Especificação Técnica: NIPS Corporativo

1. Objeto

1.1. Consulta pública para aquisição da Solução de NIPS (Network Intrusion Prevention System) de uso Corporativo na forma de Appliance físico e gerência;

2. Especificação do Objeto a ser Contratado

2.1. Arquitetura de Hardware:

2.1.1. A solução do NIPS, deve ser do tipo Appliance físico dedicado;

2.1.2. Tanto o Hardware quanto o Software da Solução devem ter arquitetura específica, desenvolvida para a finalidade de Next Generation Intrusion Prevention System (NGIPS);

2.1.3. Não serão aceitas solução em OEM, com software de um fabricante e hardware de outro fabricante ou solução de uso geral, tais como: Chassi servidor (Server Chassis), Estação de Trabalho (Desktop) e Equipamento Blade;

2.1.4. Os equipamentos que compõem a solução deve possuir garantia de “fim de linha” (End-of-Life) superior a 5 (cinco) anos, a contar do aceite da solução;

2.1.4.1. Caso o fabricante publique o anúncio de End-of-Life da solução antes do aceite, o fornecedor deve entregar o modelo equivalente ou superior da solução de NIPS que entrou em fim de linha;

2.1.4.2. Caso o fabricante publique o anúncio de End-of-Life da solução após o aceite, o fim de linha não deve ter fim de suporte (End-Of-Support) até o final do contrato em vigor;

2.2. Detecção de Ataques:

2.2.1. O fabricante da solução de NIPS deve possuir avaliação pela NSS Labs, a partir de 2013, independentemente da solução avaliada;

2.2.2. Deve confirmar uma taxa de bloqueio de ataques (efetividade de segurança) superior à 95% (noventa e cinco por cento);

2.2.3. Deve confirmar imunidade à tentativas de evasão;

2.2.4. Suportar análise e decodificação de protocolos de rede, entre a camada 2 (Layer-2) e camada 7 (Layer-7) do modelo OSI (Open System Interconnection), para no mínimo 170 (centro e setenta) protocolos, entre eles: ARP, BOOTP, DCCP, DHCP, DNS, EIGRP, FINGER, FTP, HTTP, HTTPS, ICMP (versão 4 e versão 6), IMAP, IP (versão 4 e versão 6), LDAP, NetBIOS, NFS, POP3, RADIUS, SMTP, SNMP, SSH, RPC, TCP, TELNET, TFTP e UDP;

2.2.5. Deve suportar identificação de ataques para protocolos de rede independente das portas de comunicação utilizadas, para no mínimo: DNS, FTP, HTTP, IMAP, POP3, SMTP, SNMP e RPC;

2.2.6. Deve suportar tanto análise Stateful Inspection, mantendo-se o estado das sessões monitoradas, quanto Stateless Inspection;

2.2.7. Deve suportar análise de tráfego na direção servidor-cliente, isto é, ataques originados externamente e direcionados à clientes ou usuários internos (Client-side Attacks ou Drive-by Attacks);

2.2.8. Deve suportar detecção e bloqueio de ataques direcionados a servidores de aplicação Web (Web Application), através de tecnologia heurística, isto é, detecção

heurística e bloqueio de ataques SQL Injection;

2.2.9. Deve suportar obtenção de informações detalhadas sobre ataques, para no mínimo: reputação de arquivo, reputação de endereço IP, reputação de aplicação e protocolo, e localização geográfica;

2.2.10. Deve suportar mecanismo de criação de perfis de dispositivos, permitindo a descoberta de sistemas operacionais (OS fingerprinting) destes dispositivos através da análise do tráfego de forma passiva;

2.2.11. Deve suportar algoritmo de pontuação para relevância de um ataque, conforme padrão de mercado e definido por entidade independente (Common Platform Enumeration), permitindo distinguir quando um ataque for bem-sucedido e quando um ataque falhar;

2.2.12. Deve suportar análise do nível de relevância de um ataque, permitindo uma demonstração de faixas de relevância para no mínimo 5 (cinco) níveis;

2.2.13. Deve suportar criação de políticas de Firewall para controle de aplicativos, possuindo no mínimo 1.000 (mil) identificações de aplicativos e protocolos (App. ID), permitindo criação de regras de acesso para aplicativos comuns, tais como: Facebook, Yahoo! Instant Messenger e Gmail;

2.2.14. Deve suportar categorias de ataques e tipos de ameaças, conforme padrões de mercado e definidos por entidades independentes (Common Weakness Enumeration e Common Attack Pattern Enumeration and Classification), para no mínimo: CAPEC-10, CAPEC-100, CAPEC-112, CAPEC-119, CAPEC-123, CAPEC-14, CAPEC-16, CAPEC-49, CWE-119, CWE-120, CWE-121, CWE-122, CWE-129, CWE-131, CWE-20, CWE-200, CWE-205, CWE-227, CWE-264, CWE-307, CWE-400, CWE-436, CWE-506, CWE-507, CWE-509, CWE-512, CWE-514, CWE-553, CWE-680, CWE-770, CWE-78, CWE-805, CWE-806, CWE-88, CWE-89 e CWE-94;

