ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1 - SOLUÇÃO DE GERÊNCIA E SEGURANÇA DE REDE NGFW TIPO A

CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

a. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
b. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.
c. A Solução de Segurança e Gerência de Redes NGFW em Cluster de Alta Disponibilidade, deve ser composto por no mínimo 02(dois) equipamento ambos licenciados para operar em modo ATIVO-ATIVO.
d. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.
e. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.
f. Firewall com capacidade mínima de processamento de 70(setenta) Gbps.
g. IPS com capacidade mínima de processamento de 13 (treze) Gbps.
h. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 10(dez) Gbps.
i. Inspeção SSL Throughput com capacidade mínima de processamento de 8 (oito) Gbps.
j. VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec.
k. VPN SSL com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego.
l. Deverá suportar 8.000.000 (oito milhões) conexões simultâneas.
m. Deverão ser licenciados para suportar, pelo menos, 9.000 (nove mil) usuários de VPN SSL.
n. Deverá suportar, pelo menos, 500.000 (quinhentas mil) novas conexões por segundo.
o. Deverá suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.
p. Deverá suportar, pelo menos, 45.000 (quarenta e cinco mil) túneis de VPN Client-Site.
q. Deverá possuir, pelo menos, 4 (quatro) interfaces SFP28 25GE.
r. Deverá possuir, pelo menos, 4 (quatro) interfaces SFP+ 10GE.
s. Deverá possuir, pelo menos, 8 (oito) interfaces SFP 01GE.
t. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45.
u. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 500

(quinhentos) Pontos de Acesso sem fio.

v. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 90 (noventa) equipamentos.
w. Deverá incluir licença para a funcionalidade de VPN SSL.
x. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatoria”.
y. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

TREINAMENTO OFICIAL

a. Deverá ser fornecedor 04 (quatro) vouchers para treinamento Oficial do Fabricante com carga horaria mínima de 36 (trinta e seis) Horas;
b. Os vouchers deverão ter validade de pelo menos 6 (seis) meses a partir da data de sua emissão;
c. O treinamento deverá ser disponibilizado no formato EAD de acordo com o calendário de treinamentos do fabricante;
d. A capacitação técnica deverá ser oficial do fabricante e ser realizada por empresa devidamente credenciada pelo mesmo;
e. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante;
f. O conteúdo programático do treinamento deverá no mínimo os conteúdos sobre: visão geral da solução; configuração inicial do equipamento; Políticas de Firewall; IPS; Controle de Aplicação; Sandboxing; Identificação do Usuário; Filtro de Conteúdo WEB; Antivírus; NAT; VPN; QoS; SD-WAN; Alta Disponibilidade; Gerência Centralizada; Geração de Relatórios; Monitoramento;
g. A capacitação ofertada poderá ser composta por um ou mais treinamentos oficiais do fabricante;
h. Deverá(ão) ser informado(s) o(s) código(s) do(s) treinamentos junto ao fabricante e o(s) respectivo(s) conteúdo(s) programático(s);
i. O conteúdo programático deverá ser comprovado por meio de documentação oficial do fabricante;
j. O treinamento deverá ser ministrado no idioma português do Brasil;
k. Deverá ser fornecido material didático do fabricante relativo ao conteúdo programático, podendo este ser no idioma português do Brasil ou inglês;
l. Deverá ser fornecido certificado de participação ao final do treinamento. Este certificado deverá obrigatoriamente ser reconhecido pelo fabricante;
m. O conjunto das capacitações deverá ser suficiente ou corresponder ao conjunto mínimo necessário para realização de prova de certificação oficial do produto. A inscrição e/ou

custos diretos e relativos à certificação não fazem parte do voucher.

2 - SOLUÇÃO DE GERÊNCIA E SEGURANÇA DE REDE NGFW TIPO B

CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

a. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
b. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.
c. A Solução de Segurança e Gerência de Redes NGFW em Cluster de Alta Disponibilidade, deve ser composto por no mínimo 02(dois) equipamento ambos licenciados para operar em modo ATIVO-ATIVO.
d. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.
e. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.
f. Firewall com capacidade mínima de processamento de 10(dez) Gbps.
g. IPS com capacidade mínima de processamento de 2(dois) Gbps.
h. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1(um) Gbps.
i. Inspeção SSL Throughput com capacidade mínima de processamento de 1(um) Gbps.
j. VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec.
k. VPN SSL com capacidade de, pelo menos, 1 (um) Gbps de tráfego.
l. Deverá suportar 1.000.000 (um milhão) conexões simultâneas.
m. Deverão ser licenciados para suportar, pelo menos, 400 (quatrocentos) usuários de VPN SSL.
n. Deverá suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.
o. Deverá suportar, pelo menos, 1.000 (mil) túneis de VPN Site-Site.
p. Deverá suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
q. Deverá possuir, pelo menos, 2 (duas) interfaces SFP+ 10GE.
r. Deverá possuir, pelo menos, 6 (seis) interfaces SFP 01GE.

