ETP - ESTUDO TÉCNICO PRELIMINAR

1. INFORMAÇÕES BÁSICAS

Número do Processo Digital 5512/2026

2. DESCRIÇÃO DA NECESSIDADE

2.1. Em resumo, a Secretaria de Administração e de Gestão de Pessoas através da Gerência Municipal de Tecnologia da Informação, justificou a contratação com o objetivo assegurar a continuidade da proteção da infraestrutura tecnológica da Prefeitura Municipal de Anchieta mediante a renovação do licenciamento e do suporte técnico especializado da solução de segurança perimetral Sophos XGS3300, atualmente integrada e em pleno funcionamento no ambiente de rede corporativa municipal.

2.2. O equipamento atua como elemento central da arquitetura de conectividade institucional, sendo responsável pelo roteamento do tráfego de dados, autenticação de usuários, compartilhamento de acesso à internet por meio de NAT e interligação segura entre o prédio sede da Prefeitura e suas unidades descentralizadas, abrangendo Secretarias Municipais, escolas da rede pública, Unidades de Saúde da Família, Pronto Atendimento e estruturas operacionais da Guarda Municipal. A indisponibilidade dessa solução comprometeria diretamente a prestação de serviços públicos essenciais, dada a dependência das atividades administrativas e finalísticas em relação à conectividade digital.

2.3. O cenário contemporâneo de segurança da informação caracteriza-se pelo aumento significativo da complexidade e da frequência de ameaças cibernéticas, incluindo ataques de ransomware, tentativas de intrusão e exploração de vulnerabilidades em sistemas públicos. Nesse contexto, a manutenção de solução classificada como Next-Generation Firewall mostra-se indispensável para garantir a confidencialidade, a integridade e a disponibilidade das informações institucionais.

2.4. Considerando que o contrato atualmente vigente possui término previsto para 23 de setembro de 2026, torna-se necessário o planejamento antecipado da renovação contratual, evitando a expiração do licenciamento e a consequente desativação automática de funcionalidades críticas do sistema, situação que poderia ocasionar paralisação sistêmica da rede municipal e interrupção de serviços digitais essenciais.

2.5. A contratação encontra aderência às diretrizes de governança de tecnologia da informação da Administração Municipal, especialmente no que se refere à continuidade dos serviços públicos digitais, à gestão de riscos operacionais e à proteção de dados pessoais tratados pela municipalidade.

2.6. A solução contribui diretamente para o atendimento das exigências da Lei Geral de Proteção de Dados Pessoais, ao viabilizar mecanismos de auditoria, rastreabilidade e armazenamento estruturado de logs de segurança, fortalecendo a capacidade institucional de monitoramento e resposta a incidentes. Além disso, a manutenção da plataforma tecnológica atualmente adotada preserva investimentos públicos já realizados e assegura estabilidade operacional da infraestrutura de rede.

3. ÁREA REQUISITANTE

3.1. Secretaria Municipal de Administração e Gestão de Pessoas (SAGP), através da Gerência Municipal de Tecnologia da Informação (GMTI).

3.2. Equipe Técnica da responsável pela atuação na fase interna do processo

3.2.1. Alexandre Oliveira dos Santos Gerente Municipal de Tecnologia da Informação

3.2.2. Edione Carlos Nunes Ribeiro Coordenador de Gestão e Segurança da Informação

4. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. A renovação do licenciamento deverá assegurar a continuidade integral das funcionalidades já implementadas na arquitetura tecnológica municipal, incluindo conectividade baseada em SD-WAN para balanceamento e monitoramento inteligente de múltiplos links de internet, inspeção profunda de pacotes, prevenção contra intrusões, proteção contra ataques de negação de serviço e inspeção de tráfego criptografado.

4.2. A solução deverá manter recursos avançados de defesa contra ameaças modernas, atualização contínua das assinaturas de segurança e geração de relatórios gerenciais e operacionais, garantindo capacidade permanente de prevenção, detecção e resposta a incidentes cibernéticos.

4.3. Adicionalmente, deverá ser assegurado suporte técnico especializado do fabricante, com níveis de atendimento compatíveis com a criticidade da infraestrutura municipal, incluindo atuação em nível

avançado de engenharia para correção de falhas, atualizações de firmware e apoio em incidentes complexos que extrapolem a operação rotineira da equipe local.

