TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS

COMPANHIA DE SANEAMENTO DE SERGIPE – DESO

PREGÃO ELETRÔNICO Nº /2018-DGC

Processo Administrativo nº /2018

1. OBJETIVO

O presente processo consiste na realização de Pregão Eletrônico para Registro de Preços visando a eventual contratação de empresa especializada, para fornecimento de equipamentos, sistemas de gestão e repositório de Logs, instalação, manutenção corretiva e preventiva, suporte técnico dos Sistemas, subscrição do fabricante da solução e assessoria técnica em Infraestrutura de redes para as unidades da DESO, conforme exigências mínimas apresentadas e descritas neste Termo de Referência.

A proposta deverá contemplar o fornecimento de todos os insumos de Hardware, Software, subscrições dos fabricantes nos principais componentes e subcomponentes que o integram objetivando garantir a total conectividade e interoperabilidade entre seus componentes, que deverão resultar na prestação dos serviços com níveis de desempenho adequados aos fins a que se destinam no contexto apresentado.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

Esta contratação visa aquisição de solução, incluindo serviços especializados, em atendimento às atuais necessidades de infraestrutura tecnológica, bem como das que advirão no futuro conforme Planejamento da COMPANHIA DE SANEAMENTO DE SERGIPE – DESO

Com o dinamismo no surgimento de novas tecnologias e a crescente demanda, tal projeto surge como resposta às necessidades permanentes em manter-se a alta disponibilidade, alto de-

sempenho, segmentação das redes, segurança lógica e controle, para que todos unidades, sistemas, dados e usuários das redes da DESO.

Os equipamentos deverão fornecer segmentação segura, controle e visibilidade em toda infraestrutura das redes de dados da DESO. A solução é de alto impacto para a produtividade e segurança das informações institucionais, sistemas e usuários. Há necessidade de contar com soluções atualizadas, serviços de vacinas e proteção às vulnerabilidades, serviços especializados de assessoria, suporte técnico e subscrições do fabricante associados.

Com esta implementação, objetiva-se ampliar qualidade de serviços de TIC para todas unidades da DESO, promovendo;

• Segmentação Segura das Redes, para trafego controlado nos segmentos internos, entre unidades e Internet.

• Maior nível de Segurança aos acessos internos e externos.

• Maior velocidade de acessos.

• Maior proteção aos dados e sistemas.

• Maior Visibilidade do Trafego das Redes.

• Controle Pró-Ativo aos incidentes, riscos e vulnerabilidades.

• Armazenamento dos Logs e Registros do Trafego da Rede.

Este processo foi definido em lote único porque os equipamentos necessitam de total integração entre si, que só é assegurada quando os equipamentos são produzidos pelo mesmo fabricante. Isso garante a eficiência e economicidade do processo. A implantação necessita ser realizada por única contratada, caso contrário, teríamos dificuldades em atribuir responsabilidades nos casos de integração, já que tudo faz parte de uma solução. Além disso, o fracionamento encareceria por demais o processo, uma vez que seríamos obrigados a adquirir mais equipamentos, sem garantia de uma completa integração dessa solução.

3. – DESCRIÇÃO DOS EQUIPAMENTOS E SERVIÇOS

3.1 – LOTE ÚNICO

ITEM	DESCRITIVO	Tipo	QUANTIDADE
1	Solução de Segmentação e Segurança de Redes.	**Tipo I**	2
2	Solução de Segmentação e Segurança de Redes	**Tipo 2**	21
3	Solução de Segmentação e Segurança de Redes	**Tipo 3**	40
4	Dispositivo de rede sem fio – WIFI	**Tipo 4**	60
5	Dispositivo de relatórios e reposição de log's centralizados	**Tipo 5**	1
6	Serviços de Instalação e Suporte – Projeto, montagem, configuração e teste. Serviços de suporte técnico remoto e Local de Solução de Segmentação e Segurança de Redes, Alta disponibilidade, Tipo 1.	**Tipo 1**	2
7	Serviços de Instalação e Suporte – Projeto, montagem, configuração e teste. Serviços de suporte técnico remoto e Local de Solução de Segmentação e Segurança de Redes Tipo 2 e Tipo 3	**Tipos 2 e 3**	61
8	Serviços de Instalação e Suporte – Projeto, montagem, configuração e teste. Serviços de suporte técnico remoto e Local de Solução Relatórios e Repositório de Logs centralizados Tipo 5	**Tipo 5**	1
9	Serviços de Instalação e Suporte – Projeto, montagem, configuração e teste. Serviços de suporte técnico remoto e Local de dispositivo de rede sem fio WIFI	**Tipo 4**	60
10	Treinamento Hands on – Teórico e Prático, 24hs em Aracaju para até 8 participantes	-	1

4. ESPECIFICAÇÕES GERIAS – SOLUÇÃO E SERVIÇOS

4.1 CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS COMUNS AOS EQUIPAMENTOS DA SOLUÇÃO **Tipo 1, Tipo 2 e Tipo 3**:

4.1.1. Solução de Segurança da Informação, Balanceamento de links, SD-WAN e Segmentação Segura das redes, deve ser baseada em appliance (equipamentos) com múltiplas funções e sistema de gestão, monitoração e repositório de Logs Centralizado;

