CRA-BA
Conselho Regional de Administração da Bahia

Conselho Regional de Administração da Bahia

O Sistema CFA/CRAs tem como missão promover a Ciência da Administração valorizando as competências profissionais, a sustentabilidade das organizações e o desenvolvimento do país.

Administrativo
Avenida Tancredo Neves, 999 - Ed. Metropolitano Alfa - 6º andar - Salas 601/602 e 401/402, Salvador/BA, CEP 41820-021
Telefone: (71) 3311-2583 e Fax: @fax_unidade@ - www.cra-ba.org.br

Salvador, 16 de novembro de 2023.

1. ORGÃO INTERESSADO

Conselho Regional de Administração da Bahia

2. RESPONSÁVEL PELA ELABORAÇÃO DO PROJETO BÁSICO:

Joel Silva Gomes / Assessor Técnico de Tecnologia e Segurança da Informação

3. OBJETO DA CONTRATAÇÃO

Contratação de empresa especializada para locação e prestação de suporte técnico, manutenção, garantia e licenciamento de solução de segurança de redes e gerenciamento unificado de ameaças (**Firewall**) e AP'S de Rede Wi-fi da mesma marca.

Na composição mínima **02** (dois) Firewall com concentração de logs e geração de relatórios por um período mínimo de **01** (um) ano e **04** (quatro) **AP'S** de rede Wi-Fi **da mesma marca do Firewall** para atender as demandas e proteção do ambiente de rede interna de dados e recurso de TI do CRA-BA.

4. DESCRIÇÃO:

Solução de Firewall e AP'S de rede Wi-fi ambos do mesmo fabricante, suporte técnico, manutenção, garantia e licenciamento de solução de segurança de redes.

4.1. ESPECIFICAÇÕES TÉCNICAS FIREWALL

- Throughput de, no mínimo, 10 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6
- Suporte a, no mínimo, 1.400.000 conexões simultâneas
- Suporte a, no mínimo, 40.000 novas conexões por segundo
- Throughput de, no mínimo, 06 Gbps de VPN IPSec
- Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos
- Estar licenciado para, ou suportar sem o uso de licença, 600 túneis de clientes VPN IPSEC simultâneos
- Throughput de, no mínimo, 700 Mbps de VPN SSL
- Suporte a, no mínimo, 200 clientes de VPN SSL simultâneos
- Suportar no mínimo 1.3 Gbps de Throughput de IPS
- Suportar no mínimo 700 Mbps de Throughput de Inspeção SSL
- Suportar no mínimo 1.8 Gbps de throughput de Controle de Aplicação
- Suportar no mínimo 850 Mbps de throughput de NGFW
- Permitir gerenciar ao menos 40 Acess Points
- Possuir ao menos 08 interfaces 1Gbps Gigabit Ethernet do tipo RJ45

- Possuir ao menos 02 interfaces 1Gbps Gigabit Ethernet do tipo SFP;
- Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
- A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração; Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris ou GNU/Linux;
- O equipamento de firewall deve ser capaz de gerenciar de forma centralizada os switches já existentes.
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças,
- Identificação de usuários e controle granular de permissões;
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
- Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
- Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Deve implementar o protocolo ECMP;
- Deve suportar SD-WAN de forma nativa;
- Deve implementar balanceamento de link por hash do IP de origem;
- Deve implementar balanceamento de link por hash do IP de origem e destino;
- 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;
- Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais; 2.34) 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;
- Enviar log para sistemas de monitoração externos, simultaneamente;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 2.37) Proteção anti-spoofing;
- Implementar otimização do tráfego entre dois equipamentos;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Suportar OSPF graceful restart;
- O equipamento a ser ofertado deverá ser novo e estar em plena fabricação. Não serão aceitos equipamentos que possuam avisos de “End-of-life” emitidos pelo fabricante ou que estejam na iminência de serem substituídos por modelos de famílias subsequentes.

