**ESTUDOS PRELIMINARES**

**I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO**

**1. — DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS**

**Requisitos de negócio**

Ter dispositivo de segurança ***tipo firewall*** de próxima geração (Next Generation Firewall), que implemente filtros para controlar as conexões e comunicações que trafegam de uma rede para outra, cujos filtros possuem a ação de permitir ou negar o acesso entre redes. Este dispositivo denominado de firewall tem várias características, as quais se destacam: ajudar a impedir que a rede, servidores e ativos sejam acessados sem autorização; evitar que informações sejam capturadas; bloquear programas indesejados na rede como compartilhamento de dados e de mensagens instantâneas; fechar portas não utilizadas, racionalizando o uso da Internet; permitir a auditoria nos acessos a recursos da rede; permitir a limitação da banda por serviços e monitoramento dos links de dados que passam pelo equipamento.

1.1. Detalhamento dos bens e serviços que compõem a solução:

1.1.1. Fornecimento de serviços de suporte técnico para a solução de eventuais problemas que possam ocorrer nos equipamentos de firewall pelo período da garantia, incluindo substituições de hardwares quando necessário, durante a vigência da garantia dos equipamentos;

1.1.2. Todas as funcionalidades descritas nos requisitos técnicos deverão funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

1.1.3. O equipamento deverá ser baseado em hardware desenvolvido como dispositivo de segurança tipo firewall, ou seja, não sendo aceitas soluções baseadas em plataforma PC ou equivalente.

1.1.4. Fornecimento e ativação das licenças dos serviços nos firewalls, pelo período de garantia dos equipamentos;

1.1.5. Fornecimento dos serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras do firewall, configuração de VPNs entre firewall concentrador e firewalls de pequeno porte, configuração como roteador entre as Vlans dos usuários e a Vlan dos servidores, configuração de pelo menos 5 regras de firewall para pelo menos 5 servidores de rede, enfim, todos os serviços para a efetiva migração da solução de firewall do Tribunal até alcançar plena estabilidade operacional;

1.1.6. Os novos equipamentos deverão manter a mesma arquitetura existente no TRE-MA em cluster de firewall funcionando com duas appliances em alta disponibilidade (HA), podendo ser ativo-ativo ou ativo-passivo, sendo os gateways de segurança idênticos em cluster, garantindo que em caso de falha de um equipamento o outro assuma o processamento evitando a indisponibilidade dos serviços oferecidos pelo datacenter;

1.1.7. Treinamento para a equipe de técnicos do Tribunal composta de 5 (cinco) pessoas, podendo o treinamento ser na modalidade “in company”;

1.1.8. Os equipamentos deverão ser novos, estarem em linha de produção, terem o fim do ciclo de vida superior a 5 (cinco) anos a partir da entrega, ou seja, não serão aceitos equipamentos em modo “End of Life e End of Support”;

1.1.9. **Deve ter garantia total de pelo menos 5 (cinco) anos, com garantia de funcionamento.** Esta exigência visa garantir a funcionalidade e disponibilidade da solução que se pretende adquirir, a qual é de extrema criticidade dentro do datacenter do TRE-MA, uma vez que o Firewall tem por objetivo aplicar e manter uma política de segurança na rede de computadores deste Tribunal. A garantia contratada nestes termos, além de ser uma prática recorrente no mercado, afasta a temeridade de haver interrupção na prestação de assistência técnica e uma possível indisponibilidade dos serviços suportados pela solução de firewall do TRE-MA, evitando a ocorrência de incidentes da rede. Ademais, esse requisito de garantia tem um melhor custo/benefício para a Administração, considerando os custos elevados de uma possível contratação de extensão

de garantia, conforme demonstrado pelo Doc. PAD n.º 92020/2019.

1.1.10. As atualizações de assinaturas dos serviços, tais como, AntiSpam, antivírus, etc. e atualizações de software e suporte técnico 24x7 deverão ocorrer por pelo menos 5 (cinco) anos;

1.1.11. Deverão ser fornecidos todos os cabos, suportes, parafusos e porca gaiola para a instalação dos equipamentos em rack 19´´;

Requisitos técnicos

**1.2. Firewall tipo 1 - Next Generation Firewall.**

1.2.1. Os equipamentos de firewall CONCENTRADOR deverão ter, **no mínimo**, as seguintes características técnicas:

1.2.1.1. Mínimo de 9 Gbps de statefull Throughput;

1.2.1.2. Mínimo de 6 Gbps de IPS Throughput;

1.2.1.3. Mínimo de 3 Gbps de Application Inspection Throughput;

1.2.1.4. Mínimo de 5.4 Gbps de Anti-Malware Throughput;

1.2.1.5. Mínimo de 1.6 Gbps de DPI Throughput;

1.2.1.6. Mínimo de 4.5 Gbps de VPN Throughput;

1.2.1.7. Mínimo de 02 Interfaces SFP+ de 10 GbE ativas/licenciadas. Os gbics para cada interface devem ser fornecidos junto com o equipamento;

