

Estudo Técnico Preliminar 18/2023

1. Informações Básicas

Número do processo: 23066.017887/2023-19

2. Descrição da necessidade

2.1 OBJETO

Contratação de empresa especializada no fornecimento de solução de segurança da informação (Firewall). Pretende-se com o Estudo Técnico Preliminar, verificar a forma mais vantajosa de se estabelecer a contratação de empresa especializada no fornecimento de solução de segurança da informação (Firewall) para proteção de acessos à rede LAN (interna) e WAN (externa), no intuito de garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Universidade Federal da Bahia - UFBA, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação dessa Universidade.

Atualmente, a UFBA utiliza a solução (appliance) de Firewall “ **FortiGate-3200D e FortiAnalyzer-2000E**” da empresa Fortinet;

ITEM	PART NUMBER	DESCRIÇÃO / MODELO	MARCA / MODELO	QTD
01	FG3K2D3Z17800025 / FG3K2D3Z17800027	8x10 GE SFP + slots, 2x GE RJ45 Gestão, SPU NP6 e CP8 aceleração de hardware, SSD de 960 GB de armazenamento a bordo, e dual fontes de alimentação DC com licenciamento Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 FortiCare)	Fortinet / FortiGate-3200D	02
02	FL-2KE3R17000151	FortiAnalyzer-2000E gerenciador de logs, análise e plataforma de relatórios, fornecendo às organizações um painel único orquestração, automação e resposta para segurança simplificada operações, identificação proativa e remediação de riscos, e visibilidade completa de toda a superfície de ataque	Fortinet / FortiAnalyzer-2000E	01

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Redes e Infraestrutura (CRI)	Edmilson Nascimento

4. Necessidades de Negócio

A necessidade da contratação decorre da finalização da garantia dos equipamentos que compõem o Datacenter da Universidade Federal da Bahia. Equipamentos adquiridos no ano de 2017 e que se encontram em pleno funcionamento. Essa solução de segurança instalada na STI/UFBA é responsável pela inspeção do tráfego da rede interna e da Internet, prevenindo intrusões e permitindo o acesso remoto seguro e provendo a infraestrutura necessária para a prestação de diversos serviços na Universidade. Uma possível falha nesses equipamentos acarretaria em prejuízos para toda a rede UFBA.

É política da STI manter os equipamentos de TI de seu Datacenter cobertos por garantia que possibilite o suporte rápido e eficiente em caso emergencial. Atualmente a UFBA possui uma comunidade de usuários altamente dependentes dos serviços instalados nestes equipamentos, oferecidos pela STI. A quebra destes equipamentos e a lentidão para o reparo dos mesmos podem gerar impactos bastante negativos para a comunidade.

Com essa aquisição pretende-se garantir:

- a) Preservação da integridade e da confidencialidade dos dados dos usuários, sejam eles docentes, discentes e técnicos administrativos em educação desta Universidade para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018); e
- b) Autenticação e rastreabilidade das informações de acesso dos usuários, sejam eles docentes, discentes e técnicos administrativos em educação desta Universidade pelo período mínimo de 01 ano de acordo com o Marco Civil da Internet Lei nº 12.965/2014.

Por este motivo, torna-se imprescindível, pelos critérios de eficiência e economicidade, manter tal solução atualizada, com novo processo licitatório para contratação de empresa especializada no fornecimento de equipamentos de segurança, de maneira a permitir a escalabilidade das soluções de TIC na UFBA.

5. Necessidades Tecnológicas

5.1.1. O Firewall deverá suportar e estar licenciado para o uso das diversas ferramentas de segurança incluídas em um Next Generation Firewall, como Antivírus, IPS, Filtragem Web, Controle de Aplicações, Proteção contra Botnets, Proteção contra Malwares Avançados e AntiSpam de Gateway.

5.1.2. O equipamento deverá ser fornecido com licenciamento 24x7 FortiCare Premium, para habilitar todas as funcionalidades descritas neste Termo de Referência por 36 meses;

5.1.3. A solução a ser fornecida deverá ser preferencialmente compatível com a ferramenta FortiAnalyzer-2000E, atualmente em uso para análise de logs na STI/UFBA. Caso a contratada ofereça uma solução incompatível com a ferramenta citada, deverá fornecer outra ferramenta de análise de logs, podendo ser implementada pelo próprio firewall ou virtual, desde que seja semelhante ou superior.