4.1.1.1. Por Segmentação Segura entende-se a capacidade de controlar todo e qualquer fluxo de informações nas redes, realizando os roteamentos adequados, reconhecendo as aplicações, prevenindo ameaças, gerenciando a identidade dos usuários e controlando granularmente as permissões;

4.1.2. As funcionalidades de Segmentação, Balanceamento, SD-WAN e Segurança da Informação, que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam e atendam a todos os requisitos desta especificação;

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

4.1.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

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

4.1.6. Os dispositivos devem possuir suporte a VLAN Tags 802.1q;

4.1.7. Os dispositivos devem possuir suporte a agregação de links 8023ad e LACP;

4.1.8. Os dispositivos devem possuir suporte a Policy based routing ou policy based forwarding;

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

4.1.10. Os dispositivos devem possuir suporte a DHCP Relay;

4.1.11. Os dispositivos devem possuir suporte a DHCP Server;

4.1.12. Os dispositivos devem possuir suporte a Jumbo Frames;

4.1.13. Os dispositivos devem suportar subinterfaces ethernet lógicas

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

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

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

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

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

4.1.19. Deve suportar Tradução de porta (PAT);

4.1.20. Deve suportar NAT de Origem;

4.1.21. Deve suportar NAT de Destino;

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

4.1.23. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo proble-

mas de roteamento assimétrico;

4.1.24. Deve suportar NAT64 e NAT46;

4.1.25. Deve implementar o protocolo ECMP;

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

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

4.1.28. 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;

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

4.1.30. 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

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

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

4.1.33. Proteção anti-spoofing;

4.1.34. Implementar otimização do tráfego entre dois equipamentos;

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

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

4.1.37. Suportar OSPF graceful restart;

4.1.38. 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);

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1.52. 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;

4.1.53. 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;

4.1.54. 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);

4.1.55. Controle por Politica de Firewall;

4.1.56. Deverá suportar controles por zona de segurança;

4.1.57. Controles de políticas por porta e protocolo;

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

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

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

4.1.61. Controle, inspeção e descriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

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

4.1.63. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

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

4.1.65. 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;

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

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

4.1.68. Suporte a objetos e regras IPV6;

4.1.69. Suporte a objetos e regras multicast;

4.1.70. 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;

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

4.1.72. Controle de Aplicações

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

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

4.1.72.3. Reconhecer pelo menos 1700 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;

4.1.72.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebo-

ok, 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;

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

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

4.1.72.7. 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

4.1.72.8. 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;

4.1.72.9. 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 específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

4.1.72.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.1.72.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

4.1.72.13. 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;

4.1.72.14. 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;

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

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

4.1.72.17. 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

4.1.72.18. 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

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

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

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

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

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

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

4.1.72.24. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc)

4.1.72.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação

4.1.72.26. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação

4.1.73. **Prevenção de Ameaças**

4.1.73.1 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;

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

4.1.73.3. 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;

4.1.73.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.1.73.5. 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;

4.1.73.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

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

4.1.73.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.1.73.9. 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

4.1.73.10. Deve permitir o bloqueio de vulnerabilidades

4.1.73.11. Deve permitir o bloqueio de exploits conhecidos

4.1.73.12. Deve incluir proteção contra ataques de negação de serviços

4.1.73.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

4.1.73.14. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

4.1.73.15. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

4.1.73.16. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;

4.1.73.17. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

4.1.73.18. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;

4.1.73.19. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;

4.1.73.20. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP

flood, etc;

4.1.73.21. Detectar e bloquear a origem de portscans;

4.1.73.22. Bloquear ataques efetuados por worms conhecidos;

4.1.73.23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.1.73.24. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.1.73.25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.1.73.26. 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;

4.1.73.27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.1.73.28. Identificar e bloquear comunicação com botnets;

4.1.73.29. 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;

4.1.73.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

4.1.73.31. 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

4.1.73.32. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

4.1.73.33. Os eventos devem identificar o país de onde partiu a ameaça;

4.1.73.34. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms

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

4.1.73.36. 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

diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança

4.1.74. Filtro de URL

4.1.74.1. 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);

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

4.1.74.3. 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;

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

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

4.1.74.6. Possuir pelo menos 60 categorias de URLs;

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

4.1.74.8. Permitir a customização de página de bloqueio;

4.1.74.9. 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 o usuário continuar acessando o site);

4.1.75. IDENTIFICAÇÃO DE USUÁRIOS

4.1.75.1. 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;

4.1.75.2. 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;

4.1.75.3. 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;

4.1.75.4. 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 como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;

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

4.1.75.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

4.1.75.7. 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);

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

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

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

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

4.1.76. QOS E TRAFFIC SHAPING

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;

4.1.76.1 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

4.1.76.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

4.1.76.3. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

4.1.76.4. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

4.1.76.5. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

4.1.76.6. O QoS deve possibilitar a definição de tráfego com banda garantida;

4.1.76.7. O QoS deve possibilitar a definição de tráfego com banda máxima;

4.1.76.8. O QoS deve possibilitar a definição de fila de prioridade;

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

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

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

4.1.76.12. Suportar QOS (traffic-shapping), em interfaces agregadas ou redundantes;

4.1.77. Filtro de Dados

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

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

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

4.1.77.4. 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;

4.1.78. Geo Localização

4.1.78.1.Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

4.1.78.2. Possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.1.78.3. Possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