2.2.15. Deve suportar administração, configuração e manutenção no mínimo para:

2.2.15.1. Perfis de DoS (Denial of Service – Negação de Serviço);

2.2.15.2. Regras de ACL (Access Control List – Lista de Controle de Acesso);

2.2.15.3. Virtual IPS (Intrusion Prevention System – Sistema de Prevenção de Intrusão) por meio de sub-interfaces. IPS virtuais podem ser configurados por VLAN (IEEE 802.1Q) e CIDR (Classless Inter-Domain Routing);

2.2.16. Deve suportar detecção e bloqueio de ataques do tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS) de forma nativa, para no mínimo:

2.2.16.1. Detecção e bloqueio efetivo baseado em assinaturas de ataques às vulnerabilidades DoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1996-26, CA-1997-28, CA-1998-13, CVE-1999-0015, CVE-1999-0016, CVE-1999-0128, CVE-1999-0153, CVE-1999-0258, CVE-1999-0345, CVE-1999-0969, CVE-2000-0305, CVE-2004-0230, CVE-2004-0790, CVE-2005-0688 e CVE-2005-0048;

2.2.16.2. Detecção e bloqueio efetivo baseado em assinaturas de atividades de agentes (zumbis) DDoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1999-17, CA-2000-01, CVE-2000-0138, IN-99-07, IN-2000-01 e IN-2000-05;

2.2.16.3. Detecção e bloqueio baseado em modo aprendizagem (Learning Mode), através de anomalias estatísticas (Statistical Anomalies) e desequilíbrio de volume de tráfego, que permite utilização de perfil de tráfego U+0064e, para Flood (Volume) DoS Attacks,

conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures), para no mínimo: CA-1996-21, CA-1996-01, CA-1998-01 e CVE-2002-1712;

2.2.17. Detecção e bloqueio de ataque SYN, que permita limitar e controlar a quantidade de requisições de conexões;

2.2.18. Detecção e bloqueio baseados em políticas de Firewall, para no mínimo:

2.2.18.1. Filtros de origem e destino por: país, nome (DNS), endereço IP, porta, bloco de endereços, rede ou grupo de redes;

2.2.18.2. VlanID, para no mínimo 4094 Vlans;

2.2.18.3. Filtros de aplicação: aplicação, grupo de aplicações, porta de comunicação customizada, serviço ou grupo de serviços;

2.2.18.4. Filtro de resposta: bloqueio (drop), negação (deny), quarentena e ignorar;

2.2.18.5. Detecção e bloqueio baseados em limite de conexões, que permite definição de valores threshold para limitar o número de conexões que podem ser estabelecidas de, e para, uma máquina e URI específicas;

2.2.18.6. Detecção e bloqueio baseados em proteção de servidores DNS (Domain Name Service) e contra ataques com ou sem a presença de endereços IP forjados (IP Spoofing);

2.2.18.7. Deve permitir utilizar apenas do protocolo TCP para resolução de nomes (name lookup/resolve) e portanto não deve ser utilizado o protocolo UDP para esta finalidade;

2.2.19. Suportar detecção e bloqueio de tráfego de aplicações Instant Messenger e P2P (Peer-to-Peer), para no mínimo: AOL Instant Messenger, Ares, Azureus, Bearshare, Bittorrent, Blubster, DirectConnect, eDonkey, eMule, Enppy, ICQ, FileNara, Gnucleus, Gnutella, Grokster, Groove, JAP Anonymizer, Kazaa, Limewire, Morpheus, MSN Messenger, Mutella, MyNapster, Mxie, OpenLITO, Overnet, Phex, Piolet, RockItNet, Shareaza, Skype, SoulSeek, Swapper, Xolox, WinMX, Yahoo! Messenger, Dropbox e Proxies Anônimos (como TOR e Ultrasurf);

2.2.20. Deve suportar detecção e bloqueio de ataques através de túneis para no mínimo: IPv4-in-IPv4, IPv4-in-IPv6 e IPv6-in-IPv6;

2.2.21. Deve suportar detecção e bloqueio de ataques através de segmentos encapsulados, para no mínimo: ECLB (EtherChannel Load Balancing), GRE (Generic Routing Encapsulation), Jumbo Frames, MPLS (Multi Protocol Label Switching), Stacked VLAN, SSL (Secure Sockets Layer) e VLAN (IEEE 802.1Q);

2.2.22. Deve ser transparente para os protocolos de roteamento e redundância de rota no mínimo: OSPF, BGP, VRRP, IS-IS e HSRP;

2.2.22.1. Não deve interromper ou alterar segmentos monitorados com protocolos de roteamento e redundância de rotas, mesmo que trafegados dentro do protocolo LACP (Link Aggregation Control Protocol);

2.2.23. Deve permitir a criação de novas assinaturas e alteração de parâmetros das assinaturas existentes;

2.2.24. Deve suportar administração, configuração e manutenção de ACL em camada 3, com as seguintes respostas:

2.2.24.1. Permitir: O tráfego é enviado Inline sem inspeção completa dos pacotes;

2.2.24.2. Permitir e Prevenir Ataques: O tráfego é enviado Inline para inspeção completa dos pacotes;

2.2.24.3. Descartar: O tráfego será descartado;

2.2.24.4. Suportar detecção e bloqueio de ataques, no mínimo, das seguintes modalidades:

2.2.24.4.1. Inspeção de tráfego Stateful: IP defragmentation e TCP stream reassembly;

2.2.24.4.2. Anomalias;

2.2.24.4.3. Por assinaturas: Definidas pelo fabricante, Definidas pelo usuário e Open-source;

2.2.24.4.4. Por protocolos de camada 7 do modelo OSI;

2.2.24.5. Suportar detecção e bloqueio de ataques, independente do sistema operacional alvo;

2.2.25. Suportar detecção heurística e consulta de reputação de atividades de agentes (zumbis) internos que pertençam a Botnet;