1.2.1.8. Mínimo de 16 portas GbE, sendo que destas no mínimo 8 portas devem ser de 1 GbE (Ethernet RJ45). Caso as outras interfaces sejam fibra, os gbics para cada interface devem ser fornecidos junto com os equipamentos e se essas interfaces forem de velocidades diferentes de 1Gbps elas devem permitir que sejam configuradas para trabalhar na velocidade de 1Gbps;

1.2.1.9. Possuir no mínimo 01 interface de 1 GbE dedicada para gerenciamento e 01 para console;

1.2.1.10. Possuir no mínimo 1 (uma) interface dedicada para sincronismo de estados da solução de alta disponibilidade;

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

1.2.1.12. Suporte no mínimo 400 interfaces de Vlan (802.1q);

1.2.1.13. Deve ser fornecido com dupla ventilação;

1.2.1.14. Deve ser fornecido com fonte redundante;

1.2.1.15. Capacidade mínima de 2000 túneis VPNs IPSEC Site-to-site já licenciadas;

1.2.1.16. Capacidade mínima de 2000 túneis VPNs IPSEC Client-to-Site já licenciadas;

1.2.1.17. Ter capacidade de no mínimo 1000 túneis SSL VPN, devendo fornecer os equipamentos com no mínimo 100 conexões já licenciadas por pelo menos 5 (cinco) anos;

1.2.1.18. Implementar protocolo DHCP Relay;

1.2.1.19. O equipamento deve ser fornecido com a capacidade máxima de memória e processamento;

1.2.1.20. Deve possibilitar a visualização da utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede na sua interface de gerência e/ou em sistema de gerência centralizado;

1.2.1.21. Deve implementar decriptografia e inspeção de tráfego SSL. Esta funcionalidade já deve estar licenciada por pelo menos 5 (cinco) anos;

1.2.1.22. Deve implementar administração/controle de largura de banda (QoS);

1.2.1.23. Deve suportar os protocolos:

(a) IPV4 e IPV6;
(b) VLAN 802.1.q
(c) Agregação de links 802.3x;
(d) DHCP e DHCPv6;
(e) NTP;
(f) Roteamento estático e dinâmico em IPv4 e IPv6;
(g) Roteamento RIP v1/v1, OSPF v2 e OSPF v3 e BGP v4;

(h) Deve suportar SNMP v2c e SNMP v3;

1.2.1.24. Deve permitir acesso ao equipamento via CLI (console), SSH e interface web HTTPS;

1.2.1.25. Deve possuir funcionalidade de backup/restore da configuração e políticas de segurança;

1.2.1.26. Ter capacidade de suporte de até 60 mil novas conexões/segundo;

1.2.1.27. Deve possuir a funcionalidade de acelerador WAN;

1.2.1.28. Deve possuir a capacidade de identificação de ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimentos automáticos, mesmo que necessite de licenciamento específico para esta finalidade;

1.2.1.29. Deverá ser fornecido com pelo menos 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable, com alimentação nominal 100~120AC e 210~230AC e frequência 50 ou 60 Hz.

1.2.2. Devem ser fornecidas todas as licenças de software com no mínimo as seguintes características:

1.2.2.1. A Contratada deverá fornecer licenças com validade de 60 (sessenta) meses, tal exigência é comum no mercado pois é disponível em sites de fabricantes de equipamentos o período exigido como tempo de garantia, nos serviços dos itens “a” ao “f” que compõem a solução de firewall:

a) Antivírus e antispyware;
b) Serviço de prevenção contra intrusão;
c) Controle de aplicações (aplication control);
d) Serviço de filtragem de conteúdo;
e) Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana);
f) Atualizações e upgrades de softwares e firmwares.

1.2.2.2. O licenciamento deve prover a atualização automática e em tempo real dos filtros de conteúdo WEB, através da categorização contínua de novos sites da internet, dos mecanismos de prevenção a intrusão e recursos de segurança contra novos vírus, spywares, vulnerabilidades de softwares e códigos maliciosos;

1.2.3. As atualizações e upgrades de software e firmware devem ser disponibilizadas à CONTRATANTE para download no site da CONTRATADA ou do fabricante;

1.2.4. O serviço de suporte técnico pelo período contratado deverá ser prestado através do acionamento da CONTRATADA, para atendimento das necessidades de informação e restabelecimento de funcionalidades nas condições e prazos a seguir:

1.2.4.1. SEVERIDADE BAIXA – prazo máximo de 48 horas para solução: correção de falha que não impede a continuidade da maior parte dos negócios e solicitações de informações sobre os produtos, incluindo configuração e instalação;

1.2.4.2. SEVERIDADE MÉDIA – prazo máximo de 24 horas para solução: problemas que causem impactos significativos nos negócios incluindo degradação de desempenho;

1.2.4.3. SEVERIDADE ALTA – prazo máximo de 06 horas para solução: os serviços se encontrarem indisponíveis;

1.2.5. Ocorrendo problemas técnicos ou físicos nos equipamentos cuja recuperação ao status operacional fique prejudicada, durante a vigência da garantia, a contratada deverá substituir os equipamentos envolvidos;

1.2.6. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

1.2.7. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.2.8. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que

obedeçam a todos os requisitos desta especificação;

1.2.9. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

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

1.2.11. O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;

1.2.12. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

1.2.13. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;

