# TERMO DE REFERÊNCIA

## TERMO DE REFERÊNCIA - CARACTERÍSTICAS DA CONTRATAÇÃO

### 1 OBJETIVO

1.1 Contratação de soluções de proteção de redes para o TRE-GO, com garantia técnica, compostas por clusters de firewalls NGFW (Next-Generation Firewall, ou Firewall de Próxima Geração). As soluções devem incluir seus dispositivos, softwares, e as consoles de gerenciamento integrado, mediante criação de Ata de Registro de Preços.

### 2 OBJETO A SER CONTRATADO

2.1 Aquisição de soluções de firewalls NGFW com garantia técnica, para prover segurança perimetral com administração e gerenciamento das políticas de segurança, incluindo os dispositivos de proteção de rede Firewalls, com controle de acesso e de ameaças, funcionalidades de NGFW incluindo as consoles para gerenciamento centralizado desses firewalls, mediante criação de Ata de Registro de Preços;

2.1.1 Os equipamentos que compõem esta aquisição devem ser novos e não ter a descontinuidade anunciada pelo fabricante e que estejam íntegros.

2.2 As soluções devem compreender os seguintes itens:

| Grupo | Item | Tipo | Descrição | CATMAT/ CATSER | Qtde |
|---|---|---|---|---|---|
| 1 | 1 | Appliance físico | Cluster de alta disponibilidade TIPO 1, de firewalls com funcionalidades de NGFW (Next Generation Firewall). | 609340 | 1 |
| | 2 | Appliance físico | Cluster de alta disponibilidade TIPO 2, de firewalls com funcionalidades de NGFW (Next Generation Firewall) para segmentação de rede interna. | 609340 | 1 |
| | 3 | Appliance virtual | Console de gerenciamento centralizado | 27472 | 1 |
| | 4 | Serviço | Serviço de migração de firewalls para a nova solução. | 26972 | 2 |
| | 5 | Appliance físico | Firewalls com funcionalidades de NGFW (Next Generation Firewall) de menor porte para unidades remotas. | 609340 | 200 |
| | 6 | Serviço | Treinamento (Repasse de conhecimento) | 20052 | 1 |

### 3 JUSTIFICATIVA/MOTIVAÇÃO/RESULTADOS ESPERADOS

**3.1 Motivação/Justificativas:**

| Item | Tipo | Justificativas | Qtde |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Appliance físico - Cluster de alta disponibilidade TIPO 1 | Substituição dos equipamentos em uso que estão fora de garantia e com serviços a serem descontinuados pela fabricante. Padronização dos equipamentos para obter uma gerência única e facilitada através de uma única plataforma, por se tratar de uma solução de segurança complexa e crítica presente no datacenter no Tribunal. | 1 |
| 2 | Appliance físico - Cluster de alta disponibilidade TIPO 2 | Substituição dos equipamentos em uso que estão fora de garantia e com serviços a serem descontinuados pela fabricante. Padronização dos equipamentos para obter uma gerência única e facilitada através de uma única plataforma, por se tratar de uma solução de segurança complexa e crítica presente no datacenter no Tribunal Regional Eleitoral de Goiás. Segmentação da rede interna. | 1 |
| 3 | Appliance virtual - Console de gerenciamento centralizado | Software necessário para gerência (configuração e manutenção) e monitoramento dos equipamentos descritos nos itens 1,2 e 5. | 1 |
| 4 | Serviço - migração de firewalls para a nova solução | Serviços necessários para migração da solução existente para a nova solução referente aos dos itens 1 e 2. | 2 |
| 5 | Appliance físico - Firewalls com funcionalidades de NGFW de menor porte | Substituição dos equipamentos em uso que estão fora de garantia e com serviços a serem descontinuados pela fabricante. Padronização dos equipamentos para obter uma gerência única e facilitada através de uma única plataforma, por se tratar de uma solução de segurança complexa e crítica presente nas Zonas Eleitorais e outros locais onde o Tribunal possui conexões. | 200 |
| 6 | Serviço - Treinamento | Necessário para nivelamento da equipe do TRE-GO nas operações dos equipamentos e a sua utilização. | 1 |

**3.2 Objetivos Táticos**

| Objetivo | Necessidade de Negócio |
|---|---|
| Garantir a Sustentabilidade Tecnológica | Assegurar a disponibilidade, estabilidade e reparabilidade dos equipamentos de TIC por meio da aquisição de soluções novas e com garantia estendida |
| Sustentar a Segurança e a Gestão de Dados (OE.07 do PDTIC) | Fortalecer os mecanismos de segurança da informação, privacidade e continuidade dos serviços essenciais ao funcionamento do Tribunal |
| Promover Serviços de Infraestrutura Corporativa (OE.09 do PDTIC): | Prover os recursos tecnológicos necessários aos serviços do TRE-GO, com os níveis de qualidade e disponibilidade requeridos |

**3.3 Objetivos Operacionais**

| Objetivo | Necessidade de Negócio |
|---|---|
| Garantir a Conectividade Segura | Implementar uma solução unificada de Firewall/Gateway VPN para garantir a conectividade de rede segura entre as unidades remotas e a sede do TRE-GO |
| Aprimorar o Controle de Acesso | Melhorar o nível de segurança do acesso aos dados, além dos controles e mecanismos de monitoramento e administração dos serviços de rede desta Justiça Eleitoral |
| Substituição de Ativos Obsoletos | Substituir o parque de equipamentos de rede de segurança que foram descontinuados, inviabilizando a contratação de suporte e atualização essenciais |

**3.4 Benefícios esperados:**

| Tipo | Benefício | Justificativa |
|---|---|---|

| | | |
|---|---|---|
| Eficácia e Performance | Aumento da performance e velocidade do tráfego de dados | A Solução deve proporcionar maior velocidade e segurança no tráfego de dados, adequada à capacidade do novo Backbone |
| Segurança e Confiabilidade | Implementação de maior segurança e controles na rede de dados | Contribui para o Objetivo Estratégico OE-10 ("Fortalecer a Estratégia Nacional de TIC e de Proteção de Dados"). A aquisição fortalece a infraestrutura de rede para atender às novas demandas e tecnologias. |
| Garantia e Disponibilidade | Aumento da disponibilidade, estabilidade e reparabilidade dos equipamentos | Exigência de garantia de, no mínimo, 60 meses, prevenindo que os bens se tornem inservíveis a curto prazo. |
| Economicidade | Redução da necessidade de futuras licitações em curto prazo. | A contratação de equipamentos não descontinuados e com garantia estendida propicia economia ao Tribunal e diminui a necessidade de trocas frequentes |
| Conformidade Legal | Cumprimento das diretrizes da LGPD e ENSEC-PJ. | O planejamento está alinhado com a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), garantindo que os novos mecanismos de proteção de dados estejam em conformidade com a Lei Geral de Proteção de Dados (LGPD). |

## 4 **ALINHAMENTO ESTRATÉGICO**

A aquisição da Solução de Firewall (NGFW) alinha-se com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2021-2026 (revisão 2024) do Tribunal Regional Eleitoral de Goiás (TRE-GO), que visa aprimorar a segurança da informação e a infraestrutura tecnológica. A iniciativa responde à necessidade de substituição de equipamentos descontinuados, garantindo a conectividade de rede segura entre unidades remotas e a Sede, e promovendo segurança, confiabilidade e desempenho no tráfego de dados. A contratação está em consonância com o Objetivo Estratégico OE-10 do Planejamento Estratégico da Justiça Eleitoral de Goiás ("Fortalecer a Estratégia Nacional de TIC e de Proteção de Dados"), e com os objetivos do PDTIC de "Promover a segurança da informação e a Gestão de Dados" (OE.07) e "Promover Serviços de Infraestrutura e Soluções Corporativas" (OE.09). A compra se enquadra nas categorias de Infraestrutura (INF) e Segurança Cibernética (SEG) do Anexo V – Plano de Iniciativas do PDTIC. Operacionalmente, busca-se garantir a conectividade segura, aprimorar o controle de acesso e aprimorar a infraestrutura de rede.

Os Benefícios e Resultados esperados justificam a contratação em termos de eficácia, eficiência, economicidade e conformidade legal. Em termos de Eficácia e Performance, espera-se o aumento da velocidade do tráfego de dados, adequado à capacidade do novo Backbone. Quanto à Economicidade, a aquisição de ativos novos e com garantia estendida (mínimo de 60 meses) visa aumentar a disponibilidade, estabilidade e reparabilidade dos equipamentos, evitando que se tornem inservíveis a curto prazo. Finalmente, em relação à Conformidade Legal, a solução contribui para a implementação de maior segurança e controles na rede de dados, alinhando o planejamento à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e garantindo a proteção de dados em conformidade com a Lei Geral de Proteção de Dados (LGPD).

## 5 **FONTE DE RECURSOS**

Para execução desta ação entendemos, s.m.j., que os recursos financeiros deverão ser provenientes da verba destinada para Aquisição de Equipamentos de Informática da programação Orçamentária de 2025/2026.

## 6 **ESTIMATIVA DE PREÇOS**

As planilhas de cálculo para estimativa de preços e os orçamentos seguem no Anexo I deste Termo de Referência.

## 7 **ESPECIFICAÇÕES TÉCNICAS:**

**7.1 Características gerais das soluções de proteção de redes, clusters de alta disponibilidade, ITEM 1 e ITEM 2:**

7.1.1 A solução deve, por meio de seus itens e componentes (que devem ter desempenho suficiente para ativação simultânea de todas as funcionalidades e recursos) permitir a configuração e implementação de políticas de segurança que incluem as seguintes funcionalidades e recursos de NGFW: Controle de Acesso por protocolo, por endereçamento e por aplicação, IPS (Intrusion Prevent System, ou Sistema de Prevenção a Intrusão), Anti-malware, Filtro de URL, Identificação de Usuário, Threat Prevention (Prevenção a Ameaças), e Anti-bot para todos os firewalls e seus clusters de alta disponibilidade especificados a seguir;

7.1.2 As soluções do Item 1 e Item 2 devem ser do mesmo fabricante;

7.1.3 Deve suportar análise em camada 7 (sete), permitindo implementar políticas baseadas em protocolos e aplicações;

7.1.4 As funcionalidades de firewall NGFW descritas nesta especificação devem ser disponibilizadas por clusters de alta disponibilidade, cada um com 02 (dois) dispositivos de proteção de rede (firewalls) em hardware (do tipo “físico”);

7.1.5 Todas as funcionalidades dos dispositivos de firewalls NGFW devem ser implementadas no mesmo conjunto de equipamentos, não sendo aceitas soluções que necessitem de combinação de diferentes produtos para composição dos dispositivos de segurança de rede;

7.1.6 Os equipamentos fornecidos devem ter sido projetados para montagem em rack 19″ (dezenove) polegadas, acompanhados de todos os acessórios necessários para operacionalização – incluindo kit tipo trilho para

adaptação, se necessário, e cabos de alimentação;

7.1.7 Os equipamentos fornecidos devem possuir alimentação elétrica (2P+T) a partir de, no mínimo, 02 (duas) fontes independentes, redundantes e com funcionalidade de hot-swap (em caso de falha de um dos componentes, o equipamento deve continuar a funcionar sem prejuízo às aplicações), capazes de operar entre 110 a 240V AC com frequência de 60 (sessenta) Hertz, com reconhecimento automático do nível de tensão e cabos separados de alimentação (padrão C13/14);

7.1.8 O software da solução de segurança deve ser fornecido em sua última versão disponibilizado pelo fabricante;

7.1.8.1 Não será permitido atendimento de requisitos do Edital através de promessa de versões futuras;

7.1.8.2 Não serão aceitas versões experimentais, versões de teste, versões customizadas para clientes específicos ou que não estejam publicadas no site do próprio fabricante;

7.1.8.3 A solução de segurança deve ser disponibilizada com licenças de uso perpétuo para o pleno funcionamento, pelo menos, das funcionalidades de Firewall, VPN, gerência centralizada e logs.

