Apêndice

1. **DESCRITIVO TÉCNICO DOS PRODUTOS**
    1. **REQUISITOS ESPECÍFICOS – ITEM 1 – FIREWALL DE BORDA TIPO 1 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
        a. Deve suportar, no mínimo, 155 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes
        b. Deve suportar, no mínimo, 24.5 Gbps de throughput IPS
        c. Deve suportar, no mínimo, 54 Gbps de throughput de VPN IPSec
        d. Deve suportar, no mínimo, 9 Gbps de throughput de VPN SSL
        e. Deve suportar, no mínimo, 16 Gbps de throughput de Inspeção SSL
        f. Deve suportar, no mínimo, 72 Gbps de throughput de Controle de Aplicação
        g. Deve suportar, no mínimo, 19 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.
        h. Suporte a, no mínimo, 15 milhões de conexões simultâneas;
        i. Deve suportar o gerenciamento de no mínimo 500 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 1000 em modo “Bridge”, com saída local na unidade;
        j. Deve suportar o gerenciamento de no mínimo 75 Switches do mesmo fabricante por equipamento;
        k. Suporte a, no mínimo, 690 mil novas conexões por segundo
        l. Estar licenciado para, ou suportar sem o uso de licença, 1800 túneis de VPN IPSEC Site-to-Site simultâneos
        m. Estar licenciado para, ou suportar sem o uso de licença, 45.000 túneis de clientes VPN IPSEC simultâneos
        n. Estar licenciado para, ou suportar sem o uso de licença, 9.000 clientes de VPN SSL simultâneos
        o. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
        p. Possuir ao menos 14 interfaces 1Gbps RJ-45
        q. Possuir ao menos 8 interfaces 1Gbps SFP
        r. Possuir ao menos 2 interfaces SFP+ 10 Gigabit
        s. Possuir ao menos 4 interfaces SFP28 25 Gigabit
        t. Deverá possuir interface USB 3.0 para exportação de backups;
        u. Deverá possuir interface do tipo console para utilização de CLI
        v. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
        w. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
        x. Possuir no máximo 1 RU de altura
        y. Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;

    2. **REQUISITOS ESPECÍFICOS – ITEM 2 – FIREWALL DE BORDA TIPO 2 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
        a. Deve suportar, no mínimo, 132 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes
        b. Deve suportar, no mínimo, 13.2 Gbps de throughput IPS
        c. Deve suportar, no mínimo, 54 Gbps de throughput de VPN IPSec

d. Deve suportar, no mínimo, 4 Gbps de throughput de VPN SSL
e. Deve suportar, no mínimo, 8.5 Gbps de throughput de Inspeção SSL
f. Deve suportar, no mínimo, 30 Gbps de throughput de Controle de Aplicação
g. Deve suportar, no mínimo, 10 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.
h. Suporte a, no mínimo, 8 milhões de conexões simultâneas;
i. Deve suportar o gerenciamento de no mínimo 500 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 1000 em modo "Bridge", com saída local na unidade;
j. Deve suportar o gerenciamento de no mínimo 80 Switches do mesmo fabricante por equipamento;
k. Suporte a, no mínimo, 500 mil novas conexões por segundo
l. Estar licenciado para, ou suportar sem o uso de licença, 1.600 túneis de VPN IPSEC Site-to-Site simultâneos
m. Estar licenciado para, ou suportar sem o uso de licença, 40.000 túneis de clientes VPN IPSEC simultâneos
n. Estar licenciado para, ou suportar sem o uso de licença, 7.500 clientes de VPN SSL simultâneos
o. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
p. Possuir ao menos 14 interfaces 1Gbps RJ-45
q. Possuir ao menos 6 interfaces 1Gbps SFP
r. Possuir ao menos 4 interfaces 25Gbps SFP28
s. Possuir ao menos 4 interfaces 10Gbps SFP+
t. Deverá possuir interface USB 3.0 para exportação de backups;
u. Deverá possuir interface do tipo console para utilização de CLI
v. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
w. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
x. Possuir no máximo 1 RU de altura
y. Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;