4.4. Dada a característica técnica do serviço, a empresa deve comprovar experiência prévia com o tipo de serviço a ser prestado, bem como comprovar possuir qualificação técnico-profissional.

5. SOLUÇÃO

5.1. A presente contratação trata-se da renovação do licenciamento da solução do appliance Sophos XGS3300 já integrada e operacional na infraestrutura da PMA, e não da aquisição de um novo modelo de appliance.

5.2. A GMTI apontou que a renovação do licenciamento dos equipamentos existentes evita custos desnecessários com a substituição de hardware físico em perfeito estado de funcionamento, além de eliminar a curva de aprendizado e horas técnicas necessárias para reconfiguração completa de uma nova topologia de segurança.

5.3. A continuidade dessa solução visa assegurar a manutenção dos padrões de segurança já estabelecidos, garantindo total compatibilidade com o ecossistema de TI municipal sem a necessidade de reconfigurações complexas que poderiam comprometer a eficiência operacional.

5.4. A implementação de soluções distintas traria incertezas quanto à capacidade de oferecer, de imediato, o mesmo nível de segurança e granularidade de controle atualmente garantidos pela solução Sophos.

5.5. Considerando que a PMA lida com dados sensíveis de cidadãos e sistemas críticos de saúde e educação, o risco de vulnerabilidades durante uma transição tecnológica deve ser ponderado. A manutenção do sistema atual evita a exposição desnecessária a ameaças que possam resultar em vazamentos de dados ou indisponibilidade de serviços essenciais.

5.6. A equipe da Gerência Municipal de Tecnologia da Informação (GMTI) já possui experiência consolidada e domínio prático na administração da plataforma Sophos. A curva de aprendizado para uma nova ferramenta demandaria tempo e recursos que impactariam a agilidade na resposta a incidentes. A indicação da marca Sophos para este processo encontra respaldo no princípio da padronização e na jurisprudência do Tribunal de Contas da União (TCU). Conforme a Súmula nº 270 do TCU, é possível a indicação de marca quando esta for estritamente necessária para atender exigências de padronização, desde que devidamente justificada.

Súmula nº 270, TCU:

"Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação."

5.7. Essa interpretação, que preserva tanto os padrões de qualidade quanto a clareza na definição do objeto licitado, ajusta-se ao caso em questão, promovendo a aplicação do princípio da padronização, conforme disposto no artigo 40, inciso V, alínea "a", e no artigo 47, inciso I, da Lei 14.133/2021.

"Art. 40: O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

(...)

V - atendimento aos princípios:

a) da padronização, considerando a compatibilidade de especificações estéticas, técnicas ou de desempenho;

(...)

Art. 47: As licitações de serviços atenderão aos princípios:

I - da padronização, considerando a compatibilidade de especificações estéticas, técnicas ou de desempenho.

5.8. O processo de padronização, previsto no artigo 43 da Lei 14.133/2021, deve preceder à licitação que estabelece a indicação de marca com esse fundamento. É importante mencionar que a padronização é reconhecida e aceita pelo TCU há muito tempo: Acórdão 1547/2004 - Primeira Câmara: "O princípio da padronização não conflita com a vedação de preferência de marca, desde que a decisão administrativa que identifica o produto pela marca seja devidamente justificada e comprove ser essa a escolha mais vantajosa para a administração, tanto tecnicamente quanto economicamente."

5.9. A indicação da marca Sophos não fere o princípio da isonomia ou da competitividade. Por se tratar de uma solução amplamente consolidada no mercado global, existe uma vasta rede de parceiros e revendas autorizadas capazes de competir no certame.

5.10. A indicação de marca não se confunde com exclusividade; a ampla oferta de fornecedores garante que a Administração obtenha o produto necessário por meio de um processo competitivo justo.

> "Acórdão 568/2009 - Primeira Câmara: "A demonstração de exclusividade de marca não comprova o requisito de inviabilidade de competição necessário para fundamentar inexigibilidade de licitação."