5.1.4. CARACTERÍSTICAS DE HARDWARE:

5.1.4.1. Deve suportar, no mínimo, 190 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes

5.1.4.2. Deve suportar, no mínimo, 21 Gbps de throughput IPS

5.1.4.3. Deve suportar, no mínimo, 55 Gbps de throughput de VPN IPSec

5.1.4.4. Deve suportar, no mínimo, 10 Gbps de throughput de VPN SSL

5.1.4.5. Deve suportar, no mínimo, 11 Gbps de throughput de Inspeção SSL

5.1.4.6. Deve suportar, no mínimo, 33 Gbps de throughput de Controle de Aplicação

5.1.4.7. Deve suportar, no mínimo, 14.5 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.

5.1.4.8. Suporte a, no mínimo, 11 milhões de conexões simultâneas;

5.1.4.10. Deve suportar o gerenciamento de no mínimo 190 Switches do mesmo fabricante por equipamento;

5.1.4.11. Suporte a, no mínimo, 700 mil novas conexões por segundo

5.1.4.12. Estar licenciado para, ou suportar sem o uso de licença, 15 mil túneis de VPN IPSEC Site-to-Site simultâneos

5.1.4.13. Estar licenciado para, ou suportar sem o uso de licença, 90 mil túneis de clientes VPN IPSEC simultâneos

- 5.1.4.14. Estar licenciado para, ou suportar sem o uso de licença, 5 mil clientes de VPN SSL simultâneos
- 5.1.4.15. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
- 5.1.4.16. Possuir ao menos 8 interfaces 1Gbps SFP
- 5.1.4.17. Possuir ao menos 14 interfaces 1Gbps RJ-45
- 5.1.4.18. Possuir ao menos 10 Interfaces SFP28 de até 25Gbps, permitindo também o uso de transceivers 10Gbps SFP+ e Gigabit SFP, com fornecimento de 2(dois) transceivers SFP + (SR 10GE);
- 5.1.4.19. Possuir ao menos 4 Interfaces 40Gbps compatível com transceivers QSFP+;
- 5.1.4.20. Deve possuir disco Onboard Storage do tipo Solid State Drive NVMe (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB de armazenamento do sistema operacional e registro de logs;
- 5.1.4.21. Deverá possuir interface USB 3.0 para exportação de backups;
- 5.1.4.22. Deverá possuir interface do tipo console para utilização de CLI
- 5.1.4.23. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
- 5.1.4.24. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
- 5.1.4.25. Possuir no máximo 2 RU de altura e acompanhar kit de instalação em rack
- 5.1.4.26. Deverá possuir fontes de alimentação internas redundantes, do tipo hot-swappable;
- 5.1.4.27. O fabricante ofertado deve estar posicionado no quadrante "Leader" do quadrante mágico do Gartner de 2022, na categoria Network Firewalls.

5.1.5. CARACTERÍSTICAS GERAIS DE FUNCIONALIDADES

- 5.1.5.1. 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;
- 5.1.5.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 5.1.5.3. 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;
- 5.1.5.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 5.1.5.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 5.1.5.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 5.1.5.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
- 5.1.5.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
- 5.1.5.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- 5.1.5.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 5.1.5.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 5.1.5.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 5.1.5.13. Os dispositivos de proteção de rede devem suportar sFlow;
- 5.1.5.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 5.1.5.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 5.1.5.16. Deve suportar NAT dinâmico (Many-to-1);
- 5.1.5.17. Deve suportar NAT dinâmico (Many-to-Many);
- 5.1.5.18. Deve suportar NAT estático (1-to-1);
- 5.1.5.19. Deve suportar NAT estático (Many-to-Many);
- 5.1.5.20. Deve suportar NAT estático bidirecional 1-to-1;

- 5.1.5.21. Deve suportar Tradução de porta (PAT);
- 5.1.5.22. Deve suportar NAT de Origem;
- 5.1.5.23. Deve suportar NAT de Destino;
- 5.1.5.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 5.1.5.25. Deve poder combinar NAT de origem e NAT de destino na mesma política
- 5.1.5.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 5.1.5.27. Deve suportar NAT64 e NAT46;
- 5.1.5.28. Deve implementar o protocolo ECMP;
- 5.1.5.29. 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;
- 5.1.5.30. Enviar log para sistemas de monitoração externos, simultaneamente;
- 5.1.5.31. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 5.1.5.32. Proteção anti-spoofing;
- 5.1.5.33. Suportar otimização do tráfego entre dois equipamentos;
- 5.1.5.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 5.1.5.35. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
- 5.1.5.36. Suportar OSPF graceful restart;
- 5.1.5.37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 5.1.5.38. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 5.1.5.39. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 5.1.5.40. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 5.1.5.41. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- 5.1.5.42. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3;
- 5.1.5.43. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- 5.1.5.44. A configuração em alta disponibilidade (HA) deve sincronizar: Sessões;
- 5.1.5.45. A configuração em alta disponibilidade (HA) deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- 5.1.5.46. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- 5.1.5.47. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
- 5.1.5.48. O HA deve possibilitar monitoração de falha de link;
- 5.1.5.49. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 5.1.5.50. 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;
- 5.1.5.51. 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;
- 5.1.5.52. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces;
- 5.1.5.53. Controle, inspeção e descryptografia 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);

5.1.5.54. O console de administração deve suportar pelo menos inglês, espanhol e português.

5.1.5.55. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de e-mail, firewall de aplicativos, proxy, cache e ameaças avançadas.

5.1.5.56. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

5.1.6. FUNCIONALIDADES DE CONTROLE POR POLÍTICAS

5.1.6.1. Deverá suportar controles por zona de segurança;

5.1.6.2. Controles de políticas por porta e protocolo;

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

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

5.1.6.5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

5.1.6.6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

5.1.6.7. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.

5.1.6.8. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

5.1.6.9. Deve suportar o protocolo padrão da indústria VXLAN;

5.1.6.10. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall

5.1.6.11. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução

5.1.6.12. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de e-mail e firewall de aplicativos da Web.

5.1.7. FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO

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

5.1.7.2. 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;

5.1.7.3. Reconhecer pelo menos as seguintes aplicações: BitTorrent, gnutella, Skype, facebook, LinkedIn, 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;

5.1.7.4. 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;

5.1.7.5. 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;

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

5.1.7.7. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

5.1.7.10. 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;

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

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

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

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

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

5.1.7.16. 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.);

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

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

5.1.7.19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente

5.1.8. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

5.1.8.1. 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;

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

5.1.8.3. 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;

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

5.1.8.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.1.8.6. Deve permitir o bloqueio de vulnerabilidades;

5.1.8.7. Deve incluir proteção contra-ataques de negação de serviços;

5.1.8.8. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;

5.1.8.9. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;

5.1.8.10. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

5.1.8.11. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

5.1.8.12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;

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

5.1.8.14. Detectar e bloquear a origem de portscans;

5.1.8.15. Bloquear ataques efetuados por worms conhecidos;

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

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

5.1.8.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do

produto;

5.1.8.19. Identificar e bloquear comunicação com botnets;

5.1.8.20. 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;

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

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

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

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

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

5.1.8.26. 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 diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

5.1.8.27. Suportar e estar licenciado com proteção contra-ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;

5.1.9. FUNCIONALIDADES DE FILTRO DE URL

5.1.9.1. 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);

5.1.9.2. 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, em modo de proxy transparente e explícito;

5.1.9.3. Suportar proxy Web transparente e Explicit Web Proxy;

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

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

5.1.9.6. Possuir pelo menos 60 categorias de URLs;

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

5.1.9.8. Permitir a customização de página de bloqueio;

5.1.9.9. 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).

