PREFEITURA MUNICIPAL DE ITARANA

Estado Do Espirito Santo

MODELO DE PROPOSTA DE PREÇO

PROPOSTA COMERCIAL

Pregão Eletrônico Nº 000014/2019
Empresa Proponente:
Endereço:
CNPJ:
Validade da Proposta:_____(_____) dias.

LOTE 001 - Sistema de Firewall DPI (Deep Packet Inspection)

Lote	*Especificação*	*UNID.*	*Marca / Modelo*	*Quantidade*	*Unitário*	*Valor Total*
00001	Sistema de Firewall DPI (Deep Packet Inspection) Descrição Técnica: Em appliance com no máximo 2U de altura, com kit de montagem em rack de 19”. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP. Mínimo de 512 MB de memória RAM Memória Flash para armazenamento do sistema operacional de no mínimo 32 MB. Sistema Operacional do Tipo “Harderizado” não serão aceitos. Apenas os que forem armazenados em memória flash. Fonte de alimentação interna ou externa com operação automática entre 110/220V. Possuir no mínimo 7 (set) interfaces 10/100/1000Base-TX autosense, operando em half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atender as funções de: 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 métricas pré-definidas pelo sistema; c) Segmento LAN ou rede interna; d) Segmento LAN ou rede interna podendo ser configurado como 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. Performance de Firewall SPI (Stateful Packet Inspection) igual ou superior a 600 mbps. * Metodologia de teste: Performance de analise será baseada na RFC 2544 (para firewall) Performance de Gateway de Antivírus integrado no mesmo appliance sem nenhuma limitação para analise de diferentes tamanhos de arquivos: 115mbps ou superior. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para analise de arquivos ou pacotes de dados. A atualização das assinaturas deverá ocorrer de forma automática sem nenhuma intervenção humana. Performance de IPS de 190 Mbps ou superior. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para analise de arquivos ou pacotes de dados. A atualização das assinaturas deverá ocorrer automaticamente sem a necessidade de intervenção humana. Caso o fornecedor não possa comprovar este item em documentações públicas, o mesmo deverá comprometer-se que tais testes comprovatórios serão dados em bancada com ejetor de pacotes.	UN	*Marca :* *Modelo:*	1	R$	R$

Lote	Especificação	UNID.	Marca / Modelo	Quantidade	Unitário	Valor Total
	Capacidade mínima de conexões suportadas em modo firewall deverá ser de 80.000 ou superior. Suportar no mínimo 2.000 novas conexões por segundo. Suportar no mínimo 25 interfaces de vlan (802.1q) suportando a definição de seus endereços IP através da interface gráfica; Suportar no mínimo túneis VPN IPSEC do tipo site-to-site já licenciadas; Suportar no mínimo 25 túneis VPN IPSEC do tipo client-to-site sendo no mínimo 2 (Duas) delas já licenciadas; Suportar no mínimo 2 conexões clientes do tipo SSL sem custo e 10 licenças/conexões futuras baseadas em licenciamento adicional; Não possuir limitação lógica na capacidade nós; Suportar no mínimo 100 usuários autenticados com serviços ativos e identificados pelo dispositivo de segurança de forma transparente ao mesmo, sem que seja solicitada um segundo método de autenticação como browser ou instalação de agentes em cada estação de trabalho em um único dispositivo. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo; Possuir porta console (serial) para possíveis manutenções no produto; Possibilitar o controle do tráfego para os protocolos TCP, UDP e ICMP baseados nos endereços de origem e destino e no serviço utilizado em uma comunicação; Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos e; Devem ser aplicados por usuário e por grupo e; Associado sua ação políticas de horários e dias da semana e; Podem ser associados a endereçamento IP baseados em sub-redes e; Permitindo a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime; Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa; Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada. O appliance deve permitir a utilização de políticas de Anti-Virus, Anti-Spyware e IPS/IDP e filtro de Conteúdo segmentos (todos os serviços devem ser suportados no mesmo segmento) ou por zonas de acesso ou VLANS. Ter capacidade de análise Forense e profunda de pacotes com alta capacidade de processamento sem a perca e descarte de pacotes. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/AntiSpyware. Possibilitar o controle do tráfego para os protocolos GRE, H323, SIP e IGMP baseados nos endereços origem e destino da comunicação; Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar; Prover mecanismos de proteção contra-ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com “malwares”. O recurso deverá prevenir ataques e analises aos seguintes endereços: ?? Node-local address 127.0.0.1 ?? Link-local address 169.254.0.0/24 ?? Multicast address 224.0.0.0/24 ?? Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN.					

