GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL - SETD
CENTRO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO – PRODERJ

# ANEXO X – ROTEIRO PARA O TESTE DE BANCADA

Ref. Pregão Eletrônico para Registro de Preços - PRODERJ – PE-RP nº 002/2023.

| ESPECIFICAÇÕES TÉCNICAS | ATENDE? SIM / NÃO / PARCIALMENTE | RESPONSÁVEL PELA APROVAÇÃO |
|---|---|---|
| **1. Appliance Firewall (Item 1)** | | |
| **1.1. Características Gerais** | | |
| 1.1.1. Deve possuir o throughput mínimo de 200 Mbps com as funcionalidades de Filtro de Pacotes, IPS, Controle de aplicações e Proteção contra Malwares habilitadas simultaneamente. | | |
| 1.1.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 1 Gbps. | | |
| 1.1.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 400 Mbps. | | |
| 1.1.4. Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 200 Mbps, juntamente com as funcionalidades do Item 1.1.1.1. | | |
| 1.1.5. Deve permitir, no mínimo, 400.000 conexões simultâneas. | | |
| 1.1.6. Deve permitir, no mínimo, 18.000 novas conexões por segundo. | | |
| 1.1.7. Deve permitir, no mínimo, 4000 VLANs. | | |
| 1.1.8. Deve permitir, no mínimo, 10 túneis VPN site-to-site simultâneos. | | |
| 1.1.9. Deve permitir, no mínimo, 100 túneis VPN client-to-site simultâneos. | | |
| 1.1.10. O appliance deve possuir, no mínimo, 4 (quatro) portas 10/100/1000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers. | | |
| **1.2. Funcionalidades Específicas** | | |

| | | |
|---|---|---|
| **1.2.1. Arquitetura** | | |
| 1.2.1.1. A solução presente neste documento é composta por equipamentos de firewalls gerenciados de forma centralizada. | | |
| 1.2.1.2. Os firewalls gerenciados devem ser capazes de encaminhar pacotes para serem analisados pelo firewall concentrador. | | |
| 1.2.1.3. O gerenciamento centralizado é composto por um sistema que administra, configura e gerencia todos os firewalls da solução ofertada. | | |
| **1.2.2. Licenciamento** | | |
| 1.2.2.1. Todos os equipamentos alugados deverão estar devidamente licenciados pelo fabricante, e não serão aceitas cobranças adicionais relativas ao licenciamento dos equipamentos. | | |
| **1.2.3. Hardware** | | |
| 1.2.3.1. Deve ser fornecido em formato appliance físico. | | |
| 1.2.3.2. Deve ser entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos. | | |
| 1.2.3.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support no dia do Pregão Eletrônico. | | |
| 1.2.3.4. Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C. | | |
| 1.2.3.5. Deve possuir fonte com alimentação nominal de 100~230VAC (Auto). Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136. | | |
| 1.2.3.6. Deve possuir, no mínimo, 1 (uma) interface Ethernet ou USB dedicada para gerenciamento. | | |
| 1.2.3.7. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais, inclusive com seus respectivos transceivers instalados, sem custos adicionais. | | |
| 1.2.3.8. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7. | | |
| **1.2.4. Funcionalidades Básicas** | | |
| 1.2.4.1. Deve possuir indicadores de estado do hardware e de performance do equipamento. | | |
| 1.2.4.2. Deve suportar o envio de notificações via e-mail e/ou SNMP; | | |
| 1.2.4.3. Deve permitir o acesso ao equipamento via SSH e interface web HTTPS autenticada. | | |
| 1.2.4.4. Deve informar a utilização dos recursos de CPU, memória e atividade de rede. | | |
| 1.2.4.5. Deve possuir visibilidade sobre aplicações, ameaças, URLs, endereços de origem, endereços de destino, quantitativo de sessões, de consumo de banda e categorização. | | |
| 1.2.4.6. Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a solução de gerenciamento de logs. | | |
| **1.2.5. Rede** | | |
| 1.2.5.1. Deve suportar os protocolos IPv4 e IPv6. | | |

1.2.5.2. Deve suportar VLAN no padrão 802.1q.

1.2.5.3. Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.

