações e à possibilidade de não haver vencedores em determinados lotes ou processo, devido a eventualidades.

A divergência nos tempos de contratação entre os diferentes lotes é um ponto crítico que pode gerar atrasos e descoordenação na implementação das soluções tecnológicas. Cada lote, ao seguir seu próprio cronograma, pode enfrentar tempos de entrega distintos, resultando em uma implantação fragmentada e desalinhada das soluções. Esse descompasso compromete não apenas a eficiência da gestão do projeto como um todo, mas também impacta a operacionalidade da Defensoria, podendo atrasar a disponibilização de serviços críticos para o público.

Além disso, a possibilidade de não se identificar vencedores para determinados lotes, seja por insuficiência de propostas qualificadas, questões jurídicas ou falhas no processo licitatório, introduz um risco significativo de interrupção ou atraso na execução do projeto como um todo, até mesmo a não finalização. Tal cenário pode exigir a realização de novos processos licitatórios, prolongando ainda mais os prazos de

implementação e potencializando os custos associados, sem contar o impacto direto nas operações da Defensoria e na entrega de seus serviços à população.

Para atender às demandas do DPE-PA é crucial compreender as implicações da divisão de contratações em lotes distintos em um edital. Embora esta estratégia possa inicialmente parecer uma forma de otimizar custos e eficiência, ela introduz uma série de desvantagens e riscos que podem comprometer significativamente a operacionalidade, a segurança e a capacidade de integração das tecnologias adotadas pela organização.

Nesta esteira, além da interdependência entre os hardwares, software e serviços acessórios devem ser fornecidos por uma única empresa, pois é incoerente no caso desta contratação, que a empresa que forneça a solução e faça sua instalação seja diversa da que prestará o suporte técnico, treinamento e serviços de manutenções evolutivas.

Além disso o agrupamento dos itens em Lote Único é imprescindível, pois em se tratando de gestão contratual torna-se inviável que os serviços acessórios como neste caso sejam fornecidos por diferentes fornecedores, dado que traz maior complexidade, custo de gestão e controle da DEFENSORIA PÚBLICA.

Em se tratando do viés econômico, o parcelamento dos serviços acessórios do objeto pode impactar diretamente os custos da contratação, considerando que a execução desses serviços por uma única empresa se traduz em diluição do custo administrativo, possibilitando menor preço global.

Todas essas razões inviabilizam a deflagração de mais de um procedimento licitatório.

Isso também porque, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

DA FUNDAMENTAÇÃO LEGAL

A presente licitação, que trata da aquisição objeto deste Termo de Referência e seus anexos, será realizada conforme regulamentação da Lei nº Lei nº 14.133/2021, na modalidade PREGÃO ELETRÔNICO do tipo SRP – SISTEMA DE REGISTRO DE PREÇOS.

Os serviços que constituem o objeto deste Termo de Referência enquadram- se no conceito de serviço comum, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

Vedação à participação de consórcios. Quando o objeto a ser licitado envolve questões de alta complexidade, via de regra, a Administração, com intuito de aumentar o número de participantes, admite a formação de consórcio. No entanto, no contexto em análise, essa hipótese não se aplica, pois, o objeto pretendido, Proteção e Gerenciamento Seguro da rede LAN/WLAN/WAN está consolidado no mercado e no âmbito da Administração Pública, vez que são serviços comuns prestados por diversas empresas atualmente.

Destaca-se que a participação de consórcios em processos licitatórios com esse objeto, além de não garantir o aumento de competitividade, poderá causar prejuízos à Administração Pública na sustentação dos serviços em casos de dificuldades operacionais de um dos consorciados, sobrecarregando os demais participantes.

A DEFENSORIA PÚBLICA espera como resultado deste processo, contar com fornecedor único para o processo de atendimento às demandas, com ampla experiência na execução de atividades operacionais e gerenciais de atendimento, suportadas por ferramentas e processos adequados e aderentes às necessidades de informações, gestão administrativa, execução interna

da licitação e execução de contratos e projetos das diversas áreas gestoras do Órgão, facilitando assim o processo de integração de dados e informações vitais ao desenvolvimento da Administração Pública.

Neste modelo de serviço, o atendimento das demandas deve ser estabelecido de forma estruturada e padronizada, de maneira a evitar os riscos operacionais, motivos pelos quais se optou pela vedação da participação de consórcio.

Outra desvantagem em que o consórcio poderá gerar complicações para a Unidade com relação à gerência e garantia da perfeita execução do contrato e a gestão e fiscalização da execução contratual seriam prejudicadas pela dificuldade em lidar com empresas que possuem processos de trabalhos diferentes e remunerações desiguais por profissionais alocados com atribuições similares.

Em relação ao escopo do objeto, é possível a ampla participação de empresas atuantes no mercado, que de forma isolada, consigam atender às condições e os requisitos de habilitação previstos neste documento.

