INSTITUTO NACIONAL DO SEGURO SOCIAL
Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

**Anexo**

**PROJETO BÁSICO - Anexo I**

1. **ESPECIFICAÇÕES TÉCNICAS**

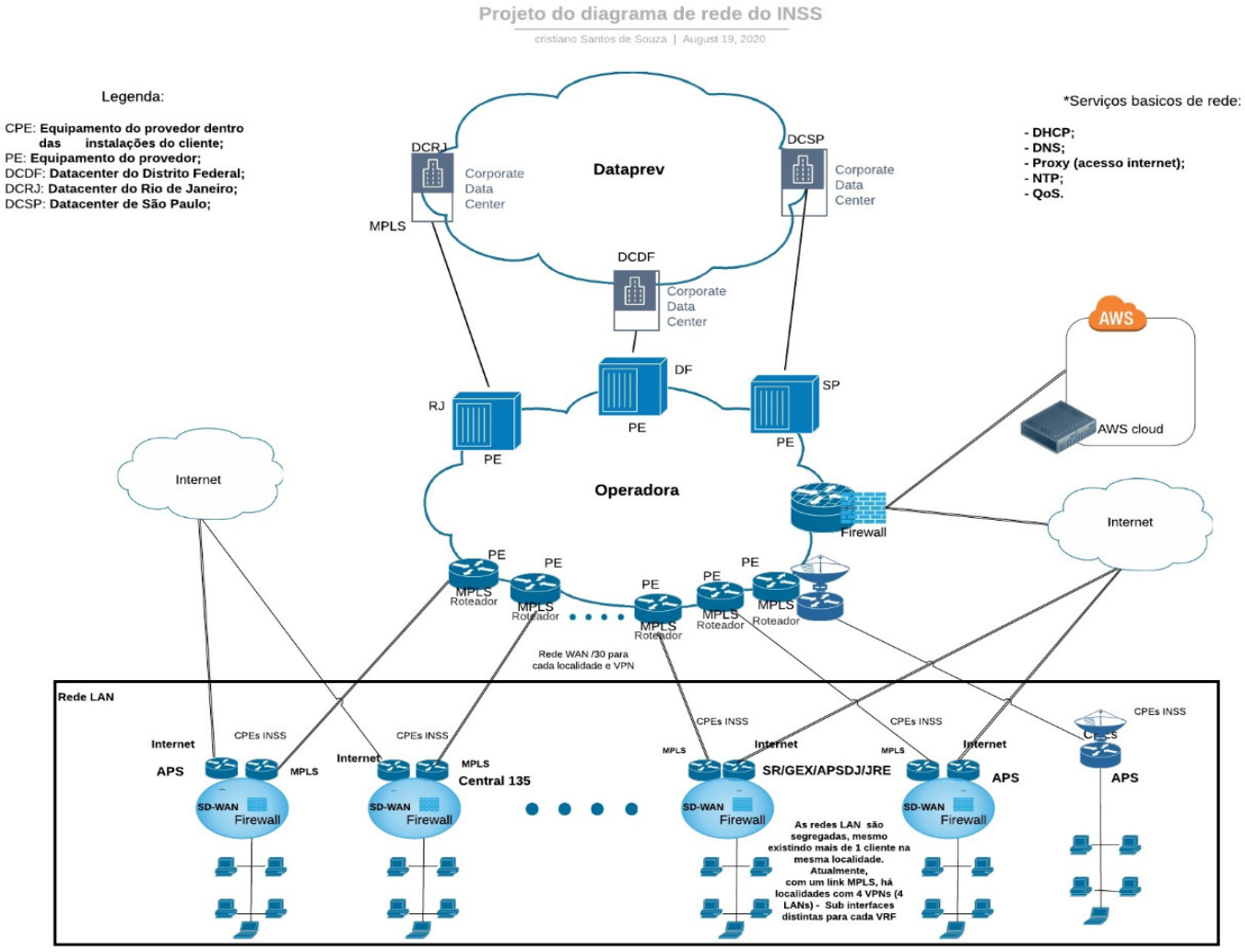
1.1. A CONTRATADA deve prover serviço de comunicação objetivando a interligação de endereços de interesse do CONTRATANTE situados em todo território nacional, além de acesso direto à Internet a partir desses endereços, contemplando:

1.2. Tecnologia de link dedicado para tráfego de dados, voz e vídeo entre todos endereços do contratante, com garantia de largura de banda, confiabilidade e velocidade full-duplex (upload e download iguais);

1.3. Acesso à INTERNET através de circuito assimétricos ou simétricos com garantia de banda por meio privativo e independente;

1.4. Os serviços a serem prestados incluem a elaboração prévia de um Projeto Executivo de rede, a ser analisado pela equipe técnica do INSS para aprovação, conforme especificações incluídas no item 4.10 do Termo de Referência

1.5. A topologia lógica proposta para a modernização da rede de dados deverá ser a seguinte:




1.6. As unidades da CONTRATANTE foram divididas em grupos conforme a quantidade de pessoas e a capacidade de seus links, conforme disposto no item 3.3.6 do Termo de Referência. Esses parâmetros serão utilizados para definir as capacidades mínimas dos equipamentos SD-WAN, conforme disposto no item 1.64.2 deste documento.

1.7. A solução deve funcionar permanentemente, durante as 24 (vinte e quatro) horas do dia e os 7 (sete) dias da semana (24x7).

2. **SDWAN e internet**

2.1. A solução de comunicação de dados utilizará a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar ao máximo o uso da rede.

2.2. A rede de dados contratada deverá se interconectar com a rede da prestadora de serviços previdenciários de Tecnologia da Informação para o INSS - DATAPREV. A forma de conexão entre as duas redes deverá ser definida no projeto executivo. As características desse projeto executivo estão presentes nos itens 4.10 e 4.11 do Termo de Referência.

2.3. O tráfego de saída de Internet deverá ser descentralizado em todas unidades do INSS.

2.4. Todas as unidades do INSS estarão contempladas pela rede contratada e em cada unidade deverá ser instalado o equipamento SD-WAN e os links de Internet dedicado e de internet, conforme disposto neste documento e no Termo de Referência.

2.5. Os concentradores SD WAN da rede receberão o tráfego de todas as unidades do INSS e devem ser instalados nos *datacenters* da empresa que presta serviços previdenciários de Tecnologia da Informação para o INSS - DATAPREV. A forma de roteamento desse tráfego será definida no projeto executivo.

2.6. Os concentradores deverão encaminhar o tráfego corporativo para a rede da empresa que presta serviços previdenciários de Tecnologia da Informação para o INSS - DATAPREV.

2.7. O contingenciamento dos concentradores deverá prever o encaminhamento do tráfego para os demais concentradores ativos, conforme será definido no projeto executivo.

2.8. A rede contratada deverá suportar minimamente protocolos BGP, OSPF, RIP, IGMP.

2.9. O plano de endereçamento IP será definido no projeto executivo.

2.10. A rede contratada deverá se conectar com a estrutura de nuvem do prestador que atende a CONTRATANTE diretamente pela Internet ou pela rede da DATAPREV, conforme será definido no Projeto Executivo. A CONTRATADA deverá conectar todas as unidades ao ambiente de nuvem contratado pelo INSS por meio de VPN site-to-site, utilizando os links de Internet que saem dos concentradores da rede ou conforme será definido no Projeto Executivo.

2.11. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando a solução SD-WAN.

2.12. O serviço de DHCP das redes locais das unidades deverá ser provido pelo equipamento SD-WAN.

2.13. A rede contratada deverá oferecer o serviço de DNS externo para as saídas de tráfego Internet.

2.14. Todos os dispositivos CPE da rede de acesso devem ser dimensionados de forma que tenham capacidade de encaminhamento de pacotes IP, em pacotes por segundo, compatíveis com as velocidades dos links WAN conectados.

2.15. Os links devem transportar pacotes IPv4 e IPv6 com 1500 (mil e quinhentos) bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

2.16. A velocidade de todos os links terrestres deverá ser simétrica e disponível de forma simultânea, ou seja, mesma velocidade de entrada e de saída (links *full-duplex*).

2.17. A velocidade de todos os links com enlace satelital poderá ser entregue de forma assimétrica.

2.18. A CONTRATADA poderá entregar, nas unidades da rede de acesso, os links diretamente nos *appliances* SD-WAN.

2.19. Para as unidades da CONTRATADA poderá entregar os links diretamente nos appliances SD-WAN ou poderá opcionalmente utilizar roteadores específicos para interconectar cada um dos links. Caso seja feita opção por utilizar roteadores, não poderá haver custo adicional para tais equipamentos e todos os demais requisitos para a utilização da solução devem ser mantidos e respeitados.

