

FUNDAÇÃO UNIVERSIDADE DO AMAZONAS/AM

Estudo Técnico Preliminar 242/2025

1. Informações Básicas

Número do processo: 23105.040523/2025-82

2. Descrição da necessidade

O ICSEZ necessita aprimorar sua infraestrutura de segurança de rede e gestão de múltiplos links de internet, substituindo o atual firewall baseado em software livre (pfSense) por uma solução corporativa com recursos de **alta disponibilidade (HA)**, **balanceamento inteligente de links (SD-WAN)** e **gestão centralizada de políticas**.

O **Relatório Técnico de Monitoramento de Link – outubro/2025**, constante do **processo SEI nº 23105.046854/2025-26**, identificou **53,3% de indisponibilidade operacional** e **latência média de 118 ms** no link principal do campus, com falhas contínuas entre os dias 6 e 18/10/2025. Essas interrupções afetam diretamente o acesso a sistemas institucionais como **SEI**, comprometendo atividades acadêmicas e administrativas.

A contratação visa garantir **resiliência na gestão de múltiplos links, continuidade e segurança da informação**, em conformidade com o **Decreto nº 10.222/2020 (PPSI)** e a **IN SGD/ME nº 94/2022**.

3. Área requisitante

Área Requisitante	Responsável
Gerência de Tecnologia da Informação – GTI/ICSEZ/UFAM.	Rafel Reis Mafra

4. Necessidades de Negócio

A estabilidade e a segurança da rede são fundamentais para o funcionamento das atividades administrativas e acadêmicas, bem como para o acesso contínuo aos sistemas institucionais da UFAM e aos serviços públicos digitais. A solução atualmente em uso não assegura a continuidade operacional nem oferece autenticação centralizada, o que compromete o cumprimento das metas institucionais e o alinhamento às políticas de transformação digital do Governo Federal.

5. Necessidades Tecnológicas

- Considerando a crescente complexidade do ambiente de rede e a dependência dos sistemas da UFAM, torna-se necessário dispor de uma **infraestrutura tecnológica resiliente**, capaz de garantir **proteção perimetral avançada**, **gerenciamento automatizado de múltiplos enlaces de internet**, e **autenticação centralizada de usuários**.

O cenário atual, caracterizado por instabilidade de conectividade e ausência de mecanismos de alta disponibilidade, demonstra a necessidade de adoção de um **firewall de próxima geração (Next Generation Firewall – NGFW)** com recursos integrados de monitoramento, controle e mitigação de ameaças, que permita elevar o nível de governança de TIC no campus ICSEZ.

Assim, as principais necessidades tecnológicas a serem atendidas pela solução incluem:
 - Alta disponibilidade (HA) nativa e balanceamento dinâmico de múltiplos links (SD-WAN) com failover automático;
 - Integração nativa com o Active Directory (ICSEZ.LOCAL), permitindo autenticação centralizada e controle por perfis;
 - Essas características permitirão ao ICSEZ manter a disponibilidade dos serviços críticos e garantir a segurança das comunicações institucionais.

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

A solução a ser contratada deve atender a requisitos técnicos, contratuais e operacionais que assegurem o desempenho, a continuidade e a conformidade da infraestrutura de segurança de rede do ICSEZ, garantindo o funcionamento ininterrupto dos serviços institucionais críticos.

6.1 Requisitos de Garantia Técnica

- Garantia mínima de **12 (doze) meses**, incluindo suporte técnico, substituição de peças e manutenção preventiva;
- **Atualizações automáticas de firmware e assinaturas de segurança** durante o período de garantia;
- **Suporte técnico de Nível 3 (fabricante)**, com atendimento remoto e/ou presencial conforme a necessidade;
- Disponibilização de **licença temporária de contingência** em caso de manutenção corretiva, assegurando continuidade de operação;
- Geração de relatórios de auditoria e conformidade, de acordo com as políticas do PPSI.

6.2 Requisitos Contratuais da Solução

- **Licenciamento completo UTM/NGFW**, incluindo: Firewall, IPS, AppControl, WebFilter, VPN SSL/IPSec, Anti-Malware, e Secure SD-WAN;
- **Treinamento técnico operacional** voltado à equipe da GTI/ICSEZ para administração e manutenção da solução;
- **Entrega e implantação** do equipamento em até **45 (quarenta e cinco) dias corridos** após a emissão da nota de empenho;
- A contratada deverá disponibilizar **suporte técnico e manutenção corretiva durante todo o período de 12 meses.**
-

6.3 DOS REQUISITOS TÉCNICOS APPLIANCE NGFW: CARACTERÍSTICAS DO HARDWARE.

- Appliance NGFW de no mínimo 38 Gbps de capacidade de Firewall, para links até 4.2 Gbps.
- O equipamento deverá suportar instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack;
- Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- Possuir painel/led indicador on/off, disco e devices de rede;
- Possuir throughput de no mínimo 38 Gbps para tráfego UDP;
- Suportar no mínimo 20.000.000 (vinte milhões) conexões simultâneas;
- Suportar no mínimo 138.000 (cento e trinta e oito mil) novas conexões por segundo;
- Possuir throughput mínimo de 7.0 Gbps para tráfego IPS/IDS;
- Possuir throughput mínimo de 6.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);
- Possuir throughput mínimo de 2.5 Gbps para tráfego VPN SSL com criptografia (AES-256);
- Possuir throughput mínimo de 2.0 Gbps para tráfego SSL Inspection;
- Possuir throughput mínimo de 4.2 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

- Mínimo de 4 (quatro) interfaces de rede do tipo 10Gbps SFP+, com os respectivos transceivers bidirecional, com conector LC;
- Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;
- Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;
- Possuir no mínimo 2 (duas) portas USB para conexão de dispositivos externos;
 - A interface USB deve suportar o uso de modem 4G/5G para conexão de link de Internet.

6.4 CARACTERÍSTICAS DO SOFTWARE: DAS FUNCIONALIDADES DO FIREWALL, SD-WAN, VPN IPSEC/SSL

CARACTERÍSTICAS GERAIS

- Quaisquer licenças que forem entregues para atender aos recursos da solução especificado no termo de referência, deverão ter seu vencimento de acordo com o período de contrato;
- O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de menor capacidade;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;
- Os desempenhos dos appliances ofertados deverão ser mensurados através da metodologia baseada em proxy (Proxy Based), não serão aceitos appliances mensurados somente no método baseado em fluxo (Flow Based);
- Interface em português, espanhol e inglês;
- Suportar notificações de vencimento da licença na janela de alertas, por e-mail e trap SNMP com os dias restantes da data vencimento;
- O gerenciamento da solução deve suportar acesso via SSH, cliente, WEB (HTTPS) ou API aberta;
- Suportar acesso à Web por HTTP e CLI por TELNET;
- Permitir alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPS e CLI;
- Atualização de modo “offline”, onde poderá ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- Restore de Snapshot sem executar o Wizard e sem licenciamento;
- A solução deve oferecer suporte ao NAT444 (CGNAT) ou funcionalidade que implemente a persistência no NAT de saída independente da porta de destino, de forma que o endereço IP e porta traduzidos para um determinado usuário se mantenham os mesmos nas novas sessões que cheguem com o mesmo endereçamento IP e porta de origem;
- Suportar segundo fator de autenticação para usuários administradores da solução (2FA/MFA);
- Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;
- O sistema deverá permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

- O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura;
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;
- Todos os recursos detalhados no termo de referência deverão ser providos por um único software;
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3;
- Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;
- A Solução deverá prover inspeção SSL;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;
- Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:
 - Endereço do servidor;
 - Porta do servidor;
 - Usuário;
 - Senha.
 - Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:
 - Desempenho total (throughput);
 - Conexões simultâneas;
 - Usuários autenticados;
 - Serviços habilitados ou desabilitados;
 - Quantidade de endereços distribuídos pelo DHCP;
 - Endereço de IP das Interfaces;
 - Modelo do appliance;
 - Monitorar o status dos tuneis de VPN IPSEC;
 - Status do serviço de Alta disponibilidade.
- Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;
- A Solução deverá permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;

- Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;
- Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;
- Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX);
- Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware deverão ser disponibilizados em perfis e estes deverão ser inseridos em uma única política;
- Deve implementar o protocolo ECMP;
- Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;
- Esta condição deverá permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo;
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 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;
- A solução deverá possuir um assistente baseado em inteligência artificial que automatize tarefas administrativas e simplifique a criação de políticas de segurança, proporcionando maior rapidez, precisão e eficiência na configuração e gestão dos recursos, com capacidade de sugestão de regras, validação e comparação de configurações e detecção de inconsistências;
- A solução deverá possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução;
- A solução deverá exibir, por meio da interface web (GUI), o status de conectividade das interfaces de rede, incluindo informações como estado operacional (ativo/inativo);
- A solução deverá possuir a funcionalidade de Encrypted Traffic Analysis (ETA), permitindo a análise de tráfego criptografado sem necessidade de descryptografia, identificando padrões, anomalias e potenciais ameaças com base em fingerprints TLS/SSL, fluxos de comunicação e estatísticas de tráfego;
- A Solução deverá exibir estatísticas em tempo real do tráfego por interface. Devendo exibir no mínimo:
 - A aplicação, quantidade de pacotes e bytes por aplicação;
 - Quantidade de bytes descartados por interface;
 - Quantidades de pacotes TCP / UDP por interface;
 - Quantidades de pacotes por VLAN atrelada a interface;
 - Quantidades de pacotes MPLS por interface;
 - Quantidades de pacotes PPOE por interface;
 - Quantidades de pacotes fragmentados por interface;

