MINISTÉRIO PÚBLICO DA UNIÃO

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS

ESPECIFICAÇÃO TÉCNICA E QUANTIDADES

ANEXO I – ESPECIFICAÇÃO TÉCNICA

(Contratação de serviço de gerenciamento de segurança de perímetro)

1. SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO

1. HARDWARE

1.1.1. Os equipamentos devem ser do tipo Appliance, ou seja, hardware e software integrados. Não serão aceitas soluções compostas por hardwares genéricos;

1.1.2. A solução será implementada em modo cluster de alta disponibilidade com uso de 2 equipamentos e capaz de suportar um throughput de 2 Gbps, com todas as funcionalidades habilitadas;

1.1.2.1. Para a funcionalidade de sistema de e-mail poderá ser fornecida outra solução em modo cluster de alta disponibilidade, com uso de 2 equipamentos físicos ou virtuais, desde que possua total integração entre as plataformas.

1.1.2.2. Na hipótese de o cluster de e-mail ser físico, cada equipamento deve possuir no máximo 2U.

1.1.3. A solução deve ser do tipo Bundle (Hardware/Software) obrigatoriamente do mesmo fabricante, com capacidade suficiente para atender os requisitos exigidos.

1.1.4. A solução deverá ser composta por sistema operacional proprietário, desenvolvido para ser seguro e robusto e otimizado para as suas funcionalidades;

1.1.5. Todos os equipamentos, produtos, peças ou softwares necessários à para a implementação da solução não deverão constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por contratos de suporte a atualização de versão do fabricante. Os produtos utilizados devem possuir licenciamento, suporte e garantia do fabricante por todo o período contratual;

1.1.6. Não há necessidade de utilização de equipamentos de primeiro uso desde que atendidos os requisitos do item anterior.

1.1.7. Serão permitidas soluções virtuais ou em nuvem do próprio fabricante para gerência da solução, guarda de logs e emissão de relatórios, desde que, no caso de soluções virtuais, haja suporte e compatibilidade com ambiente de virtualização VMware ESXi 7.0.3.

1.1.7.1. Caso a solução virtual não seja oficialmente suportada pela virtualização VMware ESXi 7.0.3, mas seja permitida a instalação neste ambiente, a responsabilidade de manter a funcionalidade da solução é da CONTRATADA.

1.1.7.2. Caso haja problemas relacionados a incompatibilidade com o sistema de virtualização, a CONTRATADA deverá prover servidor próprio, licenças, cabos e demais acessórios necessários para seu pleno funcionamento;

1.1.8. A CONTRATANTE poderá fornecer no máximo os seguintes recursos de virtualização para provisionar as máquinas virtuais necessárias para solução:

1.1.8.1. 12 processadores virtuais;

1.1.8.2. 48 GB de memória RAM;

1.1.8.3. 6 TB de armazenamento.

1.1.9. Os equipamentos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação;

1.1.10. Possuir no máximo 2RU (Rack Units);

1.1.11. Possuir no mínimo:

1.1.11.1. 8 interfaces, incluindo a de gerência e sincronismo, compatíveis com cabeamento de rede UTP com conector RJ-45 no padrão 100/1000Base-T Gigabit Ethernet;

1.1.11.2. 4 interfaces, compatíveis com cabeamento SFP+ 10 GbE.

1.1.12. Possuir fonte de alimentação redundante e hot swap interna;

1.1.13. Implementar a configuração de cluster de alta disponibilidade (cluster H.A.) Ativo/Passivo e permitir extensão de licença do equipamento para suportar o modo Ativo/Ativo.

1.1.14. O cluster H.A. deve sincronizar:

1.1.14.1. Todas as sessões TCP;

1.1.14.2. Todas as Associações de Segurança das VPNs;

1.1.14.3. Todas as assinaturas de Antivírus, Antispyware e Aplicações;

1.1.14.4. Todas as configurações;

1.1.14.5. Todas as configurações necessárias para que não haja perda de funcionalidade em caso de falha;

1.1.15. Todos os LOGs devem ser disponibilizados de modo a permitir acesso aos logs independente de qual unidade do cluster que estiver ativo.

1.1.16. Permitir a monitoração de falha de conexão entre os dispositivos do cluster com possibilidade de gerar alertas via SNMP e e-mail;

1.1.17. Implementar compatibilidade com sistemas de monitoramento como Nagios e Cacti via SNMP v2;

1.1.18. A solução deve possuir minimamente as seguintes especificações técnicas:

1.1.18.1. Throughput de Firewall de pelo menos 37 Gbps;

1.1.18.2. Throughput de IPS de pelo menos 13 Gbps;

1.1.18.3. Admitir 160.000 novas conexões por segundo;

1.1.18.4. Tratar 4.000.000 de sessões simultâneas;

1.1.18.5. Caso haja mais de um valor apresentado no datasheet para os itens acima, será considerado o de maior valor.

1.2. SOFTWARE

1.2.1. Os equipamentos da solução devem ser otimizados para análise de conteúdo de aplicações em camada 7 do modelo OSI;

1.2.2. O equipamento deve possuir certificação da ICSA Labs na modalidade "ICSA Labs Certified Firewall Product" ou Common Criteria EAL4+.

1.2.3. O fabricante do equipamento deve ser membro do programa "Microsoft Active Protections Program" (MAPP). Membros do MAPP recebem acesso antecipado a informações de vulnerabilidades para que estas sejam corrigidas de modo rápido reduzindo a exposição do cliente a ameaças.

1.2.4. Implementar transmissão de logs em rede IP por meio do padrão syslog.

1.2.5. Implementar funcionamento em TapMode (Via porta espelhada, Tap ou SPAN port).

1.2.6. Implementar tecnologia de filtragem de pacotes baseada em estados (stateful inspection);

1.2.7. Implementar tecnologia de filtragem capaz de atuar em múltiplas camadas (stateful multilayer inspection),

1.2.8. Capacidade de atuar como um proxy, de modo a inspecionar conteúdo do tráfego de aplicações e filtrar URLs acessadas.

1.2.9. Registrar os fluxos de dados relativos a cada sessão iniciada, informar para cada uma destas:

1.2.9.1. Protocolo;

1.2.9.2. Aplicação;

1.2.9.3. Endereços de origem e destino dos pacotes;

1.2.9.4. Portas TCP e UDP de origem e destino;

1.2.9.5. Quantidade de pacotes trafegados;

1.2.9.6. Quantidade de dados trafegado.

1.2.10. Implementar toda a pilha de protocolos do modelo TCP/IP, com as seguintes funcionalidades:

1.2.10.1. IPv4 e IPv6;

1.2.10.2. Roteamento estático e dinâmico de tráfego;

1.2.10.3. RIP v2;

1.2.10.4. OSPF;

1.2.10.5. BGP v4;

1.2.10.6. Suporte a roteamento IPv6;

1.1.1.1. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6

1.2.10.7. Randomizar o número de sequência TCP, atuando como um proxy de número de sequência TCP ou possuir outra técnica para prevenção de ataques de roubo de sessão TCP (TCP Session Hijacking);

1.2.11. Suportar a criação de regras de filtragem por:

1.2.11.1. Endereço de origem e destino;

1.2.11.2. Sub-rede IP;

1.2.11.3. Porta de destino;

1.2.11.4. Tipo de protocolo;

1.2.11.5. Tipo de serviço ou aplicação;

1.2.11.6. Código de País (Por exemplo: BR, USA, UK, RUS);

1.2.12. Permitir a definição de período de validade de regras, ou seja, determinar a validade por um horário e data;

1.2.13. Implementar NAT (Network Address Translation) e PAT (Port Address Translation);

1.2.14. Implementar tags de VLAN Tagging (802.1q), sendo possível configurar 48 (quarenta e oito) vlan-id em uma mesma interface física;

1.2.15. Implementar pelo menos 1000 (mil) regras de firewall;

1.2.16. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

1.2.17. Implementar sincronização do relógio utilizando o protocolo NTP para sincronizar com bases externas;

1.2.18. Ser compatível com o estabelecimento ou passagem de túneis VPN Site-to-Site e Client-To-Site (L2TP, PPTP e GRE). Por estabelecimento entendemos que a solução é capaz de fechar túneis VPN entre ela e os clientes e vice-versa. Por passagem entendemos que a solução permite, por exemplo, que clientes em um segmento de rede interno fechem túneis VPN com clientes na internet e vice-versa.

1.2.19. Permitir criar dinamicamente, a partir da análise da sinalização H.225 (Call Setup) e H.245 (Call Control), as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre a MCU e as estações de videoconferência do MPDFT com estações remotas, consistindo essas permissões em combinações de:

1.2.19.1. IP e porta de origem (elemento originador da chamada);

1.2.19.2. IP e porta de destino (elemento chamado);

1.2.19.3. Redes de origem e destino do tráfego de vídeo com inspeção stateful.

1.2.20. Implementar Framework H.323;

1.2.21. Implementar multicast e unicast;

1.2.22. Para autenticação VPN e aplicação de regras baseadas em usuários/grupos do serviço de diretórios, implementar os seguintes protocolos de autenticação:

1.2.22.1. RADIUS;

1.2.22.2. LDAP;

1.2.22.3. Windows AD;

1.2.23. Para administração da ferramenta implementar os seguintes protocolos de autenticação:

1.2.23.1. RADIUS;

1.2.23.2. Autenticação Local.

1.2.24. Implementar compatibilidade com Microsoft Active Directory 2008 e 2012;

1.2.25. Ser administrado por ferramenta com interface gráfica remota segura, preferencialmente web, a partir de plataforma Windows 7 e Windows 10.

