3.37. Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

3.38. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

CONTROLE DE APLICAÇÕES

3.39. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.39.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

3.39.2. Reconhecer pelo menos 1700 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;

3.39.3.

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

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

3.39.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

3.39.6. 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.

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

3.39.8. 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;

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

3.39.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

3.39.11. Atualizar a base de assinaturas de aplicações automaticamente;

3.39.12. Reconhecer aplicações em IPv6;

3.39.13. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

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

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

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

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

3.39.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.39.19. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

3.39.19.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

3.39.20. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

3.39.21. Deve alertar o usuário quando uma aplicação for bloqueada;

3.39.22. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

3.39.23. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;

3.39.24. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;

3.39.25. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

3.39.26. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

3.39.27. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

3.39.27.1. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

3.39.27.2. Nível de risco da aplicação.

3.39.27.3. Categoria e sub-categoria de aplicações.

3.39.27.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

PREVENÇÃO DE AMEAÇAS

3.40. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

3.41. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.42. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.43. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

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

3.45. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

3.46. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

3.47. Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

3.48. Deve permitir o bloqueio de vulnerabilidades.

3.49. Deve permitir o bloqueio de exploits conhecidos.

3.50. Deve incluir proteção contra ataques de negação de serviços.

3.51. Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 3.51.1. Análise de padrões de estado de conexões;
- 3.51.2. Análise de decodificação de protocolo;
- 3.51.3. Análise para detecção de anomalias de protocolo;

3.51.4. Análise heurística;
3.51.5. IP Defragmentation;
3.51.6. Remontagem de pacotes de TCP;
3.51.7. Bloqueio de pacotes malformados.

3.52. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

3.53. Detectar e bloquear a origem de portscans;

3.54. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

3.55. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.56. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

3.57. Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.58. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

3.59. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

3.60. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

3.60.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

3.61. Suportar bloqueio de arquivos por tipo;

3.62. Identificar e bloquear comunicação com botnets;

3.63. Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

3.64. Deve suportar referencia cruzada com CVE;

3.65. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.65.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

3.66. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;

3.67. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

3.68. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

3.69. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

3.70. Os eventos devem identificar o país de onde partiu a ameaça;

3.71. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

3.72. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

3.73. Rastreamento de vírus em pdf.

3.74. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

3.75. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada politica de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

ANÁLISE DE MALWARES MODERNOS

3.76. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir

funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

3.77. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

3.78. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

3.79. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

3.80. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

3.81. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

3.82. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

3.83. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

3.84. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

3.85. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

3.86. O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

3.87. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

3.88. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

3.89. Deve permitir visualizar o resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

3.90. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

3.91. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

3.92. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

3.93. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

3.94. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class) e Android APKs no ambiente controlado;

3.95. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência mínima de 15 minutos

3.96. Permitir o envio de arquivos para análise no ambiente controlado via de forma automática via API.

FILTRO DE URL

3.97. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

3.97.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.97.2. Deve ser possível a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

3.97.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

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

3.97.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.97.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

3.97.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

3.97.8. Possui pelo menos 60 categorias de URLs;

3.97.9. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

3.97.10. Suporta a criação categorias de URLs customizadas;

3.97.11. Suporta a exclusão de URLs do bloqueio, por categoria;

3.97.12. Permite a customização de página de bloqueio;

3.97.13. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

3.97.14. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

3.97.15. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

3.98. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da

integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

3.99. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

3.100. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

3.101. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

3.102. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

3.102.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

3.103. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

3.104. Suporte a autenticação Kerberos;

3.105. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

3.106. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

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

3.108. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

3.109. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.110. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

QOS

3.111. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

3.112. Suportar a criação de políticas de QoS por:
- 3.112.1. Endereço de origem
- 3.112.2. Endereço de destino
- 3.112.3. Por usuário e grupo do LDAP/AD.
- 3.112.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 3.112.5. Por porta;

3.113. O QoS deve possibilitar a definição de classes por:
- 3.113.1. Banda Garantida
- 3.113.2. Banda Máxima
- 3.113.3. Fila de Prioridade.