2.2.26. Suportar administração, configuração e manutenção de controle de limites de conexões (Connection Limiting) para no mínimo:

2.2.26.1. Direção: Inbound, Outbound e Bidirecional;

2.2.26.2. Tipo de Regra: Baseada em Protocolo, Porta, URL, URI e Aplicação;

2.2.27. Suportar administração, configuração e manutenção de bloqueio do trafego definido, para no mínimo:

2.2.27.1. Direção: Inbound, Outbound e Bidirecional;

2.2.27.2. Tipo de Regra: Baseada em Protocolo, Porta, URL, URI e Aplicação;

2.2.28. Suportar as categorias de ataques e tipos de ameaças para no mínimo:

2.2.28.1. Reconnaissance: Brute Force, Host Sweep, OS Fingerprinting, Port Scan e Service Sweep;

2.2.28.2. Exploits: Arbitrary Command Execution, Backdoor, Bot, Buffer Overflow, Denial of Service, DDoS Agent Activity, Code/Script Execution, Evasion Atempt, Privileged Access, Probe, Protocol Violation, Remote Access, Shellcode Execution, Trojan, Virus, Read Exposure, Worms e Write Exposure;

2.2.28.3. Volume DoS: Statistical Deviation e Over Threshold;

2.2.28.4. Policy Violations: Audit, Command Shell, Covert Channel, Non-standard Port, Phising, PuP (Potential Unwanted Program), Restricted Access, Restricted Application, Sensitive Content e Unauthorized IP;

2.2.29. Suportar assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS e DDoS (Denial of Service e Distributed Denial of Service), para no mínimo: Bonk Attack, Jolt Attack, Land Attack, Ping of Death Attack, Newtear Attack e Teardrop Attack, Amplification Attack, Slow Read Attack;

2.2.30. Suportar assinaturas para detecção e bloqueio de atividades de agentes (zumbis) DDoS (Distributed Denial of Service), para no mínimo: Trinoo, Tribal Flood Network (TFN), TFN2K, Stacheldraht, Shaft, Trinity e Mstream;

2.2.31. Suportar detecção e bloqueio baseado em modo aprendizagem (Learning Mode), através de anomalias estatísticas (Statistical Anomalies) e desequilíbrio do tráfego, para Flood (Volume) DoS Attacks, para no mínimo: TCP SYN, TCP Full Connect, TCP ACK/FIN, TCP RST, DNS Flood, UDP Flood e ICMP Flood;

2.2.32. Suportar aplicação, extensão e remoção de quarentena (IPS Quarantine) sob demanda por períodos programáveis e por remoção explícita;

2.2.33. Suportar ajuste de bloqueio inteligente, baseado em assinaturas recomendadas pelo fabricante para bloqueio;

2.2.34. Todos os bloqueios de pacotes e de conexões precisam obrigatoriamente serem registrados no Banco de Dados e serem apresentados e mostrados na console de gerência do equipamento, independente do motivo do bloqueio;

2.2.35. Suportar detecção e bloqueio para conexões P2P (Peer-to-Peer) evasivas que utilizem transferências de arquivos criptografadas ou com técnicas de “Obfuscated Binary”;

2.3. Detecção de Ameaças (malwares) Avançadas:

2.3.1. Suportar tecnologias de detecção e bloqueio de códigos maliciosos, ameaças malwares e malwares avançados em tempo real, para no mínimo:

2.3.1.1. Mecanismo de lista local de arquivos confiáveis (lista branca), os quais não precisarão ser analisados por serem notoriamente confiáveis;

2.3.1.2. Mecanismo de lista com valores Hash de arquivos que sejam códigos maliciosos e ameaças (malwares) conhecidas e armazenado em uma base de dados local (lista negra);

2.3.1.3. Mecanismo de detecção de códigos maliciosos e ameaças (malwares), que deve operar em tempo real e permitindo o uso de reputação de arquivos;

2.3.1.4. Mecanismo de detecção de códigos malicioso e ameaças (malwares) em ,no mínimo, os seguintes tipos de arquivos:

2.3.1.4.1. Capacidade de análise de arquivos PDF, mesmo quando criptografados;

2.3.1.4.2. Objetos e arquivos Flash, arquivos Executáveis e arquivos Microsoft Office;

2.3.2. Suportar tecnologia de detecção e bloqueio de códigos maliciosos e ameaças (malwares) baseada em mecanismo de análise que inclua técnicas Machine Learning, Assinatura e reputação de arquivos em tempo real;

2.4. Respostas à Ataques:

2.4.1. Suportar TCP Reset;

2.4.2. Suportar bloqueio (Drop) de pacotes;

2.4.3. Suportar aplicação, extensão e remoção de quarentena (IPS Quarantine) sob demanda;

2.4.4. Suportar configuração e atualização global de bloqueio para um ataque, propagando esta configuração e atualização em todas as políticas;

