TERMO DE REFERÊNCIA

PROCESSO ADMINISTRATIVO Nº 147/2025

Município de Getúlio Vargas/RS
Câmara de Vereadores de Getúlio Vargas - RS
Objeto da contratação: Contratação de empresa na prestação de Serviços Gerenciados de Cibersegurança, incluindo o fornecimento, instalação e gerenciamento de soluções de Firewall de Próxima Geração (Next Generation Firewall - NGFW) e Proteção (Antivírus), em regime de comodato, na Câmara de Vereadores do Município de Getúlio Vargas.
Modalidade de licitação: Dispensa de licitação n.º 127/2025

DEFINIÇÃO DO OBJETO E FUNDAMENTAÇÃO DA CONTRATAÇÃO

Contratação de empresa na prestação de Serviços Gerenciados de Cibersegurança, incluindo o fornecimento, instalação e gerenciamento de soluções de Firewall de Próxima Geração (Next Generation Firewall - NGFW) e Proteção (Antivírus), em regime de comodato, na Câmara de Vereadores do Município de Getúlio Vargas. A contratação visa garantir a proteção da infraestrutura de tecnologia e dos usuários de ameaças cibernéticas durante um período de 12 meses, conforme as especificações detalhadas neste Termo de Referência.

Item	ESPECIFICAÇÃO	UN.	QTDE.	VLR. UNIT.	VLR. TOT.
01	IMPLANTAÇÃO, QUE INCLUI: A) INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE FIREWALL NA CÂMARA DE VEREADORES; B) INSTALAÇÃO E CONFIGURAÇÃO DO ANTIVÍRUS NOS 20 (VINTE) PONTOS.	UN.	01	R$ XXXXXX	R$ XXXXX
02	CIBERSEGURANÇA COMO SERVIÇO, QUE INCLUI: A) COMODATO DE 01 (UM) EQUIPAMENTO DE FIREWALL E LICENCIAMENTO; B) COMODATO DE 20 (VINTE) LICENÇAS DE ANTIVÍRUS; C) SUPORTE TÉCNICO; D) MONITORAMENTO; E) DETECÇÃO E REAÇÃO À INCIDENTES DE SEGURANÇA; F) ANÁLISE E APRESENTAÇÃO DE RELATÓRIOS PARA MELHORIA CONTÍNUA DA SEGURANÇA.	UN.	12 MESES	R$ XXXXXX	R$ XXXXX

O presente Termo de Referência visa estabelecer as diretrizes e requisitos para a contratação de uma empresa na prestação de Serviços Gerenciados de Cibersegurança para a Câmara de Vereadores de Getúlio Vargas. Reconhecendo a crescente importância da Segurança da Informação e da Segurança Cibernética no contexto atual, a Câmara de Vereadores de Getúlio Vargas busca fortalecer seus mecanismos de proteção, garantindo a integridade, confidencialidade e disponibilidade de seus sistemas e dados.

Diante do cenário de ameaças cibernéticas em constante evolução, é imprescindível que a Câmara de Vereadores de Getúlio Vargas adote medidas robustas para salvaguardar suas informações sensíveis e garantir o adequado funcionamento de suas operações. Nesse sentido, a contratação de serviços especializados, apoiados em ferramentas modernas e eficientes é essencial para mitigar riscos, prevenir incidentes de segurança e assegurar a continuidade das atividades institucionais.

As Soluções de Cibersegurança desempenham um papel crucial na proteção dos ativos digitais da Câmara de Vereadores de Getúlio Vargas, atuando como uma barreira de defesa que controla o fluxo de dados entre redes, monitorando e filtrando o tráfego com base em regras predefinidas. Essas tecnologias oferecem uma camada adicional de proteção, permitindo o estabelecimento de políticas de segurança rigorosas, a identificação de atividades suspeitas e a prevenção de acessos não autorizados.

A escolha adequada de uma empresa na Proteção de Dados é fundamental para garantir que a Câmara de Vereadores de Getúlio Vargas esteja alinhado às melhores práticas de Segurança da Informação e Segurança Cibernética e às normas e regulamentações vigentes. Isso inclui a observância aos Artigos 23 e 37 da Constituição Federal, que delineiam as competências e responsabilidades dos entes federativos na administração pública e na proteção dos direitos dos cidadãos. Também são fundamentais os artigos 6, 46, 49 e 51 da Lei Geral de Proteção de Dados (LGPD), que estabelecem os princípios de proteção de dados, as sanções administrativas e as responsabilidades dos agentes de tratamento.

Além disso, a conformidade com as diretrizes estabelecidas pelo Tribunal de Contas do Estado do Rio Grande do Sul (TCE-RS) é crucial. Recomendações recentes do TCE-RS a diversos municípios destacam deficiências críticas na Segurança da Informação e na Segurança Cibernética, ressaltando a urgência de ações corretivas para sanar as inconformidades identificadas. Esses alertas servem como um aviso para todos os órgãos públicos sobre as potenciais consequências de não atender às diretrizes do Tribunal, incluindo a possibilidade de futuras auditorias e ações regulatórias. Portanto, é essencial que a Câmara de Vereadores de Getúlio Vargas adote soluções eficazes de proteção, como Antivírus, Controle de Acesso à Internet, Firewalls de Rede e de Aplicações para garantir a segurança dos dados.

Adicionalmente, a conformidade com as normas da ABNT NBR ISO/IEC 27000, especificamente a ISO/IEC 27002, que define as práticas recomendadas para os controles de Segurança da Informação, reforça o compromisso da Câmara de Vereadores de Getúlio Vargas com a manutenção de um padrão elevado de segurança e a melhoria contínua dos processos de proteção de dados e informações.