1.2.26. Implementar, junto com as características acima detalhadas, as seguintes funcionalidades simultaneamente habilitadas e integradas:

1.2.26.1. Sistema de VPN;

1.2.26.2. Sistema de prevenção e detecção de intrusão (IPS/IDS);

1.2.26.3. Sistema de categorização / filtragem de conteúdo e URL;

1.2.26.4. Sistema de antimalwares (antivírus e antispyware);

1.2.26.5. Sistema de inspeção de pacotes SSL/TLS (de-criptografia de pacotes);

1.2.26.6. Sistema de controle de aplicações (reconhecimento e filtragem de aplicações);

1.2.26.7. Sistema de QoS.

1.3. GERÊNCIA E ADMINISTRAÇÃO CENTRALIZADA

1.3.1. Permitir a replicação de configurações e a aplicação de atualização de softwares entre os elementos do cluster;

1.3.2. Permitir a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e logs;

1.3.3. Permitir a geração das seguintes informações, por período e elemento:

1.3.3.1. Auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

1.3.3.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;

1.3.3.3. Informações estatísticas de fluxo de tráfego;

1.3.3.4. Informações estatísticas de quantidade de sessões ou conexões e

1.3.3.5. Informações estatísticas de quantitativo de ataques identificados por tipo.

1.3.4. Possuir mecanismo que permite emitir os seguintes relatórios:

1.3.4.1. Sites com maior volume de dados acessados por usuário;

1.3.4.2. Sites acessados por determinados usuários (ou IPs), classificado por username, IP ou data/hora;

1.3.4.3. Sites bloqueados por determinados usuários (ou IPs), classificado por username, IP ou data/hora;

1.3.4.4. Usuários que acessaram determinado site por determinado período;

1.3.4.5. Sites bloqueados;

1.3.4.6. Malware encontrados;

1.3.4.7. Computadores e usuários que mais acessaram páginas HTTP e HTTPS, em MB;

1.3.4.8. Computadores e usuários que tiveram mais requisições bloqueadas;

1.3.4.9. Estatísticas de acesso HTTP e HTTPS por site em volume de dados (MB);

1.3.4.10. Estatísticas de acesso HTTP e HTTPS por sub-rede IP em volume de dados (MB);

1.3.4.11. Estatísticas de acesso HTTP e HTTPS por sub-rede IP e por computadores e usuários, em volume de dados (MB);

1.3.4.12. Estatísticas de acesso HTTP e HTTPS por extensão de arquivo acessado em volume de dados (MB).

1.3.5. Exportar os relatórios em pelo menos 2 dos seguintes formatos: HTML; PDF; CSV ou outro compatível com programa de planilha; XML.

1.3.6. Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis os dados dos últimos 90 (noventa) dias;

1.4. SISTEMA DE VPN

1.4.1. IPSec VPN Site-to-Site e Client-To-Site;

1.4.2. SSL VPN;

1.4.3. Atribuição de IPs nos clientes remotos de VPN;

1.4.4. Atribuição de DNS nos clientes remotos de VPN;

1.4.5. Estar licenciada para 1000 clientes de VPN simultâneos, sendo pelo menos 500 clientes IPSec e 500 clientes de VPN SSL.

1.4.6. IPSec VPN deve implementar:

1.4.6.1. 3DES e AES (128, 192 ou 256-bit);

1.4.6.2. Autenticação MD5, SHA-1 e SHA-256;

1.4.6.3. Diffie Hellman Group 1, Group 2 e Group 5

1.4.6.4. Algoritmo Internet Key Exchange (IKE) e certificados X.509;

1.5. SISTEMA DE PREVENÇÃO E DETECÇÃO DE INTRUSÃO (IPS/IDS)

1.5.1. Fazer inspeção profunda de pacotes (DPI), incluindo o payload, identificando perfis de tráfego anômalos, inclusive na modalidade Stateful Inspection;

1.5.2. Reconhecer e responder a ataques à rede e aos hosts, em tempo real;

1.5.3. Implementar configuração de perfis que permitam selecionar quais assinaturas que devem ser aplicadas a um grupo de dispositivos;

1.5.4. Implementar o bloqueio de vulnerabilidades por assinatura;

1.5.5. Implementar o bloqueio de exploits conhecidos;

1.5.6. Implementar os seguintes mecanismos de inspeção de IPS e efetuar suas respectivas proteções:

1.5.6.1. Análise de padrões de estado de conexões;

1.5.6.2. Análise de decodificação de protocolo;

1.5.6.3. Análise para detecção de anomalias de protocolo;

1.5.6.4. Remontagem de pacotes de TCP;

1.5.6.5. Bloqueio de pacotes malformados;

1.5.7. Bloquear os comportamentos e técnicas maliciosas abaixo:

1.5.7.1. Cabeçalhos inválidos de protocolo.

1.5.7.2. Técnicas de reconhecimento ativas, como varredura de IPs e portas e mapeamento de aplicações e sites web (Web Crawler);

1.5.7.3. Técnicas de invasão de aplicações web como Cross-site scripting e Injection (SQL, LDAP, OS commands, argumentos de programas).

1.5.7.4. Técnicas de negação de serviço como DOS (Denial of Service), SYN Flood, UDP Flood e ICMP Flood;

1.5.7.5. Consultas DNS de domínios maliciosos;

1.5.7.6. Acessos a serviços e IPs conhecidamente maliciosos;

1.5.7.7. Canal de comando de controle de malwares e botnets;

1.5.7.8. Estouro de pilha (buffer overflow);

1.5.7.9. Tráfego com perfil malicioso gerado por ameaças como: Spywares, Adware, Backdoor, Keylogger, Password stealer, Trojan, Rootkit e Network worm;

1.5.8. Detectar e prevenir ataques não orientados a conexão (stateless);

1.5.9. Permitir a aplicação de novas políticas sem interrupção de tráfego;

1.5.10. Executar as suas funções sem a instalação de agentes nos hosts a serem protegidos;

1.5.11. Identificar hosts conectados à rede que apresentem comportamento anormal potencialmente danoso, como propagação de malwares e botnets;

1.5.12. Capturar e armazenar a perfil do tráfego associado a cada dispositivo de rede, disponibilizando relatórios com as seguintes informações:

1.5.12.1. Endereço IP;

1.5.12.2. Serviços e portas utilizadas;

1.5.12.3. Tipo e volume de tráfego;

1.5.12.4. Aplicativos;

1.5.12.5. Vulnerabilidades ou ameaças associadas a cada dispositivo;

1.5.13. Identificar serviços sendo executados em portas não autorizadas;

1.5.14. Bloquear automaticamente o tráfego oriundo e destinado a hosts cujo comportamento esteja fora de conformidade com as políticas estabelecidas, ou seja, identificado como efetivamente ou potencialmente danoso.

1.5.15. Suportar assinaturas, seja nativamente ou por meio de configurações, para protocolos de aplicação, entre os quais devem constar, no mínimo, os seguintes:

1.5.16. HTTP, SMTP, FTP, RPC (MS-RPC), POP3, TELNET, DNS, IMAP, DHCP, TFTP, NNTP, RTSP, SNMP, SYSLOG, SSH, SMB (NetBIOS), MS-RPC, VNC, NTP, LDAP, NBNAME, SSL, NBDS e RADIUS;

1.5.16.1. AOL-IM, Yahoo-IM, Microsoft Live Messenger e IRC;

1.5.16.2. SIP.

1.5.17. Manter dados sobre ataques, com o número de vezes que um ataque ocorreu, quando e de que forma ele ocorreu e informações sobre quais aplicações foram usadas;

1.5.18. Deve suportar referência cruzada com CVE;

1.5.19. Em cada proteção de segurança, deve estar incluso informações como:

1.5.19.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

1.5.19.2. Severidade;

1.5.19.3. Tipo de ação a ser executada.

1.5.20. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.5.21. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.5.22. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.6. SISTEMA DE CATEGORIZAÇÃO / FILTRAGEM DE CONTEÚDO E URL

1.6.1. Filtrar o tráfego criptografado via SSL/TLS independente de porta, tanto na entrada quanto na saída (inbound e outbound), atuando como man-in-the-middle;

1.6.2. Verificar certificados de URL solicitadas, permitindo bloqueio, caso o certificado seja classificado como inválido;

1.6.3. Aplicar para o conteúdo criptografado os mesmos filtros utilizados para o protocolo HTTP.

1.6.4. Implementar filtros de URL bidirecionais (inbound e outbound) incluindo o exame de conteúdo de todas as requisições e respostas (requests e responses);

1.6.5. Implementar filtros de URL customizados por políticas;

1.6.6. Implementar filtros de URL baseados em base de dados armazenada localmente nos equipamentos ou armazenada remotamente em nuvem de alta disponibilidade, com opção de cache local das informações já consultadas;

