ESPECIFICAÇÃO TÉCNICA

1. OBJETO

Estabelecer requisitos técnicos para aquisição de Solução de Segurança de Alta Disponibilidade para tráfego de rede com características de "Next Generation Firewall", com garantia de funcionamento, reposição e atualização de assinaturas de proteção pelo prazo de:
Ponto em Curitiba 60 (sessenta) meses
Ponto em Londrina 36 (trinta e seis) meses.

2. OBJETIVO

Implementar melhoria de segurança cibernética na Rede do CECS.

3. ESCOPO

Solução de Segurança com características de "Next Generation Firewall" composta de 2 (dois) equipamentos dedicados (appliance).

Garantia/Suporte da Solução de "Next Generation Firewall":
Ponto Curitiba 60 (sessenta) meses;
Ponto Londrina 36 (trinta e seis) meses.

Atualizações de software e assinaturas de segurança da Solução de Next Generation Firewall por
Ponto Curitiba 60 (sessenta) meses;
Ponto Londrina 36 (trinta e seis) meses.

4. CARACTERÍSTICAS

CARACTERÍSTICAS BÁSICAS DA SOLUÇÃO DE SEGURANÇA DE ALTA DISPONIBILIDADE

Deve ser composta por, no mínimo, 2 (dois) equipamentos dedicados (appliance), todos com hardware e software fornecidos pelo mesmo fabricante;

Deve suportar e estar licenciada para operação em cluster "ativo-ativo" ou "ativo-passivo";

Deve sincronizar entre os appliances de um mesmo cluster: todas as configurações, sessões TCP/IP, tabelas NAT, listas de assinaturas utilizadas para proteção contra ameaças, tabelas FIB e associações de segurança das VPNs;

Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um appliance do cluster, a falha de qualquer componente ou processo crítico de um do appliance do cluster;

Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sem interrupções de tráfego;

O equipamento (appliance) que compõem um cluster de alta disponibilidade devem compartilhar o mesmo conjunto de regras e configurações;

A solução de segurança deve ter capacidade para implementar de forma integrada e simultânea as funcionalidades de:

Alta disponibilidade – equipamentos operando em conjunto, podendo operar em modo "Ativo/Ativo" ou "Ativo/Passivo";

Geração de relatórios das atividades de inspeção e segurança;

Registro de LOG das atividades de inspeção e segurança;

Filtro de pacotes do tipo "Statefull Inspection";

Controle de aplicações;

Integração com serviços de autenticação de usuários (LDAP/Active Directory);

Identificação de todos os usuários no tráfego inspecionado;

Administração de largura de banda (QoS – Quality of Service);

VPN (Virtual Private Network) IPSec ("site-to-site" e "client-to-site") e SSL;

IPS – Intrusion Prevention System (Deteção e prevenção de Intrusos);

Prevenção contra ameaças de vírus, spywares, malwares, botnets;

Inspeção e bloqueio de ameaças em tráfego SSL;

Atualização de bases de assinaturas sem necessidade de "reset" de equipamentos;

Os equipamentos devem ser novos e sem uso, deve estar "em linha de produção", ou seja, ainda são produzidos pelo seu fabricante e devem ter suporte de seu fabricante. Os softwares também devem ser de versão mais recente do fabricante e devem ter suporte. Não serão aceitos equipamento ou softwares em modo "End of Life" (fabricante parou de fabricar), "End of Support" (fabricante parou de oferecer suporte) ou "End of Sale" (fabricante anunciou o fim das vendas) na data da proposta;
A garantia de funcionamento da solução deve contemplar todos os serviços e atividades necessários para manter a solução atualizada tecnologicamente e em perfeito estado de funcionamento, tais como: manutenção corretiva, substituição de peças e componentes, atualizações de versões (com novas funcionalidades ou correções) dos programas (softwares, firmwares, drivers), ajustes técnicos ou de configurações, etc.;

A garantia de funcionamento deve contemplar a atualização de assinaturas de proteção de todos os serviços e atividades, manuais ou automatizados, necessários para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação e

classificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa, etc.;

O suporte técnico da solução deve contemplar todos os serviços e atividades necessários ao esclarecimento de dúvidas ou orientação técnica da equipe técnica do CECS, visando ao uso adequado e otimizado da solução. Deverá ser disponibilizado o acesso, por meio da Internet, de base de documentos e conhecimentos mantida pelo fabricante da solução, contemplando seus manuais de instalação, utilização e correção de problemas, incluindo exemplos de configuração e melhores práticas de uso.

5. LICENCIAMENTO E ATUALIZAÇÃO

Todos os componentes de software e/ou firmware da solução deverão ser fornecidos com licença de uso em caráter permanente para todas as funcionalidades, assinaturas, listas e demais métodos de detecção e de prevenção de ameaças, bem como quantidades do contrato;

Durante o período de vigência do contrato de garantia o CECS terá direito às versões mais atualizadas de software, firmwares, bases de assinaturas, demais bases de informações e/ou documentações, disponibilizadas pelo fabricante;

As funcionalidades de controle de aplicações, IPS, Antivírus e Antispyware, VPN IPSec e SSL, QoS, Descriptografia SSL e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