DOS REQUISITOS TÉCNICOS

O presente TERMO DE REFERÊNCIA visa a aquisição de Solução para proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede. Os detalhamentos dos demais requisitos técnicos e funcionais mínimos obrigatórios estão a seguir:

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS (PACOTE 5G/LOG DIA)	5
8	SWITCH CONCENTRADOR (CORE)	4
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20
13	SWITCH DE ACESSO 8 PORTAS POE	77
14	PONTO DE ACESSO - TIPO 01	155
15	PONTO DE ACESSO - TIPO 02	80
16	TRANSCEIVER SFP+ 10GBASE-T	50
17	TRANSCEIVER SFP+ 10GBASE-SR	50
18	TRANSCEIVER SFP+ 10GBASE-LR	50
19	CONTROLE DE ACESSO A REDE (NAC)	1
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	02
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229
25	SERVIÇOS DE INSTALAÇÃO DE APs	235
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16

KIT SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPOS 01 A 04

A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. 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;

Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

O fornecedor deverá comprovar que é representante, revenda autorizada ou distribuidor devidamente registrado no Brasil e autorizado pelo fabricante para ofertar, fornecer e prestar serviços especializados nos produtos.

Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, IPS, Threat Prevention, DNS Security, DLP, análise e prevenção de malware avançado, URL Filtering, AntiMalware, Anti-bot, AntiSpam, detecção e prevenção de intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, contextos virtuais e SD-WAN como parte integrante dos produtos.

Os desempenhos solicitados para cada tipo de NGFW deverão ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes como comprovação destes itens de desempenho.

Todos os equipamentos e licenças fornecidos deverão ser novos, atuais, de primeiro uso e não constar de listas de End of Life (EOL) ou End of Support (EOS) do fabricante.

Todos os equipamentos deverão ser homologados pela ANATEL.

FUNCIONALIDADES DE REDE E FIREWALL

O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

Os dispositivos de proteção de rede devem possuir suporte a Vlans;

Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (*Network Address Translation*), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Deverá suportar sFlow ou Netflow;

Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

Deve suportar o protocolo padrão da indústria VXLAN;

Deve implementar o protocolo ECMP;

Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

Enviar log para sistemas de monitoração externos;

Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

Deve possui mecanismos de proteção anti-spoofing;

Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

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

Suportar OSPF graceful restart;

Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

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

O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

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

Deverá suportar controle por zonas de segurança;

Deverá suportar controles de políticas por porta e protocolo;

Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

Suporte a objetos e regras IPV6;

Suporte a objetos e regras multicast;

Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

FUNCIONALIDADE DE 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 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

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;

Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

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 utilização da rede Tor;

Para tráfego criptografado SSL, deve decriptografar 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;

Identificar o uso de táticas evasivas via comunicações criptografadas;

Atualizar a base de assinaturas de aplicações automaticamente;

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 múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

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;

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 a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

Deve permitir forçar o uso de portas específicas para determinadas aplicações;

FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

Deve permitir o bloqueio de vulnerabilidades;

Deve permitir o bloqueio de exploits conhecidos;

Deve incluir proteção contra-ataques de negação de serviços;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

Detectar e bloquear a origem de portscans;

Bloquear ataques efetuados por worms conhecidos;

Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

Possuir assinaturas para bloqueio de ataques de buffer overflow;

Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

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

Identificar e bloquear comunicação com botnets;

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

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

Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

As funcionalidades de IPS, Antivírus e Anti-Spyware 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 e caso o licenciamento/funcionalidade não seja permanente, o fornecedor deverá prover as funcionalidades por mais 12 (doze) meses;

Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

Possuir pelo menos 70 (setenta) categorias de URLs;

Deve possuir a função de exclusão de URLs do bloqueio;

Permitir a customização de página de bloqueio;

Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

FUNCIONALIDADE DE IDENTIFICAÇÃO DE 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, eDirectory e base de dados local;

Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de 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);

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

Deve suportar o envio e recebimento de credenciais via RADIUS;

Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

FUNCIONALIDADE DE FILTRO DE DADOS

Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

Suportar a identificação de arquivos criptografados e a aplicação de políticas 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.

FUNCIONALIDADE DE GEOLOCALIZAÇÃO

Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

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

FUNCIONALIDADE DE VPN

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

Suportar IPSec VPN;

Suportar SSL VPN;

A VPN IPSEc deve suportar 3DES;

A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

Deve permitir habilitar e desabilitar 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 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;

Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

Suportar leitura e verificação de CRL (Certificate Revocation List);

Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

Deverá manter uma conexão segura com o portal durante a sessão;

O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 8.1 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 e Mac OS X (v10.10 ou superior), CentOS (7 ou superior), Redhat (7 ou superior), Fedora (27 ou superior), Ubuntu (16.04 ou superior), e Android e iOS;

FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, 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 e Traffic Shaping para os seguintes itens:

Endereço de origem;

Endereço de destino;

Usuário e grupo;

Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

Por porta;

O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

O QoS deve possibilitar a definição de fila de prioridade;

Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

Suportar marcação de pacotes Diffserv, inclusive por aplicação;

Suportar modificação de valores DSCP para o Diffserv;

Suportar priorização de tráfego usando informação de ToS (Type of Service);

Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

Deve possibilitar a definição de bandas distintas para download e upload;

FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

A solução deve ser capaz de agregar vários links em uma interface virtual;

A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

A solução deve suportar nativamente conectores com clouds públicas;

Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

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 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, três links;

O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos

deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo,

Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;

A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de

sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

A solução deve permitir a configuração do captive portal com endereço IPv6;

A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna.