2.20. Em situações de falha ou de uso intenso da rede, Internet Dedicada , alternativamente os tráfegos corporativos devem ser encaminhados utilizando túneis VPN IPSEC que devem ser estabelecidos pela Internet. Os túneis VPN IPSEC devem utilizar a topologia *hub-and-spoke*, com centralização nos equipamentos SD-WAN concentradores.

2.21. Em situações de falha ou uso intenso dos links de internet com garantia de banda dos endereços do CONTRATANTE, o tráfego deve ser encaminhado pela rede Internet dedicada.

2.22. Para os links de Internet dedicados e Internet com garantia de banda deverão ser utilizados enlaces de comunicação terrestre, somente serão aceitos no máximo 2,5% do total de unidades em meios não confinados terrestres**.**

2.23. A utilização excepcional de meios não confinados terrestres nos acessos deverá ser submetida, por escrito, à apreciação e aprovação prévia do CONTRATANTE, acompanhada das justificativas para a utilização dessas tecnologias. Caso as justificativas sejam aceitas, o CONTRATANTE emitirá termo de autorização para a utilização do meio, sem prejuízo dos prazos de implantação, restrições e critérios de desempenho estabelecidos no corpo desta especificação.

2.24. Os acessos providos devem ser preferencialmente por fibra óptica. Alternativamente, a CONTRATADA poderá utilizar meios não ópticos terrestres nesses acessos.

2.25. Os acessos em meios não confinados terrestres deverão ser trocados por meios confinados, preferencialmente fibra óptica, imediatamente, quando houver condições para tal. Para isso a CONTRATADA deverá apresentar periodicamente quando solicitado pela CONTRATANTE, no mínimo a cada 6 (seis) meses, e no máximo, a cada 1 (um) ano, o plano de viabilidade dessas unidades, para ser aprovado pelo CONTRATANTE.

2.26. Onde não for possível comprovadamente entregar acesso terrestre, será aceito acesso Satelital em banda Ka, nas velocidades de enlace dispostas no Termo de Referência, 20 Mbps de download e 3 Mbps de upload , com e fator de compartilhamento em banda Ka de 1:40 para download e 1:10 para upload.

2.27. Serão aceitos no máximo 3,5 % , do total de acessos, em meio satelital.

2.28. Nos acessos satelitais deverão ser utilizados mecanismos para aumentar o desempenho da comunicação TCP/IP em redes de alto retardo.

2.29. Nos acessos satelitais, caso a implantação implique a necessidade de execução de obras civis nos endereços de interesses do CONTRATANTE, estas ficarão a cargo da CONTRATADA.

2.30. Nos acessos satelitais, as estações terrenas remotas deverão ser de pequeno porte, tipo VSAT.

2.31. Os acessos satelitais deverão ser trocados para acessos terrestres, imediatamente, quando houver condições para tal.

2.32. Não serão aceitos enlaces híbridos, com acessos terrestres e backbone satelital.

2.33. Não serão aceitos enlaces de rádio para prover a última milha dos acessos.

2.34. Enlaces de rádio serão permitidos somente no backhaul, entre o backbone e a rede de acesso/pop da contratada.

2.35. O CONTRATANTE deverá ter acesso do tipo leitura nos equipamentos da rede de acesso instalados nos seus endereços de interesse. Por acesso entende-se permissão de ingresso utilizando interface web, protocolo https, linha de comando utilizando ssh e possibilidade de obtenção de dados via SNMP e syslog.

2.36. Todos os equipamentos destinados ao funcionamento do serviço, alocados em ambiente da CONTRATADA, deverão ser acessíveis a partir de plataformas de gerenciamento SNMP, localizadas na rede interna do INSS.

2.37. As redes serão construídas por meio de circuitos de dados privativos e independentes, com velocidades ou largura de bandas simétricas ou assimétricas para download e upload, onde a banda especificada para cada circuito é a banda livre, respeitando o percentual máximo de 5% (cinco por cento) de overhead gerado por protocolos de comunicação.

2.38. Todos os equipamentos e links deverão suportar o respectivo tráfego da banda completamente ocupada sem degradação do desempenho, atendendo aos níveis de serviço pretendidos. Para isso deverão apresentar configuração de memória, de CPU e capacidade de vazão compatíveis (de forma qualitativa e quantitativa) com as características e componentes desta especificação.

2.39. A rede da CONTRATADA deverá estar com a hora de seus elementos de rede ajustado com o relógio do ON (Observatório Nacional) e sincronizados por meio do protocolo NTP (Network Time Protocol) – RFC1305 ou do protocolo SNTP (Simple Network Time Protocol) versão 4 – RFC2030.

2.40. Caso solicitado, a CONTRATADA deverá realizar alterações nas taxas de transmissão contratadas, com a adequação dos recursos necessários, garantindo o alto desempenho do serviço.

2.41. Os *appliances* SD-WAN e UTM devem ser– fornecidos em formato de equipamento físico dedicado, sendo permitido a implementação das funcionalidades SD-WAN e UTM em um mesmo hardware, ou em hardwares distintos. Um mesmo equipamento pode implementar todas as funcionalidades de roteamento, SD-WAN e UTM,

2.42. Todos os dispositivos CPE da rede de acesso devem ser dimensionados para operar com carga máxima de CPU e memória de 70% (setenta por cento). Caso seja identificado, durante a execução do contrato, um CPE ~~roteador~~ com uso de CPU ou memória acima desse limite , em média apurada durante 30 dias, este deverá ser substituído ou atualizado, sem ônus adicional para a CONTRATANTE.

2.43. O equipamento CPE que receberá os canais de comunicação pode ser o mesmo equipamento onde serão implementados os serviços de SD-WAN e UTM, não sendo necessária a implementação de um roteador dedicado para este fim, desde que atenda a todos os requisitos e funcionalidades de roteamento deste Termo de Referência

2.44. Além das interfaces utilizadas para acesso a rede WAN (Internet dedicada, Internet com garantia de banda )o *appliance* SD WAN deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T), que serão utilizadas na rede interna do CONTRATANTE.

2.45. Deve ser possível implementar o CPE SD-WAN e realizar a recuperação de falhas através de um roteador compatível (configuração de *cluster*).

2.46. **Acomodação dos equipamentos**

2.46.1. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, 23" ou 24", incluindo kit tipo trilho para adaptação, se necessário. Os equipamentos podem ser fixos nos planos do Rack ou sobre bandeja, observando que as laterais de ventilação do equipamento não sejam obstruídas, e caso seja necessário devem ser fornecidos adaptadores para racks ou bandejas.

2.46.2. A CONTRATADA deverá instalar os equipamentos no ambiente indicado pela CONTRATANTE,

2.46.3. O ambiente disponibilizado pela CONTRATANTE dispõe da infraestrutura adequada (espaço físico, energia e climatização) para acomodação dos equipamentos da CONTRATADA.

2.46.4. A CONTRATADA disponibilizará tomadas e/ou PDUs para os racks, no padrão e voltagem compatíveis com cada unidade da CONTRATANTE.

2.47. **Dupla abordagem**

2.47.1. A CONTRATADA deverá instalar os *links* Internet Dedicada e Internet com garantia de banda com dupla abordagem de fibra óptica nos endereços do CONTRATANTE dos grupos 1, 2, 3 e 10

2.47.2. Os *links* poderão ser atendidos pelo mesmo POP da CONTRATADA.

2.47.3. Os circuitos com dupla abordagem não poderão ser instalados no mesmo PE - *Provider Edge*. Nos casos em que houverem limitação prediais nas unidades, serão aceitas, desde que devidamente justificado e autorizado pelo CONTRATANTE, a utilização dos mesmos encaminhamentos nesse acesso predial.

2.47.4. Os *links* com dupla abordagem, em fibra óptica, devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois *links* de comunicação. Por ponto de falha comum entende-se:

a) Utilização compartilhada dos mesmos equipamentos no ambiente da CONTRATADA ou em ambientes públicos: roteadores, multiplexadores, switches, conversores ópticos e outros. Será permitido o compartilhamento de equipamentos dentro das instalações da CONTRATANTE apenas;

b) Utilização compartilhada de *links* físicos ou lógicos no ambiente da CONTRATADA ou em ambientes públicos, como: utilização dos mesmos encaminhamentos, dutos, caixas de passagem, DIOs e outros. Será permitido o compartilhamento da caixa de passagem (na calçada do prédio da CONTRATANTE) e dos dutos da caixa de passagem até o rack dentro das instalações da CONTRATANTE apenas.

2.48. **Domain Name System - DNS**

2.48.1. A solução deverá prover serviço de DNS para a consulta e resolução de nomes da Internet, e deve ser capaz de encaminhar ao DNS do CONTRATANTE as requisições e consultas a endereços internos da rede do CONTRATANTE.