Portanto, este Termo de Referência estabelece o que é necessário para a seleção de uma empresa para a prestação de Serviços Gerenciados de Segurança que atendam aos requisitos específicos da Câmara de Vereadores de Getúlio Vargas. Busca-se, assim, estabelecer um ambiente seguro e resiliente, capaz de enfrentar as ameaças em constante evolução e garantir a continuidade dos serviços prestados, protegendo efetivamente os ativos digitais da Câmara de Vereadores e assegurando a confiança e a integridade das operações legislativas.

ESTRUTURA DE PRESTAÇÃO DE SERVIÇOS

LOCAIS PRESTAÇÕES DE SERVIÇO

Os serviços acordados podem ser realizados à distância pela CONTRATADA, mas também podem ser executados in loco, mediante acordo entre as partes, nos casos em que o acesso remoto não seja viável ou quando a situação exija, cobrindo toda a infraestrutura de segurança e usuários da CONTRATANTE.

As atividades de implantação, descritas no item 1, devem ser realizadas presencialmente (in loco) nas instalações físicas da CONTRATANTE.

HORÁRIOS DA PRESTAÇÃO DE SERVIÇO

Os Serviços Gerenciados de Cibersegurança devem ser fornecidos remotamente em período integral, 24x7 (24 horas por sete dias da semana), com a possibilidade de atendimento presencial nas instalações do CONTRATANTE em caso de incidentes graves de segurança que afetem a disponibilidade, integridade ou confidencialidade das informações.

DESCRIÇÃO DOS SERVIÇOS

Fornecer, implementar e gerenciar as soluções de segurança da informação detalhados neste Termo de Referência, por meio de equipe especializada da CONTRATANTE.

Os serviços compreendidos nos Serviços Gerenciados de Cibersegurança deverão abranger as seguintes soluções:

Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW).

Serviço de Proteção de Endpoints (Endpoint Protection).

A CONTRATADA deverá ter processos estabelecidos que assegurem a proteção das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.

SERVIÇO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL - NGFW)

A CONTRATADA deverá fornecer a ferramenta de Next Generation Firewall - NGFW durante a vigência do contrato para prestação do serviço, a solução deverá atender ao ITEM 2 deste Termo de Referência.

A CONTRATADA será responsável por executar as seguintes atividades de implementação e gerenciamento da solução de Firewall de Próxima Geração (Next Generation Firewall - NGFW), incluindo, mas não se limitando, aos seguintes serviços: Filtro de Conteúdo Web, IPS, VPN, Gateway Antivírus, Filtragem DNS, AntiSpam, Controle de Aplicações e Proteção contra Ameaças Avançadas, de acordo com as boas práticas do fabricante e atividades descritas nesse Termo de Referência.

A CONTRATADA será responsável pela manutenção, ativação e gestão de licenciamento, bem como, a atualização da solução durante a vigência do contrato.

A CONTRATADA deverá efetuar análise de riscos e impacto para definir as configurações, regras e atualizações da solução.

SERVIÇO DE PROTEÇÃO DE ENDPOINTS (ENDPOINT PROTECTION)

A CONTRATADA deverá fornecer a ferramenta de Proteção de Endpoints (Endpoint Protection) durante a vigência do contrato para prestação do serviço, a solução deverá atender ao ITEM 2 deste Termo de Referência.

A CONTRATADA será responsável por executar as seguintes atividades de implementação e gerenciamento da solução de Proteção de Endpoints (Endpoint Protection), incluindo, mas não se limitando, aos seguintes serviços: proteção contra malwares e scripts maliciosos, controle de dispositivos e processos em memória e inventário de aplicações, de acordo com as boas práticas do fabricante e atividades descritas nesse Termo de Referência.

A CONTRATADA será a responsável pela manutenção, gestão de licenciamento e atualização da solução durante a vigência do contrato;

A CONTRATADA deverá efetuar análise de riscos e impacto para definir as configurações, regras e atualizações da solução.

INFORMAÇÕES COMPLEMENTARES

É vedada a subcontratação dos serviços que compõem o objeto desta dispensa de licitação, total ou parcialmente.

A CONTRATADA deverá atender todos os itens apresentados nesse Termo de Referência para prestação dos serviços contemplados.

A CONTRATADA deverá incluir, em sua proposta, todos os custos necessários para a completa prestação dos serviços especificados neste documento, abrangendo hardware, software e quaisquer licenças adicionais que sejam consideradas necessárias para a execução dos serviços.

REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

A CONTRATADA é exclusivamente responsável pelo dimensionamento adequado das equipes para a execução dos Serviços Gerenciados de Segurança Cibernética, garantindo o cumprimento integral dos níveis de serviço exigidos. Para assegurar a qualidade e eficiência na prestação dos serviços, a equipe técnica da CONTRATADA deve incluir, no mínimo, um (01) profissional que possua as seguintes certificações:

EXIN Data Protection Officer (DPO);

EXIN Information Security Foundation based on ISO/IEC 27001;

Huawei Certified ICT Associate (HCIA);

Cisco Certified Network Associate (CCNA);

MikroTik Certified Network Associate (MTCNA);

UNS (Unifi Network Specialist);

UBNT (Ubiquiti Enterprise Wireless Admin);

A equipe técnica da CONTRATADA deve atender aos seguintes requisitos de certificação do fabricante da solução ofertada, garantindo a competência técnica necessária para executar os serviços especificados neste contrato:

A equipe deve incluir, no mínimo, dois (02) profissionais habilitados para à solução ofertada.

A CONTRATADA deverá disponibilizar, no mínimo, um (01) profissional qualificado para realizar os atendimentos presenciais previstos neste contrato, observando as seguintes condições: ATENDIMENTOS PRESENCIAIS NA REGIÃO.

O profissional designado deverá estar disponível para atender às demandas da CONTRATANTE, cumprindo rigorosamente os prazos de atendimento presencial estabelecidos no Acordo de Nível de Serviço (ANS) deste termo de referência.