s. Deverá possuir, pelo menos, 14 (quatorze) interfaces RJ 45.
t. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 60 (sessenta) Pontos de Acesso sem fio.
u. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 30 (trinta) equipamentos.
v. Deverá incluir licença para a funcionalidade de VPN SSL.
w. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatoria”.
x. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.
y. Deverá incluir treinamento oficial do fabricante

3 - SOLUÇÃO DE GERÊNCIA E SEGURANÇA DE REDE NGFW TIPO C

CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

a. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
b. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.
c. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.
d. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
e. Firewall com capacidade mínima de processamento de 7 (sete) Gbps.
f. IPS com capacidade mínima de processamento de 1 (um) Gbps.
g. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 800 (oitocentos) Mbps.
h. Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos)

Mbps.

i. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.
j. VPN SSL com capacidade de, pelo menos, 900 (novecentos) Mbps de tráfego.
k. Deverá suportar 1.000.000 (um milhão) conexões simultâneas.
l. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.
m. Deverá suportar, pelo menos, 40.000 (quarenta mil) novas conexões por segundo.
n. Deverá suportar, pelo menos, 100 (cem) túneis de VPN Site-Site.
o. Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Client-Site.
p. Deverá possuir, pelo menos, 2 (duas) interfaces SFP 01GE.
q. Deverá possuir, pelo menos, 6 (seis) interfaces RJ 45.
r. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 45 (quarenta e cinco) Pontos de Acesso sem fio.
s. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 15 (quinze) equipamentos.
t. Deverá incluir licença para a funcionalidade de VPN SSL.
u. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatoria”.
v. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

4- **SOLUÇÃO DE GERÊNCIA E SEGURANÇA DE REDE NGFW TIPO D**

CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

a. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
b. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.
c. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.
d. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
e. Firewall com capacidade mínima de processamento de 5 (cinco) Gbps.
f. IPS com capacidade mínima de processamento de 1 (um) Gbps.
g. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de

processamento de 600 (seiscentos) Mbps.

h. Inspeção SSL Throughput com capacidade mínima de processamento de 600 (seiscentos) Mbps.
i. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.
j. VPN SSL com capacidade de, pelo menos, 800 (oitocentos) Mbps de tráfego.
k. Deverá suportar 600.000 (seiscentos mil) conexões simultâneas.
l. Deverão ser licenciados para suportar, pelo menos, 180 (cento e oitenta) usuários de VPN SSL.
m. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.
n. Deverá suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site-Site.
o. Deverá suportar, pelo menos, 400 (quatrocentos) túneis de VPN Client-Site.
p. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45.
q. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 30 (trinta) Pontos de Acesso sem fio.
r. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 15 (quinze) equipamentos.
s. Deverá incluir licença para a funcionalidade de VPN SSL.
t. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatoria”.
u. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

5- SOLUÇÃO DE GERÊNCIA E SEGURANÇA DE REDE NGFW TIPO E

CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

a. Solução baseado em appliance virtual compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud) e IBM Cloud.
b. Deverá possuir e estar licenciados com as funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, Controladora Wireless e Virtualização, pelo período de 60 (sessenta) meses.
c. Deverá suportar, pelo menos, 4 (quatro) vCPU Cores.
d. Deverá suportar, pelo menos, 1 (um) Terabyte de storage.
e. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 500 (quinhentos) Pontos de Acesso sem fio.

f. Deverá incluir licença para a funcionalidade de VPN SSL.
g. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatoria”.
h. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

6- REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS A TODOS OS MODELOS ACIMA (SOLUÇÕES DE GERÊNCIA E SEGURANÇA DE REDE – NGFW TIPO “A”, “B” , “C”, “D” e “E”)