2.48.2. O serviço de DNS externos dos endereços de interesse (unidades) deverá ser provido pela CONTRATADA.

2.48.3. A solução deverá prover serviço de DNS com a função recursiva.

2.48.4. O serviço de cache DNS dos equipamentos SD-WAN deverá ser habilitado e operacional.

2.49. **Tunelamento e Criptografia**

2.49.1. A solução deverá permitir a comunicação indireta entre localidades por meio de topologia “hub and spoke”.

2.49.2. A solução deverá permitir a comunicação por meio de localidades em que se faz necessária a centralização do tráfego utilizando uma topologia “hub and spoke”.

2.49.3. A solução SD-WAN deverá criar dinamicamente os túneis criptografados entre as localidades que possuam SD-WAN.

2.49.4. Os equipamentos utilizados na solução SD-WAN deverão implementar túneis VPN IPSEC com capacidade de integração com equipamentos de outros fabricantes.

2.50. **Roteamento e Políticas**

2.50.1. A solução SD-WAN deverá ser capaz de balancear o tráfego das aplicações entre múltiplos links simultaneamente.

2.50.2. A Solução SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento do fluxo, ou dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação do fluxo, ou dos pacotes de um mesmo fluxo no outro extremo.

2.50.3. A Solução SD-WAN deve monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente.

2.50.4. A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos CPEs, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas.

2.50.5. Os CPE SD-WAN deverão ser entregues em alta disponibilidade (ativo/ativo e/ou ativo/passivo) nas unidades definidas no item 3.3.6,5 do Termo de Referência.

2.50.6. A solução deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando um dos links estiver prejudicado ou os dois links estiverem prejudicados.

2.50.7. A Solução deverá permitir que os endereços de interesse do CONTRATANTE acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN.

2.50.8. A solução deve permitir criar políticas para a modelagem do tráfego.

2.50.9. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas, respeitando o tempo limite de expiração dessas sessões

2.50.10. A rede deve suportar o roteamento das unidades para os concentradores pela métrica de intenção de tráfego.

2.51. **Características gerais de Segurança da Informação**

2.51.1. A solução deverá possuir as seguintes funcionalidades mínimas, porém não exaustivas, de segurança, em face da evolução contínua das boas práticas deste tipo de serviço:

a) Firewall stateful;

b) Controle de Aplicação;

c) Filtro de Conteúdo Web;

d) Sistema de Prevenção de Intrusão (IDS/IPS);

e) Antimalware / Antivírus;

f) VPN IPSEC (Client-to-Site e Site-to-Site) e SSL/TLS;

g) Suporte a qualidade de serviço (QoS) com traffic shaping.

2.51.2. A solução deverá permitir a configuração de perfis e políticas de segurança atribuídos de forma dinâmica.

2.51.3. A solução SD WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN.

2.51.4. A solução deve incluir PKI integrada para emissão automática de certificados digitais utilizados durante autenticação dos túneis VPN.

2.51.5. A solução deve suportar segmentação de tráfego local e fim a fim, de acordo com requerimentos PCI(Payment Card Industry).

2.51.6. **A** solução deve suportar VPNs do tipo Hub Spoke.

2.51.7. **CONCENTRADORES INTERNET DEDICADA**

2.51.7.1. A CONTRATADA deverá implantar 1 (um) concentrador da rede SD WAN em cada um dos datecenters da DATAPREV, conforme endereços dispostos no item 3.3.6,7 do Termo de Referência.

2.51.7.2. A CONTRATADA deverá garantir a interconexão entre a rede rede ~~VPN IP~~ do CONTRATANTE e a rede da DATAPREV.

2.51.7.3. A CONTRATADA deverá prover em cada concentrador a solução SD WAN/UTM, em alta disponibilidade(ativo/ativo) e de acordo com as especificações definidas neste Termo de Referência e seus Anexos ou conforme definido no Projeto Executivo.

2.51.8. **Qualidade de Serviço ( QoS)**

2.51.8.1. A solução da CONTRATADA deverá suportar a arquitetura Diffserv sobre redes Internet

2.51.8.2. De acordo com as prioridades e níveis de serviços definidos, os diferentes tipos de tráfego que serão encaminhados pela Rede do CONTRATANTE poderão ser classificados, a pedido do CONTRATANTE, em classes de serviços (Diffserv) pela rede CONTRATADA

2.51.8.3. A marcação da classe de serviço dos pacotes deve ser feita pela CONTRATADA utilizando o campo DSCP dos pacotes IP nos CPEs, ou seja, roteadores ou appliances SD-WAN.

2.51.8.4. O mapeamento dos tráfegos e larguras de banda de cada classe será definido pela CONTRATANTE.

2.51.9. **CIRCUITO INTERNET**

2.51.9.1. O circuito dedicado de acesso à Internet deverá ser fornecido por meio de circuito de dados privativo e independente, com velocidade ou largura de banda simétrica para download e upload, onde a banda especificada é a banda livre, respeitando o percentual máximo de 5% (cinco por cento) de overhead gerado por protocolos de comunicação.

2.51.9.2. O circuito com garantia de banda por meio privativo e independente de acesso à Internet deverá ser fornecido por meio de circuito de dados privativo e independente, com velocidade ou largura de banda simétrica ou assimétrica COM ~~para~~ 100% download e 50% upload para as velocidades menores que 100Mbps, e 100% download e 30% upload para as velocidades iguais ou maiores que 100Mbps, onde a banda especificada é a banda livre, respeitando o percentual máximo de 5% (cinco por cento) de overhead gerado por protocolos de comunicação

2.51.9.3. A CONTRATADA fornecerá, para cada endereço de interesse do CONTRATANTE, bloco de sua propriedade, de, no mínimo, 4 endereços IPs válidos para a Internet.

2.51.9.4. Os endereços IP deverão ser reservados pela CONTRATADA exclusivamente para o CONTRATANTE, independentemente de utilização;

2.51.9.5. Os blocos de endereços IP para os links de Internet podem ser em IPV4 ou IPV6;

2.52. **GERÊNCIA DE REDE E SERVIÇOS (GRS)**

2.52.1. **Características gerais**

2.52.1.1. A CONTRATADA deverá prover um serviço de Gerência de Rede e Serviços que contemple as áreas funcionais de gerência de falhas, desempenho (monitoração de desempenho, gerência de tráfego e administração de tráfego), configuração, capacidade, segurança e de nível de serviço.

2.52.1.2. A CONTRATADA deverá prover o serviço de Gerência de Rede e Serviços por meio de Centro de Operações de Rede - NOC (*Network Operations Center*) instalado no Brasil, atuando em regime 24X7, todos os dias do ano, com atendimento em língua portuguesa e equipe técnica especializada e capacitada em Gerenciamento de Rede e Serviços, seguindo as melhores práticas do mercado para o funcionamento deste serviço.

2.52.1.3. A Gerência de Rede e Serviços deverá executar todas as tarefas previstas neste Termo de Referência e seus Anexos.

2.52.1.4. A CONTRATADA deve possuir uma estrutura de gerência de rede em formato de NOC 24x7x365, operando em território nacional, em língua portuguesa do Brasil, com acesso para chamados via telefone 0800 e e-mail.

2.52.1.5. A Arquitetura de Gerência, e as Soluções de Gerenciamento devem suportar os principais padrões de mercado em Gerenciamento de Redes e Sistemas, tais como: TCP/IP, DNS, ICMP, HTTP, HTTPS, SSH, sFTP, SNMPv3 e MIB-II, com suporte a MIBs estendidas de fabricantes.

2.52.1.6. A CONTRATADA deverá prover um Sistema de Gerência de Rede e Serviços (SGRS), com acesso seguro (HTTPS) e certificação digital, acessível via web, inclusive a partir de dispositivos móveis, com atualizações em tempo real das informações relevantes, além de visibilidade do comportamento da rede e de todos os circuitos gerenciados; e com informações on-line, com *polling*s a cada 5 minutos e de forma gráfica, dos serviços, de modo a permitir o acompanhamento e monitoração do estado global da rede.

2.52.1.7. A Gerência de Rede e Serviços da CONTRATADA deverá abranger todos os equipamentos e links da solução, independentemente de suas tecnologias, necessários para a prestação dos serviços e o seu gerenciamento.

2.52.1.8. Todas as informações da MIB (*Management Information Base*) dos equipamentos deverão ser populadas com todos os dados disponíveis.