1.6.7. Bloquear requisições por meio de filtros de extensão de arquivos;

1.6.8. Implementar controle de acesso a sites HTTP, HTTPS baseado em lista negra e lista branca;

1.6.9. Controlar o acesso a sites HTTP e HTTPS, permitindo a definição de perfis de acesso diferenciados para determinados serviços, endereços de origem, endereços de destinos, domínios, URLs, faixa de tempo, e usuários e grupos da rede Windows (utilizando a base de usuários e grupos do Active Directory);

1.6.10. Permitir ou bloquear sites ou categorias de sites, por:

1.6.10.1. Usuário do Active Directory;

1.6.10.2. Grupo do Active Directory e

1.6.10.3. Faixa de tempo.

1.6.11. Permitir o uso de wildcards, máscaras ou expressões regulares, permitindo que seja filtrado conteúdo presente no header HTTP;

1.6.12. A base de URLs deve ser atualizada automaticamente, por meio de conexão internet, no site do fabricante e deve possuir:

1.6.12.1. 20 (vinte) milhões de sites (domínios) registrados em pelo menos 50 (cinquenta) categorias pré-definidas;

1.6.12.2. Sites em 5 (cinco) idiomas, incluindo, necessariamente, inglês, português e espanhol;

1.6.12.3. Permitir a criação de categorias customizadas (user defined);

1.6.12.4. Permitir que qualquer site seja colocado manualmente em categoria customizada, diferente da original categorização de reputação do site.

1.6.13. Definir tempo de expiração de conexões para os protocolos HTTP, HTTPS, FTP;

1.6.14. Bloquear "scripts" como ActiveX e Javascript;

1.6.15. Bloquear download de arquivos baseado no tipo. Detectar o tipo de arquivo por meio das seguintes formas:

1.6.15.1. Parâmetro tipo de conteúdo (Content-Type) no cabeçalho da resposta HTTP e

1.6.15.2. Extensão do arquivo a ser recebido.

1.6.16. Controlar aplicações WEB, sendo possível definir ações de monitoramento e bloqueio de aplicações, incluindo: Instant Messaging e Streaming Media.

1.6.17. Registrar regras de exceção a sites HTTPS ou categoria de sites que não devem ter seu tráfego inspecionado;

1.6.18. Definir políticas que possam ser aplicadas por:

1.6.18.1. Categorias;

1.6.18.2. Horários do dia;

1.6.18.3. Dias da semana;

1.6.18.4. Endereço IP;

1.6.18.5. Usuário do Active Directory;

1.6.18.6. Grupo do Active Directory;

1.6.18.7. Expressões de request de URL e

1.6.18.8. Terminação de URLs (ex. "gov.br").

1.6.19. Possuir mecanismo que permite ao administrador do sistema definir determinada página como resposta quando a URL for bloqueada;

1.7. SISTEMA DE ANTIMALWARE

1.7.1. Inspecionar conteúdo para verificação e eliminação de vírus e malwares;

1.7.2. Inspecionar simultaneamente mais de um arquivo;

1.7.3. Efetuar análise de objetos encapsulados tais como ZIP, RAR e TAR permitindo configuração de bloqueio;

1.7.4. As verificações de malware devem ocorrer de forma concorrente para cada objeto analisado, em tempo real, sem enfileiramento;

1.7.5. Verificar tráfego analisando os dados de aplicação, identificando estações de trabalho da rede interna possivelmente infectadas por malwares.

1.7.6. Identificar e bloqueia aplicações maliciosas, inclusive dos tipos:

1.7.6.1. Java Scripts;

1.7.6.2. Java applets;

1.7.6.3. Java applications;

1.7.6.4. ActiveX;

1.7.6.5. Flash;

1.7.6.6. Executáveis Windows;

1.7.6.7. Potencialmente não desejados (spywares);

1.8. SISTEMA DE INSPEÇÃO DE PACOTES SSL/TLS (DE-CRIPTOGRAFIA DE PACOTES)

1.8.1. Controlar, inspecionar e de-criptografar SSL/TLS por política para tráfego de entrada (Inbound) e Saída (Outbound):

1.8.1.1. Deve identificar, de-criptografar e analisar o tráfego SSL/TLS em conexões de saída (Outbound);

1.8.1.2. Deve identificar, de-criptografar e analisar o tráfego SSL/TLS em conexões de entrada (Inbound);

1.8.2. A inspeção de SSL/TLS deve permitir a diferenciação de conexões pessoais (Bancos, Shopping etc.) e tráfegos não pessoais;

1.8.3. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

1.9. SISTEMA DE CONTROLE DE APLICAÇÕES (RECONHECIMENTO E FILTRAGEM DE APLICAÇÕES)

1.9.1. Implementar a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.9.2. Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos e controlar o uso da largura de banda que cada aplicação utiliza ou que cada usuário utiliza.

1.9.3. Reconhecer pelo menos 3000 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, bittorrent, gnutella, skype, facebook, linked-in, twitter, logmein, teamviewer, msrdp, 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, google-docs, spotify, netflix, etc;

1.9.4. Deve inspecionar o payload do pacote de dados com o objetivo de determinar, através de assinaturas de aplicações conhecidas pelo fabricante, a que tipo de aplicação pertence, mesmo quando

usada com portas não padrão;

1.9.5. 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.

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

1.9.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

1.9.8. Atualizar a base de assinaturas de aplicações automaticamente;

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

1.9.10. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

1.9.11. Implementar controle de largura de banda para priorização por aplicações (como por exemplo Skype, Bittorrent, YouTube, Spotify, Azureus) ou grupos de aplicações (como por exemplo Instant Messaging ou P2P);

1.9.12. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;

1.10. SISTEMA DE QOS

1.10.1. Implementar a criação de políticas de QoS por:

1.10.1.1. Endereço de origem;

1.10.1.2. Endereço de destino;

1.10.1.3. Por usuário ou Grupo do AD;

1.10.1.4. Por porta.

1.10.2. O QoS deve possibilitar a definição de classes por:

1.10.2.1. Banda Garantida;

1.10.2.2. Banda Máxima;

1.10.2.3. Fila de Prioridade.

1.10.3. Implementar priorização RealTime de protocolos de voz (VOIP) como H.323 e SIP.

1.10.4. Implementar marcação de pacotes Diffserv;

1.11. SISTEMA DE E-MAIL

1.11.1. Com todas as funcionalidades habilitadas, proteger 5.000 (cinco mil) usuários ou caixas postais de correio eletrônico;

1.11.2. Processar, no mínimo, 15.000 (quinze mil) mensagens por hora;

1.11.3. Implementar o protocolo SMTP (Simple Mail Transfer Protocol);

1.11.4. Controlar sessões SMTP e limitar o tráfego de mensagens baseado em endereço IP, range de IPs, subnet IP, nome de domínio, nome parcial de domínio e reputação do emissor;

1.11.5. Integrar-se com servidores de autenticação Microsoft Active Directory (LDAP ou Kerberos) para verificação de destinatários validos;

1.11.6. Inspecionar e bloquear mensagens baseando-se em:

1.11.6.1. Tamanho máximo de mensagem;

1.11.6.2. Número máximo de destinatários por mensagem;

1.11.6.3. Número máximo de destinatários por período (hora ou meia hora);

1.11.6.4. Número máximo de mensagens por conexão e

1.11.6.5. Número máximo de conexões simultâneas, por IP.

1.11.7. Possibilitar não aplicar (bypass) o filtro de verificação de DNS reverso para grupos de conexões de entrada. Possibilitando, por exemplo, que domínios de e-mail mal configurados não sejam bloqueados.

1.11.8. Possibilitar o bloqueio de maus remetentes e definir políticas individuais por remetente (tanto externo quanto interno) baseado em:

1.11.8.1. IP emissor;

1.11.8.2. Range de IP ou sub-rede;

1.11.8.3. Domínio;

1.11.8.4. Reputação do emissor;

1.11.8.5. Lista DNS;

1.11.9. Rejeitar mensagens baseado no remetente do envelope (usuario@domínio), usuário do envelope, domínio do envelope, inclusive com o uso de regex;

1.11.10. Possibilitar configurar filtro de Vírus e AntiSpam antes da chegada ao ambiente;

1.11.11. Possibilitar rate limit controlado por endereço de IP, domínio ou reputação do emissor: deve ser capaz de definir o fluxo de tráfego, baseado em períodos (em minutos);

1.11.12. Controle granular de políticas capazes de:

1.11.12.1. Checar DNS reverso e atribuir políticas;

1.11.12.2. Habilitar TLS preferido ou obrigatório;

1.11.12.3. Autenticação SMTP preferido ou obrigatório;

1.11.13. Deve possuir capacidade de implementar comunicação segura via TLS (Transport Layer Security);

1.11.14. Possuir DLP baseado em políticas que podem acionar automaticamente a criptografia ou bloquear/notificar o administrador com base na presença de dados confidenciais em e-mails que saem da organização;

1.11.15. Permitir o envio de mensagens através de TLS por domínio de destino;

1.11.16. Prevenir ataques de diretório (Directory Harvest Attack - DHA);

1.11.17. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento dos usuários válidos e ações de Ameaças, Spam e Filtragem de Conteúdo diferenciado por grupos do LDAP;