FUNCIONALIDADES ESPECÍFICAS

a. Deve possuir controle de acesso à internet por endereço IP de origem e destino;
b. Deve possuir controle de acesso à internet por sub rede;
c. Deve suportar tags de VLAN (802.1q);
d. Deve possuir ferramenta de diagnóstico do tipo tcpdump;
e. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
f. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
g. Deve suportar single-sign-on para Active Directory, RADIUS;
h. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
i. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
j. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
k. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
l. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
m. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
n. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
o. Deve suportar aplicações multimídia, como: H.323 e SIP;
p. Deve possuir tecnologia de firewall do tipo Statefull;
q. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
r. Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;
s. Deve suportar PBR – Policy Based Routing;
t. Deve permitir a criação de VLANS no padrão IEEE 802.1q;
u. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
v. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
w. Deve permitir forwarding de camada 2 para protocolos não IP;
x. Deve suportar forwarding multicast;
y. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
z. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
aa. Deve permitir o agrupamento de serviços;
bb. Deve permitir o filtro de pacotes sem a utilização de NAT;
cc. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
dd. Deve possuir mecanismo de anti-spoofing;

ee. Deve permitir criação de regras definidas pelo usuário;
ff. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;
gg. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;
hh. Deve possuir a funcionalidade de balanceamento e contingência de links;
ii. Deve suportar sFlow;
jj. O dispositivo Deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.
kk. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
ll. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
mm. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
nn. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
oo. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
pp. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
qq. Deve suportar SIP, H.323 e SCCP NAT Traversal;
rr. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
ss. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

a. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
b. Deve permitir modificação de valores DSCP para o DiffServ;
c. Deve permitir priorização de tráfego e suportar ToS;
d. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
e. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
f. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
g. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
h. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
i. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
j. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de

origem e destino;

k. Deve ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

a. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
b. Deve possuir filtragem de e-mail por palavras chaves;
c. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
d. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;
e. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;
f. Deve ter a capacidade de permitir a criação de perfis de anti-spam específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

a. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;
b. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
c. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
d. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
e. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

→ Proxy anônimo;
→ Webmail;
→ Instituições de saúde;
→ Notícias;
→ Phishing;
→ Hackers;
→ Pornografia;
→ Racismo;
→ Websites pessoais;
→ Compras;

f. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
g. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

h. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
i. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;
j. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
k. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
l. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
m. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
n. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
o. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
p. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
q. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
r. Deve filtrar o conteúdo baseado em categorias em tempo real;
s. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
t. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
u. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
v. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;
w. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
x. Deve permitir o bloqueio de redirecionamento HTTP;
y. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
z. Deve possuir Proxy Explícito e Transparente;
aa. Deve implementar roteamento WCCP e ICAP;
bb. Deve ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

a. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
b. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
c. Deve estar orientado à proteção de redes;
d. Deve permitir funcionar em modo transparente, sniffer e router;
e. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
f. Deve permitir a criação de padrões de ataque manualmente
g. Deve possuir integração à plataforma de segurança;
h. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
i. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
j. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
k. Deve ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows;
l. Deve possuir mecanismos de detecção/proteção de ataques;
m. Deve possuir reconhecimento de padrões;
n. Deve possuir análise de protocolos;
o. Deve possuir detecção de anomalias;
p. Deve possuir detecção de ataques de RPC (Remote Procedure Call);
q. Deve possuir proteção contra-ataques de Windows ou NetBios;
r. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
s. Deve possuir proteção contra-ataques DNS (Domain Name System);
t. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
u. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
v. Deve possuir métodos de notificação de detecção de ataques;
w. Deve possuir alarmes na console de administração;
x. Deve possuir alertas via correio eletrônico;
y. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
z. Deve ter a capacidade de resposta/logs ativa a ataques;
aa. Deve prover a terminação de sessões via TCP resets;
bb. Deve armazenar os logs de sessões;
cc. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
dd. Deve mitigar os efeitos dos ataques de negação de serviços;
ee. Deve permitir a criação de assinaturas personalizadas;
ff. Deve possuir filtros de ataques por anomalias;
gg. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
hh. Deve permitir filtros de anomalias de protocolos;
ii. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
jj. Deve suportar verificação de ataque na camada de aplicação;
kk. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
ll. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