O equipamento a ser ofertado deve possuir uma plataforma otimizada para análise de conteúdo de aplicações em camada 7 do modelo OSI.
O equipamento a ser ofertado deve possuir e estar equipado com todo o hardware e as licenças de softwares necessárias para o seu correto funcionamento no ambiente do CRA-BA.
O equipamento a ser ofertado deve deverá ser fornecido em sua versão mais recente e atualizada.

O equipamento de firewall deve ser capaz de gerenciar de forma centralizada os switches já existentes.
O equipamento a ser ofertado deve suportar o gerenciamento da solução através de acesso via SSH, cliente ou WEB (HTTPS).
O equipamento a ser ofertado deve possuir dispositivos de proteção de rede com pelo menos as seguintes funcionalidades:

4.2 Suporte a DHCP Relay, DHCP Server;

O equipamento a ser ofertado deve suportar os seguintes tipos de NAT:
NAT dinâmico (Many-to-1); NAT dinâmico (Many-to-Many); NAT estático (1-to-1); NAT estático (Manyto-Many); NAT estático bidirecional 1-to-1; Tradução de porta (PAT); NAT de Origem; NAT de Destino;
O equipamento a ser ofertado deve suportar NAT de Origem e NAT de Destino simultaneamente.
O equipamento a ser ofertado deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede.
O equipamento a ser ofertado deve enviar log para sistemas de monitoração externos, simultaneamente.
O equipamento a ser ofertado deve oferecer e possuir a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL ou syslog.
O equipamento a ser ofertado deve possuir proteção anti-spoofing.
O equipamento a ser ofertado deve 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) do modelo OSI.
Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
Modo Camada – 2 (L2) do modelo OSI, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.
Modo Camada – 3 (L3) do modelo OSI, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas.
O equipamento a ser ofertado deve suportar a configuração de alta disponibilidade em pelo menos na camada 3 do modelo OSI.
O equipamento a ser ofertado deve permitir em modo HA (modo de Alta-Disponibilidade) a monitoração de falha de link.
O equipamento a ser ofertado deve suportar a configuração em alta disponibilidade possibilitando a instalação de cada membro, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP) do modelo OSI.

4.3 FUNÇÕES DE PROTEÇÃO DO SOFTWARE
4.3.1 CONTROLE DE POLÍTICAS:
O software a ser ofertado deve suportar controles por zona de segurança.
O software a ser ofertado deve possuir Controles de Políticas por porta e protocolo.
O software a ser ofertado deve possuir Controle de Políticas por Aplicações, Grupos Estáticos de Aplicações,
Grupos Dinâmicos de Aplicações (baseados em características e comportamento das aplicações) e Categorias de Aplicações.
O software a ser ofertado deve possuir Controle de Políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
O software a ser ofertado deve possuir Controle de Inspeção e de Criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
O software a ser ofertado deve suportar a Inspeção de conexões SSL de entrada (Inbound).
O software a ser ofertado deve criptografar tráfego Inbound e Outbound em conexões negociadas com TLS
1.2. O software a ser ofertado deve bloquear os seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3.

4.3.2 CONTROLE DE APLICAÇÕES:
O software a ser ofertado deve possuir em seus dispositivos de proteção de rede, a capacidade de reconhecer aplicações, independente de porta e protocolo.
O software a ser ofertado deve possuir a capacidade liberação e bloqueio pelos meios mais variados, como, por exemplo: aplicações, portas, protocolos.
O software a ser ofertado deve reconhecer aplicações diferentes, incluindo o tráfego relacionado a peer-topeer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.
O software a ser ofertado deve reconhecer no mínimo as seguintes aplicações: bittorrent, gnutella, skype,

facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, httptunnel, 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, webex , google-docs.

O software a ser ofertado deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

O software a ser ofertado deve, para o tráfego criptografado SSL, descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

O software a ser ofertado 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.

O software a ser ofertado deve identificar o uso de táticas evasivas via comunicações criptografadas;.