6. CAPACIDADES INDIVIDUAIS – EQUIPAMENTO

Suportar 270Mbps de throughput de “Threat Prevention” ou “Threat Protection” com pelo menos as seguintes funcionalidades habilitadas para todo o tráfego: firewall, controle de aplicação, IPS (Intrusion Prevention System), antivirus, antibot ou antispyware. Observação: esses valores de capacidade se referem a simulações com tráfego “Enterprise” ou “blend de protocolos” ou “tráfego real corportativo”, e não com tráfego em condições ideais (exemplo: simulações com tráfego UDP de 1518 bytes) que não correspondem à realidade do tráfego de um ambiente corporativo heterogêneo;

Prevenção de ameaças (Mbps) 500

Firewall de última geração (Mbps) 970

Taxa de transferência IPS (Mbps) 1.050

Taxa de transferência do firewall (Mbps) 2.800

Pacotes UDP de 1518 bytes de firewall (Mbps) 6.400

Taxa de transferência VPN AES-128 (Mbps) 1.950

Conexões por segundo 15.750

Conexões simultâneas 500.000

Estas capacidades deverão ser comprovadas em documentos oficiais e públicos disponibilizados pelo fabricante em sua página web oficial;
Esta capacidade se refere ao equipamento individual, não considerando eventual utilização em cluster.

A ausência de documentos comprobatórios mencionados acima reservará ao CECS o direito de aferir o desempenho do equipamento em bancada, assim como atendimento de todas as funcionalidades especificadas neste documento. Caso seja comprovado o não atendimento das capacidades e/ou especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei.

7. CARACTERÍSTICAS GERAIS DO HARDWARE – (APPLIANCE)

O equipamento (hardware) deve ser do tipo appliance de propósito específico, comercializado, em conjunto com seu software, para segurança de rede. Não serão aceitos equipamentos ou servidores de uso genérico;

Deve possuir fonte de alimentação de 12VDC, ou acompanhar inversor/conversor externo dedicado e adequadamente dimensionado para que o equipamento seja alimentado.

Deve possuir, no mínimo, as seguintes quantidades de interfaces:

01 (uma) porta do tipo USB 3.0 USB Port;

01 (uma) entrada de SD Card;

01 (uma) porta xDSL RJ11 ADSL2 (Annex A or B) and VDSL2 (up to 17a);

08 (oito) interfaces de rede 10/100/1000Base-T em portas de cobre (RJ-45), sendo possível o atendimento com portas 1000Base-T SFPs, desde que sejam entregues equipadas com os respectivos transceivers;

01 (uma) porta do tipo “console” para configuração e gerenciamento via linha de comando (CLI), com respectivo cabo e/ou conector, se for o caso de cabo diferente do padrão Ethernet deve ser fornecido 1 (um) cabo padrão da porta coso tipo USB-C;

01 (uma) interface de rede 10/100/1000Base-T em cobre ou padrão 1000Base- X com transceiver multimodo dedicada para gerenciamento, além das demais interfaces descritas anteriormente;

Deve ser fornecido em sua capacidade máxima de processamento e memória;

01 (uma) porta interface de rede 10/100/1000Base-T RJ 45 DMZ Port;

Deve ser fornecido com todas as suas portas de comunicação, interfaces de rede e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;

Deve possuir as certificações, registros e liberações para comercialização e operação no Brasil, estando em conformidade com as normas da ANATEL, na data da entrega do equipamento.

8. FUNCIONALIDADES BÁSICA DO EQUIPAMENTO (APPLIANCE) DA SOLUÇÃO

Deve permitir o acesso ao equipamento via CLI (interface de linha de comando) (console), SSH e interface Web HTTPS;

Deve possuir mecanismo de busca por comandos no gerenciamento via console SSH, facilitando a localização de comandos;

Não deve possuir restrições quanto ao número de máquinas ou usuários protegidos;

Deve aplicar novas regras de segurança sem provocar indisponibilidade do serviço ou perda de conexões ativas que não sejam as conexões atingidas pelas regras alteradas;

Deve implementar os protocolos IPV4 e IPV6;

Deve suportar “statefull inspection” de tráfego IPV4 e IPV6;

Deve suportar a utilização simultânea de políticas de segurança em IPV4 e IPV6;

Deve possuir MIB SNMP contemplando, no mínimo, indicadores de estado do hardware (consumo de CPU, temperatura, utilização de memória) e de desempenho do equipamento;

Deve implementar “policy based routing”, ou “police based forwarding”, em IPV4 e IPV6, possibilitando implementação de políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;

Deve suportar, simultaneamente no mesmo appliance, o funcionamento nos modos “sniffer” (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3 e suas combinações;

Deve possuir funcionalidade de backup/restore de sua configuração e das regras de segurança;

Deve ter suporte a sFlow ou NetFlow;

Deve permitir o agendamento automático dos backups;

Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para outros servidores externos por meio dos protocolos FTP e SCP;

Deve implementar regras de acesso por endereço IP de origem e de destino, bem como por agrupamentos de IPs de origem e de destino;

Deve implementar regras de acesso por sub-rede IP, tanto de origem como de destino;

Deve implementar regras de acesso por usuário e por grupos de usuários existentes no LDAP/Active Directory;

Deve implementar regras de acesso para máquinas do domínio;

Deve implementar mecanismo de captura de pacotes;

Deve ter suporte a aplicações de voz como as baseadas em protocolos H.323 e SIP;

Deve implementar alta disponibilidade, podendo operar tanto no modo "Ativo/Passivo" como no modo "Ativo/Ativo", com todas as licenças de software habilitadas para tal e sem perda de conexões;