1.11.18. Deverá possuir funcionalidade de bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM) e Sender Policy Framework (SFP);

1.11.19. Rejeitar mensagens para destinatários inválidos durante o diálogo SMTP (prevenir Non-Delivery Report Attack);

1.11.20. Possuir detecção de spams, através da utilização de no mínimo 4 (Quatro) mecanismos distintos que permitam aumentar a exatidão na detecção de mensagens inválidas;

1.11.21. Deverá possuir monitoramento do tráfego de mensagens em tempo real, que permita identificar parâmetros críticos como volume de mensagens, histórico de conexões, conexões aceitas e rejeitadas, taxa de aceitação e de limites, filtros de reputação correspondentes, número de mensagens de spam positivos e suspeitos e número de vírus identificados;

1.11.22. Deverá possuir monitoramento do fluxo de mensagens em tempo real. Os fluxos de entrada e saída de mensagens devem ser exibidos separadamente;

1.11.23. Deverá possuir estatísticas em tempo real de destinatários inválidos, bloqueados por reputação, spams e vírus encontrados, além das mensagens limpas;

1.11.24. Permitir a checagem da rede global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens. O sistema de reputação deve utilizar dados de uma rede de monitoração de tráfego web e de e-mail para definir a reputação dos remetentes;

1.11.25. O sistema de reputação deverá checar a reputação dos remetentes em redes participantes com cobertura global. A rede de reputação não está somente baseada em informações de fluxo da própria base de Appliances instalada, mas sim, em inúmeros outros relatórios provenientes de gaiolas de Spam, listas de URL, listas de equipamentos comprometidos, composição da mensagem, IPs em blacklist, volume global de tráfego, listas brancas, composição da mensagem e web crawlers;

1.11.26. Possibilitar o controle de tráfego de e-mail por reputação atribuída pela rede de reputação, de cada IP que solicitou uma conexão. A rede de reputação deve monitorar parâmetros de e-mail e de Web;

1.11.27. Informações da rede de reputação também são utilizadas para análise das mensagens, pelo filtro de AntiSpam, utilizado no appliance;

1.11.28. Permitir tratamento de exceções ao bloqueio por reputação com base em IP, range de IP ou domínio;

1.11.29. Suportar tráfego de entrada e saída no mesmo appliance, com gerenciamento de políticas separadas;

1.11.30. Deverá permitir atribuição de diferentes endereços IP ao mesmo Appliance, possibilitando a administração de diversos domínios com MXs diferentes;

1.11.30.1. Suporte a múltiplos domínios por endereço IP, ou múltiplos domínios utilizando diferentes IPs no mesmo appliance;

1.11.31. Permitir gerenciar políticas por usuário ou grupo de usuários (baseado em endereço/domínio de remetente/destinatário, ou grupo do LDAP, como por exemplo, quando um único e-mail é enviado para diversos destinatários, será processado pela política específica de cada um dos destinatários);

1.11.32. Deverá possuir controle de fluxo baseado em grupo de remetentes:

1.11.32.1. Blacklists (IP, domínio ou reputação);

1.11.32.2. Whitelists (IP, domínio ou reputação);

1.11.32.3. Possibilitar a criação de vários grupos (por IP, domínio ou reputação);

1.11.32.4. RBLs/ORBLs de terceiros ou proprietárias; e

1.11.32.5. Whitelist e blacklist de endereços de remetentes e destinatários.

1.11.33. Permitir criar filtros definidos pelo tamanho de mensagem;

1.11.34. Permitir criar regras distintas para mensagem que entram e saem do ambiente;

1.11.35. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho e número de anexos;

1.11.36. Possuir regra específica para anexos protegidos por senha;

1.11.37. Possibilitar o bloqueio de mensagens que contenham anexos corrompidos;

1.11.38. Identificar arquivos anexados pelo seu tipo real, pelo seu nome, pela sua extensão e pelo seu tipo MIME;

1.11.39. Capaz de identificar arquivos pelo tipo de arquivo FileType (Finger Print) e extensões reais, incluindo-se arquivos de texto, executáveis, compactados, planilhas, documentos do MS Office e do OpenOffice, arquivos de imagem e arquivos de banco de dados (access, dbase);

1.11.40. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

1.11.41. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho e número de anexos;

1.11.42. Armazenar mensagens classificadas como SPAM em quarentena no próprio appliance ou em outro hardware especializado;

1.11.43. Permitir armazenar 30 dias de mensagens em quarentena, podendo o limite ser ajustado para valor inferior, de acordo com as políticas vigentes durante a execução do contrato;

1.11.44. Possibilitar adicionar na quarentena, duplicar e adicionar na quarentena, remover o anexo, redirecionar as mensagens para outro host ou destinatário, substituir a mensagem inteira ou apenas o anexo com modelo de notificação pré-definido;

1.11.45. Possuir configurações de criptografia:

1.11.45.1. A solução deve conter módulo de criptografia das mensagens. A solução deverá ser integrada ao appliance ou em um appliance específico para criptografar as mensagens. Neste caso deverá estar explícito a marca e modelo do equipamento utilizado para tal fim;

1.11.45.2. Ser capaz de criar perfis de criptografia tanto para uso de servidores externos quanto servidores internos;

1.11.45.3. Ser capaz de criptografar mensagens localmente ou de redirecionar mensagens para solução externa de criptografia através de criação de regras que especifiquem quais mensagens devem ser criptografadas. As regras deverão ser de acordo com a necessidade do órgão no mínimo por destinatário e remetente;

1.11.45.4. Ser capaz de criar perfis diferentes para cada regra específica de mensagens a serem criptografadas;

1.11.45.5. O método de criptografia utilizado não deve depender da instalação de softwares ou plugins na máquina do remetente e do destinatário;

1.11.45.6. Deve permitir que os receptores das mensagens criptografadas possam responder e/ou encaminhar à mensagem de forma criptografada, para garantir a segurança da informação;

1.11.45.7. As regras de mensagens a serem criptografadas podem ser criadas para estar de acordo com as normas de conformidade, tais como HIPAA, SOX e GLB;

1.12. SISTEMA SANDBOX

1.12.1. A Sandbox deverá ser integrada a solução, podendo ser on premisses ou na nuvem, sendo obrigatória a integração com o NGFW.

1.12.1.1. Esse sistema será usado, no mínimo, pelos sistemas de EMAIL, ANTIMALWARE e FILTRO DE CONTEÚDO E URL;

1.12.2. Deverá ser possível analisar arquivos suspeitos incluindo, mas não se limitando, as extensões .exe, .com e .dll, .doc, .docx, .rtf, .pdf, .zip, .RAR e .7Z com até 10MB.

1.12.3. Deverá fazer análise dinâmica do comportamento do malware em ambientes que simulam ambientes reais.

1.12.3.1. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.12.3.2. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.12.4. O tempo para análise de um arquivo de 10MB não pode ultrapassar 120 segundos.

1.12.5. A solução de segurança deverá enviar o hash do arquivo suspeito para a Sandbox para determinar se ele foi analisado anteriormente. Se o hash do arquivo foi analisado anteriormente, a Sandbox determina se o arquivo é entregue no dispositivo do usuário ou bloqueado.

1.12.6. Se o hash for desconhecido para a Sandbox, uma cópia do arquivo suspeito deverá ser enviada e analisada pela Sandbox. Uma vez analisado, a Sandbox determina se o arquivo é entregue no dispositivo do usuário ou bloqueado.

1.12.6.1. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.12.6.2. Número de arquivos emulados;

1.12.6.3. Numero de arquivos com malware.

1.12.7. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

2. DO SERVIÇO DE SEGURANÇA DE PERÍMETRO

2. DESCRIÇÃO

2.1.1. O Serviço de Gerenciamento de Segurança de Perímetro com uso de firewall tipo “Next Generation Firewall – NGFW” é composto pelo fornecimento de proteção, controle e resposta a incidentes de rede, monitoração e administração dos sistemas descritos neste documento, pelo fornecimento, instalação e configuração de hardware e softwares da solução, e pela transferência de conhecimento.

2.1.2. O serviço será pago mensalmente.

2.2. REQUISITOS DE SEGURANÇA

2.2.1. Todos os profissionais que prestarem serviços relativos à solução devem ser credenciados junto ao MPDFT para que sejam autorizados a prestar serviços nas dependências do órgão.

2.2.2. A contratada deverá observar, rigorosamente, todas as normas, padrões e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do MPDFT.

2.2.3. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE.

2.2.4. Caberá à CONTRATADA comunicar ao MPDFT qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do MPDFT, porventura colocados à disposição para realização dos serviços contratados.

2.2.5. Deve ser mantido sigilo sobre todos os ativos de informações e de processos do MPDFT e da CONTRATADA que se refiram ao MPDFT.

2.2.6. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do MPDFT, sob pena de aplicação das sanções cabíveis.

2.2.7. Manter em caráter confidencial, as informações relativas à política de segurança adotada pelo MPDFT e as configurações de hardware e de Softwares decorrentes.

2.2.8. Manter em caráter confidencial, as informações relativas ao processo de instalação, configuração e adaptações de produtos e ferramentas.