O software a ser ofertado deve atualizar a base de assinaturas de aplicações automaticamente.

O software a ser ofertado deve limitar a banda (download/upload) usada por aplicações (Rate Limiting), baseado no IP de origem, usuários e grupos do LDAP/AD;

O software a ser ofertado deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory (AD), permitindo, se for o caso, a instalação de agentes.

O software a ser ofertado deve permitir ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

O software a ser ofertado deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

O software a ser ofertado deve alertar o usuário quando uma aplicação for bloqueada;

O software a ser ofertado deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

O software a ser ofertado deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.:Bittorrent, emule, neonet) possuindo granularidade de controle/políticas para os mesmos.

4.3.3 IPS – Intrusion Prevention System:

O software a ser ofertado deve possuir para proteção do ambiente contra-ataques, dispositivos de proteção utilizando módulo de IPS e Anti-Malware integrados no próprio Appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

O software a ser ofertado deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos.

O software a ser ofertado deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade.

O software a ser ofertado deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão.

O software a ser ofertado deve implementar exceções por IP de origem ou de destino através de regras e de assinatura a assinatura.

O software a ser ofertado deve suportar granularidade nas políticas de IPS , possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

O software a ser ofertado deve permitir o bloqueio de vulnerabilidades.

O software a ser ofertado deve permitir o bloqueio de exploits conhecidos.

O software a ser ofertado deve incluir proteção contra ataques de negação de serviços.

O software a ser ofertado deve possuir os seguintes mecanismos de inspeção de IPS:

Análise de padrões de estado de conexões;

Análise de decodificação de protocolo;

Análise para detecção de anomalias de protocolo;

IP Defragmentation;
Remontagem de pacotes de TCP;
Bloqueio de pacotes malformados
O software a ser ofertado deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
O software a ser ofertado deve detectar e bloquear a origem de portscans.
O software a ser ofertado deve bloquear ataques efetuados por Worms conhecidos, permitindo ao administrador acrescentar novos padrões.
O software a ser ofertado deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
O software a ser ofertado deve possuir assinaturas para bloqueio de ataques de buffer overflow.
O software a ser ofertado deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
O software a ser ofertado deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações.
O software a ser ofertado deve permitir o bloqueio de vírus e Spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3.
O software a ser ofertado deve suportar bloqueio de arquivos por tipo. O software a ser ofertado deve identificar e bloquear comunicação com botnets.
O software a ser ofertado deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas: Nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
O software a ser ofertado deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
O software a ser ofertado deve incluir proteção contra vírus em conteúdo HTML e Javascript, software espião (Spyware) e Worms.
O software a ser ofertado deve possuir e implementar proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos.

4.3.4 FILTRO DE URL:
O software a ser ofertado deve possuir as funcionalidades de filtro de URL.
O software a ser ofertado deve possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
O software a ser ofertado 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.
O software a ser ofertado deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
O software a ser ofertado deve possuir base ou cache de URLs local no Appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.
O software a ser ofertado deve possuir pelo menos 60 (Sessenta) categorias de URLs.
O software a ser ofertado deve permitir a criação de categorias de URLs customizadas.
O software a ser ofertado deve possuir a função de exclusão de URLs do bloqueio, por categoria.
O software a ser ofertado deve permitir a customização de página de bloqueio.
O software a ser ofertado deve 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).

4.3.5 IDENTIFICAÇÃO DE USUÁRIOS:
O software a ser ofertado 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 base de dados local.
O software a ser ofertado 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.
O software a ser ofertado deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, Windows Server 2012.
O software a ser ofertado deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

4.3.6 FILTRO DE DADOS:
O software a ser ofertado deve permitir a criação de filtros para arquivos e dados pré- definidos.
O software a ser ofertado deve permitir que os arquivos possam ser identificados por extensão e assinaturas.
O software a ser ofertado deve identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP). Entende-se como transferência o controle de download.