5.11. A análise técnica considerou que a substituição da solução atualmente adotada implicaria reestruturação completa da arquitetura de segurança, demandando aquisição de novos equipamentos, reconfiguração integral da rede, treinamento especializado da equipe técnica e possíveis interrupções operacionais durante o período de migração.

5.12. Tais fatores introduziriam riscos adicionais de vulnerabilidade temporária, especialmente relevantes considerando que o Município administra dados sensíveis relacionados à saúde, educação e gestão administrativa.

5.13. A manutenção da solução existente apresenta-se, portanto, como alternativa tecnicamente mais segura e economicamente racional.

5.14. Sobre o Suporte Técnico, conforme detalhado no DFD desta Gerência, o Firewall é o ponto central de toda a rede da Prefeitura de Anchieta. Qualquer falha técnica sem suporte especializado pode resultar na paralisação prolongada de serviços essenciais, como o Pronto Atendimento (PA) e as Unidades de Saúde (ESFs).

5.15. A contratação de suporte com SLA (Service Level Agreement) definido garante que, em caso de falha crítica, a Administração conte com tempo de resposta garantido para o restabelecimento dos serviços, transferindo o risco operacional ao fornecedor.

5.16. Embora a equipe da Gerência Municipal de Tecnologia da Informação (GMTI) possua expertise consolidada na operação da solução, o suporte técnico do fabricante atua como Nível 3 "N3 - Suporte Avançado do fabricante". Ele é acionado em casos de bugs de software, instabilidades imprevistas no firmware ou necessidades de ajustes arquiteturais complexos que fogem da rotina operacional. Portanto, o suporte não substitui a equipe local, mas a instrumentaliza com recursos de engenharia do próprio fabricante.

5.17. A contratação de suporte técnico evita o "gasto dobrado". É mais econômico contratar o suporte remoto do que arcar com os custos de remediação de um incidente de segurança ou com a inatividade de servidores públicos e sistemas municipais por falta de conectividade. A manutenção de um sistema de segurança sem suporte oficial é, por definição, uma fragilidade na gestão de riscos da Administração.

5.18. Pelo exposto, a contratação integrada do licenciamento e do suporte técnico especializado da solução Sophos XGS3300 configura-se como a única alternativa tecnicamente viável e administrativamente segura, plenamente alinhada aos princípios da continuidade do serviço público, da padronização e da eficiência administrativa.

5.19. Tal integração assegura não apenas o funcionamento ininterrupto da infraestrutura de rede e dos serviços essenciais da Prefeitura Municipal de Anchieta, como também garante a proteção contínua e dinâmica contra ameaças cibernéticas, bem como a preservação da integridade do patrimônio público, por meio da atualização permanente das políticas e mecanismos de segurança, além da garantia de substituição de hardware em caso de falhas ou defeitos.

5.20. A Gartner posiciona a Sophos como Líder no Quadrante Mágico para Network Firewalls, reconhecendo sua capacidade de execução e visão estratégica. Além disso, o fabricante possui certificações internacionais e aderência a boas práticas de segurança, assegurando confiabilidade, conformidade e suporte técnico especializado, aspectos essenciais para a continuidade dos serviços públicos municipais.

5.21. Dessa forma, a renovação conjunta do licenciamento e do suporte técnico mitiga riscos críticos de interrupção operacional (“apagão tecnológico”), ao mesmo tempo em que consolida uma estratégia de segurança da informação robusta, eficiente e economicamente vantajosa, em estrita conformidade com os preceitos estabelecidos na Lei nº 14.133/2021.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

6.1. RENOVAÇÃO DE LICENCIAMENTO DE SOFTWARE PARA O EQUIPAMENTO SOPHOS XGS 3300, CONTEMPLANDO DOIS APPLIANCES (PRINCIPAL E HA), PELO PERÍODO DE 36 MESES (3 ANOS)

6.1.1. A licença ofertada deverá contemplar os dois equipamentos atualmente instalados no Centro de Processamento de Dados do Município de Anchieta, pelo período de 36 (trinta e seis) meses.