1.2.5.4. Deve suportar Jumbo Frames.

1.2.5.5. Deve suportar sub interfaces Ethernet lógicas.

1.2.5.6. Deve suportar o protocolo NTP.

1.2.5.7. Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N);

1.2.5.8 Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

1.2.5.9. Deve suportar tradução de porta (PAT).

1.2.5.10. Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.

1.2.5.11. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

1.2.5.12. Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.

1.2.5.13. Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente.

1.2.5.14. Deve suportar os protocolos SNMP v2 e SNMP v3.

1.2.5.15. Deve permitir monitorar, via SNMP, ao menos as seguintes informações: Status do equipamento, número de túneis estabelecidos na VPN, utilização de CPU e memória e estatísticas de uso das interfaces de rede.

1.2.5.16. Deve suportar Roteamento baseado em políticas, de modo a possibilitar políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

| **1.2.6. Autenticação e Identificação de Usuários** | | |
|---|---|---|

1.2.6.1. Deve promover a integração com serviços de diretório LDAP e Active Directory, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

1.2.6.2. Deve identificar os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory.

1.2.6.3. Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.

1.2.6.4. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.

1.2.6.5. Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.

1.2.6.6. Deve registrar os eventos dos usuários em tempo real;

1.2.6.7. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

| **1.2.7. Geolocalização** | | |
|---|---|---|

1.2.7.1. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.

1.2.7.2. Deve armazenar as listas de geolocalização no próprio equipamento.

1.2.7.3. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

1.2.7.4. Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

| **1.2.8. VPN** | | |
|---|---|---|

1.2.8.1. Deve suportar VPN site-to-site;

1.2.8.2. Deve suportar criptografia 3DES, AES-128, AES-256.

1.2.8.3. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

1.2.8.4. Deve suportar o protocolo IKE, fases I e II.

1.2.8.5. Deve suportar os algoritmos RSA e Diffie-Hellman groups;

1.2.8.6. Deve suportar Certificado Digital X.509.

1.2.8.7. Deve suportar NAT-T (NAT Transversal).

1.2.8.8. Deve permitir a criação de túneis VPN SSL/TLS e IPSec.

1.2.8.9. Deve suportar VPN IPSec client-to-site (acesso remoto).

1.2.8.10. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado em ao menos um dos seguintes sistemas operacionais: Windows, Mac OS ou Linux, ou ainda por meio de interface web (HTTPS).

.2.8.11. O acesso VPN, caso ocorra por meio da interface Web, deverá ser compatível, no mínimo, com dois dos seguintes navegadores: Microsoft Edge, Firefox, Google Chrome e Safari;

1.2.8.12. Deve suportar atribuição de endereço IP nos clientes remotos de VPN, caso o acesso não seja feito via browser;

1.2.8.13. Deve suportar atribuição de DNS nos clientes remotos de VPN, caso o acesso não seja feito via browser;

1.2.8.14. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP;

1.2.8.15. O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.

1.2.8.16. O túnel IPSec VPN client-to-site deve também possuir autenticação em fator duplo (2FA) aos usuários.

1.2.8.17. Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.

1.2.8.18. Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.

1.2.8.19. Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.

1.2.8.20. Desejável suportar os seguintes métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.

1.2.8.21. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.

1.2.8.22. Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol) ou CSR (Certificate Signing Requests).

2.8.23. Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists).

1.2.8.24. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

| **1.2.9. Qualidade de Serviço (QoS)** | | |
|---|---|---|

1.2.9.1. Deve permitir o controle de políticas de uso com as seguintes opções: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação, usuário ou host.

1.2.9.2. Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).

1.2.9.3. Deve suportar a priorização de protocolos de voz (VoIP) como H.323, SIP.

1.2.9.4. Deve suportar a marcação de pacotes DiffServ.

1.2.9.5. Deve permitir o monitoramento do uso de aplicações.

| **1.2.10. Balanceamento de Links** | | |
|---|---|---|

1.2.10.1. Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 2 (dois) links WAN.

1.2.10.2. Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.

1.2.10.3. Deve possuir roteamento baseado em políticas.

1.2.10.4. Deve permitir a configuração de failover entre o link principal e secundário, caso o link utilizado ultrapasse os limites previamente definidos de jitter, latência e perda de pacotes.