O profissional deverá possuir formação e experiência compatíveis com o objeto do contrato. Serão aceitos diplomas de formação de nível técnico ou superior em Tecnologia da Informação ou áreas correlatas, ou atestadas de Capacidade Técnica

fornecida por pessoa jurídica de direito público ou privado, que comprovem a aptidão para desempenhar funções semelhantes às especificadas no contrato.

Para fins de habilitação, a CONTRATADA deverá apresentar os seguintes documentos:

Declaração de Disponibilidade Profissional, contendo:

Nome completo do profissional designado.

Qualificação técnica e experiência profissional: Conforme descrito no ITEM 2, serão aceitos diplomas ou atestados de Capacidade Técnica.

Compromisso de atendimento aos prazos estabelecidos no ANS e ciência dos requisitos de atendimento presencial.

Apresentar comprovante de residência do profissional designado, demonstrando que este reside em localidade que permita o cumprimento dos prazos de atendimento presencial estabelecidos no ANS.

A CONTRATADA deverá disponibilizar, no mínimo, um (01) profissional com diploma de Tecnólogo em Redes de Computadores ou áreas correlatas, emitido por instituição de ensino superior reconhecida pelo Ministério da Educação (MEC), e com registro no Conselho Regional de Engenharia e Agronomia (CREA).

Adicionalmente, a CONTRATADA deve comprovar que possui em seu quadro permanente, na data prevista para entrega da proposta, profissional de nível superior em Tecnologia da Informação. Este profissional deverá possuir diploma de graduação de nível superior em Tecnologia da Informação ou áreas correlatas, fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação (MEC).

A CONTRATADA deverá apresentar, na fase de habilitação, a documentação comprobatória dos profissionais que comporão a equipe técnica. Também deverá ser apresentada a comprovação do vínculo desses profissionais com a empresa, mediante um dos seguintes documentos:

Carteira de Trabalho e Previdência Social (CTPS), no caso de empregados;

Contrato de prestação de serviços, devidamente formalizado entre as partes;

Os profissionais indicados pela CONTRATADA para fins de comprovação da capacitação técnico-profissional deverão participar efetivamente dos serviços objeto da dispensa de licitação, admitindo-se a substituição por profissionais de experiência equivalente ou superior, desde que aprovada previamente pela CONTRATANTE

A CONTRATANTE se reserva o direito de solicitar, a qualquer momento, a substituição de qualquer profissional que não atenda às exigências do contrato ou cujo desempenho seja considerado insatisfatório.

DECLARAÇÃO DO FABRICANTE

Declaração emitida pelo fabricante da solução ofertada, atestando que está autorizada capacitada a comercializar, implementar e prestar suporte técnico para os produtos e serviços propostos.

ATESTADO DE CAPACIDADE

A empresa deverá apresentar Atestado de Capacidade, sendo obrigatório pelo menos 03 (três) atestados fornecidos por pessoa jurídica de direito público que comprove aptidão para o desempenho dos serviços iguais ou compatíveis em características, quantidades e prazos com o objeto da dispensa de licitação. Serão aceitos apenas atestados emitidos por entes públicos do Rio Grande do Sul. Os atestados deverão comprovar a contratação, a alta disponibilidade da solução e a execução satisfatória dos serviços com características equivalentes ou de superior complexidade tecnológica, operacional e intelectual.

Os atestados deverão estar emitidos em papel timbrado da empresa ou órgão contratante, com a identificação clara do signatário e do cargo que ocupa.

Não serão aceitos Atestados de Capacidade Técnica emitida por empresas do mesmo grupo econômico da licitante ou por suas subcontratadas.

SERVIÇOS DE IMPLANTAÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL - NGFW) E PROTEÇÃO DE ENDPOINTS (ANTIVÍRUS)

REQUESITOS GERAIS

A CONTRATADA deverá executar a instalação física e a configuração lógica dos produtos, conforme especificado nos ITENS 1 e 2 da tabela presente no Objeto deste Termo de Referência.

Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados, incluindo deslocamento e demais despesas de seus profissionais para às unidades onde as soluções serão instaladas;

Caberá a CONTRATANTE subsidiar toda infraestrutura necessária para implantação das soluções de firewall, exemplo: locais de instalação dos appliances de Firewalls (racks e gavetas);

Os serviços de implantação deverão ser executados presencialmente nas instalações da CONTRATANTE por técnico(s) da CONTRATADA capacitado(s) para tal;

Após o recebimento dos equipamentos e das licenças, a CONTRATANTE deverá definir, juntamente com a CONTRATADA, o cronograma de instalação e configuração

dos mesmos, enviando a CONTRATADA, documento contendo informações de data, hora, local, e soluções a serem instaladas;

FASES DO SERVIÇO DE IMPLANTAÇÃO

As fases da implantação dos serviços devem contemplar:

Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento da solução a ser implementada, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, bem como quaisquer outros itens que sejam necessários para a implantação da respectiva solução. Deve-se considerar as janelas de manutenção da CONTRATANTE, plano de rollback e o escopo definido. Os responsáveis técnicos da CONTRATANTE acompanharão e aprovarão o planejamento;

Implantação: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

Etapa de Testes: todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço;

Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pela CONTRATANTE.