7.1.8.4 As funcionalidades referentes a bases de conhecimento ou assinaturas de ataques, aplicações, vulnerabilidades ou técnicas de evasão de dados, relacionados nos requisitos 7.1.10.22.6 (“Deve atualizar a base de assinaturas de aplicações manual ou automaticamente; “), e 7.1.10.23.2 (Deve incluir o fornecimento e atualização de bases de conhecimento ou de assinaturas para prevenção de instrução (IPS) e bloqueio de arquivos maliciosos (anti-malware); “) podem ter o fornecimento vinculado ao período de vigência do contrato;

7.1.9 Durante a vigência do contrato devem ser fornecidas todas as atualizações, de sistemas operacionais, software, patches (correções), incluindo também as necessárias para as funcionalidades dependentes de atualizações fornecidas pelo fabricante, como: de bases de assinaturas de ataques, de aplicações, e evasão de dados;

7.1.10 Recursos e funcionalidades dos firewalls NGFW:

7.1.10.1 Os dispositivos de proteção de rede devem possuir, no mínimo, as seguintes funcionalidades:

7.1.10.2 Suportar IPv4 e IPV6, inclusive simultaneamente (dual-stack, ou pilha dupla);

7.1.10.3 Suporte a pelo menos 4094 VLANs (VLAN tags) 802.1q;

7.1.10.4 Agregação de links 802.3ad e LACP (Link Aggregation Control Protocol);

7.1.10.4.1 Suportar ao menos 128 VLANs por conjunto de links 802.3ad;

7.1.10.5 Permitir a manipulação dos tempos de time-out (expiração) de conexões e sessões, sejam novas ou já estabelecidas;

7.1.10.6 Permitir a manipulação dos tempos de sessão estabelecidos, possibilitando sua customização por protocolo;

7.1.10.7 Suportar roteamento baseado em políticas (PBR, ou Policy Based Routing), nos seguintes critérios:

7.1.10.7.1 Baseado em protocolo;

7.1.10.7.2 Baseado em porta de destino;

7.1.10.7.3 Baseado no endereçamento de origem;

7.1.10.8 Suportar roteamento de protocolo IP:

7.1.10.8.1 Para IPv4: deve suportar roteamento estático, dinâmico e multicast;

7.1.10.8.2 Para IPv6: deve suportar roteamento estático e dinâmico;

7.1.10.9 Suportar os protocolos de roteamento dinâmico:

7.1.10.9.1 BGP, com suporte a extensões de múltiplos protocolos, conforme descrito nestas RFCs, ou outras que a substituam ou atualizem:

7.1.10.9.1.1 RFC 2545,

7.1.10.9.1.2 RFC 2858,

7.1.10.9.1.3 RFC 3392;

7.1.10.9.2 OSPF;

7.1.10.9.3 RIP;

7.1.10.9.4 IGMP;

7.1.10.10 Roteamento multicast, incluindo PIM-SM;

7.1.10.11 Suportar a adição na tabela de roteamento de, no mínimo, 20.000 (dez mil) rotas dinâmicas;

7.1.10.12 Suportar a configuração como:

7.1.10.12.1 DHCP Relay;

7.1.10.12.2 DHCP Server;

7.1.10.13 Suportar os seguintes tipos de NAT:

7.1.10.13.1 NAT dinâmico (N:1), ou seja, 1(um) endereço de NAT para vários endereços IP (many-to-1);

7.1.10.13.2 NAT dinâmico (N:N), ou seja, vários endereços de NAT para vários endereços IP;

7.1.10.13.3 NAT estático (1:1), ou seja, 1(um) endereço de NAT para 1 endereços IP ;

7.1.10.13.4 NAT estático (N:N)

7.1.10.13.5 NAT estático bidirecional 1:1;

7.1.10.13.6 Tradução de porta (PAT);

7.1.10.13.7 NAT de Origem;

7.1.10.13.8 NAT de Destino;

7.1.10.14 Suportar a configuração de NAT:

7.1.10.14.1 NAT de origem e NAT de destino simultaneamente;

7.1.10.14.2 NAT para objetos dinâmicos, como: listas externas de endereços IPs, nomes de domínios, URLs, FQDN e Data Centers;

7.1.10.14.3 CGNAT (Carrier Grade Network Address Translation), 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;

7.1.10.15 Permitir a divulgação de endereços ARP de NATs, usando proxy ARP ou recurso semelhante;

7.1.10.16 Proteção contra spoofing;

7.1.10.17 Os dispositivos de proteção devem ser capazes de operar nos seguintes modos:

7.1.10.17.1 Modo camada 2 (dois), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

7.1.10.17.2 Modo camada 3 (três), para inspeção de dados em linha e ter visibilidade e controle de tráfego em nível de aplicação operando como default gateway das redes protegidas;

7.1.10.17.3 Modo misto de trabalho, camada 2 (dois) e 3 (três) em diferentes interfaces físicas;

7.1.10.18 Os clusters devem permitir:

7.1.10.18.1 A solução a ser adquirida deve ser capaz de utilizar dinâmica e automaticamente todos os seus recursos de processamento (seja para de tráfego de rede ou de firewall), de forma a evitar o esgotamento de parte destes recursos enquanto outros semelhantes ainda estejam disponíveis ou ociosos;

7.1.10.18.1.1 Independente da forma que a solução atenda o requisito anterior, isso deve ocorrer sem a necessidade de ajustes manuais ou reboot (reinicialização) dos equipamentos.

7.1.10.18.2 A solução deve ser capaz de detectar altos volumes de tráfego (elephant flows), como também de evitar a sobrecarga do(s) recurso(s) (seja a interface de rede, core de processamento, ou processador etc.) alocado(s) para o processamento deste tráfego.

7.1.10.18.2.1 Independente da forma que a solução atenda o requisito anterior, ela deve fazê-lo sem a necessidade de ajustes manuais ou reboot (reinicialização) dos equipamentos.

7.1.10.18.3 A formação do cluster deve ocorrer por meio da infraestrutura de rede do TRE-GO;

7.1.10.18.3.1 Toda troca de informações de sincronismo entre os dispositivos dos clusters deve ocorrer por meio da infraestrutura de switches do TRE-GO;

7.1.10.18.3.2 Não serão admitidas soluções que necessitem de conexão fisicamente direta entre os dois equipamentos do cluster;

7.1.10.18.3.3 Deve ser possível a configuração do cluster onde, os dois dispositivos que o compõe, fiquem distantes um do outro, no mínimo, 3 quilômetros, em prédios distintos que possuem, entre si, conexão de camada 2 (dois).

7.1.10.19 Alta Disponibilidade ou HA (High Availability):

7.1.10.19.1 A solução de firewall deve suportar a configuração dos dispositivos em cluster de Alta Disponibilidade, na configuração Ativo/Stand-by, na qual um equipamento recebe a carga de tráfego enquanto o outro é apenas redundância;

7.1.10.19.2 A solução deve suportar também a sua configuração em modo Ativo/Ativo, na qual ambos os equipamentos do cluster recebem e distribuem entre si o tráfego de rede, simultaneamente.

7.1.10.19.3 Os clusters devem permitir determinar qual de seus dispositivos ficará preferencialmente ativo, ao mesmo tempo que deve comutá-los automaticamente entre equipamentos, em caso de falha de um de seus dispositivos.

7.1.10.19.4 A configuração em alta disponibilidade deve sincronizar, entre os equipamentos:

7.1.10.19.4.1 Sessões;

7.1.10.19.4.2 Configurações, incluindo, mas não limitado à, de políticas de Firewall, NAT e objetos de configuração (de rede, nuvem, GeoIP, e dinâmicos);

7.1.10.19.4.3 Associações de Segurança das VPNs;

7.1.10.19.4.4 A alta disponibilidade deve possibilitar monitoração dos equipamentos do cluster:

7.1.10.19.4.4.1 Por falha de link nas interfaces de rede dos seus equipamentos;

7.1.10.19.4.4.2 Por falha de componentes ou processos internos essenciais para a solução de firewall no dispositivo;

7.1.10.19.4.4.3 Por diferença de configurações entre os dispositivos dos cluster.

7.1.10.20 Controle de políticas de segurança e VPN:

7.1.10.20.1 A solução de segurança deve usar a tecnologia Stateful Inspection para controlar o fluxo de rede nos dispositivos, verificando o estado da conexão nos mesmos;

7.1.10.20.2 A solução deve possuir os seguintes controles:

7.1.10.20.2.1 Controle de políticas por porta, serviço e protocolo;

7.1.10.20.2.2 Controles de políticas por aplicações, grupos de aplicações e categorias de aplicações;

7.1.10.20.2.3 Controles de políticas por usuários, grupos de usuários, endereços IP (IPv4 e IPv6), redes, range de IPs e grupo de endereços IP;

7.1.10.20.2.4 Controle de políticas por interface de rede ou por grupos de interfaces;

7.1.10.20.3 O controle de acesso deve ser implementado através de regras definidas a partir de:

7.1.10.20.3.1 Objetos com informações estáticas, incluindo endereços, redes e ranges de endereços específicos;

7.1.10.20.3.2 Objetos com informações dinâmicas, incluindo a capacidade de uso de listas externas para obtenção de endereços IPs, nomes de domínios, URLs, FQDN e Data Centers (como SDDC Software-defined datacenter e SDN Software-defined Network) para este controle;

7.1.10.20.3.2.1 Capacidade de se conectar com Data Centers e fontes externas, relacionadas no requisito 7.1.12.4.1 (“Suportar integração nativa com, no mínimo AWS, AZURE, Google Cloud, além de soluções como OpenStack, Cisco ACI, VMware NSX-T, VMWare Vcenter, e Kubernetes.”), para criar objetos dinâmicos com informações de redes ou IP e utilizar estes objetos como origens ou destinos em regras;

7.1.10.20.3.2.2 A obtenção e atualização, pela solução, das informações de objetos dinâmicos nessas fontes externas deve ocorrer de forma automatizada com intervalo máximo de 01 (um) minuto, ou com frequência configurável, para que a política de segurança possa ser atualizada sem a necessidade de inserção e remoção de endereços IPs dessas fontes, e implementada em seus firewalls sem a necessidade a instalação de nova base de regras.

