

ESPECIFICAÇÃO DE FIREWALL - LICENÇA - SUPORTE		
Tema	Item (RNP)	Obrigatório/Desejável (RNP)
Hardware	Possuir fonte 120/240 AC ou DC, redundante e hot-swappable.	Obrigatório
Hardware	Possuir cooler hot-swappable.	Obrigatório
Interfaces	Possuir no mínimo, 08 interfaces de rede 10 Gbps SFP+, 08 interfaces GE SFP e 18 portas GE RJ45, fixas e/ou disponibilizadas por meio de slot de expansão	Obrigatório
Interfaces	Possuir no mínimo, 1 (uma) interface para HA	Obrigatório
Interfaces	Possuir no mínimo, 1 (uma) interface do tipo console ou similar.	Obrigatório
Interfaces	Possuir no mínimo, 1 (uma) interface do tipo USB.	Obrigatório
Interfaces	Possuir no mínimo, 1 (uma) interface do tipo Gerenciamento.	Obrigatório
Interfaces	Permitir a visualização da console local por meio de monitor interligado diretamente à appliance;	Obrigatório
Desempenho	Os throughputs deverão ser comprovados por documento de domínio público do fabricante.	Obrigatório
Desempenho	Suporte a no mínimo 10 domínios virtuais	Obrigatório
Desempenho	Deverá suportar 10.000 políticas	Obrigatório
Desempenho	Deverá possuir throughput de Firewall de, no mínimo, 70 Gbps	
Desempenho	Deverá possuir um throughput mínimo de 9 Gbps com as seguintes funcionalidades habilitadas simultaneamente (para todas as assinaturas que a plataforma de segurança possuir, devidamente ativadas e atuantes): Firewall, IPS, Application Control e Malware Protection habilitados.	Obrigatório
Desempenho	Suporte a, no mínimo, 7.000.000 de conexões simultâneas.	Obrigatório
Desempenho	Suporte a, no mínimo, 500.000 novas conexões HTTP por segundo.	Obrigatório
Desempenho	Ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deverá estar comunicável através de uma rota.	Obrigatório
Desempenho	Caso haja falha na comunicação o firewall deverá ter a capacidade de usar rota alternativa para estabelecer a comunicação.	
Desempenho	Suportar NAT: dinâmicos, estáticos, origens e destinos simultaneamente e tradução de porta (PAT) .	Obrigatório
Desempenho	Suporte a 4094 VLANs tags 802.1q.	Obrigatório
Desempenho	Agregação de links 802.3ad e LACP.	Obrigatório
Desempenho	Políticas baseadas por rotas e encaminhamentos.	Obrigatório
Desempenho	DHCP Relay	Obrigatório
Desempenho	DHCP Server	Obrigatório
Desempenho	Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3.	Obrigatório
Desempenho	Deverá implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico.	Obrigatório
Desempenho	Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD.	Obrigatório
Desempenho	Deverá suportar em modo automático e transparente "Single Sign-On" na autenticação dos usuários do Active Directory e eDirectory.	Obrigatório
Desempenho	Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino.	Obrigatório
Desempenho	Deverá implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance deverão ser acessíveis via SNMP.	Obrigatório
Desempenho	Deverá suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64 ou Dual stack IPv4/IPv6, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEC, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação.	Obrigatório
Desempenho	Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo (HA).	Obrigatório
Desempenho	Deverá notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.	Obrigatório
Desempenho	A configuração em alta disponibilidade deverá sincronizar: - Sessões; - Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;	Obrigatório
Desempenho	- Certificados decriptografados; - Associações de Segurança das VPNs; - Tabelas FIB;	Obrigatório
Desempenho	- O HA (modo de Alta-Disponibilidade) deverá possibilitar monitoração de falha de link As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPSec e SSL, QOS, decriptografia SSL e SSH, DHCP server, DHCP relay, NAT, suporte a VLAN e protocolos de roteamento dinâmico deverão 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.	Obrigatório
Segurança	Suportar gerenciamento centralizado, com automação em um painel único.	Desejável
Segurança	Suportar o modelo de segurança de confiança zero (Zero Trust).	Obrigatório
Segurança	Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).	Obrigatório
Segurança	Suportar no mínimo 5.000 (cinco mil) clientes de VPN SSL simultâneos.	Obrigatório
Segurança	Suportar no mínimo 2.000 (dois mil) túneis de VPN IPSEC simultâneos.	Obrigatório
Segurança	Deverá permitir autenticação centralizada, tanto da rede cabeada como da rede sem fio, utilizando-se da base LDAP existente.	Obrigatório
Segurança	Reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.	Obrigatório

Segurança	A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7.	Obrigatório