Lote	Especificação	UNID.	Marca / Modelo	Quantidade	Unitário	Valor Total
	Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay; Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como IP Helper suportando os protocolos e portas: Time service—UDP porta 37 DNS—UDP porta 53 DHCP—UDP portas 67 e 68 Net-Bios DNS—UDP porta 137 Net-Bios Datagram—UDP porta 138 Wake On LAN—UDP porta 7 e 9 mDNS—UDP porta 5353 Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, SIP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro; Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa; Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos; Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino; Possuir mecanismo que permita conversão de portas (PAT); Possuir gerenciamento de tráfego inboud e outbound por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida. Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points); Permitir remarcação de pacotes utilizando TOS e/ou DSCP; Possuir suporte ao protocolo SNMP, através de MIB2; Possui suporte a log via syslog; Possuir suporte aos protocolos de roteamento RIP e OSPF, com configuração pela interface gráfica;					

Lote	Especificação	UNID.	Marca / Modelo	Quantidade	Unitário	Valor Total
	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. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication; Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário; 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 da administração; Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema; Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica; Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento; Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real; Possuir mecanismo de Alta Disponibilidade, com as implementações de Fail Over e Load Balance, sendo que na implementação de Load Balance o estado das conexões e sessões TCP e UDP devem ser replicadas de forma integral sem restrições de serviços como, por exemplo, tráfego multicast. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes. 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 no 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 FTP, HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD; QUANTO AS CERTIFICAÇÕES: Possuir certificações ICSA para Firewall 4.1 e VPNC. AUTENTICAÇÃO a) Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores NT e Unix, de forma simultânea; b) Permitir a utilização de LDAP, AD e RADIUS					

Lote	Especificação	UNID.	Marca / Modelo	Quantidade	Unitário	Valor Total
	c) Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo; d) 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; e) Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado; f) Possuir perfis de acesso hierárquicos; e g) Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando. h) Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão; i) Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet; WWW: a) Possuir módulo integrado ao mesmo Firewall ips (Deep Packet Inspection) para classificação de páginas web com no mínimo 56 categorias distintas, com mecanismo de atualização automática. b) Deverão ser fornecidas licenças de Filtro de Conteúdo com validade de xxx anos para cada equipamento e quantidade de usuários ilimitada, a contar da data de sua ativação. c) Controle de conteúdo filtrado por categorias de filtragem com base de dados continuamente atualizada e extensível; d) Capacidade de submissão instantânea de novos sites e palavras chaves; e) Permitir a classificação dinâmica de sites Web, URLs e domínios; f) Suporte a filtragem para, no mínimo, 56 categorias e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo,drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar , hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting; g) O administrador de política de segurança poderá definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet; h) O administrador de política de segurança poderá personalizar quais zonas de segurança, em cada um dos firewalls da rede, terão aplicadas as políticas de filtragem de WEB, e de maneira centralizada; i) O administrador poderá adicionar filtros por palavra-chave de modo específico e individual em cada um dos firewalls da rede, de forma centralizada; j) A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana. k) Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode					

Lote	Especificação	UNID.	Marca / Modelo	Quantidade	Unitário	Valor Total
	ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação. l) Possibilitar a filtragem da linguagem Javascript e de applets Java e Active-X em páginas WWW, para o protocolo HTTP; ADMINISTRAÇÃO a) 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 da administração; b) Fornecer gerência remota, com interface gráfica nativa, através do aplicativo ActiveX ou Java. c) A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos firewalls sem a necessidade de se executar várias interfaces; d) A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem; e) Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema; f) Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica; g) Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões; h) Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento; i) 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 e em forma tabular e gráfica; j) Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração. k) Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail; l) Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web); m) Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática em pelo menos três servidores web diferentes, através do protocolo FTP; LOG a) Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo; b) Prover mecanismo de consulta às informações registradas integrado à interface de administração; c) Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento e descrito no item ADMINISTRAÇÃO.					

PREFEITURA MUNICIPAL DE ITARANA

Estado Do Espirito Santo

Lote	*Especificação*	*UNID.*	*Marca / Modelo*	*Quantidade*	*Unitário*	*Valor Total*
	d) Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica; e) Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado; f) Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP; g) Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual; h) Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado; TREINAMENTO A empresa vencedora deverá fornecer treinamento durante 16 horas para capacitar até 2 (dois) técnicos em todas as funcionalidades exigidas nos descritivos para gerenciamento do firewall solicitado (Appliance, funcionalidades e gerenciamento). Ao final do treinamento todos os alunos instruídos deverão receber provas e executar testes para verificar total capacitação de gerenciamento de todas as funcionalidades do firewall de acordo com as normas e melhores práticas do fabricante.					
1 Itens				**Valor Total do Lote**	**R$**	
				Valor Total da Proposta	**R$**	

Valor Total da Proposta por Extenso:

Local e Data

_____

Nome do representante legal da empresa
Empresa:_____
CNPJ nº._____