- Tamanho máximo do pacote por interface.
- A Solução deverá exibir estatísticas de risco por protocolos em tempo real do tráfego por interface;

RECURSOS GERAIS DE FIREWALL

- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização;
- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em dispositivo USB conectado localmente;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças;
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deverá permitir o agendamento diário ou semanal;
- O sistema deverá permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente;
- As cópias de segurança deverão ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall;
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo tcpdump em tempo real e permitir o download em formato PCAP;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP, LDAPS, Microsoft Active Directory, Google Workspace;
- A solução deverá permitir integração com o Google Workspace (antigo G Suite) para autenticação de usuários e grupos via LDAP seguro, suportando funcionalidades como SSO (Single Sign-On) e autenticação multifator (MFA);
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para vários e vários para um;
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPFv2, OSPFv3, BGP e suportar duplicação de pacotes;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- A solução deverá permitir a criação de múltiplos perfis de servidor DHCP, com possibilidade de associação individual a interfaces de rede físicas, subinterfaces e VLANs, permitindo a gestão de escopos de IP isolados por segmento de rede;
- A solução deverá possuir suporte à configuração de opções DHCP (DHCP Option), permitindo a seleção do código da opção para valores dentro do intervalo de 1 a 250, conforme especificado pelo padrão [RFC 2132 ou equivalente];
- A funcionalidade deve possibilitar a configuração personalizada para cada opção selecionada, permitindo a definição de valores de acordo com as necessidades específicas da rede, incluindo, mas não se limitando a parâmetros de roteamento, servidores de tempo, servidores DNS, e demais parâmetros aplicáveis;
- A configuração deve ser realizada por meio de interface gráfica, garantindo a flexibilidade na administração da solução. Além disso, deve ser possível associar as opções DHCP a diferentes escopos, sub-redes ou grupos de clientes, conforme as políticas definidas pelo administrador da rede. Deve ser possível configurar um servidor RADIUS para a validação de usuários;
- A solução deverá permitir a reserva de endereços IP estáticos no servidor DHCP, associando um endereço IP a um endereço MAC específico, com possibilidade de gerenciamento individual por dispositivo;
- A solução deve consultar o Servidor RADIUS integrado ao Servidor DHCP, caso o Servidor RADIUS autorize, o NGFW deve entregar o endereço IP do range; caso contrário, não fornece endereço IP e a máquina não recebe o endereço, ficando sem acesso à rede;
- A solução deverá disponibilizar uma interface de gerenciamento de endereços concedidos (DHCP Leases), permitindo a visualização dos seguintes dados para cada dispositivo conectado: nome do host, endereço MAC, IP atribuído, data/hora da concessão;
- A solução deverá permitir a exclusão manual de leases ativos, forçando o cliente a realizar uma nova requisição DHCP e possibilitando ajustes de rede imediatos por parte do administrador;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de mínimo 4090 VLANs no padrão IEEE 802.1q por interface de rede;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Possuir mecanismo de anti-spoofing;

- Possuir a funcionalidade de balanceamento e contingência de links;
- Possibilitar a configuração dos timeouts de resposta dos protocolos de conexão, devendo suportar no mínimo a definição das opções do timeout padrão do ICMP, estabelecimento do TCP, envio do SYN em sessões TCP;
- Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP;
- Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams;
- Funcionalidades de Diagnóstico de Conectividade com SIMET;
- A solução deverá incorporar nativamente um mecanismo de medição de qualidade de conexão baseado no projeto SIMET, desenvolvido pelo NIC.br, sem a necessidade de instalação de equipamentos externos (ex: SIMET Box) ou agentes adicionais;
- A ferramenta de medição deverá ser executada diretamente na interface do equipamento NGFW, como funcionalidade embarcada no firmware, dispensando a utilização de plugins, pacotes adicionais ou servidores externos instalados localmente;
- A solução deverá suportar medições automáticas e sob demanda dos seguintes parâmetros de qualidade de conexão:
- Velocidade de download;
- Velocidade de upload;
- Latência (RTT);
- Jitter (variação de latência);
- Perda de pacotes.
- As medições deverão ser executadas sobre os protocolos IPv4 e IPv6, com suporte completo à avaliação dual stack.

POLÍTICAS DE SEGURANÇA

- Permitir limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede;
- A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;
- Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
- Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.
- Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inspection, Application Control, assim como definir roteamento de aplicativos por SD-WAN, limitação de taxa de DOS por pacotes em uma única política.
- Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.
- Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.

- Possibilitar a duplicação de uma política, otimizando tempo de configuração;

IDENTIFICAÇÃO DE USUÁRIO

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, Webfilter, IPS e Controle de aplicação integradas ao repositório de usuários sendo: locais (criados na própria solução), Microsoft Active Directory, LDAP, LDAPS, RADIUS e Google Workspace e integrações OAUTH com Google, Facebook e X (antigo Twitter);
- Deve possuir integração com Microsoft Active Directory, LDAP, LDAPS e Google Workspace para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- A solução deverá suportar múltiplos Servidores de Autenticação (MS AD e/ou LDAP) atuando no modo failover;
- CAPTIVE-PORTAL (Portal Web de autenticação Segura)
- A solução deverá permitir a criação de múltiplos perfis de Captive Portal, com configurações distintas de comportamento, aparência, autenticação e permissões, podendo ser aplicados por no mínimo:
 - Endereço IP ou Rede IPv4;
 - Endereço IP ou Rede IPv6;
 - Domínio.
- A solução deverá permitir que o Captive Portal utilize certificados digitais para autenticação de usuários, sendo possível habilitar a exigência de certificado cliente como método de validação da identidade;
- A solução deverá permitir a seleção da Autoridade Certificadora (CA) a ser utilizada para validação do certificado do usuário, podendo ser uma CA interna (local) ou uma CA externa confiável;
- A solução deverá permitir a verificação de revogação de certificados digitais durante o processo de autenticação, por meio do uso de listas CRL (Certificate Revocation List) ou outro método suportado;
- O certificado apresentado pelo usuário deverá ser validado quanto à sua integridade, validade, assinatura pela CA definida e, se configurado, presença em lista de revogação ativa;
- A solução deverá permitir que o certificado digital definido no perfil do Captive Portal seja utilizado para a proteção da conexão HTTPS entre o usuário e o portal de autenticação, garantindo a confidencialidade, integridade e autenticidade da comunicação;
- A solução deverá suportar registro de visitantes via Captive Portal, com a opção de ativação automática de conta e associação a grupos de acesso pré-definidos, sem intervenção do administrador;
- O Captive Portal deverá permitir integração nativa com provedores de login social, via OAuth 2.0, incluindo no mínimo:
 - Facebook;
 - Google;
 - X (antigo Twitter).
- O Captive Portal deverá oferecer, para o usuário autenticado, uma interface com funcionalidades adicionais configuráveis, incluindo:
 - Visualização e alteração de dados pessoais;

- Alteração de senha;
- Acesso ao Virtual Office (VPN SSL);
- Consulta à quarentena de arquivos.
- A interface do Captive Portal deverá permitir a personalização completa do conteúdo, incluindo:
 - Inclusão de logotipo personalizado (formato SVG com fundo transparente);
 - Edição do conteúdo dos termos de uso com editor HTML visual;
 - Definição de textos informativos e instruções para o usuário final.
- A solução deverá ser capaz de identificar nome do usuário, login, endereço IP, mac address e o método de autenticação dos usuários autenticados pela integração com os servidores de autenticação suportados;
- Suportar segundo fator de autenticação de usuários da solução (2FA/MFA) via token / OTP (One Time Password) e identificação segura via certificados PKI;
- A solução deve suportar autenticação por Single Sign-On (SSO) utilizando WMI (Windows Management Instrument), ou seja, não deve ser necessário instalar nenhum agente no servidor de autenticação;
- A solução deve suportar a integração com no mínimo 3 servidores WMI simultaneamente;
- A solução deve suportar agentes de Single Sign-On (SSO), desenvolvidos e fornecidos pelo próprio fabricante da solução ofertada, para sistemas operacionais Linux, permitindo a autenticação centralizada de usuários por meio de integração com serviços de diretório, como SAMBA, LDAP e/ou Active Directory, com registro de auditoria e aplicação de políticas de acesso;
- A solução deverá suportar a funcionalidade de sincronismo de sessões de autenticação, permitindo que dispositivos NGFW localizados em unidades remotas (filiais/branches) repliquem sessões autenticadas previamente validadas na matriz (head office), evitando a necessidade de reautenticação local;
- O sincronismo deverá ocorrer de forma unidirecional, onde a unidade remota (filial) consulta e replica as sessões válidas da unidade central (matriz), que é a responsável pela integração com os servidores de autenticação corporativos, como locais, Microsoft Active Directory, LDAP, LDAPS, SSO, Google Workspace e Integrações baseadas em OAuth 2.0, com suporte a provedores como Google, Facebook e X (antigo Twitter);
- A solução deverá permitir que o processo de sincronismo de sessões de autenticação da matriz para a filial seja realizado de forma filtrada e seletiva, garantindo que apenas as sessões relevantes para a respectiva unidade filial sejam replicadas;
- A funcionalidade deverá operar de forma nativa na solução, sem a necessidade de instalação de agentes externos, appliances adicionais ou soluções de terceiros;
- O mecanismo de sincronismo deverá ser compatível com múltiplos métodos de autenticação utilizados na matriz, incluindo:
 - Microsoft Active Directory;
 - LDAP e LDAPS;
 - RADIUS;
 - Google Workspace (via LDAP seguro);