2.4.5. Suportar administração, configuração e manutenção de controle de limites de conexões (Connection Limiting) e bloqueio do trafego definido, para no mínimo:

2.4.5.1. Direção: Inbound, Outbound e Bidirecional;

2.4.5.2. Tipo de Regra: Baseada em Protocolo, Porta, URL, URI, Aplicação e ataque, propagando esta configuração e atualização em todas as políticas;

2.4.6. Suportar captura de pacotes para análise de evidências em formato LIBPCAP (Library for Packet Capture);

2.4.7. Suportar envio de SNMP Trap para SNMPv2c e SNMPv3;

2.4.8. Suportar envio de e-mail;

2.5. Descriptografia de tráfego SSL:

2.5.1. Análise de conexões seguras de SSL (Secure Sockets Layer) e TLS (Transport Layer Security), no mínimo para: SSL versão 2, SSL versão 3, TLS versão 0.9, TLS versão 1.0, TLS versão 1.1 e TLS versão 1.2;

2.5.2. Análise de tráfego de todo tipo de tráfego TLS (Transport Layer Security) e SSL (Secure Sockets Layer), protocolos da camada de Transport (OSI) e da camada de Aplicação (OSI) que estabeleçam conexões seguras com criptografia TLS (Transport Layer Security) e SSL (Secure Sockets Layer) em servidores WEB, IMAPS, SMTPS, POP3S utilizando certificados PKCS12 (extensões “.pkcs12” e “.pfx”), nas versões SSLv2, SSLv3 e TLS e com codificações RC4, 3DES e AES;

2.5.3. Suportar a importação no mínimo de 1000 (mil) certificados em formato PKCS #12 (extensões ".pkcs12", ".p12" e ".pfx") e em formato PEM, com chave(s) privada(s) RSA de 1024-bit e 2048-bit;

2.5.4. Suportar algoritmos de chaves simétricas, no mínimo para: RC4 (Rivest Cipher 4), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) e AES (Advanced Encryption Standard);

2.5.5. Suportar funções de hashing, no mínimo para: MD5 (Message-Digest Algorithm 5) e SHA-1 (Secure Hash Algorithm 1);

2.5.6. A decriptografia de tráfego SSL deve ser executada em equipamento externo ou interno na solução de NIPS;

2.5.7. Possuir interface dedicada para conexão a console;

2.5.8. A descriptografia do protocolo SSL/TLS quando realizada através de equipamento externo deverá entregar o resultado para a solução de NIPS fornecida;

2.5.8.1. O equipamento de SSL/TLS não deve realizar qualquer tipo de análise;

2.5.9. Suportar configuração em modo proxy transparente;

2.5.10. Suportar no mínimo os seguintes tamanhos de Chaves RSA:

2.5.10.1. 2048 bits;

2.5.10.2. 4096 bits;

2.5.10.3. 8172 bits;

2.5.11. Deve permitir importar certificados de servidores WEB de tal forma a possibilitar a decriptação dos dados direcionados a um determinado Common Name (ex.: www.serpro.gov.br). Uma vez instalado o certificado, o equipamento de descriptogarfia SSL deve descriptografar os pacotes SSL e encaminhar o tráfego para inspeção de um sensor IPS;

2.6. Interfaces de Inspeção:

2.6.1. As interfaces podem ser fixas ou fornecidas com os respectivos transmissores-receptores, os quais devem ser consideradas no momento da elaboração da proposta;

2.6.2. As interfaces com fornecimento dos respectivos transmissores-receptores devem ser do tipo substituível (hot-swap), permitindo instalação, substituição e funcionamento (inspeção de tráfego), sem a necessidade de remoção ou reinicialização da solução de NIPS e também de seu sistema;

2.6.3. As interfaces devem possuir, individualmente, indicadores luminosos (LED) sobre seus estados e atividades;

2.6.4. As interfaces devem permitir, individualmente, configuração de seu estado tanto para ativas quanto para inativas;

2.6.5. As interfaces devem permitir, individualmente, configuração em caso de falhas do equipamento (hardware ou software) ou ausência de energia; conforme abaixo:

2.6.5.1. Disponibilidade (Fail-Open) dos segmentos monitorados, através de dispositivo interno ou externo de Bypass;

2.6.5.2. Indisponibilidade (Fail-Close) dos segmentos monitorados;

2.6.6. Todas as interfaces de proteção devem possuir a funcionalidade de Bypass, exceto para a interface de gerência;

2.6.7. Deve desativar automaticamente uma interface, caso detecte a queda de link na outra interface do mesmo segmento de rede;

2.6.8. Deve suportar configuração flexível de pass-through em camada 2 para tráfego que ultrapasse a análise de tráfego agregado suportado pela solução de NIPS;

2.7. Desempenho e Escalabilidade:

2.7.1. Pode inserir latência de no máximo 150 µs (cento e cinquenta microssegundos) para tráfego não criptografado nos segmentos de rede monitorados, com exceção nos casos onde houver necessidade de consulta externa, tais como consulta DNS;

2.7.2. Para o tráfego criptografado (SSL e HTTPS) a latência deve ser no máximo de 5 ms (cinco milissegundos);

2.7.3. Deve monitorar e proteger os segmentos de rede monitorados em modo transparente, assim como operar na camada 2 (Layer-2) do modelo OSI (Open System Interconnection), isto é, as interfaces de monitoração não devem requerer endereços IP e endereços MAC;