3.114. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

3.115. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

3.116. Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

3.117. Disponibilizar estatísticas RealTime para classes de QoS.

3.118. Deve suportar QOS (traffic-shapping), em interface agregadas;

3.119. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

FILTRO DE DADOS

3.120. Permite a criação de filtros para arquivos e dados pré-definidos;

3.121. Os arquivos devem ser identificados por extensão e assinaturas;

3.122. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

3.123. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;

3.124. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

3.125. Permitir listar o número de aplicações suportadas para controle de dados;

3.126. Permitir listar o número de tipos de arquivos suportados para controle de dados;

Geo-localização

3.127. Suportar a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.

3.128. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

3.129. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

VPN

3.130. Suportar VPN Site-to-Site e Cliente-To-Site;

3.131. Suportar IPSec VPN;

3.132. Suportar SSL VPN;

3.133. A VPN IPSEc deve suportar:
- 3.133.1. 3DES;
- 3.133.2. Autenticação MD5 e SHA-1;
- 3.133.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
- 3.133.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
- 3.133.5. AES 128, 192 e 256 (Advanced Encryption Standard)
- 3.133.6. Autenticação via certificado IKE PKI.

3.134. Deve possuir interoperabilidade com os seguintes fabricantes:
- 3.134.1. Cisco;
- 3.134.2. Checkpoint;

3.134.3. Juniper;
3.134.4. Palo Alto Networks;
3.134.5. Fortinet;
3.134.6. Sonic Wall;

3.135. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

3.136. A VPN SSL deve suportar:

3.136.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.136.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

3.136.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

3.136.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

3.136.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

3.136.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

3.136.7. Atribuição de DNS nos clientes remotos de VPN;

3.136.8. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

3.136.9. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

3.136.10. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.136.11. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

3.136.12. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

3.136.13. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

3.136.14. Suporta leitura e verificação de CRL (certificate revocation list);

3.136.15. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.136.16. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

3.136.17. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

3.136.18. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

3.136.18.1. Antes do usuário autenticar na estação;
3.136.18.2. Após autenticação do usuário na estação;
3.136.18.3. Sob demanda do usuário;

3.136.19. Deverá Manter uma conexão segura com o portal durante a sessão.

3.136.20. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8 e Mac OSx;

CONSOLE DE GERÊNCIA E MONITORAÇÃO

3.137. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.

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

3.139. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

3.140. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi;

3.141. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

3.142. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

3.143. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

3.144. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;

3.145. Deve permitir a criação de objetos e políticas compartilhadas;

3.146. Deve consolidar logs e relatórios de todos os dispositivos administrados;

3.147. Deve permitir que exportar backup de configuração automaticamente via agendamento;

3.148. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

3.149. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

3.150. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

3.151. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

3.152. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

3.153. O gerenciamento deve permitir/possuir:

3.153.1. Criação e administração de políticas de firewall e controle de aplicação;

3.153.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

3.153.3. Criação e administração de políticas de Filtro de URL;

3.153.4. Monitoração de logs;

3.153.5. Ferramentas de investigação de logs;
3.153.6. Debugging;
3.153.7. Captura de pacotes.

3.154. Acesso concorrente de administradores;

3.155. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

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

3.157. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

3.158. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;

3.159. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

3.160. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

3.161. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

3.162. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

3.163. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

3.164. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

3.165. Criação de regras que fiquem ativas em horário definido;

3.166. Criação de regras com data de expiração;

3.167. Backup das configurações e rollback de configuração para a última configuração salva;

3.168. Suportar Rollback de Sistema Operacional para a ultima versão local;

3.169. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

3.170. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

3.171. Validação de regras antes da aplicação;

3.172. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

3.173. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

3.174. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

3.175. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

3.176. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

3.177. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

3.178. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

3.179. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

3.180. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

3.181. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

3.182. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

3.183. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

3.184. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

3.185. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

3.186. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

3.187. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

3.188. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

3.189. Deve ser possível exportar os logs em CSV;

3.190. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

3.191. Rotação do log;

3.192. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

3.193. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

3.193.1. Situação do dispositivo e do cluster;

3.193.2. Principais aplicações;

3.193.3. Principais aplicações por risco;

3.193.4. Administradores autenticados na gerência da plataforma de segurança;

3.193.5. Número de sessões simultâneas;

3.193.6. Status das interfaces;

3.193.7. Uso de CPU;

3.194. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

3.194.1. Resumo gráfico de aplicações utilizadas;

3.194.2. Principais aplicações por utilização de largura de banda de entrada e saída;

3.194.3. Principais aplicações por taxa de transferência de bytes;

3.194.4. Principais hosts por número de ameaças identificadas;

3.194.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

3.194.6. Deve permitir a criação de relatórios personalizados;

3.195. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

3.195.1. Gerar alertas automáticos via:
3.195.2. Email;
3.195.3. SNMP;
3.195.4. Syslog;

3.196. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

4. Item 02 - CONSOLE DE GERÊNCIA E MONITORAÇÃO

4.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.