Ao operar no modo de alta disponibilidade deverá sincronizar entre os membros do cluster: sessões, configurações (incluindo, mas não se limitando a regras de firewall, NAT, QoS e objetos de rede), certificados descriptografados, associações de segurança das VPNs, tabelas FIB;

Ao operar no modo de alta disponibilidade deve possibilitar monitoramento de falha de link;

Deve permitir o funcionamento em modo transparente do tipo "bridge";

Deve possibilitar o sincronismo de configurações entre os equipamentos do cluster de forma automática ou através de console de gerência;

Deve possuir mecanismo de "anti-spoofing";

Deve implementar os seguintes tipos de tradução de endereços (NAT): um-para- um, N-para-um, um-para-N, N-para-N;

Deve implementar tradução de portas (PAT);

Deve implementar NAT que possibilite que um endereço tenha mais de um NAT associado, dependendo da origem, destino ou porta;

Deve implementar NAT de origem e NAT de destino simultaneamente na mesma política;

Deve permitir o registro de eventos de NAT no LOG, com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

Deve possibilitar o registro em LOG de informações de cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos, IPs de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado);

Deve implementar o protocolo ECMP;

Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

Deve suportar o balanceamento de, no mínimo, 2 (dois) links distintos;

Deve implementar o protocolo Link Layer Dicovery (LLDP);

Deve possibilitar a configuração e o envio simultâneo de LOGs para mais de um servidor de LOG;

Deve permitir bloquear sessoes TCP que usarem variações do 3-way hand- shake, conhecido também como "TCP Split-Handshake Attack", prevenindo desta forma possíveis tráfegos maliciosos;

Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver descriptografia de SSL;

Deve ser capaz de descriptografar, inspecionar e criptografar novamente o tráfego criptografado SSL, "inbound" e "outbound";

Deve permitir a criação de políticas de inspeção de tráfego para bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

Deve suportar objetos IPV6 e permitir a criação de regras com esses objetos;

Deve suportar agendamento de ativação de políticas, permitindo habilitar e desabilitar, automaticamente, políticas em horários pré-definidos;

9. FUNCIONALIDADES DE INSPEÇÃO DE TRÁFEGO CRIPTOGRAFADO (DESCRIPTOGRAFIA SSL) REQUERIDA DO EQUIPAMENTO (APPLIANCE) DA SOLUÇÃO

Deve ser capaz de inspecionar tráfego criptografado SSL, "inbound" e "outbound";

Deve permitir a configuração de regras para inspeção SSL, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

Deve permitir a configuração de regras de exceção para que o tráfego SSL não seja inspecionado, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

Deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e conexões não pessoais por meio de classificação automática.

10. FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES DO EQUIPAMENTO (APPLIANCE) DA SOLUÇÃO

Os equipamentos que compõem a solução devem suportar e implementar políticas e regras segurança baseadas no reconhecimento de aplicações, permitindo o bloqueio ou liberação do tráfego de aplicações (e grupos de aplicações) independentemente de porta e protocolo que utilizem;

Devem implementar o controle de aplicações para grupos estáticos de aplicações, para grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e para categorias de aplicações pré-existentes na ferramenta;

Devem reconhecer pelo menos 2.000 (duas mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a "peer-to-peer", redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, "proxy", mensageiros instantâneos, compartilhamento de arquivos, e-mail;

Devem reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp,4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote e google-docs;

Deve reconhecer pelo menos os seguintes protocolos industriais, identificando requisições de escrita e de leitura: DNP3 e ICCP; permitindo aplicar filtros granulares como por ex.: somente permitir comandos de leitura;

Deve reconhecer o protocolo Routed-GOOSE sobre UDP utilizado para transferência de estados e dados entre unidades de medição;

Devem inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a sua porta padrão ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

Devem identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

Devem descriptografar os pacotes do tráfego SSL para possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

Devem permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

Devem identificar o uso de táticas evasivas via comunicações criptografadas;

A solução deve atualizar a sua base de assinaturas de aplicações automaticamente, registrando em LOG as alterações efetuadas;

Devem reconhecer aplicações em IPV6;

Devem limitar a banda (download/upload) usada por aplicações (traffic shaping), com base no IP de origem, usuários e grupos de usuários do LDAP/Active Directory;

A solução deve possibilitar ativar o controle de aplicações em todas as regras de segurança do dispositivo e não somente em algumas regras;

Devem suportar múltiplos métodos de identificação e classificação das aplicações, incluindo ao menos: checagem de assinaturas, decodificação de protocolos e análise heurística;

Devem suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

Devem permitir a criação de assinaturas personalizadas, sem a necessidade de ação do fabricante;

O fabricante da solução deve permitir a solicitação de inclusão de aplicações na base de assinaturas global;

Devem alertar o usuário quando uma aplicação for bloqueada;

Devem possibilitar que o controle de portas seja aplicado para todas as aplicações;

Devem possibilitar a identificação e controle de tráfego de forma granular para os seguintes tipos de aplicações: peer-to-peer (exemplo: bittorrent, emule, etc.), instant messaging (exemplos: Facebook Chat, Whatsapp, etc.), aplicações proxies (exemplo: ghostsurf, freegate, etc.), streaming de áudio e vídeo, update de software, redes sociais, anonymizers, acesso e controle remoto, VoIP e e- mail;

A solução deve permitir que os administradores criem grupos de aplicações personalizados a partir da base de aplicações existentes na ferramenta;