A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

A solução deve possuir ferramentas de diagnósticos e debug;

A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

A solução deve suportar comunicação com elementos externos através de REST API;

A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

Deve montar a topologia da rede de maneira automática;

Deve ser capaz de configurar os switches da rede;

Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

Deve ser capaz de configurar parâmetros SNMP dos switches;

A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

Deve prover indicadores de saúde dos elementos críticos do ambiente;

Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

ITEM 01 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01

Deve suportar, no mínimo, 12 (doze) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;

Deve suportar, no mínimo, 7 (sete) milhões de conexões simultâneas;

Deve suportar, no mínimo, 370.000 (trezentos e setenta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 40 (quarenta) Gbps de desempenho VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 12.000 (doze mil) túneis de clientes Global Protect Client VPN simultâneos e caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total do mesmo fabricante;

Deve suportar, no mínimo, 18 (dezoito) Gbps de throughput de IPS;

Deve suportar, no mínimo, 6 (seis) Gbps de throughput de Inspeção SSL;

Deve possuir latência de firewall menor que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.

Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet 10GBase-T com conectores RJ-45;

Deve possuir, pelo menos, 8 (oito) interfaces com suporte a SFP de 1 Gigabit Ethernet;

Deve possuir, pelo menos, 8 (oito) interfaces com suporte a SPF+ de 10 Gigabit Ethernet;

Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP28 de 25 Gigabit Ethernet;

Deve possuir, pelo menos, 2 (duas) interfaces com suporte a conectores QSFP28 de 100 Gigabit Ethernet;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;

Deve estar licenciado para gerenciar até 150 (cem e cinquenta) switches e 500 (quinhentos) pontos de acesso sem fio simultaneamente em um único appliance;

Deve suportar, no mínimo, de 4094 (quatro mil e noventa e quatro) VLANs;

Deve possuir, pelo menos, 01 (uma) interface dedicada para gerenciamento segregada das interfaces de tráfego de dados da rede corporativa;

Deve possuir fonte de alimentação AC redundante e HotSwap;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 02 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02

Deve suportar, no mínimo, 3 (três) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6.

Deve suportar, no mínimo, 3 (três) milhões de conexões simultâneas;

Deve suportar, no mínimo, 250.000 (duzentas e cinquenta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 15 (quinze) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentas) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.500 (mil e quinhentos) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;

Deve suportar, no mínimo, 05 (cinco) Gbps de throughput de IPS;

Deve suportar, no mínimo, 02 (dois) Gbps de throughput de Inspeção SSL;

Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.

Deve possuir, pelo menos, 12 (doze) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;

Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;

Deve estar licenciado para gerenciar até 60 (sessenta) switches e 120 (cento e vinte) pontos de acesso sem fio simultaneamente em um único appliance;

Deve possuir fonte de alimentação AC redundante;

Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 03 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL PRÓXIMA GERAÇÃO (NGFW) - TIPO 03

Deve suportar, no mínimo, 1 (um) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;

Deve suportar, no mínimo, 1.5 Milhão (um milhão e quinhentas mil) conexões simultâneas;

Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 08 (oito) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 150 (cento e cinquenta) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam incluídas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;

Deve suportar, no mínimo, 02 (dois) Gbps de throughput de IPS;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de Inspeção SSL;

Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.

Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve possuir, pelo menos, 08 (oito) interfaces Gigabit Ethernet com conectores SFP;

Deve possuir, pelo menos, 02 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+;

Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;

Deve estar licenciado para gerenciar até 30 (trinta) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;

Deve possuir fonte de alimentação AC redundante;

Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 04 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) – TIPO 04

Deve suportar, no mínimo, 700 (setecentos) Mbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;

Deve suportar, no mínimo, 500.000 (quinhentos mil) conexões simultâneas;

Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;

Deve Suportar, no mínimo, 5 (cinco) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;

Deve suportar, no mínimo, 500 (quinhentos) Mbps de throughput de Inspeção SSL;

Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.

Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;

Deve estar licenciado para gerenciar até 20 (vinte) switches e 30 (trinta) pontos de acesso sem fio simultaneamente em um único appliance;

Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 05 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05

Deve suportar, no mínimo, 500 (quinhentos) Mbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;

Deve suportar, no mínimo, 500.000 (quinhentos mil) conexões simultâneas;

Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 04 (quatro) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;

Deve suportar, no mínimo, 300 (trezentos) Mbps de throughput de Inspeção SSL;

Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.

Deve possuir, pelo menos, 05 (cinco) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;

Deve estar licenciado para gerenciar até 04 (quatro) switches e 08 (oito) pontos de acesso sem fio simultaneamente em um único appliance;

Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 06 - GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO

Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;

A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;

Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);

Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

Permitir usar palavras chaves ou cores para facilitar identificação de regras;

Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

Permitir criação de regras que fiquem ativas em horário definido;

Permitir criação de regras com data de expiração;

Realizar o backup das configurações para permitir o retorno de uma configuração salva;

Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.

Gerar alertas automáticos via Email, SNMP e Syslog;

Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.

Permitir backup das configurações e rollback de configuração para a última configuração salva;

Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;

Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;

Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.

A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

Deve suportar o gerenciamento de pontos de acesso de forma centralizada.

Deve suportar o gerenciamento centralizado de switches.

A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.