6.1.2. A licença ofertada deve corresponder ao pacote **“Xstream Protection”** (ou superior), contemplando obrigatoriamente a atualização de firmware, garantia de hardware, suporte técnico do fabricante e os seguintes módulos de proteção ativos:

6.1.3. **Firewall de Base**: Firewall com inspeção de estado, VPN, sem fio;

6.1.4. **Proteção de Rede**: Gerenciamento de dispositivo SD-RED, IPS, Sophos X-Ops;

6.1.5. **Proteção da Web**: Controle e segurança da web, Controle de aplicativo, Proteção contra malware;

6.1.6. **NDR Essentials for Firewall**: Network Detection and Response

6.1.7. **Proteção de dia zero**: Machine Learning, Análise de arquivo de sandbox, Inteligência de ameaças;

6.1.8. **Central Orchestration** : SD-WAN VPN Orchestration, CFR Advanced ;

6.1.9. **DNS Protection**: Gerenciar o DNS Protection e definir as políticas de DNS no Sophos Central;

6.1.10. **Suporte Aprimorado**: Suporte aprimorado do fabricante;

6.1.11. **Suporte Aprimorado Plus**: Acesso prioritário 24/7, análise rápida de malware, recursos técnicos seniores, consultoria remota e gerentes dedicados.

6.1.12. A licença deve consistir de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

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

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

6.1.15. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

6.1.16. A descrição completa do item consta no Anexo I deste ETP.

6.2. SUPORTE TÉCNICO 24x7 E MONITORAMENTO PARA NEXT GENERATION FIREWALL

6.2.1. DESCRIÇÃO GERAL DO SERVIÇO

6.2.1.1. Suporte técnico remoto 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, com monitoramento contínuo e proativo, para o equipamento **Sophos Firewall XGS 3300**, assegurando a confidencialidade, disponibilidade, integridade, desempenho e segurança do ambiente de rede da Prefeitura Municipal de Anchieta.

6.2.2. ESCOPO DOS SERVIÇOS

6.2.2.1. Os serviços compreendem, de forma contínua e ininterrupta, as seguintes atividades:

I. **Atendimento e Monitoramento**

a) Atendimento técnico remoto 24x7, incluindo finais de semana e feriados;

b) Suporte especializado para o Sophos Firewall XGS 3300;

c) Monitoramento ativo e contínuo (24x7) do firewall, incluindo:

1) Disponibilidade do equipamento e dos serviços;

2) Utilização de CPU, memória e interfaces;

3) Status de saúde dos links de comunicação;

4) Detecção de falhas operacionais e alertas críticos de segurança;

II. **Gestão de Configurações e Incidentes**

a) Diagnóstico e resolução de incidentes que afetem o funcionamento, desempenho ou segurança do firewall;

b) Suporte técnico avançado para configurações de:

1) Regras de firewall e políticas de segurança;

2) NAT (DNAT, SNAT);

3) VPN (Site-to-Site, Client-to-Site e SSL VPN);

4) Roteamento Avançado;

5) Alta disponibilidade (HA);

6) Integração com Active Directory (AD).

C) Apoio na análise e mitigação de incidentes de segurança relacionados ao firewall;

D) Planejamento e execução de atualizações de firmware e hotfixes, mediante autorização prévia, incluindo obrigatoriamente a **realização de backup integral das configurações antes da execução** e a garantia de procedimento de **rollback (reversão)** imediato em caso de falha ou incompatibilidade da nova versão;

E) Abertura, acompanhamento e interação com o suporte oficial do fabricante Sophos, quando necessário;

F) Registro, acompanhamento e encerramento dos chamados técnicos, com histórico das ações executadas.

III. MODALIDADE DO ATENDIMENTO

A) Disponibilizar canais de abertura de chamados redundantes, disponíveis 24 horas por dia e 7 dias por semana (24x7), contemplando obrigatoriamente:

1) Plataforma Web para registro e acompanhamento de chamados;

2) Abertura de chamados via e-mail (informar o e-mail do suporte técnico);

3) Número telefônico (fixo ou 0800) para abertura de incidentes críticos em caso de indisponibilidade de internet na CONTRATANTE;

4) Suporte técnico via Whatsapp para comunicação ágil.