1.2.14. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

1.2.15. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

1.2.16. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

1.2.17. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

1.2.18. Os dispositivos de proteção de rede devem suportar sFlow;

1.2.19. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

1.2.20. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

1.2.21. Deve suportar NAT dinâmico (Many-to-1);

1.2.22. Deve suportar NAT dinâmico (Many-to-Many);

1.2.23. Deve suportar NAT estático (1-to-1);

1.2.24. Deve suportar NAT estático (Many-to-Many);

1.2.25. Deve suportar NAT estático bidirecional 1-to-1;

1.2.26. Deve suportar Tradução de porta (PAT);

1.2.27. Deve suportar NAT de Origem;

1.2.28. Deve suportar NAT de Destino;

1.2.29. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

1.2.30. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.2.31. Deve suportar NAT64 e NAT46;

1.2.32. Deve implementar balanceamento de link por hash do IP de origem;

1.2.33. Deve implementar balanceamento de link por hash do IP de origem e destino;

1.2.34. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

1.2.35. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

1.2.36. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

1.2.37. Enviar log para sistemas de monitoração externos, simultaneamente;

1.2.38. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

1.2.39. Proteção anti-spoofing;

1.2.40. Implementar otimização do tráfego entre dois equipamentos;

1.2.41. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.2.42. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.2.43. Suportar OSPF graceful restart;

1.2.44. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de

suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.2.45. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

1.2.46. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

1.2.47. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;

1.2.48. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

1.2.49. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

1.2.50. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

1.2.51. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;

1.2.52. A configuração em alta disponibilidade deve sincronizar: Sessões;

1.2.53. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

1.2.54. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

1.2.55. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

1.2.56. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

1.2.57. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

1.2.58. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

1.2.59. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

1.2.60. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

1.2.61. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

1.2.62. Controle por Política de Firewall

1.2.62.1. Deverá suportar controles por zona de segurança;

1.2.62.2. Controles de políticas por porta e protocolo;

1.2.62.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

1.2.62.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança

1.2.62.5. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

1.2.62.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

1.2.62.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

1.2.62.8. Deve descriptografar tráfego Inbound e Outbound em

conexões negociadas com TLS 1.2;

1.2.62.9. Controle de inspeção e descriptografia de SSH por política;

1.2.62.10. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.2.62.11. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

1.2.62.12. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

1.2.62.13. Suporte a objetos e regras IPV6;

1.2.62.14. Suporte a objetos e regras multicast;

1.2.62.15. Deve suportar no mínimo três tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com 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;

1.2.62.16. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.2.63. Controle de Aplicações

1.2.63.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

1.2.63.3. Reconhecer pelo menos 2200 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;

1.2.63.4. 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;

1.2.63.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

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

1.2.63.7. 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 utilização da rede Tor;

1.2.63.8. 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;

1.2.63.9. 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;

1.2.63.10. Identificar o uso de táticas evasivas via comunicações

criptografadas;

1.2.63.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

1.2.63.13. 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;

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

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

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

1.2.63.17. 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;

1.2.63.18. 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: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

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

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

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

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

1.2.63.23. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

1.2.63.24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

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

a) Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
b) Nível de risco da aplicação;
c) Categoria da aplicação.

1.2.64. Prevenção de Ameaças

1.2.64.1. 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;

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

1.2.64.3. 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, garantindo que o equipamento fique operacional mesmo fora de garantia;

1.2.64.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
1.2.64.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
1.2.64.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
1.2.64.7. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
1.2.64.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
1.2.64.9. Deve suportar granularidade nas políticas 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;
1.2.64.10. Deve permitir o bloqueio de vulnerabilidades;
1.2.64.11. Deve permitir o bloqueio de exploits conhecidos;
1.2.64.12. Deve incluir proteção contra-ataques de negação de serviços;
1.2.64.13. Deverá possuir o seguinte mecanismos de inspeção de IPS:
a) Análise de padrões de estado de conexões;
b) Análise de decodificação de protocolo;
c) Análise para detecção de anomalias de protocolo;
d) Análise heurística;
e) IP Defragmentation;
f) Remontagem de pacotes de TCP;
g) Bloqueio de pacotes malformados.
1.2.64.14. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
1.2.64.15. Detectar e bloquear a origem de portscans;
1.2.64.16. Bloquear ataques efetuados por worms conhecidos;
1.2.64.17. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
1.2.64.18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
1.2.64.19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
1.2.64.20. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
1.2.64.21. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
1.2.64.22. Suportar bloqueio de arquivos por tipo;
1.2.64.23. Identificar e bloquear comunicação com botnets;
1.2.64.24. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
1.2.64.25. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
1.2.64.26. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
1.2.64.27. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
1.2.64.28. Os eventos devem identificar o país de onde partiu a ameaça;
1.2.64.29. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

1.2.64.30. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

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

1.2.65. Filtro de URL

1.2.65.1. 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);

1.2.65.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.2.65.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

1.2.65.4. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

1.2.65.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.2.65.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

1.2.65.7. Possuir pelo menos 60 categorias de URLs;

1.2.65.8. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

1.2.65.9. Permitir a customização de página de bloqueio;

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

1.2.66. Identificação de Usuários

1.2.66.1. 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;