2.2.9. Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pelo MPDFT, durante o tempo de permanência nas dependências do órgão.

2.3. MONITORAMENTO DOS EQUIPAMENTOS E RELATÓRIOS DE OPERAÇÃO E GESTÃO DA SOLUÇÃO

2.3.1. A contratada deverá prover informações de monitoramento dos serviços/elementos que compõem a solução e disponibilizar consultas online, cujos resultados permitam a verificação da conformidade com o estabelecido no Níveis Mínimos de Serviço Exigidos (NMSE), bem como o planejamento de capacidade e a análise da efetividade da solução;

2.3.2. Deverão ser monitorados não só os equipamentos, mas os sistemas da solução, incluindo, mas não limitado ao IPS, filtro de URLS e antimalware.

2.3.3. O monitoramento e as consultas de que tratam o item anterior devem ser disponibilizas por meio de interface Web e/ou interface de gerência dos equipamentos;

2.3.4. Deve permitir consultas online que contemplem, no mínimo, mas não limitado a:

2.3.4.1. Gerar relatórios administrativos e técnicos, ambos customizáveis de modo a permitir a seleção de períodos de abrangência, em forma de textos e gráficos, com possibilidade de exportar para HTML ou PDF.

2.3.4.2. Visualizar informações relacionadas aos chamados técnicos: data e hora de abertura da solicitação; Identificação do solicitante, código de identificação da solicitação, descrição da solicitação, andamento da solicitação (worklog), data e hora de fechamento da solicitação;

2.3.4.3. Visualizar informações relacionadas a notificação e tratamento de incidentes: Data e hora de registro do incidente, identificação do responsável pelo registro, código de identificação do incidente, descrição do incidente, severidade do incidente, data e hora da notificação do incidente e tratamento adotado para o incidente;

2.3.4.4. Visualizar o desempenho dos equipamentos que compõem a solução, como utilização de disco, memória, CPU, tráfego na interface de rede;

2.3.4.5. Visualizar os logs dos equipamentos que compõem a solução;

2.3.4.6. Visualizar a disponibilidade e desempenho dos elementos/serviços da solução em tempo real e por período;

2.3.4.7. Visualizar bloqueios efetuados pelo serviço de firewall;

2.3.4.8. Visualizar bloqueios efetuados pelo serviço de filtragem de email;

2.3.4.9. Visualizar bloqueios efetuados pelo serviço de filtragem de conteúdo, categorizados por tipo de conteúdo;

2.3.4.10. Visualizar bloqueios feitos pelo serviço de prevenção de intrusão, totalizados por assinatura e/ou por endereços IP de origem e de destino;

2.3.4.11. Visualizar endereços IP de origem e de destino com maior número de acessos, endereços IP de origem e de destino cujos acessos produziram o maior volume de tráfego;

2.3.4.12. Visualizar volume de tráfego por protocolo e por aplicação.

2.3.5. A CONTRATANTE também realizará o monitoramento dos serviços/elementos que compõem a solução;

2.3.6. Todos os equipamentos responsáveis pela execução dos serviços contratados deverão ser acessíveis a partir de plataformas de gerenciamento e monitoramento SNMP localizadas na rede interna do CONTRATANTE.

2.3.7. As ferramentas de monitoramento utilizadas pela CONTRATANTE são CACTI e Nagios;

2.3.8. A CONTRATADA deve fornecer os templates de monitoramento dos equipamentos que compõem a solução ou as informações de OID's (identificadores de objetos) das MIB´s (Base de Informação de Gerenciamento) que devem ser monitoradas via SMNP.

2.3.9. O monitoramento será utilizado para gerar relatórios mensais de disponibilidade e desempenho da solução e aplicações de penalidades.

2.3.10. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (indisponibilidade) da solução de forma interativa ("on-line"), a partir do início do Período de Funcionamento Experimental (PFE), dando acesso ao sistema de monitoramento da CONTRATADA ou implementando o monitoramento na infraestrutura da CONTRATANTE;

2.3.11. A CONTRATADA terá de apresentar relatórios técnicos mensalmente contendo informações de desempenho, para que seja identificada com antecedência a necessidade de adição/substituição de hardware/software;

2.3.12. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 5 (cinco) minutos, a CONTRATADA deverá entregar ao MPDFT, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível;

2.3.13. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar à CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências da CONTRATANTE, por ações ou solicitações da CONTRATANTE ou ainda por manutenções programadas.

2.4. MONITORAMENTO DE REDES E ANÁLISE E REPOSTA A INCIDENTES DE SEGURANÇA

2.4.1. No intuito de identificar, analisar e responder a incidentes de segurança, A CONTRATADA deverá monitorar todos os elementos do Serviço de Segurança de Perímetro em regime de 24 horas por dia, 7 dias da semana, 365 dias por ano;

2.4.2. O monitoramento deverá ser realizado através de sensores, que coletarão as informações e enviarão de forma segura ao Centro de Monitoramento e Resposta a Incidentes (CMRI);

2.4.3. Os sensores deverão coletar minimamente, mas não limitado a:

2.4.3.1. Informações relevantes sobre o desempenho dos elementos monitorados;

2.4.3.2. Informações relevantes sobre a disponibilidade dos elementos monitorados;

2.4.3.3. Informações relevantes sobre a segurança dos elementos monitorados;

2.4.4. Os sensores deverão identificar e reportar, em tempo real, as ameaças, ataques e intrusões detectados pela Solução de Segurança de Perímetro;

2.4.5. As informações monitoradas, detectadas ou coletadas deverão ser enviadas sempre de forma segura (comunicação criptografada) ao Centro de Monitoramento e Resposta a Incidentes;

2.4.6. Em caso de perda de comunicação com o Centro de Monitoramento e Resposta a Incidentes, os sensores deverão realizar armazenamento local (cache) das informações coletadas até que a comunicação seja reestabelecida, momento no qual a sonda irá enviar todos os dados históricos ao CMRI, de forma que não ocorram perdas de dados (gaps);

2.4.7. Os sensores deverão ter capacidade de armazenamento local (cache) de, no mínimo, 7 dias de dados;

2.4.8. O acesso ao CMRI deve ser restrito apenas a funcionários autorizados;

2.4.9. O CMRI deverá contar com funcionários capacitados e altamente profissionais para a realização das atividades de monitoramento de redes e análise e reposta a incidentes de segurança, contendo, no mínimo, um profissional com certificado válido para cada uma das competências abaixo:

2.4.9.1. ISO/IEC 27002;

2.4.9.2. Operação e administração dos equipamentos que compõe os serviços de segurança de perímetro;

2.4.10. Ao detectar tentativas de ataques à rede interna da CONTRATANTE ou aos serviços disponíveis em seu ambiente, a CONTRATADA deverá adotar, de imediato, as medidas de combate ao ataque independentemente das que forem estabelecidas pela CONTRATANTE. No caso dessas medidas implicarem interrupções e/ou descaracterização dos serviços em uso, a CONTRATADA deverá entrar em contato com a CONTRATANTE em, no máximo, 2 (duas) horas, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las. A CONTRATANTE se responsabilizará por eventuais danos causados pela não autorização de ações recomendadas pela CONTRATADA.

2.4.11. Caberá à CONTRATADA o registro, monitoração, triagem e classificação prévia de severidade de todos os alertas de incidentes emitidos pelos serviços administrados, em especial os relacionados a tentativas de ataques em direção à rede do CONTRATANTE ou por ela originados; adotar, de imediato, as medidas de tratamento que forem acordadas com o CONTRATANTE, cabendo a este a classificação final da severidade. Tais medidas estarão relacionadas com o grau de severidade constante na assinatura do ataque indicado pelo Serviço de Prevenção de Intrusão.

2.5. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS (NMSE)

2.5.1. DESEMPENHO DOS EQUIPAMENTOS DA SOLUÇÃO:

2.5.1.1. Será considerado degradação de desempenho dos equipamentos da solução a ocorrência de quaisquer dos eventos a seguir:

2.1.1.1. Perda de pacotes superior a 1%;

2.5.1.1.1. Uso de recurso computacional (CPU e taxa de utilização de espaço em disco) que ultrapasse 85% por um período mínimo de 15 (quinze) minutos ininterruptos;

2.5.1.1.2. Média semanal (de segunda-feira a sexta-feira, exceto feriados e recessos forenses) de consumo de CPU, hora a hora, durante o pico de horário de trabalho, das 14 horas às 18 horas, superior a 75%;

2.5.1.2. A operação dos equipamentos com taxas superiores à especificada no item anterior implicará adequação ou reconfiguração do equipamento por parte da CONTRATADA.

2.5.2. DISPONIBILIDADE

2.5.3. Será considerado INDISPONIBILIDADE o período no qual ocorrer interrupção, falha ou degradação de desempenho de equipamento ou sistema, ativos do cluster, que compõem o serviço detectado pelo monitoramento da CONTRATANTE ou da CONTRATADA, o que ocorrer primeiro;

2.5.4. O percentual de disponibilidade corresponde ao período, durante um período mensal de operação, em que todos os serviços da solução estiverem em condições normais de funcionamento, sem

interrupção, falha ou degradação de desempenho de equipamento, funcionalidade ou serviço registrado pelo monitoramento, seja da CONTRATADA ou do CONTRATANTE;

2.5.5. A solução deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive sábados, domingos, feriados e no Período de Funcionamento Experimental - PFE;

2.5.6. O percentual mínimo aceitável de disponibilidade mensal de todos os serviços que compõem a solução de segurança de perímetro é de 99,7%.

