TERMO DE REFERÊNCIA

Aquisição de Next Generation Firewall Para o SESC-ES

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de firewall corporativo para atender as demandas de proteção da rede internade dados e dos recursos de TI do SESC – ES e suas respectivas Unidades Operacionais;

2. ESCOPO

2.1. A aquisição ocorrerá de acordo com o quadro abaixo:

Item	Descrição	Un	Qtde
01	Equipamento firewall SEDE	Un	01
02	Equipamento firewall Unidades Operacionais	Un	16
03	Licença de software e manutenção	Mês	36
04	Suporte técnico padrão do FABRICANTE (nível helpdesk: 5x8)	Mês	36
05	Garantia do equipamento	Mês	36
06	Serviço de instalação, configuração inicial e Treinamento	Un	01

3. JUSTIFICATIVA DA CONTRATAÇÃO

3.1. NECESSIDADE DA CONTRATAÇÃO

3.1.1. O firewall corporativo é um ativo de segurança da informação fundamental numa rededede dados empresarial, uma vez que ele regula/monitora todo o tráfego de entrada e saída na rede (norte - sul), assim como o tráfego lateral (leste – oeste), principalmente considerando segmentos corporativos (vlans), servidores físicos, virtuais e dmz, IoT e ambiente de rede sem fio para visitantes;

3.1.2. Por meio da introspecção dos dados de rede, o firewall corporativo é capaz de bloquear acessos não autorizados, mediar o uso de internet, criar conexões seguras com escritórios e clientes, bem como oferecer atualizações automáticas para ameaças de dia zero (zero-day malware);

3.1.3. As Soluções de Firewall de Próxima Geração (Next Generation Firewall são tecnologias modernas de Firewall que representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes confiáveis e não confiáveis (Internet) e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Isso é possível, através de um sistema de detecção de intrusões, anti-malware na camada de rede, filtragem de tráfego web malicioso e a inspeção de tráfego SSL na busca de ameaças camufladas sobre a camada de criptografia;

3.1.4. Considerando a relevância que a SESC - ES adquire no setor de educação, serviços e turismo e a previsão de ampliação da atividade, torna-se ainda mais necessário o investimento em segurança da informação;

3.1.5. O SESC - ES atualmente possui um equipamento Firewall atuando nas conexões de borda, protegendo o tráfego que entra ou sai da rede interna. Para realizar a proteção de todaa rede interna, é necessário equipamento com especificações superiores, uma vez que o tráfego a ser analisado é substancialmente maior;

3.2. JUSTIFICATIVA PARA CARACTERISTICAS TÉCNICAS

3.2.1. Todos os equipamentos devem ser do mesmo fabricante, devido a padronização do ambiente e unificação da ferramenta de gerenciamento. Desta forma, utilizando um equipamento firewall central do mesmo fabricante das unidades remotas, a equipe de TI pode aplicar regras integradas e homogêneas, eliminando prejuízos causados por eventuais incompatibilidades;

3.3. MÉTRICAS DE DESEMPENHO DO EQUIPAMENTO ATUAL

3.4. Para assegurar o correto dimensionamento do equipamento a ser adquirido, abaixo, apresentamos o sumário das métricas médias de desempenho monitoradas ao longo de duas semanas:

Item Recurso Monitorado

01 Número de sessões ativas 27.223

02 Número de usuários ativos 633

04 Throughput (Mbps por segundo) 2.000

05 Novas conexões por segundo 259

4. ESPECIFICAÇÕES TÉCNICAS DO EQUIPAMENTO FIREWALL

4.1. ASPECTOS GERAIS – Solução de NGFW e SD-WAN seguro com Gerenciamento Centralizado

4.1.1. O equipamento a ser ofertado deverá ser novo e estar em plena fabricação. Não serão aceitos equipamentos que possuam avisos de "End-of-life" emitidos pelo fabricante ou que estejam na iminência de serem substituídos por modelos de famílias subsequentes;