2.7.4. Deve suportar, de forma homogênea e heterogênea, os seguintes modos de operação:

2.7.4.1. Prevenção (inline) – monitoração e proteção de segmentos de rede em ambas as direções, permitindo monitorar e responder à ataques em tempo real, mantendo-se o estado das conexões (Stateful);

2.7.4.2. Bloqueio Simulado (inline) – monitoração e simulação de proteção de segmentos de rede em ambas as direções, permitindo monitorar e alertar os ataques em tempo real, reportando quais ataques seriam bloqueados, mantendo-se o estado das conexões (Stateful);

2.7.4.3. Monitoração (SPAN) – monitoração de segmentos de rede, permitindo monitorar e alertar os ataques em tempo real;

2.7.5. Deve suportar captura de todos os pacotes para finalidade de troubleshooting em formato LIBPCAP (Library for Packet Capture), podendo ser através de ferramenta específica (ex.: TCPDUMP) ou através de interface gráfica que permita regras de captura, sem afetar a disponibilidade e desempenho dos segmentos de rede;

2.7.6. Deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando no modo de operação inline;

2.8. Itens De Capacidade:

2.8.1. Para Regional SERPRO de Brasília, a solução de NIPS deve:

2.8.1.1. Suportar tráfego total (throughput) de 60 Gbps (sessenta gigabits por segundo) e um total de análise e inspeção de tráfego de 30 Gbps (trinta gigabits por segundo), sendo que deste tráfego de análise e inspeção 4 Gbps (quatro gigabits por segundo) devem ser analisados com SSL, utilizando chaves de 2048 bits (26 Gbps de inspeção de tráfego em claro + 4 Gbps de inspeção SSL). Ambos os tráfegos (total e de inspeção)

devem ser medidos em padrão IMIX (Internet Mix);

2.8.1.2. Suportar uma taxa de no mínimo 23.000.000 (vinte e três milhões) de conexões concorrentes e taxa de no mínimo 700.000 (setecentas mil)para novas conexões TCP por segundo;

2.8.1.3. Ser composta no mínimo de 32 interfaces 10gbps (fibra), com fail-open interno ou externo;

2.8.1.4. Ser entregue com 2 ou 3 equipamentos, totalizando o throughput, interfaces e métricas acima especificados;

2.8.2. Para Regional SERPRO de São Paulo, solução de NIPS deve:

2.8.2.1. Suportar tráfego total (throughput) de 40 Gbps (quarenta gigabits por segundo) e um total de análise e inspeção de tráfego de 20 Gbps (vinte gigabits por segundo), sendo que deste tráfego de análise e inspeção 2 Gbps (dois gigabits por segundo) devem ser analisados com SSL, utilizando chaves de 2048 bits (18 Gbps de inspeção de tráfego em claro + 2 Gbps de inspeção SSL). Ambos os tráfegos (total e de inspeção) precisam ser medidos em padrão IMIX (Internet MIX);

2.8.2.2. Suportar uma taxa de no mínimo 15.000.000 (quinze milhões) de conexões concorrentes e taxa de no mínimo 400.000 (quatrocentos mil) para novas conexões TCP por segundo;

2.8.2.3. Ser composta no mínimo de 28 (vinte e oito) interfaces 10 Gbps (dez gigabits por segundo) em fibra, com fail-open interno ou externo;

2.8.2.4. Ser entregue com 2 ou 3 equipamentos, totalizando o throughput, interfaces e métricas acima especificados;

2.8.3. Para Regional SERPRO de Rio de Janeiro, a solução de NIPS deve:

2.8.3.1. Suportar tráfego total (throughput) de 10 Gbps (dez gigabits por segundo) e um total de análise e inspeção de tráfego de 5 Gbps (cinco gigabits por segundo), sendo que deste tráfego de análise e inspeção 1 Gbps (um gigabits por segundo) deverão ser analisados com SSL (4 Gbps de inspeção de tráfego em claro + 1 Gbps de inspeção SSL). Ambos os tráfegos (total e de inspeção) precisam ser medidos em padrão IMIX (Internet MIX);

2.8.3.2. Suportar uma taxa de no mínimo 7.000.000 (sete milhões) de conexões concorrentes e taxa de no mínimo 200.000 (duzentas mil) para novas conexões TCP por segundo;

2.8.3.3. Ser composta no mínimo de 16 interfaces 10 Gbps (dez gigabits por segundo) em fibra, com fail-open interno ou externo;

2.8.3.4. Ser entregue com 2 equipamentos, totalizando o throughput, interfaces e métricas acima especificados;

2.8.4. Para a inspeção SSL serão aceitos equipamentos externos;

2.8.4.1. Caso o fornecedor opte pela utilização de equipamento externo para realizar a função de inspeção SSL, o equipamento deve suportar a inspeção da mesma quantidade de segmentos do appliance de NIPS definido para cada localidade;

2.9. Demais Características do Hardware da Solução:

2.9.1. A solução deve suportar a montagem em rack (bastidor) de 19 polegadas, com utilização de até 4-RU (Quatro unidades de bastidor) de altura;