5.1.10. FUNCIONALIDADES DE IDENTIFICAÇÃO DE USUÁRIOS

5.1.10.1. 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;

5.1.10.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.1.10.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas 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.;

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

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

5.1.10.6. 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);

5.1.10.7. 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;

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

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

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

5.1.11. FUNCIONALIDADES DE QOS E TRAFFIC SHAPING

5.1.11.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, 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 máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

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

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

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

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

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

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

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

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

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

5.1.11.11. Suportar modificação de valores DSCP para o Diffserv;

5.1.11.12. Suportar priorização de tráfego usando informação de Type of Service;

5.1.11.13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

5.1.12. FUNCIONALIDADES DE FILTRO DE DADOS

5.1.12.1. Permitir a criação de filtros para arquivos e dados pré-definidos;

5.1.12.2. Os arquivos devem ser identificados por extensão e tipo;

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

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

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

5.1.12.6. 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.

5.1.13. FUNCIONALIDADES DE ZTNA (ZERO TRUST NETWORK ACCESS)

5.1.13.1. A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:

5.1.13.1.1. Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:

5.1.13.1.1.1. Informação pessoal do sistema operacional;

5.1.13.1.1.2. LinkedIn;

5.1.13.1.1.3. Google;

5.1.13.1.1.4. Salesforce;

5.1.13.1.2. Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:

5.1.13.1.2.1. DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DHCP específico

5.1.13.1.2.2. DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico

5.1.13.1.2.3. Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento

5.1.13.1.2.4. Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico

5.1.13.1.2.5. Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway.

5.1.13.1.2.6. Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede

5.1.13.1.2.7. VPN Tunnel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Túnel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil

5.1.13.1.3. Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso.

5.1.14. GEOLOCALIZAÇÃO

5.1.14.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

5.1.14.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.1.14.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

5.1.15. FUNCIONALIDADES DE VPN

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

5.1.15.2. Suportar IPsec VPN;

5.1.15.3. Suportar SSL VPN;

5.1.15.4. A VPN IPsec deve suportar Autenticação MD5 e SHA-1;

5.1.15.5. A VPN IPsec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.1.15.6. A VPN IPsec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

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

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

5.1.15.9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPsec IPv6;

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

5.1.15.11. 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;

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

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

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

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

5.1.15.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior);

5.1.15.17. Deve suportar Auto Discovery Virtual Private Network (ADVPN);

5.1.15.18. Deve suportar agregação de túneis IPsec;

5.1.15.19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em

agregação de túneis IPSec;

5.1.15.20. A VPN IPSec deve suportar Forward Error Correction (FEC);

5.1.15.21. Deve suportar TLS 1.3 em VPN SSL.

5.1.16. FUNCIONALIDADES DE SD-WAN

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

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

5.1.16.3. 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.

5.1.16.4. Deve implementar balanceamento de link por custo configurado do link.

5.1.16.5. Deve suportar o balanceamento de, no mínimo, 256 links;

5.1.16.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

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

5.1.16.8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;

5.1.16.9. Deve suportar Zero-Touch Provisioning;

5.1.16.10. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;

5.1.16.11. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;

5.1.16.12. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;

5.1.16.13. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS

5.1.16.14. Suportar UDP Hole Punching em arquitetura ADVPN;

5.1.16.15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;

5.1.16.16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;

5.1.16.17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;

5.1.16.18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

5.1.17. FUNCIONALIDADES DE WIRELESS CONTROLLER

5.1.17.1. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

5.1.17.2. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;

5.1.17.3. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;

5.1.17.4. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

5.1.17.5. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

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

5.1.17.7. 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 devem ser tunelados até o controlador wireless;

5.1.17.8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;

- 5.1.17.9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
- 5.1.17.10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
- 5.1.17.11. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 5.1.17.12. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;
- 5.1.17.13. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 5.1.17.14. 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 dBm;
- 5.1.17.15. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 5.1.17.16. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 5.1.17.17. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
- 5.1.17.18. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
- 5.1.17.19. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 5.1.17.20. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 5.1.17.21. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 5.1.17.22. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 5.1.17.23. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 5.1.17.24. Deve permitir restringir o número máximo de dispositivos conectados por ponto de

acesso e por rádio;

5.1.17.25. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

5.1.17.26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

5.1.17.27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

5.1.17.28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

5.1.17.29. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

5.1.17.30. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

5.1.17.31. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

5.1.17.32. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

5.1.17.33. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

5.1.17.34. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

5.1.17.35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

5.1.17.36. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

5.1.17.37. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

5.1.17.38. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

5.1.17.39. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;

5.1.17.40. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de Inspeção SSL que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;

5.1.17.41. A base de reconhecimento de aplicações através de Inspeção SSL deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;

5.1.17.42. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de Inspeção SSL;

- 5.1.17.43. A solução deve ainda, através da técnica de Inspeção SSL, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
- 5.1.17.44. "A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
- 5.1.17.45. - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
- 5.1.17.46. - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
- 5.1.17.47. - ASLEAP;
- 5.1.17.48. - Null Probe Response / Null SSID Probe Response;
- 5.1.17.49. - Long Duration;
- 5.1.17.50. - Ataques contra Wireless Bridges;
- 5.1.17.51. - Weak WEP;
- 5.1.17.52. - Invalid MAC OUI;
- 5.1.17.53. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
- 5.1.17.54. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
- 5.1.17.55. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
- 5.1.17.56. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
- 5.1.17.57. Deve implementar autenticação administrativa através do protocolo RADIUS;
- 5.1.17.58. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 5.1.17.59. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 5.1.17.60. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 5.1.17.61. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 5.1.17.62. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 5.1.17.63. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 5.1.17.64. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 5.1.17.65. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 5.1.17.66. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 5.1.17.67. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 5.1.17.68. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 5.1.17.69. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 5.1.17.70. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 5.1.17.71. A solução deve garantir que usuários se autenticuem em captive portal que faça uso

de endereço IPv6;

5.1.17.72. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

5.1.17.73. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

5.1.17.74. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;