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

4.3. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

4.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi;

4.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

4.6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

4.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

4.8. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;

4.9. Deve permitir a criação de objetos e políticas compartilhadas;

4.10. Deve consolidar logs e relatórios de todos os dispositivos administrados;

4.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;

4.12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

4.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

4.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

4.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.16. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

4.17. O gerenciamento deve permitir/possuir:
- 4.17.1. Criação e administração de políticas de firewall e controle de aplicação;
- 4.17.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 4.17.3. Criação e administração de políticas de Filtro de URL;
- 4.17.4. Monitoração de logs;
- 4.17.5. Ferramentas de investigação de logs;
- 4.17.6. Debugging;
- 4.17.7. Captura de pacotes.

4.18. Acesso concorrente de administradores;

4.19. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

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

4.21. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

4.22. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;

4.23. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

4.24. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

4.25. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.26. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

4.27. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

4.28. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

4.29. Criação de regras que fiquem ativas em horário definido;

4.30. Criação de regras com data de expiração;

4.31. Backup das configurações e rollback de configuração para a última configuração salva;

4.32. Suportar Rollback de Sistema Operacional para a ultima versão local;

4.33. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

4.34. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

4.35. Validação de regras antes da aplicação;

4.36. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

4.37. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

4.38. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

4.39. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

4.40. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

4.41. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

4.42. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

4.43. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

4.44. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

4.45. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

4.46. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

4.47. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

4.48. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

4.49. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

4.50. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

4.51. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

4.52. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

4.53. Deve ser possível exportar os logs em CSV;

4.54. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

4.55. Rotação do log;

4.56. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

4.57. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

4.57.1. Situação do dispositivo e do cluster;

4.57.2. Principais aplicações;

4.57.3. Principais aplicações por risco;

4.57.4. Administradores autenticados na gerência da plataforma de segurança;

4.57.5. Número de sessões simultâneas;

4.57.6. Status das interfaces;

4.57.7. Uso de CPU;

4.58. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

4.58.1. Resumo gráfico de aplicações utilizadas;

4.58.2. Principais aplicações por utilização de largura de banda de entrada e saída;

4.58.3. Principais aplicações por taxa de transferência de bytes;

4.58.4. Principais hosts por número de ameaças identificadas;

4.58.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

4.58.6. Deve permitir a criação de relatórios personalizados;

4.59. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

4.59.1. Gerar alertas automáticos via:
4.59.2. Email;
4.59.3. SNMP;
4.59.4. Syslog;

4.60. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

5. MODELO DE PLANILHA DE ATENDIMENTO A REQUISITOS

O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta**.**

Item	Documento	Página	Localização

6. AMOSTRA

6.1. **P**oderá haver teste de bancada para comprovar a conformidade dos dispositivos oferecida caso a instituição julgue necessário;

6.2. Caso a instituição solicite amostra da solução, a licitante deverá fornecer amostra dos equipamentos para que seja verificado o atendimento aos itens do edital, incluindo a capacidade do equipamento e as funcionalidades exigidas.

6.3. A proponente deverá fornecer todos os equipamentos para geração de tráfego de acordo com as solicitações de performance descritas neste edital sem custo para a instituição;

6.4. O teste de bancada poderá aferir o desempenho dos equipamentos como as funcionalidades que fazem uso de assinaturas, habilitadas para todas as assinaturas que a plataforma de segurança possuir, bem como amostra de todos os recursos solicitados;

6.5. Os testes deverão ser executados nas dependências da sede da instituição em um prazo máximo de 30 dias após a solicitação da amostra;

6.6. A amostra deverá ser identificada com o número da licitação, o objeto, o nome do licitante, seu telefone e endereço.

6.7. A amostra aprovada ficará retida para confronto com os materiais, quando do seu recebimento pela instituição.

6.8. A instituição se reserva o direito de não aceitar a amostra, independentemente da informação contida na proposta em relação à marca, caso não atenda às especificações exigidas ou seja de qualidade inferior à dos materiais solicitados.

