**A N E X O I – B**

CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO PROPOSTA

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipamentos NGFW** | | |  |
| 1 | 1. **SOLUÇÃO NGFW TIPO 1 PARA DATACENTER**    1. CARACTERÍSTICAS ESPECÍFICAS       1. Throughput de, no mínimo, 34 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4;       2. Suporte a, no mínimo, 8 Milhões conexões simultâneas;       3. Suporte a, no mínimo, 400 Mil novas conexões por segundo;       4. Throughput de, no mínimo, 20 Gbps de VPN IPSec;       5. Estar licenciado para, ou suportar sem o uso de licença, 2 Mil túneis de VPN IPSEC Site-to-Site simultâneos;       6. Estar licenciado para, ou suportar sem o uso de licença, 50 Mil túneis de clientes VPN IPSEC simultâneos;       7. Throughput de, no mínimo, 6 Gbps de VPN SSL;       8. Suporte a, no mínimo, 5000 clientes de VPN SSL simultâneos;       9. Suportar no mínimo 9 Gbps de throughput de IPS;       10. Suportar no mínimo 7 Gbps de throughput de Inspeção SSL;       11. Throughput de, no mínimo, 7 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;       12. Possuir ao menos 8 interfaces SFP 1Gbps;           1. Deverão ser fornecidos 2 transceivers 1 GE SFP SX;           2. Deverão ser fornecidos 2 transceivers 1 GE SFP LX;           3. Os transceivers fornecidos deverão ser do mesmo fabricante da solução NGFW;       13. Possuir ao menos 4 interfaces 1000Base-T;       14. Possuir ao menos 2 interfaces SFP+ TenGigabit Ethernet 10Gbps;           1. Deverão ser fornecidos 2 transceivers 10 GE SFP+ SR;           2. Os transceivers fornecidos deverão ser do mesmo fabricante da solução NGFW;       15. Possuir ao menos 2 interfaces para Gerenciamento/HA;       16. Disco de, no mínimo, 480 GB SSD para armazenamento de informações locais;       17. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;       18. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.    2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE       1. CARACTERÍSTICAS GERAIS    3. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;    4. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;    5. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;    6. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;    7. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19’, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;    8. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;    9. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;    10. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;    11. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;    12. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);    13. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;    14. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;    15. Os dispositivos de proteção de rede devem suportar sFlow ou tecnologia similar;    16. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;    17. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;    18. Deve suportar NAT dinâmico (Many-to-1);    19. Deve suportar NAT dinâmico (Many-to-Many);    20. Deve suportar NAT estático (1-to-1);    21. Deve suportar NAT estático (Many-to-Many);    22. Deve suportar NAT estático bidirecional 1-to-1;    23. Deve suportar Tradução de porta (PAT);    24. Deve suportar NAT de Origem;    25. Deve suportar NAT de Destino;    26. Deve suportar NAT de Origem e NAT de Destino simultaneamente;    27. Deve poder combinar NAT de origem e NAT de destino na mesma política    28. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;    29. Deve suportar NAT64 e NAT46;    30. Deve implementar o protocolo ECMP;    31. Deve implementar balanceamento de link por hash do IP de origem;    32. Deve implementar balanceamento de link por hash do IP de origem e destino;    33. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;    34. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;    35. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;    36. Enviar log para sistemas de monitoração externos, simultaneamente;    37. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;    38. Proteção anti-spoofing;    39. Implementar otimização do tráfego entre dois equipamentos;    40. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);    41. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);    42. Suportar OSPF graceful restart;    43. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;    44. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;    45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;    46. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;    47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;    48. A configuração em alta disponibilidade deve sincronizar: Sessões;    49. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede;    50. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;    51. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;    52. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;    53. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;    54. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;    55. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;    56. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces;    57. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);    58. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede;    59. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;    60. CONTROLE POR POLITICA DE FIREWALL        1. Deverá suportar controles por zona de segurança;        2. Controles de políticas por porta e protocolo;        3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;        4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;        5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;        6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;        7. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);        8. Deve suportar o protocolo padrão de indústria 'syslog' para armazenamento usando o formato Common Event Format (CEF);        9. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supera a velocidade de upload;        10. Deve suportar o protocolo padrão da indústria VXLAN;    61. CONTROLE DE APLICAÇÕES        1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;        2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;        3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;        4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;        5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;        6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;        7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;        8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;        9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;        10. Identificar o uso de táticas evasivas via comunicações criptografadas;        11. Atualizar a base de assinaturas de aplicações automaticamente;        12. Limitar a banda (download/upload) usada por aplicações (traffic shaping) baseado no IP de origem, usuários e grupos;        13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;        14. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;        15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;        16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;        17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;        18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;        19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;        20. Deve alertar o usuário quando uma aplicação for bloqueada;        21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;        22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;        23. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;        24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;        25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);        26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;        27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;        28. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.    62. PREVENÇÃO DE AMEAÇAS        1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;        2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);        3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;        4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;        5. 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;        6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;        7. Deve ser possível, a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;        8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;        9. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;        10. Deve permitir o bloqueio de vulnerabilidades;        11. Deve permitir o bloqueio de exploits conhecidos;        12. Deve incluir proteção contra ataques de negação de serviços;        13. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;        14. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo;        15. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;        16. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise heurística;        17. Deverá possuir os seguintes mecanismos de inspeção de IPS: IP Defragmentation;        18. Deverá possuir os seguintes mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;        19. Deverá possuir os seguintes mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;        20. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;        21. Detectar e bloquear a origem de portscans;        22. Bloquear ataques efetuados por worms conhecidos;        23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;        24. Possuir assinaturas para bloqueio de ataques de buffer overflow;        25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;        26. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;        27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;        28. Suportar bloqueio de arquivos por tipo;        29. Identificar e bloquear comunicação com botnets;        30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;        31. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;        32. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;        33. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;        34. Os eventos devem identificar o país de onde partiu a ameaça;        35. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;        36. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;        37. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;        38. O Firewall deve permitir que se analisasse a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que possam ser usadas para melhorar a segurança e o desempenho geral da rede;        39. Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis;        40. Análises de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint;        41. Fornecem proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem);    63. FILTRO DE URL        1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);        2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;        3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;        4. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;        5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;        6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;        7. Possuir pelo menos 60 categorias de URLs;        8. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;        9. Permitir a customização de página de bloqueio;        10. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);        11. Além do Explicit Web Proxy, suportar proxy Web transparente;    64. IDENTIFICAÇÃO DE USUÁRIOS        1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;        2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;        3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;        4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;        5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;        6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;        7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);        8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;        9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;        10. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;        11. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;    65. QOS E TRAFFIC SHAPING        1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;        2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;        3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;        4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;        5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;        6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;        7. O QoS deve possibilitar a definição de tráfego com banda garantida;        8. O QoS deve possibilitar a definição de tráfego com banda máxima;        9. O QoS deve possibilitar a definição de fila de prioridade;        10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;        11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;        12. Suportar modificação de valores DSCP para o Diffserv;        13. Suportar priorização de tráfego usando informação de Type of Service;        14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;        15. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;    66. FILTRO DE DADOS        1. Permitir a criação de filtros para arquivos e dados pré-definidos;        2. Os arquivos devem ser identificados por extensão e tipo;        3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);        4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;        5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;        6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;    67. GEO LOCALIZAÇÃO        1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;        2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;        3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;    68. VPN        1. Suportar VPN Site-to-Site e Cliente-To-Site;        2. Suportar IPSec VPN;        3. Suportar SSL VPN;        4. A VPN IPSEc deve suportar 3DES;        5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;        6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;        7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);        8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);        9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;        10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;        11. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;        12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;        13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;        14. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;        15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;        16. Atribuição de DNS nos clientes remotos de VPN;        17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;        18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;        19. Suportar leitura e verificação de CRL (certificate revocation list);        20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;        21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;        22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;        23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;        24. Deverá manter uma conexão segura com o portal durante a sessão;        25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior); | UND | 06 |