7.1.10.20.4 Controle e inspeção SSL por política para tráfego de entrada (Inbound) e saída (Outbound);

7.1.10.20.5 Deve possibilitar regras de exceção, para não inspecionar o tráfego SSL (Secure Socket Layer), baseado em origem e destino;

7.1.10.20.6 Deve permitir a definição de políticas por grupos “globais” ou “gerais” (a serem aplicadas em todos os dispositivos de firewall gerenciados), e “locais” ou “específicas” (designadas por equipamento, grupos de firewalls, ou localidade);

7.1.10.20.7 Deve permitir a criação de regras que fiquem ativas em horário definido;

7.1.10.20.8 Deve permitir a criação de regras com data ou prazo de expiração;

7.1.10.20.9 Deve permitir a autenticação de usuários para aplicação de políticas, através de portal de autenticação (captive portal);

7.1.10.20.9.1 O portal deve estar disponibilizado para usuários de forma permanente, para que se autentiquem antecipadamente ao tráfego a ser autorizado no perímetro protegido pelos firewalls da solução;

7.1.10.20.9.2 A autenticação de usuários deve possibilitar a identificação do seu endereçamento de origem, para aplicação da política de segurança relacionada ao usuário;

7.1.10.20.9.3 Uma vez autenticado através do portal de autenticação da solução, deve haver o compartilhamento da identidade do usuário entre os demais firewalls da solução, fazendo com que não seja necessária uma nova autenticação para acesso no perímetro protegido pela solução;

7.1.10.20.9.4 Todos os firewalls da solução devem suportar, no mínimo, 9.000 (nove mil) usuários autenticados simultaneamente;

7.1.10.20.10 A solução deve permitir a integração com bases externas de usuários e grupos, para a autenticação e autorização de usuários e grupos, baseados em diretório padrão Microsoft Active Directory e LDAP (X.500);

7.1.10.20.11 Para tanto, deve possuir capacidade para executar consultas nessas bases externas, permitindo associar as estruturas de diretórios citadas no requisito anterior, ao controle de acesso dos escopos de inspeção configurados na solução;

7.1.10.20.12 Suportar SAML (Security Assertion Markup Language) para autenticação em bases e serviços de autenticação externos;

7.1.10.20.13 Receber dados ou informações de identidade por meios externos através de API REST;

7.1.10.20.14 Deve decifrar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e 1.3;

7.1.10.20.15 Deve possuir recurso para redirecionar o tráfego Web (HTTP e HTTPS) outbound (de saída para a Internet) para o endereço IP de um proxy-server ou filtro de conteúdo externo, que esteja em rede remota, através de funcionalidade como HTTP/HTTPS Mapped, Redirect (Redirecionamento) ou técnica semelhante.

7.1.10.20.16 Deve conter controle de banda usando técnicas de traffic shaping e QoS baseado em Políticas (Prioridade, Garantia e Máximo);

7.1.10.20.17 A solução deve suportar os seguintes esquemas de autenticação nos módulos de administração de Firewall e VPN: usuários locais, TACACS, e RADIUS;

7.1.10.20.18 Deve oferecer as funcionalidades de backup de forma manual e automática, bem como permitir o agendamento do backup das configurações;

7.1.10.20.19 Deve suportar a restauração do Sistema Operacional para a última versão salva;

7.1.10.20.20 A solução deve ser capaz de apresentar contagem de utilização das regras;

7.1.10.20.21 A solução deve identificar regras não utilizadas, ou a data de sua última utilização;

7.1.10.20.22 A solução deve ser capaz de identificar objetos e configurações redundantes, sugerindo a utilização dos já existentes, ou de fazer a validação de políticas antes de sua aplicação, informando qual regra está sendo sobreposta pela configuração redundante;

7.1.10.20.23 Deve possuir mecanismo de validação de regras e políticas antes que a mudança seja efetivada no ambiente;

7.1.10.20.24 A validação de políticas deve informar quando houver regras que, ofusquem ou conflitem com outras regras existentes;

7.1.10.20.25 Deve possuir um recurso de controle, visualização e recuperação das versões anteriores da política de segurança salvas nos últimos 7 (sete) dias;

7.1.10.20.26 Deve registrar toda alteração de políticas e definições em log para auditoria posterior, com possibilidade de visualização na console de gerenciamento centralizado;

7.1.10.20.27 Deve permitir a ativação e desativação de regras de forma programada conforme a data e hora;

7.1.10.20.28 Deve permitir a integração com ferramentas de otimização, validação, e implementação de políticas segurança;

7.1.10.20.29 Deve implementar VPNs com as seguintes tecnologias:

7.1.10.20.29.1 IPSec VPN;

7.1.10.20.29.1.1 Nos equipamentos do ITEM 1, devem estar licenciadas para, no mínimo, 1600 conexões gateway-to-gateway;

7.1.10.20.29.1.2 Nos equipamentos do ITEM 1, devem estar licenciadas para, no mínimo, 1400 conexões client-to-gateway;

7.1.10.20.29.1.3 Os dois itens anteriores devem ser fornecidos de forma que funcionem simultaneamente em sua totalidade;

7.1.10.20.29.2 SSL VPN;

7.1.10.20.29.2.1 Nos equipamentos do ITEM 1, devem estar licenciadas para, no mínimo, 1500 conexões;

7.1.10.20.30 A VPN IPSEc deve suportar:

7.1.10.20.30.1 3DES;

7.1.10.20.30.2 Autenticação MD5, SHA-1 e SHA-256;

7.1.10.20.30.3 Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

7.1.10.20.30.4 Algoritmo Internet Key Exchange (IKE), devendo suportar os métodos IKEv1 e IKev2;

7.1.10.20.30.5 AES 128 e 256 (Advanced Encryption Standard);

7.1.10.20.30.6 Autenticação via certificado IKE PKI e Pre-Shared Key;

7.1.10.20.30.7 NAT Traversal (NAT-T);

7.1.10.20.31 Deve ser capaz de implementar VPNs nos modelos:

7.1.10.20.31.1 Site-to-site (entre gateways);

7.1.10.20.31.2 Tunnel Interface;

**7.1.10.21 SD-WAN:**

7.1.10.21.1 Deve operacionalizar no mínimo os seguintes critérios de SD-WAN:

7.1.10.21.2 A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal;

7.1.10.21.3 As configurações de perfis de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades;

7.1.10.21.4 A solução deve permitir operar em caráter de diagrama hub-spoke;

7.1.10.21.5 A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacotes;

7.1.10.21.6 O dispositivo deve compreender o que está causando degradação de desempenho para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível;

7.1.10.21.7 O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link de satélite desde que a sua terminação permita conectividade com interfaces ethernet;

7.1.10.21.8 A solução deve ter inteligência para executar no mínimo as seguintes lógicas de operação:

7.1.10.21.8.1 Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS;

7.1.10.21.8.2 Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresentem resultados abaixo dos limites definidos;

7.1.10.21.8.3 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

7.1.10.21.9 O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho;

7.1.10.21.10 O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta;

7.1.10.21.11 O SD-WAN deve permitir o monitoramento de integridade do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos cenários onde houver a implementação do SD-WAN com link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação;

7.1.10.21.12 Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste "path" para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;

7.1.10.21.13 Deve ter licenciamento para uso sem restrições nos equipamentos do item 1 do GRUPO 1;

**7.1.10.22 Controle de aplicação e filtro Web:**

7.1.10.22.1 A solução deve possuir ferramentas de visibilidade e controle de aplicações Web integrada na

própria solução de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações Web;

7.1.10.22.2 A solução de segurança deve possuir capacidade de reconhecer aplicações, independente de porta e protocolo;

7.1.10.22.3 Possuir uma base de assinaturas aplicações e suas categorias reconhecidas pela solução;

7.1.10.22.4 Reconhecer aplicações, mesmo com uso de técnicas de evasão, independente da porta e protocolo ao qual ela estiver aplicada, visando bloquear o tráfego;

7.1.10.22.5 Deve ser capaz de inspecionar tráfego criptografado (SSL 3.0, e TLS 1.0, 1.1, 1.2, e 1.3) a fim de identificar funcionalidades específicas de cada aplicação, possibilitando o controle granular das mesmas, não se limitando apenas a aplicação principal;

7.1.10.22.6 Deve atualizar a base de assinaturas de aplicações manual ou automaticamente;

7.1.10.22.6.1 A atualização automática deve poder ocorrer em horários pré-definidos, e ser desabilitada por completo;

7.1.10.22.7 Deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.1.10.22.8 Deve permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade daquelas criadas pelo TRE-GO;

7.1.10.22.9 Deve alertar ao usuário quando uma aplicação web for bloqueada;

7.1.10.22.10 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em suas características, tais como:

7.1.10.22.10.1 Categoria Principal;

7.1.10.22.10.2 Nível de risco;

7.1.10.22.11 Deve possibilitar a integração da solução com base do Active Directory e LDAP (nas versões 2.x e 3.x) para criação de políticas, possibilitando a criação de regras utilizando:

7.1.10.22.11.1 Usuários;

7.1.10.22.11.2 Grupo de usuários;

7.1.10.22.11.3 Endereço IP;

7.1.10.22.11.4 Endereço de Rede;

7.1.10.22.12 Deve limitar a banda de download e upload usada por aplicações (traffic shaping), baseado em IP de origem, usuários e grupos LDAP;

7.1.10.22.13 Deve possuir capacidade de identificar o usuário de rede com integração ao LDAP (nas versões 2.x e 3.x), sem necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.1.10.22.14 Deve possuir capacidade para executar consultas nessas bases externas, permitindo associar as estruturas de diretórios citadas no requisito anterior, ao controle de acesso dos escopos de inspeção configurados na solução;

7.1.10.22.15 A solução de segurança deve possuir controle granular para as funcionalidades de proteção;

7.1.10.22.15.1 Inspeção de tráfego através de endereços IP e SSL para os tráfegos de saída (Outbound);

7.1.10.22.15.2 É obrigatório que seja possível desligar a inspeção para sites de bancos baseados em categorização automática executada pelo fabricante;

7.1.10.22.16 Os equipamentos ofertados devem permitir a inspeção, sem perda de funcionalidades, em todas as portas físicas;

7.1.10.22.17 O recurso de controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;

7.1.10.22.18 A solução deve possuir uma interface ou portal do próprio fabricante para buscas/consultas de Aplicações e URLs;

7.1.10.22.19 A solução deve categorizar:

7.1.10.22.19.1 URLs, por Categoria do conteúdo e Reputação;

7.1.10.22.19.2 Aplicações, por Fator de Risco;

7.1.10.22.20 A solução deve receber atualizações para sua base de aplicações e URLs de um serviço baseado em nuvem;

7.1.10.22.21 A solução deve possuir uma interface única para gerenciar regras de aplicação e URLs;

7.1.10.22.22 A solução deve prover a opção de editar a notificação de bloqueio e redirecionar os usuários para um portal com mensagens personalizadas;

7.1.10.22.23 A solução deve incluir o mecanismo de listas (blacklist e whitelist) permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URLs independente da categoria;

7.1.10.22.24 A funcionalidade de Aplicação e filtros de URL deve possuir relatório de utilização;

7.1.10.22.25 Deve permitir o controle por credencial para os dispositivos que não estão integrados ao Controlador de Domínio, através de captive portal (portal de autenticação) nativo;

7.1.10.22.26 Deve permitir a autenticação de usuários para aplicação de políticas, através de captive portal (portal de autenticação);

7.1.10.22.27 A solução deve permitir a integração com bases externas de usuários e grupos, para a autenticação e autorização de usuários e grupos, baseados em diretório padrão Microsoft Active Directory e LDAP (X.500), no captive portal (portal de autenticação);

7.1.10.22.28 Para tanto, deve possuir capacidade para executar consultas nessas bases externas, permitindo associar as estruturas de diretórios, citadas no requisito anterior, às diferentes políticas de segurança configuradas na solução de firewall.