3. **REQUISITOS ESPECÍFICOS – ITEM 3 – FIREWALL DE BORDA TIPO 3 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
   a. Deve suportar, no mínimo, 76 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes
   b. Deve suportar, no mínimo, 11 Gbps de throughput IPS
   c. Deve suportar, no mínimo, 50 Gbps de throughput de VPN IPSec
   d. Deve suportar, no mínimo, 3 Gbps de throughput de VPN SSL
   e. Deve suportar, no mínimo, 8 Gbps de throughput de Inspeção SSL
   f. Deve suportar, no mínimo, 26 Gbps de throughput de Controle de Aplicação
   g. Deve suportar, no mínimo, 8 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.
   h. Suporte a, no mínimo, 7 milhões de conexões simultâneas;
   i. Deve suportar o gerenciamento de no mínimo 250 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 500 em modo "Bridge", com saída local na unidade;
   j. Deve suportar o gerenciamento de no mínimo 60 Switches do mesmo fabricante por equipamento;
   k. Suporte a, no mínimo, 450 mil novas conexões por segundo
   l. Estar licenciado para, ou suportar sem o uso de licença, 1.500 túneis de VPN IPSEC Site-to-Site simultâneos
   m. Estar licenciado para, ou suportar sem o uso de licença, 35.000 túneis de clientes VPN IPSEC simultâneos
   n. Estar licenciado para, ou suportar sem o uso de licença, 3.000 clientes de VPN SSL simultâneos

o. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
p. Possuir ao menos 15 interfaces 1Gbps RJ-45
q. Possuir ao menos 6 interfaces 1Gbps SFP
r. Possuir ao menos 8 interfaces 10Gbps SFP+
s. Deverá possuir interface USB 3.0 para exportação de backups;
t. Deverá possuir interface do tipo console para utilização de CLI
u. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
v. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
w. Possuir no máximo 1 RU de altura
x. Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;

4. **REQUISITOS ESPECÍFICOS – ITEM 4 – FIREWALL DE BORDA TIPO 4 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
   a. Deve suportar, no mínimo, 36 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes
   b. Deve suportar, no mínimo, 5 Gbps de throughput IPS
   c. Deve suportar, no mínimo, 32 Gbps de throughput de VPN IPSec
   d. Deve suportar, no mínimo, 1.2 Gbps de throughput de VPN SSL
   e. Deve suportar, no mínimo, 3 Gbps de throughput de Inspeção SSL
   f. Deve suportar, no mínimo, 6 Gbps de throughput de Controle de Aplicação
   g. Deve suportar, no mínimo, 2.5 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.
   h. Suporte a, no mínimo, 3 milhões de conexões simultâneas;
   i. Deve suportar o gerenciamento de no mínimo 50 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 100 em modo “Bridge”, com saída local na unidade;
   j. Deve suportar o gerenciamento de no mínimo 30 Switches do mesmo fabricante por equipamento;
   k. Suporte a, no mínimo, 120 mil novas conexões por segundo
   l. Estar licenciado para, ou suportar sem o uso de licença, 1.500 túneis de VPN IPSEC Site-to-Site simultâneos
   m. Estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de clientes VPN IPSEC simultâneos
   n. Estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos
   o. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
   p. Possuir ao menos 16 interfaces 1Gbps RJ-45
   q. Possuir ao menos 6 interfaces 1Gbps SFP
   r. Possuir ao menos 4 interfaces 10Gbps SFP+
   s. Deverá possuir interface USB 3.0 para exportação de backups;
   t. Deverá possuir interface do tipo console para utilização de CLI
   u. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
   v. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
   w. Possuir no máximo 1 RU de altura
   x. Deverá ser fornecido com fonte de alimentação interna redundante;