4.3.7 VPN:
O software a ser ofertado deve suportar VPN Site-to-Site.
O software a ser ofertado deve suportar IPSec VPN.

A VPN IPSEc deve suportar:3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKEv1
e v2) e AES 128, 192 e 256 (Advanced Encryption Standard);
O software a ser ofertado deve suportar autenticação via certificado IKE PKI.
O software a ser ofertado deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução.

5. ESPECIFICAÇÕES TÉCNICAS AP-ROUTER

AP Indoor compatível com padrão 802.11 a/n/ac Wave 2 classe empresarial de alto rendimento.

Deve possuir pelo menos uma porta 1 Gigabit Ethernet para diversidade POE.

O AP deve fornecer varredura 24 horas por dia, 7 dias por semana em ambas as bandas 2,4 GHz e 5 GHz.

Deve ser compatível para gerenciamento através do NGFW deste Termo de Referencia;

Possui capacidade de preparação de até 16 SSIDs;

Deve ser pelo menos MIMO 2x2;

Equipamento deve ser fornecido com seu respectivo PoE Injector;

5.1 Número de antenas:
4 2.4GHz band WiFi + 8 5GHz band WiFi + I Dual band Scanning + 1 2.4GHz

5.2. Interfaces:

1 x 10/100/1000 Base-T RJ45

5.3 Transferência de dados

Deve possuir capacidade de no mínimo 400 Mbps na frequencia 2.4GHz e 800 Mbps na frequência de 5 GHz.

Deve possuir capacidade de no mínimo 200mW de TX Power na frequencia de 2.4GHz e 250mW na frequencia 5GHz;

6. CONFIGURAÇÃO INICIAL DA SOLUÇÃO:

FORNECEDOR deverá auxiliar remotamente a instalação física e as configurações iniciais do equipamento.

O FORNECEDOR informará na reunião de início de projeto as configurações que deverão ser realizadas nesta etapa e solicitar novas informações da topologia de rede, caso necessário.

O FORNECEDOR deverá realizar a configuração inicial do firewall para monitorar o tráfego de rede. A implantação deverá iniciar em no máximo 15 dias após a notificação para a execução do serviço e ser cumprida em no máximo 5 dias úteis

7. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO:

No prazo máximo de 5 (cinco) dias úteis contados da assinatura do contrato, a CONTRATADA deve apresentar:

a) cronograma dos serviços de manutenção preventiva, sendo que a primeira visita deverá ocorrer até 30 (trinta) dias após assinatura do contrato;

b) endereço eletrônico, número de telefone e/ou procedimento específico para abertura de chamados;

c) número de telefone específico e/ou endereço eletrônico para prestação do serviço de suporte técnico remoto.

Os serviços de manutenção e suporte técnico serão prestados em datas e horários pré-acordados com a CONTRATANTE, devendo a CONTRATADA comunicar ao gestor do contrato, com antecedência mínima de 2 (dois) dias úteis, a realização de quaisquer serviços que possam interferir no perfeito funcionamento do equipamento ou na rotina do ambiente de TI da CONTRATADA.

A abertura de chamados, assim como a solicitação de suporte remoto, será efetuada no regime 24 x 7, ou seja, vinte e quatro horas por dia, sete dias por semana de forma ilimitada.
Deverá ser executada pela empresa contratada uma análise da situação atual e elaborar, em conjunto com a equipe interna, um plano de ação para otimização de recursos, rotinas, procedimentos e processos para o ambiente de segurança da informação.

Essa documentação deverá ser entregue, pela empresa contratada, em formato digital;
Deverá ser oferecido treinamento hands-on de atualização tecnológica da solução implantada, com o mínimo de 8 (oito) horas, em dias úteis, nas instalações da contratante, para no mínimo 2 (dois) técnicos da CONTRATADA;

A contratada deve realizar Análise de Vulnerabilidades trimestral dos equipamentos.