4.1.2. O equipamento a ser ofertado deve permitir instalação em Rack, através de suporte de sustentação lateral (Rack Mount). Caso necessário, O equipamento deverá ser fornecido com os trilhos para deslizamento e instalação no Rack;

4.1.3. O equipamento a ser ofertado deve ser físico e não virtual, considerando ASICS desenvolvidos pelo próprio fabricante;

4.2. INTERFACE

4.2.1. O equipamento a ser ofertado para a SEDE deve possuir:

Throughput de, no mínimo, 3 Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

Throughput de, no mínimo, 13 Gbps de VPN IPSec para ser utilizado no SD-WAN;

Estar licenciado para, ou suportar sem o uso de licença, 2000 túneis de VPN IPSEC Site-to-Site simultâneos;

Suportar no mínimo 4 Gbps de throughput de Inspeção SSL;Com

no mínimo as seguintes interfaces:

- USB 1x

- Console 1x

- Alta Disponibilidade/Gerenciamento RJ45 2x

- 1Gigabit Ethernet RJ45 16x

- 10Gigabit Ethernet SFP+ 2x

- 10Gigabit Ethernet SFP+ FortiLink Slots 2x

- 1Gigabit Ethernet SFP Slots 8x

- Alimentação: Duas Fontes de Alimentação AC

Equipado com:

- 4 SFP+ de 10G Duplex LC;

- 4 SFP de 1G Duplex LC;

(Referência FortiGate 200F, as SFP também deverão ser do mesmo fabricante)

4.2.2. O equipamento a ser ofertado para as Unidades Operacionais deve possuir, no mínimo as seguintes interfaces:

- USB 1x

- Console 1x

- Porta WAN Gigabit Ethernet RJ45 2x

- Porta DMZ Gigabit Ethernet RJ45 1x

- Gigabit Ethernet RJ45 FortiLink 2x

- Gigabit Ethernet RJ45 5x

- Alimentação: Uma Fontes de Alimentação AC

(Referência FortiGate 60F)

4.3. CARACTERÍSTICAS DE FUNCIONAMENTO

4.3.1. O equipamento a ser ofertado deve possuir uma plataforma otimizada para análise de conteúdo de aplicações em camada 7 do modelo OSI;

4.3.2. O equipamento a ser ofertado deve possibilitar o acesso direto ao mesmo para aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização através de isolamento do processamentode gerenciamento e do processamento do tráfego inspecionado;

4.3.3. O equipamento a ser ofertado deve possuir e estar equipado com todo o hardware e as licenças de softwares necessárias para o seu correto funcionamento no ambiente da SESC – ES;

4.3.4. O equipamento a ser ofertado deve deverá ser fornecido em sua versão mais recente e atualizada;

4.3.5. O equipamento a ser ofertado deve suportar o gerenciamento da solução através de acesso via SSH, cliente ou WEB (HTTPS);

4.3.6. O equipamento a ser ofertado deve possuir dispositivos de proteção de rede com pelo menos as seguintes funcionalidades:

- Suporte a DHCP Relay, DHCP Server;

4.3.7. O equipamento a ser ofertado deve suportar os seguintes tipos de NAT:

- NAT dinâmico (Many-to-1);

- NAT dinâmico (Many-to-Many);

- NAT estático (1-to-1);

- NAT estático (Many-to-Many);

- NAT estático bidirecional 1-to-1;

- Tradução de porta (PAT);

- NAT de Origem; NAT de Destino;

- O equipamento a ser ofertado deve suportar NAT de Origem e NAT de Destino simultaneamente;

4.3.9. O equipamento a ser ofertado deve permitir monitorar via SNMP falhas de hardware,uso de recursos e estatísticas de uso das interfaces de rede;

4.3.10. O equipamento a ser ofertado deve enviar log para sistemas de monitoração externos, simultaneamente;

4.3.11. O equipamento a ser ofertado deve oferecer e possuir a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL ou syslog;