1.2.66.2. 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;

1.2.66.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

1.2.66.4. 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, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso;

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

1.2.66.6. Deve possuir integração com LDAP para identificação de

usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

1.2.66.7. 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);

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

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

1.2.66.10. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

1.2.66.11. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

1.2.67. QoS e Traffic Shaping

1.2.67.1. 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;

1.2.67.2. Suportar a criação de políticas de QoS e Traffic Shaping por:

a) Endereço de origem;
b) Endereço de destino;
c) Usuário e grupo;
d) Aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
e) Porta;

1.2.67.3. O QoS deve possibilitar a definição de tráfego:

a) Com banda garantida;
b) Com banda máxima;
c) De fila de prioridade;

1.2.67.4. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

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

1.2.67.6. Suportar modificação de valores DSCP para o Diffserv;

1.2.67.7. Suportar priorização de tráfego usando informação de Type of Service;

1.2.67.8. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

1.2.67.9. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

1.2.68. Filtro de Dados

1.2.68.1. Permitir a criação de filtros para arquivos e dados pré-definidos;

1.2.68.2. Os arquivos devem ser identificados por extensão e tipo;

1.2.68.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

1.2.68.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.2.68.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.2.68.6. 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;

1.2.69. Geo Localização

1.2.69.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

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

1.2.69.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

1.2.70. VPN

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

1.2.70.2. Suportar IPSec VPN;

1.2.70.3. Suportar SSL VPN;

1.2.70.4. A VPN IPSEc deve suportar:

a) 3DES;
b) Autenticação MD5 e SHA-1;
c) Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
d) Algoritmo Internet Key Exchange (IKEv1 e v2);
e) AES 128, 192 e 256 (Advanced Encryption Standard);
f) Autenticação via certificado IKE PKI

1.2.70.5. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.2.70.6. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

1.2.70.7. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

1.2.70.8. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

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

1.2.70.10. 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;

1.2.70.11. Atribuição de DNS nos clientes remotos de VPN;

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

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

1.2.70.14. Suportar leitura e verificação de CRL (certificate revocation list);

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

1.2.70.16. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma:

a) Antes do usuário autenticar na estação;
b) Após autenticação do usuário na estação;
c) Sob demanda do usuário.

1.2.70.17. Deverá manter uma conexão segura com o portal durante a sessão;

1.2.70.18. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

1.3. **Firewall tipo 2 – De pequeno porte.**

1.3.1. Estes equipamentos deverão contemplar os serviços de suporte no mínimo na modalidade 8x5 (oito horas/dia e 5 dias/semana) para o período de 60 (sessenta) meses. O equipamento ofertado deve possuir, no mínimo, as características técnicas do modelo de referência SonicWall SOHO Wireless que é utilizado pelo TRE-MA e atende atualmente os requisitos técnicos de estabelecimento de VPN (rede privada virtual) na solução instalada no TRE-MA, dentre os requisitos temos em destaque as seguintes características:

1.3.1.1. Deve possuir no mínimo 4 interfaces 10/100/1000 Gbe. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:

a) Segmento WAN, ou externo;
b) Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métrica pré-definidas pelo sistema;
c) Segmento LAN ou rede interna;
d) Segmento LAN ou rede interna podendo ser configurado com DMZ (zona desmilitarizada);
e) Segmento LAN ou rede interna ou porta de sincronismo para funcionamento em alta disponibilidade;
f) Segmento ou Zona dedicada para controle de dispositivos wireless dedicado com controle e configuração destes dispositivos;

1.3.1.2. A fonte de alimentação deve ser com operação automática entre 110/220V;

1.3.1.3. Deve possuir no mínimo 01 interface USB com suporte à conexão 3G/4G (wan failover);

1.3.1.4. Deve possuir controlador Wireless padrão 802.aa a/b/g/n;

1.3.1.5. Possuir performance de firewall SPI (Stateful Paccket Inspection) igual ou superior a 300 Mbps;

1.3.1.6. Possuir performance para inspeção de Anti-Malware integrado no mesmo appliance: 50 Mbps ou superior;

1.3.1.7. Possuir a capacidade mínima de conexões suportadas em modo firewall de 10.000 (dez mil) conexões;

1.3.1.8. Deve suportar no mínimo 1.800 novas conexões por segundo;

1.3.1.9. Deve suportar no mínimo 25 interfaces de vlan (802.1q) suportando a definição de seus endereços IP através da interface gráfica;

1.3.1.10. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, onde o mesmo deverá ser descriptografado de forma transparente a aplicação;

1.3.1.11. Possuir performance de VPN IPSEC (3DES & AES 256) de 100 Mbps ou superior;

1.3.1.12. Deve ter a capacidade de prover servidor DHCP interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;

1.3.1.13. Deve suportar no mínimo 10 túneis VPN IPSEC do tipo site-to-site já licenciados;

1.3.1.14. Deve suportar no mínimo 5 túneis VPN IPSEC do tipo client-to-site, devendo disponibilizar junto com cada equipamento no mínimo 01 licença/conexão, sem custo adicional;