5. **REQUISITOS EM COMUM PARA OS ITENS 1, 2, 3, 4 E 5**
   a. O Firewall deverá suportar e estar licenciado para o uso das diversas ferramentas de segurança incluídas em um Next Generation Firewall, como Antivírus, IPS, Filtragem Web, Controle de Aplicações, Proteção contra Botnets, Proteção contra Malwares Avançados e Antispam de Gateway.
   b. O projeto deverá contemplar serviço de instalação, configuração e treinamento de toda a

solução;

c. Todas as soluções deverão ser fornecidas com 36 meses de garantia pelos fabricantes, na modalidade NBD (Next Business Day);
d. O fabricante ofertado deve estar posicionado no quadrante “Leader” do quadrante mágico do Gartner de 2023 ou mais recente, na categoria Network Firewalls;
e. CARACTERÍSTICAS GERAIS DE FUNCIONALIDADES
    1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
    2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
    3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
    4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
    5. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de protecção da rede;
    6. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
    7. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
    8. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
    9. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
    10. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
    11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
    12. Os dispositivos de proteção de rede devem suportar sFlow;
    13. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
    14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
    15. Deve suportar NAT dinâmico (Many-to-1);
    16. Deve suportar NAT dinâmico (Many-to-Many);
    17. Deve suportar NAT estático (1-to-1);
    18. Deve suportar NAT estático (Many-to-Many);
    19. Deve suportar NAT estático bidirecional 1-to-1;
    20. Deve suportar Tradução de porta (PAT);
    21. Deve suportar NAT de Origem;
    22. Deve suportar NAT de Destino;
    23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
    24. Deve poder combinar NAT de origem e NAT de destino na mesma política
    25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
    26. Deve suportar NAT64 e NAT46;
    27. Deve implementar o protocolo ECMP;
    28. 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;
    29. Enviar log para sistemas de monitoração externos, simultaneamente;
    30. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
    31. Proteção anti-spoofing;
    32. Suportar otimização do tráfego entre dois equipamentos;
    33. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
    34. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
    35. Suportar OSPF graceful restart;

36. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
37. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
38. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
39. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
40. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
41. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
42. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
43. A configuração em alta disponibilidade deve sincronizar: Sessões;
44. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
45. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
46. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
47. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
48. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
49. 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;
50. 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;
51. 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 interfaces;
52. 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);
53. O console de administração deve suportar pelo menos inglês, espanhol e português.
54. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas.
55. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

f. FUNCIONALIDADES DE CONTROLE POR POLÍTICAS
    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. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.
    8. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o

formato Common Event Format (CEF);

9. Deve suportar o protocolo padrão da indústria VXLAN;
10. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
11. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução
12. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email e firewall de aplicativos da Web.

g. FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3. 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;
4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
5. 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;
6. Identificar o uso de táticas evasivas via comunicações criptografadas;
7. Atualizar a base de assinaturas de aplicações automaticamente;
8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
9. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
11. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
14. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
15. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
18. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente

h. FUNCIONALIDADES DE 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 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;
6. Deve permitir o bloqueio de vulnerabilidades;
7. Deve incluir proteção contra ataques de negação de serviços;
8. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
9. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
10. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
11. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;
12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;
13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
14. Detectar e bloquear a origem de portscans;
15. Bloquear ataques efetuados por worms conhecidos;
16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
17. Possuir assinaturas para bloqueio de ataques de buffer overflow;
18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
19. Identificar e bloquear comunicação com botnets;
20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
21. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
23. Os eventos devem identificar o país de onde partiu a ameaça;
24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
27. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;

i. FUNCIONALIDADES DE 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 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;
3. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
5. Possuir pelo menos 60 categorias de URLs;
6. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
7. Permitir a customização de página de bloqueio;
8. 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);
9. Além do Explicit Web Proxy, suportar proxy Web transparente;

j. FUNCIONALIDADES DE 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/políticas baseadas em usuários e grupos de usuários;
3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

k. FUNCIONALIDADES DE 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 marcação de pacotes Diffserv, inclusive por aplicação;
11. Suportar modificação de valores DSCP para o Diffserv;
12. Suportar priorização de tráfego usando informação de Type of Service;
13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

l. FUNCIONALIDADES DE 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;