2.9.1.1. Devem ser fornecidos todos os acessórios necessários para sua montagem;

2.9.2. Deve suportar no mínimo 2 (duas) fontes de energia internas, para Corrente

Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V a 240V (50 e 60Hz), conforme informado abaixo:

2.9.2.1. As fontes de energia devem permitir utilização de circuitos elétricos distintos;

2.9.2.2. As fontes de energia devem ser do tipo substituível (hot-swap), permitindo instalação e/ou substituição sem a necessidade de remoção do equipamento;

2.9.2.3. As fontes de energia devem ser suficientes para manter todas as operações da solução, mesmo no caso de falha de uma das fontes de energia, independentemente da quantidade de interfaces em uso ou funcionalidades habilitadas;

2.9.2.4. As fontes de energia devem vir acompanhadas com cabos de energia com no mínimo 1,80 m (hum metro e oitenta centímetros) de comprimento;

2.9.3. Deve suportar umidade relativa e temperatura ambiente, sem condensação;

2.9.3.1. Em operação: 10% à 85% de umidade com 10°C à 35°C de temperatura;

2.9.4. Deve possuir unidades de ventilação redundantes, pode ser do tipo substituível (hot-swap), permitindo que fluxo de ar (exaustão) ocorra em direção a parte traseira do Rack;

2.9.5. Deve possuir as interfaces de monitoração localizadas na parte frontal;

2.9.6. Deve possuir interface serial RS-232 ou interface USB ou interface RJ45 exclusiva e dedicada para acesso à console do equipamento, sendo necessário o fornecimento do respectivo cabo compatível;

2.9.7. Deve permitir acesso remoto, através de SSH, à console do equipamento;

2.9.8. Deve possuir no mínimo 1 (uma) interface 1 GigE (Gigabit Ethernet), para cabeamento de cobre (100Base-TX ou 1000Base-T) exclusiva e dedicada para gerência, onde a interface pode ser fixa ou ser fornecida com o respectivo transmissor-receptor;

2.9.9. Deve ser fornecida com todos os respectivos cabeamentos, transmissores-receptores e conectores necessários para operação das interfaces de monitoração;

2.9.9.1. Os Módulos de interfaces que necessitem de seus respectivos transmissores-receptores devem ser fornecidos integralmente, isto é, caso os módulos de interfaces do equipamento excedam as quantidades mínimas requeridas, ainda assim devem ser fornecidos os seus respectivos transmissores-receptores;

2.9.9.2. Para interface 1000BASE-T deve ser adotado cabeamento CAT6A e para interface 10GBASE-SR deve ser adotado cabeamento composto por fibras multi-modo OM3 de diâmetro 50µm/125µm;

2.9.10. O funcionamento do bypass (fail-open) não deve afetar o tráfego de rede em caso de falha das interfaces;

2.9.11. O funcionamento do bypass (fail-open) não deve afetar o tráfego de rede em caso de falha do equipamento;

2.9.11.1. Os cabos devem ser fornecidos já conectorizados e testados;

2.9.12. Deve possuir configurações de CPU e memória (RAM e Flash) suficientes para a implementação de todas as funcionalidades descritas nestes requisitos técnicos;

2.9.13. Deve possuir armazenamento do tipo SSD (Solid State Disk):

2.9.13.1. Não será permitido utilização de armazenamento do tipo HDD (Hard Disk Drive);

2.10. Gerenciamento da Solução:

2.10.1. Permitir gerenciamento centralizado da solução de NIPS;

2.10.2. Deve ser fornecido, tanto o software quanto hardware, para a funcionalidade única e exclusiva de gerenciamento da solução de NIPS;

2.10.3. Suportar no mínimo 2 (duas) fontes de energia internas para Corrente Alternada (AC - Alternating Current), com chaveamento automático e capacidade de operação em 100V a 240V (em 50 e 60Hz);

2.10.4. Possuir capacidade de armazenamento redundante (RAID – Redundant Array of Independent Drives), atendendo aos requerimentos do item 2.10.17;

2.10.5. Possuir no mínimo 1 (uma) interface 1GigE (Gigabit Ethernet), para cabeamentos Cobre (100Base-TX ou 1000Base-T), onde a interface pode ser fixa ou ser fornecida com o respectivo transmissor-receptor;

2.10.6. A solução de gerência deve considerar a instalação em alta disponibilidade no modo ativo/passivo, onde:

2.10.6.1. Uma das gerências deve ser primária (ativa);

2.10.6.2. Uma das gerências deve ser secundária (passiva);

2.10.6.3. Em caso de falha da gerência primária (ativa), automaticamente a secundária (passiva) deve assumir o gerenciamento centralizado da solução de NIPS;

2.10.6.4. As configurações devem ser sincronizadas em tempo real entre a gerência primária (ativa) e a gerência secundário (passiva);

2.10.7. Possuir políticas baseadas em assinaturas recomendadas pelo fabricante para bloqueio, as quais são baseadas nas recomendações provenientes de equipe de pesquisa do fabricante;

2.10.8. Suportar atualização de software e firmware da solução de NIPS, de forma remota e centralizada, conforme abaixo:

2.10.8.1. Online: automática e manual de conteúdo de segurança e produto através da Internet, podendo ser realizada sem interferência do usuário;

2.10.8.2. Offline: automática e manual de conteúdo de segurança e produto através de pacotes de atualização importados pela gerência, sem conexão com a Internet;