7.1.10.22.29 Suportar SAML para autenticação em bases e serviços de autenticação externos;

7.1.10.22.30 Deve possibilitar base de URLs local no firewall, evitando delay (atraso) de comunicação e validação da URLs;

7.1.10.22.31 Deve possibilitar a criação de Categorias de URLs customizadas;

7.1.10.22.32 Deve possibilitar a exclusão de URLs do bloqueio por categoria;

7.1.10.22.33 Deve possibilitar a categorização e recategorização de URL;

7.1.10.22.34 Deve possibilitar a customização de página de bloqueio de interação com usuário;

7.1.10.22.35 Os logs da solução devem incluir informações das atividades dos usuários;

**7.1.10.23 Detecção e prevenção de ameaças e ataques:**

7.1.10.23.1 Para proteção em tempo real do ambiente contra-ataques, os dispositivos de proteção devem possuir funcionalidades de IPS (Intrusion Prevent System, ou Sistema de Prevenção a Intrusão), e Anti-Malware integrados na própria solução de Firewall;

7.1.10.23.2 Deve incluir o fornecimento e atualização de bases de conhecimento ou de assinaturas para prevenção de instrução (IPS) e bloqueio de arquivos maliciosos (anti-malware);

7.1.10.23.2.1 A solução deve permitir a atualização automática ou manual das bases de assinaturas junto ao fabricante da solução, assim que novas assinaturas forem disponibilizadas.

7.1.10.23.2.2 A atualização automática deve poder ocorrer em horários pré-definidos, e ser desabilitada por completo;

7.1.10.23.3 A solução deve possuir serviço de inteligência para ameaças cibernéticas proprietário do fabricante responsável pela atualização de segurança dos dispositivos;

7.1.10.23.4 Deve permitir o bloqueio de ataques a vulnerabilidades, as quais ainda não tenham sido corrigidas;

7.1.10.23.5 Deve permitir o bloqueio de exploits;

7.1.10.23.6 A funcionalidade de IPS deve fazer a inspeção de toda a sessão, independentemente do tamanho;

7.1.10.23.7 O mecanismo de inspeção deve receber e implementar em tempo real as atualizações para os ataques emergentes sem a necessidade de reinício do dispositivo;

7.1.10.23.8 Em cada assinatura fornecida em sua base, o fabricante deve incluir informações como: código CVE ou equivalente, tipo de impacto, severidade, e tipo de ação que a mesma executará;

7.1.10.23.9 A solução deve permitir a configuração granular na ação de cada proteção, como:

7.1.10.23.9.1 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar TCP Reset (RST).

7.1.10.23.9.2 Deve ser capaz de implementar regras de exceção, baseadas em assinaturas, endereços ou segmentos específicos, visando o tratamento de falso positivos;

7.1.10.23.9.3 Deve ser possível colocar a funcionalidade de IPS do NGFW em um modo passivo, onde todo o tráfego é permitido, mas o sistema deve enviar os registros de alerta de acordo com as políticas aplicadas.

7.1.10.23.10 A solução deve possibilitar a captura de pacotes para uma determinada proteção ou assinatura do módulo de IPS;

7.1.10.23.11 Deve possuir os seguintes mecanismos de inspeção de IPS:

7.1.10.23.11.1 Análise Heurística;

7.1.10.23.11.2 Análise de padrões de estado de conexões;

7.1.10.23.11.3 Análise de decodificação de protocolo;

7.1.10.23.11.4 Análise para detecção de anomalias de protocolo;

7.1.10.23.11.5 Fragmentação de pacotes;

7.1.10.23.11.6 DoS;

7.1.10.23.11.7 Bloqueio de pacotes malformados;

7.1.10.23.11.8 Identificar e bloquear comunicações originadas ou destinadas a botnets;

7.1.10.23.12 Suportar bloqueio de arquivos por tipo, no mínimo para os seguintes tipos: executáveis, .EXE, .BAT, PDF;

7.1.10.23.12.1 Permitir o bloqueio de malware no mínimo, para os seguintes protocolos: HTTP, HTTPS, FTP, SMTP e POP3;

7.1.10.23.13 Os eventos devem identificar o país de onde partiu a ameaça detectada;

7.1.10.23.14 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate, tais como zip e gzip;

7.1.10.23.15 Deve possuir capacidade de criar regras independentes para cada segmento monitorado;

7.1.10.23.16 Deve incluir o mecanismo de listas (blacklist e whitelist) permitindo ao administrador do sistema aplicar ou não as políticas de segurança, de acordo com os endereços IP definidos;

7.1.10.23.17 Permitir escrever novas assinaturas de ataques;

7.1.10.23.18 Deve implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle);

7.1.10.23.19 Analisar padrões de comunicação C&C (Command & Control) e não apenas o servidor DNS de destino;

7.1.10.23.20 A solução deve permitir configurar se as conexões serão permitidas ou bloqueadas no caso de falha

do mecanismo de inspeção do anti-malware;

7.1.10.23.21 Deve ser capaz de detectar e prevenir ataques DNS tunneling;

7.1.10.23.22 Deve possuir mecanismo de geolocalização para controle granular por regiões geográficas distintas;

7.1.10.23.23 Deve suportar a criação de políticas por geolocalização, permitindo o tráfego de entrada, saída, ou ambos, de determinada região sejam bloqueados;

7.1.10.23.24 Deve permitir a visualização dos países de origem e destino nos logs dos acessos;

**7.1.10.24 Monitoração, logs e relatórios:**

7.1.10.24.1 Deve possuir uma interface gráfica para investigação de logs de forma simples e amigável, onde seja possível realizar filtros e pesquisas, necessários para investigações de acessos e bloqueios realizados;

7.1.10.24.2 Deve permitir acesso concorrente de administradores;

7.1.10.24.3 Deve permitir a localização das regras nas quais um determinado endereço IP, rede ou objetos estão sendo utilizados;

7.1.10.24.4 Deve permitir visualizar regras que fiquem ativas em horário definido;

7.1.10.24.5 Deve permitir visualizar regras com data de expiração;

7.1.10.24.6 Deve possibilitar a integração com soluções de SIEM de mercado;

7.1.10.24.7 Deve possuir logs de auditoria detalhados, informando as configurações ou mudanças realizadas, o administrador que as executou, e com o respectivo horário da alteração;

7.1.10.24.8 Deve permitir exportar os logs para servidor de Syslog, versão 3.0 (RFC 5424);

7.1.10.24.9 Deve permitir exportar os logs para arquivo CSV;

7.1.10.24.10 Deve possuir mecanismos para rotação automática dos arquivos de log por dia e tamanho;

7.1.10.24.11 Deve possuir recursos para definição de políticas de retenção de logs das funcionalidades do NGFW (por exemplo: logs de acesso, aplicação, IPS, ataques, etc.);

7.1.10.24.12 Deve permitir a exibição das seguintes informações, de forma histórica e em tempo real:

7.1.10.24.12.1 Verificar a situação do dispositivo e do cluster;

7.1.10.24.12.2 Verificar as principais aplicações em uso;

7.1.10.24.12.3 Verificar as principais aplicações por risco;

7.1.10.24.13 Deve permitir a geração de relatórios contendo, no mínimo, as seguintes informações:

7.1.10.24.13.1 Resumo gráfico de aplicações utilizadas;

7.1.10.24.13.2 Principais aplicações por utilização de largura de banda;

7.1.10.24.13.3 Principais aplicações por taxa de transferência;

7.1.10.24.13.4 Principais hosts por número de ameaças identificadas;

7.1.10.24.14 Deve permitir a criação de relatórios personalizados;

7.1.10.24.15 Deve permitir utilizar nos relatórios, múltiplos critérios de filtragem (por exemplo.: 10 (dez) redes distintas; vários protocolos simultaneamente etc.). Exceto no campo horário, onde deve ser possível definir uma faixa de tempo como critério de pesquisa;

7.1.10.24.16 Gerar alertas automáticos via e-mail e SNMP;

7.1.10.24.17 Deve permitir visualizar informações a respeito das assinaturas utilizadas: código CVE ou equivalente, tipo de impacto, severidade, e tipo de ação executada;

**7.1.11 Recursos dos equipamentos que compõem os clusters de firewalls:**

7.1.11.1 Os dispositivos de proteção de rede devem possuir, no mínimo, as seguintes funcionalidades:

7.1.11.2 Devem ser dispositivos de proteção de rede (firewall) em hardware do tipo appliance físico (fabricado para esta finalidade), do mesmo fabricante do software de firewall.

7.1.11.3 Devem implementar as funcionalidades disponibilizadas pelas licenças, permitindo a configuração e implementação de políticas de segurança que incluem as funcionalidades e recursos de NGFW: Controle de Acesso por protocolo, endereçamento, aplicação, IPS (Intrusion Prevent System, ou Sistema de Prevenção a Intrusão), Anti-malware, Filtro de URL e Identificação de Usuário para todos os dispositivos de firewall, Threat Prevention (Prevenção a Ameaças) e Anti-bot;

7.1.11.4 Devem ser fornecidos 2 (dois) equipamentos idênticos para garantir o seu funcionamento em cluster de HA (High Availability, ou Alta Disponibilidade);

7.1.11.5 Deve possuir no mínimo 01 (uma) interface do tipo console;

7.1.11.6 Deve possuir no mínimo 01 (uma) interface de gerenciamento fora da banda (outof-band) que permita o gerenciamento do equipamento de forma remota, através de uma interface que funcione independentemente do sistema operacional, possibilitando desligá-lo e religá-lo remotamente;

7.1.11.7 Caso as funcionalidades descritas no requisito anterior não sejam implementadas de forma nativa pelos dispositivos de firewall, a solução pode ser composta por equipamentos adicionais dedicados à função, desde que compatíveis com os firewalls e que funcionem e sejam administrados de forma integrada a solução, sem prejuízo as demais funcionalidades.

**7.1.12 Recursos e funcionalidades do gerenciamento centralizado da solução:**

7.1.12.1 A solução deve ser fornecida com, ao menos, 01 (um) produto de gerenciamento centralizado e integrado aos dispositivos de firewalls, e suas políticas de segurança;

7.1.12.1.1 A console poderá ser composta por mais de produto com diferentes funções, desde que estes atuem em conjunto para compor uma solução de gerenciamento centralizado, com todas as características gerais aqui exigidas;

7.1.12.2 Deve permitir, a partir de uma console centralizada, o gerenciamento e administração dos firewalls NGFW desta solução, bem como a implementação e operação das políticas de segurança que utilizarão as funcionalidades;

7.1.12.3 Deve permitir a criação e administração de políticas de acesso baseadas em objetos (identificando hosts, redes, gateways, nuvens, data-centers, usuários, grupos, diretórios) que permitam sua utilização em diversas regras e configurações, mesmo simultaneamente;

7.1.12.4 Deve permitir a integração com os principais ambientes de nuvem do mercado:

7.1.12.4.1 Suportar integração nativa com, no mínimo AWS, AZURE, Google Cloud, além de soluções como OpenStack, Cisco ACI, VMware NSX-T, VMWare Vcenter, e Kubernetes.