IV. MONITORAMENTO DO FIREWALL

A) O serviço deverá contemplar monitoramento contínuo e proativo (24x7) do Sophos Firewall XGS 3300, com o objetivo de:

1) Identificar preventivamente falhas, indisponibilidades e degradação de desempenho;

2) Gerar alertas para eventos críticos;

3) Atuar de forma preventiva sempre que possível;

4) Acionar procedimentos de suporte conforme o nível de severidade do incidente.

V. EQUIPE TÉNCICA

A) O serviço deverá ser executado por equipe técnica qualificada, composta por profissionais que atendem, no mínimo, aos seguintes requisitos:

1) Profissionais com certificação oficial Sophos, incluindo certificação Sophos Architect válida;

2) Experiência comprovada em administração e suporte de Sophos Firewall XGS, especialmente o modelo XGS 3300;

3) Conhecimento técnico em redes, segurança da informação e resposta a incidentes;

4) Capacidade de atuação em ambientes críticos.

VI. ACORDO DE NÍVEL DE SERVIÇO (SLA)

A) O serviço é prestado conforme o seguinte Acordo de Nível de Serviço (SLA):

Severidade	Descrição	Tempo Máximo de Resposta	Início do Atendimento
Crítica	Indisponibilidade total do firewall ou falha que interrompa serviços essenciais	Até 1 hora	Imediato
Alta	Falha com impacto significativo na operação	Até 2 horas	Até 2 horas
Média	Falha com impacto parcial ou risco potencial	Até 8 horas	Até 8 horas
Baixa	Ajustes, dúvidas ou solicitações sem impacto imediato	Até 24 horas	Agendado

B) Para incidentes de severidade Crítica e Alta, entende-se por "Resposta" o início efetivo da atuação técnica qualificada. Caso a solução definitiva dependa de engenharia do fabricante (Sophos), a CONTRATADA deverá apresentar uma Solução de Contorno (Workaround) em até 4 horas para restabelecer a conectividade mínima, ou apresentar justificativa técnica formal comprovando a impossibilidade.

VII. GESTÃO DE BACKUPS

a) Implementação e gerenciamento de rotina de backups automatizados diários e após qualquer alteração significativa de todas as configurações do Sophos Firewall XGS 3300;

b) Armazenamento dos arquivos de backup em repositório externo seguro (**off-site**) e criptografado, garantindo a recuperação das configurações mesmo em caso de perda total do appliance físico;

c) A CONTRATADA deverá disponibilizar à CONTRATANTE, sempre que solicitado e sem custos adicionais, cópia integral e atualizada dos arquivos de backup de configuração vigentes. A entrega deverá ocorrer em formato digital seguro no prazo máximo de **4 (quatro) horas** após a solicitação.

VIII. CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

A) Todas as informações, dados, configurações e acessos tratados durante a prestação do serviço **deverão ser mantidos sob sigilo absoluto**, em conformidade com a legislação vigente, especialmente a **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD)**, bem como com as boas práticas de Segurança da Informação.

B) No tratamento de dados pessoais a que tiver acesso durante a execução do objeto, a **CONTRATADA** atuará na qualidade de **OPERADORA**, devendo observar integralmente as disposições da **Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018 - LGPD)**, comprometendo-se a: 1**)** Tratar os dados exclusivamente mediante instruções da **CONTRATANTE** e para a estrita execução do suporte técnico e monitoramento contratado; 2**)** Implementar medidas técnicas e organizativas de segurança aptas a proteger os dados pessoais e institucionais contra acessos não autorizados, vazamentos, destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito; 3**)** Comunicar imediatamente à **CONTRATANTE** (no prazo máximo de 24 horas) a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados ou à infraestrutura municipal.

C) É estritamente vedado à **CONTRATADA** a transferência, cópia ou armazenamento de dados extraídos da infraestrutura da Prefeitura Municipal de Anchieta para ambientes externos, nuvens privadas não homologadas ou terceiros sem prévia e expressa autorização formal da **CONTRATANTE**, sob pena de responsabilização civil, administrativa e penal.

D) A **CONTRATADA** responderá solidariamente pelos danos patrimoniais, morais,

individuais ou coletivos que venha a causar em decorrência do descumprimento das normas de proteção de dados, isentando a **CONTRATANTE** de quaisquer ônus decorrentes de sua conduta culposa ou dolosa.