4.1.79. VPN

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

4.1.79.2. Suportar IPSec VPN;

4.1.79.3. Suportar SSL VPN;

4.1.79.4. A VPN IPSEc deve suportar 3DES;

4.1.79.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

4.1.79.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

4.1.79.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

4.1.79.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

4.1.79.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

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

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

4.1.79.12. 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;

4.1.79.13. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.1.79.14. 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;

4.1.79.15. Atribuição de DNS nos clientes remotos de VPN;

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

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

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

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

4.1.79.20. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

4.1.79.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;

4.1.79.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;

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

4.1.79.24. 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);

4.1.80. WIRELESS CONTROLLER

Ser capaz de gerenciar centralizadamente outros Pontos de Acesso do mesmo fabricante

Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless

Suportar IPv4 e IPv6 por SSID

Permitir escolher se o tráfego de cada SSID será enviado à controladora ou comutado diretamente pela interface do Access Point em determinada VLAN

Permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do Access Point

Suporte a monitoração e supressão de Ponto de Acesso indevido

Prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS

Permitir autenticar usuários da rede wireless de forma transparente em domínio Windows

Deverá permitir a visualização dos clientes wireless conectados

Deverá prover suporte a Fast Roaming

Possuir Captive Portal por SSID

Permitir configurar o bloqueio de tráfego entre SSIDs

Deverá suportar Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de AES e/ou TKIP.

Deverá suportar 802.1x através de RADIUS na controladora wireless

Permitir configurar parâmetros de rádio, como banda e canal, na controladora wireless

Possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.

Possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

Possuir proteção contra ataques do tipo ARP Poisoning na controladora wireless.

Implementar Protected Management Frames de acordo com norma WiFi alliance para 802.11ac

Possuir WIDS integrado com detecção de ataques de Broadcast De-authentication

Possuir WIDS integrado com detecção de ataques de Spoofed De-authentication

Possuir WIDS integrado com detecção de senha WEP fraca

Possuir WIDS integrado com detecção de bridge wireless

Implementar provisionamento automático de canais dos Access Points, de forma a minimizar interferência entre eles

Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points

Permitir definir em quais horários determinado SSID estará disponível

A controladora wireless deverá oferecer Firewall integrado, baseado em identidade do usuário

Possibilitar definir número máximo de clientes permitidos por SSID

Deve permitir criar, gerenciar e disponibilizar redes wireless mesh

Possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por email ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha

A comunicação entre o Access Point e a controladora wireless deve poder ser efetuada de forma criptografada.

Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois access points gerenciados

Possuir mecanismo de balanceamento de tráfego/usuários entre Access Points

Possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou radios dos Access Points

Deve permitir a identificação do firmware utilizado em cada Access Point gerenciado e permitir o upgrade via interface gráfica;

Permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa

Permitir bloquear clientes wireless que tenham sinal fraco, definindo um valor do sinal a partir do qual tais clientes serão ignorados

Deve permitir suprimir Rogue APs detectados.

Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz

Deve permitir selecionar individualmente em cada Access Point quais os SSIDs que serão propagados

Deve permitir bloquear tráfego interno entre usuários de um mesmo SSID

Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID

Deve indicar graficamente os dispositivos conectados em cada SSID, assim como a quantidade de banda consumida, tempo de conexão e login

Deve permitir visualizar as aplicações e ameaças por dispositivo wireless

Havendo licença para controle de aplicação, tal feature deve ser atualizada de forma automática

Com a devida licença, a controladora deve dispor de, no mínimo, 1000 aplicações para reconhecimento do tráfego.

A controladora wireless deve possuir interface de gerência embarcada no próprio equipamento

Prover autenticação através de TACACS+.

5. CARACTERÍSTICAS E ESPECIFICAÇÃO DA SOLUÇÃO ESPECÍFICAS POR UNIDADE

Tipo 1 – Solução de Segmentação e Segurança de Redes em ALTA Disponibilidade:

Todo licenciamento, assinaturas e subscrições, necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

Throughput de, no mínimo, 32 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote.

Suporte a, no mínimo, 7M conexões simultâneas utilizando o protocolo TCP

Suporte a, no mínimo, 250K novas conexões por segundo

Throughput de, no mínimo, 18Gbps em VPN utilizando IPSec

Estar licenciado para, ou suportar sem o uso de licença, no minimo 1K túneis de VPN IPSEC Site-to-Site simultâneos

Estar licenciado para, ou suportar sem o uso de licença, 43K túneis de clientes VPN IPSEC simultâneos

Throughput de, no mínimo, 4 Gbps de VPN SSL

Suporte a, no mínimo, 400 clientes de VPN SSL simultâneos

Suportar no mínimo 5 Gbps de throughput de IPS

Suportar no mínimo 6 Gbps de throughput de Inspeção SSL

Throughput de, no mínimo, 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

Possuir ao menos 08 interfaces RJ45 1Gbps

Possui ao menos 02 interfaces SFP+ 10Gpps

Possui ao menos 08 interfaces SFP 1Gbps

Permitir Gerenciar no mínimo 250 pontos de Acesso.

Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 domínios virtuais lógicos (Contextos) por appliance

Tipo 2 – Solução de Segmentação e Segurança de Redes:

Todo licenciamento, assinaturas e subscrições, necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

Throughput de, no mínimo, 2.0 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote.