A solução deverá permitir o bloqueio de aplicações e sites de forma granular e informar ao usuário através da exibição de uma página de bloqueio customizada;

A solução deve possibilitar o controle de banda (traffic shaping) para aplicações e categorias de aplicações;

A solução deve ser capaz de realizar o bloqueio e a liberação de aplicativos, sites e categorias durante um determinado período de tempo;

A solução deve permitir a criação de regras para o controle de uso de aplicações baseadas em endereços de rede, zonas de segurança, domínios e baseadas na identidade de usuários/grupos de usuário e máquinas do LDAP/Active Directory;

A solução deve permitir a criação de usuários administrativos específicos para as funcionalidades de controle de acesso a aplicações;

Para cada regra de controle de acesso às aplicações, a solução deve ser capaz de desabilitar o registro de log, habilitar o registro de log e registrar a quantidade de trafego enviado, recebido e o tempo de navegação.

11. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS/CONTEÚDO MALICIOSO DA SOLUÇÃO (IPS, ANTIVÍRUS, MALWARES, SPYWARES, BOTNETS)

Os equipamentos (appliances) que compõem a solução devem possuir funcionalidades de IPS (Intrusion Prevention System), Antivírus e Anti-Malware (adware, spyware, hijackers, keyloggers, etc.) integrados nos próprio appliance;

Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e AntiSpyware);

Deve armazenar as bases de assinaturas no próprio equipamento;

As funcionalidades de IPS, Antivírus e Antispyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que o CECS não renove os termos de garantia e não tenha mais direito de receber atualizações das bases de assinaturas das funcionalidades. Desta forma as funcionalidades passariam a operar com a última atualização antes do encerramento dos serviços de garantia;

A solução deve sincronizar entre os equipamentos do cluster as assinaturas de IPS, Antivírus, Antispyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

A solução deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos;

A solução deve ser capaz de identificar e bloquear ataques de Brute Force;

Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar “tcp-reset”;

Deve permitir que as assinaturas sejam ativadas ou desativadas, ou ainda habilitadas apenas em modo de “monitoração”;

Deve possuir base de assinaturas de IPS com, no mínimo, 5.000 (cinco mil) ataques conhecidos;

Deve permitir criar exceções nas regras por IP de origem ou de destino para todas as assinaturas, e para cada assinatura de forma individual;

Deve suportar granularidade nas regras de IPS, Antivírus e Antispyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e

a combinação de todos esses itens;

Deve permitir a criação de políticas para bloqueio de vulnerabilidades conhecidas;

Deve permitir a criação de políticas para bloqueio de exploits conhecidos;

Deve fornecer proteção contra ataques de negação de serviços;

Deve permitir a criação de regras de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque, com origem/destino em determinado endereço IP/rede;

Deve implementar inspeção/proteção de IPS pelo mecanismo de análise de padrões de estado de conexões;

Deve implementar inspeção/proteção de IPS pelo mecanismo de análise de decodificação de protocolo;

Deve implementar inspeção/proteção de IPS pelo mecanismo de análise e detecção de anomalias de protocolo;

Deve implementar inspeção/proteção de IPS pelo mecanismo de análise heurística;

Deve implementar inspeção/proteção de IPS pelo mecanismo de “IP fragmentation”;

Deve implementar inspeção/proteção de IPS pelos mecanismos de Remontagem de pacotes de TCP;

Deve implementar inspeção/proteção de IPS pelos mecanismos de bloqueio de pacotes malformados;

Deve prover proteção contra ataques conhecidos como: “Synflood”, “ICMPflood”, “UDPfloof”, etc;

Deve prover proteção contra ataques de RPC (Remote procedure call);

Deve prover proteção contra ataques de Windows ou NetBios;

Deve prover proteção contra ataques DNS (Domain Name System);

Deve prover proteção contra ataques a FTP, SSH , Telnet ou rlogin;

Deve prover proteção contra ataques de ICMP (Internet Control Message Protocol);

Deve ser capaz de, quando configurada para isso, registrar em LOG todas as sessões e ameaças detectadas/monitoradas/bloqueadas, com informações básicas do tipo: nome/categoria da ameaça, IP de origem da ameaça, IP de destino, máquina do domínio, identificação do usuário, entre outros;

Deve prover proteção contra “portscans”, permitindo criar exceções para endereços IPs conhecidos ou de ferramentas de monitoramento da organização;

Deve possibilitar a criação de assinaturas customizadas pelos administradores;

Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

Deve possuir assinaturas para bloqueio de ataques de buffer overflow;

Deve prover proteção contra vírus e spywares em, pelo menos, os seguintes protocolos: HTTP/HTTPS, FTP, SMB, SMTP e POP3;

Deve prover proteção contra malware (vírus, spyware, worms) em conteúdo HTML e javascript;

Deve prover proteção contra malware (vírus, spyware, worms) embutidos em arquivos do tipo “PDF”;

Deve prover proteção contra malware (vírus, spyware, worms) embutidos em arquivos comprimidos (exemplo: zip, gzip, etc.);

A solução deve prover proteção contra malware (vírus, spyware, worms) e/ou códigos maliciosos para outros tipos de arquivos além de arquivos do tipo PDF, javascript, HTML e arquivos comprimidos;

Deve prover proteção contra tráfego de “botnets” (identificar e bloquear comunicação com redes “botnet”);