5.1.17.75. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

5.1.17.76. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

5.1.17.77. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

5.1.17.78. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

5.1.17.79. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

5.1.17.80. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

5.1.17.81. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;

5.1.17.82. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

5.1.17.83. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernetlike MIB);

5.1.17.84. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato. pcap;

5.1.17.85. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

5.1.17.86. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

5.1.17.87. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

5.1.17.88. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

5.1.17.89. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

5.1.17.90. A solução deve possuir ferramentas de diagnósticos e debug;

5.1.17.91. A solução deve suportar comunicação com elementos externos através de APIs;

5.1.17.92. A solução deverá ser compatível e gerenciar pontos de acesso do mesmo fabricante;

O fabricante ofertado deve estar posicionado no quadrante “Leader” do quadrante mágico do Gartner de 2021, na categoria WAN Edge Infrastructure.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1	Suporte técnico 24x7, por parte do fabricante/contratado. O suporte técnico deve ser disponibilizado durante 24horas, 7 dias por semana. Esse suporte é essencial em caso de sinistro com o equipamento;
6.2	Os procedimentos para realização de atendimento remoto, serão seguidos pela Política de Segurança da Informação da UFBA;
6.3	Os procedimentos e instruções serão informados na reunião de início dos serviços após assinatura do contrato;
6.4	Serão elaborados termos de confidencialidade a fim de evitar vazamento de informações classificadas como sigilosas pela instituição. Atendendo assim, as legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014) para manter a integridade dos dados e das informações sensíveis dos sistemas da universidade;
6.5	Toda documentação gerada e entregue para UFBA deverá estar no Idioma Português-Brasil;
6.6	Os horários de execução dos serviços devem ser respeitados de acordo com fuso horário de Brasília-DF;
6.7	A ativação do suporte ao Fabricante deve ser realizada por empresa autorizada pelo fabricante no Brasil.

7. Estimativa da demanda - quantidade de bens e serviços

A Universidade Federal da Bahia disponibiliza uma infraestrutura de TI para cerca de 61.000 (sessenta e um mil) usuários da comunidade acadêmica, sendo composta por alunos, professores e técnicos administrativos em educação. Cabe ressaltar, a solução Firewall UTM ora em licitação servirá aos serviços e sistemas de informação administrativos da Universidade Federal da Bahia.

Atualmente, a solução da Fortinet FortiGate 3200D permite um nível de segurança na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI, Filtro de Botnet, Gateway (Antivírus, Anti-Spyware, Prevenção de Intrusão) filtro de conteúdo, possibilidade de atualização de software e firmware, alta disponibilidade, gerenciamento centralizado das configurações, alertas e logs.

Outro fator a ser ressaltado é o uso do FortiAnalyzer, que permite o monitoramento do tráfego e analisa os relatórios da rede em um único sistema, fornecendo maior conhecimento de eventos de segurança e relatórios sobre o uso da banda, auxiliando um diagnostico de forma rápida e eficiente das causas de possíveis ataques cibernéticos ou lentidão na rede.

ITEM	CÓDIGO CATMAT /CATSER	PART NUMBER	DESCRIÇÃO / MODELO	MARCA / MODELO	QTD
01	27740	FG3K2D3Z17800025 / FG3K2D3Z17800027	8x10 GE SFP + slots, 2x GE RJ45 Gestão, SPU NP6 e CP8 aceleração de hardware, SSD de 960 GB de armazenamento a bordo, e dual fontes de alimentação DC com licenciamento Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 FortiCare)	Fortinet / FortiGate- 3200D	02
02	27740	FL-2KE3R17000151	FortiAnalyzer-2000E gerenciador de logs, análise e plataforma de relatórios, fornecendo às organizações um painel único orquestração, automação e resposta para segurança simplificada operações, identificação proativa e remediação de riscos, e visibilidade completa de toda a superfície de ataque	Fortinet / FortiAnalyzer- 2000E	01

8. Levantamento de soluções

Foi realizado levantamento de soluções, baseado nos aspectos da referida Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022. Art. 11.

a) Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

Em levantamento realizado na ferramenta DataWarehouse (DW) SIASG (<https://dw.comprasnet.gov.br/dwcompras/servlet/mstrWeb>), foram identificadas algumas contratações dos últimos 12 meses, referentes a aquisição de solução de firewall já implantadas em outras instituições públicas, conforme tabela abaixo:

Cod UResp Compra	Objeto Compra	CPF/CNPJ Fornecedor	Nome Fornecedor	Marca Material Compra	Qtde Ofertada	Valor Unitário Homologado
150002	Objeto: Pregão Eletrônico - Seleção de propostas por meio do Sistema de Registro de Preços, com vistas à eventual contratação de empresa, para aquisição de nova solução para mitigação de ataques de negação de serviço (DoS/DDoS) e serviços agregados de implantação, instalação, configuração, operação assistida, garantia e suporte técnico dos equipamentos de acordo com as especificações técnicas e condições previstas no Termo de Referência e seus Encargos.	9024896000113	INB TECNOLOGIA LTDA	NETSCOUT	1	R\$4.227.500,00
943001	Objeto: Pregão Eletrônico - Registro de preços para futuras e eventuais contratações de solução de proteção de redes incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, de acordo com as especificações e quantitativos previstos no Anexo I - Termo de Referência deste edital.	9137728000215	NTSEC SOLUCOES EM TELEINFORMATICA LTDA	CHECK POINT	6	R\$1.159.757,00
925866	Objeto: Pregão Eletrônico - Registro de preço para eventual fornecimento, instalação e configuração de Solução de Balanceamento de Carga com Firewall de Segurança Avançada de Aplicações WEB Integrado para o Tribunal de Justiça do AM, incluindo testes operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, bem como os serviços de Migração, Treinamento, Consultoria e de Suporte Técnico.	18753084000108	IPTRUST ADVANCE TECNOLOGIA DA INFORMACAO LTDA	F5 NETWORKS	2	R\$4.058.000,00
453860	Objeto: Pregão Eletrônico - O objeto desta licitação consiste na seleção da proposta mais vantajosa para a Administração, visando a aquisição de solução de segurança de redes de computadores, contendo firewalls de rede, firewalls de aplicações web, sistema de gerenciamento e emissão de relatórios, sandboxing e autenticação, com serviço de instalação, migração inicial e capacitação, e suporte técnico pelo período mínimo de 60 (sessenta) meses, conforme Anexo I - Termo de Referência.	31862002000113	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	F5 NETWORKS	2	R\$1.710.000,00
240106	Objeto: Pregão Eletrônico - Eventual aquisição de elementos ativos de rede de comunicação de dados, compostos por switches, sistema de segurança unificado, interfaces GBIC, pontos de acesso e equipamentos de telefonia VoIP, para integrar a infraestrutura de comunicação de dados das unidades do INPE, em atendimento às características técnicas especificadas.	5795607000129	WISEIT - SISTEMAS E INFORMATICA LTDA	CISCO	1	R\$1.619.000,00
255000	Objeto: Pregão Eletrônico - Contratação de solução de proteção de dados (Backup) composto por hardware, licenciamento de software, configuração e garantia da solução por 36 meses, incluindo suporte e manutenção com substituição de peças em regime 24x7.	9137728000134	NTSEC SOLUCOES EM TELEINFORMATICA LTDA	VERITAS NETBACKUP	1	R\$1.180.000,00
250057	Objeto: Pregão Eletrônico - Aquisição por pregão eletrônico tradicional de solução de Firewall redundante com suporte e garantia por 60 meses	4892991000115	TELTEC SOLUTIONS LTDA	PALO ALTO	1	R\$1.465.639,00
110404	Objeto: Pregão Eletrônico - Aquisição de soluções de segurança de TI.	10647012000166	FAST SECURITY	TRELLIX	2	R\$1.395.000,00
530001	Objeto: Pregão Eletrônico - Aquisição de solução de equipamentos firewall de próxima geração e firewall de aplicação web, balanceador de carga e publicador de DNS, para proteção do perímetro da rede de dados, dos ativos de hardware e software e das aplicações web do Ministério, compreendendo gerência centralizada, instalação e configuração da solução, com garantia e suporte técnico pelo período de 60 (sessenta) meses, conforme condições, quantidades e exigências estabelecidas no Edital.	31862002000113	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	F5 NETWORKS	2	R\$1.290.000,00
70010	Objeto: Pregão Eletrônico - Aquisição de firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia de 60 meses, de acordo com as especificações constantes do Termo de Referência (ANEXO I) do Edital.	76535764000143	OI S.A. - EM RECUPERACAO JUDICIAL	FORTINET	4	R\$1.528.377,66
70014	Objeto: Pregão Eletrônico - Aquisição de dois firewalls da Palo Alto modelo PA-3430, configurados em alta disponibilidade no modo Ativo/Passivo, com suporte Premium e subscrições Threat Prevention , Advanced URL Filtering , GlobalProtect e "Virtual System" por um período de 5 (cinco) anos, e serviço técnico de implantação.	24376542000121	APPROACH TECNOLOGIA LTDA	PALO ALTO NETWORKS	2	R\$1.799.900,00
240010	Objeto: Pregão Eletrônico - Aquisição de cluster de Application Delivery Controller (ADC), solução de segurança da informação, com funções de balanceador de carga e aceleração web com módulos de Loading Balance, Global Server Load Balancing, Web Application Firewall e SSL offload e inspection (LB/GSLB/WAF/SSL), incluindo garantia e suporte técnico especializado de 60 (sessenta) meses e serviços agregados de instalação/migração e treinamento, para atender às necessidades do MRE, conforme Edital e anexos.	9024896000113	INB TECNOLOGIA LTDA	CITRIX	1	R\$3.530.000,00
154043	Objeto: Pregão Eletrônico - Appliance de segurança para a rede UFU composto por: firewall de pequeno porte com suporte e garantia de 60 meses, firewall de médio porte com suporte e garantia de 60 meses e analisador de tráfego, armazenamento de log e relatórios com suporte e garantia de 60 meses, todos conforme termo de referência.	5359927000136	PROTEGA - SECURITY SOLUTIONS LTDA	FORTINET	1	R\$1.599.000,00

b) As alternativas do mercado;

Para se conhecer as soluções disponíveis no mercado, foram identificados através do quadrante mágico da empresa Gartner (<https://www.gartner.com/en>), alguns fornecedores atuantes que atenderiam a demanda de fornecimento de firewall.

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

Durante a elaboração do estudo técnico preliminar, foram realizadas reuniões, com alguns representantes dos fabricantes listado abaixo, com intuito de conhecer mais detalhes sobre os tipos de soluções, forma de prestação de serviço e funcionalidades dos equipamentos disponíveis atualmente no mercado.

Fornecedores
SIGMATELECOM SISTEMAS INTELIGENTES DE COMUNICAÇÃO
PISONTEC COMERCIO E SERVICOS EM TECNOLOGIA DA INFORMACAO EIRELI
ARPSIST SERVICOS DE ENGENHARIA LTDA
ARPER INFORMATICA LTDA
BFF COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA EIRELI
COMDADOS COMERCIO E SERVICOS ELETRONICOS LTDA.
APPROACH TECNOLOGIA LTDA
SIGMAFONE TELECOMUNICACOES LTDA

VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI
NCT INFORMATICA LTDA
IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI

c) A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações;

Não foram identificados softwares públicos.

d) As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis;

Foi avaliado o padrão de governo e-PING para definição da solução de segurança.

e) As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual;

Para o caso de contratação de nova solução de firewall, seja por aquisição ou serviço, ficará a cargo da CONTRATADA.

f) Os diferentes modelos de prestação do serviços;

Durante o levantamento de possíveis soluções, foram mapeados 03(três) modelos de contratações de soluções de segurança da informação de firewall. Considerando a criticidade do ambiente, os recursos e demais variáveis existentes na UFBA, seguem conforme alternativas abaixo:

Item	Descrição do Modelo de Contratação	Métrica
1	Aquisição de Novo Equipamento	Unidade
2	Contratação de Solução de Firewall na Modalidade de Serviço	Mês
3	Serviço de Manutenção Preventiva e Corretiva	Mês

g) Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

Conforme a Análise comparativa de soluções. (Tópico 9)

h) A possibilidade de aquisição na forma de bens ou contratação como serviço;

Sim.

i) A ampliação ou substituição da solução implantada;

Não se aplica.

j) As diferentes métricas de prestação do serviço e de pagamento;

Não se aplica.