- Integrações baseadas em OAuth 2.0, com suporte a provedores como Google, Facebook e X (antigo Twitter).
- A replicação das sessões deverá ocorrer de forma segura e criptografada, assegurando a integridade e confidencialidade dos dados de autenticação durante o processo de sincronização;
- A unidade filial deverá ser capaz de consultar o status de sessões sincronizadas, visualizar o tempo restante de validade, IP de origem, nome do usuário autenticado e método utilizado na matriz;
- A solução deverá suportar a configuração e operação de múltiplos servidores de autenticação de forma simultânea, permitindo a utilização de, no mínimo, um servidor de cada um dos seguintes tipos:
 - Locais (criados na própria solução);
 - Microsoft Active Directory;
 - LDAP e LDAPS;
 - RADIUS;
 - Google Workspace (via LDAP seguro);
- Integrações baseadas em OAuth 2.0, com suporte a provedores como Google, Facebook e X (antigo Twitter).
- A solução deverá permitir a criação de múltiplas regras de autenticação baseadas em políticas personalizadas, com possibilidade de definir ações do tipo permitir ou recusar acesso, de acordo com critérios pré-definidos pelo administrador;
- As regras de autenticação deverão permitir correlação condicional por múltiplos atributos, incluindo no mínimo:
 - Nome do usuário;
 - Grupo de usuários;
 - Endereço IP de origem ou rede;
 - Zona de Rede (Múltiplas Zonas);
 - Lista de palavras chaves ou conjunto de combinações de expressões regulares, (Objetos de Dicionários);
 - Intervalo de tempo (horário de acesso);
 - Agendamento com data de início e fim.
- A solução deverá permitir definir, por política de autenticação:
 - Número máximo de sessões simultâneas permitidas por usuário;
 - Número máximo de tentativas de login antes de bloqueio automático;
 - Tempo de bloqueio (timeout) após falha repetida;
 - Tempo de expiração da sessão (session timeout) após inatividade ou desconexão.
- As regras de autenticação deverão ser processadas com base em ordenação e precedência lógica (TOP-DOWN), garantindo que a primeira regra correspondente (match) seja aplicada;
- A solução deverá permitir substituição de sessões ativas, conforme login de novos usuários no mesmo dispositivo.

DAS FUNCIONALIDADES DA VPN

- Possuir suporte a VPN IPSEC
- A solução de VPN IPSEC deve ser implementada por meio de um appliance dedicado, ou seja, um dispositivo físico ou virtualizado especializado para gerenciar e operar a VPN garantindo maior desempenho, segurança e confiabilidade;
- A solução não deve ser apenas baseada em software instalado em servidores genéricos;
- Possuir suporte a VPNs IPSec site-to-site, ADVPN (Auto Discovery VPN), VPN Baseado em rotas e RAS (Remote Access Service);
- Possuir algoritmos de criptografia para túneis VPN: AES, 3DES, BLOWFISH, CAMELLIA e CAST128;
- Suporte a autenticação para construção de VPNs:
 - Suporte a certificados PKI X.509 (XAuth/RSA);
 - Suporte a chave compartilhada (XAuth/PSK);
 - Suportar tamanho de chaves de 128, 192 e 256 para os algoritmos AES, BLOWFISH e CAMELLIA, nas Fase 1 e 2 da VPN IPSEC;
 - Integridade MD5, SHA-1, SHA-256, SHA384, SHA512, AESCMAC e AES-XCBC, nas Fase 1 e 2 da VPN IPSEC;
 - Suporte ao algoritmo Internet Key Exchange (IKE) versões I e II;
 - Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo 32, nas Fase 1 e 2 da VPN IPSEC;
 - Suporte na VPN IPSEC NAT-T, Re-Auth e Fragmentation;
 - Suporte a compressão de dados na VPN IPSEC, para economia de banda.
- A solução deverá suportar VPN IPSEC do tipo baseada em rotas (route-based VPN), por meio da criação de interfaces virtuais dedicadas ao túnel, que possam ser tratadas como interfaces de rede e integradas ao roteamento estático ou dinâmico (BGP, OSPF, RIP) da solução;
- Possuir integração com o módulo de SD-WAN através de interfaces virtuais do tipo GRE, XFRM ou VTI;
- A solução deverá suportar configuração de túneis VPN IPSEC redundantes (lan-to-land) para o mesmo ponto remoto, permitindo alta disponibilidade da comunicação entre redes em caso de falhas de conectividade;
- A solução deverá suportar Auto Discovery VPN (ADVPN), permitindo o estabelecimento dinâmico de túneis IPSEC nos modos estrela (Hub/Spoke) e full mesh (Hub/Spoke e Spoke/Spoke), eliminando a necessidade de configurações manuais complexas, otimizando a comunicação para reduzir a latência, gerando menor consumo de largura de banda e maior eficiência no roteamento do tráfego entre os sites;
- Suportar as topologias Full Mesh e Star (HUB-Spoke);
- A solução deverá permitir a configuração de failover automático entre túneis VPN IPSEC, priorizando rotas configuradas e reativando a comunicação com a rede de destino sem necessidade de intervenção manual, caso o túnel principal fique indisponível;

- O recurso de VPN Failover, utilizando o status de múltiplos links WAN para monitorar a disponibilidade do túnel VPN em tempo real;
- A funcionalidade de VPN IPSEC com Failover deverá possibilitar a definição de:
 - Níveis de prioridade entre túneis IPSEC;
 - Túnel principal (ativo) e túneis de backup (failover);
 - Critérios de ativação por falha de rota, link físico, por latência, jitter, perda de pacotes e consumo de banda.
- Possuir suporte a VPN SSL
- A solução de VPN SSL deve ser implementada por meio de um appliance dedicado, ou seja, um dispositivo físico ou virtualizado especializado para gerenciar e operar a VPN SSL garantindo maior desempenho, segurança e confiabilidade;
- Possuir suporte a VPNs SSL com suporte as topologias client-to-server e site-to-site.
- A solução deverá suportar VPN SSL do tipo client-to-server, permitindo que usuários remotos se conectem com segurança à rede corporativa utilizando túnel com autenticação baseada em:
 - Autenticação por usuário e senha (XAuth);
 - Autenticação por usuário e senha (XAuth / MFA), com suporte a certificado de usuário (p12);
 - Certificados PKI X.509.
- A solução deverá suportar VPN SSL do tipo site-to-site, permitindo que um servidor de VPN se conecte como um cliente com segurança à rede corporativa utilizando túnel com autenticação baseada em:
 - Autenticação por chave PSK e ID de identificação;
 - Certificados PKI X.509 (RSA).
- Possuir suporte a VPN RAS
- VPN RAS (Remote Access Service) via IPSEC.
- A solução deverá suportar VPN do tipo (Remote Access Service) via IPSEC, permitindo que usuários remotos se conectem com segurança à rede corporativa utilizando túnel IPSEC com autenticação baseada em:
 - Certificados PKI X.509 (XAuth/RSA);
 - Chave compartilhada (XAuth/PSK);
 - MFA por Suporte a certificados PKI X.509 (XAuth/RSA) e chave compartilhada (XAuth/PSK);
 - Suportar segundo fator de autenticação de usuários da solução (2FA/MFA) via token / OTP (One Time Password).
- Suportar controle de acesso granular controlando as permissões de conexão por no mínimo via acesso a VPN RAS IPSEC e SLL por usuários, grupos de usuários, faixa de horários e dia da semana;
- Suporte a VPN RAS IPSEC deve suportar no mínimo:
 - Algoritmos de criptografia para túneis VPN: AES, 3DES, BLOWFISH, CAMELLIA e CAST128;
 - Tamanho de chaves de 128, 192 e 256 para os algoritmos AES, BLOWFISH e CAMELLIA, nas Fase 1 e 2 da VPN IPSEC;

- Integridade MD5, SHA-1, SHA-256, SHA384, SHA512, AESCMAC e AES-XCBC, nas Fase 1 e 2 da VPN IPSEC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo 32, nas Fase 1 e 2 da VPN IPSEC;
- Atribuição de endereço IP fixo por usuários.
- Suporte a compressão de dados na VPN RAS IPSEC, para economia de banda.
- VPN RAS (Remote Access Service) via SSL.
- A solução deverá suportar VPN do tipo (Remote Access Service) via SSL, permitindo que usuários remotos se conectem com segurança à rede corporativa utilizando túnel SSL com autenticação baseada em:
 - Usuário e senha;
 - Certificados PKI X.509 (XAuth/RSA);
 - MFA por Suporte a certificados PKI X.509 (XAuth/RSA) e chave compartilhada (XAuth/PSK).
 - Suporte a VPN RAS SSL deve suportar no mínimo:
 - Algoritmos de criptografia para túneis VPN: AES, 3DES e CAMELLIA;
 - Tamanho de chaves de no mínimo de 1024, 2048 e 4096 para os algoritmos AES e CAMELLIA;
 - Integridade MD5, SHA-1, SHA-256, SHA512;
 - Suporte a compressão de dados na VPN SSL, para economia de banda;
 - Atribuição de endereço IP fixo por usuários.
 - Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site;
 - Suportar a ativação de todo os tipos de VPN simultaneamente;
- Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:
 - RDP;
 - VNC;
 - SSH;
 - WEB;
 - SMB (compartilhamento de arquivos);
 - Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site;
 - Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
 - A VPN RAS deve suportar o estabelecimento automático da VPN nos protocolos ICMP ou DNS (53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada;