ITEM 07 - GERENCIAMENTO DE LOGS E RELATÓRIOS CENTRALIZADO

Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

A solução deve suportar receber, no mínimo, 5 (cinco) GB de logs diários;

A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;

Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

Possuir suporte para SNMP versão 2 e 3;

Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

Deve permitir gerar alertas de eventos a partir de logs recebidos;

A solução deve ter relatórios predefinidos;

Permitir importação e exportação de relatórios

Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

Deve possuir mecanismos de remoção automática para logs antigos;

Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

Permitir o envio por e-mail relatórios automaticamente;

Deve permitir que o relatório seja enviado por Email para o destinatário específico;

Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

Deve permitir o uso de filtros nos relatórios;

Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

Permitir especificar o idioma dos relatórios criados;

Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

Deve permitir exportar os logs no formato CSV;

Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

Deve permitir visualizar em tempo real os logs recebidos;

Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

Deve possuir relatório de uso de aplicações e mídias sociais;

Deve possuir relatório de prevenção de perda de dados (DLP);

Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

Deve possuir relatório diário resumido de eventos e incidentes de segurança;

Deve possuir um relatório de tráfego DNS e e-mail;

Deve possuir relatório das 10 principais aplicações utilizadas na rede;

Deve possuir relatório dos 10 principais sites web utilizados na rede;

Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

Deve suportar recursos de automação (*playbooks*) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

ITEM 08 – SWITCH CONCENTRADOR (CORE)

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;

Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;

Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

Deve possuir 1 (uma) interface USB;

Deve possuir capacidade de comutação de pelo menos 1.76 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.5 Bpps (bilhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;

Deve possuir tabela MAC com suporte a 144.000 endereços;

Deve operar com latência igual ou inferior à 1us (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;

Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol - LACP);

Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;

Deve suportar a comutação de Jumbo Frames;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;

Deve implementar serviço de DHCP Server e DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;

Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve suportar o protocolo PTP (Precision Time Protocol);

Deve implementar Netflow, sFlow ou similar;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve possuir ferramenta para captura de pacotes que auxíliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;

Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 40º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

Deve ser fornecido com cabo DAC (Direct Attach Cable) 40GbE QSFP+ de 3 metros;

ITEM 09 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 01

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 180W;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir 1 (uma) interface USB;

Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve possuir tabela MAC com suporte a 32.000 endereços;

Deve operar com latência igual ou inferior à 1us (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

Deve suportar a comutação de Jumbo Frames;

Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve implementar serviço de DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 45º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 10 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 02

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir 1 (uma) interface USB;

Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve possuir tabela MAC com suporte a 32.000 endereços;

Deve operar com latência igual ou inferior à 1us (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

Deve suportar a comutação de Jumbo Frames;

Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve implementar serviço de DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 45º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 11 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 01

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir 1 (uma) interface USB;

Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve possuir tabela MAC com suporte a 32.000 endereços;

Deve operar com latência igual ou inferior à 1us (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

Deve suportar a comutação de Jumbo Frames;

Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve implementar serviço de DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 45º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 12 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 02

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 740W a serem alocados em qualquer uma das portas 1000Base-T;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir 1 (uma) interface USB;

Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve possuir tabela MAC com suporte a 32.000 endereços;

Deve operar com latência igual ou inferior à 1us (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

Deve suportar a comutação de Jumbo Frames;

Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve implementar serviço de DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 45º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 13 - SWITCH DE ACESSO 8 PORTAS POE

Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

Deve possuir 08 (oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

Adicionalmente, deve possuir 02 (dois) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 65W;

Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

Deve possuir capacidade de comutação de pelo menos 20 Gbps e ser capaz de encaminhar até 25 Mpps (milhões de pacotes por segundo);

Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

Deve possuir tabela MAC com suporte a 8.000 (oito mil) endereços;

Deve operar com latência igual ou inferior à 4 µs (microsegundo);

Deve implementar Flow Control baseado no padrão IEEE 802.3X;

Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

Deve suportar a comutação de Jumbo Frames;

Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

Deve implementar serviço de DHCP Relay;

Deve suportar IGMP snooping para controle de tráfego de multicast;

Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

Deve suportar MAC Authentication Bypass (MAB);

Deve implementar RADIUS CoA (Change of Authorization);

Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

Deve suportar o envio de mensagens de log para servidores externos através de syslog;

Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

Deve permitir ser gerenciado através de IPv6;

Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

Deverá suportar ser configurado e monitorado através de REST API;

Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

Deve suportar temperatura de operação de até 45º Celsius;

Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

ITEM 14 - PONTO DE ACESSO SEM FIO - TIPO 01

Ponto de acesso (AP) que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;

Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve identificar automaticamente o controlador wireless ao qual se conectará;

Deve permitir ser gerenciado remotamente através de links WAN;

Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

Deve permitir operação em modo Mesh;

Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

Deve suportar OFDMA;

Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

Deve suportar BSS Coloring;

Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;

Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

Deve implementar o padrão IEEE 802.11e;

Deve implementar o padrão IEEE 802.11h;

Deve implementar o padrão IEEE 802.3az;

Deve suportar ser gerenciado via SNMP;

Deve suportar consultas via REST API;

Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

Deve possuir indicadores luminosos (LED) para indicação de status;

O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

Deve possuir certificado emitido pela Wi-Fi Alliance;

Deve estar homologado pela ANATEL na data de execução do pregão;

ITEM 15 - PONTO DE ACESSO SEM FIO - TIPO 02

Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;

Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

Deve identificar automaticamente o controlador wireless ao qual se conectará;

Deve permitir ser gerenciado remotamente através de links WAN;

Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN;

Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento;

O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

Deve permitir operação em modo Mesh;

Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz;

Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;

Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);

Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

Deve implementar recurso de Target Wake Time (TWT) configurado por SSID;