m. FUNCIONALIDADES DE ZTNA
   1. A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:
      1. Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:
         1. Informação pessoal do sistema operacional;
         2. LinkedIn;
         3. Google;
         4. SalesForce;
      2. Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:
         1. DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DCHP específico
         2. DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico
         3. Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento
         4. Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico
         5. Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway.
         6. Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede
         7. VPN Tunnel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Tunel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil
      3. Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso;

n. 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;

o. FUNCIONALIDADES DE 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 Autenticação MD5 e SHA-1;
   5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
   6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
   7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
   8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
   9. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
   10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
   11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
   12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
   13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
   14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
   15. Deverá manter uma conexão segura com o portal durante a sessão;
   16. 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);
   17. Deve suportar Auto-Discovery Virtual Private Network (ADVPN)
   18. Deve suportar agregação de túneis IPSec
   19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec
   20. A VPN IPSec deve suportar Forward Error Correction (FEC)
   21. Deve suportar TLS 1.3 em VPN SSL

p. FUNCIONALIDADES DE SD-WAN
   1. Deve implementar balanceamento de link por hash do IP de origem;
   2. Deve implementar balanceamento de link por hash do IP de origem e destino;
   3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
   4. Deve implementar balanceamento de link por custo configurado do link.
   5. Deve suportar o balanceamento de, no mínimo, 256 links;
   6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec
   7. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
   8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde
   9. Deve suportar Zero-Touch Provisioning
   10. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes
   11. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado
   12. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.
   13. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS

14. Suportar UDP Hole Punching em arquitetura ADVPN
15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado
16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.
17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN
18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link

q. FUNCIONALIDADES DE WIRELESS CONTROLLER

1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;
9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
10. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não

autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
25. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
26. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
27. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
28. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
29. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
30. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
31. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
32. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
33. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e

resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

34. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
35. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
36. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
37. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
38. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
39. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
40. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;
41. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de Inspeção SSL que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;
42. A base de reconhecimento de aplicações através de Inspeção SSL deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;
43. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de Inspeção SSL;
44. A solução deve ainda, através da técnica de Inspeção SSL, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
45. "A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
46. - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
47. - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
48. - ASLEAP;
49. - Null Probe Response / Null SSID Probe Response;
50. - Long Duration;
51. - Ataques contra Wireless Bridges;
52. - Weak WEP;
53. - Invalid MAC OUI."
54. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
55. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
56. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
57. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;

58. Deve implementar autenticação administrativa através do protocolo RADIUS;
59. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
60. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
61. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
62. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
63. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
64. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
65. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
66. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
67. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
68. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
69. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
70. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
71. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
72. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
73. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
74. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
75. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
76. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
77. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
78. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
79. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
80. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
81. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
82. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de

emitir notificações através da geração de traps;

83. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
84. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet -like MIB);
85. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato. pcap;
86. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
87. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
88. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
89. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
90. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
91. A solução deve possuir ferramentas de diagnósticos e debug;
92. A solução deve suportar comunicação com elementos externos através de APIs;
93. A solução deverá ser compatível e gerenciar pontos de acesso e switches do mesmo fabricante;
94. Os serviços de instalação deverão contemplar:
    1. Consultoria para diagramação e arquitetura de rede, de forma que seja sugerida a melhor topologia de acordo com as boas práticas de mercado;
    2. Instalação física dos Firewalls;
    3. Migração das configurações atuais, quando houver;
    4. Configuração de Alta Disponibilidade nos Firewalls e integração com a rede atual;
    5. Ativação de recursos no Firewall, como:
        1. Antivírus
        2. WebFilter
        3. Application Control
        4. DNS Filter
        5. SSL Inspection para navegação web
        6. SSL Inspection para servidores publicados
        7. IPS
    6. Configurações de redes e rotas para os dispositivos de rede;
    7. Configurações de autenticação e integração com o Active Directory do ÓRGÃO LICITANTE;
    8. Integração dos Switches com os Firewalls Concentradores para gestão centralizada;
    9. Configuração de domínios de Spanning Tree e Root Bridge;
    10. Configuração de VLANs;
    11. Treinamento completo de uso da solução para 6 alunos, de forma teórica e hands-on de no mínimo 12 horas, distribuído em três dias;
        1. O treinamento deve conter ementa referente à utilização das soluções de Firewall, Relatoria e logs, e Gerenciamento centralizado, a ser fornecida neste certame;
    12. O treinamento deverá ser realizado por técnico certificado pelo fabricante, o certificado deverá ser anexado nas documentações de habilitação do ÓRGÃO LICITANTE;
    13. O ÓRGÃO LICITANTE será responsável por prover o espaço para realização do treinamento.