2.52.1.9. A Gerência de Rede e Serviços da CONTRATADA deverá atuar de forma pró-ativa, antecipando-se aos problemas e garantindo a qualidade dos serviços estabelecidos no Termo de Referência e seus Anexos, realizando abertura, acompanhamento e fechamento de chamados técnicos (Trouble Tickets) relacionados com indisponibilidade e desempenho nos serviços, e gerenciamento de rede e segurança, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

2.52.1.10. A contratada deverá manter atualizadas as versões de software/firmware dos dispositivos envolvidos na solução, efetuando o monitoramento dos parâmetros e indicadores necessários para o perfeito funcionamento da solução, de forma a mitigar os riscos de segurança e ocorrência de falhas.

2.52.1.11. O SGRS deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados.

2.52.1.12. O SGRS deverá permitir o acesso simultâneo de no mínimo 5 (cinco) usuários, possibilitar a proteção dos elementos de rede de acessos não autorizados e dentro dos acessos autorizados, permitir a criação de perfis de acesso, baseado na garantia do acesso individual, na validação do acesso através de senha pessoal e na definição de limites de acessos para diferentes perfis de usuários. O acesso às ferramentas de gerência deve ser realizado por meio de contas individuais, não havendo o uso de contas genéricas ou compartilhadas para esse fim.

2.52.1.13. A visualização das informações de gerenciamento providas pelo SGRS deverá ser feita por meio de um Portal de Gerência acessado via interface web, pela Internet. O Portal de Gerência deverá prover o acesso individual por usuário, com senhas exclusivas, utilizando conexão segura (HTTPS) incluindo certificação digital padrão X509 que deverá ser disponibilizado ao CONTRATANTE.

2.52.1.14. O SGRS deverá possuir uma interface única para acesso às suas funcionalidades independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

2.52.1.15. O SGRS deverá disponibilizar funcionalidade para consulta da configuração dos equipamentos e deverá emitir notificações quando houver modificações de configuração.

2.52.1.16. O SGRS deverá fornecer, por meio do portal, visualização de informações on-line (com *pollings* a cada 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

a) Topologia da rede, incluindo os equipamentos da rede de acesso e seus links, com visualização do estado operacional de todos os elementos da rede, atualizados automaticamente;

b) Alarmes e eventos ocorridos na rede com informações de data e hora de ocorrência e identificação dos recursos afetados;

c) Consumo de banda dos links (entrada e saída) com os valores instantâneos, médios e de pico durante todo o contrato, separados por semana e dia, com diferenciação de dias úteis e horário comercial;

d) Consumo de banda por classe de serviço, caso estas estejam configuradas, com os valores instantâneos, médios e de pico durante todo o contrato, separados por semana e dia, com diferenciação de dias úteis e horário comercial;

e) Consumo de banda por tipo de aplicação, com os valores instantâneos, médios e de pico durante todo o contrato, separados por semana e dia, com diferenciação de dias úteis e horário comercial;

f) Utilização de memória e CPU dos equipamentos da rede de acesso;

g) Estratificação de tráfego (entrada e saída) classificado por tipo (IP de origem e de destino), portas (de origem e de destino), serviço, protocolos, classes de serviço de todos os links e respectivos volumes, permitindo a agregação e/ou junção de tipos diferentes de tráfego e a sumarização dos dados coletados;

h) Retardo dos links com valores instantâneos, médios e de pico;

i) Inventário dos equipamentos e links da rede contendo, no mínimo, as seguintes informações: *enlace, com código de identificação, tecnologia e nível de serviço; appliance/roteador, com fabricante, modelo, configuração lógica e física (placas, interfaces, memória, slots e demais); e endereçamento lógico, com IPs e máscaras.*

2.52.1.17. A visualização das informações deverá se referir a um elemento da rede ou a um grupo de elementos de uma maneira que melhor reflita a estruturação das unidades prediais e da hierarquia administrativa da CONTRATANTE, serviços da CONTRATANTE e as tecnologias empregadas na rede.

2.52.1.18. Deverá disponibilizar, para consulta on-line pelo prazo mínimo de 2 meses~~,~~ com possibilidade de análise em tempo real, todos os registros referentes a: acesso ao equipamento; IPS; IDS; acesso VPN; acessos à internet, redes internas e servidores; bem como, outras informações pertinentes para fins de auditoria e/ou verificação de acessos e efetividade de configurações. Após este período, os registros deverão ser armazenados de forma off-line para consulta durante toda a vigência contratual.

2.52.1.19. O SGRS deverá registrar no log de históricos todos os acessos realizados, com autenticação de usuário, data e hora e deverá permitir a recuperação do registro de histórico.

2.52.1.20. O SGRS deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados.

2.52.1.21. O SGRS deverá assegurar a continuidade da coleta dos dados de gerenciamento em casos de perda de comunicação entre o sistema de gerência e os elementos gerenciados, de maneira a garantir que não exista perda de informação no gerenciamento dos recursos.

2.52.1.22. O SGRS deverá possuir um manual de usuário, em português brasileiro, apresentando seus módulos, suas funcionalidades e o esquema de monitoração, de maneira a facilitar o seu uso por parte dos usuários designados pelo CONTRATANTE.

2.52.1.23. O SGRS da CONTRATADA deverá possuir ferramenta capaz de receber e analisar tráfego dos roteadores, appliances SD-WAN e links da solução, utilizando Netflow, IPFIX ou similar, necessários para a prestação dos serviços e o seu gerenciamento.

2.52.1.24. console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN.

2.52.1.25. A console de Gerência deverá informar o status ACESSÍVEL/INACESSÍVEL/CONFIGURATION SYNC/ TUNNELS UP/TUNNELS DOWN de cada dispositivo SD-WAN e UTM.

2.52.1.26. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.

2.52.1.27. A estrutura de gerenciamento da rede e serviços deverá ser hospedada nas dependências da CONTRATADA ou em espaço de *datacenter* gerenciado pela CONTRATADA.

2.52.1.28. A CONTRATADA deve ter um plano de gerenciamento contínuo da capacidade da rede, a fim garantir que o desempenho dos serviços esteja de acordo com os Níveis de Serviço (NMS) acordados.

2.52.1.29. A CONTRATADA deverá disponibilizar consultas online, por meio da console WEB dos produtos e/ou do portal de serviço da contratada, cujos resultados permitam a verificação da conformidade com o estabelecido no Acordo de Nível de Serviço (NMS), e ter insumos para o planejamento de capacidade e a análise da efetividade da solução.

2.52.1.30. As consultas deverão permitir a seleção de períodos de abrangência, com possibilidade de exportação para arquivos HTML ou PDF, contendo todas as informações necessárias para análise da capacidade dos serviços e para as predições.

2.52.1.31. Pelo menos as seguintes informações deverão estar disponíveis:

a) Solicitações de alterações e inclusões de novas políticas, regras e filtros, com data e hora de abertura, identificação do solicitante, código de identificação, descrição, andamento (worklog), data e hora de fechamento;

b) Registros de incidente com data e hora, identificação do responsável, código de identificação, descrição, severidade, data e hora da notificação e tratamento adotado;

c) Bloqueios efetuados pelo serviço de firewall;

d) Bloqueios efetuados pelo serviço de filtragem de conteúdo, categorizados por tipo de conteúdo;

e) Bloqueios efetuados pelo serviço de prevenção de intrusão, totalizados por assinatura e/ou por endereços IP de origem e de destino;

f) Endereços IP de origem e de destino com maior número de acessos;

g) Endereços IP de origem e de destino cujos acessos produziram o maior volume de tráfego;

h) Volume de tráfego por protocolo;

i) Disponibilidade diária dos equipamentos;

j) Utilização de CPU, de memória RAM e tráfego nas interfaces de rede, aferidos em dias úteis;

k) Taxa de ocupação de espaço em disco, se os equipamentos dispuserem deste recurso, aferidos em dias úteis.

2.52.1.32. A CONTRATADA deve analisar os dados obtidos para a geração de predições futuras acerca da capacidade dos recursos de rede.

2.52.1.33. Sempre que os limites de desempenho dos equipamentos forem ultrapassados, sem que tenha havido alterações nos parâmetros de rede estabelecidos, a CONTRATADA deverá promover a adequação ou reconfiguração do equipamento em um prazo máximo de 10 (dez) dias corridos.

2.52.1.34. A CONTRATADA deverá dispor de gráficos de Capacity Planning que permitam criar cenários para projeções de tendências de um determinado recurso da rede.

2.52.1.35. O SGRS deve ser capaz de agrupar os tráfegos em aplicações utilizando pelo menos os seguintes critérios: redes de origem/destino, protocolo da camada de transporte, lista de porta de origem/destino da camada de transporte. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas aplicações em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das aplicações.

2.52.1.36. O SGRS deve ser capaz de agrupar os tráfegos em classes de QoS. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas classes de Qos em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das classes de QoS.

2.52.1.37. O SGRS deve permitir o agrupamento de interfaces de hosts diferentes, formando uma interface agregada para fins de detalhamento de tráfego.