| 2 | 1. **SOLUÇÃO NGFW TIPO 2 PARA DATACENTER**    1. CARACTERÍSTICAS ESPECÍFICAS       1. Throughput de, no mínimo, 80 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4;       2. Suporte a, no mínimo, 7 Milhões conexões simultâneas;       3. Suporte a, no mínimo, 400 Mil novas conexões por segundo;       4. Throughput de, no mínimo, 40 Gbps de VPN IPSec;       5. Estar licenciado para, ou suportar sem o uso de licença, 10 Mil túneis de VPN IPSEC Site-to-Site simultâneos;       6. Estar licenciado para, ou suportar sem o uso de licença, 50 Mil túneis de clientes VPN IPSEC simultâneos;       7. Throughput de, no mínimo, 7 Gbps de VPN SSL;       8. Suporte a, no mínimo, 8000 clientes de VPN SSL simultâneos;       9. Suportar no mínimo 10 Gbps de throughput de IPS;       10. Suportar no mínimo 8 Gbps de throughput de Inspeção SSL;       11. Throughput de, no mínimo, 7 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;       12. Possuir ao menos 16 interfaces 1Gbps;       13. Possuir ao menos 4 interfaces SFP+ TenGigabit Ethernet 10Gbps;           1. Deverão ser fornecidos 4 transceivers 10 GE SFP+ SR;           2. Os transceivers fornecidos deverão ser do mesmo fabricante da solução NGFW;       14. Possuir ao menos 2 interfaces QSFP+ FortyGigabit Ethernet 40Gbps;           1. Deverão ser fornecidos 2 transceivers 40 GE QSFP+ SR;           2. Os transceivers fornecidos deverão ser do mesmo fabricante da solução NGFW;       15. Possuir ao menos 2 interfaces 25G SFP28;       16. Possuir ao menos 2 interfaces para Gerenciamento/HA;       17. Disco de, no mínimo, 960 GB SSD para armazenamento de informações locais;       18. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;       19. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.    2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE       1. CARACTERÍSTICAS GERAIS    3. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;    4. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;    5. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;    6. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;    7. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19’, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;    8. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;    9. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;    10. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;    11. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;    12. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);    13. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;    14. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;    15. Os dispositivos de proteção de rede devem suportar sFlow ou tecnologia similar;    16. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;    17. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;    18. Deve suportar NAT dinâmico (Many-to-1);    19. Deve suportar NAT dinâmico (Many-to-Many);    20. Deve suportar NAT estático (1-to-1);    21. Deve suportar NAT estático (Many-to-Many);    22. Deve suportar NAT estático bidirecional 1-to-1;    23. Deve suportar Tradução de porta (PAT);    24. Deve suportar NAT de Origem;    25. Deve suportar NAT de Destino;    26. Deve suportar NAT de Origem e NAT de Destino simultaneamente;    27. Deve poder combinar NAT de origem e NAT de destino na mesma política    28. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;    29. Deve suportar NAT64 e NAT46;    30. Deve implementar o protocolo ECMP;    31. Deve implementar balanceamento de link por hash do IP de origem;    32. Deve implementar balanceamento de link por hash do IP de origem e destino;    33. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;    34. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;    35. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;    36. Enviar log para sistemas de monitoração externos, simultaneamente;    37. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;    38. Proteção anti-spoofing;    39. Implementar otimização do tráfego entre dois equipamentos;    40. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);    41. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);    42. Suportar OSPF graceful restart;    43. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;    44. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;    45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;    46. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;    47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;    48. A configuração em alta disponibilidade deve sincronizar: Sessões;    49. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede;    50. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;    51. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;    52. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;    53. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;    54. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;    55. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;    56. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces;    57. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);    58. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede;    59. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;    60. CONTROLE POR POLÍTICA DE FIREWALL        1. Deverá suportar controles por zona de segurança;        2. Controles de políticas por porta e protocolo;        3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;        4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;        5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;        6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;        7. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);        8. Deve suportar o protocolo padrão de indústria 'syslog' para armazenamento usando o formato Common Event Format (CEF);        9. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supera a velocidade de upload;        10. Deve suportar o protocolo padrão da indústria VXLAN;    61. CONTROLE DE APLICAÇÕES        1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;        2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;        3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;        4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;        5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;        6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;        7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;        8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;        9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;        10. Identificar o uso de táticas evasivas via comunicações criptografadas;        11. Atualizar a base de assinaturas de aplicações automaticamente;        12. Limitar a banda (download/upload) usada por aplicações (traffic shaping) baseado no IP de origem, usuários e grupos;        13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;        14. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;        15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;        16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;        17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;        18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;        19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;        20. Deve alertar o usuário quando uma aplicação for bloqueada;        21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule etc.) possuindo granularidade de controle/políticas para os mesmos;        22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;        23. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;        24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;        25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);        26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;        27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;        28. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.    62. PREVENÇÃO DE AMEAÇAS        1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;        2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);        3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;        4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;        5. 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;        6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;        7. Deve ser possível, a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;        8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;        9. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;        10. Deve permitir o bloqueio de vulnerabilidades;        11. Deve permitir o bloqueio de exploits conhecidos;        12. Deve incluir proteção contra ataques de negação de serviços;        13. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;        14. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo;        15. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;        16. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise heurística;        17. Deverá possuir os seguintes mecanismos de inspeção de IPS: IP Defragmentation;        18. Deverá possuir os seguintes mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;        19. Deverá possuir os seguintes mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;        20. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;        21. Detectar e bloquear a origem de portscans;        22. Bloquear ataques efetuados por worms conhecidos;        23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;        24. Possuir assinaturas para bloqueio de ataques de buffer overflow;        25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;        26. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;        27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;        28. Suportar bloqueio de arquivos por tipo;        29. Identificar e bloquear comunicação com botnets;        30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;        31. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;        32. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;        33. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;        34. Os eventos devem identificar o país de onde partiu a ameaça;        35. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;        36. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;        37. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;        38. O Firewall deve permitir que se analisasse a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que possam ser usadas para melhorar a segurança e o desempenho geral da rede;        39. Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis;        40. Análises de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint;        41. Fornecem proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem);    63. FILTRO DE URL        1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);        2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;        3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;        4. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;        5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;        6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;        7. Possuir pelo menos 60 categorias de URLs;        8. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;        9. Permitir a customização de página de bloqueio;        10. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);        11. Além do Explicit Web Proxy, suportar proxy Web transparente;    64. IDENTIFICAÇÃO DE USUÁRIOS        1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;        2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;        3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;        4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;        5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;        6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;        7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);        8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;        9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;        10. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;        11. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;    65. QOS E TRAFFIC SHAPING        1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;        2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;        3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;        4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;        5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;        6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;        7. O QoS deve possibilitar a definição de tráfego com banda garantida;        8. O QoS deve possibilitar a definição de tráfego com banda máxima;        9. O QoS deve possibilitar a definição de fila de prioridade;        10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;        11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;        12. Suportar modificação de valores DSCP para o Diffserv;        13. Suportar priorização de tráfego usando informação de Type of Service;        14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;        15. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;    66. FILTRO DE DADOS        1. Permitir a criação de filtros para arquivos e dados pré-definidos;        2. Os arquivos devem ser identificados por extensão e tipo;        3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);        4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;        5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;        6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;    67. GEO LOCALIZAÇÃO        1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;        2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;        3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;    68. VPN        1. Suportar VPN Site-to-Site e Cliente-To-Site;        2. Suportar IPSec VPN;        3. Suportar SSL VPN;        4. A VPN IPSEc deve suportar 3DES;        5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;        6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;        7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);        8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);        9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;        10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;        11. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;        12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;        13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;        14. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;        15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;        16. Atribuição de DNS nos clientes remotos de VPN;        17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;        18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;        19. Suportar leitura e verificação de CRL (certificate revocation list);        20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;        21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;        22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;        23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;        24. Deverá manter uma conexão segura com o portal durante a sessão;        25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior); | UND | 02 |
| 3 | 1. **SOLUÇÃO PARA ARMAZENAMENTO DE LOGS E RELATÓRIOS**    1. CARACTERÍSTICAS ESPECÍFICAS       1. Deve suportar receber logs de ao menos 10K dispositivos       2. Possuir capacidade de receber ao menos 25 GBytes de logs diários       3. Possuir ao menos 10 TB de espaço em disco       4. Possuir ao menos 4 interfaces de 1Gbps RJ-45    2. Requisitos Mínimos de Funcionalidade       1. Funcionalidades Gerais       2. Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.       3. Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);       4. Caso a solução seja virtualizada, deverá ser compatível com ambiente VMware ESXi 5.5/6.0/6.5/6.7 e 7.0;       5. Caso a solução seja virtualizada, deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e 2016;       6. Caso a solução seja virtualizada, deverá ser compatível com ambiente Citrix XenServer 6.0+       7. Caso a solução seja virtualizada, deverá ser compatível com ambiente Open Source Xen 4.1+       8. Caso a solução seja virtualizada, deverá ser compatível com ambiente KVM em Redhat 6.5+ e Ubuntu 17.04       9. Caso a solução seja virtualizada, deverá ser compatível com ambiente Nutanix AHV (AOS 5.10.5)       10. Caso a solução seja virtualizada, deverá ser compatível com ambiente Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) e Alibaba Cloud (AliCloud)       11. Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;       12. Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;       13. Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração       14. Suportar SNMP versão 2 e versão 3 na solução de relatórios       15. Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado       16. Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios       17. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet       18. Autenticação integrada a servidor Radius       19. Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela;       20. Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas;       21. Autenticação integrada ao Microsoft Active Directory       22. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações       23. Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos;       24. Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado       25. Possuir mecanismo para que logs antigos sejam removidos automaticamente       26. Permitir a importação e exportação de relatórios       27. Deve possuir a capacidade de criar relatórios nos formatos HTML       28. Deve possuir a capacidade de criar relatórios nos formatos PDF       29. Deve possuir a capacidade de criar relatórios nos formatos XML       30. Deve possuir a capacidade de criar relatórios nos formatos CSV       31. Deve ser possível exportar os logs em CSV       32. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração       33. Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar.       34. A solução deve possuir relatórios pré-definidos       35. Possuir envio automático de logs para um servidor FTP externo a solução       36. Possibilitar a duplicação de relatórios existentes e edita-los logo após       37. Possuir a capacidade de personalização de capas para os relatórios       38. Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log       39. Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.       40. Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios       41. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;       42. Dever ser possível fazer download dos arquivos de logs recebidos       43. Deve possuir agendamento para gerar e enviar automaticamente relatórios       44. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades.       45. Permitir o envio de maneira automática de relatórios por email       46. Deve permitir a escolha do email a ser enviado para cada relatório escolhido       47. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador       48. Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados       49. Deve ser possível definir filtros nos relatórios       50. Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros       51. Permitir que relatórios criado sejam no idioma Português       52. Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros       53. Deve permitir o envio automático de relatórios criado a um servidor de SFTP ou FTP externo a solução       54. Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios       55. Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros       56. Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado.       57. Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios       58. Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs       59. A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes       60. Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante       61. Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios       62. Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar       63. Deve permitir ver em tempo real os logs recebidos    3. Relatórios       1. Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;       2. Deve possuir um Indicador de Comprometimento (IoC), que mostre usuários finais com utilização web suspeita, devendo informar no mínimo: endereço ip do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça), número de ameaças detectadas.       3. Deve possuir relatório de PCI DSS Compliance       4. Deve possuir relatório de utilização de aplicações SAAS       5. Deve possuir relatório detalhado de prevenção de perda de dados (DLP)       6. Deve possuir relatório de VPN       7. Deve possuir relatório de Sistemas de prevenção de intrusão (IPS)       8. Deve possuir relatório de reputação do cliente       9. Deve possuir relatório de análise de segurança do usuário       10. Deve possuir relatório de avaliação da ameaça cibernética       11. Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada       12. Deve possuir relatório de análise aplicações web, se há uma plataforma de segurança web | UND | 01 |