Segurança	Suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários.	Obrigatório
Segurança	Deverá os registros de logs para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL.	Obrigatório
Segurança	Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs.	Obrigatório
Segurança	Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH.	Obrigatório
Segurança	Deverá implementar Proteção contra anti-spoofing	Obrigatório
Segurança	Deverá permitir bloquear sessões TCP que usem variações do 3-way handshake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos.	Obrigatório
Segurança	Deverá permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake.	Obrigatório
Segurança	Os dispositivos de proteção deverão 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 (I2) e camada 3 (I3):	Obrigatório
	- Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;	
	- Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;	
	- Modo Camada – 3 (L3), para inspeção de dados em linha e ter 16 visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; e,	
Segurança	- Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.	Obrigatório
Segurança	Deverá suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações usuários, grupos de usuários, endereço IP e redes.	Obrigatório
Segurança	Deverá suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Obrigatório
Segurança	Deverá permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs.	Obrigatório
Segurança	Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall.	Obrigatório
Segurança	Deverá permitir controle, inspeção e decriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).	Obrigatório
Segurança	Deverá permitir offload de certificado em inspeção de conexões SSL de entrada (Inbound).	Obrigatório
Segurança	Deverá permitir decriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.	Obrigatório
Segurança	Deverá permitir decriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm	Obrigatório
Segurança	Deverá permitir Controle de inspeção e de-criptografia de SSH por política.	Obrigatório
Segurança	A decriptografia de SSH deverá possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança	Obrigatório
Segurança	Deverá permitir espelhamento de tráfego decriptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras).	Obrigatório
Segurança	Deverá permitir bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg.	Obrigatório
Segurança	Deverá suportar objetos e regras IPV6.	Obrigatório
Segurança	Deverá suportar objetos e regras multicast.	Obrigatório
Segurança	Deverá permitir no mínimo 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.	Obrigatório
	Deverá suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.	
Garantia	O licenciamento deverá conter: Garantia de 3 anos para todas as peças com atendimento para o próximo dia útil;	Obrigatório
Garantia	Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções.	Obrigatório
Garantia	Durante o prazo de garantia, deverá ser possível realizar a atualização das assinaturas de proteção da solução.	Obrigatório
Serviços de suporte	Abertura de chamados técnicos por meio de Central de Atendimento (Call Center)	Obrigatório
Serviços de suporte	O suporte da fornecedor deverá estar disponível para atendimento por um período de até 60 meses.	Desejável
	O suporte da fabricante deverá estar disponível em regime 24/7 (vinte e quatro horas por dia, sete dias por semana)	Obrigatório
	SLA para solução:	
	- Crítica: Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno;	Obrigatório
Serviços de suporte	- Alta: Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;	
	- Média: Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;	
	-Baixa - Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial;	
Serviços de suporte	Disponibilização de área para download de upgrades de software e firmwares	Obrigatório
Serviços de suporte	Disponibilização de base de conhecimento atualizada, com as principais dúvidas recebidas (FAQ) informações de troubleshooting, artigos sobre configuração, entre outras informações, para consulta através da web	Obrigatório
Serviços de suporte	Realizar todo o processo de Return Merchandise Authorization (RMA) de equipamentos que estiverem dentro do período de garantia e que apresentem falhas que sejam constatados pela equipe de suporte como irreparáveis	Obrigatório
Serviços de suporte	O serviço de suporte deverá ser prestado diretamente pelo próprio fabricante. Não será aceito serviço de suporte realizado por revendas ou equivalentes.	Obrigatório
Implementação	Apoio na configuração do equipamento, na migração das regras e na "virada de chave" no dia da mudança.	Obrigatório