FUNCIONALIDADE DE VPN

a. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
b. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
c. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
d. Deve possuir suporte a VPN SSL;
e. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
f. A VPN SSL Deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
g. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
h. A VPN SSL Deve suportar cliente para plataforma Windows, Linux e Mac OS X;
i. Deve permitir a arquitetura de VPN hub and spoke;
j. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

a. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
b. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
c. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
d. P2P
e. Instant Messaging;
f. Web client;
g. Transferência de arquivos;
h. VoIP;
i. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
j. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
k. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
l. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
m. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
n. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
o. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
p. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
q. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
r. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
s. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
t. Deve permitir criação de padrões de aplicação manualmente;
u. Deve ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

a. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway Deve funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também Deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;
b. Deve inspecionar, no mínimo, os tráfegos de e-mail, HTTP;

c. Sobre o tráfego de e-mail, Deve inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;
d. Deve realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;
e. Deve fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;
f. Deve aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
g. Deve verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;
h. Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;
i. Deve tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;
j. Deve permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;
k. Deve permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

a. Deve permitir a criação de endereços IPs virtuais;
b. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
c. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
d. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;
e. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;
f. Deve permitir que seja mantido o IP de origem;
g. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;
h. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
i. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

FUNCIONALIDADE DE VIRTUALIZAÇÃO

a. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;
b. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;
c. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

a. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;
b. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
c. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;
d. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;
e. Deverá permitir a visualização dos clientes conectados;
f. Deverá prover suporte a Fast Roaming;

g. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;
h. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
i. Deverá possuir Captive Portal por SSID;
j. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;
k. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;
l. Deverá suportar os seguintes métodos de autenticação EAP:
m. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;
n. Deverá suportar 802.1x através de RADIUS;
o. Deverá suportar filtro baseado em endereço MAC por SSID;
p. Deverá permitir configurar parâmetros de rádio, como: banda e canal;
q. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;
r. Deverá possuir mecanismo de identificação e controle de rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;
s. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);
t. Deverá possuir WIDS com, ao menos, os seguintes perfis:

Rogue/Interfering AP Detection;

Ad-hoc Network Detection;

Wireless Bridge Detection;

Weak WEP Detection;

MAC OUI Checking;

u. Deverá permitir o uso de voz e dados sobre um mesmo SSID;
v. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
w. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;
x. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;
y. Deverá permitir a criação de políticas de traffic shaping;
z. Deverá permitir a criação de políticas de firewall baseadas em horário;
aa. Deverá permitir NAT nas políticas de firewall;
bb. Deverá possibilitar definir número de clientes por SSID;
cc. Deverá permitir e/ou bloquear o tráfego entre SSIDs;
dd. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;
ee. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;
ff. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;
gg. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;
hh. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;
ii. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;
jj. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

kk. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;
ll. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;
mm. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;
nn. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;
oo. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;
pp. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;
qq. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;
rr. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;
ss. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;
tt. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;
uu. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;
vv. Deverá possuir as seguintes certificações:
ww. Certificação Wi-Fi Alliance;
xx. Certificação ICSA para Firewall
yy. Certificação ICSA para Antivírus;
zz. Certificação ICSA para VPN SSL;
aaa. Certificação ICSA para VPN IPSec;
bbb. Certificação ICSA para IPS;
ccc. O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.
ddd.

FUNCIONALIDADE DE SD-WAN

a. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
b. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.
c. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.
d. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.
e. Solução deve ser capaz de prover Zero Touch provisioning.

f. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.
g. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.
h. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.
i. A configuração VPN IPSEC Deve oferecer suporte para DH Group: 14 e 15.
j. Reconhecimento em camada 7 totalmente segregado da camada 4.
k. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.
l. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
m. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)
n. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6
o. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
p. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.
q. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.
r. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema;
s. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

FUNCIONALIDADES DE RELATORIOS DE FIREWALL

a. Deverá possuir relatório de conformidade com o PCI DSS;
b. Deverá possuir um relatório de uso do aplicativo SaaS;
c. Deverá possuir um relatório de prevenção de perda de dados (DLP);
d. Deverá possuir um relatório de VPN;
e. Deverá possuir um relatório IPS (Intruder Prevention System);
f. Deverá possuir um relatório de reputação do cliente;
g. Deverá possuir um relatório de análise de segurança do usuário;
h. Deverá possuir um relatório de análise de ameaças cibernéticas;
i. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança;
j. Deverá possuir um relatório de tráfego DNS;
k. Deverá possuir um relatório de tráfego de e-mail;
l. Deverá possuir um relatório dos 10 principais aplicativos usados na rede;
m. Deverá possuir um relatório dos 10 principais sites usados na rede;
n. Deverá possuir um relatório de uso de mídia social;

ESCOPO DO FORNECIMENTO

a. Correrá por conta exclusiva da CONTRATADA a responsabilidade por todas as despesas de instalação inicial, bem como deslocamento dos seus técnicos ao local da instalação, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes;
b. Instalação inicial restringe-se a entrega do equipamento, conferência de itens e teste inicial de funcionamento;
c. Caso a LICITANTE 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;
d. Todos os componentes e subcomponentes objetos deste Termo de Referência deverão ser novos, de primeiro uso, sem previsão de descontinuidade anunciada, com tecnologia atualizada e avançada, em linha de produção atendendo às características técnicas presentes nos anexos deste Termo de Referência.