1.3.1.15. Deve suportar no mínimo 10 conexões clientes tipo SSL, devendo disponibilizar junto com cada equipamento no mínimo 01 licença/conexão, sem custo adicional;

1.3.1.16. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

1.3.1.17. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client

authentication;

1.3.1.18. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda de circuito primário;

1.3.1.19. Deve permitir utilização de LDAP, AD e RADIUS;

1.3.1.20. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

1.3.1.21. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras de firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como, por exemplo, para os serviços de navegação a internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

1.3.1.22. Deve ter a capacidade de suportar no mínimo 250 usuários autenticados com serviços ativos e identificados, passando por este tipo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo;

1.3.1.23. Deve permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas de administração;

1.3.1.24. Deve possibilitar gerência remota, com interface gráfica nativa;

1.3.1.25. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do firewall através da interface gráfica remota, em tempo real;

1.3.1.26. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização;

1.3.1.27. O equipamento deverá ser baseado em hardware para firewall, não em plataforma X86 ou equivalente;

1.3.2. A CONTRATADA deverá auxiliar a CONTRATANTE em todo o processo de renovação de todas as licenças e atualização de todos os hardwares contratados, dentre eles: gerar e fornecer os arquivos necessários, executar a renovação no portal de gerência do fabricante para todos os firewalls, e demais demandas que forem necessárias;

1.4. **Serviço De Instalação/Migração e Treinamento Hands-on**

1.4.1. A licitante deverá fornecer ao Tribunal os seguintes serviços:

1.4.1.1. Treinamento para a equipe de técnicos do Tribunal composta de 5 (cinco) pessoas, podendo o treinamento ser na modalidade “in company”, com carga horária mínima de 24h;

1.4.1.2. Os serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras de firewall, configuração de VPNs entre firewall concentrador e firewalls de pequeno porte, configuração dos firewalls como roteador entre as Vlans dos usuários e dos servidores, criação de pelo menos 5 regras de firewall para pelo menos 5 servidores de aplicação, enfim, todos os serviços para a efetiva migração da solução de firewall do Tribunal até alcançar plena estabilidade operacional;

1.4.2. Tais serviços devem ser realizados obedecendo aos seguintes critérios:

1.4.2.1. **SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO**

a) A licitante vencedora deverá disponibilizar técnicos devidamente certificados junto ao fabricante da solução ofertada para realizar todos os serviços de

instalação/migração;

b) Os técnicos designados para os serviços de instalação/migração deverão possuir experiências no processo de implantação de solução de firewall, demonstrada via atestado de capacidade técnica, que deverão ser apresentados no momento de efetiva prestação dos serviços;

c) Toda configuração existente em termos de enlace de redes, VPNs, rotas, objetos e regras de firewalls, etc., deverão ser migrados para a nova solução ofertada;

d) Deverá ser criada pelo menos 5 regras de firewall para pelo menos 5 servidores de aplicações do TRE-MA;

e) Configuração de VPNs entre a solução de firewall com equipamento Contivity existente no TRE-MA;

f) Todos os serviços serão assistidos pela equipe da Seção de Suporte a Redes Locais do Tribunal, a qual dará todo o apoio e condições necessárias para a realização das atividades;

g) O serviço de instalação e migração somente serão aceitos de forma provisória quando todas as funcionalidades estiverem com status operacionais;

h) O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada;

1.4.2.2. **TREINAMENTO HANDS-ON**

a) O curso deverá abranger todos os recursos técnicos da solução ofertada em nível avançado de configuração e gerenciado da solução;

b) Deverá disponibilizar material didático oficial para cada treinamento;

c) Cada treinando que atingir as exigências do treinamento deverá receber Certificado;

d) O treinamento poderá ser realizado na modalidade “in company”, com carga horária mínima de 24 (vinte e quatro) horas;

e) Para a realização do curso deverá ser utilizado equipamentos iguais aos ofertados para fins de realização das baterias de exercícios e laboratórios;

**1.5. Solução de Gerenciamento Centralizado**

1.5.1. Deve permitir gerenciar ao menos 30 dispositivos;

1.5.2. Deve ser fornecido em virtual appliance;

1.5.3. Deverá ser compatível com ambiente VMware ESXi 5.5 e 6.0, Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e Citrix XenServer 6.0+;

1.5.4. Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;

1.5.5. Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;