7.1.12.4.2 Essa integração deve permitir recuperar dinamicamente os objetos gerados por essas ferramentas para uso nas políticas de controle de acesso, ou seja, que a solução de firewall possa reconhecer os objetos criados da plataforma de nuvem de forma automática, e sem a necessidade de interação manual com as consoles de gerenciamento de ambas.

7.1.12.4.3 Deve ser possível gerar novos objetos, a partir dessas integrações, baseados em pesquisas feitas por, no mínimo, endereço IP e TAG, inclusive associando-as.

7.1.12.4.4 Deve ser possível realizar integração a ambientes para fins de leitura dos objetos e uso nas políticas de controle de acesso através de integração nativa, API, ou mesmo de forma genérica, por arquivos ou bases exportadas (como por exemplo um arquivo em repositório no git labs);

7.1.12.5 Deve suportar agendamento da implementação das políticas, com objetivo de aplicação automática em datas e horários pré-definidos;

7.1.12.6 Deve fornecer recursos para monitoração e gerenciamento, em tempo real, do status e desempenho dos equipamentos gerenciados;

7.1.12.7 Fornecer interface para visualização e controle de logs e eventos registrados nos firewalls gerenciados;

7.1.12.8 Deve possibilitar a utilização de múltiplos administradores simultâneos na mesma gerência, com permissão de escrita e com proteção na base de dados, de tal forma que um não interfira na criação da regra de outro;

7.1.12.9 Deve possuir módulo de API para automação de configuração por Ansible, suportando, no mínimo;

7.1.12.9.1 Consulta, criação, manipulação e remoção de objetos, regras e NATs;

7.1.12.9.2 A API também deve permitir a configuração e manipulação de VPNs;

7.1.12.10 Gerenciamento e monitoração centralizada de logs e eventos:

7.1.12.10.1 Deve possuir uma interface gráfica para investigação de logs de todos os firewalls administrados, de forma simples e amigável, onde seja possível realizar filtros e pesquisas, necessários para investigações de acessos e bloqueios realizados;

7.1.12.10.2 Deve permitir acesso concorrente de administradores;

7.1.12.10.3 Deve permitir a localização das regras nas quais um determinado endereço IP, rede ou objetos estão sendo utilizados;

7.1.12.10.4 Deve permitir visualizar regras que fiquem ativas em horário definido;

7.1.12.10.5 Deve permitir visualizar regras com data de expiração;

7.1.12.10.6 Deve possibilitar a integração com soluções de SIEM de mercado;

7.1.12.10.7 Deve possuir logs de auditoria detalhados, informando as configurações ou mudanças realizadas e o administrador que executou com o respectivo horário da alteração;

7.1.12.10.8 Deve permitir exportar os logs para servidor de Syslog, versão 3.0 (RFC 5424);

7.1.12.10.9 Deve permitir exportar logs no formato CEF (Common Event Format), versão 1.0 ou 0.1;

7.1.12.10.10 Deve permitir exportar os logs para arquivo CSV;

7.1.12.10.11 Deve possuir mecanismos para rotação automática dos arquivos de log por dia e tamanho;

7.1.12.10.12 Deve possuir recursos para definição de políticas de retenção de logs dos recursos de NGFW (por exemplo: logs de acesso, aplicação, IPS, ataques);

7.1.12.10.13 Deve permitir a exibição das seguintes informações, de forma histórica e em tempo real:

7.1.12.10.13.1 Verificar a situação do dispositivo e do cluster;

7.1.12.10.13.2 Verificar as principais aplicações em uso;

7.1.12.10.13.3 Verificar as principais aplicações por risco;

7.1.12.10.14 Deve permitir a geração de relatórios contendo, no mínimo, as seguintes informações:

7.1.12.10.14.1 Resumo gráfico de aplicações utilizadas;

7.1.12.10.14.2 Principais aplicações por utilização de largura de banda;

7.1.12.10.14.3 Principais aplicações por taxa de transferência;

7.1.12.10.14.4 Principais hosts por número de ameaças identificadas;

7.1.12.10.14.5 Principais ameaças ou ataques identificados;

7.1.12.10.15 Deve permitir a criação de relatórios personalizados;

7.1.12.10.16 Deve permitir a geração de relatórios configurados, de forma automática e programada;

7.1.12.10.17 Deve permitir utilizar nos relatórios, múltiplos critérios de filtragem (por exemplo: 10 (dez) redes

distintas; vários protocolos simultaneamente), exceto no campo horário, onde deve ser possível definir uma faixa de tempo como critério de pesquisa;

7.1.12.10.18 Gerar alertas automáticos via e-mail e SNMP;

7.1.12.10.19 Deve permitir visualizar informações a respeito das assinaturas utilizadas: código CVE ou equivalente, tipo de impacto, severidade, e tipo de ação executada;

7.1.12.10.20 Deve possuir recurso de correlacionamento de eventos e remediação automática, com as seguintes funcionalidades:

7.1.12.10.20.1 Implementar o correlacionamento de logs, que identifique e sumarize eventos distintos ocorridos em um ou mais dispositivos e seus recursos de NGFW, mas que sejam correlatos ou semelhantes;

7.1.12.10.20.2 Implementar a classificação dos eventos (tanto manual como automaticamente), quanto a sua severidade;

7.1.12.10.20.3 Deve permitir a definição de threshold ou outra forma configurável de limites para a tolerância de eventos semelhantes;

7.1.12.10.20.4 Deve possuir recurso para a remediação de eventos detectados, através de bloqueios automatizados;

7.1.12.10.21 Deve gerar relatórios sobre os eventos detectados, por critérios como consumo de banda, nível de risco, controle de aplicações;

**7.2 Características dos equipamentos que compõem os clusters de firewalls da solução (ITENS 1 e 2 do GRUPO 1):**

7.2.1 Especifica os equipamentos que compõem clusters de firewalls “físicos”, com 02 (dois) dispositivos, incluindo seu firmware, sistema operacional, software e licenças, visando compor uma solução de firewalls

7.2.1.1 Devem fornecer todos os recursos e funcionalidades de NGFW (Next Generation Firewall), especificados no requisito 7.1 (“Características gerais das soluções de proteção de redes: “).

7.2.1.2 Devem ser disponibilizadas todas as licenças necessárias para o pleno funcionamento das funcionalidades exigidas neste Edital;

7.2.2 Recursos específicos dos dispositivos de proteção de redes que compõem os clusters de firewalls.

7.2.2.1 Cada equipamento componente do clusters de alta-disponibilidade deve possuir a capacidade para suportar, no mínimo:

| | | | **ITEM 1** | **ITEM 2** |
|---|---|---|---|---|
| | | | **TIPO 1** | **TIPO 2** |
| 2.3.2.1.1.1 | Throughput (vazão) de NGFW | | 45 Gbps | 45 Gbps |
| 2.3.2.1.1.2 | Throughput de Threat Prevention | | 20 Gbps | 20 Gbps |
| 2.3.2.1.1.3 | Throughput de IPsec VPN | | 20 Gbps | - |
| 2.3.2.1.1.4 | Suportar, ao menos, 01 (um) dos indicadores de capacidade: | Novas sessões por segundo | 390.000 | 390.000 |
| | | Conexões por segundo | 270.000 | 270.000 |
| 2.3.2.1.1.4 | Conexões simultâneas | | 5.000.000 | 5.000.000 |

7.2.2.1.2 Para cálculo de throughput (vazão), as seguintes funcionalidades devem estar habilitadas:

7.2.2.1.2.1 NGFW: Firewall, Application Control (Controle de Aplicações), e IPS.

7.2.2.1.2.2 Threat Prevention: Firewall, Application Control (Controle de Aplicações), IPS e Malware Protection (Proteção anti-malware).

7.2.2.2 Cada equipamento componente do clusters de alta-disponibilidade deve possuir, ao menos, 01 (um) dos seguintes conjuntos de interfaces, dedicadas ao tráfego de produção:

| | **ITEM 1** | **ITEM 2** |
|---|---|---|

| | | |
|---|---|---|
| | **TIPO 1** | **TIPO 2** |
| 7.2.2.2.1.1 | No mínimo, 08 (oito) interfaces 10GBase-F SFP+; | No mínimo, 08 (oito) interfaces 10GBase-F SFP+; |
| 7.2.2.2.1.2 | No mínimo, 04 (quatro) interfaces 25GBase-F SFP28. | No mínimo, 04 (quatro) interfaces 25GBase-F SFP28. |

7.2.2.3 As interfaces de sincronismo/alta disponibilidade e gerenciamento/administração devem ser dedicadas e exclusivas para estas finalidades, ou seja, separadas das interfaces de produção descritas no requisito anterior, sendo que:

7.2.2.3.1 As interfaces de sincronismo/alta disponibilidade devem ser 1000Base-T RJ45 ou 10GBase-F SFP+;

7.2.2.3.2 As interfaces de gerenciamento/administração devem ser 1000Base-T RJ45 ou 10GBase-F SFP+;

7.2.2.4 Para cada interface SFP+ ou SFP28 solicitada, devem ser fornecidos os respectivos transceivers GBIC nas velocidades especificadas, todos com conectores LC e do tipo short range, para uso com fibras multimodo;

7.2.2.5 O item anterior também se aplica a qualquer outra interface fornecida, mesmo que não solicitada, que seja necessária ao perfeito funcionamento ou administração/gerenciamento do cluster de firewalls;

7.2.2.6 Cada equipamento deve possuir discos redundantes com capacidade de, no mínimo, 480GB SSD (Solid-State Drive) ou Cfast;

**7.3 Características da console de gerenciamento centralizado (ITEM 3 do GRUPO 1):**

7.3.1 Especifica a console de gerenciamento centralizado, composta por seus appliances, softwares e licenças com funcionalidades.

7.3.1.1 Deve fornecer todos os recursos e funcionalidades da console de gerenciamento dos firewalls NGFW (Next Generation Firewall), especificados no requisito 7.1.11.7 (“Recursos e funcionalidades do gerenciamento centralizado da solução: “);

7.3.1.2 Devem ser disponibilizadas todas as licenças necessárias para o pleno funcionamento das funcionalidades exigidas deste ITEM;

7.3.1.3 As funcionalidades exigidas podem ser oferecidas através de múltiplos appliances dedicados a funções diferentes, desde que estes atuem em conjunto para compor uma solução de gerenciamento centralizado com todas as características gerais do produto exigidas no item 7.1.11.7;

7.3.1.4 Caso a solução possua limitações referentes a armazenamento ou processamento de logs e eventos, a solução deve ser entregue com a licença de maior capacidade ou ilimitada;

7.3.2 Recursos específicos do appliance para console de administração de firewalls.

7.3.2.1 O dispositivo a ser fornecido deve atender aos seguintes requisitos:

7.3.2.1.1 Deve ser fornecido em appliance virtual;

7.3.2.1.2 Deve ser do mesmo fabricante dos firewalls;

7.3.2.1.3 A imagem deve estar disponível para download oficialmente no site do fabricante;

7.3.2.1.3.1 Deve ser possível realizar, nativamente, a implantação nas seguintes soluções de virtualização: VMware, Hyper-V e Nutanix.