6.9. Amostras não aprovadas permanecerão à disposição dos respectivos licitantes, para retirada, pelo prazo de 90 (noventa) dias úteis após a conclusão do processo licitatório. As amostras não retiradas serão descartadas pela instituição.

6.10. A proponente deve apresentar via original ou fotocópia autenticada, da seguinte documentação: A marca, o modelo e o fabricante de cada produto ofertado, bem como apresentar os catálogos e descritivos técnicos; de maneira a deixar bem claras quais são suas verdadeiras características e que todas elas atendam às especificações técnicas contidas neste TERMO DE REFERÊNCIA.

6.11. Será emitido um relatório sucinto descrevendo os exames realizados e contendo a aprovação ou não do material/produto.

7. DA IMPLANTAÇÃO E CONFIGURAÇÃO

7.1. DA IMPLANTAÇÃO:

7.1.1. Fica facultado a CONTRATADA, em fase paralela à entrega dos componentes, de acordo com os prazos estipulados, solicitar a realização de atividades relativas ao conhecimento do ambiente tecnológico da CONTRATANTE (Vistoria), no sentido de conhecer condições físicas e lógicas para implantação da solução e colher subsídios para a elaboração do plano de implantação, não podendo, a CONTRATADA, posteriormente, alegar o desconhecimento do ambiente físico e lógico da CONTRATANTE para deixar de cumprir obrigação contratual, justificar qualquer acréscimo de valores em sua proposta ou ainda construir plano de implantação não exeqüível nas condições apresentadas.

7.1.2. O Coordenador do Projeto da CONTRATADA deverá comunicar ao gestor da CONTRATANTE responsável pelo acompanhamento da implantação da solução, a conclusão de cada macro-fase.

7.1.3. Imediatamente após o recebimento do comunicado de conclusão, a CONTRATANTE realizará encontro de homologação para decidir sobre o aceite de finalização da macro-fase. Este encontro contará com a presença, mínima, dos seguintes profissionais:

- Coordenador do Projeto (CONTRATADA);
- Representante da equipe técnica (CONTRATADA);

- Gerente de projeto (CONTRATANTE);
- Representante da equipe técnica (CONTRATANTE).

7.1.4. Em caso de não aceitação de conclusão, a CONTRATADA fica obrigada a adotar medidas imediatas visando corrigir quaisquer situações que possam estar impedindo a devida finalização da macro-fase.

7.1.5. O plano de implantação deverá considerar os prazos e interdependências entre fases previstas.

7.2. DO PERÍODO DE FUNCIONAMENTO EXPERIMENTAL (PFE):

7.2.1. Este período consiste na continuidade do funcionamento da solução, quando a solução será colocada em operação no ambiente de produção da CONTRATANTE em caráter piloto, com aprofundamento da verificação das características funcionais, sistêmicas e de operação.

7.2.2. A CONTRATADA deverá implantar parte da solução (subconjunto pré-definido de funcionalidades) capaz de atender a um ambiente operacional, a critério da CONTRATANTE, em caráter experimental, funcionando em produção e implementando os requisitos deste termo, quando aplicáveis.

7.2.3. Durante o PFE, deverão ser eliminadas todas as pendências de qualquer natureza (qualidade da documentação técnica dos componentes, instalação, ativação, funcionamento etc.) que porventura existirem, sendo que o início do Período Sem falhas (PSF), descrito a seguir, será postergado, por no máximo 1 (uma) vez, até que isso ocorra efetivamente.

7.2.4. Quando todas as pendências forem eliminadas, será marcado o início de um período considerado parte do PFE e denominado Período Sem Falhas (PSF), que se estenderá pelo tempo definido neste Termo de Referência, no qual os produtos não deverão apresentar falhas de qualquer natureza ou quaisquer outras condições em desacordo com as exigências técnicas para a solução.

7.2.5. Toda vez que for detectada uma nova falha ou condição em desacordo com as exigências técnicas para a solução, o PSF será reiniciado.

7.2.6. Se, por limitação da CONTRATADA, o PSF não for atendido, a mesma terá o contrato rescindido. A CONTRATANTE procederá com a chamada do segundo licitante classificado.