6. **SOLUÇÃO DE RELATORIA E CENTRALIZAÇÃO DE LOGS**

a. A solução deve ser baseada em máquina virtual do mesmo fabricante da solução de NGFW e SD-WAN e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração;
b. Poderá ser entregue em formato appliance virtual, a ser instalado no ambiente de VMs da IFSul;
c. Deverá estar devidamente licenciada para suportar a coleta de, no mínimo, 25 GB de logs diários;
d. Caso a solução seja entregue como appliance virtual, este deve suportar:
    1. Deve ser compatível com os hypervisor VMWare ESXi, Hyper-V e KVM;
    2. Não deverá existir limite para o número de vCPUs no appliance virtual;
    3. Não deverá existir limite para a expansão da memória RAM no appliance virtual;
    4. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
    5. 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;
    6. Realizar o backup das configurações para permitir o retorno de uma configuração salva;
    7. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
    8. Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
    9. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
    10. Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
    11. Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
    12. Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
    13. Deve oferece um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;
    14. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
    15. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
    16. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
    17. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
    18. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
    19. Deve possuir mecanismos de remoção automática para logs antigos;
    20. Permitir importação e exportação de relatórios
    21. Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
    22. Deve permitir exportar os logs no formato CSV;
    23. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
    24. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
    25. A solução deve ter relatórios predefinidos;
    26. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
    27. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

28. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
29. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
30. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
31. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
32. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
33. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
34. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
35. Permitir o envio por e-mail relatórios automaticamente;
36. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
37. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
38. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
39. Deve permitir o uso de filtros nos relatórios;
40. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
41. Permitir especificar o idioma dos relatórios criados;
42. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
43. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
44. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
45. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
46. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
47. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
48. Deve permitir visualizar em tempo real os logs recebidos;
49. Deve permitir o encaminhamento de log no formato syslog;
50. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
51. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
52. Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;
53.
54. Deve permitir gerar alertas de eventos a partir de logs recebidos;
55. Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo período mínimo de 36 meses;
56. Os serviços de instalação deverão contemplar:
    1. Implementação da solução em máquina virtual fornecida pelo ÓRGÃO LICITANTE;
    2. Integração com a solução de firewall deste certame para envio de logs à solução;
    3. Configuração de servidor SMTP para disparo de alertas e relatórios;
    4. Criação de 2 relatórios personalizados de acordo com as necessidades de cada câmpus da IFSul, visando recebimento recorrente de informações que apoiem a tomada de decisão dos campi;
    5. Criação de thresholds de alerta;
    6. Separação da visibilidade de logs em domínios administrativos por campus;
    7. Repasse de conhecimento;