1.2.10.5. Deve suportar a configuração de regras que permita o failback imediato.

1.2.10.6. Deve realizar o gerenciamento de tráfego por tipo de aplicação.

1.2.10.7. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem.

1.2.10.8. Deve suportar o monitoramento de link com ping e TCP echo.

| **1.2.11. Recursos de Segurança** | | |
|---|---|---|

1.2.11.1. Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Malware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web, Controle de Aplicação.

1.2.11.2. Deve suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3, de forma simultânea em uma única instância de firewall.

1.2.11.3. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.

1.2.11.4. Deve suportar as atualizações automáticas das bases de assinaturas utilizadas na identificação de vírus, intrusões

(IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, e sem reinicialização do equipamento.

1.2.11.5. Deve suportar as atualizações das listas de geolocalização e das listas e categorias de URLs sem a necessidade de reinicialização do equipamento.

1.2.11.6. Deve possuir proteção contra ataques, no mínimo, dos tipos: IP Spoofing, Negação de Serviço, SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Port Scanning.

1.2.11.7. Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound), com suporte a HTTP/2 e TLS 1.2 e 1.3.

1.2.11.8. Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças.

1.2.11.9. Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática.

1.2.11.10. Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.

1.2.11.11. Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos.

1.2.11.12. Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP.

| **1.2.12. Filtro de Pacotes** | | |
|---|---|---|

1.2.12.1. Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).

1.2.12.2. Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6.

1.2.12.3. Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.

1.2.12.4. Deve suportar o protocolo SIP.

1.2.12.5. Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti- spoofing).

1.2.12.6. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.

1.2.12.7. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.

1.2.12.8. Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

1.2.12.9. Deve suportar granularidade nas políticas de IPS, antivírus e anti-malware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

| **1.2.13. Filtro de Conteúdo** | | |
|---|---|---|

1.2.13.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.

1.2.13.2. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

1.2.13.3. Deve ser capaz de identificar aplicações criptografadas usando SSL.

1.2.13.4. Deve ser capaz de identificar diversos tipos de aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

1.2.13.5. Deve armazenar a base de assinaturas no próprio equipamento.

1.2.13.6. Deve classificar as aplicações em categorias.

1.2.13.7. Deve permitir o agrupamento de aplicações em grupos personalizados.

1.2.13.8. Deve identificar os usuários que estão utilizando as aplicações.

1.2.13.9. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.2.13.10. Deve permitir a utilização ou bloqueio individualizado das aplicações para determinados usuários ou grupos de usuários.

1.2.13.11. Deve permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.

1.2.13.12. Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.2.13.13. Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.

1.2.13.14. Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware.

1.2.13.15. Deve permitir a inclusão de URLs customizadas por política (whitelist).

1.2.13.16. Deve armazenar as listas de categoria no próprio equipamento.

1.2.13.17. Deve identificar os usuários que estão acessando as páginas web.

1.2.13.18. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.2.13.19. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.

1.2.13.20. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.

1.2.13.21. Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

1.2.13.22. Deve possuir o recurso “safe search”, permitindo o bloqueio do acesso a resultados inapropriados em sites de busca (Google, Bing, Yahoo).

