ANEXO I

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

LOTE 1/ ITENS	QTDE.	UND	DESCRIÇÃO DETALHADA DO OBJETO
1	01	UND	**Aquisição de Equipamento para Segurança de Rede, tipo Next Generation Firewall** **Características Gerais** • O equipamento deve se encaixar no perfil de Next Generation Firewall (NGFW) - Firewall de próxima geração; • Taxa de transferência mínima de Firewall (Para qualquer tamanho de pacote UDP): 20 Gbps; • Taxa de transferência de IPSec VPN (Com pacotes de 512 Bytes): 20 Gbps; • Conexões simultâneas: 8 milhões; • Novas sessões (TCP) por segundo: 300.000; • Capacidade mínima de inspeção SSL – HTTPS: 5 Gbps; • Capacidade para proteção combinada contra ameaças: 4 Gbps; • Deve estar com as funcionalidades habilitadas simultaneamente e devidamente atuantes com o licenciamento do item 2: Controle de Aplicação, medidas com parâmetros de Throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais; • Quantidade mínima de interfaces 1Gbps com conectores RJ-45, considerando conexão LAN, WAN, DMZ e Gerência: 8 (oito); • Quantidade mínima de slots SFP para transceptores 1GbE: 08 (Oito); • Quantidade mínima de slots SFP+ para transceptores 10GbE: 02 (Duas); • Deve possuir fonte de alimentação redundante; • Armazenamento interno mínimo de 400 GB; • Deve ter tecnologia de firewall do tipo stateful; • Deve realizar VLANs com tags padrão 802.1q; • Deve possuir suporte a agregação de links 802.3ad e LACP; • Deve realizar roteamento multicast (PIM-SM e PIM-DM); • Deve realizar DHCP relay e DHCP server; • Deve possuir suporte a sub-interfaces Ethernet lógicas;

			• Deve suportar NAT64 e NAT46; • Deve realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); • Deve realizar, para IPv6, roteamento estático e dinâmico (OSPFv3); • Deve suportar OSPF graceful restart; • Deve suportar modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede; • Deve suportar configuração de alta disponibilidade ativo/passivo ou ativo/ativo; • Deve implementar no mínimo 05 (cinco) sistemas virtuais; • 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 diferentemente; • Deve realizar controles por zona de segurança; • Deve realizar controles de políticas por porta e protocolo; • Suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; • Suportar controle de políticas por código de país (por exemplo: br, usa, uk, rus); • Suportar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (inbound) e saída (outbound); • Suportar offload de certificado em inspeção de conexões SSL de entrada (inbound); • Deve implementar objetos e regras IPv6; • Deve implementar objetos e regras multicast; • Deve realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré- definidos automaticamente. • Deve criar políticas de QoS e Traffic Shaping por endereço de origem e destino; • Deve realizar a criação de políticas de QoS e Traffic Shaping por porta; • Deve realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade; • Deve realizar QoS (Traffic Shaping) em interfaces agregadas ou redundantes; • Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;

			• Deve identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos; • Deve criar políticas por geolocalização, permitindo que o tráfego de determinado país/países seja(m) bloqueados; • Deve permitir a visualização dos países de origem e destino nos logs dos acessos. • 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; • Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas; • A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN • A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores. • A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links • A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de Saúde melhor que o link atual • A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema; • A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em: • Número de Sessões, • Volume de Tráfego, • IP de Origem e Destino e • Transbordo de Link (Spillover) • Deve criar VPN dos tipos: site-to-site e client-to-site; • Deve suportar e criar IPsec VPN e SSL VPN; • Deve suportar nativamente a criação de VPN IPsec utilizando Triple Data Encryption Standard (3DES); • Deve suportar nativamente a criação de VPN IPsec utilizando Advanced Encryption Standard (AES) 128, 192 ou 256 bits; • Deve suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1 • Deve suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-Hellman, grupos: 1, 2, 5 e 14;

			• Deve suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKE) v1 e v2; • Características Gerais do Serviço de Instalação e Configuração do Firewall • A instalação e as configurações do equipamento deve contemplar o planejamento estruturado de execução, testes e repasse de conhecimento através de documentação de conclusão do projeto “As-built”; • A fase inicial da instalação deverá conter um plano de execução que terá a composição mínima dos seguintes itens: • Posicionamento do equipamento nos bastidores/racks existentes (Bayface); • Conexões dos uplinks para planejamento do plano de face; • Diagrama lógico e físico da rede; • Visão das configurações através de descritivos de funções e protocolos de rede que serão usados; • Os procedimentos envolvidos nos processos de instalação deverão ser previamente autorizados pela CONTRATANTE; • Deverá ser obrigação da CONTRATADA a instalação física do equipamento e conexões dos cabos de rede no local indicado pela CONTRATANTE; • Serão realizadas as configurações do equipamento do ambiente de rede de acordo com as seguintes premissas: • As configurações devem ser baseadas nos padrões da indústria em conjunto com as boas práticas de mercado; • Deve-se buscar sempre a melhor organização e aplicação das configurações visando a redundância e performance dos equipamentos; • Levar em consideração situações e aplicações de rede existentes no ambiente da CONTRATANTE para melhor interoperabilidade; • Em caso de migração pela existência de rede prévia, alterações de rede existentes devem ser acordadas entre a CONTRATANTE e a CONTRATADA visando o menor tempo de inoperância da rede. • Em conjunto com a CONTRATANTE, após as configurações deverão ser realizados testes de validação da solução implantada; • Após o término das instalações e da ativação da solução, a CONTRATADA deverá em até 30 (trinta) dias corridos realizar a entrega do documento “As-Built” contendo, no mínimo, um descritivo detalhado das configurações lógicas e • físicas da rede tais como: • Diagrama contendo todos os equipamentos instalados e suas respectivas conexões;