Esta análise deve ser realizada por um **profissional certificação Nível 5 ou acima pelo fabricante do Firewall** da CONTRATADA.

Disponibilizar durante a vigência de contrato, um monitoramento online dos equipamentos e dos links de comunicação conectados diretamente nos equipamentos objeto desse edital, com envio de alertas automáticos por e-mail e aplicativos de mensagem instantânea.

A solução de monitoramento deve ser capaz de:
Deve coletar o uso de CPU por Core do processador
Deve ser capaz de identificar a quantidade de Core automaticamente
Deve ser capaz de coletar o processamento
Deve identificar a quantidade total de memória
Deve ser capaz de identificar o uso de memória em percentual e em MegaBytes
Deve monitorar o consumo de todas as interfaces de rede dos equipamentos, sem a necessidade de cadastro manual de interfaces pelo administrador
Coletar serial number de todos os equipamentos
Deve coletar versão de Firmware do equipamento
Deve coletar Uptime do equipamento+ Quantidade de Túneis IPsec ativos

Quantidade de usuários online através da SSL VPN
Deve identificar a quantidade de intrusões detectadas por tipo de severidade (crítica, alta, média, baixa e informação)
Deve coletar a versão de Database do IPS no equipamento
Deve coletar a quantidade de sessões IPv4 ativas
Deve identificar a versão de Sistema Operacional
Deve extrair os resultados de Performance SLA do Software-Defined WAN
Deve identificar a quantidade de pacotes com erro em cada interface;
Deve identificar a velocidade de cada interface (Gigabit ou Fastethernet)
Deve detectar e emitir alertas caso uma interface mude o status de conectada para desconectada e vice-versa
Deve ser capaz de emitir alertas caso a velocidade de rede
Deve ser capaz de alertar quando a versão de firmware for modificada
Deve ser capaz de disparar comandos remoto para o equipamento no caso de alguma condição de indisponibilidade de módulo ou condição personalizável
Deve permitir o envio de alerta em até 02 minutos após o reboot do equipamento;
Deve ser possível o envio de alertas via SMS
Deve ser possível o envio de alertas via e-mail;
Deve ser possível envio de dados via Webhook

8. Manutenção preventiva

.Entende-se como manutenção preventiva a série de procedimentos feitos de forma sistemática a fim de reduzir ou evitar falhas ou quedas no desempenho dos equipamentos, envolvendo tarefas como inspeções, instalação de versões, releases, patches, atualizações e correções de firmware e softwares em geral.
.A primeira visita presencial para realização de manutenção preventiva deverá ocorrer até 30 (trinta) dias após assinatura do contrato.

9. Manutenção corretiva

.Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar o equipamento em seu perfeito estado de uso, com eliminação de defeitos, compreendendo testes e regulagens, substituição de peças ou componentes, incluindo reparo ou troca de peças e cabos de ligação entre equipamentos, ajustes, reparos, atualizações e correções necessárias, e todas as configurações solicitadas.

.Caso ocorra substituição de peças ou componentes, a CONTRATADA deverá responsabilizar-se pela retirada dos materiais substituídos, dando-lhes destinação adequada e amparada por lei.
.A manutenção corretiva deverá ser realizada quantas vezes forem necessárias, sempre que o CRA-BA abrir chamado técnico.
.O prazo para a resolução do problema será de 8 (oito) horas após a abertura do chamado técnico.
.Se, em razão da complexidade dos reparos, for necessária a remoção do equipamento para centros de atendimento da CONTRATADA, observar-se-á o seguinte:
A remoção somente será possível mediante justificativa, devidamente aceita pela CONTRATANTE.
Todas as despesas referentes ao transporte e seguro do equipamento correrão por conta da CONTRATADA, sendo sua exclusiva responsabilidade reparar quaisquer avarias decorrentes deste transporte.
A CONTRATADA assinará termo de responsabilidade na própria autorização para saída do equipamento.
Será considerado encerrado o atendimento quando o equipamento estiver disponível para uso, em perfeitas condições de funcionamento, em seu local de instalação.