7.3.3 Funcionalidades específicas da console de gerenciamento centralizado.

7.3.3.1 Deve possuir recurso para administração de firewalls e seus clusters, e suas políticas de segurança;

7.3.3.2 Deve permitir a administração das políticas de segurança e suportar e implementar um número de, no mínimo, 2 (dois) clusters de firewalls (ITEM 1 e 2 do GRUPO 1);

7.3.3.3 Deve permitir a administração de 200 firewalls de menor porte (ITEM 5 do GRUPO 1);

7.3.3.4 Deve permitir a administração das configurações de SD-WAN nos equipamentos do ITEM 1 e ITEM 5 do GRUPO 1.

7.3.3.5 Devem ser fornecidas todas as licenças necessárias para a administração e gerência dos Item 1, 2 e 5 nas quantidades totais especificadas neste Termo de Referência;

**7.4 Características do serviço de migração de firewalls para a nova solução (ITEM 4 do GRUPO 1):**

7.4.1 Especifica o serviço a ser contratado para a migração dos clusters de firewalls NGFW da atual plataforma de firewalls do TRE-GO (Check Point R81.x) para a nova solução de cluster de alta disponibilidade TIPO 1 e TIPO 2 (ITENS 1 e 2 do GRUPO 1).

7.4.2 O serviço deve ser executado por cluster de firewalls a ser migrado, incluindo:

7.4.2.1 Suas configurações e políticas de segurança;

7.4.2.2 Regras de acesso;

7.4.2.2.1 O levantamento feito pelo TRE-GO em seus atuais firewalls aponta uma média de 600 regras por cluster;

7.4.2.3 Políticas de IPS e Conteúdo;

7.4.2.4 Configurações e objetos de NAT (estáticos e dinâmicos);

7.4.2.5 Configurações de interfaces e endereçamento;

7.4.2.6 Configurações de roteamento estáticos e dinâmicos;

7.4.2.7 VPNs;

7.4.2.8 Regras e configurações de identidade dos usuários;

7.4.2.9 Objetos de hosts, redes e ranges de endereços;

7.4.2.10 Objetos de usuários e grupos;

7.4.2.11 Objetos de tempo;

7.4.2.12 Objetos de Data Center;

7.4.2.13 Objetos de FQDN;

7.4.2.14 Todos e quaisquer objetos e recursos de NGFW descritos neste edital.

7.4.3 A migração deve ser feita de forma escalonada, por firewall, e deve prever o planejamento, levantamento de informações, importação de configurações, conversão e replicação das configurações nos novos dispositivos, testes e ativação no ambiente de produção do TRE-GO.

7.4.3.1 A migração deve ser executada no tempo necessário para assegurar a plena configuração dos dispositivos e componentes da nova solução, bem como a migração e replicação das configurações da atual solução, por firewall a ser implementado.

7.4.3.2 A migração deve prever o período de operação assistida por 48hs de cada cluster de firewalls migrado, para possibilitar a resolução de problemas no ambiente implementado, ou mesmo, no caso de não resolução, o rollback (retorno) do ambiente para o firewall antigo.

7.4.4 O serviço de migração deve ser executado presencialmente no TRE-GO.

7.4.4.1 A critério do TRE-GO, o fornecedor poderá realizar remotamente as etapas de levantamento de informações, exportação, conversão, importação e testes, a serem executados em ambiente interno do TRE-GO;

7.4.4.2 A migração de fato, e o acompanhamento durante a operação assistida, deverão ser realizados presencialmente;

7.4.5 Deverá ser realizada a configuração do serviço de SD-WAN em, no mínimo, 4 localidades a serem escolhidas pelo TRE-GO.

7.4.5.1 Deverão ser configuradas, no mínimo, 4 perfis de SD-WAN a serem escolhidos pelo TRE-GO.

**7.5 Recursos dos equipamentos: Firewalls com funcionalidades de NGFW de menor porte (ITEM 5 do GRUPO 1):**

7.5.1 O equipamento fornecido deve possuir alimentação elétrica (2P+T) capaz de operar entre 110 a 240V AC com frequência de 60 (sessenta) Hertz, com reconhecimento automático do nível de tensão;

7.5.2 O software da solução de segurança deve ser fornecido em sua última versão disponibilizado pelo fabricante para o seu segmento/categoria;

7.5.2.1 Não será permitido atendimento de requisitos do Edital através de promessa de versões futuras;

7.5.2.2 Não serão aceitas versões experimentais, versões de teste, versões customizadas para clientes específicos ou que não estejam publicadas no site do próprio fabricante;

7.5.3 Deve possuir a capacidade para suportar, no mínimo:

| | | | |
|---|---|---|---|
| 7.5.3.1 | Throughput (vazão) de NGFW | | 1,5 Gbps |
| 7.5.3.2 | Throughput de Threat Prevention | | 1,0 Gbps |
| 7.5.3.3 | Throughput de IPsec VPN | | 1.0 Gbps |
| 7.5.3.4 | Suportar, ao menos, 01 (um) dos indicadores de capacidade: | Novas sessões por segundo | 20.000 |
| | | Conexões por segundo | 20.000 |
| 7.5.3.5 | Conexões simultâneas | | 200.000 |

7.5.4 Deve suportar as seguintes funcionalidades: Controle de aplicação, IPS, URL Filtering;

7.5.5 O equipamento deve ser da mesma fabricante dos itens 1 e 2;

7.5.6 Deve suportar, com o uso de duas unidades do modelo, a configuração em Alta Disponibilidade, no mínimo, no modo Ativo/Stand-by;

7.5.7 Especificações de hardware:

7.5.7.1 Deve possuir Porta Console dedicada;

7.5.7.2 Deve possuir porta USB ou micro USB;

7.5.7.3 Deve possuir, no mínimo, 8 (oito) interfaces físicas de 1 Gbps do tipo RJ-45 com as seguintes configurações simultaneamente:

7.5.7.3.1 No mínimo, 6 portas LAN;

7.5.7.3.2 No mínimo, 2 portas WAN;

7.5.7.3.2.1 Este item pode ser atendido com uma porta nominada WAN somada a uma outra porta que possa ser configurada como uma segunda porta WAN, desde que não haja, nessa configuração, o consumo das 6 portas LAN exigidas do item 7.5.7.3.1;

**7.5.7.4 SD-WAN:**

7.5.7.4.1 Deve operacionalizar no mínimo os seguintes critérios de SD-WAN:

7.5.7.4.1.1 A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal;

7.5.7.4.1.2 As configurações de perfis de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades;

7.5.7.4.1.3 A solução deve permitir operar em caráter de diagrama hub-spoke;

7.5.7.4.1.4 A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacotes;

7.5.7.4.1.5 O dispositivo deve compreender o que está causando degradação de desempenho para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível;

7.5.7.4.1.6 O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link de satélite desde que a sua terminação permita conectividade com interfaces ethernet;

7.5.7.4.1.7 A solução deve ter inteligência para executar no mínimo as seguintes lógicas de operação:

7.5.7.4.1.8 Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS;

7.5.7.4.1.9 Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresentem resultados abaixo dos limites definidos;

7.5.7.4.1.10 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

7.5.7.4.1.11 O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho;

7.5.7.4.1.12 O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta;

7.5.7.4.1.13 O SD-WAN deve permitir o monitoramento de integridade do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos cenários onde houver a implementação do SD-WAN com link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação;

7.5.7.4.1.14 Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste "path" para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;

**7.6 Treinamento**

7.6.1 A atividade de repasse de conhecimento deve ser executada de forma teórica e prática e trata-se da transferência de conhecimento da CONTRATADA para a equipe do TRE-GO que efetuará a configuração, operação e gestão da solução e seus componentes;

7.6.2 Deve fornecer todo o material didático necessário;

7.6.3 A CONTRATADA deve prover toda a logística e o todo o material necessário à execução do Repasse de Conhecimento teórico e prático, ou seja, infraestrutura adequada, ambientes de laboratório, equipamentos, manuais e apostilas;

7.6.4 A data de início do repasse de conhecimento será definida pelo TRE-GO de acordo com suas necessidades.

7.6.4.1 O TRE-GO deverá comunicar formalmente à CONTRATADA, com antecedência mínima de 5 (cinco) dias, a ocorrência de fato impeditivo para a realização do Repasse de Conhecimento.

7.6.4.2 A CONTRATADA deve informar ao TRE-GO nome completo e e-mail de cada profissional que ministrará o repasse de conhecimento;

7.6.4.2.1 O profissional que irá ministrar o repasse deverá ser certificado pelo fabricante nas tecnologias ofertadas nesse processo;

7.6.5 Deverá ser entregue ao TRE-GO, em até 45 (quarenta e cinco) dias corridos após o início da vigência do contrato, a ementa no idioma em português do Brasil contendo: nome, objetivo, pré-requisitos, conteúdo programático e carga horária, bem como o material do repasse.

7.6.6 A CONTRATADA deverá providenciar o repasse de conhecimento para 1 turma, com 5 participantes.

7.6.7 A carga horária mínima deverá ser de 40 (quarenta) horas;

7.6.7.1 O repasse de conhecimento deverá ser realizado durante a vigência do contrato, no turno matutino, com duração de 4 horas diárias.

7.6.7.2 O repasse de conhecimento deve ser prestado em local externo ao TRE-GO, de responsabilidade da CONTRATADA.

7.6.8 O repasse de conhecimento poderá ser realizado de forma remota.

7.6.8.1 A CONTRATADA poderá utilizar ferramenta Zoom ou outra plataforma, compatível com as do TRE-GO.

7.6.8.2 Deverá abordar a operação básica e avançada da Solução contratada, cobrindo todas as funcionalidades exigidas neste edital, com seguinte conteúdo mínimo:

7.6.8.2.1 Instruções de instalação, incluindo resolução de problemas;

7.6.8.2.2 Instruções de manuseio e operação, incluindo resolução de problemas;

7.6.9 Após o repasse a CONTRATADA deve emitir certificado para cada participante de acordo com a carga horária;

7.6.9.1 O certificado no formato digital deve conter as seguintes informações: Nome completo do participante, Nome do curso, Período de Realização, Carga Horária, Ementa do Treinamento realizado e assinatura digital ou digitalizada do responsável.

7.6.9.2 Os certificados deverão ser encaminhados em até 10 (dez) dias corridos após o término do repasse de conhecimento para os participantes.

7.6.10 A CONTRATADA deverá disponibilizar todo o material didático em formato eletrônico, sem custo adicional para o TRE-GO, devendo ainda estar em língua portuguesa (Brasil);

7.6.10.1 A CONTRATADA deverá disponibilizar manuais de gestão, operação e configuração de todas as ferramentas, soluções e recursos que compõem a solução contratada necessários à completa operacionalização dos recursos exigidos nesta especificação, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

7.6.11 Ao final do repasse de conhecimento, se a CONTRATADA atender a todos os requisitos, a Seção de Suporte aos Serviços de Rede realizará o Aceite de Repasse de Conhecimento.