- Possuir recurso para configurar vários túneis simultâneos da VPN RAS, com o objetivo de aumentar o desempenho do tráfego;
- A VPN RAS SSL deve suportar criação de diversos HUBs, permitindo definir endereços IPs atribuídos distintos por usuário e grupo de usuários;
- A VPN RAS SSL deve suportar definir se o tráfego integral do cliente seja roteado pela VPN RAS SSL ou somente redes específicas;

SD-WAN:

- Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Suportar modo de duplicação de pacotes de dados pelos links WAN, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego;
- Permitir utilizar VPN IPSEC, ADVPN e VPN baseado em rotas para interligar unidades remotas;
- Possuir integração com o módulo de SD-WAN através de interfaces virtuais do tipo GRE, XFRM ou VTI;
- Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN;
- A solução deverá permitir a criação de múltiplos perfis de SD-WAN, com parâmetros operacionais e thresholds de desempenho configuráveis, como latência, jitter, perda de pacotes e largura de banda necessária, que poderão ser utilizados para a seleção automática do melhor caminho (failover/seleção dinâmica);
- A solução deverá permitir a utilização dos perfis definidos para criação de regras de roteamento baseado em política (Policy-Based Routing – PBR), com suporte a critérios como endereços de origem, destino, usuários, grupos de usuários, grupo de objetos, portas e aplicações;
- A solução deverá possuir mecanismo de roteamento sensível a aplicações (Application-Aware Routing), capaz de identificar, classificar e direcionar o tráfego de rede com base no tipo e na prioridade da aplicação, inclusive quando esta trafegar sobre conexões criptografadas (SSL/TLS);
- O mecanismo deverá:
 - Realizar classificação em tempo real de aplicações e subaplicações, mesmo em tráfego criptografado;
 - Permitir políticas de roteamento baseadas em desempenho de link (latência, jitter, perda e throughput) e no tipo de aplicação;
 - Suportar redirecionamento dinâmico entre múltiplos enlaces WAN (broadband, MPLS, LTE, etc.) conforme a qualidade percebida (QoE) da aplicação;

- Integrar-se nativamente à inspeção SSL/TLS, garantindo visibilidade e controle sobre aplicações encapsuladas em HTTPS.
- O roteamento deverá ser inteligente e automatizado, priorizando, por exemplo, tráfego de videoconferência (Teams, Zoom, Meet) em links de menor latência e backups ou atualizações em enlaces de menor custo;
- O recurso de SD-WAN deverá suportar roteamento de tráfego com base em aplicação, permitindo que o encaminhamento seja feito de acordo com a identificação da aplicação em tempo real, e não apenas com base em portas e protocolos tradicionais;
- O appliance SD-WAN deverá permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100;
- A solução de SD-WAN NGFW deverá permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;
- Deve suportar 2 (duas) conexões 4G/LTE simultâneas;
- O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;
- A solução deverá suportar os seguintes métodos de seleção de link:
 - Failover;
 - Load Balance;
 - Spillover;
 - Dynamic Selection.
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:
 - Consumo de banda;
 - Perda de pacotes;
 - Jitter;
 - Latência.
- A solução deverá suportar tráfego de rede do tipo Overlay e Underlay, permitindo o transporte de aplicações por túneis lógicos (overlay) sobre infraestruturas físicas distintas (underlay), com isolamento lógico, priorização de tráfego e políticas independentes;
- O tráfego Overlay deverá permitir a criação de túneis criptografados sobre redes IP públicas e privadas, garantindo segurança, otimização e controle de tráfego;
- O tráfego Underlay deverá permitir o uso eficiente dos links físicos disponíveis, incluindo MPLS, Internet dedicada, banda larga, 4G/5G e outros meios de conectividade;
- A solução deverá suportar a topologia de redirecionamento total de tráfego da filial para a matriz (Full Tunnel Mode), permitindo que todo o tráfego de rede da filial (inclusive para a internet) seja encaminhado via túnel VPN para o equipamento localizado na matriz, onde poderão ser aplicadas as políticas de segurança, NAT, inspeção ou saída para a internet;

- A solução a ser contratada não deverá impor qualquer limitação quanto à quantidade de túneis VPN suportados, devendo possibilitar a criação e utilização de múltiplos túneis simultâneos conforme a necessidade;
- A solução deverá permitir o monitoramento passivo da saúde dos enlaces;
- Deverá suportar o mecanismo de Forward Error Correction (FEC), aplicável por enlace ou túnel, para recomposição de pacotes perdidos em tempo real e redução de retransmissões, melhorando a qualidade das transmissões sem depender de recursos do provedor de acesso;
- A solução deve suportar roteamento estático e dinâmico (BGP4/BGP4+, OSPFv2/v3 e RIPv1/v2).

DAS FUNCIONALIDADES DE QOS

- Adotar solução de Qualidade de Serviço baseada em appliance;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP;
- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;
- Deverá permitir a criação de políticas de QoS em camada 7 (por aplicação/grupo de aplicações) associadas percentualmente à largura de banda provisionada da interface virtual SD-WAN (overlay), para uplink e downlink;
- A solução deverá permitir aplicar o código de DiffServ (DSCP) ao pacote ESP.

ALTA DISPONIBILIDADE

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over;
- O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;
- No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;
- Deverá suportar a persistências de sessão de usuários e conexões estabelecidas, entre os membros da Alta Disponibilidade;
- A solução deverá suportar agregação de múltiplos túneis IPsec baseados em rota em um único perfil/grupo SD-WAN, com balanceamento por pacote entre os túneis.

DAS FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO E WEB PROXY: CONTROLE DE APLICAÇÕES

- As funcionalidades abaixo deverão ser baseadas em appliance:
 - Deverá reconhecer no mínimo 8000 aplicações;
 - Deverá possuir, no mínimo, 20 categorias para classificação de aplicações.
- A solução deverá permitir a criação de múltiplos perfis, contendo a seleção das aplicações, grupos e subgrupos de aplicações com as ações de Bloqueio e Liberação no mesmo perfil;
- A solução deverá permitir a utilização dos perfis definidos para criação de regras de roteamento baseado em política (Policy-Based Routing – PBR), com suporte a critérios como endereços de origem, destino, usuários, grupos de usuários, grupo de objetos, portas e aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
 - P2P;
 - Web;
 - Transferência de arquivos;
 - Social;
 - Proxy;
 - Streaming.
 - Bloqueio de anúncios (ads blocking);
 - Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
 - Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
 - Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
 - Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
 - Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
 - Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
 - Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
 - Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
 - Deverá 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;
 - A solução deverá possuir mecanismo de Controle de Aplicações (Application Control) capaz de identificar, classificar e aplicar políticas de uso sobre aplicações e subaplicações, inclusive em conexões criptografadas (SSL/TLS);
 - O controle deverá permitir reconhecimento granular de aplicações dentro de portais ou plataformas, como por exemplo:

- Facebook Chat, Facebook Games e Facebook Video dentro do portal Facebook;
- YouTube, Gmail e Drive (Google) e Teams, OneDrive e Outlook Web (Microsoft 365).
- A inspeção e o controle deverão ocorrer em tempo real, com base em assinaturas, decodificação de protocolo e análise de tráfego cifrado, garantindo políticas distintas para cada subserviço identificado;
- A solução deverá permitir ao administrador a criação e personalização de assinaturas de detecção de aplicações e serviços, possibilitando o registro de aplicações customizadas não presentes na base padrão do fabricante;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
- Tecnologia utilizada nas aplicações (client-server, browse based, network protocol, etc);
- Nível de risco da aplicação;
- Categoria e subcategoria de aplicações.

FILTRO DE CONTEÚDO WEB

- Possuir solução de filtro de conteúdo web integrado a solução de segurança;
- Possuir pelo menos 85 categorias para classificação de sites web;
- Possuir base mínima contendo, 50 milhões de sites internet web já registrados e classificados;
- A solução deverá permitir a criação de múltiplos perfis, contendo a seleção das categorias, listas de URL e regex com ações de Bloqueio e Liberação no mesmo perfil;
- A solução deverá permitir a utilização dos perfis definidos para criação de regras de roteamento baseado em política (Policy-Based Routing – PBR), com suporte a critérios como endereços de origem, destino, usuários, grupos de usuários, grupo de objetos, portas, aplicações, categorias, listas de URL e regex;
- Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
 - Webmail;
 - Instituições de Saúde;
 - Notícias;
 - Pornografia;
 - Restaurante;
 - Mídias Sociais;
 - Esporte;
 - Educação;
 - Games;
 - Compras.
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

- Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
- Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;
- Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
- Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
- Possibilitar a integração com servidores de cache WEB externos;
- Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update, Youtube, Sourceforge, Downloads, Facebook, Google Maps;
- Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por lista de palavras chaves com suporte inclusive a expressões regulares;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários locais (criados na própria solução), Microsoft Active Directory, LDAP, LDAPS, RADIUS e Google Workspace e integrações OAUTH com Google, Facebook e X (antigo Twitter);
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Possuir Logs e Relatórios de tempo de navegação de sites web - Domínios Web;
- Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio, conhecido como DNS Content Filter, com suporte a Safe-Search para no mínimo os buscadores Google, Youtube e Bing;
- A solução deverá permitir o bloqueio de arquivos por tipo e extensão durante o acesso web, sendo possível configurar regras específicas para upload e download de arquivos;
- A solução deverá permitir a aplicação de mecanismos de Safe Search (busca segura), forçando o uso de filtros de conteúdo em motores de busca como Google, Bing e Yahoo;
- A solução deverá suportar a definição de quotas de navegação (surfing quotas) por perfil, incluindo:
 - Tempo máximo de navegação por dia (em horas);
 - Tráfego máximo diário (em MB);
 - Tamanho máximo de upload e download de arquivos via web.