7.2.7. O encerramento desta etapa será marcado pela comunicação formal a CONTRATADA e emissão, por parte da CONTRATANTE, do Termo de Aceitação Provisória (TAP), atestando a qualidade e adequação preliminar da solução às necessidades especificadas, permitindo a continuidade dos trabalhos de implantação em produção.

7.2.8. Os itens a seguir determinam as condições estabelecidas para o período de funcionamento experimental (PFE):

7.2.8.1. Implantação deverá ser realizada observando os eventos os prazos definidos;

7.2.8.2. Os serviços serão considerados implantados quando: os serviços corporativos e sistemas aplicativos de negócios disponibilizados puderem ser utilizados com sucesso, observando os SLAs especificados e os serviços estiverem operacionais e atendendo os níveis de serviços especificados.

7.3. DA IMPLANTAÇÃO DA SOLUÇÃO EM AMBIENTE DE PRODUÇÃO:

7.3.1. Será realizado pela CONTRATADA, com acompanhamento por parte da CONTRATANTE, a implantação dos componentes da solução não implantados no PFE, contemplando os diversos ambientes da CONTRATANTE que funcionam em produção e implementando todos os requisitos deste termo, quando aplicáveis.

7.3.2. O Termo de Aceitação Definitiva (TAD) será emitido após a efetiva implantação de toda a solução adquirida integrada ao ambiente tecnológico da CONTRATANTE.

7.3.3. O TAD não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas pelos componentes da solução. A emissão do TAD não terá caráter de atestado de capacidadetécnica.

7.3.4. No TAD poderão constar, comoanexos, os testes realizados e os resultados obtidos e validados pela CONTRATANTE, nas etapas de homologação da solução, se a CONTRATADA assim o desejar.

7.3.5. Somente após a emissão do TAD deverá ser iniciado o período de manutenção e suporte técnico, especificado neste termo.

7.4. DAS CONDIÇÕES PARA A PRESTAÇÃO DOS SERVIÇOS:

7.4.1. A CONTRATADA deve fornecer pessoal necessário e tecnicamente habilitado à boa e integral execução e manutenção dos serviços.

7.4.2. A CONTRATADA deve fornecer todos os materiais e serviços próprios e adequados à execução dos trabalhos.

7.4.3. A CONTRATADA deve retirar da prestação dos serviços qualquer empregado que, a critério da CONTRATANTE seja julgado inconveniente ao bom andamento dos trabalhos.

7.4.4. A CONTRATADA deve comunicar, imediatamente, por escrito quaisquer dificuldades encontradas pelos técnicos alocados para execução dos serviços que, eventualmente, possam prejudicar a boa e pontual execução dos trabalhos, sob a pena de serem tais dificuldades consideradas inexistentes.

7.4.5. A CONTRATADA deverá ter, no mínimo, profissionais com os certificados especificados na tabela abaixo; de forma a garantir a prestação adequada dos serviços de Segurança da Informação previstos:

7.4.6. A CONTRATADA deverá ser revenda autorizada e/ou canal integrador dos fabricantes das soluções por ela ofertadas em todas as soluções especificadas por este documento.

7.4.7. A comprovação do item anterior será realizada através de declaração do fabricante no Brasil dirigido especificamente a CONTRATADA e ao processo licitatório comprovando a parceria entre a CONTRATADA e o(s) fabricante(s) da(s) solução(ões).

7.4.8. Não será permitida a participação de consórcios e nem tampouco sublocação de serviços em parte ou de modo global.

8. DA TRANSFERÊNCIA DE TECNOLOGIA

8.1. A CONTRATADA deverá fornecer treinamento na plataforma ofertada para 8 (oito) profissionais da CONTRATANTE, no formato “hands-on”, com uma carga horária mínima de 24 (vinte e quatro) horas e certificado de participação.

8.2. O treinamento deverá ser ministrado por técnico certificado e qualificado da fabricante da solução.
8.3. A comprovação se dará através de certificado emitido pelo fabricante da solução informando o nível de certificação do técnico.
8.4. O treinamento deverá ocorrer na sede do Tribunal de Justiça do Amazonas, situado à Avenida André Araújo, S/N, CEP 69060-000, Manaus, Amazonas.
8.5. As despesas com deslocamento e hospedagem ocorrerão por conta da CONTRATADA.