Suporte a, no mínimo, 500K conexões simultâneas

Suporte a, no mínimo, 20K novas conexões por segundo

Throughput de, no mínimo, 200 Mbps de VPN IPSec

Estar licenciado para, ou suportar sem o uso de licença, 100 túneis de VPN IPSEC Site-to-Site simultâneos

Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de clientes VPN IPSEC simultâneos

Throughput de, no mínimo, 180 Mbps de VPN SSL

Suporte a, no mínimo, 50 clientes de VPN SSL simultâneos

Suportar no mínimo 300 Mbps de throughput de IPS

Suportar no mínimo 180 Mbps de throughput de Inspeção SSL

Throughput de, no mínimo, 150 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso

o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

Possuir ao menos 5 interfaces RJ45 1Gbps

Permitir Gerenciar no mínimo 5 Pontos de Acesso

Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 5 sistemas virtuais lógicos (Contextos) por appliance

Tipo 3 – Solução de Segmentação e Segurança de Redes:

Todo licenciamento, assinaturas e subscrições, necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

Throughput de, no mínimo, 900 Mbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote

Suporte a, no mínimo, 500K conexões simultâneas

Suporte a, no mínimo, 12K novas conexões por segundo

Throughput de, no mínimo, 50 Mbps de VPN IPSec

Estar licenciado para, ou suportar sem o uso de licença, 100 túneis de VPN IPSEC Site-to-Site simultâneos

Estar licenciado para, ou suportar sem o uso de licença, 80 túneis de clientes VPN IPSEC simultâneos

Throughput de, no mínimo, 30 Mbps de VPN SSL

Suporte a, no mínimo, 70 clientes de VPN SSL simultâneos

Suportar no mínimo 250 Mbps de throughput de IPS

Suportar no mínimo 150 Mbps de throughput de Inspeção SSL

Throughput de, no mínimo, 150 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

Possuir ao menos 05 interfaces RJ45 1Gbps

Permitir Gerenciar no mínimo 2 Pontos de Acesso

Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 5 sistemas virtuais lógicos (Contextos) por appliance

Tipo 4 – Dispositivo de Rede sem Fio – WIFI

Todo licenciamento, assinaturas e subscrições, necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

Deverá ser gerenciado por controladora de forma centralizada, pela Solução de Segmentação e Segurança de Redes Tipos I, II e III;

Deverá possuir, ao menos, 1 interface de rede 10/100/1000 RJ45;

Deverá suportar, ao menos, 16 SSIDs simultâneos por Ponto de Acesso, sendo, pelo menos, 8 por rádio;

Deverá possuir potência de transmissão de, ao menos, 20 dBm;

Deverá possuir ganho mínimo de 3 dBi por antena em 2.4 GHz e 4dBi por antena em

5 GHz;

Deverá suportar operação na temperatura de 0 a 40 ºC;

Suporte no mínimo 300 usuários por Ponto de Acesso;

Deverá ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede;

Deverá suportar os padrões 802.11a/b/g/n/ac;

Deverá possuir 2 rádios para atuar nas frequências 2.4 GHz b/g/n e 5 GHz a/n/ac simultaneamente;

Deverá possuir, ao menos, a tecnologia MIMO (Multiple-In/Multiple-Out) – 2x2;

Deverá suportar taxas de transferência nominais de, no mínimo, 300 Mbps para o padrão 802.11n e 800 Mbps para o padrão 802.11ac;

Deverá possuir PoE (Power over Ethernet), padrão 802.3af, possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta ethernet;

Deverá suportar extensão multimídia WME;

Deverá ser capaz de encontrar automaticamente a Controladora Wireless;

Deverá suportar o padrão 802.11n High-Throughput (HT) Support: HT 20/40;

Deverá suportar a criação de redes mesh;

Deverá suportar a criação de enlaces de bridge entre dois Access Point;

Deverá permitir a configuração individual para cada SSID, se o tráfego será tunelado até a controladora ao qual ele está registrado e/ou se será comutado localmente;

Deverá suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação;

Deverá suportar Adaptive Radio Resource Provisioning (ARRP);

Deverá possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais;

Deverá implementar 802.11n A-MPDU e A-MSDU packet aggregation;

Deverá implementar LPDC – Low Density Parity Checking;

Deverá implementar MLD – Maximum Likelihood Demodulation;

Deverá implementar TxBF – Transmit Beamforming;

Deverá implementar MRC – Maximum Ratio Combining.

Tipo 5 – Dispositivo de relatórios e reposição de logs centralizado:

Todo licenciamento, assinaturas e subscrições necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

A solução poderá ser entregue em forma de appliance, deve possuir padrão 19” para fixação em rack, ou virtualizado compatível com as plataformas VMware v Sphere, Xen, KVM e Hyper-V

Ser compatível com os dispositivos de especificados neste TR nos itens tipo 1,2 e 3

Possuir capacidade de receber ao menos 05 GBytes de logs diários

Possuir ao menos 03 TB de espaço de armazenamento

Funcionalidade Mínimas

Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução;

Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);

Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2

(dois) perfis para administração e monitoração;

Suportar SNMP versão 2 e versão 3 na solução de relatórios;

Deve permitir a criação de administradores que acessem todas as instâncias de virtualização da solução de relatórios;

Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

Autenticação integrada a servidor Radius;

Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela;

Autenticação integrada ao Microsoft Active Directory

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

Possuir mecanismo para que logs antigos sejam removidos automaticamente;

Permitir a importação e exportação de relatórios;

Deve possuir a capacidade de criar relatórios nos formatos PDF;

Deve ser possível exportar os logs em CSV;

Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar;

A solução deve possuir relatórios pré definidos;

Possuir envio automático de logs para um servidor FTP externo a solução;

Possibilitar a duplicação de relatórios existentes e edita-los logo após;

Possuir a capacidade de personalização de capas para os relatórios;

Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;

Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;

Possuir a capacidade de personalização de gráficos como barra, linha e tabela para in-

serção aos relatórios;

Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;

Dever ser possível fazer download dos arquivos de logs recebidos;

Deve possuir agendamento para gerar e enviar automaticamente relatórios;

Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;

Permitir o envio de maneira automática de relatórios por e-mail;

Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido;

Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;

Deve ser possível definir filtros nos relatórios;

Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;

Gerar alertas automáticos via E-mail, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros;

Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;

Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;

Deve permitir ver em tempo real os log recebidos;

Relatórios de UTM/NGFW;

Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

6. CONDIÇÕES TÉCNICAS:

Os serviços deverão prever todos os equipamentos, componentes e subcomponentes, objetivando garantir a total conectividade e interoperabilidade, que deverão resultar no perfeito funcionamento do conjunto, com níveis de desempenho adequados aos fins a que se destinam no contexto de melhorias nos Serviços de TIC da DESO.

Correrá por conta exclusiva da CONTRATADA a responsabilidade pelo deslocamento do seu(s) técnico(s) ao local da instalação e da manutenção dos equipamentos, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes.

Caso a CONTRATADA necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente neste Termo de Referência, mas necessários para atender as funcionalidades exigidas, o custo desses deverão estar inseridos no preço total ofertado.

Todos os componentes e subcomponentes objetos deste Termo de Referência deverão atuais, sem previsão de descontinuidade anunciada pelo fabricante, não se admitindo peças reparadas, com tecnologia desatualizada, ou fora de linha de produção.

A CONTRATADA deverá disponibilizar, para efeito de instalação da solução proposta, sua garantia e prestação dos serviços, incluindo manutenção corretiva, preventiva, atendimento on-site e treinamento e de acordo com os demais itens deste Termo de Referência, uma equipe com perfil técnico adequado às atividades previstas, com técnicos treinados pelo fabricante para a operação e configuração de todos os componentes ofertados.

A DESO poderá, a seu critério, em qualquer tempo, solicitar a substituição total ou parcial da equipe apresentada, caso venha a ser constatado pela DESO que a equipe disponibilizada, total ou parcialmente, não detém os conhecimentos técnicos necessários.

7. NÍVEIS DE SERVIÇO:

Para efeito dos atendimentos, suporte Técnico e resolução de problemas a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

- Plantão e Suporte de atendimento 8X5.
- Plantão e Suporte on-line 8x5 (oito horas/dia, 5 dias por semana).
- Atendimento Emergencial local para serviços indisponíveis, em até 6hs.
- Atendimento Emergencial local para indisponibilidade parcial ou degradação dos tempos de acesso e resposta dos serviços, em até 8hs.

- Atendimento para Análises, alterações de parâmetros, consulta e suporte geral em até 24hs.

Os chamados de suporte e manutenção deverão ser abertos pela DESO junto à CONTRATADA, formalmente, por escrito em ambiente WEB ou por mensagem eletrônica, ou ainda através de uma Central de Atendimento com telefone 0800 ou número local, durante toda vigência do contrato. Os serviços de abertura de chamados deverão estar disponíveis em regime 8X5.

No caso de necessidade de ações preventivas ou corretivas a DESO agendará com antecedência junto a CONTRATADA as implementações das correções, fora do horário comercial, preferencialmente em finais de semana, sem ônus para a DESO;

No caso de necessidade de ação corretiva ou danos nos HARDWARES que serão instalados compondo a solução, a CONTRATADA disponibilizará garantia do fabricante do hardware sem ônus para a DESO, com troca expressa em até 72hs.

8. DO PRAZO, VIGÊNCIA E EXECUÇÃO DOS SERVIÇOS

Da execução/prazo de entrega: Os serviços serão executados de acordo com cronograma definido pela DESO e toda Solução deverá ser entregue e instalada, em plena operação, em até 60 dias após assinatura da Ordem de Fornecimento.

Do prazo de garantia: O prazo de Garantias, Subscrições do fabricante, suporte técnico remoto e local é de 48 (quarenta e oito) meses.

9. DAS INSTALAÇÕES

A instalação de todas solução abrange todos os equipamentos, componentes e subcomponentes em suas devidas localidades, incluindo sistema de Relatoria e Repositório de Logs Centralizado de acordo com o descritivo que se segue:

Os equipamentos deverão ser entregues com seus acessórios (equipamentos e demais componentes), cabos, conectores, e demais itens necessários à sua montagem, testes e perfeito funcionamento.

A CONTRATADA deve instalar os equipamentos observando as exigências legais, orientações da equipe de TIC da DESO e conforme as práticas aplicáveis.

A solução deverá instalada em rack fornecido pela DESO, devendo dimensionar acomodação

correta a solução a ser contratado e a segurança física do ambiente.