- A solução deverá permitir restringir os domínios autorizados a acessar os serviços do Google Apps (como Gmail, Google Drive, Google Classroom, entre outros), possibilitando ao administrador definir, de forma centralizada, quais domínios estão habilitados a acessar as aplicações e informações hospedadas no ecossistema Google.

RECURSOS DO PROXY

- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy Transparente;
- A solução deve ser capaz de identificar o comportamento do protocolo SSH onde poderá ser feito através da inspeção do protocolo;
- Suportar serviço de Proxy SSH atuando como intermediário entre cliente e servidor, habilitando criptografia interna e externa em conexões SSH para inspeção e prevenção de tunelamentos não autorizados;
- Integrar o Proxy SSH ao módulo de Threat Protection, suportando controle de reputação de IP e bloqueio automático de ameaças durante sessões SSH;
- Deverá permitir configurar a porta do Proxy Explícito;
- O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado;
- Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);
- O tráfego descriptografado por SSL/HTTPS Inspection deve estar disponível ao mecanismo de roteamento sensível a aplicações;
- A solução deverá realizar inspeção profunda de tráfego criptografado SSL/TLS (Deep Inspection) de forma nativa e integrada, com suporte às versões TLS 1.1, 1.2 e 1.3, sem dependência de módulos externos ou limitação de hardware;
- Deverá permitir a inspeção de conexões HTTPS, SMTPS, POP3 e outras aplicações sobre TLS, garantindo visibilidade e controle de conteúdo criptografado.

DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO E THREAT PROTECTION: DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO

- A Detecção de Intrusão deverá ser baseada em appliance;
- Possuir no mínimo 90.000 (noventa mil) assinaturas ou regras de IPS/IDS;
- Permitir a criação de assinaturas customizadas pelo administrador do NGFW;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;
- A solução deverá possuir mecanismo de Prevenção de Intrusões (IPS) com capacidade de analisar e bloquear tráfego malicioso, inclusive em conexões criptografadas via SSL/TLS, sem degradação significativa de desempenho;
- O IPS deverá operar em conjunto com o motor de inspeção SSL, permitindo a detecção de ataques e vulnerabilidades em payloads cifrados;
- Registrar no 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;

- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- A solução deverá permitir a criação de múltiplos perfis, contendo a seleção das aplicações, grupos e subgrupos de aplicações com as ações de Bloqueio, detecção e envio do endereço IP para a quarentena no mesmo perfil;
- A solução deverá permitir a utilização dos perfis definidos para criação de regras de roteamento baseado em política (Policy-Based Routing – PBR), com suporte a critérios como endereços de origem, destino, usuários, grupos de usuários, grupo de objetos, portas, DNAT e zonas;
- Possuir opção para administrar as listas estáticas de endereço IP permitidos, e bloqueados com prioridade sobre as assinaturas selecionadas nos perfis existentes e quarentena;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra-ataques de Windows ou NetBios;
- Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol), POP (Post Office Protocol);
- Proteção contra-ataques DNS (Domain Name System);
- Proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- Proteção contra-ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;
- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;

- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;
- A solução deverá suportar, em tráfego criptografado, a realização de verificações automáticas para prevenção de vazamento de dados (DLP) em arquivos transferidos, com capacidade de identificar e prevenir a transmissão de informações sensíveis, tais como:
 - Números de CPF;
 - Endereços de e-mail;
 - Números de cartões de crédito.
- A solução deverá permitir a criação de políticas personalizadas para inspeção e bloqueio de arquivos, além de possibilitar a geração de alertas e registros para auditoria dos eventos relacionados ao vazamento de dados;
- Deverá permitir o administrador ativar automaticamente proteções, com base em parâmetros configuráveis (gravidade da ameaça e ação Monitorar ou Bloquear);
- A solução de IPS deverá possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;
- O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis com base na gravidade da ameaça;
- Deverá suportar referência cruzada com CVE;
- Em cada proteção de segurança, deverá estar incluso informações como:
 - Código CVE (Common Vulnerabilities and Exposures);
 - Severidade;
 - Tipo de ação a ser executada.
- A solução de segurança a ser contratada deverá possuir a funcionalidade nativa de Virtual Patching, permitindo aplicar correções virtuais contra vulnerabilidades conhecidas, sem necessidade imediata de atualização de sistemas operacionais ou serviços expostos.

DAS FUNCIONALIDADES DO THREAT PROTECTION

- Deverá possuir mecanismo de detecção de tráfego malicioso baseado em assinatura, com base em base de dados local e em nuvem, para proteção contra no mínimo para ameaças como exploits, ransomwares, trojans, bots, adware, spyware, hijackers, keyloggers;

- Deverá suportar bloqueio de ameaças com base em comportamento de rede e aplicação, mesmo na ausência de assinaturas conhecidas, utilizando mecanismos de proteção contra ameaças de dia zero;
- A plataforma deverá permitir atualização automática das assinaturas de ameaças, sem a necessidade de intervenção manual, com conectividade a serviços de Threat Intelligence da fabricante;
- Deverá dispor de mecanismos de proteção contra-ataques persistentes e direcionados (APT), com inspeção avançada de tráfego;
- A solução deverá permitir a criação de múltiplos perfis de proteção avançada contra ameaças (ATP), permitindo o uso de configurações distintas por política de segurança, interface ou grupo de usuários;
- Cada perfil de ATP deverá permitir a seleção granular de tipos de arquivos e extensões a serem inspecionados ou bloqueados, com base em extensão do arquivo (ex: .exe, .zip, .js) e/ou tipo MIME (ex: application/x-msdownload, application/javascript, application/pdf);
- A solução deverá suportar a aplicação de perfis de ATP distintos por protocolo, incluindo HTTP, HTTPS (via SSL Inspection), FTP, SMTP e SMB;
- A solução deverá integrar mecanismos de Proteção Avançada Contra Ameaças (ATP), antivírus de fluxo e sandboxing, capazes de realizar análise de conteúdo e detecção comportamental de arquivos, URLs e scripts trafegados em sessões criptografadas SSL/TLS;
- Cada perfil de ATP deverá possibilitar a habilitação do mecanismo de bloqueio de ameaças baseado em reputação de IP, com categorização automática de endereços de origem e destino;
- A solução deverá suportar a categorização de reputação de IP em no mínimo 5 categorias;
- O mecanismo de reputação de IP deverá ser atualizado automaticamente, com base em feed de Threat Intelligence provido pelo fabricante;
- A solução deverá permitir a detecção de aplicativos potencialmente indesejados (PUA/PUP), com opção de bloqueio automático ou quarentena, por política de segurança;
- A solução deverá permitir bloquear o download ou envio de arquivos criptografados, cuja análise de conteúdo não seja possível, garantindo a proteção contra ameaças ocultas em arquivos cifrados;
- Deverá ser possível ativar modo passivo de operação, no qual os eventos de ameaça são apenas registrados sem gerar bloqueio automático, para fins de auditoria ou cenários de homologação;
- A plataforma deverá permitir definir o tamanho máximo de arquivos a serem analisados pelo mecanismo de threat protection, com configuração por perfil de proteção;
- A solução deverá dispor de mecanismo de quarentena de arquivos suspeitos, com parâmetros configuráveis como:
 - Tempo de retenção (dias);
 - Espaço máximo reservado em disco (em GB);
 - Política de exclusão automática de arquivos expirados ou excedentes.
- A solução deverá possibilitar habilitar análises comportamentais e dinâmicas de arquivos em trânsito, como etapa complementar à análise estática, com detecção de ameaças em tempo real baseada em comportamento.