A CONTRATANTE terá o prazo de 02 (dois) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite);

O serviço será aceito se, e somente se, houver comprovação de que todos os requisitos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos utilizados, consulta à documentação fornecida e verificação dos serviços de instalação e configurações, comparadas aos itens deste Termo;

No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados;

O processo de instalação, implantação e configuração deverá ter início em no máximo 15 (quinze) dias após a assinatura do contrato. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

Após a conclusão dos serviços de instalação, o técnico da CONTRATADA deverá realizar o monitoramento da solução por pelo menos 04 (quatro) dias úteis, com acompanhamento da equipe da CONTRATANTE, a fim de identificar e sanar eventuais inconsistências;

Ao término da instalação, a CONTRATADA deverá entregar Caderno de Documentação "As Built" do Projeto, no qual constem todos os detalhes da instalação, tais como:

Descrição dos serviços implantados;

Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

Definição de responsabilidades;

Recursos de alta disponibilidade;

Procedimentos para abertura e atendimento a chamados;

Procedimentos de recuperação de equipamentos;

Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

Documentação dos processos de trabalho associados ao item;

Desenho dos racks onde estão instalados os equipamentos (bayface);

Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);

ESCOPO DOS SERVIÇOS DE IMPLANTAÇÃO

Instalação das Soluções de Firewall, conforme contratado;

Configurar as Soluções de Firewall conforme segmentação de rede definida pela CONTRATANTE;

Atualização e aplicação de correções nas soluções de Firewall;

Implementação/migração de regras de Filtragem;

Implementação/migração de regras de NAT;

Implementação/migração de regras de QoS;

Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;

Implementação de alta disponibilidade, quando aplicável;

Implementação de monitoramento de links, quando aplicável;

Integração com o Active Directory;

Tunning de configuração e regras de filtragem, removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados;

Testes gerais, validando o funcionamento das aplicações após a implementação dos Firewalls;

Registrar e associar todos os dispositivos de firewall a solução de gerenciamento;

Configuração de comunicação para permitir o tráfego entre a solução de gerenciamento e dispositivos firewalls;

Importar configurações existentes, quando aplicável;

Configuração de alertas e notificações para eventos críticos de segurança;

Definição de grupos de administração;

Não faz parte do Escopo dos Serviços de Implantação da Solução de Firewall:

Passagens de cabo que não compreendam as necessárias para conectividade das soluções de firewall e proteção da rede;

Instalação de demais soluções e equipamentos que não compreendam os mencionados neste serviço de implantação;

Configuração de equipamentos de terceiros;

SERVIÇOS ESPECIALIZADOS DE GESTÃO E SUPORTE CONTÍNUO

CARACTERÍSTICAS GERAIS

O serviço de gestão e suporte contínuo será realizado como prestação de serviço durante todo o período do contrato. Este serviço deverá contemplar o gerenciamento, monitoramento e suporte continuado das soluções de Firewall de Próxima Geração (Next Generation Firewall - NGFW) e Proteção e Endpoints (Antivírus);

A CONTRATADA deverá realizar a gestão continuada das soluções, bem como a prestação de suporte técnico, sem limitação de horas mensais, assegurando a disponibilidade total para atender às necessidades do CONTRATANTE;

O serviço poderá ser realizado remotamente ou presencialmente, conforme necessidade para a solução da requisição/incidente;

A CONTRATANTE poderá exigir, no ato de abertura do incidente ou requisição, dependendo do nível de criticidade do atendimento, que o atendimento seja feito de maneira presencial ou de maneira remota;

A solicitação do serviço será feita pelo CONTRATANTE, através de chamado (eletrônico ou telefônico), e-mail ou documento oficial, expedido ao prestador;

O período de abertura e resolução dos chamados será contabilizado no regime 24x7 (24 horas por sete dias da semana);

Os prazos de atendimento deverão obedecer a suas devidas classificações, descritas no item “Acordo de Nível de Serviço (ANS)” mais adiante;

A CONTRATADA deverá dispor de telefone um número de telefone 0800 ou permitir ligações a cobrar para a abertura de chamados;

A CONTRATADA deverá disponibilizar e-mail para a abertura de chamados;

A CONTRATANTE poderá exigir a realização de pelo menos 1 (uma) vistoria presencial a cada 15 (quinze) dias promovida por profissional da CONTRATADA nas dependências da CONTRATANTE, a fim de verificar presencialmente a saúde do ambiente. Essa vistoria não exime a contratada de realizar atividades inerentes aos chamados solicitados se estes demandarem presença física do técnico;

O acesso ao ambiente (incluindo o caso de atendimento remoto) será supervisionado por profissional da CONTRATANTE. A CONTRATADA obriga-se a respeitar as políticas de segurança e de sigilo impostas pela CONTRATANTE;

A CONTRATADA deverá dispor de software próprio para registro e controle dos chamados, com registro de hora e data do evento, descrição do caso relatado, técnico responsável pelo atendimento, histórico e continuidade da solicitação e emissão de estatísticas e relatórios fixos ou sob demanda;

A CONTRATADA deverá realizar atividades proativas (sem necessidade de abertura de chamado pela CONTRATANTE), contemplando o gerenciamento, monitoramento e suporte diário do ambiente contendo as seguintes atividades:

Monitorar constantemente o tráfego de rede através da solução de firewall buscando identificar e mitigar atividades maliciosas;

Avaliar de forma constante as regras e políticas da solução, bem como sinalizar a CONTRATANTE sobre as mesmas, para que a segurança seja aprimorada de forma contínua;

Monitorar, notificar e buscar corrigir os seguintes eventos da solução Firewall:

Intrusões detectadas pelos módulos de IPS e antivírus do equipamento de Firewall;

Indisponibilidade do cluster, quando houver;

Indisponibilidade de VPN;

Indisponibilidade dos links de Internet;

Sobrecarga de processamento;

É necessário a apresentação de relatório mensal com atividades/chamados e o tempo de atendimento específico de cada um deles;

As atividades que compreendem o atendimento reativo compreendem as seguintes:

Dúvidas técnicas sobre a configuração dos componentes de hardware e software que compõem o projeto, ou outras;

Atualizações de firmwares/microcódigos de todos os componentes de hardware e software da solução;

Testes de desempenho, segurança e disponibilidade dos serviços;

Inclusão/exclusão/alteração de regras, nos equipamentos Firewall, com análise crítica a fim de garantir a gestão de mudanças no ambiente da CONTRANTE;