Deve registrar no LOG para visualização via gerência de pelo menos as seguintes informações sobre as ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, IP de origem e de destino da comunicação, além da ação tomada pelo dispositivo (bloqueio, liberação, monitoramento, etc.);

Deve prover proteção contra downloads automáticos de arquivos executáveis maliciosos através do protocolo HTTP;

Deve possibilitar a criação de políticas para bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;

Deve possibilitar a criação de políticas para bloqueio de download ou upload de arquivos;

A solução deve possuir na própria interface de gerência centralizada, representações gráficas com informações em tempo real sobre as atividades recentes de malware (vírus, spyware, worms) detectados, permitindo visualização por país de origem, através de IP ou URL;

A solução deve permitir a criação (e utilização nas regras de segurança) de perfis diferenciados de proteção, possibilitando seu uso em regras por usuário/grupo de usuários do LDAP/ActiveDirectory ou rede, sendo possível escolher um perfil diferente para cada regra;

A solução deve prover proteção contra conexões do tipo “callback”, com mecanismo de detecção e alerta onde seja possível configurar bloqueio/desbloqueio da conexão;

A solução deve possibilitar a geração de relatórios através da interface gráfica onde contenha no mínimo as seguintes informações: tipo de malware, identificador de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, IP de origem, IP de destino e nome do usuário infectado de acordo a base do LDAP/Active Directory;

Deve possibilitar a pesquisa aos eventos já reconhecidos e por diferentes intervalos de tempo;

A solução deve possibilitar a visualização e a geração de relatório de hosts infectados, do tipo “sumário executivo”, com possibilidade de customização para apresentação corporativa/gerencial;

A solução de antimalware e antivírus deve possuir recurso onde o administrador consiga criar as regras de segurança de forma granular e aplicá-las em modo “detecção/monitoramento” ou no modo de “inspeção/bloqueio”;

A solução de antibot deve possuir mecanismos de detecção variados e que incluam pelo menos: verificação de endereço IP e descrição da comunicação;

A solução deve implementar atualização da base de dados/assinaturas de forma automática, recebendo as atualizações a qualquer momento, mas permitindo também o agendamento diário e o período e/ou horário de cada atualização. Essas atividades devem ser registradas em LOG;

A solução deve receber e implantar as atualizações de assinaturas de segurança sem a necessidade de reiniciar os equipamentos que compõem a solução de alta disponibilidade;

A solução deve ser capaz de inspecionar tráfego criptografado HTTPS (inbound/Outbound) e também criar regras com exceções à esse tipo de inspeção baseadas em IP de origem, IP de destino, usuário/grupo de usuários do LDAP/Active Directory, máquina do domínio;

A solução deve possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de troubleshooting e/ou análise forense.

12. FUNCIONALIDADES DE QOS (“QUALITY OF SERVICE”) DO EQUIPAMENTO (APPLIANCE) DA SOLUÇÃO

A solução deve prover funcionalidades para controle e gerenciamento do tráfego (“Traffic Shaping”/ QoS – “Quality of Service”) de entrada e saída (tráfego inbound e outbound) da rede ou zona de segurança;

Deve possibilitar a configuração de políticas de traffic shaping por regra de segurança, por IP de origem do tráfego, por IP de destino do tráfego, por usuário/grupo de usuário do LDAP/Active Directory;

Deve possibilitar a configuração de políticas de traffic shaping por tipo de aplicação, incluindo, mas não se limitando, aplicações de áudio/vídeo (exemplo: Skype, Youtube), aplicações de

compartilhamento de arquivos do tipo peer-to- peer (exemplo: Bittorrent), aplicações de redes sociais (Facebook, Instagram), aplicações de comunicação (exemplo: Whatsapp), aplicações de armazenamento em nuvem (exemplo: Dropbox, OneDrive, Google Drive);

Deve possibilitar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP e aplicações como Skype, por usuário/grupo de usuários do LDAP/Active Directory;

Deve suportar a marcação de pacotes DiffServ.

13. FUNCIONALIDADES DE IDENTIFICAÇÃO DE USUÁRIOS DA SOLUÇÃO

A solução deve possibilitar a criação de políticas de segurança baseadas na visibilidade e controle dos usuários que utilizam/acessam as aplicações e serviços Web. Essa funcionalidade deve ser implementada através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Radius e base de dados local (usuários criados na própria ferramenta);

Deve possuir integração com Microsoft Active Directory com múltiplos controladores de domínio, para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados nas regras de segurança, possibilitando à solução: identificar, autenticar, autorizar e registrar os eventos de acessos ou ameaças detectadas;

Deve registrar a identificação do usuário em todos os LOGs de eventos de acesso ou de ameaças gerados pela solução;

Deve registrar os eventos dos usuários em “tempo real”, sem a utilização de processos em lote (batches) ou processos de correlação executados após a ocorrência do evento, possibilitando de forma ágil a análise das informações;

A solução deve ter capacidade e estar licenciada para a identificação e autenticação de pelo menos 30 (trinta) usuários diferentes, não simultaneamente;

Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados nas regras de segurança;

A identificação dos usuários por meio de integração com o Microsoft Active Directory, RADIUS e proxies internos, deverá ocorrer sem qualquer tipo de agente/software/cliente de software instalado nos controladores de domínio da rede/zona de segurança e estações dos usuários;

A funcionalidade de identificação de usuário/grupos de usuários deverá se integrar com outras funcionalidades da solução, para que regras de segurança possam ser criadas com base em usuários/grupos de usuários (firewall, IPS, controle de aplicação, inspeção de tráfego criptografado, etc.);

Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (“Captive Portal”– Interface onde o usuário pode informar suas credenciais), sem a necessidade de instalação de cliente de software;

A funcionalidade de “Captive Portal” deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory;

Deve suportar o recebimento de eventos de autenticação de controladores wireless, dispositivos 802.1x e soluções NAC (Network Access Control), para a identificação de endereços IP e usuários;

Deve suportar a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes virtuais Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular;

Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo “x-forwarded-for” do protocolo HTTP.