DAS FUNCIONALIDADES DE GERENCIAMENTO E AÇÕES SOBRE ARQUIVOS EM QUARENTENA

- A solução deverá manter registro detalhado de todos os arquivos analisados pelo mecanismo de proteção contra ameaças, incluindo: data/hora, usuário, origem, destino, nome do arquivo, hash (MD5) e status da análise;
- A plataforma deverá disponibilizar tela de quarentena com funcionalidades de busca e filtro avançado, permitindo localização de arquivos por período, nome, usuário, status, hash ou origem/destino;
- A solução deverá permitir, para os arquivos em quarentena no mínimo:
 - Bloquear;
 - Liberar;
 - Efetuar o download direto pela estação do administrador;
 - Excluir.
- Todas as ações realizadas sobre arquivos em quarentena deverão ser registradas em log com data/hora, nome do arquivo, resultado da análise e identidade do administrador responsável pela ação;
- A solução deverá suportar análise de arquivos em ambiente de Sandbox, possibilitando a execução controlada de arquivos suspeitos em ambiente isolado, para verificação de comportamentos maliciosos antes da liberação;
- A solução deverá permitir que a classificação de ameaças identificadas em ambiente de análise comportamental (sandbox) seja utilizada como critério de decisão automatizada, permitindo ações como liberação ou bloqueio com encaminhamento à quarentena, com base em parâmetros de probabilidade ou risco configuráveis pelo administrador;
- Todos os arquivos submetidos ao Sandbox deverão ser registrados com data/hora, hash, nome do arquivo, status da análise e decisão aplicada (bloqueio/liberação).

SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL: FUNCIONALIDADES DE GERENCIAMENTO

- Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;
- A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados;
- A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança;
- O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;
- Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;
- A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;
- A solução deverá permitir a alteração das portas padrão dos serviços de gerenciamento, como SSH e HTTPS, de forma a adequar-se às políticas de segurança e requisitos da rede local;
- Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;
- A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

- A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que poderá ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho;
- Deve possibilitar a gerência de “logs”, realizando as configurações de relatórios de todos os “firewalls” integrados;
- Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet;
- O gerenciamento deverá permitir/possuir:
 - Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;
 - Monitoração de logs;
 - Debugging.
- Deve permitir usar palavras chaves para facilitar identificação de regras;
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Autenticação integrada à base de dados local;
- Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, sub-rede) na base de regras;
- Criação de regras que fiquem ativas em horário definido;
- Habilidade de upgrade via interface de gerenciamento;
- Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;
- Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;
- Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;
- Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Criação de regras que fiquem ativas em horário definido;
- Criação de regras com data de expiração;
- Deve permitir a criação de objetos e políticas compartilhadas;
- Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
- Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais;
- A solução deverá permitir gerenciar templates de customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW's gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

- Título da Página;
- Ícone (favicon);
- Logotipo;
- Imagem de fundo;
- Cores do menu (primária e secundária).
- O sistema deve ser capaz de gerenciar de modo central as políticas de backup do equipamento remotos;
- O sistema deverá permitir habilitar uma mensagem de Disclaimer na página de login da Interface de Administração. Ou seja, a página de login deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema;
- Deve suportar orquestração de VPNs site-to-site e Star (HUB-Spoke);
- Deve suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada;
- Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Identity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);
- A solução deverá oferecer controle de acesso com granularidade de permissões para usuários administradores, permitindo restringir visualização e gerenciamento apenas aos dispositivos designados a cada administrador. Deverá ainda suportar ambiente multi-tenant, com separação lógica de recursos e escopos de administração por usuário ou grupo;
- A solução deverá suportar autenticação de usuários por meio de servidores externos LDAP e RADIUS. Deverá, ainda, oferecer suporte a autenticação multifator (MFA), aumentando a segurança no acesso à interface de gerenciamento;
- Suportar API para integração com sistemas de terceiros;
- Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- Deve ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;
- A Solução deverá permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;
- Ao instalar um equipamento no site remoto, cabear-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;
- A solução deverá permitir a criação de múltiplos e distintos pacotes de configurações:

- De políticas de NGFW;
- Templates de configurações dos serviços;
- Templates de configurações do "zero-touch";
- De backup dos dispositivos gerenciados;
- Dos Perfis de Web filter, Application control, Threat Protection, Intrusion Prevention, Inspeção SSL e SD-WAN.
- Permitir aplicar as configurações acima por dispositivo gerenciado e por grupo de dispositivos.
- A solução de gerenciamento centralizado deverá suportar a visualização georreferenciada dos dispositivos gerenciados, por meio de integração com serviços de mapa como o Google Maps, permitindo a plotagem automática da localização dos equipamentos em interface gráfica;
- A geolocalização deverá ser possível de duas formas:
 - Automática, com base no endereço IP público do dispositivo no momento da conexão com a console de gerenciamento;
 - Manual, mediante o cadastro de coordenadas geográficas (latitude e longitude) diretamente no perfil do dispositivo.
- A funcionalidade deverá permitir a identificação visual da posição geográfica de cada dispositivo, possibilitando filtros, buscas e seleção direta no mapa, para fins de gerenciamento distribuído, troubleshooting regionalizado ou controle de ativos.
- Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- A solução deverá permitir a realização de backups centralizados das configurações dos dispositivos NGFW gerenciados, com suporte a agendamento automático, armazenamento seguro, download e restauração de versões anteriores, além de registro de logs das operações realizadas;
- A solução deverá permitir a criação de políticas de controle de acesso à interface de gerenciamento, restringindo conexões apenas a endereços IP autorizados, de forma a garantir maior segurança e impedir acessos indevidos ao ambiente administrativo.

ALTA DISPONIBILIDADE

- Deve suportar recurso de Alta-Disponibilidade (HA), sendo um primário e outros em modo secundário com sincronização e replicação das configurações;
- O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heartbeat;
- Deve suportar definir o intervalo do sincronismo em minutos;
- Permitir definir o número máximo de falhas dos testes do heartbeat e a solução somente irá convergir para o segundo equipamento após atingir o valor definido;
- Suportar inserir um endereço de e-mail para receber notificações relacionadas ao cluster.

SOLUÇÃO DE ARMAZENAMENTO E GERENCIAMENTO DE LOGS E EVENTOS

- A solução de armazenamento e gerenciamento de logs e eventos, deverá suportar e estar licenciada para receber no mínimo 50GB de logs por dia;

- A solução de armazenamento e gerenciamento de logs e eventos poderá ser entregue na mesma solução de gerenciamento centralizado, desde que atenda aos requisitos solicitados;
- A solução de armazenamento e gerenciamento de logs e eventos deverá ser do mesmo fabricante da solução de segurança e compatível com a ferramenta de gerenciamento centralizado;
- Deverá prover análise de tráfego de rede de modo centralizado;
- Deve possuir análise de tráfego de rede e ameaças por geolocalização;
- Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:
- Análise de ameaças e incidentes de segurança;
- Análise de tráfego e uso de categorias Web;
- Análise de tráfego e uso de aplicativos;
- Análise de tráfego e ameaças por usuário;
- Análise de desempenho de políticas de segurança.
- A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;
- Deverá possuir ferramenta para salvar consultas avançadas;
- Deve permitir a criação de relatórios e Dashboards personalizados. No mínimo os seguintes relatórios deverão ser gerados:
- Consumo de banda;
- Resumo gráfico de aplicações utilizadas;
- Principais aplicações por utilização de largura de banda;
- Monitoramento de jitter, latência, perda de pacotes.
- Possuir a capacidade de personalização de gráficos como mapa de calor, pizza, área, barra, linha e tabela;
- Possuir mecanismo para que logs antigos sejam removidos automaticamente;
- Deverá ser capaz de efetuar o arquivamento de relatórios;
- Deve possuir agendamento de relatórios;
- Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);
- Permitir o envio de relatórios por e-mail para até 5 endereços distintos;
- Capacidade de coletar logs de múltiplos dispositivos de segurança e rede, consolidando as informações em um único ponto para facilitar a análise e o monitoramento;
- Relatório por Dispositivo;
- Relatório por grupo de dispositivo;

- Relatório Consolidado;
- Possibilidade de construir dashboards customizados e interativos que apresentem informações em tempo real, com suporte a diversos tipos de visualizações gráficas;
- Implementação de filtros avançados que permitam segmentar os dados por critérios como período, tipo de evento, dispositivo ou usuário;
- Opções para personalizar a aparência dos relatórios e dashboards, incluindo logotipo da organização, cores e layout, alinhando-os à identidade visual institucional;
- Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- A solução deverá suportar o uso de múltiplos dispositivos Loggers, permitindo a coleta e centralização de logs;
- A solução deverá permitir a configuração de cluster de Loggers com alta disponibilidade, suportando servidores redundantes com replicação automática e em tempo real dos logs, além de failover automático para garantir a continuidade da coleta em caso de falha do servidor principal.

6.5 REQUISITOS PARA A INSTALAÇÃO

- Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;
- Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;
- A instalação **deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;**

6.6 REQUISITOS PARA TREINAMENTOS

- Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware ou software) para a equipe do cliente;
- Carga Horária mínima de 30 horas em modo presencial;
- Deve ser fornecido treinamento do tipo hands-on de, no mínimo, 08 (oito) horas para repasse de conhecimento, ou acesso a plataforma EAD com aulas gravadas para administração da solução ofertada de NGFW;
- O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;
- O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas;
- Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação (coffee break), instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
- O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;
- Caso fornecido em modo presencial, deverá ser fornecido um 01 lanche (coffee break) no período da manhã e outro no período da tarde, suficiente para todos os alunos;
- Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;

- Este treinamento poderá ser realizado em ambiente externo ao da CONTRATANTE, inclusive com os recursos para laboratórios (hands-on) salvo em caso de necessidade e acordo entre CONTRATADA e CONTRATANTE;
- Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE;
- A CONTRATADA deverá ofertar as instalações na localidade da CONTRATANTE para a realização dos treinamentos com os requisitos mínimos de infraestrutura de sala de treinamento;

6.7 REQUISITOS PARA SUPORTE TÉCNICO

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 8x5 (Segunda a sexta-feira das 09:00 às 17:00, exceto feriados, horário de Brasília), pelo tempo de contrato, com as seguintes características:
- A contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;
- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.