2.5.7. Mensalmente, deverá ser calculado o percentual de disponibilidade da solução de segurança de perímetro, com base na seguinte fórmula:

*D = [(Tm-Ti)/Tm]*100, onde:*

D = Percentual de disponibilidade

Ti = Somatório dos minutos em que forem observadas inoperâncias que caracterizem indisponibilidade em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento;

Tm = é o tempo total mensal de operação, em minutos, no mês de faturamento;

2.5.8. Sempre que forem apurados percentuais de disponibilidade que estejam abaixo do limite mínimo estabelecido (99,7%), os somatórios dos tempos de inoperância, dentro do período de faturamento, serão descontados dos valores mensais da solução, tomando-se como base a seguinte fórmula:

***Dc** = 5*Vm*(Ti/Tm), onde:*

***Dc** = Valor do desconto;*

Vm = Valor mensal da solução;

Ti = Somatório dos minutos em que forem observadas inoperâncias que caracterizem indisponibilidade em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento;

Tm = é o tempo total mensal de operação, em minutos, no mês de faturamento;

2.5.8.1. Ficam também estabelecidos limites de tolerância para os percentuais de disponibilidade calculados, que ao serem excedidos, determinarão glosas específicas nos valores da solução, conforme demonstrado a seguir:

2.5.8.2. Percentuais de disponibilidade igual ou inferiores a 95% ensejarão a glosa de 50% do valor mensal da solução;

2.5.8.3. Percentuais de disponibilidade igual ou inferiores a 90% ensejarão a glosa de 90% do valor mensal da solução.

2.1.1.2. Nos casos em que forem efetuadas a glosa acima, não se aplicará o desconto no valor mensal calculado pela fórmula "Dc = 5*(Vm*Ti)/Tm".

2.5.9. Será computado como tempo de indisponibilidade (Ti):

2.5.9.1. O período compreendido desde o evento gerador da interrupção, falha ou degradação de desempenho de equipamento, funcionalidade ou serviço até sua total recuperação;

2.5.9.2. O tempo total decorrido entre a primeira e a última ocorrência no caso de ocorrências sucessivas de indisponibilidade dentro de um intervalo inferior a 12 (doze) horas do surgimento da primeira. Tais períodos serão considerados de "recorrência" da primeira ocorrência de indisponibilidade;

2.5.10. Não será computado como tempo de indisponibilidade (Ti) as seguintes situações que ocorram nas instalações do MPDFT:

2.5.10.1. Falta de energia no local;

2.5.10.2. Indisponibilidade da rede lógica do MPDFT à qual o item esteja conectado;

2.5.10.3. Manutenções programadas pelo MPDFT e manutenções programadas pela contratada, desde que autorizadas previamente pelo MPDFT, desde que realizadas durante a janela de tempo acordada;

2.5.10.4. Problemas derivados de ocorrências no ambiente do MPDFT, onde comprovadamente a indisponibilidade não esteja sendo controlada pela contratada;

2.6. MANUTENÇÃO PREVENTIVA

2.6.1. Entende-se como Manutenção Preventiva: o monitoramento, operação, administração e assistência técnica de todos os componentes do serviço fornecido pela CONTRATADA;

2.6.2. A Manutenção Preventiva será iniciada junto com o Período de Funcionamento Experimental - PFE estendendo-se por todo o período de vigência do Contrato;

2.6.3. A Manutenção Preventiva deverá cobrir a localidade de Brasília/DF e outra localidade, onde, porventura, a CONTRATADA venha a instalar hardware da solução, devendo ser feito pela CONTRATADA, pelo fabricante ou empresas credenciadas pela fabricante;

2.6.4. Os serviços de suporte técnico devem operar em regime de 24 horas por dia, 7 dias da semana, 365 dias por ano;

2.6.5. Sem apresentar qualquer ônus adicional à CONTRATANTE, a Manutenção Preventiva de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, incluindo, mas não se limitando, a esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias, substituição total ou parcial do produto como peças, partes, componentes ou acessórios;

2.6.6. A CONTRATANTE poderá, a qualquer momento, determinar à CONTRATADA a execução de rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos;

2.6.7. Serviços de assistência técnica deverão ser executados pela CONTRATADA sempre que se fizer necessário, independentemente de haver solicitação por parte da CONTRATANTE;

2.6.8. A realização de assistência técnica preventiva deverá ser combinada entre as partes com antecedência mínima de 2 dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção da CONTRATANTE;

2.6.9. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho;

2.6.10. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

2.6.11. Deverão ser abertos chamados de severidade Alta ou Média para a realização da assistência técnica corretiva.

2.6.12. Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar ao CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos nos acordos de níveis de serviço;

2.6.13. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados remotamente a todos os produtos fornecidos pela CONTRATADA, podendo ser realizada nas dependências da CONTRATANTE, desde que haja necessidade e prévia autorização pela CONTRATANTE ou a pedido desta.

2.6.14. A CONTRATADA não poderá deixar de executar a assistência técnica preventiva e/ou corretiva nos produtos fornecidos sob nenhum pretexto;

2.6.15. A CONTRATADA deverá manter atualizados os equipamentos destinados à execução dos serviços, implementando as últimas versões estáveis, atualizações e correções de hardware e software recomendadas pelo fabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção, de forma programada em acordo com a equipe de infraestrutura de produção do MPDFT.

2.6.16. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do Contrato;

2.6.17. A CONTRATADA deverá substituir qualquer equipamento que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.6.17.1. Degradação de desempenho insolúvel por meio de adequação/reconfiguração;

2.6.17.2. Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva relativos ao mesmo problema dentro de um período contínuo de 30 (trinta) dias;

2.6.18. A CONTRATADA deverá substituir, no prazo máximo e condições definidos para chamados de severidade média ou alta, qualquer peça ou componente que apresente falha ou indício de falha;

2.6.19. Na impossibilidade de atendimento do prazo de solução definitiva, será permitida a substituição temporária do equipamento, peça ou componente, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva por até 60 dias corridos;

2.6.20. Tanto na substituição temporária quanto na definitiva, só será admitida com anuência da CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça ou componente ofertado, em relação àquele que está sendo substituído;

2.6.21. A CONTRATADA somente poderá efetuar manutenção técnica que tenha previsão de indisponibilidade na solução e seus componentes após aprovação por parte da CONTRATANTE. Caso a manutenção seja efetuada sem essa aprovação, será considerado como indisponibilidade. O mesmo ocorrerá quando ultrapassado o prazo acertado para manutenção;

2.6.22. Se houver substituição temporária ou definitiva em decorrência de assistência técnica, o equipamento, peça ou componente deverá ser homologado pelo fabricante dos equipamentos e, no mínimo, apresentar as mesmas características de desempenho do serviço antes da apresentação do problema;

2.6.23. Caso seja necessário enviar o equipamento, peça ou componente para um centro de assistência técnica fora das dependências da CONTRATANTE, a CONTRATADA deverá desinstalar, embalar, transportar e reinstalar, bem como deverá arcar com todos os custos necessários;

2.6.24. O envio de equipamentos para centros de assistência técnica em outra localidade não exime a CONTRATADA do cumprimento dos prazos estabelecidos nos níveis de serviço exigidos;

2.6.25. Para a remoção de equipamento, peça e componente será necessária autorização de saída por escrito emitida por servidor da CONTRATANTE, a ser concedida ao funcionário da CONTRATADA, formalmente identificado;

2.6.26. Caberá à CONTRATADA gerenciar permanentemente durante toda a vigência do contrato, de forma proativa, toda a solução adquirida, garantindo os níveis de serviço acordados.

2.6.27. Caso seja necessária a instalação de equipamentos de administração da solução nas instalações do CONTRATANTE, a CONTRATADA deverá fornecer todos os recursos necessários para tanto. O CONTRATANTE ficará responsável apenas pelo fornecimento de alimentação elétrica e portas lógicas para as conexões;

2.6.28. O acesso aos equipamentos eventualmente hospedados no MPDFT dar-se-á por meio de VPNs via Internet, a serem implementadas pela CONTRATADA. De forma a possibilitar a administração remota, a CONTRATADA poderá optar por proceder a instalação e a manutenção de canal de comunicação direto com os equipamentos sob sua responsabilidade, devendo se responsabilizar e garantir total segurança para este acesso. Atuações locais, que necessitem de acesso físico direto ao ambiente e ao equipamento, deverão ser previamente comunicados e acordados com a equipe do MPDFT.

2.6.29. O CONTRATANTE possui link de internet que poderá ser utilizado para o estabelecimento das VPNs mencionadas no item anterior;

2.6.30. A CONTRATADA deverá, por meio da administração remota, ser capaz de implementar políticas, regras, filtros ou quaisquer outros recursos e implementações lógicas, necessárias a manutenção do serviço em conformidade com o especificado. As solicitações de alterações e inclusões de novas políticas, regras e filtros efetuados pelo CONTRATANTE não serão limitadas e deverão ser implementadas, de acordo com o ANS.