| 4 | 1. **SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO PARA OS FIREWALLS NGFW**    1. Solução de Relatórios tipo 1 (1 unidades)       1. Deve permitir gerenciar ao menos 10 dispositivos       2. Deve suportar RAID       3. Possuir ao menos 4 interfaces de 1Gbps RJ-45       4. Possuir ao menos 0.1 TB de espaço em disco;    2. Requisitos Mínimos de Funcionalidade       1. Deve permitir e estar licenciado para operar em alta disponibilidade (HA) sincronizando as mudanças na base de dados entre as estações de gerência       2. Caso a solução seja virtualizada, deverá ser compatível com ambiente VMware ESXi 5.5/6.0/6.5/6.7 e 7.0;       3. Caso a solução seja virtualizada, deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e 2016;       4. Caso a solução seja virtualizada, deverá ser compatível com ambiente Citrix XenServer 6.0+       5. Caso a solução seja virtualizada, deverá ser compatível com ambiente Open Source Xen 4.1+       6. Caso a solução seja virtualizada, deverá ser compatível com ambiente KVM em Redhat 6.5+ e Ubuntu 17.04       7. Caso a solução seja virtualizada, deverá ser compatível com ambiente Nutanix AHV (AOS 5.10.5)       8. Caso a solução seja virtualizada, deverá ser compatível com ambiente Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) e Alibaba Cloud (AliCloud)       9. Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;       10. Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;       11. 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;       12. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;       13. Permitir acesso concorrente de administradores;       14. Possuir interface baseada em linha de comando para administração da solução de gerência       15. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;       16. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;       17. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;       18. Gerar alertas automáticos via Email       19. Gerar alertas automáticos via SNMP       20. Gerar alertas automáticos via Syslog       21. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora.       22. Deve ser permitido ao administrador transferir os backups para um servidor FTP.       23. Deve ser permitido ao administrador transferir os backups para um servidor SCP       24. Deve ser permitido ao administrador transferir os backups para um servidor SFTP       25. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante       26. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS       27. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS       28. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP       29. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS       30. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI)       31. Deve suportar sincronização do relógio interno via protocolo NTP.       32. Deve registrar as ações efetuadas por quaisquer usuários       33. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade.       34. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência       35. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet       36. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado       37. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização    3. Funcionalidades de APIs       1. Deve suportar XML API       2. Deve suportar JSON API    4. Funcionalidades de Gerência de UTM/NGFW       1. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;       2. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;       3. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;       4. Permitir localizar quais regras um objeto está sendo utilizado;       5. Deve atribuir sequencialmente um número a cada regra de firewall;       6. Deve atribuir sequencialmente um número a cada regra de DOS;       7. Permitir criação de regras que fiquem ativas em horário definido;       8. Permitir backup das configurações e rollback de configuração para a última configuração salva;       9. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);       10. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;       11. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência.       12. Cada servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall.       13. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.       14. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.       15. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.       16. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas elas somente sejam aplicadas após aprovação de outro administrador       17. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos       18. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando ele for adicionado à solução de gerência       19. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware.       20. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos       21. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração       22. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos       23. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência       24. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada       25. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos       26. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada       27. Permitir criar regras anti DoS de forma centralizada       28. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada       29. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia | UND | 01 |
| 5 | 1. **SOLUÇÃO PARA PONTO DE ACESSO TIPO I** **(FAP-231F)**    1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas em controlador wireless;    2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;    3. Deve identificar automaticamente o controlador wireless ao qual se conectará;    4. Deve permitir ser gerenciado remotamente através de links WAN;    5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;    6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;    7. O ponto de acesso deve possuir rádio Wi-Fi dedicado para executar funções de sensor com objetivo de identificar interferências e ameaças de segurança em tempo real e com operação 24x7;    8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;    9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;    10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;    11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;    12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;    13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;    14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;    15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;    16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;    17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;    18. Deve permitir operação em modo Mesh;    19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;    20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;    21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);    22. Deve suportar OFDMA;    23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;    24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;    25. Deve suportar BSS Coloring;    26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;    27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);    28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;    29. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;    30. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;    31. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;    32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;    33. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);    34. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;    35. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);    36. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;    37. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;    38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;    39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;    40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;    41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;    42. Deve implementar o padrão IEEE 802.11e;    43. Deve implementar o padrão IEEE 802.11h;    44. Deve implementar o padrão IEEE 802.3az;    45. Deve suportar ser gerenciado via SNMP;    46. Deve suportar consultas via REST API;    47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;    48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;    49. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;    50. Deve possuir indicadores luminosos (LED) para indicação de status;    51. Devido a necessidade de compatibilidade do ambiente legado, o ponto de acesso deverá ser gerenciado através de Firewall Fortigate;    52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;    53. Deve possuir certificado emitido pela Wi-Fi Alliance;    54. Deve estar homologado pela ANATEL na data de execução do pregão; | UND | 80 |