2.10.9. Suportar aplicação de políticas, regras, de forma remota e centralizada, sem afetar a detecção e bloqueio;

2.10.10. Suportar comunicação criptografada com a solução de NIPS;

2.10.11. Permitir envio de registros de eventos através de integração com servidor SYSLOGD;

2.10.12. A solução de gerência deve suportar integração, através de SNMPv2c e SNMPv3;

2.10.12.1. Deve fornecer os respectivos arquivos de MIBs;

2.10.13. Permitir sincronismo de horário da solução através de integração com servidor NTP (Network Time Protocol);

2.10.14. Suportar operação e armazenamento com Sistema Gerenciador de Banco de Dados Relacional (SGBDR – Relational Database Management System ou RDBMS) que utilize linguagem de pesquisa declarativa SQL (Structured Query Language);

2.10.15. Suportar arquivamento (backup) dos eventos gerados pela solução de NIPS, conforme abaixo:

2.10.15.1. Manual: arquivamento (backup) dos eventos sob demanda;

2.10.15.2. Automático: arquivamento (backup) dos eventos de forma agendada e automática;

2.10.16. Permitir tarefas tanto de arquivamento (backup) quanto de restauração (restore) de sua base de dados;

2.10.17. A solução de gerência deve ser capaz de armazenar 30.000.000 (trinta milhões) de eventos em Sistema Gerenciador de Banco de Dados Relacional (SGBDR – Relational Database Management System ou RDBMS);

2.10.17.1. Permitir uma retenção de eventos no mínimo de 6 (seis) meses;

2.10.18. Suportar administração, configuração e manutenção de contas de acesso de usuários e administradores através de autenticação via:

2.10.18.1. LOCAL: usuários e administradores cadastrados na gerência, permitindo definir políticas de composição de senhas;

2.10.18.2. LDAP: usuários e administradores importados;

2.10.18.3. Windows AD (Active Directory);

2.10.18.4. RADIUS: usuários e administradores importados e integrados com servidor RADIUS;

2.10.19. A solução de gerência deve suportar atribuição de perfis para usuário e administradores, para no mínimo:

2.10.19.1. Administrador;

2.10.19.2. Superusuário;

2.10.19.3. Perfil nulo;

2.10.20. Permitir monitoração dos recursos alocados na solução NIPS, no mínimo para:

2.10.20.1. Utilização de processamento dos equipamentos da solução de NIPS;

2.10.20.2. Taxa de transferência dos equipamentos da solução de NIPS;

2.10.20.3. Taxa de transferência das interfaces dos equipamentos da solução de NIPS;

2.10.21. Suportar notificação de falhas de sistema, permitindo envio de informação sobre falha de sistema, conforme subitens abaixo:

2.10.21.1. Através de integração com servidor SYSLOGD;

2.10.21.2. Através de integração com servidor SNMP;

2.10.22. Possuir capacidade de geração de relatórios;

2.10.22.1. Não será permitido a utilização de solução de terceiros ou externa para esta finalidade;

2.10.23. Possuir capacidade de gerar relatórios, de forma remota e centralizada, para os eventos e alertas dos equipamentos da solução NIPS, conforme abaixo:

2.10.23.1. Manual: geração de relatórios sob demanda;

2.10.23.2. Automático: geração de relatórios de forma agendada e automática;

2.10.24. Permitir exportar relatórios para arquivos HTML, CSV e PDF;

2.10.25. Deve possuir relatórios pré-definidos, no mínimo para:

2.10.25.1. Resumo executivo;

2.10.25.2. Resumo de reputação da origem do ataque;

2.10.25.3. Resumo de reputação do destino do ataque;

2.10.25.4. Ataques de reconhecimento;

2.10.25.5. Análise de tendências;

2.10.25.6. Os 10 (dez) ataques mais detectados;

2.10.25.7. As 10 (dez) ameaças (malwares) mais detectados;

2.10.25.8. As 10 (dez) origens que mais atacaram;

2.10.25.9. Os 10 (dez) destinos que mais foram atacados;

2.10.26. Permitir customização e criação de relatórios sob demanda, permitindo utilização de filtros específicos, no mínimo para:

2.10.26.1. Endereço IP de origem;

2.10.26.2. Endereço IP de destino;

2.10.26.3. País de origem;

2.10.26.4. País de destino;

2.10.26.5. Identificação do usuário de origem;

2.10.26.6. Identificação do usuário de destino;

2.10.26.7. Nome do ataque;

3. Níveis de Serviço

3.1. Garantia, Suporte e Atualização:

3.1.1. A garantia da solução, bem como da atualização dos softwares e patches será de 36 (trinta e seis) meses, a partir do recebimento definitivo do SERPRO;

3.1.2. A garantia de 36 (trinta e seis) meses contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto ofertado, bem como a atualização dos softwares;

3.1.3. A atualização deverá englobar o fornecimento de versões, releases e patches mais recentes e de versões mais recente da base de conhecimento;

3.1.4. O serviço de atualização deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

3.1.5. A cada nova versão instalada, a CONTRATADA deverá apresentar as novas funcionalidades de acordo com a solicitação do SERPRO, sem ônus adicional;