## 8 **ENTREGA, AVALIAÇÃO E ACEITE DOS SERVIÇOS**

### 8.1 Entrega:

8.1.1 Os equipamentos e os softwares deverão ser entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Nota de Empenho;

8.1.2 Os equipamentos deverão ser entregues no TRE-GO - Praça Cívica, n° 300, Setor Central, Goiânia, Goiás, 5° andar, Ala B, na Seção de Suporte aos Serviços de Rede (SESRE);

8.1.3 A Contratada deverá entregar os softwares e suas licenças por meio eletrônico pelo site do fabricante ou da Contratada, com opção de download ilimitado e acesso exclusivo ao Contratante ou, através de mídia física de instalação para a Seção de Suporte aos Serviços de Rede (SESRE);

8.1.4 A prestação dos serviços contratados deverá ser realizada após a emissão da Nota de Empenho e agendada com a Seção de Suporte aos Serviços de Rede (SESRE);

8.1.5 Para o item 4 do Grupo 1, os serviços serão executados mediante cronograma e data a ser acordado pelo TRE-GO.

8.1.6 Os produtos especificados neste contrato serão entregues pela CONTRATADA em perfeitas condições de operação, no endereço e prazo a seguir mencionado, salvo quando ocorrerem situações fora do controle da mesma, tais como: greves nos serviços de transportes, guerras e perturbações de caráter social, político ou econômico, devidamente comprovadas e formalmente aceitas pelo TRE-GO;

### 8.2 CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE

### 8.3 Avaliação e critérios de aceitação (Recebimento provisório):

8.3.1 Será realizada uma verificação sumária e inicial de conformidade entre a especificação técnica dos equipamentos e softwares entregues com os itens descritos neste Termo de Referência e a nota fiscal pela Seção de Suporte aos Serviços de Rede (SESRE);

8.3.2 Caso seja constatada alguma desconformidade com o item 8.3.1, a Seção de Suporte às Redes (SESRE) comunicará a CONTRATADA para efetuar a correção dos problemas;

8.3.3 A correção para possíveis desconformidades detectadas estabelecida no item 8.3.2 deverá ser efetuada em até 10 (dez) dias úteis, contados a partir da data da comunicação;

8.3.4 Níveis de Serviços Exigidos (NSE) e Critérios de Aceitação:

8.3.4.1 Métrica 1

8.3.4.2 Indicador 1 – equipamentos, softwares e licenças adquiridos serem entregues em conformidade com as especificações do Edital.

8.3.4.3 Mínimo aceitável: 100%

8.3.4.4 Ferramentas de medição: Análise técnica dos equipamentos e acesso ao website do fabricante.

8.3.4.5 Periodicidade de aferição: Na entrega.

### 8.4 Termo de aceite (Recebimento definitivo):

8.4.1 O termo de aceite técnico será emitido pela Seção de Suporte aos Serviços de Rede (SESRE) com ciência da Coordenadoria de Infraestrutura (CINF) em até 10 (dez) dias úteis após o recebimento provisório a dos equipamentos e softwares, e somente se estes atenderem plenamente todas as exigências deste Termo de Referência.

8.4.2 A correção para atender as especificações técnicas deste Edital estabelecida no item 8.4.1 deverá ser efetuada em até 10 (dez) dias úteis, contados a partir da data da comunicação;

8.4.3 Os serviços de migração (Item 4) serão aceitos após a execução total do cronograma.

8.5 Mecanismos formais de comunicação:

8.5.1 Documento: Ordem de serviço ou abertura de chamado.

8.5.2 Emissor: Contratante.

8.5.3 Destinatário: Contratada/Fabricante.

8.5.4 Meio de comunicação: Telefone, e-mail ou sítio na internet.

8.5.5 Periodicidade: De acordo com a demanda.

## 9 **FORMA DE PAGAMENTO**

9.1 A contratada deverá apresentar no ato da entrega dos produtos e serviços Nota Fiscal/Fatura para liquidação e pagamento da despesa pelo TRE-GO, que ocorrerá em até 10 (dez) dias úteis após realizado o Termo de Aceite pela equipe técnica da SESRE (Recebimento Definitivo).

## 10 **DEVERES E RESPONSABILIDADES DA CONTRATADA**

10.1 Fornecer os produtos e serviços no prazo e demais condições estipuladas.

10.2 Entregar os produtos instalados e configurados neste Regional, sem que isso implique acréscimo no preço constante da proposta.

10.3 Se constatada qualquer irregularidade nos produtos, a empresa deverá substituí-los, no prazo máximo de 10 (dez) dias úteis.

10.4 Não transferir a outrem, no todo ou em parte, o objeto contratado, sem prévia anuência do TRE-GO.

10.5 Manter durante a execução do contrato todas as condições de habilitação e qualificação exigidas na licitação.

10.6 Prestar suporte aos equipamentos e softwares, responsabilizando-se pela manutenção corretiva dos mesmos, durante o período de vigência do suporte/garantia, sem que isso implique acréscimo no preço constante da proposta.

10.7 Executar os serviços técnicos especializados utilizando profissional(is) capacitado(s) e certificado(s) pelo fabricante dos produtos e serviços descritos neste Termo de Referência.

## **11 DEVERES E RESPONSABILIDADES DO CONTRATANTE:**

11.1 Efetuar o pagamento à Contratada, de acordo com as condições, no preço e no prazo estabelecidos.

11.2 Exercer a fiscalização dos serviços prestados.

11.3 Permitir acesso dos profissionais da contratada às dependências, equipamentos, softwares do contratante, necessários à execução dos serviços.

11.4 Comunicar oficialmente à contratada as falhas verificadas no cumprimento do contrato.

## 12 **QUALIFICAÇÃO TÉCNICA**

12.1 Requisitos de Capacitação e Experiência:

12.1.1 Deverá possuir atestado de capacidade técnica emitido por instituição ou empresa de direito público ou privado no Brasil, comprovando que a licitante forneceu os produtos e os serviços de características semelhantes ao especificado neste termo de referência, prestando os devidos serviços de manutenção e suporte técnico;

12.1.2 Justificativa para qualificação técnica:

12.1.2.1 A exigência de qualificação técnica, comprovada por atestado de capacidade técnica é fundamental para assegurar a seleção de um fornecedor apto a entregar e manter uma solução de infraestrutura de Tecnologia da Informação e Comunicação (TIC) de alta criticidade, garantindo a continuidade, segurança e desempenho da rede do Tribunal Regional Eleitoral de Goiás (TRE-GO).

## 13 **GARANTIA E SUPORTE**

13.1 Para os itens 1, 2 e 5 deste Termo de Referência:

13.1.1 Deverão ter garantia de 60 (sessenta) meses on-site, incluindo suporte para Hardware e Software, prestado pelo fabricante dos equipamentos ou pela Contratada, com janela de abertura de chamado 24x7 e tempo de resposta de 24 horas, a partir do registro do chamado, e substituição do hardware em até 72 horas;

13.1.2 Serviço de atendimento 24x7 (incluindo finais de semana e feriados) através de linha telefônica 0800 do fabricante ou da Contratada (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte de Software;

13.1.3 Entende-se como on-site o atendimento a ser realizado nas dependências do TRE-GO na cidade de Goiânia-GO;

13.2 Para o item 3:

13.2.1 Deverá ter suporte de 60 (sessenta) meses direto do fabricante;

13.2.2 Deverá fornecer o direito de “updates” e “upgrades” durante o período de suporte, sem custo adicional para o TRE-GO;

13.2.3 Serviço de atendimento 24x7 (incluindo finais de semana e feriados) através de linha telefônica 0800 do fabricante ou da Contratada (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte do Software;

13.3 Regras de garantia e suporte que se aplicam a todos os equipamentos e softwares da solução:

13.3.1 Disponibilidade de website (indicar endereço) para suporte on-line, transferência de manuais e arquivos de configuração (device drives e firmware), e registro do equipamento e notificações automáticas de eventos do equipamento;

13.3.2 A CONTRATADA deverá fornecer garantia dos equipamentos pelos períodos estabelecidos nos itens 13.1.1 e 13.2.1, contados a partir da emissão do Termo de Aceite Técnico (Recebimento Definitivo);

13.3.3 Deverão estar cobertos pela garantia todos os componentes físicos (hardware) e lógicos (software) que fazem parte deste Termo de Referência;

13.3.4 Deverão estar cobertas pela garantia quaisquer atualizações de firmware e software disponibilizadas pelo fabricante, bem como a realização dos procedimentos de instalação das atualizações;

13.3.5 Deverão estar cobertas pela garantia o fornecimento de partes e peças dos equipamentos, mão de obra, transporte, diárias, hospedagem e de quaisquer outros itens necessários à recuperação dos equipamentos ao estado de pleno funcionamento de todos os seus componentes;

13.3.6 Todas as partes de peças fornecidas deverão ser originais e novas;

13.3.7 Todo e qualquer custo envolvido na prestação da garantia deverá correr por conta da CONTRATADA, sem nenhum ônus para o TRE-GO;

13.4 Justificativa para os períodos de garantia

13.4.1 Os prazos de garantia solicitados tem como objetivo proporcionar aumento da disponibilidade, da estabilidade e da reparabilidade dos equipamentos adquiridos por um período maior de tempo do que o prazo normalmente definido pelo fabricante, evitando que, caso os equipamentos saiam da linha de produção, os bens se tornem inservíveis a curto prazo, propiciando a este Regional economia, diminuição da necessidade de realizar licitações e trocas de equipamentos.

## 14 **OBSERVAÇÕES GERAIS**

14.1 Todos os itens fornecidos, incluído todos os seus componentes e acessórios, deverão ser novos e de primeiro uso;

14.2 Devem ser fornecidos com os equipamentos todos os cabos e acessórios necessários para o funcionamento juntamente com os seus manuais e documentos;

14.3 Serão recusados os itens que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado novo pelo fornecedor dos itens;

14.4 Todos os itens devem ser fornecidos em pleno funcionamento, prontos para a utilização, com todos os acessórios e componentes;

14.5 Os equipamentos que compõem esta aquisição devem ser novos e não ter a descontinuidade anunciada pelo fabricante e que estejam íntegros.

14.6 Catálogo oficial do fabricante, de acesso público através de website, onde poderão ser conferidas todas as características exigidas para o item e subitens que compõe o item ofertado, contento informações referentes à descrição e ao part number;

14.7 Cada equipamento, licença, bem como os serviços de instalação e configuração dos mesmos deverão ser entregues, instalados e estar operacionais em até 60 (sessenta) dias corridos a partir do início da vigência do contrato.

14.8 O licenciamento para o pleno funcionamento dos equipamentos e softwares deverá atender a todas as características e especificações do Termo de Referência (TR).

14.8.1 A solução de segurança deve ser disponibilizada com licenças de uso perpétuo para o pleno funcionamento, pelo menos, das funcionalidades de Firewall, VPN, gerência centralizada e logs.