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

1.5.7. Permitir acesso concorrente de administradores;

1.5.8. Possuir interface baseada em linha de comando para administração da solução de gerência

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

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

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

1.5.12. Gerar alertas automáticos via:

1.5.12.1. Email;

1.5.12.2. SNMP;

1.5.12.3. Syslog.

1.5.13. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;
1.5.14. Deve ser permitido ao administrador transferir os backups para um servidor:
1.5.14.1. FTP;
1.5.14.2. SCP;
1.5.14.3. SFTP.
1.5.15. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;
1.5.16. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através:
1.5.16.1. De contas de usuários LOCAIS;
1.5.16.2. De base externa TACACS;
1.5.16.3. De usuários de base externa LDAP;
1.5.16.4. De base externa RADIUS;
1.5.16.5. De Certificado Digital X.509 (PKI).
1.5.17. Deve suportar sincronização do relógio interno via protocolo NTP;
1.5.18. Deve registrar as ações efetuadas por quaisquer usuários;
1.5.19. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
1.5.20. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;
1.5.21. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
1.5.22. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
1.5.23. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;
1.5.24. Deve suportar XML API;
1.5.25. Deve suportar JSON API;
1.5.26. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
1.5.27. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
1.5.28. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
1.5.29. Permitir localizar quais regras um objeto está sendo utilizado;
1.5.30. Deve atribuir sequencialmente um número a cada regra de firewall;
1.5.31. Deve atribuir sequencialmente um número a cada regra de DOS;
1.5.32. Deve possuir capacidade de criação e gerenciamento de regras SD-WAN;
1.5.33. Permitir criação de regras que fiquem ativas em horário definido;
1.5.34. Permitir backup das configurações e rollback de configuração para a última configuração salva;
1.5.35. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
1.5.36. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
1.5.37. Deve permitir que todos os controladores/concentradores sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
1.5.38. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
1.5.39. A solução deve possibilitar a distribuição e instalação remota,

de maneira centralizada, de novas versões de software dos appliances;

1.5.40. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

1.5.41. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;

1.5.42. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

1.5.43. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

1.5.44. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

1.5.45. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

1.5.46. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

1.5.47. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

1.5.48. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência

1.5.49. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

1.5.50. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

1.5.51. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

1.5.52. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

1.5.53. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

**1.6. Garantia e suporte**

1.6.1. Deverá possuir garantia mínima de 60 (sessenta) meses para os equipamentos, incluindo a atualização de software (correções, “patches”, “updates” ou novas “releases”) no regime 24x7, 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, incluindo feriados e finais de semana;

1.6.2. Deverá possuir Tempo de solução, conforme a severidade especificada no subitem 1.2.4, a partir da abertura do chamado técnico para falhas de hardware ou software

1.6.3. Deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos;

1.6.4. Deverá possuir um sistema atendimento de suporte.

**1. – AVALIAÇÃO DE SOLUÇÕES**

*A solução atualmente instalada no TRE-MA foi adquirida em 2013 e é composta por: Firewall SonicWall NSA 4500, 5500 na sede do Tribunal e TZs 200/SOHO para os locais remotos, como: zonas eleitorais e postos de atendimento itinerante. Esta solução está em operação a mais de 6 anos e também com seu ciclo de vida e suporte no final, conforme documento publicado no site do fabricante no endereço: https://www.sonicwall.com/pt-br/support/product-lifecycle-tables/.*
*Considerando a temeridade de manter uma solução de segurança cujo ciclo de vida está no final, estamos propondo um pregão eletrônico para a aquisição de uma nova solução de firewall de próxima geração (Next Generation Firewall), juntamente com os firewalls de pequeno porte.*

*Foi estudada a possibilidade de atualização da solução atual pelo fabricante SonicWall, no entanto, ao enviar sua proposta, verificou-se que o custo apresentado está equiparado com outras propostas e licitações. Portanto, optamos por adquirir uma nova solução, ao invés de atualizar a solução atual. Tal escolha favorecerá a ampliação da competitividade, possibilitando que outras empresas participem, e permite também uma unificação de modelo e capacidade de processamento da solução.*

*Para o atendimento da demanda foram analisadas contratações de outros Regionais, como é o caso do Pregão Eletrônico n.º 61/2018 do Tribunal Regional Eleitoral da Bahia e do Pregão Eletrônico n.º 58/2018 do Tribunal Regional Eleitoral do Rio Grande do Sul, que tinham a mesma necessidade de substituição dos equipamentos que o TRE-MA possui. Também foram consultados fornecedores que oferecem soluções de firewall para empresas/governo.*

*A nossa solução de firewall atualmente é composta por dois fabricantes (Sonicwall e Checkpoint) a solução Sonicwall possui quatro equipamentos em alta disponibilidade (em caso de falha de um equipamento o outro assume) onde o modelo NSA 4500 é responsável pela segurança da comunicação com a internet e o modelo NSA 5500 é responsável pela segurança dentro da rede interna do Tribunal. A solução Checkpoint é responsável pela segurança na comunicação entre o TRE-MA e o TSE. No total temos 06 (seis equipamentos — funcionando em alta disponibilidade, ou seja, são redundantes e em caso de falha de um equipamento o outro assume o processamento) instalados no CPD e pretendemos reduzir este total para 04 (quatro) equipamentos em alta disponibilidade — 2 (duas) soluções de firewall (equipamento principal + equipamento de alta garantia) — que atenderiam a rede interna, o acesso à internet e a comunicação com o TSE, baseado nas especificações técnicas deste estudo.*