A proponente deve submeter à aprovação da DESO, a programação de realização dos serviços.

Ficará por conta da CONTRATADA o fornecimento de todos os materiais e acessórios necessários à instalação dos equipamentos objeto destas especificações,

Os equipamentos deverão ser instalados de modo que esteja com sua capacidade e funcionalidades especificada disponível para uso imediato.

Deverão também ser providos os PATCH CABLES e/ou JUMPERS para a interligação com a rede da DESO.

Os testes e validação das funcionalidades e recursos deverão ser realizados na presença de representantes da DESO para aceite dos serviços executados.

Até 5 (cinco) dias antes do início dos serviços de instalação, a empresa CONTRATADA deverá submeter à aprovação a programação de realização dos serviços, composta de cronograma e projeto descritivo dos serviços a serem executados.

Deve estar incluso na instalação todas as configurações necessárias para o pleno funcionamento da Solução local e no contexto da Rede de Dados da DESO.

10. DO TREINAMENTO

O Treinamento será no modelo ‘Hands-on’, deverá ser realizado na cidade de Aracaju, por profissional habilitado e certificado pelo fabricante. O treinamento deverá ter uma carga horária mínima de 24hs, contendo módulos teórico e prático. Para o módulo prático deverá ser considerando o ambiente da DESO como modelo.

O Local do treinamento na cidade de Aracaju-SE, recursos audiovisuais, material didático eletrônico e recursos de laboratório será de total responsabilidade da CONTRATADA.

Até 5 (cinco) dias após o recebimento da ordem de fornecimento, a empresa CONTRATADA deverá submeter à aprovação a programação de realização do treinamento que deve iniciar em até 15 (quinze) dias após aprovação da DESO.

11. DAS OBRIGAÇÕES DAS PARTES

11.1. DA CONTRATADA

Assegurar a correta integração e funcionalidade da solução e serviços, em função do projeto e das especificações técnicas constantes neste Termo de Referência.

Efetuar inspeção/vistoria do local aonde ocorrerá as instalações, conforme indicação da DESO, para verificar os detalhes técnicos de execução, antes de elaborar o projeto.

Apresentar, ao final da instalação, o relatório de conclusão do projeto, contendo os seguintes documentos:

Memorial descritivo de todo o serviço e produtos utilizados;

Projeto com arquitetura Física e Lógicas das configurações;

Relação de garantias e Subscrições dos equipamentos;

Não transferir a outrem, no todo ou em parte, o objeto do presente Termo de Referência.

Manter toda estrutura de pessoal e ferramental necessários para execução dos serviços, independentemente da demanda definida pela DESO.

Responsabilizar-se por toda a logística (transporte e comunicação) necessária à execução dos serviços propostos, para atendimento imediato às solicitações da DESO, conforme a demanda.

Arcar com todas as despesas provenientes da limpeza dos locais de instalações e adequações necessárias.

Manter preposto para representá-la durante a execução dos serviços ora tratados, desde que aceito pela DESO.

Empregar, na execução dos serviços, a equipe técnica indicada na proposta, que poderá ser alterada mediante solicitação de autorização à DESO.

Arcar com todas as despesas, diretas ou indiretas, decorrente do cumprimento das obrigações assumidas sem qualquer ônus à DESO.

Arcar integralmente com todas as despesas inerentes à execução dos serviços, tais como, combustíveis, manutenção, seguros, taxas, impostos, tributos e salários.

Manter, durante toda a execução do contrato, as mesmas condições da habilitação e qualificação exigidas neste Termo de Referência

Efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente contrato, bem como observar e respeitar as legislações Federal, Estadual e Municipal relativas ao objeto do contrato.

Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e mão de obra para

execução dos serviços.

Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, os serviços objeto deste Contrato em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados, se for o caso, ou não correspondentes ao serviço.

Acatar as normas e condições deste Termo de Referência e seus anexos, independente de transcrição.

Disponibilizar um profissional que acompanhará as ações junto a DESO para recebimento de Ordens de Serviço, informações, contato com os técnicos responsáveis pelos serviços, coordenação, administração e supervisão do seu pessoal, bem como de qualquer comunicação junto à DESO.

Permitir e facilitar a atuação de auditores e inspetores de qualquer natureza, sempre que necessário.

Afastar ou substituir dentro de 24 (vinte e quatro) horas, sem ônus para a DESO, qualquer funcionário que, por solicitação justificada da Fiscalização, não tenha condição de continuar a participar da execução dos serviços.

11.2. DA DESO

Proporcionar à CONTRATADA todas as facilidades para que possa desempenhar o objeto do Termo de Referência de forma satisfatória.

Designar uma equipe técnica para fiscalizar e acompanhar a execução dos serviços prestados.

Avaliar e aprovar a execução dos serviços, funcionalidades da solução e a qualidade do projeto, solicitando à CONTRATADA a correção das não conformidades, sem que haja ônus para a DESO.

Promover o acesso às unidades da DESO das equipes da CONTRATADA que executarão os serviços.

Prestar as informações e os esclarecimentos que venham a ser solicitados pelos responsáveis da CONTRATADA.

Dar ciência à CONTRATADA de quaisquer modificações que venham a ocorrer.

Atestar as notas fiscais/faturas, por unidade competente, emitidas pela CONTRATADA, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactu-

adas.

