Diligenciamento Pregão Eletrônico PE.PPSA.003/2022 - Aquisição de 2 Firewalls Appliance para a PPSA.

Editais <editais@ppsa.gov.br>

Qui, 04/08/2022 11:42

Para: licitacao@netwarebrasil.com.br <licitacao@netwarebrasil.com.br>
Cc: Ricardo.jeronymo@netwarebrasil.com.br <Ricardo.jeronymo@netwarebrasil.com.br>
Cco: Alvaro Matias Pereira <alvaro.pereira@ppsa.gov.br>;Gustavo Falquer Macabu <gustavo.macabu@ppsa.gov.br>;Anderson de Almeida Santos <anderson.santos@ppsa.gov.br>;Vitor Martelloti <vitor.connectcom@ppsa.gov.br>

Prezado Jackson, representante da empresa NETWARE TELECOMUNICAÇÕES,

Bom dia. Conforme item 18.3 do Edital em referência estamos realizando diligenciamento para o saneamento das dúvidas abaixo em relação a documentação que foi enviada em sua proposta pelo sistema ComprasNet.

Favor encaminhar as respostas a esse diligenciamento, via **arquivo PDF** no sistema ComprasNet, até as **12 hs da próxima segunda-feira, 08 de agosto de 2022, sob pena de desclassificação do pregão em referência.** Este diligenciamento encontra-se disponibilizado no site da PPSA, na página de Licitações.

Diligenciamento: Indicar, na documentação do equipamento ofertado, na sua proposta para o Pregão Eletrônico, em referência, informada através do link (https://www.sophos.com/en-us/products/next-gen-firewall), o atendimento aos subitens destacados abaixo:

1.1 - Características técnicas gerais:
- 1.1.3 - Throughput de VPN IPsec de no mínimo 1.6 Gbps;
- 1.1.4 - No mínimo 12.500 novas conexões por segundo;
- 1.1.5 - No mínimo 190.000 sessões (IPv4 ou IPv6);

1.2 - Características funcionais gerais:
- 1.2.4 - Suporte a no mínimo 1.400 regras de segurança;
- 1.2.5 - Suporte a no mínimo 1.024 NAT rules;
- 1.2.6 - Suporte a DHCP Server e Relay;
- 1.2.7 - Suporte NAT dinâmico e estático (1-to-1,1-to-many e many-to-many);
- 1.2.8 - NAT de origem e destino;
- 1.2.9 - Suporte a NAT64 e NPTv6;
- 1.2.10 - Balanceamento de link;
- 1.2.11 - Roteamento OSPF (v2/v3), BGP, PPPoE, IGMP;
- 1.2.12 - Alta disponibilidade Ativo/Ativo e Ativo/passivo, com detecções de falhas;
- 1.2.13 - Possuir características UTM (controle de tráfego, roteamento, IPS, antivírus, antispyware, QoS e shaping, filtros de pacote, conteúdo e web; no mínimo);
- 1.2.14 - O sistema de prevenção de intrusão (IPS) deverá ser capaz, no mínimo, de identificar e prevenir as seguintes ameaças: Ataque DoS, DDoS, buffer de overflow, bloqueio de pacotes mal formados, syn flood, ICMP flood, UDP flood e botnets)

1.3 – Políticas de Firewall:
- 1.3.1 - Suporte a no mínimo 40 (quarenta) zonas de segurança;
- 1.3.2 - Controle de política por porta e protocolo;
- 1.3.3 - Controle de política por aplicações e grupos dinâmicos de aplicações (divididos em características, categorias e comportamentos);
- 1.3.4 - Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 1.3.5 - Base de objetos de endereços IP com serviços da internet que sejam atualizadas de forma dinâmica.

1.4 - Controle de Aplicações:

1.4.1 - Deverá ser capaz de reconhecer aplicações independentemente da porta ou protocolo (liberação ou bloqueio da aplicação);
1.4.3 - Identificar comunicações criptografadas;
1.4.7 - Avisar ao usuário quando houver bloqueio;

1.5 - Filtro URL:

1.5.1 - Suporte a criação de políticas baseadas em URL;

1.6 – VPN:

1.6.3 - 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;
1.6.4 - O agente de VPN deve ser compatível com pelo menos Windows 10 e Windows 11;
1.6.5 - Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.

1.7 - Identificação de usuários

1.7.1 - Capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando as aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, e base de dados local;
1.7.2 - Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
1.7.3 - Criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

3- Migração do Firewall :

3.3.4 - Capacidade de Redundância: Os 2 (dois) equipamentos deverão ser configurados para que operem em redundância, garantindo alta disponibilidade. A redundância deverá ser do tipo “ativo/passivo” – Ao apresentar falha no equipamento ativo, o equipamento passivo deverá assumir como o principal.”

4- Serviço VPN :

3.4.2 - Descrever a solução ofertada (Qual serviço será oferecido ?) contendo qual serão as opções para múltiplo fator de autenticação.

5- Licenças :

3.5.1 - Descrever a solução ofertada (Qual será o pacote de licenças ?).

6- Garantia e suporte :

3.6.1 - Descrever a solução ofertada (Qual será o serviço oferecido ?).

Atenciosamente,

Editais
Licitações e Contratos
+55 21 3513-7726
editais@ppsa.gov.br
Pré-sal Petróleo
Avenida Rio Branco, 01 | 4º Andar
Centro | Rio de Janeiro | RJ
CEP:20090-003