5.5.53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
5.5.54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
5.5.55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
5.5.56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
5.5.57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;
5.5.58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
5.5.59. Deverá suportar ser configurado e monitorado através de REST API;
5.5.60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
5.5.61. Deve suportar temperatura de operação de até 45º Celsius;
5.5.62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
5.5.63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
5.5.64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
5.6. Solução de Gerenciamento e Segurança Avançada | ITEM 6
5.6.1. Características do Equipamento
5.6.1.1. Deve suportar, no mínimo, 36 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6
5.6.1.2. Deve suportar, no mínimo, 10 Gbps de throughput IPS
5.6.1.3. Deve suportar, no mínimo, 20 Gbps de throughput de VPN IPSec
5.6.1.4. Deve suportar, no mínimo, 7 Gbps de throughput de VPN SSL
5.6.1.5. Deve suportar, no mínimo, 8 Gbps de throughput de Inspeção SSL
5.6.1.6. Deve suportar, no mínimo, 15 Gbps de throughput de Controle de Aplicação
5.6.1.7. Deve suportar, no mínimo, 9.5 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.
5.6.1.8. Suporte a, no mínimo, 8 milhões de conexões simultâneas
5.6.1.9. Suporte a, no mínimo, 450.000 novas conexões por segundo
5.6.1.10. Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos
5.6.1.11. Estar licenciado para, ou suportar sem o uso de licença, 50.000 túneis de clientes VPN IPSEC simultâneos
5.6.1.12. Estar licenciado para, ou suportar sem o uso de licença, 10.000 clientes de VPN SSL simultâneos
5.6.1.13. Permitir gerenciar ao menos 1024 Access Points
5.6.1.14. Possuir ao menos 8 interfaces 1Gbps RJ45
5.6.1.15. Possuir ao menos 8 interfaces 1Gbps SFP, devendo ser entregue pelo menos dois transceivers padrão SX
5.6.1.16. Possuir ao menos 2 interfaces 1Gbps RJ45 dedicadas à gerenciamento
5.6.1.17. Possuir ao menos 2 interfaces 10Gbps SFP+, devendo ser entregue pelo menos dois transceivers 10GBASE-SR SFP+ e dois transceivers 10GBASE-SR XFP
5.6.1.18. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
5.6.1.19. Deve possuir disco local do tipo SSD de, no mínimo, 200Gb.
5.6.1.20. Possuir fonte de alimentação 100-240V AC redundante Hot Swappable
5.6.1.21. Possuir no máximo 1 RU de altura
5.6.1.22. Deve ser do mesmo fabricante das soluções dos itens 1, 2 e 3
5.6.2. Requisitos Mínimos de Funcionalidade
5.6.2.1. 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;
5.6.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
5.6.2.3. 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;
5.6.2.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5.6.2.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
5.6.2.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
5.6.2.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
5.6.2.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
5.6.2.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
5.6.2.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM- DM);
5.6.2.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
5.6.2.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
5.6.2.13. Os dispositivos de proteção de rede devem suportar sFlow;
5.6.2.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
5.6.2.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
5.6.2.16. Deve suportar NAT dinâmico (Many-to-1);
5.6.2.17. Deve suportar NAT dinâmico (Many-to-Many);
5.6.2.18. Deve suportar NAT estático (1-to-1);
5.6.2.19. Deve suportar NAT estático (Many-to-Many);
5.6.2.20. Deve suportar NAT estático bidirecional 1-to-1;
5.6.2.21. Deve suportar Tradução de porta (PAT);
5.6.2.22. Deve suportar NAT de Origem;
5.6.2.23. Deve suportar NAT de Destino;
5.6.2.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
5.6.2.25. Deve poder combinar NAT de origem e NAT de destino na mesma politica
5.6.2.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
5.6.2.27. Deve suportar NAT64 e NAT46;
5.6.2.28. Deve implementar o protocolo ECMP;
5.6.2.29. 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;
5.6.2.30. Enviar log para sistemas de monitoração externos, simultaneamente;
5.6.2.31. Deve haver a opção de enviar logs para os sistemas de monitoração externo pode ser ITPs via protocolo TCP e SSL;
5.6.2.32. Proteção anti-spoofing;
5.6.2.33. Suportar otimização do tráfego entre dois equipamentos;
5.6.2.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
5.6.2.35. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
5.6.2.36. Suportar OSPF graceful restart;
5.6.2.37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
5.6.2.38. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
5.6.2.39. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
5.6.2.40. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
5.6.2.41. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
5.6.2.42. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
5.6.2.43. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
5.6.2.44. A configuração em alta disponibilidade deve sincronizar: Sessões;
5.6.2.45. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
5.6.2.46. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
5.6.2.47. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
5.6.2.48. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
5.6.2.49. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
5.6.2.50. 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;
5.6.2.51. 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;
5.6.2.52. 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;
5.6.2.53. 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);
5.6.2.54. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
5.6.2.55. O console de administração deve suportar pelo menos inglês, espanhol e português.
5.6.2.56. O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança
5.6.2.57. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas.
5.6.2.58. 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.
5.6.2.59. Controle por Politica de Firewall
5.6.2.60. Deverá suportar controles por zona de segurança;
5.6.2.61. Controles de políticas por porta e protocolo;
5.6.2.62. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e