9. Análise comparativa de soluções

Análise da Solução 01 - Aquisição de Novo Equipamento

Os firewalls de última geração (NGFWs) são firewalls de inspeção de pacotes profundos que vão além da inspeção de porta/protocolo e do bloqueio para adicionar inspeção em nível de aplicativo, prevenção de intrusões e trazer inteligência de fora do firewall. Um **NGFW** não deve ser confundido com um sistema autônomo de prevenção de intrusões de rede (IPS), que inclui um firewall de commodity ou nonenterprise, ou um firewall e IPS no mesmo aparelho que não estão intimamente integrados.

Referência: <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws>

Esta solução é baseada na aquisição de novo equipamento incluindo o licenciamento, manutenção, garantia e capacitação;

A presente opção apresenta atualização de hardware;

Prós	Contras
<ul style="list-style-type: none">• Uso de equipamentos novos;• Atualização de Hardware;• Equipamento não estarão em fim de vida útil.	<ul style="list-style-type: none">• Não utilização do hardware instalado;• Necessidade de janela de manutenção para migração das soluções existentes;• Treinamento da equipe da Segurança Informação.

Análise da Solução 02 - Contratação de solução de firewall na modalidade de serviço

Uma nova forma de contratação de soluções de TI, como uma solução de firewall, é contratação na modalidade de serviço, onde a empresa contratada, mediante pagamentos na forma de mensalidade, prove o fornecimento da solução contratada. Existem dois modos de fornecimento da solução de firewall como serviço:

- É a modalidade onde o firewall fica hospedado na nuvem da empresa contratada ou do fabricante do firewall, não havendo a presença física do equipamento na rede de dados do cliente, e todo o tráfego de internet da rede local é direcionada para a nuvem. Nesta modalidade o pagamento da mensalidade varia de acordo com a quantidade de tráfego que é inspecionado e processado pelo firewall na nuvem, não havendo uma previsibilidade ou valor fixo a pagar mensalmente, o que dificulta o planejamento para a previsão orçamentária.
- É onde a empresa contratada realiza o fornecimento, instalação e configuração do equipamento físico na rede de dados do cliente, mediante o pagamento de um valor mensal fixo, ficando a empresa contratada responsável pela garantia, suporte e monitoramento do equipamento. Essa modalidade se assemelha a uma locação.

Em ambos os casos, o não pagamento do valor da mensalidade, em virtude de o equipamento não pertencer ao cliente, acarreta na suspensão da prestação do serviço e remoção do equipamento e, sendo o firewall um equipamento fundamental no funcionamento e proteção da rede de dados, tal suspensão na prestação do serviço traria enormes prejuízos a instituição deixando sua rede de dados e seus usuário sem proteção e expostos a ataques cibernéticos ou ainda sem acesso à Internet.

Prós	Contras
<ul style="list-style-type: none"> • Uso de equipamentos novos; • Atualização de Hardware; • Equipamento não estarão em fim de vida útil; • Não há necessidade de política de descarte de equipamento de TI; 	<ul style="list-style-type: none"> • Não utilização do hardware instalado; • Custo elevado conforme valores coletados nas cotações; • Necessidade de janela de manutenção para migração das soluções existentes; • Considerando que o caso exista algum problema orçamentário ou administrativo nos próximos anos, o órgão ficará descoberto do serviço.

Análise da Solução 03 - Serviço de Manutenção Preventiva e corretiva

Consiste na contratação de empresa especializada para Serviços de Manutenção corretiva e preventiva para equipamento de segurança do Datacenter da STI suporte 24x7 horas por dia para o firewall do modelo FORTIGATE 3200D já existentes na instituição, possibilitando que recebam adequado suporte de modo a reduzir indisponibilidades por falhas técnicas, contemplando substituição de peças quando necessário e suporte aos recursos Next-Generation Firewall, Antivírus, AntiSpam, Tentativa de invasão (IDS) e Filtro Web.

- Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar o equipamento defeituoso em perfeitas condições de uso, compreendendo inclusive as necessárias substituições de peças e componentes, ajustes e reparos, de acordo com manuais e normas técnicas específicas.
- Entende-se por manutenção preventiva, aquela que tem por finalidade executar qualquer serviço que envolva limpeza, calibração, ajustes, testes e revisões que visem evitar a ocorrência de quebras ou defeitos, bem como garantir o funcionamento dos equipamentos dentro das condições operacionais especificadas pelo fabricante, compreendendo inclusive as necessárias substituições de peças e componentes.

Prós	Contras
<ul style="list-style-type: none"> • Hardware instalado no Datacenter; • A equipe técnica da UFBA já possui conhecimento em toda solução; • Em pleno funcionamento e estável. 	<ul style="list-style-type: none"> • <i>Equipamentos encontram-se em "End of Life".</i>

9.1 Análise Comparativa de Cenários

Requisito	Solução	Sim	Não	Não se Aplica
	Solução 01	x		

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 02	x		
	Solução 03	x		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 01			x
	Solução 02			x
	Solução 03			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 01			x
	Solução 02			x
	Solução 03			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 01			x
	Solução 02			x
	Solução 03			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 01			x
	Solução 02			x
	Solução 03			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 01			x
	Solução 02			x
	Solução 03			x

10. Registro de soluções consideradas inviáveis

Soluções inviáveis

Analise da Solução 02 - Contratação de solução de firewall na modalidade de serviço

Caso seja adquirida a opção de firewall na modalidade de serviço e ocorra qualquer restrição orçamentária nos próximos anos, o órgão ficaria descoberto do serviço. Por este motivo esta solução foi considerada inviável pela equipe de planejamento da contratação.