			• Descrição dos recursos de hardware e software utilizados no equipamento; • Lista de todos os elementos instalados contendo: nome, endereço IP do equipamento, local de instalação (prédio, andar) e número de série do equipamento; • Listagem das configurações do equipamento. • Serviço de Treinamento • Todos os custos envolvidos com locomoção, realização de coffe-breaks e com a aquisição de demais materiais necessários serão de responsabilidade da CONTRATADA; • Deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente. O conteúdo abordado deve apresentar, de forma teórica e prática, as características técnicas que envolvem o novo equipamento adquirido, demonstrando como configurá-lo de acordo com a topologia, necessidades e peculiaridades do ambiente operacional da CONTRATANTE; • Deverá possuir carga horária total mínima de 32 (trinta e duas) horas; • O planejamento das datas e horários deverá ser combinado entre a CONTRATADA e a Gerência de Informações e Sistemas (GISIST) da CONTRATANTE; • Deverá ser ministrado nas dependências da CONTRATANTE, por profissional possuidor de certificação oficial do fabricante para a solução ofertada, para um público de até 5 (cinco) participantes; • Opcionalmente poderá ser ministrado em local diverso das dependências do CONTRATANTE, inclusive de forma on-line, desde que com anuência deste; • A CONTRATADA poderá utilizar o equipamento adquirido pela CONTRATANTE e informar a necessidade de equipamentos adicionais para o treinamento (ex.: servidor Windows Server ou Linux, etc.); • Disponibilizar certificado de conclusão para todos os participantes que frequentarem, no mínimo, 70% da carga horária do treinamento; **Garantia, Suporte e Licenciamento de Controle de Aplicações, IPS e Proteção Avançada contra Malware para solução Next Generation Firewall** **Informações Gerais** • Contrato de Garantia e Suporte com o fabricante do equipamento pelo período de 5 (cinco) anos; • Deve contemplar atendimento em regime 24x7 (vinte e quatro horas, sete dias por semana), acesso ao portal de suporte do fabricante, atualização de firmware e substituição de hardware em caso de defeito de fabricação. • Deve ativar as funcionalidades de Controle de Aplicações e Prevenção de Ameaças descritas a seguir.

			• Requisitos mínimos para solução de controle de aplicações: • Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo; • Deve realizar a liberação e bloqueio somente de aplicações, sem a necessidade de liberação de portas e protocolos; • Deve reconhecer, no mínimo, 1.800 (mil e oitocentas) aplicações diferentes; • Deve 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 Deep Web (ex.: rede tor); • Deve decriptografar, para tráfego criptografado SSL, pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; • Deve atualizar a base de assinaturas de aplicações automaticamente; • Deve limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/MS AD; • Deve possibilitar a solicitação de inclusão de aplicações na base de assinaturas de aplicações; • Deve garantir o funcionamento com módulos de IPS, antivírus e anti-spyware integrados no próprio appliance de firewall; • Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (antivírus e anti-spyware); • Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, anti-spyware e antivírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo; • Deve permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração; • Deve possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança; • Deve permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura; • Deve permitir o bloqueio de vulnerabilidades; • Deve permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos; • Deve incluir proteção contra-ataques de negação de serviços (DoS); • Deve possuir assinaturas específicas para a mitigação de ataques negação de

			serviços (DoS) e negação de serviço distribuído (DDoS); • Deve detectar e bloquear a origem de programas de varredura de portas (port scans); • Deve bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; • Deve possuir assinaturas para bloqueio de ataques de buffer overflow; • Deve permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti- spyware, permitindo a criação de exceções com granularidade nas configurações; • Deve permitir o bloqueio de vírus e spywares em, pelo menos, 02 (dois) dos seguintes protocolos: FTP, SMB, SMTP e POP3 e obrigatoriamente em HTTP; • Deve identificar, alertar e bloquear comunicação com botnets; • Deve 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; • Deve identificar nos eventos, o país de onde partiu a ameaça;
2	02	UND	**Transceptor Óptico SFP+ Single TX1310/RX1270nm SM - 10GbE – 10Km** **Características Gerais** • Deve ser padrão Transceptor SFP+ Óptico de alta performance para links de dados sobre uma única fibra monomodo, com alcance de 10km, transmissor no comprimento de onda 1310nm e receptor de 1270nm; • Deve suportar velocidade de 10 Gbps (Gigabit por segundo); • Deve possuir Digital Diagnostics Monitoring (DDM); • Deve possuir conector tipo LC; • Deve ser do tipo hot-plug; • Deve possuir compatibilidade com o FIREWALL ofertado, sendo fornecido pelo mesmo fabricante ou possuir os selos de qualidade CE, TUV e RoHS acrescido da customização da EEPROM para o mesmo fabricante do FIREWALL.