Deve suportar BSS Coloring;

Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);

Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz;

Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea;

Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X;

Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

Deve implementar o padrão IEEE 802.11e;

Deve implementar o padrão IEEE 802.11h;

Deve implementar o padrão IEEE 802.3az;

Deve suportar consultas SNMP diretamente no ponto de acesso;

Deve suportar consultas REST API diretamente no ponto de acesso;

Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes;

Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C;

O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção;

Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi;

O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

Deve possuir certificado emitido pela Wi-Fi Alliance;

Deve estar homologado pela ANATEL na data de execução do pregão;

ITEM 16 - TRANSCEIVER SFP+ 10GBase-T

Transceiver SFP+ compatível com o padrão 10GBase-T para cabos de par trançado (cobre) de até 30 metros;

Deve possuir conector RJ-45;

Deve ter velocidade de 10GbE;

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 17 - TRANSCEIVER SFP+ 10GBase-SR

Transceiver SFP+ para conexão de fibras ópticas multimodo;

Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m (fibra OM3) e fibras ópticas de até 400m (fibra OM4);

Deve ter velocidade de 10GbE;

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 18 - TRANSCEIVER SFP+ 10GBase-LR

Transceiver SFP+ para conexão de fibras ópticas monomodo;

Deve ser compatível com o padrão 10GBase-LR para fibras ópticas de até 10km;

Deve possuir conector LC;

Deve ter velocidade de 10GbE;

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 19 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE

CARACTERÍSTICAS GERAIS

Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;

Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;

Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;

A solução deve suportar capacidade de expansão para até 2.000 (dois mil) endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;

A solução deve estar licenciada para operação com, pelo menos, 400 (quatrocentos) endpoints conectados simultaneamente;

A solução deve ser entregue em alta disponibilidade;

A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;

A licença contemplada deverá suportar todas as características exigidas neste termo de referência;

A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;

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

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

Consultas em DHCP Fingerprint;

Consultas via protocolos HTTP/HTTPS;

Consultas via protocolo SNMP;

Consultas via protocolo SSH;

Consultas via protocolo Telnet;

Consultas de portas TCP;

Consultas de portas UDP;

MAC OUI;

Consultas via protocolo WMI;

Protocolo ONVIF;

Protocolo NetFlow;

Base assinaturas pré-definidas;

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

Endereço MAC;

Endereço IP;

Sistema operacional;

Nome do host;

Horário de conexão;

Usuário conectado;

Localização.

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

Android;

Apple iOS para iPhone, iPod e iPad;

Chrome OS;

Linux;

MacOS X;

Windows 7, 8 e 10;

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

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

Deve permitir a recategorização periódica de dispositivos;

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

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

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

A solução deve suportar RADIUS Change of Authorization;

A solução deve suportar MAC Address Bypass;

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

A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;

Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;

Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;

A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;

A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

Deve permitir a definição de complexidade da senha dos usuários visitantes;

Deve ser possível definir um período de validade para as contas de usuários visitantes;

Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

A solução deve vincular o login do visitante à máquina utilizada no acesso;

Deve suportar a validação de credenciais:

Em base local interna à ferramenta;

Em servidores RADIUS;

Em servidores LDAP.

A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;

A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;

Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;

Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;

A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;

Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

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

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

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

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

Não forçar a remediação;

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

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

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

Windows 7;

Windows 8;

Windows 10;

MacOS;

Linux.

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

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

Versão do sistema operacional;

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

Serviços em execução para estações Windows;

Informações sobre um determinado certificado digital em estações Windows;

Registros ou chaves de registro para estações Windows;

Processos em execução para estações Windows, Linux e MacOS;

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

Pacotes instalados em estações Linux e MacOS.

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

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

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

Programas de gerenciamento e distribuição de software;

GPO do Active Directory;

Captive Portal;

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

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

Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

Deve suportar integração com soluções de patching;

Deve suportar integração com soluções de análise de vulnerabilidades;

A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

A solução deve armazenar os eventos internamente e permitir que sejam exportados;

A solução deve permitir a exportação dos eventos através de syslog;

Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;

A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;

Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

Caso o CONTRATANTE não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor inclui-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;

Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

ITEM 20 – TREINAMENTO DAS SOLUÇÕES

CARACTERÍSTICAS GERAIS DOS TREINAMENTOS

Treinamento com material oficial das soluções fornecidas.

Deverá ser abordado conceitos teóricos e atividades práticas de laboratório;

Todos os treinamentos deverão ser realizados de forma presencial ou híbrida (quando a DPE autorizar);

O idioma das aulas deverá ser em português;

Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.

Ao final do treinamento deverá ser emitido certificado de conclusão a cada participante, devidamente assinado pela empresa promovente, especificando conteúdo programático completo do curso, corpo docente e carga horária.

O treinamento pode ser separado conforme o produto a ser instalado no ambiente da Contratante, contendo ao menos os seguintes módulos:

Descrição e configuração de todas as funcionalidades contratadas da solução;

Resolução de problemas – troubleshooting;

Melhores práticas utilizadas no mercado para aproveitamento dos hardwares e softwares e suas funcionalidades.