Restauração das configurações das soluções;

Criar regras de QoS para controle de tráfego de aplicações, quando aplicável;

Realizar análise e diagnóstico do ambiente para resolução de problemas;

Resolução de problemas do ambiente com base nas características mencionadas no acordo de nível de serviço;

Abrir e acompanhar os chamados de suporte junto aos fabricantes das soluções, quando for o caso;

É necessário a apresentação mensal dos seguintes relatórios:

Domínios mais acessados;

Categorias de site mais acessadas;

Relatório de malwares detectados;

SERVIÇOS DE MONITORAMENTO CONTÍNUO E BACKUP (NOC - NETWORK OPERATIONS CENTER)

CARACTERÍSTICAS GERAIS

O serviço de monitoramento contínuo será prestado durante todo o período do contrato, abrangendo o monitoramento da disponibilidade de todos os appliances de firewall que compõem a solução;

Em casos de incidentes, a CONTRATADA deverá iniciar o procedimento de escalonamento previamente acordado com a CONTRATANTE em, no máximo, 30 (trinta) minutos, o que inclui, por exemplo, contatar a operadora de internet responsável;

A CONTRATADA deverá disponibilizar acesso a um software web, protegida por login e senha, que permita a visualização em tempo real do desempenho e status dos equipamentos monitorados. Esta ferramenta deve possibilitar a personalização dos dashboards, de modo a apresentar as informações mais relevantes para a CONTRATANTE.

A CONTRATADA deverá emitir um relatório mensal detalhado contendo informações sobre:

Tempo de indisponibilidade de cada link;

Consumo de CPU e memória;

Conexões utilizadas e disponíveis;

Status da VPN e das interfaces;

Upload e Download dos links de Internet;

Número de série e versão do firmware dos equipamentos.

Uptime dos dispositivos.

A CONTRATADA deverá executar backups automáticos diariamente dos firewalls, garantindo que os dados estejam disponíveis para a CONTRATANTE em um servidor FTP seguro;

ACORDO DE NÍVEL DE SERVIÇO (ANS)

A prestação do serviço, objeto deste Termo de Referência, deverá estar disponível conforme os indicadores, níveis de prioridade e prazos detalhados abaixo.

NÍVEIS DE SERVIÇO

Tipo	**Indicador**	**Nível de Serviço**
Atendimento	Resolução de incidente dentro do prazo estipulado	90%
Atendimento	Atendimento de solicitação dentro do prazo estipulado	90%

NÍVEIS DE PRIORIDADE

Prioridade	**Descrição**
1) Emergencial	O serviço está inoperante ou há um impacto crítico nas operações para o negócio. ***O atendimento aos chamados com nível de prioridade Emergencial deve ser realizado obrigatoriamente de forma presencial (in loco) nas instalações físicas da CONTRATANTE***.
2) Alta	O serviço está comprometido ou aspectos significativos das operações foram negativamente afetados pelo desempenho insatisfatório.
3) Média	O serviço está operacional, porém com problemas menores que não afetam diretamente as operações.
4) Baixa	O desempenho operacional do serviço está comprometido, mas sem afetar sua funcionalidade ou operação.
5) Planejada	Um incidente ou evento que não interrompe ou degrada os serviços ao cliente, mas requer ação planejada.

PRAZOS DE ATENDIMENTO

Prioridade da solicitação	**Nível de Serviço (SLA) – Horas Corridas**
1) Emergencial	1 horas
2) Alta	4 horas
3) Média	12 horas
4) Baixa	48 horas
5) Planejada	60 horas

REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL - NGFW) OFERTADA

Para prestação de serviço a CONTRATADA deve fornecer a solução de NGFW que atentada aos requisitos técnicos abaixo detalhados durante todo o período de vigência do contrato.

REQUISITOS DE PERFOMANCE DOS APPLIANCES

Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 750 Mbps ou superior.

Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 300 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

Desempenho mínimo de 1 Gbps de IPS.

Suporte mínimo de 750.000 conexões simultâneas/concorrentes.

Suporte mínimo de 6.000 novas conexões por segundo.

Deverá permitir expansão de armazenamento de até 256Gb.

Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

Deve possuir 8 interfaces 1 GbE padrão RJ-45.

Deve possuir 1 interface do tipo console ou similar.

Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos.

A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 50 usuários simultâneos.

Deve suportar 50 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

Deve suportar, no mínimo, 750 Mbps de desempenho de VPN IPSEC.

Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o

direito de aferir a desempenho dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste termo de referência. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

O Equipamento deverá ser homologado pela ANATEL.

Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

O licenciamento para todos os serviços de Next Generation Firewall deverá permanecer ativo e válido durante todo o período do contrato, incluindo garantia e suporte técnico.

CARACTERÍSTICAS GERAIS

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada sete.

Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

O licenciamento dos firewalls deve permanecer ativo e válido ao longo de todo o período do contrato, garantindo que todos os serviços associados, como garantia e suporte técnico, estejam disponíveis e acessíveis durante toda a vigência contratual.

Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança.

A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações do firewall

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas.

Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos.

CARACTERÍSTICAS DIVERSAS

Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

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

Deve possuir proteção anti-spoofing.

Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

Latência;

Jitter;

Perda de pacotes.

O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

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

Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

Deve suportar DHCP relay.

Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

Deve ter suporte à proteção e identificação de hosts possivelmente infectados com "botnets". A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

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

Detectar e bloquear a origem de portscans.

Deve permitir o bloqueio de ataques.

Deve permitir o bloqueio de exploits conhecidos.

O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.

Implementar DSCP (Differentiated Services Code Points).

Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

Implementar mecanismo de sincronismo de horário através do protocolo NTP.

Possuir suporte ao protocolo SNMP versões 2 e 3.

Possuir suporte a log via syslog.

Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e email.

Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída

(Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.2 e TLS 1.3

Deve permitir a funcionalidade de ARP bridging

Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

A solução deve permitir a visualização gráfica das regras de segurança e acesso.

CARACTERÍSTICAS DE VPN

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256.

Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

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

ALTA DISPONIBILIDADE

A solução deve suportar a operação em Alta Disponibilidade (HÁ) no modo Ativo/Passivo, com as implementações de Failover.

Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

A solução deve ter a capacidade de operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET,

RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

CONTROLE DE AMEAÇAS

Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

Implementar funcionalidade de detecção e bloqueio de “call-backs”.

A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

Implementar interface CLI segura através do protocolo SSH.

Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

A solução deve permitir criar regras de exceção de acordo com a proteção.

Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

A solução deve ser capaz de proteger contra ataques a DNS.

A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

A solução deve ser capaz de prevenir acesso a websites maliciosos.

A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

A solução deverá receber atualizações de um serviço baseado em cloud.

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficiente frente ameaças exploradas por vulnerabilidades do tipo meltdown.

A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos.

PROTEÇÃO CONTRA ATAQUES AVANÇADOS

A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas. A solução deve possuir nuvem de inteligência proprietária

do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego.

Conter ameaças avançadas de dia zero.

Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

Mitigar ameaças de dia zero de forma transparente para o usuário final.

Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

Mitigar ameaças de dia zero via tráfego de internet.

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

Conter e mitigar exploits avançados.

A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

A Solução de segurança de Firewalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying ou buffering.

A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.

A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.

A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho.

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

Inspeção profunda de memória em tempo real

Inspeção profunda de pacotes livre de remontagem,

Descriptografia e inspeção TLS/SSL,

Inteligência e controle de aplicativos

Recursos SD-WAN seguros

É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

A solução de segurança não pode aplicar nenhum tipo de exceção de inspeção de tráfego (bypass) oriunda de condições de limitação de capacidade de processamento de forma automática. Toda e qualquer exceção (bypass) de inspeção e tráfego deve ser possível

apenas através de ação explícita e específica criada pelo administrador da plataforma através de configurações realizadas pela console gráfica do appliance, ou pela plataforma centralizada de gerenciamento da solução.

CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

Possuir filtro de conteúdo integrado ao NGFW com capacidade de classificar páginas da web em pelo menos 89 (oitenta e nove) categorias distintas, atualizadas e automaticamente consultadas.

Deve possuir a capacidade de criação de políticas baseadas na identificação e controle de usuários através de URLs, integrando-se com serviços de diretório, como o Active Directory, e bases de dados locais.

Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

Oferecer opções para personalizar a página de bloqueio conforme as necessidades específicas do ambiente.

Permitir a submissão de novos sites para categorização, garantindo a relevância e atualidade das classificações.

Habilitar a classificação dinâmica de sites, URLs e domínios para se adaptar às mudanças na web.

Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites da web, possibilitando o bloqueio ou permissão de categorias específicas para cada grupo, incluindo o controle de acesso a domínios específicos.

Possibilitar a aplicação de políticas de filtragem de conteúdo em zonas de segurança específicas conforme a necessidade da rede.

Permitir a aplicação de políticas de filtro de conteúdo baseadas em horários e dias específicos, oferecendo flexibilidade na gestão do acesso à web.

CARACTERÍSTICAS DE AUTENTICAÇÃO

Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o login na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

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 NGFW.

Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet

A solução deve possibilitar SSO via API

A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.

CARACTERÍSTICAS DE ADMINISTRAÇÃO

Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração.

Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão.

Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.

Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações.

A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

GERENCIAMENTO UNIFICADO E RELATÓRIOS

Deve possuir solução de gerenciamento centralizado em nuvem do mesmo fabricante, para gerenciamento de toda solução.

Armazenamento em nuvem durante 365 dias

Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem usuários.

Grupos de firewalls permitidos;

Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado;

Perfil de nível de acesso (escrita, leitura, administração, relatórios).

Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual.

Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.

Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

O gerenciamento deve permitir/possuir:

Criação e administração de políticas de firewall e controle de aplicação

Monitoração de logs;

Investigação de eventos de segurança e falhas (debugging)

Acesso concorrente de administradores, conforme políticas e perfis previamente definidos.

Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforma de gerência, e à partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma.

A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL.

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

A solução deve possuir tela situacional com todos os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador:

Nome do firewall;

Número de série;

Modelo;

Versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline.

Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez.

Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento, possibilitando comparação de configurações que evitem sobreposição de regras e conflitos de configuração.

A solução deve possuir Dashboard com sumario de alertas e informação de status de licença

A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo.

Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência.

A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN.

A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls.

A solução deve possibilitar a geração de templates de configuração a partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma.

Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais

A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações,

criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento.

Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

Durante as alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente.

A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

A solução deve oferecer monitor de auditoria de configurações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados.

A solução deve oferecer possibilidade de auditoria de configurações.

A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:

Utilização de CPU/Processamento;

Aplicações em uso e seu consumo de banda;

Interfaces em uso e utilização de banda;

Conexões concorrentes em uso.

A solução deverá permitir visualizar sumario com as informações referentes às principais ameaças protegidas pelos firewalls.

Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

A solução deverá prover relatórios com no mínimo histórico de 365 dias.

A solução deverá prover relatórios referentes às atividades dos usuários.

A solução deverá prover relatórios referentes ao uso de aplicações web, com no mínimo as seguintes informações:

Nome da aplicação;

Quantidade de conexões;

Percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados.

A solução deverá prover relatórios referentes ao consumo de rede dos usuários, com no mínimo as seguintes informações:

Nome do usuário;

Quantidade de conexões;

Percentual que tráfego do usuário representa na rede;

Quantidade de Megabytes trafegados.

A solução deverá prover relatórios referentes ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

Endereço IP;

Quantidade de conexões;

Percentual que tráfego que o IP representa na rede;

Quantidade de Megabytes trafegados.