14. FUNCIONALIDADES DE VPN (VIRTUAL PRIVATE NETWORK) DOS EQUIPAMENTOS (APPLIANCE) DA SOLUÇÃO

Os equipamentos que compõem a solução devem possuir funcionalidade de um concentrador VPN conforme listadas abaixo;

Deve implementar IPSEC VPN;

Deve implementar VPN IPSEC “site-to-site” e “client-to-site”;

Deve implementar SSL VPN;

Deve implementar SSL VPNs utilizando certificados digitais;

A solução deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de VPN SSL;

Deve implementar VPN IPSEC com suporte aos algoritmos de criptografia DES e 3DES;

Deve implementar VPN IPSEC com suporte ao algoritmo de criptografia AES 128, 192 e 256;

Deve implementar VPN IPSEC com suporte à autenticação MD5 e SHA-1;

Deve implementar VPN IPSEC com suporte a “Diffie-Hellman” Group 1 , Group 2, Group 5 e Group 14;

Deve implementar VPN IPSEC com suporte ao algoritmo “Internet Key Exchange” – IKE v1 e v2;

Deve implementar VPN IPSEC com suporte a autenticação via certificado IKE PKI;

Deve possuir interoperabilidade de VPN site-to-site com, no mínimo, os seguintes fabricantes: Cisco, Checkpoint, Fortinet, Palo Alto, Juniper, Sonic Wall;

Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução;

Deve suportar e estar licenciado para, no mínimo, 30 (trinta) clientes de VPN SSL simultâneos;

Deve suportar e estar licenciado para, no mínimo, 30 (trinta) túneis de VPN IPSEC simultâneos;

Deve implementar SSL VPN por meio de conexão via interface Web;

Deve implementar SSL VPN por meio de conexão via cliente VPN instalado no computador do usuário;

A VPN SSL deve possibilitar o acesso à rede interna e/ou zona de segurança do CECS, de acordo com a política de segurança para esta finalidade;

A VPN SSL deve suportar autenticação via LDAP/Active Directory, certificado digital e também na base de usuários local;

A VPN SSL deve fornecer uma solução de autenticação única (single-sign-on) aos usuários remotos, integrando-se com as ferramentas de login do Windows;

A VPN SSL deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário/grupo de usuários do LDAP/Active Directory;

A VPN SSL deve permitir a atribuição de endereço IP dinâmico aos usuários remotos, permitindo a configuração e utilização de faixa de endereços IP específica ou range de IPs específicos para clientes VPN;

A VPN SSL deve permitir a atribuição de endereço IP fixos aos clientes remotos;

A VPN SSL deve possibilitar configuração que direcione todo o tráfego dos usuários remotos de VPN para dentro do túnel de VPN, ou apenas o tráfego referente às rotas que o cliente recebe ao estabelecer a conexão VPN;

A VPN SSL deve possibilitar atribuição de DNS aos usuários remotos de VPN;

A solução de VPN SSL deve permitir a criação de políticas de segurança para o tráfego dos usuários remotos da VPN: inspeção de tráfego SSL, controle de aplicações, IPS, antivírus, antispyware e filtro Web;

A VPN SSL deve permitir que sejam definidos métodos de autenticação distintos por sistema operacional do usuário remoto de VPN (Mac, Windows e Chrome OS);

A solução de VPN SSL deve possuir cliente VPN para os seguintes sistemas operacionais:

MS-Windows 7;
MS-Windows 8;
MS-Windows 10;

Mac OS X;

A solução de VPN SSL deve suportar IPV4 e possuir cliente próprio para instalação em desktops (sistemas operacionais Windows e MAC OS X), suportar e estar licenciada para, no mínimo, 30 (trinta) usuários simultâneos;

Deve implementar NAT-T (NAT Transversal);

A solução deve permitir a arquitetura de VPN HUB e SPOKE.

15. GARANTIA E SUPORTE TÉCNICO CONDIÇÕES GERAIS

Todo o equipamento e softwares entregues deverão possuir garantia:
Ponto em Curitiba 60 (sessenta) meses;
Ponto em Londrina 36 (trinta e seis) meses;
Contados a partir da emissão do termo de aceitação;

A Contratada garantirá o perfeito funcionamento do sistema e seus componentes, durante o prazo de garantia;

Todos os custos relativos a correções de software, substituição de peças ou equipamentos defeituosos, serão de responsabilidade da Contratada;

Durante o período de garantia, a Contratada deve atender à solicitação do CECS, de identificação de mau funcionamento e, se necessário, o envio de pessoal qualificado para sanar o problema;

A Contratada deve dispor de um centro de suporte técnico no Brasil disponível para consultas, suporte e abertura de chamados para correção de falhas através de telefone, e/ou e-mail em regime 8x5 (horário comercial semanal), que deverá ser único para todos os componentes da solução;

Todo o atendimento de falhas será realizado na sede do CECS, sendo os custos relativos à mão-de-obra, deslocamento, hospedagem, alimentação e outros, de responsabilidade da Contratada;

Será permitido o acesso remoto via Internet para o atendimento de falhas.