14.8.2 O licenciamento na modalidade de subscrição deverá ter prazo de vigência contratual de, no mínimo, 60 (sessenta) meses, contados a partir da emissão do Termo de Aceite (Recebimento Definitivo), não se limitando ao término da vigência contratual;

14.9 Os equipamentos ofertados devem ser homologados pela Anatel e atender todos os requisitos deste Termo de Referência;

14.10 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

14.11 Entende-se por cumprimento do prazo de entrega o recebimento dos componentes da solução de firewall especificada, sua instalação e execução dos serviços no TRE-GO, deixando-os operacionais, para o recebimento definitivo. (item 1 e 2)

14.12 O TRE-GO pode, a seu interesse, alterar o local de entrega e de instalação dos equipamentos, entre seus Data Centers durante a vigência do Contrato.

## 15 **MODALIDADE E TIPO DE LICITAÇÃO**

15.1 Modalidade de Licitação: Pregão Eletrônico, conforme art. 29 da Lei nº 14.133/2021, por serem os equipamentos considerados bens comuns.

15.2 Tipo de Licitação: Menor Preço.

## 16 **PARCELAMENTO DA CONTRATAÇÃO E FORMA DE ADJUDICAÇÃO**

16.1 Parcelamento do Objeto: Não será realizado parcelamento do objeto. Verifica-se que a licitação da solução

NGFW a qual possui gerência centralizada, quando realizada em um único lote, torna a gestão contratual, e principalmente da garantia, mais eficiente, na medida em que as tratativas serão realizadas com único fornecedor. Ademais, não se verifica ganho competitivo mensurável com o parcelamento, ao contrário, o registro para um único fornecedor tem o condão de reduzir o preço unitário e aumentar o interesse do mercado e, por conseguinte, a competitividade.

16.2 Adjudicação do Objeto: A adjudicação será por grupo único, visando que um único fornecedor seja responsável pelo fornecimento integral da solução.

16.3 Não será aceito a formação de consórcio de empresas na disputa da licitação, por se tratar de um bem e serviço comum, que não exige a união de competências técnicas ou financeiras de múltiplas empresas para ser executada. A instalação e configuração dos equipamentos não demandam uma "alta complexidade" ou a combinação de expertises de diferentes áreas, tirando a razão de ser da formação de um consórcio, que é a de viabilizar a participação em projetos de grande envergadura. Ademais, este projeto requer celeridade em sua execução (entrega e instação), facilitação na gestão contratual e centralização de responsabilidades, dado que inclui a contratação de suporte integral pelo fornecedor.

## 17 **VIGÊNCIA DO CONTRATO**

17.1 A vigência será definida no termo de contrato, devendo contemplar o período de entrega, bem como o de garantia de 5 (cinco) anos e 60 (sessenta) dias, contados a partir do recebimento definitivo dos equipamentos.

## 18 **PENALIDADES**

18.1 O atendimento aos níveis de serviços mínimos deve ser considerado para fins de aplicação de sanção;

18.2 Poderão ser aplicadas à Contratada as seguintes sanções:

18.2.1 Advertência, nos casos de inexecução parcial do contrato que correspondam a pequenas irregularidades verificadas na execução contratual que não justifiquem a imposição de penalidades mais graves;

18.2.2 Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta da União, pelo prazo máximo de 3 (três) anos, nos casos de inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo; inexecução total do contrato; retardamento da execução ou da entrega do objeto contratado sem motivo justificado;

18.2.3 Declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos de declaração falsa durante a execução do contrato; comportamento inidôneo ou cometimento de fraude de qualquer natureza, prática de ato lesivo previsto no art. 5º da Lei 12.846, de 2013, bem como, nos casos especificados que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta da União.

18.3 A CONTRATADA estará sujeita ainda às seguintes multas:

18.3.1 0,5% (meio por cento) por irregularidade apontada, limitada a 5% (cinco por cento), sobre o valor total do contrato, nos casos especificados no item 18.2.1;

18.3.2 1% (um por cento) por dia, limitada a 10% (dez por cento), sobre o valor total do contrato pelo retardamento da entrega do objeto contratado sem motivo justificado;

18.3.3 5% (cinco por cento) por evento, limitada a 20% (vinte por cento), sobre o valor o valor total do contrato no caso de inexecução total do Ajuste ou no caso de inexecução parcial que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

18.3.4 10% (dez por cento), limitada a 30% (trinta por cento), sobre o valor total do contrato, nos casos especificados no item 18.2.3.

## 19 **REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS**

19.1 A aquisição dos equipamentos deverá considerar os princípios de sustentabilidade e responsabilidade social e ambiental. A CONTRATADA deverá tomar conhecimento do Plano de Logística Sustentável (PLS) do TRE-GO e observar a Resolução CNJ nº 400/2021. É fundamental que os produtos atendam aos critérios de Sustentabilidade Ambiental, Social e Econômica.

## 20 **REQUISITOS DE SEGURANÇA DA INFORMAÇÃO**

20.1 A contratação deverá estar em total conformidade com a Lei nº 13.709/2018 (LGPD) e suas alterações, Resolução CNJ nº 468/2022 (Diretrizes para STIC), e Resolução CNJ nº 396/2021 (ENSEC-PJ). Todos os envolvidos devem guardar sigilo quanto às configurações aplicadas na solução adquirida.

## **ANEXO I - PESQUISA DE PREÇOS**

Mapa Comparativo de Preços

Relatório gerado no dia 16/10/2025 17:30:49 (IP: 200.195.253.66)

Os cálculos deste relatório foram elaborados com base nas metodologias descritas na 4ª edição do Manual de Orie
de Pesquisa de Preços do Superior Tribunal de Justiça (STJ). A utilização desse manual assegura a precisão e a confiabilida
cálculos apresentados, conforme os padrões estabelecidos pelo STJ.

| Critérios Estatísticos Gerais | |
|---|---|
| 30% | Preços excessivamente elevados: valores superiores a 30% da média do rol de preços obtidos |
| 70% | Inexequível: valores inferiores a 70% da média do rol de preços obtidos |

| | | | | | | | Válido | |
|---|---|---|---|---|---|---|---|---|
| Item | Média | Mediana | Desvio Padrão Amostral | Coeficiente de Variação | Método Estatístico | Preço Mínimo | Média | Mec |
| Appliance físico - Item 1 | R$ 2.034.048,57 | R$ 1.770.885,37 | 1007778,23 | 49,55 | Média | R$ 808.230,00 | R$ 1.612.406,44 | 1.612 |
| Appliance físico - Item 2 | R$ 2.034.048,57 | R$ 1.770.885,37 | 1007778,23 | 49,55 | Média | R$ 808.230,00 | R$ 1.612.406,44 | 1.612 |
| Serviço de migração - Item 3 | R$ 89.899,54 | R$ 89.899,54 | 16192,09 | 18,01 | Média | R$ 78.450,00 | R$ 89.899,54 | R$ 89 |
| Appliance virtual - Item 4 | R$ 1.253.406,21 | R$ 1.253.406,21 | 114701,5 | 9,15 | Média | R$ 1.172.300,00 | R$ 1.253.406,21 | 1.253 |
| Appliance físico menor porte - Item 5 | R$ 36.812,64 | R$ 35.223,25 | 12256,75 | 33,29 | Média | R$ 24.000,00 | R$ 29.693,95 | R$ 28 |
| Treinamento - Item 6 | R$ 48.267,48 | R$ 48.267,48 | 37289,24 | 77,26 | Média | R$ 21.900,00 | R$ 21.900,00 | R$ 21 |

| LOTE 1: Projeto Firewall TRE-GO (6 itens) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Item | Especificação | Und | Qtd | Cotação | Parâmetros | Empresas | Porte | Valor Unit | Méd |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Checkpoint, Fortinet e Palo Alto | un | 2 | MINISTÉRIO DA SAÚDE \| Secretaria Executiva \| Subsecretaria de Assuntos Administrativos \| Coordenação-Geral de Material e Patrimônio | Compras.gov.br | GLOBAL SEC. TECNOLOGIA & INFORMACAO EIRELI | Microempresa | R$ 808.230,00 | 2.034.0 |
| | | | | PRESIDÊNCIA DA REPÚBLICA \| Advocacia Geral da União \| Diretoria Geral de Administração \| Diretoria de Logística e Gestão Documental | Compras.gov.br | NORDEN TECNOLOGIA LTDA | Microempresa | R$ 1.453.927,50 | |
| | | | | GOVERNO DO ESTADO DO CEARÁ | Compras.gov.br | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | Empresa de Pequeno Porte (EPP) | R$ 3.150.600,00 | |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 2.986.600,00 | |
| | | | | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 1.770.885,37 | |
| 2 | Checkpoint, Fortinet e Palo Alto | un | 2 | MINISTÉRIO DA SAÚDE \| Secretaria Executiva \| Subsecretaria de Assuntos Administrativos \| Coordenação-Geral de Material e Patrimônio | Compras.gov.br | GLOBAL SEC. TECNOLOGIA & INFORMACAO EIRELI | Microempresa | R$ 808.230,00 | 2.034.0 |
| | | | | PRESIDÊNCIA DA REPÚBLICA \| Advocacia Geral da União \| Diretoria Geral de Administração \| Diretoria de Logística e Gestão Documental | Compras.gov.br | NORDEN TECNOLOGIA LTDA | Microempresa | R$ 1.453.927,50 | |
| | | | | GOVERNO DO ESTADO DO CEARÁ | Compras.gov.br | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | Empresa de Pequeno Porte (EPP) | R$ 3.150.600,00 | |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 2.986.600,00 | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 1.770.885,37 | |
| 3 | Migração para nova solução | un | 2 | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 101.349,08 | 89.8 |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 78.450,00 | |
| 4 | Console de gerenciamento centralizado | un | 1 | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 1.334.512,41 | 1.253.4 |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 1.172.300,00 | |
| 5 | Console | un | 200 | PODER JUDICIÁRIO \| Justiça Federal \| JUSTIÇA FEDERAL DE PRIMEIRO GRAU SECAO JUDICIARIA DE ALAGOAS | Compras.gov.br | ARPSIST SERVICOS DE ENGENHARIA LTDA | Empresa de Pequeno Porte (EPP) | R$ 37.614,93 | 36.8 |
| | | | | GOVERNO DO ESTADO DO CEARÁ | Compras.gov.br | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | Empresa de Pequeno Porte (EPP) | R$ 48.900,00 | |
| | | | | PODER JUDICIÁRIO \| Tribunal Regional Federal \| TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO | Compras.gov.br | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | Empresa de Pequeno Porte (EPP) | R$ 24.000,00 | |
| | | | | SERVIÇO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS DO ESTADO DO PARA SEBRAE PA | Compras.gov.br | CONNECTA - CONSULTORIA, COMERCIO E SERVICOS DE INFORMATICA LTDA | Empresa de Pequeno Porte (EPP) | R$ 24.329,32 | |
| | | | | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 32.831,56 | |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 53.200,00 | |
| 6 | Repasse de conhecimento | un | 1 | --- | Preço Manual | NTSEC SOLUCOES EM TELEINFORMATICA LTDA | --- | R$ 74.634,95 | 48.2 |
| | | | | --- | Preço Manual | TELTEC SOLUTIONS LTDA | --- | R$ 21.900,00 | |

Documento assinado eletronicamente por **ROBERTO CÉSAR RODRIGUES**, **COORDENADOR(A)**, em 24/11/2025, às 09:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei4.tre-go.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1262129** e o código CRC **81E09855**.