2.52.1.38. O SGRS deve apresentar em gráficos separados o tráfego de entrada e de saída de cada link.

2.52.1.39. O SGRS deve permitir a elaboração de relatórios dos fluxos de comunicação em que deve ser possível verificar IP de origem e destino, protocolo da camada de transporte, porta de origem e destino da camada de transporte.

2.52.1.40. O SGRS deve ter capacidade suficiente para o armazenamento de histórico de pelo menos 1 (um) dos seguintes requisitos: 1 (um) TB de dados ou 6 (seis) meses de informações.

2.52.2. **Gerencia centralizada SD-WAN/UTM**

2.52.2.1. A solução SD-WAN/UTM deverá possuir gerência centralizada;

2.52.2.2. 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.*

2.52.2.3. As licenças de uso de software serão cedidas e atualizadas durante toda a vigência contratual. A solução de SD-WAN, UTM, Gerência Centralizada e todas as funcionalidades que compõe as soluções, deverão estar funcionais e acessíveis, mesmo que incapaz de atualizar softwares e assinaturas.

2.52.2.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

2.52.2.5. O orquestrador da solução SD WAN poderá ser servidor dedicado ou virtualizado, usando uma VM.

2.52.2.6. A gerência centralizada SD WAN/UTM deverá ser hospedada em ambiente de nuvem gerenciado pela CONTRATADA ou nas próprias instalações da CONTRATADA.

2.52.2.7. O sistema deverá suportar contas de usuário/senha estáticas.

2.52.2.8. O Sistema de gerência centralizada SD WAN/UTM deve permitir acesso concorrente de administradores.

2.52.2.9. A gerência centralizada SD WAN/UTM deve permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

2.52.2.10. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius.

2.52.2.11. A solução deverá suportar a automação/integração da rede e as comunicações deverão ser protegidas e criptografadas.

2.52.2.12. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento.

2.52.2.13. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria.

2.52.2.14. Os appliances SD-WAN/UTM deverão suportar SNMP.

2.52.2.15. A Gerência SD-WAN/UTM deverá enviar mensagens syslog referentes aos CPEs SD-WAN/UTM para um servidor syslog externo da CONTRATADA.

2.52.2.16. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada dispositivo SDWAN a cada 5 (cinco) minutos no mínimo.

2.52.2.17. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN.

2.52.2.18. A solução de gerência SD-WAN deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros.

2.52.2.19. Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN/UTM.

2.52.2.20. A solução SD-WAN deverá suportar exportação de registros Netflow / IPFIX.

2.52.2.21. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação.

2.52.2.22. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware.

2.52.2.23. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL.

2.52.2.24. A solução de gerenciamento deve permitir a identificação de quais regras de um objeto estão sendo utilizadas.

2.52.2.25. A solução de gerenciamento deve permitir criação de regras que fiquem ativas em horário definido.

2.52.2.26. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos *appliances.*

2.52.2.27. A solução de gerenciamento deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.

2.52.2.28. Desejável que a solução de gerenciamento permita 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.

2.52.2.29. A solução de gerência deve adicionar os dispositivos SD-WAN de forma automática.

2.52.2.30. A solução deve permitir a adição de políticas e objetos para os dispositivos.

2.52.2.31. A solução de gerenciamento deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, IP de gerência, licenças, horário do sistema e firmware.

2.52.2.32. A solução de gerenciamento deve permitir a instalação de políticas e configurações dos dispositivos por meio de "wizard" , templates ou outros meios.

2.52.2.33. A solução deve permitir criar na solução de gerência *templates* de configuração dos dispositivos.

2.52.2.34. A solução deve permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados.

2.52.2.35. Deve possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência.

2.52.2.36. A solução deve permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada.

2.52.2.37. A solução deve permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos.

2.52.2.38. A solução deve permitir criar regras que permitam a conversão entre os protocolos de internet

2.52.2.39. A solução deve permitir criar regras anti DoS de forma centralizada para os concentradores.

2.52.2.40. A solução deve permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

2.52.2.41. A solução deve 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.

2.52.2.42. A solução deve permitir provisionamento do Zero Touch que deverá funcionar de tal forma que dispositivos SD-WAN e UTM sejam enviados diretamente do fornecedor para um endereço de interesse do CONTRATANTE sem a necessidade de configuração prévia do dispositivo de acesso.

2.53. **SEGURANÇA DA INFORMAÇÃO**

2.53.1. A CONTRATADA deve aplicar em todos os elementos da solução, direitos de acesso que incluem autenticação e autorização, privacidade de dados e auditoria de violações de segurança, usando, por exemplo, a arquitetura de segurança AAA (Autenticação, Autorização e Contabilidade).

2.53.2. A CONTRATADA deverá aplicar e manter atualizados os *patches* de segurança dos seus equipamentos de redes, exclusivos para a prestação dos serviços ao CONTRATANTE.

2.53.3. A CONTRATADA deve monitorar constantemente toda a rede do CONTRATANTE, e caso sejam identificados problemas que afetem a segurança da rede, e que requeiram alteração no hardware, a CONTRATADA deverá substituir o equipamento por outro similar que garanta o Nível Mínimo de Serviço - NMS - acordado.

2.53.4. A CONTRATADA deve realizar análises periódicas nos segmentos da rede da CONTRATANTE e deve fornecer relatórios contendo os resultados das análises realizadas e situação atual da rede contratada, visando detectar possíveis falhas de segurança da rede.

2.53.5. Os dispositivos disponibilizado pela CONTRATADA não poderão ter acesso via tecnologia sem fio.

2.53.6. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados, visando a prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do CONTRATANTE.

2.53.7. A CONTRATADA deverá prover uma rede fim a fim logicamente independente e isolada de qualquer rede de terceiros, em nível lógico do e em nível 2 considerando o modelo OSI.

2.53.8. Caso solicitado pela CONTRATANTE, a CONTRATADA deverá aplicar nos equipamentos de suas redes, exclusivos para prestação de serviços à CONTRATANTE, implementações de segurança tais como: autenticação de roteador CPE, controle de acesso aos dispositivos e

listas de controle de acesso.

2.53.9. Os protocolos de roteamento empregados na solução deverão possuir autenticação, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da rede da CONTRATANTE.

2.53.10. A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o log de eventos da rede da CONTRATANTE, sincronizado-o quanto ao horário via NTP, com detalhamento apropriado, e coletá-lo de forma centralizada, armazenando-o por um período mínimo de 12 (doze) meses, para consulta futura, se necessário for. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

2.53.11. A CONTRATADA deverá disponibilizar, para consulta on-line pelo prazo mínimo de 2 (dois) meses, com possibilidade de análise em tempo real, todos os registros referentes a segurança da informação; acessos a equipamentos e à rede; IPS; IDS; a; bem como, outras informações pertinentes para fins de auditoria e/ou verificação de acessos, tentativas de ataques, incidentes de segurança da informação e efetividade de configurações. Após este período, os registros deverão ser armazenados de forma *off-line* para consulta durante toda a vigência contratual. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

2.53.12. A CONTRATADA, na execução dos serviços, deverá observar a Política de Segurança da Informação do CONTRATANTE, os normativos vigentes e as boas práticas relativas à segurança da informação, especialmente as indicadas nos normativos internos da Administração Pública Federal, em todas as atividades executadas.

2.53.13. A CONTRATADA deverá fornecer acesso a uma Interface de Monitoramento do Serviço de Segurança através de um navegador padrão para disponibilizar relatórios e informações do tráfego monitorado, bem como visualizar os eventos e alertas, contendo informações como Tipo do(s) ataque(s), Horário de início e fim, volume de tráfego bloqueado e não bloqueado; IP(s) de destino(s); os maiores alvos de ataques; os maiores ofensores (IP de origem), dentre outros.

2.54. **Serviços de Segurança da Informação**

2.54.1. **Características gerais**

2.54.1.1. A CONTRATADA deve possuir um centro de serviços de segurança no Brasil, com equipe técnica especializada em segurança de rede (monitoramento, detecção, mitigação, análise, tratamento, contenção, etc).

2.54.1.2. A CONTRATADA deve gerenciar os ativos de rede e as ferramentas de segurança, com completa visibilidade e controle de toda essa infraestrutura de rede, mantendo-a atualizada e em conformidade com todos normativos e requisitos de segurança da rede.

2.54.1.3. A CONTRATADA deverá realizar análises periódicas nos segmentos da rede da CONTRATANTE, visando detectar possíveis falhas de segurança da rede e fornecer relatórios contendo os resultados das análises realizadas e situação atual da rede contratada, sempre que solicitado pela CONTRATANTE.