*Os 20 (vinte) equipamentos de firewall de pequeno porte serão adquiridos para suprir uma carência deste Tribunal de substituir três equipamentos que estão danificados, devolver três equipamentos emprestados pelo TRE-PI (patrimônios: 00034280, 00034281 e 00034282), realizar a substituição de sete firewalls Contivity 231 da Nortel que estão instalados nos postos de atendimento dos Viva Cidadãos (Imperatriz, Presidente Dutra, Shopping da Ilha, Shopping Passeio, Shopping Pátio Norte, Sítio Novo e Godofredo Viana), estes equipamentos são antigos, com 14 anos de aquisição e com tecnologia defasada, que apresentam problemas com quedas frequentes de energia, causando transtorno no atendimento dos eleitores. E também instalar três firewalls nas zonas eleitorais com links de maior velocidade como Imperatriz, Timon, Caxias e/ou Açailândia, para criar mais uma barreira para o tráfego dos dados entre a Zona Eleitoral e a secretaria. Do total de equipamentos a serem adquiridos ficariam quatro equipamentos para utilização em novas demandas, seja na substituição de um equipamento defeituoso ou em instalação de um novo ponto de comunicação entre o TRE-MA e o posto de atendimento/transmissão.*

*A obsolescência da solução utilizada pelo TRE-MA requer a aquisição de nova solução de firewall.*

*O custo da solução é baseado na pesquisa de preços na tabela abaixo onde é considerado o custo de vários fabricantes e incluso o fabricante da solução que está instalada no parque do Tribunal.*

| *Item* | *Solução de firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses* | *Solução de firewall de pequeno porte ) com instalação assistida, configuração e com garantia de 60 meses* |
|---|---|---|
| ***Preço 1*** *Ata 46/2018 Universidade Federal de São João Del-Rei* | *R$ 480.535,00* | *Não contemplado na Ata de registro de preços* |
| ***Preço 2*** *Pregão 58/2018 do Tribunal Regional* | *R$ 357.500,00* | *Não contemplado na Ata de registro de preços* |

| | | |
|---|---|---|
| *Eleitoral do Rio Grande do Sul.* | | |
| ***Preço 3*** *Ata TRE- BA nº 61/2018* | *R$ 562.500,00* | *Não contemplado na Ata de registro de preços* |
| ***Preço 4*** *Pesquisa em sítio de internet (submarino.com.br)* | | *R$ 4.553,13* |
| ***Preço 5*** *Pesquisa em sítio de internet (amazon.com.br)* | | *R$ 8.332,10* |
| ***Preço 6*** *Pesquisa em sítio de internet (lojadaniele.com.br)* | | *R$ 4.936,96* |
| ***Preço 7*** *Solus Tencologia*[1] | *R$ 483.505,33*[4] | *R$ 7.363,59* |
| ***Preço 7*** *CH Tecnologia*[2] | *R$ 395.794,86* | *R$ 9.268,16*[5] |
| ***Preço 8*** *Approach Tecnologia*[3] | *R$ 1.170.434,68* | *Não enviou valor para o item.* |
| ***Preço 9*** *Dispensa de licitação nº 10/2018 da UFRJ* | | *R$ 4.584,00* |
| ***Preço 10*** *Dispensa de licitação nº 12/2018 da IBAMA-MS* | | *R$ 4.450,00* |
| ***Preço 11*** *Pregão 44/2018 TRE-SE* | *R$ 426.695,00*[6] | *R$ 6.486,84* |
| ***Preço Médio*** | *R$ 451.088,37* | *R$ 5.815,23* |

1. *Proposta do parceiro do fabricante da solução instalada no TRE-MA.*
2. *Proposta está com o quantitativo desatualizado para o item firewall de pequeno porte e o fornecedor não atendeu à solicitação de atualização.*
3. *Valor não considerado por estar muito acima dos valores de outras pesquisas.*
4. *Foram somados "SONICWALL NSA 5650 APPLIANCE+ SONICWALL NSA 5650 HIGH AVAILABILITY+ ANALYZER SONICWALL PARA NSA 5650+ ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 5650, 5 ANOS — R$ 438.513,15" mais "SONICWALL GMS 5 NODE SOFTWARE LICENSE+ SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 5 NODES (5ANOS) — R$ 12.992,18" mais "TREINAMENTO OFICIAL SONICWALL — R$ 6.000,00" mais "IMPLEMENTAÇÃO PRESENCIAL SONICWALL — R$ 26.000,00" totalizando R$ 483.505,33.*
5. *Foram somados "XG 86 rev.1 Security Appliance (EU/UK/US power cord) — R$ 4.275,17" mais "XG 86 FullGuard with Enhanced Support — 60 Meses — R$ 4.992,99" totalizando R$ 9.268,17 e será desconsiderado por apresentar coeficiente de variação maior que 25%.*
6. *Corresponde a soma do item 1 com o item 3 do pregão (hardware e software).*
7. *Corresponde as médias dos preços (4, 5, 6, 7, 9, 10 e 11).*

**2. — ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO**

*Para o atendimento da demanda especificada no Documento de Oficialização da Demanda (PAD nº 4296/2019), opta-se pela aquisição, através de pregão eletrônico, da aquisição de uma solução de firewall de próxima geração, juntamente com os firewalls de pequeno porte.*
*Esta aquisição visa substituir a solução de firewall instalada no nosso parque, cujo ciclo de vida encontra-se no final, de modo a garantir que o tráfego de dados entre as unidades de atendimento do TRE-MA e sua segurança sejam seguras*

*mitigando as tentativas de acesso indevidos aos dados transmitidos e armazenados no TRE-MA.*