4.3.12. O equipamento a ser ofertado deve possuir proteção anti-spoofing;

4.3.13. O equipamento a ser ofertado deve ter a capacidade de operar de forma simultâneaem uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos:

- Modo Sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3)do modelo OSI;

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

- Modo Camada – 2 (L2) do modelo OSI, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

- Modo Camada – 3 (L3) do modelo OSI, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

4.3.14. O equipamento a ser ofertado deve suportar a configuração de alta disponibilidade em pelo menos na camada 3 do modelo OSI;

4.3.15. O equipamento a ser ofertado deve permitir em modo HA (modo de Alta- Disponibilidade) a monitoração de falha de link;

4.3.16. O equipamento a ser ofertado deve suportar a configuração em alta disponibilidade possibilitando a instalação de cada membro, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP) do modelo OSI;

5. FUNÇÕES DE PROTEÇÃO DO SOFTWARE

5.1. CONTROLE DE POLÍTICAS

5.1.1. O software a ser ofertado deve suportar controles por zona de segurança;

5.1.2. O software a ser ofertado deve possuir Controles de Políticas por porta e protocolo;

5.1.3. O software a ser ofertado deve possuir Controle de Políticas por Aplicações, Grupos Estáticos de Aplicações, Grupos Dinâmicos de Aplicações (baseados em características e comportamento das aplicações) e Categorias de Aplicações;

5.1.4. O software a ser ofertado deve possuir Controle de Políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.1.5. O software a ser ofertado deve possuir Controle de Inspeção e de Criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

5.1.6. O software a ser ofertado deve suportar a Inspeção de conexões SSL de entrada (Inbound);

5.1.7. O software a ser ofertado deve criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 ou superior;

5.1.8. O software a ser ofertado deve permitir criar bloqueios para qualquer tipo de arquivo configurado pelo SESC-ES, conforme exemplos: bat, cab, dll, exe, bin, zip, tar, mp3 ;

5.2. CONTROLE DE APLICAÇÕES

5.2.1. O software a ser ofertado deve possuir em seus dispositivos de proteção de rede, a capacidade de reconhecer aplicações, independente de porta e protocolo;

5.2.2. O software a ser ofertado deve possuir a capacidade liberação e bloqueio pelos meios mais variados, como, por exemplo: aplicações, portas, protocolos;

5.2.3. O software a ser ofertado deve reconhecer aplicações diferentes, incluindo o tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e- mail;

5.2.4. O software a ser ofertado deve reconhecer pelo menos as seguintes aplicações: Microsoft Office 365 (Admin Center, Calendário Conformidade, Delve, Excel, Forms, Kaizala, Lists, OneDrive, OneNote, Outlook, Pessoas Planner, Power Apps, Power Automate, PowerPoint, Segurança, Stream, Sway, Teams, To Do, Whiteboard, Word, Yammer), Redes Sociais (facebook, linked-in, twitter, Instagram, Linktree, Wixsite, Issuu) Acesso Remoto (citrix, logmein, teamviewer, ms-rdp, vnc, AnyDesk, Ammyy), Stream (youtube), http-proxy, http- tunnel, whatsapp, db2, mysql, Sql, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http;

5.2.5. O software a ser ofertado deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

5.2.6. O software a ser ofertado deve, para o tráfego criptografado SSL, descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.2.7. O software a ser ofertado deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde coma especificação do protocolo, incluindo, mas não limitado, usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

5.2.8. O software a ser ofertado deve identificar o uso de táticas evasivas via comunicações criptografadas;

5.2.9. O software a ser ofertado deve atualizar a base de assinaturas de aplicações automaticamente;

5.2.10. O software a ser ofertado deve limitar a banda (download/upload) usada por aplicações (Rate Limiting), baseado no IP de origem, usuários e grupos do LDAP/AD;

5.2.11. O software a ser ofertado deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory (AD), permitindo, se for o caso, a instalação de agentes;