9. DA GARANTIA

9.1. Os prazos de garantia, contados a partir do termo de recebimento definitivo dos equipamentos, deverão estar de acordo com o definido neste termo de referência, ou ainda, a CONTRATADA deverá repassar a CONTRATANTE as mesmas garantias concedidas pelo fabricante dos equipamentos, caso seja superior à exigida.
9.2. A garantia será sempre exigida da CONTRATADA, portanto em nenhuma hipótese será admitida qualquer transferência de responsabilidade para terceiros.
9.3. Os equipamentos deverão ser fornecidos com garantia total de 36 (trinta e seis) meses, incluindo atualização das licenças, garantia de hardware do produto, soluções de problemas, alterações de configurações, atualizações de políticas, softwares, etc.
9.4. O atendimento on-site deverá ser na modalidade NBD (dia seguinte) e o suporte telefônico deve ter tempo de atendimento de 4 horas com solução em até 8 horas.
9.5. A responsabilidade da garantia não pode ser repassada para terceiros.
9.6. A CONTRATADA deverá informar todo processo de abertura de chamados (site, telefones etc).
9.7. Todos os componentes dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.
9.8. A assistência técnica deverá ser de acordo com o definido em cada item do relatório de materiais licitados.
9.9. O endereço para assistência técnica poderá ser comprovado pelo catálogo de assistência técnica do fabricante ou na sua falta por indicação expressa em documentação oficial do FABRICANTE direcionada a CONTRATANTE para o referido processo.
9.10. A CONTRATADA deverá fornecer a garantia do fabricante dos produtos de acordo com o definido nas especificações dos itens adquiridos. A garantia deverá ser executada por assistência técnica autorizada indicada pelo fabricante, e caso a assistência técnica autorizada esteja impedida de realizar atendimentos, os mesmos serão realizados por outra autorizada (indicada pelo fabricante) ou pelo próprio fabricante sem ônus adicional para este órgão.
9.11. Atender as solicitações para conserto e corrigir defeitos apresentados nos aparelhos/equipamentos em prazo não superior a 05 (cinco) dias úteis dentro do período de garantia.

9.12. Substituir, dentro do período de garantia, aparelhos/equipamentos que venham a apresentar falhas ou defeitos insanáveis, sem que isto acarrete ônus para a CONTRATANTE.

10. DA CLASSIFICAÇÃO DOS BENS COMUNS

10.1. Os bens a serem adquiridos enquadram-se na classificação de bens comuns, nos termos da Lei n° 10.520, de 2002, do Decreto n° 3.555, de 2000, e do Decreto 5.450, de 2005.

11. DO VALOR ESTIMADO DO OBJETO

11.1. O valor estimado do objeto a ser adquirido será levantado pela Divisão de Infraestrutura e Logística – DVIL, por meio de consulta de mercado (Apêndice I).

12. OBRIGAÇÕES DO CONTRATANTE

12.1. Receber provisoriamente o material, disponibilizando local, data e horário.
12.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos.
12.3. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de servidor especialmente designado.
12.4. Efetuar o pagamento no prazo previsto.
12.5. Proporcionar todas as facilidades para que a CONTRATADA possa cumprir suas obrigações dentro das normas e condições deste processo de venda;
12.6. Rejeitar, no todo ou em parte, o material entregue em desacordo com as especificações e obrigações assumidas pela CONTRATADA;
12.7. Atestar a nota fiscal, estando todos os itens em perfeito estado e em conformidade com as especificações técnicas e fiscalizar o contrato, se o caso, à luz das especificações técnicas, por intermédio de servidor designado da Divisão de Tecnologia da Informação e Comunicação – DVTIC – TJAM.

13. OBRIGAÇÕES DA CONTRATADA

13.1. Efetuar a entrega dos bens em perfeitas condições, no prazo e local indicado pela Administração, em estrita observância das especificações deste termo de referência, acompanhado da respectiva nota fiscal constando detalhadamente as indicações da marca, fabricante, modelo, tipo e procedência.
13.2. Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 18 e 26, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).
13.3. O dever previsto no subitem anterior implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo de 30 (trinta) (dias), o produto com avarias ou defeitos.