| 6 | 1. **SOLUÇÃO PARA PONTO DE ACESSO TIPO II (FAP-431F)**    1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas em controlador wireless;    2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;    3. Deve identificar automaticamente o controlador wireless ao qual se conectará;    4. Deve permitir ser gerenciado remotamente através de links WAN;    5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;    6. Deve suportar operação nas faixas de frequência de 2.4GHz e 5GHz;    7. O ponto de acesso deve ser tri-radio Wi-Fi, ou seja, deve possuir 3 (três) rádios capazes de operar simultaneamente, sendo 1(um) rádio dedicado para função de sensor Wi-Fi e outros 2 (dois) rádios operando para servir clientes em 2.4GHz e 5GHz;    8. O ponto de acesso deve possuir rádio Wi-Fi dedicado para executar funções de sensor com objetivo de identificar interferências e ameaças de segurança em tempo real e com operação 24x7;    9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;    10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;    11. Deve possuir 1 (uma) interface Ethernet padrão 10/100/1000/2500Base-T com conector RJ-45 para permitir a conexão com a rede LAN;    12. Adicionalmente, deve possuir 1 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir alta disponibilidade em caso de falha da interface primária;    13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at em ambas interfaces ethernet. Adicionalmente deve possuir entrada de alimentação 12VDC;    14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;    15. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;    16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;    17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;    18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;    19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;    20. Deve permitir operação em modo Mesh;    21. Deve possuir potência de irradiação mínima de 20dBm em cada rádio do ponto de acesso;    22. Deve suportar, no mínimo, operação MIMO 4x4 com 4 fluxos espaciais nos rádios que operam em 2.4 e 5GHz servindo clientes wireless;    23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);    24. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);    25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;    26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;    27. Deve suportar BSS Coloring;    28. Deve permitir operação em 5GHz com canais de 20, 40, 80MHz;    29. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);    30. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5dBi em 5GHz;    31. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;    32. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;    33. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;    34. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;    35. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);    36. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 12 (doze) SSIDs com operação simultânea;    37. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);    38. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;    39. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;    40. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-TLS, EAP-TTLS e PEAP;    41. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;    42. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;    43. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;    44. Deve implementar o padrão IEEE 802.11e;    45. Deve implementar o padrão IEEE 802.11h;    46. Deve implementar o padrão IEEE 802.3az;    47. Deve suportar ser gerenciado via SNMP;    48. Deve suportar consultas via REST API;    49. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;    50. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;    51. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;    52. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces ethernet, status dos rádios e status de atividade;    53. Devido a necessidade de compatibilidade do ambiente legado, o ponto de acesso deverá ser gerenciado através de Firewall Fortigate;    54. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;    55. Deve possuir certificado emitido pela Wi-Fi Alliance;    56. Deve estar homologado pela ANATEL na data de execução do pregão; | UND | 20 |
| 7 | 1. **SOLUÇÃO PARA PONTO DE ACESSO OUTDOOR**    1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas em controlador wireless;    2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;    3. Deve identificar automaticamente o controlador wireless ao qual se conectará;    4. Deve permitir ser gerenciado remotamente através de links WAN;    5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;    6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;    7. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;    8. Deve possuir 2 (duas) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;    9. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;    10. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;    11. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;    12. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;    13. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;    14. Deve permitir operação em modo Mesh;    15. Deve possuir potência de irradiação mínima de 24dBm em cada rádio;    16. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 867 Mbps em um único rádio;    17. Deve suportar MU-MIMO;    18. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;    19. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);    20. Deve possuir antenas externas ao equipamento com ganho mínimo de 10dBi em 2.4GHz e 10dBi em 5GHz;    21. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;    22. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;    23. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;    24. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;    25. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);    26. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea;    27. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);    28. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;    29. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;    30. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;    31. Deve suportar a técnica de Transmit Beam-Forming (TxBF);    32. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;    33. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;    34. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;    35. Deve implementar o padrão IEEE 802.11e;    36. Deve implementar o padrão IEEE 802.11h;    37. Deve suportar ser gerenciado via SNMP;    38. Deve suportar consultas via REST API;    39. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes;    40. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 65º C;    41. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcançem este grau de proteção;    42. Deve possuir indicadores luminosos (LED) para indicação de status;    43. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;    44. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;    45. Deve possuir certificado emitido pela Wi-Fi Alliance;    46. Deve estar homologado pela ANATEL na data de execução do pregão; | UND | 30 |