2.6.31. A CONTRATADA deverá criar contas de acesso, com permissões de leitura, à administração do serviço para a equipe técnica do CONTRATANTE, que permitam a observação de todas as configurações de administração e gerência da solução. Todos os acessos à administração dos serviços serão individuais, inclusive aqueles efetuados pela CONTRATADA, e deverão ser autenticados, criptografados e registrados para posterior auditoria.

2.6.31.1. As contas de acesso da CONTRATANTE poderão ter acesso privilegiado de administrador em caso de comum acordo entre CONTRATADA e CONTRATANTE.

2.6.32. A instalação, remoção ou desligamento das funcionalidades dos equipamentos deverá, sempre que possível, ser realizada sem que outros componentes da rede local do CONTRATANTE necessitem de configuração adicional.

2.6.33. A CONTRATADA deverá desempenhar suas atividades por intermédio de pelo menos dois técnicos devidamente identificados, especializados e qualificados da seguinte forma: formação específica e oficial do fabricante para as atividades de instalação, configuração e suporte, envolvendo os equipamentos e programas da solução, a ser comprovada com certificado e/ou declaração de curso(s) técnico(s), emitidos pelo fabricante dos mesmos ou empresa credenciada e qualificada para esta finalidade.

2.6.34. A CONTRATADA deverá enviar à CONTRATANTE a relação dos técnicos que devem ser autorizados a entrar nas dependências da CONTRATADA, juntamente com os documentos necessários para cadastro na segurança institucional do órgão. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE.

2.6.35. Caso a Equipe de Atendimento Técnico da CONTRATADA sofra alguma alteração em sua composição durante a vigência deste contrato, tal fato deve ser imediatamente informado ao gestor do contrato e à equipe técnica do MPDFT, incluindo as respectivas comprovações acerca dos requisitos de qualificação exigidos para esses profissionais e as informações necessárias para liberação do acesso dos técnicos às dependências do MPDFT, conforme itens anteriores.

2.6.36. Caso seja constatada a falta de conhecimento mínimo necessário para operação da solução por parte do prestador de serviço, a equipe técnica do MPDFT poderá solicitar sua substituição por técnico devidamente qualificado.

2.7. ABERTURA E ACOMPANHAMENTO DE CHAMADOS

2.7.1. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço para abertura/acompanhamento de chamados que deverá estar acessível durante 24 horas por dia, 7 dias da semana, 365 dias por ano, sem ônus adicional para a CONTRATANTE, constituído de no mínimo:

2.7.1.1. Serviço de atendimento com discagem gratuita (0800) ou de custo local para telefone fixo (DDD 61);

2.7.1.2. Sítio Web com HTTPS como meio de comunicação de disponibilidade imediata, em língua portuguesa e/ou inglesa;

2.7.1.3. E-mail;

2.7.2. A CONTRATADA informará, no momento da abertura das solicitações de suporte técnico, no mínimo, o número do chamado, a severidade, a data e hora da solicitação, nome do SOLICITANTE, descrição detalhada da solicitação;

2.7.3. A CONTRATADA encaminhará mensagem de e-mail para os contatos definidos pela CONTRATANTE informando o número de cada chamado técnico aberto, que servirá de referência para acompanhamento dos atendimentos, e sua descrição, independentemente da forma de sua abertura, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado pela da equipe técnica da CONTRATANTE.

2.7.4. A CONTRATANTE terá acesso ao sistema Web da CONTRATADA para acompanhamento, consulta, histórico dos chamados abertos, independentes da sua forma de abertura;

2.7.5. Os serviços de suporte técnico serão acionados a partir da queda, falha ou registro de indisponibilidade gerado pelo monitoramento da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica da CONTRATANTE. Esses chamados serão classificados conforme as severidades e prazos especificados a seguir:

2.7.5.1. **Severidade EMERGENCIAL**: esse nível de severidade é aplicado para chamados relacionados a ataques e ações relativas às suas respostas ou chamados condicionados à urgência da CONTRATANTE. Este último limitado a um total de 15 chamados mensais e, caso haja necessidade de abertura deste tipo de chamado além do limite previsto, este será pago adicionalmente. Prazo de solução: 2 horas após abertura do chamado ou ocorrência/detecção de evento relacionado a essa severidade.

2.7.5.2. **Severidade ALTA**: Esse nível de severidade é aplicado para o gerenciamento de políticas de tráfego, incluído, mas não limitado, a criação e alteração regras de firewall, IPS, NAT, QoS, filtragem de conteúdo, filtragem de e-mail; ou quando há indisponibilidade na solução ou em qualquer serviço que a compõe. Prazo de solução definitiva: 4 horas após abertura do chamado ou ocorrência/detecção de evento relacionado a essa severidade.

2.7.5.3. **Severidade MÉDIA**: Esse nível de severidade é aplicado para solicitações de alteração de configurações nos serviços que compõem a solução quando não forem relacionadas a gerenciamento de políticas de tráfego; ou quando há algum problema nos elementos que compões a solução embora ainda estejam disponíveis, conforme definição de disponibilidade deste termo de referência. Prazo de solução definitiva: 6 horas após abertura do chamado.

2.7.5.4. **Severidade BAIXA**: Esse nível de severidade é aplicado para: solicitação de manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos; ou atualização dos produtos que compõem a solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Prazo de solução definitiva: 3 dias úteis a partir da abertura do chamado.

2.7.6. Serão considerados para efeitos dos níveis exigidos; Prazo de Solução Definitiva: Tempo decorrido entre o registro de um evento gerador de um chamado e a solução definitiva.

2.7.7. É vedado a CONTRATADA interromper o atendimento de um chamado, exceto quando se tratar de chamado de severidade BAIXA, até que se chegue à solução definitiva, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderão acarretar custos adicionais à CONTRATANTE. A interrupção do atendimento de um chamado desse tipo de

severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar em aplicação de penalidades previstas;

2.7.8. Após concluído o suporte técnico e com o serviço efetivamente recolocado em pleno estado de funcionamento, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até o momento em que o serviço seja efetivamente recolocado em pleno estado de funcionamento pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá por e-mail, telefone ou através da interface de gerenciamento as pendências relativas ao chamado aberto;

2.7.8.1. Caso não haja manifestação dentro do prazo estipulado para o chamado em questão ou caso a CONTRATANTE entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

2.7.9. A CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 10 usuários que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério da CONTRATANTE e configurados pela CONTRATADA. Essa lista pode mudar durante o período de vigência do contrato.

3. DO SERVIÇO DE IMPLANTAÇÃO E HOMOLOGAÇÃO

3. DOCUMENTAÇÃO TÉCNICA E TRANSFERÊNCIA DE CONHECIMENTO

3.1.1. Deverá ser entregue pela CONTRATADA a "Documentação Técnica" (DT) de toda a solução implementada no ambiente da CONTRATANTE, composta de:

3.1.1.1. Plano de Implantação, contendo as configurações específicas dos equipamentos, arquiteturas e suas topologias e diagramas lógicos da solução;

3.1.1.2. Plano de Testes;

3.1.1.3. Plano de Transferência de Conhecimento.

3.1.2. Essa documentação fica sujeita à análise e à aprovação da equipe técnica da CONTRATANTE;

3.1.3. Toda a DT deverá ser entregue em mídia digital, devendo as topologias da solução serem entregues em formato a ser definido pela CONTRATANTE;

3.1.4. Essa documentação fica sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

3.1.5. Toda a DT fornecida pela CONTRATADA referente às ferramentas e solução implantadas no ambiente da CONTRATANTE é de propriedade da CONTRATANTE.

3.1.6. Toda a DT fornecida pela CONTRATADA deverá estar em português do Brasil.

3.2. PLANEJAMENTO

3.2.1. O Plano de Implantação deverá conter a descrição de, no mínimo:

3.2.1.1. Atividades a serem desenvolvidas, incluindo testes, e seus respectivos cronogramas;

3.2.1.2. Políticas de configuração dos elementos da solução;

3.2.1.3. Topologia lógica para a solução;

3.2.1.4. Ações de rollback.

3.2.2. Todo o trabalho realizado deve seguir o especificado no Plano de Implantação;

3.2.3. Para cada nova *release*, *build* ou funcionalidade, poderá ser solicitada uma nova implantação de qualquer funcionalidade presente na solução;

3.2.4. A CONTRATADA deverá realizar toda a instalação dos produtos, incluindo a configuração das ferramentas e os testes da solução, sob supervisão da CONTRATANTE;

3.2.5. Todas as atividades envolvidas na Implantação deverão ser acompanhadas pela equipe técnica da CONTRATANTE;

3.2.6. Todos os técnicos envolvidos na instalação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade de acordo com este termo de referência.