5.2.12. O software a ser ofertado deve permitir 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;

5.2.13. O software a ser ofertado deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

5.2.14. O software a ser ofertado deve alertar o operador ou administrador quando uma aplicação for bloqueada;

5.2.15. O software a ser ofertado deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

5.2.16. O software a ser ofertado deve possibilitar a diferenciação de tráfegos (ex: Banco de dados, Internet, E-mail, Videoconferência) possuindo granularidade de controle/políticas para os mesmos;

5.2.17. IPS – Intrusion Prevention System

5.2.18. O software a ser ofertado deve possuir para proteção do ambiente contra-ataques, dispositivos de proteção utilizando módulo de IPS e Anti-Malware integrados no próprio Appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;

5.2.19. O software a ser ofertado deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

5.2.20. O software a ser ofertado deve sincronizar as assinaturas de IPS quandoimplementado em alta disponibilidade;

5.2.21. O software a ser ofertado deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

5.2.22. O software a ser ofertado deve implementar exceções por IP de origem ou de destino através de regras e de assinatura a assinatura;

5.2.23. O software a ser ofertado deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.2.24. O software a ser ofertado deve permitir o bloqueio de vulnerabilidades;

5.2.25. O software a ser ofertado deve permitir o bloqueio de exploits conhecidos;

5.2.26. O software a ser ofertado deve incluir proteção contra-ataques de negação de serviços;

5.2.27. O software a ser ofertado deve possuir os seguintes mecanismos de inspeção de IPS:

- Análise de padrões de estado de conexões;
- Análise de decodificação de protocolo;
- Análise para detecção de anomalias de protocolo;
- IP Defragmentation;
- Remontagem de pacotes de TCP;
- Bloqueio de pacotes malformados;

5.2.34. O software a ser ofertado deve ser imune e capaz de impedir ataques básicos como:Syn flood, ICMP flood, UDP flood, etc;

5.2.35. O software a ser ofertado deve detectar e bloquear a origem de portscans;

5.2.36. O software a ser ofertado deve bloquear ataques efetuados por Worms conhecidos, permitindo ao administrador acrescentar novos padrões;

5.2.37. O software a ser ofertado deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

5.2.38. O software a ser ofertado deve possuir assinaturas para bloqueio de ataques de buffer overflow;

5.2.39. O software a ser ofertado deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

5.2.40. O software a ser ofertado deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

5.2.41. O software a ser ofertado deve permitir o bloqueio de vírus e Spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3;

5.2.42. O software a ser ofertado deve suportar bloqueio de arquivos por tipo;

5.2.43. O software a ser ofertado deve identificar e bloquear comunicação com botnets;

5.2.44. O software a ser ofertado deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

- Nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

5.2.45. O software a ser ofertado deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

5.2.46. O software a ser ofertado deve incluir proteção contra vírus em conteúdo HTML e Javascript, software espião (Spyware) e Worms;

5.2.47. O software a ser ofertado deve possuir e implementar proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;

5.3. FILTRO DE URL

5.3.1. O software a ser ofertado deve possuir as funcionalidades de filtro de URL;

5.3.2. O software a ser ofertado deve possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

5.3.3. O software a ser ofertado deve possuir a capacidade de criação de políticas baseadasna visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

5.3.4. O software a ser ofertado deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

5.3.5. O software a ser ofertado deve possuir base ou cache de URLs local no Appliance ouem nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

5.3.6. O software a ser ofertado deve possuir pelo menos 60 (Sessenta) categorias de URLs;

5.3.7. O software a ser ofertado deve permitir a criação de categorias de URLs customizadas;

5.3.8. O software a ser ofertado deve possuir a função de exclusão de URLs do bloqueio, por categoria;

5.3.9. O software a ser ofertado deve permitir a customização de página de bloqueio;

5.3.10. O software a ser ofertado deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessandoo site);

5.4. IDENTIFICAÇÃO DE USUÁRIOS

5.4.1. O software a ser ofertado deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local;

5.4.2. O software a ser ofertado deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadasem usuários e grupos de usuários;