1.2.13.23. Deve suportar base ou cache de URL’s local no appliance, evitando delay de comunicação/validação das URL’s.

| | | |
|---|---|---|
| **1.2.14. Prevenção de Intrusão (IPS)** | | |
| 1.2.14.1. Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura. | | |
| 1.2.14.2. Deve possuir um conjunto de assinaturas de detecção e prevenção de ataques. | | |
| 1.2.14.3. Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão. | | |
| 1.2.14.4. Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation e nível de severidade do ataque. | | |
| 1.2.14.5. Deve ser capaz de inspecionar tráfego criptografado usando SSL/TLS. | | |
| 1.2.14.6. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos. | | |
| 1.2.14.7. Deve identificar os usuários relacionados aos eventos de intrusão. | | |
| 1.2.14.8. Deve identificar os usuários relacionados aos eventos de bloqueio. | | |
| 1.2.14.9. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça. | | |
| 1.2.14.10. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça. | | |
| 1.2.14.11. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado. | | |
| 1.2.14.12. Deve bloquear malwares e spywares. | | |
| 1.2.14.13. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS, SMTP, POP3, FTP e SMB | | |
| 1.2.14.14. Deve suportar proteção contra vírus em conteúdo HTML e javascrip, software espião (spyware) e worms. | | |
| 1.1.2.14.15. Deve suportar a inspeção de vírus em arquivos comprimidos (zip, gzip etc). | | |
| 1.2.14.16. Deve armazenar as bases de assinaturas no próprio equipamento. | | |
| 1.2.14.17. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfego HTTP/2. | | |
| **2. Console de Gerenciamento Centralizado para Firewall (Item 2)** | | |
| **2.1. Características Gerais** | | |
| 2.1.1. Será admitida composição de produtos para o fornecimento deste item. | | |
| 2.1.2. A entrega do item deverá ser em formato appliance virtual. Caso o appliance virtual não seja suficiente para o pleno atendimento das necessidades da contratante, o item deverá ser fornecido como appliance físico, desde que esta alteração esteja em comum acordo entre as partes. | | |
| 2.1.3. Os appliances virtuais deverão ser compatíveis com VMWare vSphere ESXi 6.5 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 e superiores. | | |
| 2.1.4. Caso o item seja fornecido excepcionalmente em formato apppliance físico, deverá ter suporte à fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até três unidades de rack (3U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc). Neste caso, o equipamento deve ter | | |

capacidade de 4TB de área útil de armazenamento destinada aos logs.

2.1.5. Todos os equipamentos alugados deverão estar devidamente licenciados pelo fabricante, e não serão aceitas cobranças adicionais relativas ao licenciamento dos equipamentos.

| **2.2. Gerenciamento** | | |
|---|---|---|

2.2.1. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado em sistemas Windows ou Linux.

2.2.2. Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 15 equipamentos.

2.2.3. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

2.2.4. As comunicações entre a Console de Gerenciamento e os firewalls e entre a Console de Gerenciamento e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

2.2.5. Deve ser capaz de realizar todas as configurações nos firewalls descritas neste documento.

2.2.6. Deve possibilitar a aplicação simultânea de configurações em todos os firewalls gerenciados pela solução.

2.2.7. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

2.2.8. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.

2.2.9. Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.

2.2.10. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.

2.2.11. Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.

2.2.12. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

2.2.13. Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.

2.2.14. Deve suportar a identificação e utilização de usuários nas políticas de segurança.

2.2.15. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.

2.2.16. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede, de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

2.2.17. Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.2.18. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.

2.2.19. Deve ser capaz de monitorar a conectividade dos equipamentos gerenciados.

2.2.20. Deve monitorar a performance e o estado dos links conectados.

2.2.21. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.

2.2.22. Deve permitir localizar em quais regras um objeto está sendo utilizado.

2.2.23. Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, e identificar aquelas que estejam em desuso.

2.2.24. Deve suportar a geração de alertas automáticos via e-mail, SNMP e/ou syslog.

2.2.25. Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.

2.2.26. O gerenciamento da solução deve suportar ao menos duas das seguintes formas de acesso: SSH, cliente, WEB (HTTPS) ou API aberta.

| **2.3. Relatórios** | | |
|---|---|---|

2.3.1. Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.

2.3.2. Deve permitir a extração de relatórios;

2.3.3. Deve possuir relatórios pré-definidos;

2.3.4. Deve permitir customização de quaisquer relatórios fornecidos pela console.

2.3.5. Deve permitir a geração de relatórios de logs de tráfego de dados;

2.3.6. Deve permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos;

2.3.7. Deve possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza, para inserção aos relatórios;

2.3.8. Permitir o agendamento da geração de relatórios;

2.3.9. Ter a capacidade de definir filtros nos relatórios;

2.3.10. Deve permitir a criação de painéis (dashboards) customizados.

2.3.11. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados.

| **2.4. Logs** | | |
|---|---|---|

2.4.1. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc.

2.4.2. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.

2.4.3. Deve ser capaz de receber logs de todos os firewalls gerenciados pela solução.

2.4.4. Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

2.4.5. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).

2.4.6. Deve possuir funcionalidade de exportação de relatórios e logs.