13.4. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da presente aquisição.
13.5. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
13.6. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus a CONTRATANTE.
13.7. Substituir todo e qualquer item que chegar danificado.
13.8. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo até a entrega do material no almoxarifado, incluindo as entregas feitas por transportadoras.
13.9. Responsabilizar-se pelo fiel cumprimento da venda deste material.
13.10. Entregar os itens em perfeito estado (equipamentos novos de primeiro uso) e de acordo com as especificações técnicas, no prazo e local estabelecidos.
13.11. Em caso de acionamento de suporte técnico dentro do prazo de garantia, atender ao chamado técnico dentro do prazo estipulado no termo de referência constante.

14. DAS CONDIÇÕES DO FORNECIMENTO, LOCAL E PRAZO DE ENTREGA.

14.1. O prazo de entrega dos equipamentos deverá ser de até 45 (quarenta e cinco) dias úteis, contados a partir do recebimento da Nota de Empenho.
14.2. Os bens deverão ser entregues na sede do Tribunal de Justiça do Estado do Amazonas, sito Edifício Desembargador Arnoldo Péres, Av. André Araújo, S/N, Aleixo, Manaus – AM, CEP 69.060-000, no horário de expediente das 08:00 horas às 14:00 horas, de segunda à sexta, exceto feriados.
14.3. A empresa poderá emitir uma nota fiscal conjugada ou notas fiscais de venda para os materiais, notas fiscais de Software e notas fiscais de serviços individualizadas para a instalação, para a garantia e para o suporte, desde que os valores estejam discriminados no contrato e que o radical do CNPJ seja o mesmo. As notas fiscais acompanham as mercadorias entregues e devem, sempre que possível, discriminar os itens entregues para conferência e registros pertinentes.
14.4. A empresa vencedora deverá prover treinamento operacional e capacitação de acordo com o item 8 deste Termo de Referencia.
14.5. A instalação deverá ser em local indicado pelo setor requisitante.

15. DO RECEBIMENTO E CRITÉRIO DE ACEITAÇÃO DO OBJETO

15.1. Os bens serão recebidos:
15.1.1. Provisoriamente em cinco dias, a partir da entrega, para efeito de verificação da conformidade com as especificações constantes da proposta.
15.2. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

15.3. A Administração rejeitará, no todo ou em parte, a entrega dos bens em desacordo com as especificações técnicas exigidas.

16. DO CONTROLE DA EXECUÇÃO

16.1. A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.

16.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução do contrato.

16.3. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em co-responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

16.4. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

17. DO PAGAMENTO

17.1. O pagamento será realizado em moeda corrente nacional, mediante Ordem Bancária Eletrônica, e ocorrerá em 30 (trinta) dias, a contar da apresentação da nota fiscal/fatura pelo contratado, que devera ser submetida ao atesto pelo setor competente pela fiscalização do contrato.

Manaus, 27 de Setembro de 2016

_____

Thiago Facundo de Magalhães Franco
Diretor de TI – DVTIC / TJAM

_____

Breno Figueiredo Corado
Coordenador de TI – DVTIC / TJAM

ANEXO I – MODELO DE DECLARAÇÃO DE VISTORIA

PREGÃO ELETRÔNICO Nº XXX/2016.

Declaramos para todos os efeitos que o representante da empresa _____, CNPJ nº _____, compareceu e efetuou vistoria neste setor, tomando plena ciência da dimensão dos serviços a serem efetuados pela licitante.

_____/_____/_____

_____

(nome e assinatura do responsável pelo setor no TJAM)

APÊNDICE

PLANILHA DE VALOR ESTIMADO PARA REGISTRO DE PREÇOS

ITEM	DESCRIÇÃO	UNIDADE	QTDE.	VALOR UNITÁRIO ESTIMADO (R$)	VALOR TOTAL ESTIMADO (R$)
01	Aquisição de solução de proteção de rede com características de Farewal de Próxima Geração (NGFW), com suporte a administração de banda (QOS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares Zero Day, Filtro de Url.	UND	04	R$ 722.759,00	R$2.891.036,00
02	Console de Gerencia e Monitoração	UND	01	R$ 119.134,25	R$119.134,25
					R$ 3.010.170,25

OBSERVAÇÃO: OS VALORES ESTIMADOS FORAM PROVENIENTES DE PESQUISA DE MERCADO.

Manaus, 29 de agosto de 2016.

Cotado por
Hélida Valéria M. Telles de Souza
Chefe do Setor de Compras

Henrique Cerf Levy Neto
Diretor da Divisão de Infraestrutura e Logística