INSTALAÇÃO E GARANTIA

a. A CONTRATADA deverá disponibilizar a instalação dos equipamentos e sua garantia do fabricante por 60(sessenta) meses para os itens deste Termo de Referência;
b. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pelo IFS-SE presencialmente na cidade de ARACAJU e remoto nas demais unidades;
c. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pelo IFS-SE presencialmente na cidade de ARACAJU e remoto nas demais unidades;
d. Os serviços deverão ser realizados presencialmente nas dependências da unidade do IFS-SE na cidade de ARACAJU e nas demais unidades/cidades de maneira remota, utilizando-se de equipamentos e infraestrutura com capacidade operacional;
e. Os serviços deverão ser realizados por profissionais detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pelo IFS-SE;
f. Os profissionais deverão receber todas as demandas sob as responsabilidades

apresentadas pelo IFS-SE, providenciando sua inspeção, conferência, classificação e prestação de contas;

g. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pelo IFS-SE;
h. Deve ser realizado o desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; ensaios de contingência; criação de regras de segurança;
i. Deve ser realizado definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais;
j. Durante todo o período de garantia contratado, o serviço de suporte deve ser suprido 24 (vinte e quatro) horas, 07 (sete)dias por semana pelo fabricante;
k. A CONTRATADA deve disponibilizar acesso ao ambiente WEB do fabricante para download de arquivos e drivers;
l. O serviço de suporte deve proporcionar a interação com a equipe técnica do fabricante fornecendo apoio na resolução de incidentes que envolvam os componentes da oferta, garantindo seu pronto reestabelecimento.

EXIGÊNCIAS TÉCNICAS E OPERACIONAIS

a. A LICITANTE deve prever os seguintes Níveis de Serviços para garantia e suporte;
    I. Plantão técnico de suporte de atendimento do Fabricante: 24 x 7 x 365;

b. A LICITANTE não poderá transferir a outrem os compromissos assumidos, no todo ou em parte dos serviços objeto desta contratação;
c. A LICITANTE deve apresentar documentos de domínio público que comprovem todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas no Anexo A;
d. Os serviços de instalação inicial não deverão obstruir o andamento das rotinas de trabalho dos ambientes objetos de intervenção. Quando da intervenção nestes ambientes, será de responsabilidade da CONTRATADA, a recomposição total deles, deixando os locais totalmente limpos e arrumados, inclusive com relação a algum dano a eles causado quando da execução dos serviços;
e. Quando da execução dos serviços, os locais de trabalho deverão ser mantidos desobstruídos e bem-sinalizados, quando for o caso, de maneira a não comprometer a segurança daqueles que ali trafegam;
f. Após a execução dos serviços, as áreas deverão ser mantidas limpas, retirando-se toda e qualquer impureza e sobras de materiais;
g. Para facilitar os procedimentos da CONTRATANTE, a CONTRATADA deve apresentar

planilhas específicas, para cada local que foi objeto de intervenção, constando relação detalhada dos produtos efetivamente instalados, dos desempenhos esperados e especificação dos procedimentos técnicos e, se couber, dos instrumentos usualmente adotados para se efetuar os testes;

h. A recusa da aceitação dos serviços deve ser feita por escrito e conterá os elementos que motivaram a sua determinação. Assim, elencará os produtos ou serviços que estão em desacordo com as especificações e/ou os defeitos apresentados. Diante disso, a CONTRATADA se disporá a consertar, ajustar, substituir os produtos ou fazer os serviços apontados na correspondência da CONTRATANTE e no término, reapresentará o resultado;

i. Fica estabelecido que não ocorrendo nenhum comunicado da CONTRATANTE, conforme consta no item anterior, os serviços serão considerados automaticamente aceitos. Ressalva-se que fica reservado à CONTRATANTE o direito de exigir, a qualquer tempo, durante a garantia do fornecimento do serviço contratado, a substituição de qualquer acessório, componente ou produto requerido e instalado, que não apresentar as características de desempenho e funcionalidade exigidas, ou venha a apresentar falhas intermitentes não sanadas pela CONTRATADA.