7 Estimativa da demanda - quantidade de bens e serviços

A estimativa da solução será a descrita na tabela abaixo:

item	Descrição	Qtde	Vigência
1	Appliance NGFW (Hardware + Software integrados)	1	Enquanto perdurar a vida útil do equipamento
2	Licenciamento (Secure SD-WAN, IPS, ATP, WebFilter, AppControl)	1	12 meses
3	Instalação e configuração	1	Execução única
4	Suporte técnico e atualização de versões	1	12 meses
5	Treinamento operacional e de administração do firewall	3	Execução única

8 Levantamento de soluções

Foi realizado o levantamento das alternativas disponíveis no mercado para atender à necessidade de modernização da segurança perimetral do ICSEZ /UFAM.

O levantamento considerou soluções de **firewall de próxima geração (Next Generation Firewall – NGFW)** capazes de prover **alta disponibilidade, SD-WAN, controle de aplicações, inspeção SSL e integração com o Active Directory**, requisitos indispensáveis para o ambiente institucional. As informações foram obtidas a partir de **cotações públicas, atas de registros de preços e do relatório de Prova de Conceito (PoC)** constante do processo SEI nº **23105.024545/2025-03**.

As alternativas identificadas foram as seguintes:

ID	Descrição da Solução
01	Aquisição de nova solução de Firewall NGFW – BlockBit BBX700 , com licenciamento completo (IPS, Application Control, WebFilter, VPN SSL/IPSec, Anti-Malware, Sandbox AI) e suporte técnico de 12 meses, conforme proposta comercial nº 19933/2, datada de 02/09/2025.
02	Manutenção do ambiente atual baseado em pfSense , mantendo o firewall de software livre instalado em hardware genérico, sem suporte técnico oficial, sem autenticação centralizada e sem alta disponibilidade nativa.
03	Alternativas de mercado equivalentes , como Fortinet FG-600P e Palo Alto PA-3430 , avaliadas com base em especificações técnicas e valores estimados de mercado, representando soluções de referência internacional.

A partir desse levantamento, verificou-se que, entre as soluções avaliadas, o **BlockBit BBX700** se destacou por apresentar o **melhor custo-benefício** e ser a opção **mais aderente ao cenário de infraestrutura de médio porte**, equilibrando desempenho e suporte técnico nacional.

9 Análise comparativa de soluções

Foram analisadas três alternativas de solução de firewall de próxima geração e a solução de firewall atual com base nos critérios de desempenho, complexidade de administração, suporte técnico, custo de implantação e adequação ao porte da infraestrutura do **ICSEZ: pfSense (solução atual), BlockBit BBX700, Fortinet FG-600P e Palo Alto PA-3430**.

A solução atualmente empregada, **pfSense (software livre)**, apresenta **limitações técnicas relevantes**, especialmente no gerenciamento de múltiplos links, na ausência de autenticação centralizada e na falta de suporte técnico oficial. Seu modelo depende de hardware genérico e de configurações manuais, dificultando a manutenção e impedindo o cumprimento de requisitos de alta disponibilidade (HA) e segurança preconizados pela **Política de Segurança da Informação e Privacidade da Administração Pública Federal (PPSI)**.

Em contraste, a **solução BlockBit BBX700** oferece **arquitetura integrada de segurança**, com módulos de **NGFW, SD-WAN, IPS, controle de aplicações, Web Filter, VPN SSL/IPSec e armazenamento local de logs**, todos gerenciáveis por interface gráfica unificada. Durante a **prova de conceito (processo SEI nº 23105.024455/2025-03)**, o equipamento demonstrou estabilidade, fácil administração e desempenho adequado ao tráfego institucional, destacando-se pelo suporte técnico nacional e pela integração nativa de alta disponibilidade.

As soluções **Fortinet FG-600P** e **Palo Alto PA-3430**, embora apresentem maior desempenho bruto e reconhecimento internacional (inclusive com liderança no quadrante Gartner), **são direcionadas a redes de grande escala** e implicam **custos mais elevados de aquisição e manutenção**, além de **licenciamento fracionado e dependência de módulos externos** (como o FortiAnalyzer, no caso da Fortinet).

Em síntese, a comparação técnica indica que o **BlockBit BBX700** é a alternativa mais aderente ao porte e às necessidades do **ICSEZ/UFAM**, conciliando **robustez, suporte local, segurança e economicidade**, representando a melhor solução para a modernização da infraestrutura de rede.

10 Registro de soluções consideradas inviáveis

Durante o levantamento de mercado, foram analisadas as soluções **pfSense (software livre), Fortinet FG-600P e Palo Alto PA-3430**, que, após avaliação técnica e econômica, foram consideradas **inviáveis** para o cenário do **ICSEZ/UFAM**, conforme os critérios de sustentabilidade, suporte, custo total de propriedade e adequação à infraestrutura existente.

11 Análise comparativa de custos (TCO)

Para garantir **transparência e economicidade**, foi conduzida a análise do **Custo Total de Propriedade (TCO)**, abrangendo o investimento inicial, licenciamento, suporte técnico e manutenção pelo período de 12 meses.

A comparação tomou como base a **proposta comercial nº 19933/2 da BlockBit** e as **referências disponíveis no Portal Nacional de Contratações Públicas (PNCP)**, considerando equipamentos de **desempenho e porte equivalentes**.

Quadro Comparativo de Custos e Desempenho (Equipamentos Equivalentes)

Solução	Modelo / Fabricante	Desempenho NGFW / FW	Custo Estimado (R\$)	Observações
BlockBit BBX700	BlockBit Tecnologia Ltda	6,5 Gbps / 55 Gbps	51.029,30	Inclui hardware, licenças UTM completas, suporte e instalação. Suporte nacional.
Fortinet FG-600P	Fortinet Inc.	11,5 Gbps / 139 Gbps	~R\$ 210.000,00	Alto desempenho, porém custo elevado; necessita de módulos adicionais (FortiAnalyzer e FortiManager) e licenças UTM separadas.
Palo Alto PA-3430	Palo Alto Networks Inc.	9,2–10,5 Gbps / 25,5 Gbps	~R\$ 300.000,00	Equipamento corporativo de grande porte; licenciamento separado e suporte internacional com custo mais alto.

Síntese da Análise

A análise demonstra que o **BlockBit BBX700** apresenta o **menor custo total de propriedade**, mantendo desempenho compatível e todas as funcionalidades requeridas — **alta disponibilidade (HA)**, **SD-WAN inteligente**, **IPS/ATP**, **controle de aplicações**, **VPN SSL/IPSec** e **armazenamento local de logs e cache**.

Nota Metodológica – Pesquisa de Preços

Durante a pesquisa de mercado, **não foram identificadas atas federais no PNCP que apresentassem cenários equivalentes ao ambiente técnico e institucional do ICSEZ/UFAM**, envolvendo soluções de firewall de médio porte com múltiplos links e subscrição completa.

Assim, os valores apresentados foram **estimados a partir de verificações em fontes oficiais dos fabricantes e distribuidores** — incluindo **BlockBit Tecnologia Ltda, Fortinet Inc. e Palo Alto Networks Inc.** — e comparativos técnicos disponíveis em domínio público.

Essa metodologia garante **razoabilidade, transparência e aderência** às práticas de estimativa de custo previstas na **Instrução Normativa SGD/ME nº 94/2022**, assegurando parâmetros realistas para a análise de economicidade.

12 Descrição da solução de TIC a ser contratada

A solução de TIC proposta consiste na **aquisição e implementação de um firewall de próxima geração (Next Generation Firewall – NGFW) modelo BlockBit BBX700**, com licenciamento completo, suporte técnico nacional e recursos integrados de segurança e alta disponibilidade.

O equipamento tem como objetivo **substituir a atual infraestrutura baseada em pfSense** que apresenta limitações quanto à confiabilidade, suporte e escalabilidade.

Com a nova solução, o **ICSEZ** passará a dispor de um **ambiente de segurança unificado, gerenciável e aderente às políticas de segurança da informação** da Administração Pública Federal.

O **BlockBit BBX700** oferece funcionalidades avançadas, como:

- **Firewall de próxima geração (NGFW)** com inspeção profunda de pacotes e controle de aplicações;
- **SD-WAN inteligente** com balanceamento e failover automático de múltiplos links, garantindo maior disponibilidade em cenário de conectividade instável, como o do município de Parintins;
- **Sistema de prevenção e detecção de intrusões (IPS/IDS)** e **proteção avançada contra ameaças (ATP)**;
- **VPN SSL/IPSec**, autenticação centralizada, filtro de conteúdo web e controle de banda;

- **Armazenamento interno dedicado a logs e cache de proxy web**, otimizando o desempenho da rede;
- **Alta disponibilidade (HA)** integrada, dispensando hardware adicional.

A solução foi **avaliada durante prova de conceito de 30 dias** (Processo SEI nº 23105.024455/2025-03), tendo demonstrado **plena compatibilidade com o ambiente institucional, estabilidade sob carga e facilidade de administração**.