A Contratada deverá possuir técnicos especializados e certificados pelo fabricante da solução para manutenção da solução ofertada;

A Contratada deverá garantir o fornecimento de peças sobressalentes e mão-de- obra para manutenção, por um período mínimo de 6 (seis) anos;

A Contratada será responsável pelo envio, conserto e devolução do equipamento defeituoso, a partir da Sede do CECS em Curitiba;

A Contratada deverá fornecer um equipamento igual ou superior para substituição do equipamento defeituoso enquanto este estiver fora para conserto;

Estão cobertos pelo atendimento de garantia todo o equipamento (e suas partes) e softwares oferecidos na solução;

O escopo do suporte técnico será, de pelo menos, não se limitando a:

Executar procedimentos, resolver problemas e esclarecer dúvidas;

Configurar, atualizar, customizar em nível de configuração e codificação;

Resolver situações de baixo desempenho da solução;

Elaborar estudos e diagnósticos em relação ao ambiente, à customização, funcionamento e uso dos softwares;

Instalar patches de correção nos softwares integrantes das soluções;

Transferir o conhecimento referente aos problemas vivenciados e às soluções aplicadas aos técnicos do CECS, na forma a ser determinada pelas partes;

Realizar a instalação e a configuração de novas versões do produto, incluindo migração de customizações de uma versão para outra, bem como dos dados referentes ao banco de dados da solução, quando aplicável, após a disponibilização das atualizações tecnológicas pelo fabricante;

Emitir relatórios após cada chamado contendo descrição do problema e a solução adotada;

Acionamento de garantia de hardware e software;

Resolução de problemas no ambiente que limitem ou impeçam o bom e correto funcionamento da solução;

Recomendações de melhores práticas;

Análise do ambiente para avaliação de configurações.

O atendimento deverá ser prestado em idioma português do Brasil;

O CECS poderá efetuar um número ilimitado de chamados durante a vigência do serviço para suprir suas necessidades de utilização da solução;

No ato de abertura/conclusão de cada atendimento, a Contratada deverá remeter ao CECS um registro do chamado contendo no mínimo:

Número do chamado;

Data e hora da abertura/conclusão chamado;

Descrição do problema e/ou consulta;

Previsão de atendimento/Descrição da solução efetuada.

O serviço de manutenção deve incluir todas as configurações que se fizerem necessárias no sistema operacional, decorrentes de substituição ou reinstalação de componentes de hardware, para garantir seu pleno funcionamento;

Quaisquer alegações por parte da empresa Contratada contra as instalações (ambiente inadequado, rede elétrica, rede lógica) ou usuários (mau uso, etc.) do CECS, devem ser comprovadas tecnicamente através de laudos detalhados e conclusivos, emitidos pelo fabricante do equipamento. Não serão admitidas omissões baseadas em suposições técnicas sem fundamentação, "experiência" dos técnicos ou alegações baseadas em exemplos de terceiros. Enquanto não for efetuado o laudo, e esse não demonstrar claramente os problemas alegados, a empresa Contratada deve prosseguir com o atendimento dos chamados, respeitando os tempos de atendimento e resolução contratados;

O serviço de suporte técnico abrange a manutenção preventiva, manutenção corretiva e reparação da solução;

O prazo para solução (ou substituição) de um equipamento (ou de suas partes), depois de detectada a necessidade, será de 5 (cinco) dias úteis após a formalização da necessidade de substituição. Neste prazo a solução (ou substituição) deverá ser concluída e o equipamento deverá estar funcionando em sua plena capacidade e funções previamente atribuídas.

16. GARANTIA DE HARDWARE

Entende-se por garantia do hardware a cobertura sobre todo o appliance e demais equipamento fornecido (ou de suas partes, bem como cabos, acessórios, etc.) com relação a defeito, perda de funcionalidade, mau funcionamento, erro de projeto ou quaisquer outros casos semelhantes em que venha a ser constatada a necessidade de substituição física do mesmo para resolver o problema;

Garantia total por todo o período de garantia, incluindo todos os custos de suporte, instalação, reinstalação, reparação e substituição do que se fizer necessário para o perfeito funcionamento da solução proposta;

Em caso de impossibilidade de reparo de um módulo de hardware, a Contratada deverá providenciar a substituição por outro módulo novo;

A garantia deverá abranger todo e qualquer defeito de projeto, fabricação, transporte, instalação, montagem, desempenho do equipamento, softwares e acessórios envolvidos na implementação da solução ofertada, garantia de 60 (sessenta) meses em Curitiba e 36 (trinta e seis) meses em Londrina;

A atuação da equipe técnica do CECS, seguindo os procedimentos estabelecidos pelo fabricante, na operacionalização do equipamento não modificará o cumprimento integral dos Termos de Garantia;

Em caso de impossibilidade de reparo de um módulo de hardware, a Contratada deverá providenciar a substituição por outro módulo novo que deve possuir, no mínimo, o mesmo desempenho e características e deverá herdar as mesmas garantias daqueles originalmente fornecidos, sem ônus para o CECS;

O prazo para solução (ou substituição) de um equipamento (ou de suas partes), depois de detectada a necessidade, será de 5 (cinco) dias úteis após a formalização da necessidade de substituição.