12. DAS DISPOSIÇÕES GERAIS

A DESO realizará uma reunião de integração com o Fornecedor no momento da entrega do Contrato.

A CONTRATADA deverá assumir todos os custos, ônus e taxas, decorrentes do fornecimento, devendo ser previamente verificados pela empresa em sua proposta comercial. Não serão aceitos custos adicionais sob qualquer pretexto, devendo a empresa dirimir previamente todas as dúvidas e assumir inteira responsabilidade pelo fornecimento do objeto.

O adequado transporte para entrega dos materiais, no local indicado, data e prazos de fornecimento são de integral responsabilidade da CONTRATADA.

A localização das unidades da DESO poderão sofrer alterações de endereço, sem que tenha de se falar em qualquer tipo de incremento do valor contratado para a instalação inicial, tudo em acordo com as necessidades da DESO.

13. DA QUALIFICAÇÃO TÉCNICA

Apresentar documentos comprovatórios de experiência na solução apresentada:

Atestado(s) de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, certificando que a empresa tenha prestado serviços pertinentes e compatíveis com as características, quantidades e prazos similares ao objeto, Solução de Segmentação de Redes e Segurança da Informação, devidamente registrado no CREA, em nome do profissional de nível superior, legalmente habilitado, integrante do quadro(sócio e/ou funcionário) da CONTRATADA.

A licitante deve apresentar certidão de Registro ou inscrição da empresa e de seu responsável técnico no CREA, em sua plena validade.

Declaração dos fabricantes dos equipamentos, certificando a capacitação da Proponente em participar deste processo.

A Empresa proponente deve apresentar declaração de que dispõe de mão de obra adequada e disponível, local, para execução dos serviços. Deverá ser apresentado no mínimo dois técnicos, integrantes do quadro da empresa(sócio e/ou funcionário) devidamente treinados pelo fabricante das Soluções, devendo este treinamento ser comprovado por certificados de treinamento.

14. – DISPOSIÇÕES ESPECÍFICAS

14.1 - OS RECURSOS ORÇAMENTÁRIOS:

14.1.1 - Os recursos para o pagamento dos serviços objeto do Registro de Preços, provêm da previsão de Recursos Próprios da DESO, constante do Orçamento para o exercício de 2018.

14.2. Classificação Orçamentária

As despesas decorrentes do objeto desta licitação obedecerão a classificação adiante discriminada, consignada no orçamento empresarial da DESO.

Conta: **41.601.00 – EQUIPAMENTOS E BENS ADMINISTRATIVOS**

14.3 – VALIDADE DA PROPOSTA

14.3.1. O prazo de validade da proposta não pode ser inferior a 60 (sessenta) dias consecutivos, contados da data da sessão pública de abertura desta licitação.

15. DAS CONDIÇÕES DE PARTICIPAÇÃO

15.1 Poderão participar do certame todos os interessados do ramo de atividade pertinente ao objeto da contratação.

15.2 Não poderão participar os interessados que se encontrarem sob falência, concurso de credores, dissolução, liquidação, empresas estrangeiras que não funcionam no país, nem aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública, ou punidos com suspensão do direito de licitar e contratar com a Administração Pública Estadual.

15.3 Todos os equipamentos a serem fornecidos deverão ser novos, não recondicionados e/ou remanufaturados, sem qualquer uso anterior.

15.4 A participação neste certame implica aceitação de todas as condições estabelecidas neste instrumento.

16. – DAS SANÇÕES ADMINISTRATIVAS

16.1 – A contratada pelo inadimplemento de suas obrigações, garantida a prévia defesa da CONTRATADA no prazo de 10(dias) dias úteis, ficará sujeita as seguintes sanções previstas no RILC e na Lei 13.303/2016:

16.1.1 – Advertência;

16.1.2 – Multa moratória;

16.1.3 – Multa compensatória;

16.1.4 – Suspensão do direito de participar de licitação e impedimento de contatar com a DESO, pelo prazo de até 02 (dois) anos;

16.1.5 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

16.2 – As sanções constantes no subitem 16.1 poderão ser aplicadas de forma cumulativa.

16.3 – Ficará impedida de licitar e de contratar com a Administração Pública Estadual, pelo prazo de até 05 (cinco) anos, garantido o direito prévio de defesa, o fornecedor que:

16.3.1 – Ensejar o retardamento da execução do objeto desta licitação;

16.3.2 – Não mantiver proposta, injustificadamente;

16.3.3 – Comportar-se de modo inidôneo;

16.3.4 – Fizer declaração falsa;

16.3.5 – Cometer fraude fiscal;

16.3.6 – Falhar ou fraudar no fornecimento do objeto.

16.4 – São consideradas condutas reprováveis e passíveis de sanções, dentre outras, as previstas no art. 186 do RILC.

16.5- As multas estabelecidas serão entendidas como independentes e cumulativas e serão compensadas pela DESO com as importâncias em dinheiro, relativas às prestações a que corresponderem, ou da garantia do contrato, quando for o caso, cobradas judicialmente.

16.6 – A aplicação de sanção de advertência se efetiva com o registro da mesma junto ao cadastro de fornecedores e no sistema de gerenciamento de contatos da DESO, independentemente de tratar-se de pessoa cadastrada ao não.