2.54.1.4. A CONTRATADA deve usar ferramentas e tecnologias, para fazer correlação de eventos, o monitoramento contínuo da rede e sistemas inteligentes na análise dos eventos de segurança, sendo que a solução deve ter capacidade de integração com soluções de SIEM de mercado (third-party SIEM vendors).

2.54.1.5. A CONTRATADA deve detectar ameaças, e mitigar ataques e incidentes de segurança na rede.

2.54.1.6. Após a ocorrência de incidente ou ataque, a CONTRATADA deve recuperar toda a rede ao ponto antes da ocorrência.

2.54.1.7. A CONTRATADA deve coletar, manter e revisar regularmente o log de todas as atividades de rede. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

2.54.1.8. A CONTRATADA deve fazer a investigação das causas dos incidentes de segurança na rede.

2.54.1.9. A CONTRATADA deve criar e configurar as políticas de segurança a serem aplicadas na rede(elementos ativos e serviços).

2.54.1.10. A CONTRATADA é responsável pela geração e divulgação de relatórios dos ataques e incidentes de segurança, os quais devem ser disponibilizados para acesso on-line pelo CONTRATANTE.

2.54.1.11. A CONTRATADA deve elaborar e acompanhar o plano de tratamento de riscos.

2.54.1.12. Os serviços e o monitoramento de segurança devem estar disponíveis em regime de operação 24x7 durante toda a vigência do contrato.

2.54.2. **Serviço de proteção contra-ataques de negação de serviço (Distributed Denial of Service-DdoS)**

2.54.3. A CONTRATADA deverá prover o serviço de Anti-DDoS somente nos enlaces do grupo 10, conforme item 3.3.2 do Termo de Referência.

2.54.4. A CONTRATADA deverá disponibilizar em seu backbone proteção contra-ataques de negação de serviços para os enlaces do grupo 10, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DoS e DDoS.

2.54.4.1. Trata-se de proteção contra-ataques do tipo *Distributed Denial of Service-DdoS* , evitando assim a saturação da banda da Internet e indisponibilidade dos serviços considerando os requisitos mínimos a seguir:

2.54.4.2. O serviço deve ter a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

2.54.4.3. Suportar mitigação automática de ataques, utilizando múltiplas técnicas como *White Lists*, *Black Lists*, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

2.54.4.4. Prover informações de origem de ataque dos países, ranges de IP's e características do tipo de ataque.

2.54.4.5. Prover serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação.

2.54.4.6. Capacidade de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

a) Ataques de inundação (*Bandwidth Flood*), incluindo ICMP *Flood, TCP Flood, UDP Flood, SYN Flood;*

b) Ataques à pilha TCP, incluindo mal uso das *Flags TCP*, ataques de RST e FIN, *SYN*

c) *Flood* e *TCP Idle Resets*

d) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP

e) Ataques de *Botnets, Worms* e ataques que utilizam falsificação de endereços IP origem(*IP Spoofing*)

f) Ataques denominados de "*Comand-and-Contro*l", *Point of Sale Malware, Remote*

g) Access Trojans RAT's via feed atualizado diariamente

h) Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumétricos.

2.54.4.7. Capacidade realizar autenticação de conexão TCP, quando do recebimento de pacotes syn.

2.54.4.8. Limitar o número de conexões TCP simultâneas de um mesmo host

2.54.4.9. Capacidade de bloqueio de query de DNS, resposta de query de DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de recursão DNS.

2.54.4.10. Prover DNS *Black-List*; RegEx para registros específicos ou "flags de recursão". Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente

2.54.4.11. Prevenir que hosts válidos sejam adicionados a *black-list* por engano.

2.54.4.12. Capacidade de mitigação na nuvem, para apenas o tráfego atacado.

2.54.4.13. Manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro.

2.54.4.14. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

2.54.4.15. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.

2.54.4.16. A CONTRATADA deverá prover o serviço nos endereços de interesse indicados pelo CONTRATANTE.

2.54.4.17. A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque com quantidade ilimitada de eventos de ataque ao longo da vigência contratual;

2.54.4.18. A proteção será capaz de detectar e mitigar ataques em modo aprendizagem, através de anomalias estatísticas e desequilíbrio de volume de tráfego, que permita utilização de perfil de tráfego (baseline) tanto de longo quanto de curto prazo.

2.54.4.19. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por equipamentos ou nas bordas remotas (UTM/SD WAN *aplliance* ou roteadores).

2.54.4.20. Garantia de mitigação para um volume de, pelo menos, 2 vezes a banda do link de cada concentrador contratado contra ataques de origem nacional e 10 vezes a banda contratada contra ataques de origem internacional.

2.54.4.21. A mitigação deverá atuar sobre o tráfego somente em momentos de ataque, estando completamente "off-line" em situações normais.

2.54.4.22. A proteção contra ataques de negação de serviço implementará, automaticamente, mecanismos de detecção e mitigação de ataques, através de múltiplas técnicas, sendo obrigatórias, no mínimo White lists, Black lists, Limitação de taxa, Técnicas desafio resposta, Descarte de pacotes malformados, Bloqueio por localização geográfica (país) de endereços IP; Técnicas de mitigação de ataques aos protocolos HTTP e DNS e Lista dinâmica de endereços IP bloqueados;

2.54.4.23. A proteção contra-ataques de negação de serviço *(Denial of Service* - DoS e *Distributed Denial of Service* - DDoS) estará ativa em operação ininterrupta durante 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante todo o período de vigência contratual;

2.54.4.24. Sendo comprovada a indisponibilidade do serviço de acesso dedicado à Internet em decorrência de ataque não bloqueado, o tempo de duração do ataque não bloqueado será contabilizado como indisponibilidade do serviço, sujeitando a CONTRATADA às penalidades estabelecidas no CONTRATO;

2.54.4.25. Sendo comprovado que o tráfego legítimo tenha sido bloqueado indevidamente por mal funcionamento da proteção contra ataques de negação de serviço, o tempo de duração do bloqueio indevido será contabilizado como indisponibilidade do serviço de acesso dedicado à Internet, sujeitando a CONTRATADA às penalidades estabelecidas no CONTRATO.

2.55. **SD-WAN/UTM**

2.55.1. **Funcionalidades comuns para os equipamentos SD-WAN**

2.55.1.1. A solução SD-WAN deverá ser composta por dispositivos SD-WAN (SD-WAN Appliances) e Console de Gerência Centralizada.

2.55.1.2. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.

2.55.1.3. Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros:

a) IP de origem;

b) VLAN de origem;

c) IP de destino;

d) Porta TCP/UDP de destino;

e) Domínio e URL de destino;

f) Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

2.55.1.4. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp.

2.55.1.5. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente.

2.55.1.6. A Solução SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento do fluxo, ou dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação do fluxo, ou dos pacotes de um mesmo fluxo no outro extremo.

2.55.1.7. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo.

2.55.1.8. A solução deve permitir a definição do roteamento para cada aplicação.

2.55.1.9. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação.

2.55.1.10. A solução deve possibilitar a definição do link de saída para uma aplicação específica.

2.55.1.11. A solução deve implementar balanceamento de link por hash do IP de origem e destino;

2.55.1.12. A solução 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.

2.55.1.13. Deve suportar o balanceamento de, no mínimo, dois links.

2.55.1.14. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

2.55.1.15. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding.

2.55.1.16. Para IPv4, deve suportar roteamento estático e dinâmico (BGP, OSPF, RIP e IGMP);

2.55.1.17. A solução deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote ou sessão entre os mesmos.

2.55.1.18. A solução deve possuir recurso para correção de erro, possibilitando a redução das perdas de pacotes nas transmissões.

2.55.1.19. A solução deve permitir a customização dos *timers* para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido.

2.55.1.20. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, 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 *shaping*. Dentre as tratativas possíveis, a solução deve contemplar o suporte a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta.

2.55.1.21. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio.

2.55.1.22. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc.

2.55.1.23. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda.

2.55.1.24. O QoS deve possibilitar a definição de fila de prioridade.

2.55.1.25. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

2.55.1.26. A solução deve ter a capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço.

2.55.1.27. Deve possibilitar a definição de bandas distintas para download e upload.

2.55.1.28. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência).

2.55.1.29. A solução de SD-WAN deve suportar IPv6.

2.55.1.30. A solução deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN.

2.55.1.31. O dispositivo SD WAN deve ter suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo.

2.55.1.32. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN.

2.55.1.33. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site.

2.55.1.34. A solução deve ser ter a funcionalidade de bloqueio de acesso à aplicações.

2.55.1.35. A solução deve suportar NAT dinâmico bem como NAT de saída.

2.55.1.36. Deve suportar balanceamento de tráfego por sessão ***ou*** pacote.

2.55.1.37. As funcionalidades de SD-WAN podem ser fornecidas no mesmo appliance com a solução UTM, ou ofertado em appliance à parte, na mesma quantidade de dispositivos definida para os UTM.