10. Suporte técnico remoto

Entende-se como suporte técnico remoto aquele efetuado mediante atendimento telefônico ou através de endereço eletrônico para a resolução de problemas e/ou esclarecimento de dúvidas sobre a configuração e utilização do equipamento.

O suporte técnico remoto será realizado preferencialmente mediante atendimento telefônico com discagem gratuita ou telefone local, com atendimento no idioma português do Brasil, por e-mail ou através de sistema de chamado disponibilizado pela CONTRATADA.

11. QUALIFICAÇÃO TÉCNICA:

Declaração informando se a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos.

Comprovação, de que o técnico responsável pelo atendimento tenha certificação Nível 5 ou acima pelo fabricante da Solução a ser suportada pelo objeto desta licitação.

A licitante deverá apresentar atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando-se a prestação dos serviços com características e complexidade semelhantes as exigidas, ou superiores.

12. JUSTIFICATIVAS

O firewall corporativo é um ativo de segurança da informação fundamental numa rede de dados empresarial, uma vez que ele regula/monitora todo o tráfego de entrada e saída na rede.

Por meio da introspecção dos dados de rede, o firewall corporativo é capaz de bloquear acessos não autorizados, mediar o uso de internet, criar conexões seguras com escritórios e clientes, bem como oferecer atualizações automáticas para ameaças de dia zero (zero-day malware).

As atuais Soluções de Firewall são tecnologias modernas que representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes confiáveis e não confiáveis (Internet) e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Isso é possível, através de um sistema de detecção de intrusões, anti-malware na camada de rede, filtragem de tráfego web malicioso e a inspeção de tráfego SSL na busca de ameaças camufladas sobre a camada de criptografia.

O CRA-BA possui uma estrutura de Firewall e Access Point antiga descontinuada para receber as atualização de segurança por parte do seu fabricante, sendo necessário atualização para os ativos mais atuais e seguros do mercado.

A opção de aquisição baseado em serviço e suporte se dá pelo praticidade de atualizações, suporte e menor custo por licenciamento anual. Nesta modalidade o CRA-BA terá a garantia de qualquer intercorrência física ou lógicas nos equipamentos será dado a devida tratativa com base no contrato firmado.

13. DO PAGAMENTO

O pagamento será efetuado por meio de boleto bancário até o 10º (décimo) dia útil após a apresentação da Nota Fiscal Fatura correspondente ao objeto, entregue e aceito pelo CRA-BA e devidamente atestada pelo setor competente, sendo efetuada a retenção de tributos e contribuições sobre os pagamentos a serem realizados, conforme determina a legislação vigente. Só serão pagos os serviços/bens efetivamente solicitados e devidamente prestados/adquiridos. O atesto só será efetuado após a confirmação de entrega dos bens ou prestação de serviços pela a empresa contratada. A contratada deverá comprovar para fins de pagamento a regularidade perante a Seguridade Social (Certidão Negativa de Débitos), o Fundo de Garantia do Tempo de Serviço – FGTS (Certificado de Regularidade de Situação do FGTS – CRF), quanto a Receita Federal e Dívida Ativa da União (Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União) e com a Justiça do Trabalho (Certidão Negativa de Débitos Trabalhistas – CNDT), e, em sendo necessário, outros documentos que sejam exigidos pelo CRA-BA, como também toda documentação necessária ao pagamento dos serviços/bens.

Salvador, 16 de Novembro de 2023

Joel Silva Gomes
Assessor Técnico de Tecnologia e Segurança da Informação

Documento assinado eletronicamente por **Joel Silva Gomes**, **Assessor(a) de Desenvolvimento de Tecnologia da Informação**, em 16/11/2023, às 10:04, conforme horário oficial de Brasília.

A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **2286131** e o código CRC **F2C57ABC**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 476901.004712/2023-99 SEI nº 2286131