A solução deverá prover relatórios referentes aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede.

A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF.

A solução deverá permitir geração e envio agendado de relatórios.

A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-Mail com as informações relativas a este evento.

A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciados.

A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

Aplicações de maior risco, e volume de dados consumido por estas;

Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas;

Aplicações de maior utilização, por categoria.

A solução deve apresentar consoles de indicação dos principais usuários contendo:

Usuários utilizando mais conexões;

Usuários consumindo mais dados.

A solução deve apresentar console de indicação de:

Virus/Spyware bloqueados;

Intrusões bloqueadas;

Botnets bloqueados;

Origens e destinos mais utilizados.

A solução deve apresentar console de indicação de Aplicações indicando:

Aplicações identificadas;

Categorização e uso das aplicações;

Risco das aplicações.

A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

Lista de eventos correlacionados com opção de navegação "drilldown";

Modo gráfico;

Lista de logs.

A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:

Produtivas;

Não produtivas;

Aceitáveis para a política de uso corporativa;

Inaceitáveis para a política de uso corporativa;

Customizadas.

A solução deve permitir visualização de topologia do firewall e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points).

O Fabricante deverá comprovar que possui tecnologia holística capaz de integrar suas principais soluções em uma base centralizada gráfica com informações e alertas, comprovando integração de pelo menos duas de suas plataformas de segurança.

REQUISITOS MÍNIMOS PARA SOLUÇÃO DE PROTEÇÃO DE ENDPOINTS (ANTIVÍRUS)

A CONTRATADA deve fornecer uma Solução de Proteção De Endpoints (Antivírus) que atenda aos requisitos técnicos detalhados abaixo, durante todo o período de vigência do contrato.

A solução de proteção de Endpoints deve possuir de módulos de software integrados gerenciados por um único fabricante de forma a atender ao conjunto de requisitos exigidos nessa especificação.

Devido aos progressos de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessária o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez.

Deve permitir a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes de segurança da solução do fabricante.

Deve ser entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional;

Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).

Não serão aceitas soluções que dependam para sua operação de atualizações de assinaturas.

Todos os módulos de software do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade.

Suporte total para os seguintes sistemas operacionais:

a. Windows 7 (32 e 64 bits);

b. Windows 8 e Windows 8.1 (32 e 64 bits);

c. Windows Server 2008 R2 (32 e 64 bits);

d. Windows Server 2012;

e. Windows Server 2016;

f. Mac OS X 10.10 (Yosemite);

g. Mac OS Sierra;

h. Linux ou Unix em alguma versão recente recomendada

A console de gerência deverá ser centralizado com interface gráfica web.

A solução deverá prover permitir a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.

A gerência centralizada deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança.

Deve prover detecção e prevenção de ameaças em real-time;

O funcionamento da solução deve operar analisando a pré-execução e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.

Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

A solução deve aplicar análise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.

Caso seja encontrado um programa malicioso a sua execução não deve ser permitida.

A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos.

A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.

Deve utilizar a tecnologia de "Machine Learning" para identificar qualquer ameaça nos arquivos potencialmente perigosos.

Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de "Sandbox On-premises ou On-Cloud", com o objetivo de fazer uma segunda análise em diferentes sistemas operacionais.

Identificar ameaças avançadas, chamadas de "Zero-day", sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.

Seu engine deve ter passado satisfatoriamente, sob documentação a ser avaliada, nos três testes de ameaças mais recentes do MITRE@ATTACK.

Permitir o uso de Filtro de Conteúdo Categorizado.

Permitir recurso de Restaurar uma máquina no caso de uma contaminação por Ransomware.

Gerenciamento e administração centralizada para estação de trabalho

A console de monitoração e configuração deve ser feita através de uma central para o grupo de antimalware, baseada em web e em nuvem, que deve conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos;

A console deve apresentar painel com o resumo dos status de proteção dos computadores, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

Permitir sincronização com LDAP ou Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção;

Aplicar regras diferenciadas baseado em grupos ou usuários;

A instalação do agente poderá ser realizada através de soluções de distribuição de softwares ou através de GPO;

A console deve permitir criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários ou endpoint, não importando em que equipamentos eles estejam acessando;

Fornecer atualizações do agente instalado através da console de gerenciamento; aceita-se documentação.

Permitir exclusões de escaneamento para os seguintes tipos tanto a nível geral quanto específico em uma determinada política:

Caminho (Path);

Hash;

Permitir a exportação dos relatórios gerenciais.

Consideramos ainda as seguintes funcionalidades importantes

Serviço nativo de nuvem para proteção, no modelo Software como Serviço (SaaS);

As quantidades para proteção devem ser do mesmo fabricante a fim de trabalharem conjuntamente na proteção do ambiente; A correlação e relatório dos eventos poderão ser realizados com agregação de outras soluções de forma transparente ao usuário final;

O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

O agente deve ter a capacidade de submeter o arquivo desconhecido ou seus metadados à nuvem de inteligência do fabricante para detectar a presença de ameaças;

A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

A solução deve proteger a estação de trabalho independente de a estação estar conectada à internet;

Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

Suportar equipamentos com arquitetura 32-bit e 64-bit que o cliente deve ter instalado nas estações de trabalho e deve ser compatível com os sistemas operacionais: Mac OS Sonoma e superiores, Microsoft Windows 10 e 11;

Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo;

Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas ou possuir modulo capaz de prevenir a exploração de vulnerabilidades conhecidas ou desconhecidas.

Deve possuir técnicas de proteção, que inclui:

Técnica para detectar malware criptografado mais complexo;

Algoritmo correspondente padrão, onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

Possuir capacidade para a detecção de vírus polimórficos, ou vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

Verificação de ameaças web avançadas: bloquear tentativas de exploração do tipo fileless, quando o usuário abrir um site e o mesmo conter códigos malicioso, a solução deverá ser capaz de prevenir;

Ser capaz de segregar as contas de usuários de forma hierárquica com no mínimo os perfis “usuário” e “administrador”, não limitando o número de acesso de usuários simultâneos.