2.55.1.38. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de UTM.

2.55.1.39. O dispositivo SD-WAN deverá possuir serviço de servidor DHCP.

2.55.1.40. O dispositivo SD-WAN deverá possuir serviço de DHCP relay.

2.55.1.41. O dispositivo SD-WAN deverá suportar Agregação de links 802.3ad e LACP.

2.55.1.42. Deve possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link.

2.55.1.43. O dispositivo SD-WAN deverá suportar vários links de acesso, como Internet dedicada e Internet com garantia de banda por meio privativo e independente.

2.55.1.44. O equipamento SD WAN deverá ter capacidade para utilizar as tecnologias 3G/4G/ADSL ou similar. Caso necessário, a pedido do CONTRATANTE, a CONTRATADA deverá efetuar todas as configurações necessárias, no equipamento e na rede, pra efetiva utilização dessas tecnologias , com todas as funcionalidades disponíveis na solução SD WAN e UTM.

2.55.1.45. A solução deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito.

2.55.1.46. A solução deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A *probe* ou similar deve permitir verificar o acesso a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência).

2.55.1.47. Deve ter funcionalidade de proxy transparente HTTP/HTTPS (situação em que o cliente não precisa encaminhar o tráfego para o IP do proxy e não há instalação de cliente, de modo que o cliente acredita estar acessando diretamente o conteúdo desejado).

2.55.1.48. Deve possuir capacidade de agregar e balancear, no mínimo, 3 circuitos de dados utilizando uma interface dedicada para cada circuito.

2.55.1.49. Os equipamentos SDWAN/UTM funcionarão em regime de alta disponibilidade, para os enlaces dos grupos 1, 2, 3 e 10, conforme disposto no item 3.3.6,5 do Termo de Referência, devem suportar as seguintes configurações de cluster:

a) Alta disponibilidade, através do modo Ativo/Passivo;

b) Distribuição de carga entre os equipamentos em alta disponibilidade, através do modo Ativo/Ativo

c) A configuração em alta disponibilidade deve sincronizar sessões, configurações, incluindo, mas não limitado a políticas de Firewall, NAT e objetos de rede, certificados de-criptografados e Associações de Segurança das VPNs;

d) O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

2.55.1.50. Os dispositivos deverão ser instalados e funcionar em regime de alta disponibilidade, em cluster, nos grupos G1, G2, G3 e G10, conforme disposto no item 3.3.2.3 do Termo de Referência.

2.55.1.51. Os dispositivos deverão possuir fonte de alimentação com chaveamento automático de tensão de entrada 110v ou 220v.

2.55.1.52. Os dispositivos devem ser destinados ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação), e suportar temperatura ambiente de armazenamento entre 0ºC e 50ºC.

2.55.1.53. Os dispositivos de comunicação de dados utilizados pela CONTRATADA na solução, devem estar em conformidade com os normativos regulatórios nacionais, entre eles os emanados pela ANATEL.

2.55.1.54. Não serão aceitas funcionalidades que estão previstas somente em Roadmap ou versão pré-produção, sem pleno suporte pelo fabricante.

2.55.2. **Requisitos Mínimos de Capacidade dos appliance SD WAN e UTM**

2.55.2.1. *Equipamento SD-WAN/UTM Tipo 1* - Instalação nos enlaces dos grupos 6, 7, 8 e 9, conforme classificação de grupos disposta no item- 3.3.2 do Termo de Referência

a) *Throughput de, no mínimo, 3,2 Gbps com a funcionalidade de Firewall;*

b) *Throughput de, no mínimo, 250 Mbps de VPN IPSec;*

c) *Throughput de, no mínimo, 450 Mbps de IPS;*

d) *Throughput de, no mínimo, 200 Mbps de NGFW*

e) Suportar, no mínimo, 88.000 (oitenta e oito mil) de conexões simultâneas;

f) *Throughput de, no mínimo,* 150 *Mbps de Threat Prevention;*

g) Suportar, no mínimo, 12.000 (onze mil) conexões por segundo;

h) *Possuir ao menos 4 (quatro) interfaces 1 GE RJ45;*

i) *Suportar no mínimo 100 Mbps de throughput de Inspeção SSL/TLS;*

j) *Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;*

2.55.2.2. Equipamento SD-WAN/UTM Tipo 2 - Instalação nos enlaces dos grupos 2, 3, 4 e 5, conforme classificação de grupos disposta no item 3.3.2 do Termo de Referência

a) Throughput de, no mínimo, 8 Gbps com a funcionalidade de Firewall;

b) Throughput de, no mínimo, 1,5 Gbps de VPN IPSec;

c) *Throughput de, no mínimo, 1,5 Gbps de IPS;*

d) *Throughput de, no mínimo, 1 Gbps de NGFW ;*

e) *Throughput de, no mínimo,* 400 *Mbps de Threat Prevention;*

f) Estar licenciado para, ou suportar sem o uso de licença, 500 (quinhentos) túneis de VPN IPSEC Site-to-Site simultâneos;

g) Suportar no mínimo 600 Mbps de throughput de Inspeção SSL/TLS;

h) Possuir ao menos 6 interfaces 1 GE RJ45;

i) Possuir armazenamento de no mínimo de 1200GB;

j) Possuir fonte de alimentação interna e redundante;

k) Suportar, no mínimo, 42.000 (cinquenta mil) conexões por segundo;

l) Suportar, no mínimo, 1.000.000 (um milhão) de conexões simultâneas;

2.55.2.3. Equipamento SD-WAN/UTM Tipo 3 – Instalação nos enlaces do grupo 1, conforme classificação de grupos disposta no item 3.3.2 do Termo de Referência.

a) *Throughput de, no mínimo, 20 Gbps com a funcionalidade de Firewall;*

b) *Throughput de, no mínimo, 4 Gbps de VPN IPSec;*

c) *Throughput de, no mínimo, 5 Gbps de IPS;*

d) *Throughput de, no mínimo,* 3 Gbps *de NGFW ;*

e) *Throughput de, no mínimo, 1,5* Gbps *de Threat Prevention;*

f) *Estar licenciado para, ou suportar sem o uso de licença, 5.000 (cinco mil) túneis de VPN IPSEC Site-to-Site simultâneos;*

g) *Suportar no mínimo* 2 Gbps *de throughput de Inspeção SSL/TLS;*

h) *Possuir ao menos 8 interfaces 1 GE RJ45;*

i) *Possuir ao menos 2 interfaces 10 GE SFP+;*

j) *Possuir armazenamento de no mínimo de 400GB;*

k) Possuir fonte de alimentação interna, redundante e hot-swap;

l) Suportar, no mínimo, 130.000 ( cento e trinta mil) conexões por segundo;

m) Suportar, no mínimo, 2.500.000 ( dois milhões e quinhentos mil) conexões simultâneas.

2.55.2.4. Equipamento SD-WAN/UTM Tipo 4 – Instalação nos enlaces dos grupo 10, conforme classificação de grupos disposta no item 3.3.2 do Termo de Referência.

a) *Throughput de, no mínimo, 80 Gbps com a funcionalidade de Firewall;*

b) *Throughput de, no mínimo, 14 Gbps de VPN IPSec;*

c) *Throughput de, no mínimo, 10 Gbps de IPS;*

d) *Throughput de, no mínimo, 7 Gbps de NGFW;*

e) *Throughput de, no mínimo, 5 Gbps de Threat Prevention;*

f) *Estar licenciado para, ou suportar sem o uso de licença, 5.000 (cinco mil) túneis de VPN IPSEC Site-to-Site simultâneos;*

g) *Suportar no mínimo* 8 Gbps *de throughput de Inspeção SSL/TLS;*

h) *Possuir ao menos 8 interfaces 1 GE RJ45;*

i) *Possuir armazenamento de no mínimo de 480GB;*

j) Possuir fonte de alimentação interna, redundante e hot-swap;

k) Suportar, no mínimo, 250.000 ( cento e trinta mil) conexões por segundo;

l) Suportar, no mínimo, 2.500.000 ( dois milhões e quinhentos mil) conexões simultâneas.

m) Possuir ao menos 2 interfaces 10 GE SFP+;

2.56. **VPN - Virtual Private Network**

2.56.1. **Características gerais**

2.56.1.1. A solução deve suportar VPN IPSec Site-to-Site.

2.56.1.2. A VPN IPSEC deve suportar criptografia 3DES, AES128 e AES256 (Advanced Encryption Standard).

2.56.1.3. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512.

2.56.1.4. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32.