O treinamento terá um total de cinco (5) participantes definidos pela Contratante;

O material didático fornecido deve abordar todos os tópicos do curso;

A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;

É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;

Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pela Contratante, o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE FIREWALLS DE PRÓXIMA GERAÇÃO

Carga horária mínima de 36 (trinta e seis) horas;

Deverá ser abordado, no mínimo, os seguintes tópicos:

Configurações iniciais e avançadas;

Configurações de VLANs, LACP, DHCP e tipos de NAT;

Políticas de segurança;

Prevenção de ameaças, anti-malware, filtro URL e controle de aplicações;

Identificação de usuários, qualidade de serviço e regras por aplicação;

Filtro de dados;

VPN Site-to-Site e Client-To-Site;

ZTNA;

Análise de malwares modernos;

Alta disponibilidade;

Gerenciamento centralizado e relatórios;

Avaliação de boas práticas;

Otimização de políticas de firewall.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO

Carga horária mínima de 12 (doze) horas;

Deverá ser abordado, no mínimo, os seguintes tópicos:

Configurações iniciais e avançadas;

Instalação, gerenciamento e administração de dispositivos, políticas e objetos;

Configuração e administração de instâncias de virtualização;

Diagnóstico e resolução de problemas.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS

Carga horária mínima de 12 (doze) horas;

Deverá ser abordado, no mínimo, os seguintes tópicos:

Configurações iniciais e avançadas;

Configuração, visualização e gerenciamento de logs;

Configuração, visualização e gerenciamento de relatórios;

Gerenciamento de eventos, incidentes e recursos de automação (playbooks);

Configuração e administração de instâncias de virtualização.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DE ADMINISTRAÇÃO DE SWITCHES E PONTOS DE ACESSO

Carga horária mínima de 24 (vinte e quatro) horas;

Deverá ser abordado, no mínimo, os seguintes tópicos:

Fundamentos básicos de switches e pontos de acesso;

Configurações iniciais e avançadas de switches e pontos de acesso;

Gerenciamento de controlador wireless;

Configuração de autenticação 802.1X, com VLANs dinâmicas;

Priorização de tráfego;

Monitoramento, diagnóstico e resolução de problemas.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC)

Carga horária mínima de 16 (dezesseis) horas;

Deverá ser abordado, no mínimo, os seguintes tópicos:

Configurações iniciais e visibilidade de rede;

Identificação e Classificação de Dispositivos Não Autorizados;

Controle Baseado em Estado;

Políticas de Segurança;

Gerenciamento de convidados e de terceiros;

Integração de dispositivos de segurança e resposta automatizada;

Alta disponibilidade;

Monitoramento, diagnóstico e resolução de problemas.

ITEM 21 – SERVIÇO DE SUPORTE PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS, PRÓ-ATIVOS E RESPOSTAS A INCIDENTES:

A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças;

Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);

Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:

Orientações sobre uso, configuração e instalação do software ofertado;

Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

Interpretação da documentação do software ofertado;

Orientações para identificar a causa de uma falha de software;

Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado;

Orientação quanto às melhores práticas para implementação do software adquirido;

Apoio na recuperação de ambientes em caso de panes ou perda de dados;

Apoio para execução de procedimentos de atualização para novas versões do software instalado;

A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.

Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações da DPE/PA, em qualquer horário, respeitando as condições e níveis de serviços especificados a seguir:

SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;

SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;

SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.

Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado, o qual será classificado conforme as severidades especificadas no item anterior.

Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

SEVERIDADE	ATENDIMENTO	SOLUÇÃO / PALIATIVO
ALTA	4 (QUATRO) HORAS	12 (DOZE) HORAS
MÉDIA	6 (SEIS) HORAS	24 (VINTE E QUATRO) HORAS
BAIXA	24 (VINTE E QUATRO) HORAS	48 (QUARENTA E OITO) HORAS
LOCAIS REMOTOS	96 (NOVENTA E SEIS) HORAS	120 (CENTO E VINTE) HORAS

Para os chamados severidade LOCAIS REMOTOS (paralisação TOTAL das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 96 (noventa e seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 120 (centro e vinte) horas corridas a contar do início do atendimento.

Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 6 (seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 24 (vinte e quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 48 (quarenta e oito) horas corridas a contar do início do atendimento.

Para os chamados de qualquer severidade, a critério da DPE/PA, poderá ser agendado o melhor horário para atendimento.

O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia à DPE/PA quanto à efetiva solução do problema.

Qualquer chamado fechado, sem anuência da DPE/PA ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

A Contratada manterá cadastro das pessoas indicadas pela DPE/PA que poderão efetuar abertura e autorizar o fechamento de chamados.

A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

Data e hora da abertura do chamado;

Data e hora do início do atendimento;

Responsável pelo atendimento da solicitação;

Motivo da ocorrência (indicação do defeito);

Status do chamado (aberto, em tratamento, fechado etc.);

Data e hora do fechamento do chamado;

Solução adotada (resolução);

O atendimento de suporte para a solução deverá ser do tipo 8 x 5 (oito horas por dia, cinco dias por semana), e deverá ser realizado por profissionais especializados.

Não haverá limite para o número de chamados de suporte técnico.

Nos casos em que as manutenções necessitarem de paradas do ambiente, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

ITENS 22 A 25 – SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS

Caso ocorra alguma divergência entre as especificações técnicas constantes na tabela com aquelas lançadas no sistema eletrônico (Comprasnet), prevalecerá o constante neste instrumento;

O prazo de vigência da contratação é de 36 (trinta e seis), conforme vier a constar do(s) contrato(s) ou instrumento substituto (se for o caso).

Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE;

No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:

Planejamento da instalação incluindo identificação de pré-requisitos;

Instalação e configuração do módulo de gerenciamento central;

Criar a senha de acesso com privilégio Administrativo para a Contratante.

Instalação e configuração dos hardwares e softwares;

Realizar customizações caso sejam solicitadas ou necessárias;

Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;

Realizar backup das configurações;

Documentar todas as configurações realizadas no ambiente.

Os serviços de instalação serão para os seguintes itens:

SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1

SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5

SERVIÇOS DE INSTALAÇÃO DE SWITCHES

SERVIÇOS DE INSTALAÇÃO DE APs

SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19

Após a conclusão da instalação e implantação, a solução deverá ser formalmente homologada pela Contratante, o qual possuirá o prazo de 5 (cinco) dias consecutivos contados a partir da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite). O conteúdo do treinamento deve abordar os assuntos de natureza teórica e prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

A instalação e configuração, serviços opcionais, deverá ocorrer em até 15 (quinze) dias corridos, contados a partir da data de entrega da ordem de serviço. Para as unidades que optarem pelo saque do referido serviço, esse prazo deverá constar na cláusula da Minuta contratual.

Para as unidades que contratarem o serviço de “Instalação para Equipamentos na capital e em localidades com distância até 200 km da Capital ou superior a 200 km da Capital” a entrega efetiva está condicionada a conclusão da instalação e configuração dos equipamentos;

A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

O serviço de instalação consiste na acomodação física, incluindo patch cord e configuração lógica dos equipamentos;

Caberá à CONTRATADA a disponibilização de todos os recursos necessários, como hardware, software e recursos humanos necessários à execução dessa atividade;

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção individual, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

No tocante a equipamentos, periféricos, acessórios, técnicos de instalação, técnicos de manutenção, translado, transporte, estada, embalagens, necessários à execução da instalação e assistência técnica deverão ser de responsabilidade da CONTRATADA e não deverão gerar qualquer ônus à CONTRATANTE;

No processo de instalação o Responsável Técnico da CONTRATADA deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração).

DA ENTREGA E DO RECEBIMENTO

Quanto à entrega:

O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento no prazo máximo de 30 (trinta) dias, contado a partir da assinatura do contrato, recebimento da ordem de serviço, ordem de fornecimento ou instrumento hábil.

Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

Quanto ao recebimento:

PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela contratante.

DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

DO PAGAMENTO

O pagamento será efetuado, em até 30 (trinta) dias, pelo Departamento Financeiro do DPE/PA, devendo a Contratada apresentar a respectiva Nota Fiscal/Fatura, emitidos de acordo com a legislação vigente, a partir da qual se contará o prazo para pagamento.

Os pagamentos serão efetuados através de crédito aberto em conta corrente da Contratada.

O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na Nota Fiscal apresentada.

No caso de atraso no pagamento por culpa do Contratante, os valores devidos serão acrescidos de encargos financeiros de 1% (hum por cento) ao mês, calculados “pro rata die” até a data do efetivo pagamento.

No preço contratado estão incluídas todas e quaisquer despesas com mão-de-obra, material de consumo, equipamentos, treinamentos, prêmios de seguro, taxas, inclusive de administração, emolumentos e quaisquer despesas operacionais, bem como todos os encargos trabalhistas, previdenciários, fiscais e

comerciais, despesas e obrigações financeiras de qualquer natureza e outras despesas diretas e indiretas necessárias à perfeita execução do objeto DO CONTRATO, além de auxílio alimentação ou refeição, vale-transporte e quaisquer outras vantagens pagas aos empregados, enfim, todos os componentes de custo dos serviços, inclusive o lucro.

Quando houver erro, de qualquer natureza na emissão da nota fiscal/fatura, o documento será devolvido, imediatamente, para substituição e/ou emissão de nota de correção, não devendo ser computado nesse intervalo de tempo, para efeito de qualquer reajuste ou atualização do valor contratado;

Nota Fiscal apresentada para pagamento deverá ser emitida com o mesmo número do CNPJ participante da licitação e da Nota de Empenho;

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

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

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

Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada o direito ao contraditório e ampla defesa.

DAS SANÇÕES ADMINISTRATIVAS

Comete infração administrativa, nos termos da Lei no 14.133, de 2021, o Contratado que:

der causa à inexecução parcial do contrato;

der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

der causa à inexecução total do contrato;

deixar de entregar a documentação exigida para o certame;

não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato;

fraudar a contratação ou praticar ato fraudulento na execução do contrato;

comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

Multa:

moratória de 1 % (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto ou sobre o valor da parcela inadimplida, no caso de inexecução parcial;

A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante;

Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa;

Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação;

Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente;

Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei no 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

Na aplicação das sanções serão considerados:

a natureza e a gravidade da infração cometida;

as peculiaridades do caso concreto;

as circunstâncias agravantes ou atenuantes;

os danos que dela provierem para a Contratante;

a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

Os atos previstos como infrações administrativas na Lei no 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei no 12.846, de 2013, serão apurados

e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159)

A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia;

A Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal;

As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei no 14.133/21.

DAS OBRIGAÇÕES DA CONTRATADA

Executar o objeto em conformidade com as condições deste instrumento.

Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no art. 125, da Lei Federal nº 14.133/21, tomando-se por base o valor contratual.

Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo DPE/PA, contado da sua notificação.

Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da contratante.

Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria n.º 3.460/77, do Ministério do Trabalho, relativos à segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.

DAS OBRIGAÇÕES DA CONTRATANTE

Solicitar a execução do objeto à contratada através da emissão de Ordem de Serviço / Ordem de Fornecimento.

Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 14.133/21 e suas alterações.

Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

Aplicar as penalidades previstas em lei e neste instrumento.

DA FISCALIZAÇÃO

O CONTRATANTE, por meio do setor competente, exercerá ampla fiscalização sobre a execução do contrato, ficando a CONTRATADA obrigada a facilitar o exercício desse direito.

O servidor do DPE/PA designado para atuar como fiscal do contrato terá, dentre outras, as seguintes atribuições:

O fiscal designado pelo DPE/PA anotará, em registro próprio, todas as ocorrências relacionadas com a execução do contrato, inclusive quanto à observância do prazo de vigência do mesmo e aos pagamentos efetuados pelo DPE/PA, determinando o que for necessário à regularização das faltas ou defeitos existentes e encaminhar cópia à CONTRATADA para a imediata correção das irregularidades apontadas, sem prejuízo das penalidades previstas neste contrato e na lei.

As decisões e providências que ultrapassarem a competência deste fiscal deverão ser encaminhadas, em tempo hábil, ao superior para adoção das medidas necessárias e/ou convenientes.

Conferir se a aquisição está de acordo com as especificações técnicas exigidas.

Rejeitar no todo ou em parte os bens entregues, se considerados em desacordo ou insuficientes, conforme os termos discriminados na proposta da CONTRATADA e no Termo de Referência do Edital.

A fiscalização da contratação pelo CONTRATANTE não exime, nem diminui a completa responsabilidade da CONTRATADA, por qualquer inobservância ou omissão às cláusulas contratuais.

PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

Os prazos de vigência do contrato será de 36 (trinta e seis) meses a contar da data da sua assinatura.

O contrato poderá ser renovado por até 10 (dez) anos nos contratos administrativos, nos termos do art. 107 da Lei nº 14.133/2021.

DOS CRITÉRIOS DE HABILITAÇÃO

Os requisitos de habilitação serão definidos junto ao edital e nos termos da legislação vigente.

Quanto a habilitação técnica, temos:

Será requerida das empresas licitantes, para fins de habilitação, a comprovação do pleno atendimento a partir de apresentação de comparativo Ponto-a-ponto referente aos itens licitados.

Será requerida das empresas licitantes, para fins de habilitação, a comprovação de aptidão para a prestação dos serviços em características técnicas compatíveis com o objeto desta licitação, mediante a apresentação de:

Atestado(s) de capacidade técnica, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) ter fornecido ou estar fornecendo os quantitativos compatíveis em características e prazos de cada item do objeto da licitação;

Não será definido um quantitativo mínimo aceitável para ampliar a competitividade do certame e consequentemente, obter preços mais vantajosos em meio a possibilidade de participação de um número maior.

Declaração informando se a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos. Caso a licitante não possua uma das qualificações exigidas anteriormente, deverá ser apresentada declaração do próprio licitante de que a aquisição dos softwares, objeto desse edital, será realizada através de um canal do fabricante, para softwares especificados pelo fabricante para uso no Brasil.

Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.

Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.

A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s).

A comprovação de capacidade deverá ser realizada por meio de atestado ou conjunto de atestados que totalizados atendam aos critérios exigidos.

No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao

mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.

O CONTRATANTE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas neste Termo de Referência, podendo exigir apresentação de documentação complementar referente à prestação de serviços relativos aos atestados apresentados.

Caso a licitante não comprove as exigências do Edital por meio das documentações requeridas, será desclassificada.

O pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação, de acordo com as exigências do Edital.

DA PROVA DE CONCEITO

A licitante melhor classificada será convocada para realizar a Prova de Conceito – POC, com vistas a demonstrar que a solução ofertada atende os requisitos exigidos.

A POC somente será realizada para a proponente melhor classificada, não sendo requisito prévio de habilitação.

Caso a licitante melhor classificada não esteja ofertando uma solução que atenda os requisitos exigidos, ela será inabilitada, passando a convocar as licitantes na ordem de classificação da fase de lances.

A Prova de Conceito acontecerá em até 03 (três) dias úteis, contados da convocação oficial por parte da Defensoria.

A Prova de Conceito será realizada nas dependências da Defensoria Pública do Estado do Pará - DPE/PA, no horário acordado entre as partes.

Qualquer licitante poderá participar da Prova de Conceito, entretanto, será na condição de ouvinte e não poderá se manifestar durante a realização.

A Prova de Conceito consistirá na comprovação de requisitos técnicos existentes neste Termo de Referência, entretanto, a Defensoria Pública do Estado do Pará - DPE/PA se reserva ao direito de somente divulgar os requisitos

que deverão ser comprovados no momento da realização da POC, para evitar que as licitantes preparem a solução somente para passar na Prova de Conceito.

No momento da realização, a equipe de TI irá anotar em registro próprio, todos os requisitos comprováveis e o seu respectivo atendimento, podendo, inclusive, incluir comprovações.

Somente com a apresentação do(s) atestado(s) de capacidade técnica, declaração e a Prova de Conceito, a proposta será tecnicamente aceita.