3.1.6. Caso a solução fornecida seja descontinuada na linha de comercialização do fabricante, durante a vigência da garantia, a CONTRATADA deverá manter as condições da garantia nesta contratação explicitada, ou providenciar a substituição por outra solução disponível que executem as mesmas funcionalidades exigidas no edital, sem ônus adicionais para o SERPRO;

3.2. Manutenção Preventiva:

3.2.1. Para Solução ofertada, a CONTRATADA deverá realizar, no exercício da garantia, intervenções preventivas, sendo de responsabilidade da CONTRATADA prover todas as correções e atualizações necessárias, de forma sistemática e programada, de acordo com a periodicidade e os procedimentos especificados na documentação do fabricante;

3.2.2. A CONTRATADA deve entregar um cronograma de manutenção preventiva para

aprovação do SERPRO;

3.2.3. A CONTRATADA deverá entregar, a cada intervenção preventiva realizada, relatório técnico contendo os procedimentos executados;

3.2.4. Nas intervenções preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial, o SERPRO deverá ser previamente notificado para que se proceda a aprovação e o agendamento da operação em horário conveniente ao SERPRO;

3.3. Níveis de Severidade e sancionamentos:

3.3.1. O exercício da garantia para retorno de hardware e software à condição operacional da solução deverá ser realizado conforme critérios abaixo:

3.3.2. O atendimento deve ser prestado 10 (dez) horas por dia, das 8 às 18 horas, de segunda-feira a sexta-feira, excluindo os feriados, exceto para os chamados de atividades programadas;

3.3.3. O atendimento aos chamados para o exercício da garantia deverá obedecer à seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Penalidades
1 – Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	Presencial	No máximo 4 (quatro) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO	No máximo 8 (oito) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,15% (zero vírgula quinze por cento) do valor contratual, por hora ou fração de hora de atraso
2 – Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	Presencial	No máximo 6 (seis) horas após a abertura do chamado	No máximo 10 (dez) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,1% (zero vírgula um por cento) do valor contratual, por hora ou fração de hora de atraso
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes	Remoto	No máximo 10 (dez) horas após a abertura do chamado	No máximo 24 (vinte e quatro) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,075% (zero vírgula zero setenta e cinco por cento) do valor contratual, por hora ou fração de hora de atraso
4 – Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado	No máximo 72 (setenta e duas) horas após a abertura do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,05% (zero vírgula zero cinco por cento) do valor contratual, por hora ou fração de hora de atraso

3.3.4. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

3.3.5. Durante o período de garantia, a CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção;

3.3.5.1. Deve fornecer orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs;

3.3.5.2. Nos casos de problemas não documentados, os registros enviados pelo SERPRO (tais como: traces, dumps e logs) devem ser encaminhadas aos laboratórios do responsável técnico, a fim de que sejam fornecidas as devidas correções;

3.3.6. Deve possuir suporte técnico para solução e seus acessórios, durante o período de vigência do contrato, assegurando prazo de atendimento;

3.4. Chamados, Registro e Início de Prazos:

3.4.1. O atendimento aos chamados deve obedecer à tabela de classificação quanto ao nível de severidade;

3.4.2. Será aberto um chamado para cada problema reportado;

3.4.3. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado através de telefone 0800 e Web;

3.4.4. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto;

3.4.4.1. O chamado será registrado na CONTRATADA, recebendo uma identificação para acompanhamento, controle e histórico;

3.4.4.2. A contagem de tempo de atendimento será inciada a partir da hora de acionamento;

3.5. Atendimento e Manutenções:

3.5.1. A CONTRATADA deve prover todas as correções e atualizações dos hardwares instalados para nível de firmware e microcódigos;

3.5.2. Deve manter a solução compatível com os demais componentes de hardware e software dos Centro de Dados do SERPRO, sem ônus adicional para o SERPRO;

3.5.3. Em caso de manutenções, preventivas ou corretivas caso haja risco de indisponibilidade total ou parcial da solução O SERPRO deverá ser previamente notificado para que se proceda à aprovação e o agendamento da manutenção em horário conveniente ao SERPRO;

3.5.4. A CONTRATADA deve possuir acesso para suporte técnico de 2° e 3° níveis para o firmware e microcódicos da solução, sem ônus adicional para SERPRO;

3.5.5. Para todos efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.5.5.1. Suporte Técnico Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral;

3.5.5.2. Suporte Técnico Segundo Nível: equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade;

3.5.5.3. Suporte Técnico Terceiro Nível: escalonamento obrigatório ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas;

3.6. As peças e componentes em substituição, instaladas pela CONTRATADA, serão incorporadas na solução, passando a ser de propriedade do SERPRO;

3.7. Canais de Atendimento:

3.7.1. Atendimento por meio de canal telefônico gratuito 0800 ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.7.2. Chamado técnico através de site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.8. Escalação e Severidade:

3.8.1. Por necessidade de serviço ou criticidade do problema, o SERPRO poderá solicitar a escalação de chamado para níveis superiores ou inferiores de severidade ou seus respectivos prazos;

3.9. Entrega Mensal de Relatório:

3.9.1. Mensalmente deverá ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período do exercício da garantia, por regional do SERPRO;

3.9.2. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, tipo do atendimento (remoto e presencial), data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada;

3.9.3. O relatório deverá ser entregue mesmo quando não houver chamados no período.