E) O dever de confidencialidade e sigilo subsistirá mesmo após o encerramento, rescisão ou extinção do contrato, devendo a **CONTRATADA**, ao final da vigência, devolver quaisquer dados que porventura estejam em sua posse ou em seus equipamentos de monitoramento.

7. ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS

7.1. Para a correta satisfação da necessidade pública, serão realizados diuturnamente todos os serviços constantes na tabela abaixo, de acordo com os seguintes itens e quantitativos:

ITEM	DESCRIÇÃO	VIGÊNCIA	TIPO	Unidade	Qtdade
01	Xstream Protection for XGS 3300	36 meses	Renovação	UN	1
02	XGS 3300 Enhanced to Enhanced Plus Support Upgrade	36 meses	Renovação	UN	1
03	**SUPORTE TÉCNICO 24x7 E MONITORAMENTO PARA NEXT GENERATION FIREWALL**	36 meses	----------	MÊS	36

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

8.1. O valor total estimado para licenças trienais e suporte técnico por 36 meses é de **R$ 130.774,84 (cento e trinta mil setecentos e setenta e quatro reais e oitenta e quatro centavos).**

ITEM	DESCRIÇÃO	VIGÊNCIA	TIPO	Unidad	Qtdade	Valor	Total

				e		**Unitário**	
01	Xstream Protection for XGS 3300	36 meses	Renovação	UN	1	186.890,32	186.890,32
02	XGS 3300 Enhanced to Enhanced Plus Support Upgrade	36 meses	Renovação	UN	1	27.178,05	27.178,05
03	**SUPORTE TÉCNICO 24x7 E MONITORAMENTO PARA NEXT GENERATION FIREWALL**	36 meses	----------	MÊS	36	4.951,56	178.256,16

8.2. Para a estimativa dos valores da contratação foram utilizadas as pesquisas de preço constantes no processo 5512/2026, realziadas pela GMTI.

8.3. Os valores constantes no ETP, são somente uma estimativa simplificada devendo a cotação de preços ser realizada através da Coordenação de Compras, que constará em Mapa Comparativo, no Termo de Referência e em Edital.

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

9.1. A contratação ocorrerá em lote único de forma integrada, conforme justificativa da GMTI:

(A) integração assegura não apenas o funcionamento ininterrupto da infraestrutura de rede e dos serviços essenciais da Prefeitura Municipal de Anchieta, como também garante a proteção contínua e dinâmica contra ameaças cibernéticas, bem como a preservação da integridade do patrimônio público, por meio da atualização permanente das políticas e mecanismos de segurança, além da garantia de substituição de hardware em caso de falhas ou defeitos.

(...)

A renovação conjunta do licenciamento e do suporte técnico mitiga riscos críticos de interrupção operacional ("apagão tecnológico"), ao mesmo tempo em que consolida uma estratégia de segurança da informação robusta, eficiente e economicamente vantajosa, em estrita conformidade com os preceitos estabelecidos na Lei nº 14.133/2021.

10. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

10.1. Não há.

11. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

11.1. Apesar da contratação não estar prevista no Cronograma de Compras da Prefeitura de Anchieta, instituído através do Decreto Municipal 6721, de 16 de dezembro de 2025 e se alinha a necessidade da Secretaria Municipal de Administração e Gestão de Pessoas e da Prefeitura de Anchieta.

12. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

12.1. Com a contratação, espera-se assegurar a continuidade dos serviços digitais municipais, reduzir a exposição a ameaças cibernéticas, manter elevados níveis de disponibilidade da rede corporativa e fortalecer a governança de segurança da informação, garantindo ambiente tecnológico estável e seguro para execução das políticas públicas.

13. PROVIDÊNCIAS A SEREM ADOTADAS

13.1. Como providências administrativas necessárias, deverão ser realizados a elaboração do Termo de Referência, a pesquisa de preços, a verificação da disponibilidade orçamentária e a formalização dos atos preparatórios exigidos pela legislação vigente.