Caso seja necessária a substituição do equipamento ou de algum de seus componentes, esta deverá ser realizada por outro de características iguais ou superiores;

A Contratada deverá fornecer lista de todos os dados necessários para abertura de chamados técnicos (por exemplo: códigos de identificação do equipamento, descrição, versão de firmware, versão de software, etc.);

17. GARANTIA DE SOFTWARE

Entende-se por garantia de software a cobertura sobre todos os softwares fornecidos com relação a: defeito (bug), perda de funcionalidade, mau funcionamento, erro de projeto, ou quaisquer outros casos semelhantes em que venha a ser constatada a necessidade de substituição ou atualização do mesmo para resolver o problema (seja a instalação de uma correção, a adição de nova funcionalidade, a instalação de uma versão anterior ou superior, etc.), incluindo todos os custos de suporte, instalação, atualização, reparação e substituição do que se fizer necessário para o perfeito funcionamento da solução proposta;

Deverão ser fornecidas correções, patches e novas versões tão logo estas se tornem disponíveis, após aprovação por parte do CECS.

Caberá ao CECS a decisão por migrar ou permanecer em determinada versão de software, bem como aplicar ou não as atualizações de software, no caso em que estas novas versões/atualizações não forem obrigatórias e/ou críticas para seu ambiente de operação;

18. CONDIÇÕES GERAIS HOMOLOGAÇÃO DA SOLUÇÃO DE SEGURANÇA REALIZADOS DURANTE A LICITAÇÃO

Os testes descritos abaixo visam verificar se a solução ofertada atende às especificações descritas neste termo num ambiente de produção próximo do real (a infraestrutura de rede da contratada) ou que simule ao menos partes desse ambiente (via espelhamento de portas e direcionamento tráfego, por exemplo);

Todas as atividades aqui descritas serão acompanhadas pela equipe técnica do CECS, além de equipe técnica da empresa proponente;

A empresa proponente classificada em primeiro lugar no processo licitatório será convocada a instalar, dentro de 30 (trinta) dias, 1 (um) appliance na dependência do CECS, no seguinte endereço: Rua Comendador Araújo 143, no 19 andar Centro Curitiba PR, Outro equipamento no Escritório do CECS em Londrina no endereço Rua Milão, n° 204 – Jardim Piza, – Londrina/PR CEP: 86.041-180 ;

Caso os testes identifiquem que a solução não atende às especificações, a oferta da empresa proponente não será aceita e a mesma será desclassificada. Neste caso o processo de aquisição terá

prosseguimento com a convocação da próxima empresa obedecendo à ordem de classificação do certame;

A instalação e configuração dos appliance e de sua ferramenta de gerenciamento deverá ser feita pela equipe técnica empresa proponente, sempre acompanhada e supervisionada pela equipe técnica do CECS;

Para qualquer dúvida que surja durante os testes de homologação deverão ser utilizadas as especificações contidas no edital e/ou na especificação técnica associado para dirimi-la;

A empresa proponente deverá enviar antecipadamente à equipe técnica do CECS documentações, descritivos técnicos ("datasheets"), folders, páginas da Web, ou outros recursos do fabricante que descrevam as capacidades, funcionalidades, tecnologias e arquiteturas de operação da solução ofertada. Deverá enviar também material ou página da Web que comprove que os componentes da solução não estão em modo "End of Life" (fabricante parou de fabricar), "End of Support" (fabricante parou de oferecer suporte) ou "End of Sale" (fabricante anunciou o fim das vendas) na data da proposta;

Os testes serão efetuados de maneira que não haja prejuízo à operação da rede atual do CECS, em horário comercial (08:00 – 12:00h e 13:00 – 18:00h) em dias de semana (segunda à sexta-feira) e terão até 5 (cinco) dias úteis para sua conclusão;

Os testes poderão incluir qualquer item das especificações contidas na especificação técnica e envolverão, no mínimo, os seguintes itens:

Criação de usuários administradores;

Registro e visualização de atividades de administradores no LOG da solução;

Configuração de modo "sniffer" para inspeção de tráfego espelhado da rede do CECS (o espelhamento de portas será de responsabilidade da equipe técnica do CECS) e layer-3 simultaneamente;

Criação de regras de segurança de firewall baseadas em porta/protocolo, IPs de origem e destino, sub-redes, usuários/grupos de usuários do LDAP/Active Directory;

Criação de regras de segurança contra ameaças avançadas baseadas em IPs de origem e destino, sub-redes, usuários/grupos de usuários do LDAP/Active Directory;

Visualização da identificação de usuários no LOG/monitoramento via gerência;

Criação de regras de segurança do controle de aplicações baseadas em tipos de aplicações, IPs de origem e destino, sub-redes, usuários/grupos de usuários do LDAP/Active Directory;

Visualização de informações gráficas e LOGs na gerência de todas as regras de segurança criadas;

Criação de VLANs e "DMZs" e testes de inspeção de tráfego dessas interfaces;

Testes das funcionalidades de VPN: configuração de pelo menos 2 (dois) perfis de VPN diferentes (com políticas de segurança diferentes), instalação de clientes VPN em pelo menos dois computadores com sistema operacional Windows;

Estabelecimento de túnel VPN “site-to-site” com pelo menos um parceiro;