Analise da Solução 03 - Serviço de Manutenção Preventiva e corretiva

Os equipamentos objeto do referido processo foram descontinuados (End of Life) pelo fabricante. Portanto, será impossível a contratação da renovação da garantia.

11. Análise comparativa de custos (TCO)

Na IN 94/2022 – SGD/ME, Art. 11, Inciso III, é prevista a realização de comparação de custos totais de propriedade para as soluções técnica e funcionalmente viáveis. Porém, neste Estudo, tendo em vista que a equipe de planejamento identificou apenas uma solução como viável, não será possível tal comparação.

12. Descrição da solução de TIC a ser contratada

A Universidade Federal da Bahia tem como missão produzir, socializar e aplicar o conhecimento construído nos diversos campos do saber, através do ensino, da pesquisa e da extensão, indissociavelmente articulados, de modo a contribuir para o desenvolvimento social, econômico e cultural, em especial no estado da Bahia, e promover a formação de cidadãos capazes de atuar na construção da equidade, da justiça social e da democracia e de profissionais qualificados para o mundo do trabalho. Neste contexto, as áreas de negócio utilizam os serviços de Tecnologia da Informação, providos pela Superintendência de Tecnologia da Informação - STI, para consecução de suas metas e objetivos:

Cenário Descrição

Solução 01 Aquisição de equipamento de Firewall, suporte 24x7, com licenciamento pelo período de 60 meses. conforme especificações técnicas descritas no (tópico 5)

13. Estimativa de custo total da contratação

Valor (R\$): 2.563.759,34

Através de Pesquisa realizada pelo Painel de Preços, foram obtidos os seguintes preços para a contratação desse objeto:

Identificação da Compra	Número do Item	Modalidade	Código do CATMAT	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
073/2022	00013	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	2	R\$1090000	ARPSIST SERVICOS DE ENGENHARIA LTDA	JUSTICA ELEITORAL	070010 - TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	16/12/2022
011/2022	00005	Pregão	481646	EQUIPAMENTO SEGURANÇA		UNIDADE	2	R\$1290000	GLOBAL SEC. TECNOLOGIA & INFORMATICA	MINISTÉRIO DO DESENVOLVIMENTO	530001 - DIRETORIA DE ADMINISTRACAO	23/12/2022

				REDE					INFORMALCAU LTDA	REGIONAL	ADMINISTRAÇÃO	
14/3/2022	00001	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	1	R\$1465639	TELTEC SOLUTIONS LTDA	MINISTERIO DA SAUDE	250057 - INSTITUTO NACIONAL DE TRAUMATO- ORTOPEDIA	29/08/2022

14. Justificativa técnica da escolha da solução

A Tecnologia da Informação e Comunicação (TIC) tornou-se ferramenta fundamental para a execução dos serviços nos setores público e privado. Especialmente no setor público, praticamente todos os processos de trabalho já operam, diretamente ou indiretamente, com sistemas de informação. Deste modo, tais meios são amplamente disseminados e utilizados na execução das atividades administrativas, operacionais e acadêmicas da Universidade.

Como peculiaridade marcante, os meios de TIC sofrem rápido processo de obsolescência e desgaste naturais, seja por conta do tempo de uso ou pelo aumento dos recursos computacionais ofertados na instituição, que impõem aos gestores a adoção de medidas que garantam a continuidade do exercício permanente de suas atribuições institucionais. A continuidade dos serviços é um dos principais atributos a ser levado em consideração pelos gestores, tendo em vista que a interrupção da prestação dos serviços públicos causa indesejáveis prejuízos à sociedade. Além disso, a Universidade Federal da Bahia passa por um crescente aumento de sua demanda de serviços de TIC e, conseqüentemente, necessita disponibiliza-los cada vez mais à comunidade acadêmica e administrativa.

A solução de segurança atualmente em uso pela UFBA é o principal ativo de segurança da informação, sendo o responsável pela inspeção do tráfego da rede interna/externa de toda a Universidade. A aquisição de um novo equipamento de firewall visa manter a continuidade dos serviços fornecendo alta disponibilidade, integridade e confidencialidade em seus sistemas de informação nas diversas Unidades Acadêmicas e Administrativa. Incluindo os Campi Universitários geograficamente dispersos: Instituto Multidisciplinar em Saúde (Campus Vitória da conquista) e Instituto de Ciência, Tecnologia e Inovação - (Campus Camaçari).

As novas técnicas de invasão e captura de informações, por parte de pessoas e grupos mal intencionados, estão se tornando cada vez mais comum na rede mundial de computadores. Assim, esta Universidade precisa estar sempre atualizada e preparada tecnicamente para enfrentar essas tentativas de captura de dados, tanto de forma ostensiva, quanto preventiva, para manter e prover políticas de segurança da informação personalizadas para: usuários, grupos de usuários, servidores, estações de trabalho, portas, protocolos e aplicações. Permitindo a continuação dos serviços oferecidos pela UFBA.

Dessa forma, pretende-se manter um ambiente para os usuários trabalharem com segurança e eficácia em locais (interno ou externo), através de conexões de Rede Privada Virtual (VPN - do inglês Virtual Private Network) e continuar provendo infraestrutura de comunicação de dados segura para suporte às soluções de vídeo Conferencia, via Internet no Ambiente Virtual de Aprendizagem (AVA) onde são ministradas aulas EAD.

15. Justificativa econômica da escolha da solução

Em pesquisa de preços realizada no Pannel de Preços foi possível identificar três pregões com itens semelhantes, incluindo característica técnicas capazes de atender à demanda apontada pela equipe da Coordenação de Redes Infraestrutura, conforme descritos na tabela abaixo.