13.2. O contrato deve ter sua vigência iniciada, após o fim da vigência do contrato em vigor.

14. POSSÍVEIS IMPACTOS AMBIENTAIS

14.1. Não foram identificados impactos ambientais significativos.

15. DECLARAÇÃO DE VIABILIDADE

15.1 Em virtude dos aspectos técnicos e econômicos explicitados nos itens deste documento, declaramos a viabilidade da contratação do objeto deste Estudo Preliminar, desde que atendidas as considerações realizadas neste instrumento e de que haja disponibilidade orçamentária.

Anchieta, 01 de abril de 2026.

16. RESPONSÁVEL PELO ETP:

Carlos Ricardo Balbino

Membro do NPCG - Mat. 3401

17. RESPONSÁVEL PELAS INFORMAÇÕES TÉCNICAS

Alexandre Oliveira dos Santos

Gerente Municipal de Tecnologia da Informação

Edione Carlos Nunes Ribeiro

Coordenador de Gestão e Segurança da Informação

ANEXO I – DESCRIÇÃO DO OBJETO

CÓD.: 61125

RENOVAÇÃO DE LICENCIAMENTO DE SOFTWARE PARA O EQUIPAMENTO SOPHOS XGS 3300, CONTEMPLANDO DOIS APPLIANCES (PRINCIPAL E HA), PELO PERÍODO DE 36 MESES (3 ANOS)

A licença ofertada deverá contemplar os dois equipamentos atualmente instalados no Centro de Processamento de Dados do Município de Anchieta, pelo período de 36 (trinta e seis) meses.

A licença ofertada deve corresponder ao pacote **"Xstream Protection"** (ou superior), contemplando obrigatoriamente a atualização de firmware, garantia de hardware, suporte técnico do fabricante e os seguintes módulos de proteção ativos:

Firewall de Base: Firewall com inspeção de estado, VPN, sem fio;

Proteção de Rede: Gerenciamento de dispositivo SD-RED, IPS, Sophos X-Ops;

Proteção da Web: Controle e segurança da web, Controle de aplicativo, Proteção contra malware;

NDR Essentials for Firewall: Network Detection and Response

Proteção de dia zero: Machine Learning, Análise de arquivo de sandbox, Inteligência de ameaças;

Central Orchestration : SD-WAN VPN Orchestration, CFR Advanced ;

DNS Protection: Gerenciar o DNS Protection e definir as políticas de DNS no Sophos Central;

Suporte Aprimorado: Suporte aprimorado do fabricante;

Suporte Aprimorado Plus: Acesso prioritário 24/7, análise rápida de malware, recursos técnicos seniores, consultoria remota e gerentes dedicados.

A licença deve consistir de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

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

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

A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

SOBRE O SOFTWARE

O software dever ser capaz de fazer bloqueio de IP'S por países.

O software deverá ser fornecido em sua versão mais atualizada.

O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou

modo ativo-ativo e deve possibilitar monitoração de falha de link.

Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

A atualização de software deverá enviar avisos de atualização automáticos.

O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

As notificações deverão ser realizadas via email e SNMP.

Suportar SNMPv3 e Netflow.

O firewall deverá ser stateful, com inspeção profunda de pacotes.

As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

As políticas de NAT deverão ser customizáveis para cada regra.

A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

Proteção contra anti-spoofing.

Suportar IPv4 e IPv6.

Possuir certificação IPv6 Ready;

IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP).

Deve suportar Roteamento BGP com uso de IPv6;

Suportar Delegação de Prefixo IPV6 (DHCP PD);

O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integrar de terceiros;

Deve possuir tecnologia de conectividade SD-WAN;

A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces,

Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções:

a. conexão:

b. IP de origem;

c. IP de destino;

d. IP de origem e destino.

Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga.

Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

Deve suportar o uso de, no mínimo, 3 (três) links;

Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado

A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

Deve possibilitar o roteamento baseado em VPNs;

Deve suportar criar políticas de roteamento;

Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

a. Interface de entrada do pacote;

b. IPs de origem;

c. IPs de destino;

d. Portas de destino;

e. Usuários ou grupos de usuários;

f. Aplicação em camada 7.

Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento

Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

Deve suportar Extended VLAN;

O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

Deve permitir a configuração de jumbo frames nas interfaces de rede;

Deve permitir a criação de um grupo de portas layer2;

A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

Deve possuir otimização em tempo real de voz sobre IP.

Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

CONTROLE POR POLÍTICAS DE FIREWALL

Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

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

Controle de políticas por países via localização por IP.

Suporte a objetos e regras IPv6.

Suporte a objetos e regras multicast.

PREVENÇÃO DE AMEAÇAS

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;

Para a eficácia da análise de malwares Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;

A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem;

A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

Deve ter proteção em tempo real contra novas ameaças criadas.

Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

Deve permitir o bloqueio de vulnerabilidades.

Deve permitir o bloqueio de exploits conhecidos.

Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle

utilizando múltiplas camadas de DNS, AFC e firewall.

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.

Suportar bloqueio de arquivos por tipo.

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 ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: 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 usuários, origem, destino, zonas de segurança.

CONTROLE E PROTEÇÃO DE APLICAÇÕES

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3

O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas

Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)

Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

Limitar a banda usada por aplicações (traffic shaping).

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuirem acesso a estes aplicativos devem ter a utilização bloqueada.

CONTROLE E PROTEÇÃO WEB

Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Azure AD, Radius, E-directory e base de dados local;

Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

Possuir pelo menos 90 categorias de URLs;

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

Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

Deve ser capaz de forçar as restrições do Youtube

Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

Suportar a criação categorias de URLs customizadas;

Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada

Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

Deve ser possível realizar caching do conteúdo web;

Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré determinados para acessar sites na internet.

A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

Deve possuir capacidade de alguns usuários préviamente selecionados realizarem um bypass temporário na política de bloqueio atual.

A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar;

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, autenticando via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local, 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 Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64.

Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory.

Dever suportar a configuração de logon único (Single sign-on) para que os administradores façam logon no console da Web usando o Azure AD

Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

QUALIDADE DE SERVIÇO - QoS

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo 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.

A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.

Suportar priorização Real-Time de protocolos de voz (VoIP).

Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP;

REDES VIRTUAIS PRIVADAS - VPN

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

Suportar IPsec VPN.

Suportar SSL VPN.

Suportar L2TP e PPTP.

Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

Deve possuir opção de VPN IPSEC com client nativo do fabricante.

Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os appliances e o VPN da AWS.

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

Suportar autenticação via AD/LDAP, Token e base de usuários local;

Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local;

GERÊNCIA ADMINISTRATIVA CENTRALIZADA

Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

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

Estar licenciada para gerenciar as soluções de firewall de próxima geração do appliance NGFW (item 2)

Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.

Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração (item 2), sem necessidade de acesso direto aos equipamentos.

Deve permitir a criação de Templates para configurações.

Deve possuir indicadores do estado de equipamentos e rede.

Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automatico de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

Deve possibilitar o envio dos logs via syslog com conexão segura (TLS)

GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

Estar licenciada para gerenciar as soluções de Firewall de Próxima Geração.

Deverá prover relatórios baseados em usuários com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

Deve possibilitar a identicação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

Deve conter customizações dos relatórios para inserção de logotipos próprios.

Deve fornecer relatórios de compliance SOX, HIPAA, GLBA, FISMA, PCI, CIPA

Deve permitir a exportação via PDF ou Excel.

Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

Deve fornecer relatórios de tendências.

Deve fornecer logs em tempo real, de auditoria e arquivados.

Deve possuir mecanismo de procura de logs arquivados.

Deve ter acesso baseado em Web com controles administrativos distintos.

COMPATIBILIDADE

O software do NGFW (Next-Generation Firewall) deve ser do mesmo fabricante do appliance porque ambos são projetados para operar de forma integrada. Essa compatibilidade garante o melhor desempenho, segurança e estabilidade, já que o sistema operacional, os drivers e os recursos de aceleração de hardware são otimizados para trabalhar juntos. Além disso, somente com essa combinação é possível garantir atualizações contínuas, correções de vulnerabilidades, suporte técnico especializado e a manutenção da garantia do equipamento. A

instalação de software de terceiros ou de outro fabricante em um appliance pode resultar em falhas críticas, baixa performance, perda de funcionalidades e até a invalidação do contrato de suporte ou licenciamento.