13 Estimativa de custo total da contratação

Valor (R\$): 51.029,30

A estimativa de custo total foi calculada com base na **proposta comercial nº 19933/2 da BlockBit**, referente ao modelo **BBX700**, que contempla hardware, licenciamento completo, instalação e **12 meses de suporte técnico e atualização**. O valor total estimado é de **R\$ 51.029,30 (cinquenta e um mil, vinte e nove reais e trinta centavos)**.

Esse valor representa o **Custo Total de Propriedade (TCO)** da solução para o primeiro ano de uso, sem necessidade de módulos adicionais ou licenciamento complementar, o que assegura **previsibilidade orçamentária e redução de custos recorrentes**.

Observação: Durante a pesquisa, não foram identificadas atas federais com cenários equivalentes ao porte do ICSEZ/UFAM.

Assim, a contratação proposta apresenta **custo proporcional, sustentável e plenamente compatível** com a capacidade orçamentária do campus, configurando-se como a opção de **melhor relação custo-benefício**.

14 Justificativa técnica da escolha da solução

A definição da solução **BlockBit BBX700** resulta de análise técnica aprofundada, que considerou desempenho, compatibilidade com a infraestrutura atual do **ICSEZ/UFAM**, custo total de propriedade e maturidade tecnológica do fabricante.

Durante a **prova de conceito (PoC)** conduzida pela Gerência de Tecnologia da Informação (processo SEI nº 23105.024545/2025-03), o equipamento demonstrou estabilidade, desempenho consistente sob carga de tráfego institucional e plena integração com os sistemas internos. A funcionalidade **SD-WAN com failover automático** mostrou-se especialmente eficiente diante das oscilações de conectividade observadas no município de Parintins, garantindo continuidade dos serviços administrativos e acadêmicos.

Na análise comparativa de mercado, verificou-se que os modelos **Fortinet FG-600P** e **Palo Alto PA-3430** são equivalentes em porte e desempenho ao BlockBit BBX700. Entretanto, essas soluções internacionais apresentam **custos substancialmente mais elevados**.

15 Justificativa econômica da escolha da solução

A seleção da solução **BlockBit BBX700** fundamenta-se em critérios objetivos de **economicidade, eficiência operacional e racionalização de gastos públicos**, conforme o disposto no art. 11 da **Lei 14.133/2021** e nas diretrizes da **Instrução Normativa SGD/ME nº 94/2022**.

O **Custo Total de Propriedade (TCO)** da solução foi comparado com o de equipamentos equivalentes de mercado — **Fortinet FG-600P** e **Palo Alto PA-3430** — que apresentam desempenho semelhante, porém custos substancialmente mais elevados, conforme demonstrado na análise técnica.

Enquanto o **BlockBit BBX700** possui valor total de **R\$ 51.029,30**, incluindo hardware, licenças UTM completas, suporte e instalação, as soluções internacionais apresentam **valores médios entre R\$ 210 mil e R\$ 300 mil**, exigindo licenciamento fracionado e contratos adicionais de suporte e relatórios.

Além do investimento inicial reduzido, o modelo da BlockBit oferece **suporte técnico nacional e licenciamento unificado**, reduzindo despesas administrativas e eliminando custos recorrentes com módulos adicionais (como o **FortiAnalyzer**, no caso da Fortinet).

A estrutura de custos torna-se, portanto, **mais previsível e sustentável**, assegurando a continuidade dos serviços sem a necessidade de contratações complementares.

Essa solução também representa um **avanço estratégico na gestão orçamentária**, pois viabiliza a modernização da infraestrutura de segurança da informação com um investimento compatível com o porte e as restrições orçamentárias do campus de Parintins.

16 Benefícios a serem alcançados com a contratação

A presente contratação representa um **marco na modernização da infraestrutura de TIC do ICSEZ/UFAM**, marcando a transição de uma solução convencional baseada em software livre para uma **plataforma integrada de segurança de última geração**.

Com a adoção do **BlockBit BBX700**, o campus de Parintins passará a operar com padrões de conectividade e segurança equivalentes aos utilizados em centros tecnológicos de médio porte da Administração Pública Federal e similar aos equipamentos adotados na UFAM Capital

Entre os principais benefícios esperados, destacam-se:

- **Modernização tecnológica:** implantação de solução profissional, automatizada e centralizada, com gestão unificada de políticas de segurança e controle de tráfego.
- **Maior disponibilidade de rede:** os módulos de **alta disponibilidade (HA)** e **balanceamento inteligente de múltiplos links (SD-WAN)** garantem estabilidade e continuidade dos serviços institucionais, reduzindo falhas recorrentes de conectividade.
- **Fortalecimento da segurança da informação:** inspeção de tráfego, prevenção de intrusões e análise automatizada de ameaças, em conformidade com o **PPSI**.
- **Integração com sistemas institucionais:** autenticação centralizada via **Active Directory (AD/LDAP)** e controle por perfis de usuário, ampliando a governança sobre acessos.
- **Eficiência e economia:** consolidação de múltiplas funções (firewall, IDS/IPS, antivírus, proxy e cache) em um único equipamento, reduzindo custos operacionais e de manutenção.
- **Gestão e auditoria aprimoradas:** armazenamento interno de alta capacidade para logs e relatórios, viabilizando rastreabilidade e conformidade com normas de auditoria.
- **Alinhamento estratégico:** a solução está em consonância com o **Plano de Transformação Digital do Governo Federal (Decreto nº 10.332/2020)**, reforçando o compromisso do ICSEZ com a modernização e a eficiência dos serviços públicos digitais.

Assim, a contratação consolida um **salto qualitativo na gestão de segurança e desempenho da rede institucional**, elevando o ICSEZ a um novo patamar tecnológico compatível com os desafios da transformação digital.

17 Providências a serem Adotadas

Para viabilizar a contratação proposta, deverão ser adotadas as seguintes providências administrativas e técnicas:

1. **Elaboração e aprovação do Termo de Referência (TR)** com base nas informações deste Estudo Técnico Preliminar (ETP), contendo a especificação detalhada do equipamento, licenciamento, suporte técnico e critérios de aceitação.
2. **Parecer técnico e jurídico** sobre a viabilidade e conformidade da contratação, nos termos da Lei nº 14.133/2021 e da Instrução Normativa SGD /ME nº 94/2022.
3. **Definição do modelo de contratação** — aquisição direta ou via adesão a ata de registro de preços pública — observando o princípio da economicidade e os parâmetros de mercado verificados no PNCP.
4. **Encaminhamento do processo SEI nº 23105.040523/2025-82** para tramitação junto aos setores competentes da UFAM, com a devida instrução documental, incluindo:
 - este Estudo Técnico Preliminar (ETP);
 - Termo de Referência;
 - proposta comercial nº 19933/2 da BlockBit;
 - Relatório Técnico de Monitoramento de Link (SEI nº 23105.046854/2025-26).
 - Relatório Técnico da PoC (SEI nº 23105.024545/2025-03)
5. **Execução da contratação e instalação da solução**, com posterior validação técnica pela equipe da **Gerência de Tecnologia da Informação (GTI/ICSEZ)**, assegurando conformidade com os requisitos de segurança, desempenho e disponibilidade.

Essas medidas garantirão a formalização adequada do processo e a implantação de uma solução de segurança de rede moderna, eficiente e alinhada às políticas de governança digital da Administração Pública Federal.

18 Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A contratação é considerada **plenamente viável** sob os aspectos técnico e econômico, pelos seguintes motivos:

- **Desempenho comprovado:** a solução foi avaliada em **prova de conceito (PoC)** registrada no processo **SEI nº 23105.024455/2025-03**, demonstrando estabilidade, integração e eficiência no tratamento de tráfego e segurança.
- **Economicidade:** conforme cotações e **atas públicas federais** consultadas no **PNCP**, soluções equivalentes (Fortinet e Palo Alto) apresentam custos mais elevado, enquanto a BlockBit oferece funcionalidades semelhantes por **R\$ 51.029,30**, com suporte e licenciamento integrados.
- **Aderência normativa:** atende às diretrizes da **Lei nº 14.133/2021**, **IN SGD/ME nº 94/2022**, **PPSI (Decreto nº 10.222/2020)** e **Estratégia de Governo Digital (Decreto nº 10.332/2020)**.
- **Evolução tecnológica:** representa um **marco na modernização da infraestrutura de TI do ICSEZ**, substituindo o modelo atual baseado em software livre por uma **plataforma integrada de segurança de nova geração**, com alta disponibilidade, SD-WAN e armazenamento de logs.

Dessa forma, a contratação do **BlockBit BBX700** é **tecnicamente adequada, economicamente vantajosa e institucionalmente estratégica**, assegurando modernização e confiabilidade à rede do ICSEZ – Campus Parintins.

19 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](#).

Documento assinado digitalmente
 **RAFAEL REIS MAFRA**
Data: 11/11/2025 16:31:21-0300
Verifique em <https://validar.iti.gov.br>

RAFAEL REIS MAFRA
Presidente

Documento assinado digitalmente
 **GEANDRO FARIAS DE MATOS**
Data: 11/11/2025 17:06:00-0300
Verifique em <https://validar.iti.gov.br>

GEANDRO FARIAS DE MATOS
Membro da equipe de planejamento

Documento assinado digitalmente
 **JOEL BENTES DA SILVA JUNIOR**
Data: 11/11/2025 16:39:09-0300
Verifique em <https://validar.iti.gov.br>

JOEL BENTES DA SILVA JUNIOR
Membro da equipe de planejamento