7. **SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO**
    a. Deve ser do tipo appliance virtual (VM), a ser instalado em ambiente disponibilizado pelo IFSul;
    b. Deve estar licenciado para gerenciar no mínimo 20 dispositivos não sendo necessário licenciar ambos os equipamentos em caso de Cluster HA. Caso seja necessário licenciar gestão para os 2 equipamentos do cluster, deverão ser fornecidas licenças para gestão de 40 dispositivos.
    c. Deverá suportar sua implementação em:
        1. VMware ESXi 6.0+;
        2. Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;
        3. Citrix XenServer 6.0+ e Open Source Xen 4.1+
        4. KVM
        5. Nutanix AHV
        6. Amazon Web Services (AWS)
        7. Microsoft Azure.
        8. Google Cloud (GPC)
        9. Oracle Cloud Infrastructure (OCI)
    d. Não deve possuir limite na quantidade de múltiplas vCPU
    e. Não deve possuir limite para suporte a expansão de memória RAM
    f. Deve suportar alta disponibilidade
    g. Funcionalidades gerais:
        1. Deve ter a capacidade de permitir o provisionamento e o monitoramento da configuração SD-WAN de todos os dispositivos gerenciados a partir de um único console.
        2. Como parte da visibilidade SD-WAN dos dispositivos gerenciados centralmente, a solução deve ter visibilidade do status do link, desempenho do aplicativo, utilização da largura de banda e conformidade com o SLA objetivo.
        3. Deve ter a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em um único console
        4. A solução deve ter o recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zerotouch para o rápido provisionamento em massa.
        5. A solução deve poder executar backups de configuração automáticos em até 5 nós, contendo atualizações de todos os dispositivos gerenciados.
        6. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de um único console e exibir sua localização geográfica em um mapa.
        7. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança.
        8. Permitir a integração de trocas e compartilhamento de dados com terceiros por meio do pxGrid, OCI, ESXi.
        9. 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;
        10. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
        11. Permitir acesso concorrente de administradores;
        12. Possuir interface baseada em linha de comando para administração da solução de gerência
        13. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
        14. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
        15. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
        16. Gerar alertas automáticos via Email
        17. Gerar alertas automáticos via SNMP
        18. Gerar alertas automáticos via Syslog

19. 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.
20. Deve ser permitido ao administrador transferir os backups para um servidor FTP.
21. Deve ser permitido ao administrador transferir os backups para um servidor SCP
22. Deve ser permitido ao administrador transferir os backups para um servidor SFTP
23. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante
24. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS
25. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS
26. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP
27. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS
28. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI)
29. Deve suportar sincronização do relógio interno via protocolo NTP.
30. Deve registrar as ações efetuadas por quaisquer usuários
31. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade.
32. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência
33. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet
34. 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
35. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização

h. Funcionalidades de gestão de firewalls:
i. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
j. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
k. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
l. Permitir localizar quais regras um objeto está sendo utilizado;
m. Permitir criação de regras que fiquem ativas em horário definido;
n. A solução deve permitir o repositório de assinaturas de antivírus, IPS, filtragem da Web e filtragem de email para otimizar a velocidade e o download centralizado de dispositivos gerenciados
o. Deve ter a capacidade de exibir os resultados da auditoria de segurança dos dispositivos gerenciados
p. Permitir backup das configurações e rollback de configuração para a última configuração salva;
q. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
r. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
s. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência.
t. 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.
u. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de

novas versões de software dos appliances.

v. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.
w. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador
x. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos
    1. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência
    2. 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.
    3. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos
    4. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração
    5. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos
    6. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência
    7. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada
    8. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos
    9. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada
    10. Permitir criar regras anti DoS de forma centralizada
    11. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada
    12. 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
    13. Deve permitir o uso de DDNS em VPNs de forma centralizada
    14. Deve permitir o gerenciamento de pontos de acesso proprietários de forma centralizada
    15. Deve permitir o gerenciamento centralizado de switches proprietários
    16. Deve permitir o gerenciamento centralizado de perfis de segurança de software de endpoint proprietários
    17. Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo período mínimo de 36 meses;
    18. Os serviços de instalação deverão contemplar:
        1. Implementação da solução em máquina virtual fornecida pelo ÓRGÃO LICITANTE;
        2. Integração com a solução de firewall deste certame para sua gerência centralizada através da solução;
        3. Separação da visibilidade através domínios administrativos, permitindo que cada unidade possua visibilidade apenas às informações e gerência do seu câmpus, e a reitoria possua acesso à configuração e gerência de todos os campi;
        4. Criação de templates de configuração para aplicação automática de políticas em determinados campi;
        5. Repasse de conhecimento;

Documento assinado eletronicamente por:

- **Carla Simone Guedes Pires, DIRETOR(A) - CD3 - IF-DTI**, em 23/07/2024 10:52:41.

Este documento foi emitido pelo SUAP em 23/07/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsul.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 293317
Código de Autenticação: 4b1dd3edf3