16.7 – A multa poderá ser aplicada nos seguintes casos:

I – Em decorrência da interposição de recursos meramente procrastinatórios, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

II – Em decorrência da não regularização da documentação de habilitação, nos termos do artigo 43, § 1° da Lei Complementar n° 123/2006, a vista do subitem 11.3.6, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

III – Pela recusa em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido por este edital, poderá ser aplicada multa correspondente a 5% do valor máximo estabelecido para a licitação em questão.

IV – No caso de atraso na entrega da garantia contratual, quando exigida, o instrumento convocatório deverá prever, mediante competente justificativa, a incidência de multa correspondente 3% do valor total do contrato;

V – No caso de inexecução parcial, incidirá multa na razão de 10% sobre o valor da par-

cela não executada;

VI – No caso de inexecução total, incidirá multa na razão de 25% sobre o saldo remanescente do contrato;

VII – nos demais casos de atraso, incidirá multa na razão de 5% sobre o valor da parcela em atraso.

16.8 – Caso não haja o recolhimento da multa no prazo estipulado, a DESO descontará a referida importância de eventuais créditos a vencer da empresa contratada. Na ausência de créditos disponíveis para quitação da importância da multa, a DESO executará a garantia quando exigida, e quando for o caso, será cobrada judicialmente.

16.9 – A DESO poderá quando do não pagamento da multa pela Contratada, aplicar a sanção de suspensão do direito de participar de licitação e impedimento de contratar com a DESO, por até 02 (dois) anos;

16.10 – Cabe a sanção de suspensão em razão de ação ou omissão capaz de causar, ou que tenha causado dano à DESO, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, aplicando a disposição do art. 189 e 190 do RILC em face da legislação previdenciária, social ou trabalhista.

17. DA SUBCONTRATAÇÃO E ALTERAÇÃO SUBJETIVA

17.1 – Não será admitida a subcontratação do objeto licitatório.

17.2 – É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

18. DO CRITÉRIO DE JULGAMENTO

18.1 – O critério de julgamento será o de MENOR PREÇO DO LOTE

19. DO REGIME DE EXECUÇÃO

19.1 – O regime de execução será por PREÇO UNITÁRIO.

20. DO PAGAMENTO

O pagamento deverá ser efetuado em até 30 dias da emissão da fatura, após atesto do fiscal do contrato.

21. DO REAJUSTE

Os preços permanecerão fixos, irreajustáveis.

22.0 – DA GARANTIA CONTRATUAL

22.1 – A empresa CONTRATADA, para garantia da execução do Contrato, apresentará na 5.0.08.00/GFIN – Gerência Financeira e Contábil desta Companhia, no prazo de 20 (vinte) dias da emissão da Ordem de Fornecimento, a importância correspondente a 3 (Três por cento) do valor Contratual, em uma das seguintes modalidades:

a) Caução em Dinheiro;

b) Seguro-Garantia;

c) Fiança Bancária.

22.2 – Caso a Garantia prestada pela CONTRATADA seja em moeda corrente, será depositada em Conta a ser indicada pela DESO, a fim de se manter sua atualização financeira.

22.3 – A garantia prestada nas modalidades de Seguro-Garantia ou Fiança Bancária, deverá ser apresentada com validade de 03 meses após o término da vigência contratual.

22.4 – Fica estabelecido que a Garantia prestada não poderá ser parcelada nas faturas pagas à CONTRATADA.

22.5 – Se, por qualquer razão, durante a execução do objeto, for necessária a prorrogação do prazo de execução do Contrato, a CONTRATADA ficará obrigada a providenciar a renovação da garantia, nos mesmos termos e condições originalmente aprovados pela DESO.

22.6 – Se, no decorrer da execução do Contrato, a CONTRATADA solicitar a substituição da garantia prestada, a área gestora do Contrato deverá justificar a conveniência da substituição.

22.7 – A Garantia responderá pelo inadimplemento das condições contratuais, pela não conclusão ou conclusão incompleta dos serviços e pelas eventuais multas aplicadas, independentemente de outras cominações legais, quando for o caso.

22.8 – No caso das rescisões a devolução da Garantia somente se procederá depois de observado o art.182 §3º, e o art.183, incisos II e III do RILC.

22.9 – A garantia prestada pela CONTRATADA, será liberada pelo 5.0.08.00/GFIN, após emissão do "TERMO DE RECEBIMENTO DO MATERIAL".

22.10 – Cessará a guarda das Garantias que não forem resgatadas pela CONTRATADA, no prazo de 60 (sessenta) dias após sua liberação, cabendo a DESO a inutilização das mesmas.

23. LOCAL DE ENTREGA

23.1. LOCAL DE ENTREGA: Os Equipamentos deverão ser entregues na GTIC – Gerência de Tecnologia da Informação e Comunicação, localizada na Sede da DESO, Rua Campo Do Brito, No 331, Bairro Praia 13 de Julho, Aracaju/Se. Os equipamentos somente serão recebidos nos dias úteis.

23.2. HORÁRIOS DE ENTREGA: horários das 07h:00 às 12h:00 e das 14h:00 às

16h:00 e em hipótese alguma a DESO receberá os materiais aos Sábados,

Domingos, Feriados e dias Santos Nacionais, Estaduais e Municipais;

Aracaju, 06 de setembro de 2018.

Raimundo Santos Moura

2.0.03.00/GTIC