Identificação da Compra	Número do Item	Modalidade	Código do CATMAT	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
00073/2022	00013	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	2	R\$1090000	ARPSIST SERVICOS DE ENGENHARIA LTDA	JUSTICA ELEITORAL	070010 - TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	16/12/2022
00011/2022	00005	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	2	R\$1290000	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	MINISTÉRIO DO DESENVOLVIMENTO REGIONAL	530001 - DIRETORIA DE ADMINISTRAÇÃO	23/12/2022
00243/2022	00001	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	1	R\$1465639	TELTEC SOLUTIONS LTDA	MINISTERIO DA SAUDE	250057 - INSTITUTO NACIONAL DE TRAUMATO-ORTOPEDIA	29/08/2022

Sendo assim, optou-se por utilizar, para calcular o preço unitário de referência, a média dos valores obtidos na pesquisa de preços, metodologia expressamente em consonância com o disposto no art. 6º, da IN SEGES/ME nº 65/2021.

16. Benefícios a serem alcançados com a contratação

Observa-se que essa contratação resultará em benefícios ao órgão como por exemplo; não haverá necessidade de adequação de ambiente, uma vez que a solução já está em pleno uso por essa Universidade; dentre outros, conforme elencado abaixo:

- Controle efetivo do tráfego de dados através de regras de segurança;
- Detecção e prevenção contra ameaças e tentativas de invasão;
- Estabelecer regras robustas de segurança para contenção de ameaças tecnológicas;
- Monitoramento e rastreabilidade das atividades de rede;
- Manter o monitoramento abrangente e eficiente sobre acessos à internet e tráfego de dados na rede corporativa de computadores;
- Fornecimento de relatórios relacionados a todas as operações realizadas na solução, bem como atividades de rede;
- Garantir que a UFBA esteja aderente às melhores práticas nacionais e internacionais da área de Segurança da Informação, e em consonância com as normas vigentes;
- Garantir que a UFBA preste serviços de qualidade à sociedade, bem como atenda as próprias necessidades institucionais, com base nos pilares de confiabilidade, integridade e disponibilidade.
- Proporcionar aumento da disponibilidade, da estabilidade e da reparabilidade dos recursos e ferramentas de TIC.
- Manter a infraestrutura de Segurança da Informação em funcionamento, atualizada e estável;
- e
- Economicidade em TI, observando os padrões e qualidade e o atendimento às necessidades institucionais.

17. Providências a serem Adotadas

Após a realização desse Estudo Técnico Preliminar, o Termo de Referência será elaborado e caso aprovado pela Administração Central será realizada a Licitação adotando o Sistema de Registro de Preços, através de Pregão Eletrônico.

18. Alinhamento Contratação e o Planejamento

18.1 Alinhamento entre a Contratação e o Planejamento

Em consonância com o art. 6º, I, da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a referida contratação encontra-se alinhada às diretrizes da área de TIC, estabelecidas no último PDTI divulgado pela instituição. O PDTI busca identificar e planejar o atendimento às demandas por ações na área de TI que visem oferecer suporte às atividades-meio e fim da UFBA, através de instrumentos que melhor representem a política e o planejamento estratégico da instituição.

18.2 Alinhamento ao PDTIC

ALINHAMENTO AO PDTIC	
ID	Meta do PDTIC associada
M4.3	Atualizar, ampliar e manter a infraestrutura do Datacenter

18.3 Alinhamento ao PCA

ALINHAMENTO AO PCA 2023	
DFD	Classe/Grupo
249	EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Considerando que os referidos equipamentos já se encontram sem a garantia do fabricante e que existe um eminente risco de defeitos, torna-se necessário novo processo licitatório para aquisição de novo equipamento.

Após a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO – uma vez considerando os seus potenciais benefícios e, termos de eficácia, efetividade e economicidade. pelo exposto já citado em tela, RECOMENDAMOS o prosseguimento da pretensão contratual.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: PORTARIA Nº 30-2023_PROAD-ETP_PR_15-2023

JEAN MENDES ARAUJO

Técnico de Tecnologia da Informação

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Firewall - Paineis de Preços.pdf (105.23 KB)

Anexo I - Firewall - Painei de Preços.pdf



MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS



MÉDIA

R\$ 1.281.879,67

MEDIANA

R\$ 1.290.000,00

MENOR

R\$ 1.090.000

FILTROS APLICADOS

Código Material/Serviço Nome do Material (PDM)

Ano da Compra Esfera

481646

EQUIPAMENTO SEGURANÇA REDE

2022, 2023

Federal

Quantidade total de registros: 3

Registros apresentados: 1 a 3

Identificação da Compra	Número do Item	Modalidade	Código do CATMAT	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
00073/2022	00013	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	2	R\$1090000	ARPSIST SERVICOS DE ENGENHARIA LTDA	JUSTICA ELEITORAL	070010 - TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	16/12/2022
00011/2022	00005	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	2	R\$1290000	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	MINISTÉRIO DO DESENVOLVIMENTO REGIONAL	530001 - DIRETORIA DE ADMINISTRAÇÃO	23/12/2022
00243/2022	00001	Pregão	481646	EQUIPAMENTO SEGURANÇA REDE		UNIDADE	1	R\$1465639	TELTEC SOLUTIONS LTDA	MINISTERIO DA SAUDE	250057 - INSTITUTO NACIONAL DE TRAUMATO-ORTOPEDIA	29/08/2022



Emitido em 10/04/2023

ESTUDOS PRELIMINARES (ANEXO III IN 05/2017) Nº 24/2023 - STI/UFBA (12.01.42)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado eletronicamente em 26/05/2023 17:09)

EDMILSON ALVES DO NASCIMENTO

COORDENADOR

CRI/STI (12.01.42.10)

Matrícula: ###500#2

(Assinado eletronicamente em 29/05/2023 11:09)

JEAN MENDES ARAUJO

TEC DE TECNOLOGIA DA INFORMACAO

NUINFR/CRI (12.01.42.10.01)

Matrícula: ###150#0

Para verificar a autenticidade deste documento entre em <https://sipac.ufba.br/public/documentos/> informando seu número: **24**, ano: **2023**, tipo: **ESTUDOS PRELIMINARES (ANEXO III IN 05/2017)**, data de emissão: **10/04/2023** e o código de verificação: **59a0dcc7a4**