**3. — NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE**

*Não há necessidade de adequação do ambiente tendo em vista que foi suprida quando da aquisição da solução já instalada neste regional.*

**II— ANÁLISE DE RISCOS**

**4. — IDENTIFICAÇÃO DOS RISCOS**

1. *Fracassar na contratação e não ter o objeto atendido*
2. *Errar na especificação ou dimensionamento do objeto de modo que a aquisição não atenda as necessidades do TRE-MA*
3. *Especificação excessiva e consequente restrição da competitividade*
4. *Falha na execução do objeto de modo que a aquisição não atenda as necessidades do TRE-MA*

**5. — IDENTIFICAÇÃO DAS PROBABILIDADES DE OCORRÊNCIA E DOS DANOS POTENCIAIS**

1. *Probabilidade média e dano alto*
2. *Probabilidade baixa e dano alto*
3. *Probabilidade baixa e dano alto*
4. *Probabilidade média e dano alto*

**6. — DEFINIÇÃO DAS AÇÕES E RESPONSÁVEIS**

1. *Fracassar na contratação e não ter o objeto atendido*
   a. *Ação: Comprometimento das unidades envolvidas para dar celeridade ao processo de contratação e se empenharem na obtenção do sucesso do processo. Responsável: Demandante.*
   b. *Revisão dos termos da contratação ou revisão da estratégia da contratação. Responsável: Demandante, técnico e administrativo.*
2. *Errar na especificação ou dimensionamento do objeto de modo que a aquisição não atenda as necessidades do TRE-MA*
   a. *Ação: Definir requisitos que garantam a qualidade técnica da solução e homologá-las adequadamente. Responsável: Técnico.*
   b. *Dimensionar os equipamentos contemplando as demandas considerando o funcionamento do TRE-MA com as perspectivas de longo e médio prazo. Contemplar soluções tecnológicas alinhadas com o mercado futuro. Responsável: Técnico.*
3. *Especificação excessiva e consequente restrição da competitividade*
   a. *Ação: Cautela na especificação do objeto, de modo a afastar exigências que não possam ser atendidas por um conjunto de fornecedores. Responsável: Demandante, técnico e administrativo.*
4. *Falha na execução do objeto de modo que a aquisição não atenda as necessidades do TRE-MA*
   a. *Ação: Monitorar os prazos e notificar/informar a empresa em caso de descumprimento dos prazos e atendimento do edital da licitação. Responsável: Demandante e técnico.*

**III— ESTRATÉGIA PARA A CONTRATAÇÃO**

**7. — NATUREZA DO OBJETO**

*Objeto de natureza comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado. Configura uma solução de tecnologia da informação.*
*Será considerada vencedora a empresa que apresentar, além dos requisitos exigidos no Termo de Referência, a proposta com o menor preço global.*

| **8. - PARCELAMENTO DO OBJETO E FORMA DE ADJUDICAÇÃO** |
|---|
| *Opta-se pelo não parcelamento do objeto dada a necessidade de perfeita integração/compatibilidade entre o Firewall de próxima geração e os firewalls de pequeno porte, principalmente nos itens que se referem a serviços. Ou seja, garantir que um serviço disponível no item 1 seja utilizado pelo item 2, como por exemplo (IPS, Antivírus e Anti-Spyware). Evitar escolher um fornecedor de firewall que emprega estruturas de design e gerenciamento de interfaces de usuário totalmente diferentes entre gerações de produtos, complicando a implantação e trazendo curvas de aprendizado acentuadas.*<br>*Assim, em face dos obstáculos para imputar responsabilidades individualizadas, procurou-se evitar tal situação, a fim de buscar o adequado funcionamento dos itens e também salvaguardar as respectivas garantias.*<br>*Será considerada vencedora a empresa que apresentar, além dos requisitos exigidos no Termo de referência e edital, a proposta com o menor preço global. A adjudicação do objeto será, portanto, global.* |
| **9. — MODALIDADE E O TIPO DE LICITAÇÃO** |
| *O objeto da contratação pretendida possui requisitos de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado, razão por que se entende adequada a utilização do Pregão Eletrônico.* |
| **10.— CLASSIFICAÇÃO ORÇAMENTÁRIA** |
| *O orçamento para esta contratação faz parte do orçamento de manutenção geral 20GP disponível no setor Seção de Suporte a Redes Locais no Plano Interno: AREA INFORM — FUNCMANUTGER-AREA - INFORMATICA e natureza da despesa: 449052 — EQUIPAMENTOS E MATERIAL PERMANENTE* |
| **11.— VIGÊNCIA E PRAZO DE GARANTIA** |
| *O prazo de garantia será de 60 (sessenta) meses, contados da data do atesto definitivo do equipamento.* |

| **IV — CONCLUSÃO DOS ESTUDOS PRELIMINARES** | | |
|---|---|---|
| **12.— DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO** | | |
| *Declaramos a viabilidade da contratação com base nas informações levantadas neste documento.* | | |
| **Integrante Técnico** | **Integrante Demandante** | **Integrante Administrativo** |
| _____<br>Lourencio Monteiro de Melo | _____<br>Lourencio Monteiro de Melo | _____<br>Maiara da Silva Leal |