5.4.3. O software a ser ofertado deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019;

5.4.4. O software a ser ofertado deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

5.5. FILTRO DE DADOS

5.5.1. O software a ser ofertado deve permitir a criação de filtros para arquivos e dados pré-definidos;

5.5.2. O software a ser ofertado deve permitir que os arquivos possam ser identificados por extensão e assinaturas;

5.5.3. O software a ser ofertado deve identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP). Entende-se como transferência o controle de download;

5.6. VPN

5.6.1. O software a ser ofertado deve suportar VPN Site-to-Site;

5.6.2. O software a ser ofertado deve suportar IPSec VPN;

5.6.3. A VPN IPSEc deve suportar:

- 3DES, Autenticação MD5 e SHA-1;

- Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

- Algoritmo Internet Key Exchange (IKEv1 e v2) e AES 128, 192 e 256 (Advanced Encryption Standard);

5.6.4. O software a ser ofertado deve suportar autenticação via certificado IKE PKI;

5.6.5. O software a ser ofertado deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução;

5.7. CONFIGURAÇÃO INICIAL DA SOLUÇÃO

5.8. O FORNECEDOR deverá auxiliar remotamente a instalação física e as configurações iniciais do equipamento. O FORNECEDOR informará na reunião de início de projeto as configurações que deverão ser realizadas nesta etapa e solicitar novas informações da topologia de rede, caso necessário;

5.9. O FORNECEDOR deverá realizar a configuração inicial do firewall para monitorar o tráfegode rede;

5.10. A implantação deverá iniciar em no máximo 15 dias após a notificação para a execução do serviço e ser cumprida em no máximo 15 dias úteis;

5.11. Ao termino da instalação deverão ser treinados/capacitados 3 membros da equipe, com as funcionalidades implantadas, fundamentos básicos, introdução, administração e troubleshooting.

6. SUPORTE TÉCNICO PADRÃO DO FABRICANTE

6.1. O FORNECEDOR deverá informar uma senha para o acesso ao sítio do FABRICANTE na internet para suporte ao produto ofertado, fóruns, documentos, drivers, softwares ou quaisquer outras informações referentes à solução;

6.2. O acesso ao suporte técnico do FABRICANTE respeitará o horário comercial (regime 8x5),nos dias úteis da semana, obedecendo a seguinte janela de horário: 07:30 até 17:30, (fuso horário Brasilia);

6.3. O suporte técnico do FABRICANTE será de nível básico, característico a helpdesk (respostas a questionamentos).

6.4. O suporte técnico sob demanda, caso necessário, será executado somente nas situações em que a equipe técnica de Ti julgar necessário, com valores que serão acordados entre as PARTES;

6.5. O Fornecedor será corresponsável pelo suporte técnico especializado e certificado pelo Fabricante.

7. GARANTIA

7.1. O FABRICANTE deverá oferecer garantia total ao equipamento em 36 meses;

7.2. A GARANTIA compreende desde a reposição de peças até a substituição do equipamento na hipótese do mesmo apresentar sucessivos defeitos;

7.3. Entende-se como sucessivos defeitos aqueles: (1) problemas de natureza distinta que ocorrerem três vezes durante o ano. (2) problemas de mesma natureza que ocorrerem duas vezes num período de 6 meses;

7.4. Nos primeiros 90 dias após a implementação o tempo máximo para o reparo/substituição do equipamento será de 24horas corridas, após esse prazo o tempo máximo será de 120horas corridas após abertura de chamado;

7.5 O Fornecedor será corresponsável pela GARANTIA.

7.6 O Fornecedor será corresponsável pela GARANTIA junto ao Fabricante.

8. FORNECEDOR

8.1 O FORNECEDOR deverá possuir “Certificado de Revendedor Autorizado” do fabricante, assim como possuir no mínimo 3 profissionais certificados em “Network Security Architect” ou superior;