3.2.7. A CONTRATADA será responsável por dimensionar a solução a ser adotada na rede da CONTRATANTE atendendo minimamente os requisitos solicitados neste termo de referência. Esta solução estará sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

3.2.8. Tanto a solução quanto a execução do Plano de Implantação não podem causar impactos no funcionamento da rede (por exemplo, lentidão na rede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente ao usuário;

3.2.9. Caso o dimensionamento da solução feito pela CONTRATADA não apresente desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto no item anterior, a solução deverá ser redimensionada sem ônus adicional para a CONTRATANTE, mesmo que o redimensionamento envolva adição/substituição de hardware e software;

3.2.10. Junto com o Plano de Implantação, a CONTRATADA deverá apresentar um Plano de Testes à equipe técnica da CONTRATANTE para avaliação;

3.2.11. O Plano de Testes consiste num documento onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos, descritas neste Termo;

3.2.12. O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar seu acompanhamento por parte da CONTRATANTE;

3.2.13. Na tabela mencionada no item anterior, deve-se incluir os resultados esperados para cada teste realizado;

3.2.14. Os procedimentos descritos no Plano de Testes serão realizados pela CONTRATADA após a instalação e configuração dos produtos. Esses testes serão acompanhados pela equipe técnica da CONTRATANTE;

3.2.15. Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização dessas correções, os testes serão reiniciados;

3.2.16. Se todos os testes forem realizados com sucesso, os produtos serão considerados implantados;

3.2.17. A CONTRATADA deverá fornecer todos os materiais necessários à instalação física, à configuração e ao perfeito funcionamento dos equipamentos, cabos elétricos e cabos lógicos, quando for o caso. Caberá à CONTRATANTE o provimento de alimentação elétrica e das portas UTP para conexão à rede local;

3.2.18. Para a homologação da solução, será estabelecido pela CONTRATANTE um PFE - Período de Funcionamento Experimental, com duração de 10 dias corridos, para testar o perfeito funcionamento dos produtos, verificar suas funcionalidades, analisando sua aderência às especificações deste Edital e seus Anexos, bem como à Proposta da CONTRATADA, e a sua compatibilidade com a estrutura já existente na CONTRATANTE;

3.2.19. O PFE somente poderá ser iniciado após a conclusão da implantação.

3.2.20. Pelo menos um técnico da CONTRATADA deverá acompanhar presencialmente o decorrer do PFE.

3.2.21. Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos;

3.2.21.1. Caso haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização destas correções, o PFE será reiniciado.

3.2.21.2. Caso não haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a solução será considerada homologada.

3.2.22. Os produtos funcionarão de acordo com as recomendações do fabricante, levando-se em consideração que todas as funcionalidades requeridas neste Termo de Referência estarão habilitadas simultaneamente;

3.2.23. A emissão do Termo de Recebimento Definitivo está vinculada à homologação, entrega da Documentação Técnica - DT e a realização da Transferência de conhecimento, conforme mencionado neste Termo de Referência;

3.2.24. As etapas de implantação e PFE deverão ser contíguas, não havendo interstícios entre elas.

3.3. REUNIÃO DE ALINHAMENTO DE EXPECTATIVAS

3.3.1. Deverá ser realizada uma reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da infraestrutura de TI da CONTRATANTE;

3.3.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato, o Fiscal Técnico do Contrato, o Preposto e membro da equipe técnica da CONTRATADA;

3.3.3. A reunião realizar-se-á na CONTRATANTE em até 5 dias úteis após a assinatura do contrato;

3.3.4. Na reunião de Alinhamento de Expectativas a CONTRATADA deverá apresentar:

3.3.4.1. Sugestão de conjunto de políticas, regras e filtros a serem configurados nos serviços da solução de segurança de perímetro;

3.3.4.2. Sugestão de graus de classificação de severidade de incidentes e as respectivas medidas que sugere serem adotadas em resposta aos alertas emitidos pelos serviços administrados;

3.3.4.3. As sugestões deverão ser apresentadas para discussão durante a reunião e as configurações definitivas devem ser apresentadas no Plano de Implantação;

3.3.5. Durante a implantação, o conjunto de políticas, regras e filtros de que trata o item anterior poderão ser alterados conforme a necessidade da CONTRATANTE.

4. DO SERVIÇO DE TRANSFERÊNCIA DE CONHECIMENTO

4. DESCRIÇÃO

4.1.1. Para todo o produto adquirido no escopo do ITEM 1 deverá ser fornecida uma transferência de conhecimento.

4.1.2. A transferência de conhecimento deverá ser ministrada por profissional certificado pelo fabricante.

4.1.3. A CONTRATADA deverá apresentar um Plano de Transferência de Conhecimento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

4.1.4. O Plano citado no item anterior deverá apresentar o programa de cada transferência de conhecimento com conteúdo, carga horária, duração em dias e avaliações de aprendizagem;

4.1.5. A transferência de conhecimento pode ser pela manhã, manhã e tarde, ou de noite, a critério da CONTRATANTE;

4.1.6. A transferência de conhecimento deverá ser em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração e utilização delas;

4.1.7. A transferência de conhecimento deverá prever a capacitação para 6 alunos divididos em 2 turmas;

4.1.8. Para que uma transferência de conhecimento seja considerada efetiva deverá ser considerada satisfatória por pelo menos 70% dos treinandos;

4.1.9. A CONTRATANTE poderá avaliar as transferências de conhecimentos com meios próprios e, caso este seja julgado deficiente, a CONTRATADA deverá prover o devido reforço;

4.1.10. A CONTRATADA deverá prover toda a estrutura para as transferências de conhecimentos;

4.1.11. A transferência de conhecimento será realizada na modalidade de ensino a distância (EAD);

4.1.11.1. Em casos excepcionais a serem julgados pela CONTRATADA a transferência de conhecimento poderá ser realizada presencialmente em Brasília.

4.1.12. Todo material didático disponibilizado na transferência de conhecimento deverá ser fornecido pela CONTRATADA e estarão inclusos no escopo da transferência de conhecimento;

4.1.13. Ao final de cada transferência de conhecimento, cada treinando deverá receber um certificado de participação;

4.1.14. No certificado de participação de que trata o item anterior deverá constar todas as informações exigidas pela Secretaria de gestão de pessoas do MPDFT para que ele seja homologado. Minimamente, mas não limitado a: nome completo do aluno, data de execução da transferência de conhecimento, carga horária e ementa do curso;

4.1.15. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades da transferência de conhecimento;

4.1.16. A fim de que os técnicos da CONTRATANTE possam avaliar com precisão a solução durante o Período de Funcionamento Experimental (PFE), ao menos uma turma da transferência de conhecimento deve ser finalizada antes do início deste.

5. DA GARANTIA DO FABRICANTE E ATUALIZAÇÕES DE VERSÃO

5. GARANTIA DO FABRICANTE

5.1.1. A solução deverá ter garantia do fabricante para os equipamentos, produtos e seus componentes, sem quaisquer ônus para a CONTRATANTE, a contar da data de emissão do Termo de Recebimento Definitivo, estendendo-se por todo o período de vigência do contrato.

5.1.2. A CONTRATADA deverá entregar documentação comprobatória da contratação da Garantia junto ao fabricante da solução ofertada;

5.1.2.1. A contratação da garantia técnica junto ao fabricante não exime a CONTRATADA das responsabilidades contratuais;

5.1.3. A CONTRATADA é a única responsável pelos produtos fornecidos à CONTRATANTE, mesmo que tenham sido adquiridos de terceiros;

5.1.4. A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA;

5.1.5. Caso sejam detectadas falhas ou bugs nos produtos, a empresa CONTRATADA deverá realizar as atualizações necessárias à correção do problema;

5.2. ATUALIZAÇÕES

5.2.1. No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para a CONTRATANTE;

5.2.2. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

5.2.2.1. Patches, fixes, correções, updates e service packs;

5.2.2.2. Novas releases, builds e funcionalidades;

5.2.2.3. O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito;

5.2.2.4. O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do Contrato.

5.2.3. No caso de descontinuidade do produto, o mesmo deverá ser substituído pelo seu sucedâneo.

5.2.4. A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

5.2.5. A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa da CONTRATANTE;

5.2.6. Qualquer ação para atualização deve ser realizada com anuência da CONTRATANTE.

ANEXO II – Modelo de Proposta de Preços

Tabela – Modelo de Proposta de Preços

ITEM	DESCRIÇÃO	QUANTIDADE / UNIDADE	VALOR MENSAL (R$)	VALOR TOTAL (R$)
1	serviço de segurança de perímetro	36 / meses	R$	R$
VALOR TOTAL DA CONTRATAÇÃO				**R$**

_____(nome e assinatura)_____

Nome completo, telefone e e-mail

ANEXO III – Modelo de Comprovação Ponto a Ponto

Tabela – comprovação de atendimento ponto a ponto

Código do item da especificação técnica do Termo de referência	**Especificação Técnica**	**Referência na documentação oficial**	**Transcrição**
1.x.x	Os equipamentos devem ser do tipo Appliance, ou seja, hardware e software integrados. Não serão aceitas soluções compostas por hardwares genéricos;	Datasheet pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.x.x	A solução será implementada em modo cluster de alta disponibilidade com uso de 2 equipamentos e capaz de suportar um throughput de 2 Gbps, com todas as funcionalidades habilitadas;	Instalation Guide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
...	...	...	...
1.x.x	IPSec VPN Site-to-Site e Client-To-Site;	Product guide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
...	...	...	...

_____(nome e assinatura)_____

Nome completo, telefone e e-mail