| 8 | 1. SERVIÇO DE SUPORTE FORTIGATE 200D E ATUALIZAÇÕES DE SUBSCRIÇÃO    1. Serviço de suporte 24x7 para 02 (DOIS) firewalls FORTIGATE 200D e atualizações de subscrição Serial Number **FG1K5D3I14800585 E FG1K5D3I14802407** com licenciamento Unified Threat Protection (UTP) **Coterm End Date:2022-12-31** | UND | 02 |
| 9 | 1. SERVIÇO DE SUPORTE FORTIGATE 200D E ATUALIZAÇÕES DE SUBSCRIÇÃO    1. Serviço de suporte 24x7 para 01 (UM) firewalls FORTIGATE 200D e atualizações de subscrição -  Serial Number **FG200D3913804933** com licenciamento Unified Threat Protection (UTP) **Coterm End Date:2022-12-31** | UND | 02 |
| 10 | 1. SERVIÇO DE SUPORTE FORTIGATE 300D E ATUALIZAÇÕES DE SUBSCRIÇÃO    1. Serviço de suporte 24x7 para 02 (dois) firewall FORTIGATE 300D e atualizações de subscrição  Serial Number: **FGT3HD3917804104 E FGT3HD3917804029** e com licenciamento Unified Threat Protection (UTP)  **Coterm End Date:2022-12-31** | UND | 02 |
| 11 | 11.1. Serviços de implantação, suporte, operação assistida e documentação - Os serviços previstos estão na tabela abaixo:  **11.1.1. Instalação e Execução**  **11.1.1.1 Atividades da Pré-instalação**  Para os entregáveis dessa fase estamos contemplando alguns serviços que foram estruturados com as seguintes atividades:   * Planejamento e Levantamento de requisitos   + Conduzir reuniões para fazer o levantamento dos dados para:     - Descrever a metodologia de avaliação e demonstrar o objetivo da atividade.     - Definir os processos operacionais de coleta de dados.     - Fornecer recomendações iniciais e parâmetros operacionais para a coleta de dados.   + Ajudar a gerar documentos, se necessário, pertinentes ao projeto como Matriz RACI, Cronograma e demais documentos para o modelo de Controle, Administração e Monitoramento do projeto. * Desenvolvimento do Plano de Migração e Instalação, Laboratórios e Staging   + Informações sobre a infraestrutura vigente como enlaces UTP e Fibras utilizadas que serão pertinentes ao processo de implantação.   + Ajudar a gerar os documentos com o desenho lógico detalhado da solução de segurança Fortinet e seus componentes (topologia, definições de configuração, protocolos a serem utilizados na solução, etc).   + Descrever configurações especiais e considerações sobre personalização para os equipamentos descritos no desenho lógico.   + Trabalhar em conjunto para a criação do:     - Plano de migração e melhoria das regars existentes no NGFW atual;     - Análise das informações dos serviços internos no cliente;     - Criação dos modelos de configuração em conjunto da Fortinet do ambiente de projeto e simulação em Laboratório na fase de Staging;     - Definir e Aplicar toda e qualquer configuração da fase de Staging nos equipamentos que fazem parte do escopo desta proposta.     - Com isso, a CONTATADA está dimensionando um período adequado para laboratórios e simulações para que seja definido todo o ambiente para posterior criação dos planos, geração de scripts, baselines entre outros.     - Criação dos documentos de plano de instalação, migração e testes em conjunto da CONTRATANTE;   + Criação dos Documentos de instalação inicial e final Técnica da CONTATADA para o projeto. * Desenvolvimento de Documentos PPI - Projeto Provisório de Instalação e PFI - Projeto Final de Instalação (AS-BUILT)   + Gerar o Projeto Executivo com os scripts de configurações de melhores práticas a serem aplicadas de acordo com o desenho lógico detalhado para cada modelo de equipamento ofertado.   **11.1.1.2. Instalação física dos equipamentos**   * Desembalagem dos equipamentos; * Fixação em rack de 19” caso o equipamento suporte tal fixação * Ligação em rede elétrica, que deverá estar disponível dentro do rack de equipamentos, ou em parede e/ou outra superfície que suporte fixação no caso específico; * Conexão de cabos da parte lógica (RJ-45 e/ou fibra óptica) nos respectivos equipamentos.   **Obs.:**   * + - 1. **Os cabos da parte lógica serão conectados aos equipamentos (ponto de rede ao equipamento) desde que, devidamente organizados em rack e conectorizados em ambas extremidades. Não será responsabilidade da Contatada tais organizações e/ou conectorizações de cabos, assim como, o seu fornecimento.**       2. **Não está contemplado nesta proposta, o fornecimento de materiais e serviços para nenhum tipo de infraestrutura. Toda e qualquer necessidade para instalação dos equipamentos será de responsabilidade da CONTRATANTE.**   **11.1.1.3. Configuração Lógica inicial**  A configuração da solução ofertada, inclui dois *appliances* físicos instalados em uma mesma localidade e terão a configuração migrada dos firewalls Fortigate em produção que podem incluir:   * Segmentação atual da rede; * Perímetro Internet; * Políticas e regras de segurança atuais; * Zonas de segurança; * Objetos de firewall; * Políticas e regras de prevenção e detecção de intrusos; * Usuários privilegiados para operação e administração; * Aplicação de licença adquirida; * Configuração de NAT/PAT, DNS, endereçamento IP e roteamento estático existente; * Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP e/ou SMS; * Integração com a ferramenta de correlação de eventos, caso exista, para coleta, monitoramento e correlação de registros de segurança da informação; * Integração com ferramenta de monitoramento via SNMP, caso exista; * Configuração de VPNs IPsec site-to-site; * Configuração dos Firewalls em Cluster no modo ativo-passivo; * Documentação AS-BUILT, contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados; * Migração da solução atual para nova solução; * Operação assistida por 16 horas; * Passagem de conhecimento das principas mudanças em relação as versões do FortiOS da versão anterior e da versão atual.   OBS: Equipamentos, softwares e políticas que não estejam relacionados no documento (exemplo: política de senhas, appliances, relatórios), não estão cobertos pelo serviço e estarão sujeitos a uma nova proposta;  **11.1.1.4. Suporte Técnico**  O Suporte Técnico é definido como as atividades de auxílio, reparo, reconfiguração e disponibilização de atualizações corretivas de software e restauração em caso de indisponibilidade, para restabelecer o funcionamento normal dos serviços contratados pelo Cliente.  O atendimento começa remoto e em último caso o técnico vai localmente. O Suporte não se refere a serviços de operações como por exemplo: adição ou exclusão de regras.  O Suporte em cenários de RMA incluem a reinstalação do equipamento defeituoso assim que disponível no cliente atráves do processo pela Contratante e a Fortinet e atuará no modelo 24x7. | UST | 800 |