A solução deverá possuir módulo de investigação e detecção integrados.

Funcionalidade de Antivírus e Anti-Spyware.

Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

Proteção antimalware nativa da solução ou incorporada sem a utilização de agentes adicionais, desde que distribuídos pelo fabricante.

As configurações do Anti-Spyware deverão ser realizadas através da mesma console do antivírus.

Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware.

Permitir a inclusão de arquivos em listas de exclusão (whitelist) para que não sejam verificados pelo produto.

Permitir a varredura das ameaças da maneira manual e em tempo real na máquina do usuário.

Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos, através do antivírus.

Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

A solução devera possuir a capacidade de isolar o host, após a infecção, permitindo apenas a comunicação com a console de gerenciamento.

Permitir o bloqueio (ou desativação na política de Antivírus) da verificação de vírus em recursos mapeados da rede.

Funcionalidade de detecção Proativa de reconhecimento de novas ameaças

Deve possuir funcionalidade de detecção de ameaças via técnicas de deep machine learning; Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

Deve possuir capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória;

Deve possuir capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória; aceita-se documentação;

Deve possuir capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada. aceita-se documentação;

Funcionalidade de proteção contra ransomwares;

Deve dispor de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas; aceita-se documentação;

Dispor de remediação da ação de criptografia maliciosa dos ransomwares com função de Rollback na console em caso de contaminação;

A solução deve prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

Possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day. aceita-se documentação.

A solução deve trabalhar silenciosamente na máquina do usuário e deve detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deve realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve fazer a limpeza e remoção completa do ransomware na máquina do usuário sem a necessidade intervenção humana.

Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

A console de monitoração e a de configuração deve ser feita através de central, baseada em web e em nuvem ou appliance (físico ou virtual), que deve conter todas a

ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

A console deve apresentar painel com o resumo detalhado de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional.

RESPONSABILIDADES

SÃO RESPONSABILIDADES DA CONTRATANTE:

a) Cumprir pontualmente todos os compromissos financeiros de sua responsabilidade;

b) Fornecer, a qualquer tempo e com presteza, mediante solicitação da "CONTRATADA", todos os dados, documentos e informações para a execução dos serviços, com os dados informativos e cadastrais totalmente saneados para a conversão, bem como informações adicionais, dirimir dúvidas e orientá-la em todos os casos omissos.

c) Responsabilizar-se pela continuidade das rotinas técnicas incluídas nos módulos contratados durante os prazos de implantação e migração dos dados, evitando a paralisação das atividades essenciais durante o período de implantação.

d) Providenciar o recolhimento de tributos, contribuições previdenciárias e encargos sociais antes de efetuar o pagamento.

e) A responsabilidade, presente ou futura, de qualquer compromisso ou ônus decorrentes do inadimplemento da Contratada relativos às obrigações por ela assumidas não serão responsabilidade da Contratante, ficando essas ao encargo da Contratada, exclusivamente, em qualquer momento que vierem a ocorrer.

SÃO RESPONSABILIDADES DA CONTRATADA:

a) Aceitar as alterações contratuais, em especial as supressões e acréscimos, instituídos na forma da legislação vigente.

b) Manter durante toda a execução deste contrato, em compatibilidade com as obrigações aqui assumidas, todas as condições de habilitação e qualificação exigidas.

c) As despesas com deslocamentos, encargos fiscais, previdenciários e trabalhistas, além de quaisquer outras que se fizerem necessários ao cumprimento do presente contrato serão suportados pela Contratada sem qualquer ônus ou solidariedade por parte da Câmara de Vereadores.

d) Recolher todos os tributos e contribuições previdenciárias que incidirem sobre as atividades do contrato.

MODELO DE EXECUÇÃO DO OBJETO

O prazo do contrato com a empresa será de 12 meses, podendo ser reajustado, após um ano de vigência deste contrato, pelo índice médio acumulado da variação positiva dos seguintes índices; INPC/IBGE, IPCA/IBGE e IGPM/FGV.
O contrato poderá ser prorrogado sucessivamente, respeitando a vigência máxima decenal, mediante demonstração de que as condições e os preços permanecem vantajosos para o CONTRATANTE sendo permitidas eventuais negociações entre as partes, vide Artigo 107 da Lei 14.133/2021.

CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Após a emissão de nota fiscal, pagamento até o 10° dia do mês subsequente ao serviço prestado.

FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR/PRESTADOR DE SERVIÇO

O futuro contratado será selecionado mediante processo de dispensa de licitação.

ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Estima-se para a contratação almejada o valor total de R$ 33.880,00 (Trinta e três mil, oitocentos e oitenta reais), vislumbra-se que tal valor é compatível com o praticado pelo mercado correspondente.

ADEQUAÇÃO ORÇAMENTÁRIA

O dispêndio financeiro decorrente da contratação ora pretendida decorrerá da seguinte dotação orçamentária:

Despesa	Elemento	Descrição	Proj/Ativ.	Desc.Proj;Ativ	Fonte de Recurso	Quantidade por Despesa
13147	33904006000	LOCAÇÃO DE SOFTWARE	1	MANUTENÇÃO DAS ATIVIDADES DO LEGISLATIVO	Outros Recursos não Vinculados	33.880,00

Getúlio Vargas, 24 de janeiro de 2025.

Cristiane Piccoli Dalapria,

Diretora Administrativa do Poder Legislativo.

VIABILIDADE DECLARADA PELA AUTORIDADE SUPERIOR:

DATA: 24/01/2025

_____

Jeferson Wilian Karpinski,

Presidente.