2.56.1.5. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

2.56.1.6. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

2.56.1.7. Os equipamentos utilizados na solução devem possuir interoperabilidade com no mínimo os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWal, Blockbit

2.56.2. **VPN Corporativa**

2.56.2.1. A Solução poderá ser hospedada em ambiente on-premises ou em nuvem e conexões client-to-site.

2.56.2.2. Deverá ser entregue com mecanismo de alta disponibilidade, seja operando em modo cluster ou alta disponibilidade garantida por Hypervisor.

2.56.2.3. Deverá ser capaz de encaminhar eventos através de syslog ou eventos específicos para fins de segurança da informação.

2.56.2.4. Suportar minimamente cerca de 20.000 conexões usuários simultâneas e até 30.000 contas de usuários.

2.56.2.5. Suporte a autenticação multifator integrado.

2.56.2.6. Suportar conexões VPN SSL/TLS e IPSec Client-to-site e site-to-site.

2.56.2.7. Para VPN IPSec deverá suportar:

a) Padrões de criptografia 3DES, AES128, AES192 e AES256;

b) Mecanismos de autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

c) Suportar Diffie-Hellman Group 1, Group2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

d) Deverá suportar autenticação através de certificados digitais no formato X.509.

2.56.2.8. Para VPN SSL/TLS deverá suportar:

a) Deverá suportar os padrões 3DES, AES128, AES192, AES256 e EDCSA;

b) Deverá suportar SSL v2, SSL v3 e TLS,

2.56.2.9. Deverá permitir criação de perfis e grupos de usuário.

2.56.2.10. Deverá suportar autenticação integrada com base local, LDAP e RADIUS.

2.56.2.11. Deverá ser capaz de configurar nos clientes VPN quais as redes são acessíveis de forma direta e quais as redes são acessíveis pela conexão VPN. Deve também ser possível a operação no modo em que todo o tráfego do cliente VPN só poderá ser transportado através da conexão VPN.

2.56.2.12. Deverá permitir a criação de políticas de VPN distintas para cada perfil de usuário.

2.56.2.13. O software cliente VPN deverá ser compatível com os seguintes sistemas operacionais: Windows 7 ou edição superior, Linux e MacOS.

2.56.2.14. Deverá permitir banners ou mensagens do dia personalizadas para o usuário.

2.56.2.15. Deverá permitir a definição dos horários do dia e dos dias da semana que um dado usuário pode requisitar uma conexão VPN.

2.56.2.16. Deverá possuir inspeção stateful de tráfego IPv4 e IPv6.

2.56.2.17. Deverá possuir roteamento dos protocolos IPv4 e IPv6.

2.56.2.18. Deverá possuir inspeção avançada de pacotes na camada de aplicações para os protocolos: FTP, HTTP, ICMP, SIP, SMTP entre outros.

2.56.2.19. Deverá permitir a captura de pacotes que entram ou saem de suas interfaces sem o uso de probes externas.

2.56.2.20. Deverá suportar o protocolo NetFlow ou sFlow afim de análise de trafego.

2.56.2.21. Deverá estar licenciamento para executar todos os requisitos solicitados nesta especificação.

2.56.2.22. O gerenciamento e monitoramento da solução será de responsabilidade da CONTRATADA.

2.57. **Filtro de dados**

2.57.1. A solução deve permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).

2.57.2. A solução deve suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

2.57.3. A solução deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

2.57.4. A solução deve permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, possibilitando a criação de novos tipos de dados via expressão regular.

2.58. **Filtro de URLs (Web)**

2.58.1. A solução deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.58.2. A solução deve possibilitar a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

2.58.3. A solução 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, Ldap e base de dados local;

2.58.4. A solução deve permitir a identificação pela base do Active Directory e Ldap, deve permitir SSO, de forma que os usuários não precise logar novamente na rede para navegar pelo firewall;

2.58.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.58.6. A solução deve reconhecer aplicações diferentes, incluindo, mas não limitado a tráfego relacionado à peer-to-peer, redes sociais, acesso remoto, streaming de vídeo, anonymizer;

2.58.7. Reconhecer pelo menos as seguintes aplicações: bittorrent, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, vnc, gmail, youtube, http-proxy, http-tunnel, fecebook chat, gmail chat, whatsapp, Telegram, 4shared, dropbox, google drive, skydrive, mysql, oracle, webex, evernote, google-docs, etc;

2.58.8. Atualizar a base de assinaturas de aplicações automaticamente;

2.58.9. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao LDAP, sem necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

2.58.10. Deve alertar ao usuário quando uma aplicação web for bloqueada;

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

a) Categoria Principal;

b) Categorias Secundárias;

c) Tags;

d) Nível de risco.

2.58.12. Deve possibilitar a integração da solução com base do Active Directory e Ldap para criação de políticas. Possibilitando a criação de regras utilizando:

a) Usuários;

b) Grupo de usuários;

c) Endereço IP;

d) Endereço de Rede.

2.58.13. Deve ser capaz de inspecionar trafego SSL/TLS a fim de identificar funcionalidades específicas de cada aplicação, possibilitando o controle granular das mesmas, não se limitando apenas a aplicação principal.

2.58.14. A solução deve deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.58.15. A solução deve possuir pelo menos 60 categorias de URLs;

2.58.16. A solução deve possuir a função de exclusão de URLs do bloqueio;

2.58.17. A solução deve permitir a customização de página de bloqueio;

2.58.18. A solução deverá incluir o mecanismo de listas (Black e White) permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URLs independente da categoria;

2.58.19. A funcionalidade de Aplicação e filtros de URL deverá possuir relatório de utilização;

2.58.20. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs.

2.58.21. Deverá possibilitar a criação de Categorias de URLs customizadas;

2.58.22. Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

2.58.23. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categoriza ou categorizada incorretamente;

2.58.24. Deve possibilitar a customização de pagina de bloqueio de interação com usuário;

2.58.25. Os logs do produto devem incluir informações das atividades dos usuários;

2.58.26. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

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

2.58.28. A solução deverá receber atualizações para sua base de aplicações e URL de um serviço baseado em cloud.

2.58.29. A solução deve ser capaz de identificar qualquer tipo de aplicação Web independente de porta e protocolo;

2.58.30. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;

2.58.31. A solução deverá possuir uma interface de fácil utilização para buscas de Aplicações e URLs;

2.58.32. A solução deverá categorizar por Fator de Risco aplicações e URLS.

2.58.33. **Identificação de usuários**

2.58.33.1. A solução 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;

2.58.33.2. A solução 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;

2.58.33.3. A solução deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior, Active Directory na nuvem e Ldap;

2.58.33.4. A solução 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;

2.58.33.5. A solução deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.58.33.6. A solução deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

2.58.33.7. A solução 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);

2.58.33.8. A solução 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;

2.58.33.9. A solução deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

2.58.33.10. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;

2.58.33.11. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;

2.58.33.12. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

2.58.33.13. A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;

2.58.33.14. A solução deve, nativamente (sem o redirecionamento para equipamentos de terceiros), proporcionar a integração de clientes finais para oferecer autenticação 802.1X, por exemplo um cliente que utilize Windows poderá configurar seu equipamento para o suporte 802.1X;

2.58.33.15. A solução deve suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;

2.58.33.16. A solução deve suportar interoperabilidade com equipamentos de acesso (swtiches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;

2.58.33.17. A solução deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo;

2.59. **UTM**

2.59.1. **Características gerais**

2.59.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado).

2.59.1.2. As funcionalidades de UTM podem ser fornecidas no dispositivo SD-WAN ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os SD-WANs.

2.59.1.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

2.59.1.4. As funcionalidades de segurança que compõem a solução devem funcionar em equipamento único obedecendo a todos os requisitos desta especificação, com suporte de gerenciamento centralizado.

2.59.1.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

2.59.1.6. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;

2.59.1.7. Para todos os equipamentos deverá ser fornecido bandeja ou suporte para montagem em rack;

2.59.1.8. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) ou outro mecanismo de integração/interoperabilidade;

2.59.1.9. Os dispositivos de proteção de rede devem possuir suporte a pelo menos 256 Vlans para os dispositivos do Tipo 1 e no mínimo 4096 Vlans para os dispositivos dos Tipos 2 e 3;

2.59.1.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast;

2.59.1.11. A solução deve suportar BGP, OSPF, RIP e roteamento estático;

2.59.1.12. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

2.59.1.13. A solução deve suportar NAT dinâmico (Many-to-Many) nos concentradores definidos na arquitetura da rede corporativa de dados;

2.59.1.14. A solução deve suportar NAT estático (1-to-1);

2.59.1.15. A solução deve suportar NAT estático bidirecional 1-to-1;

2.59.1.16. A solução deve suportar Tradução de porta (PAT);

2.59.1.17. A solução deve suportar NAT de Origem;

2.59.1.18. A solução deve suportar NAT de Destino;

2.59.1.19. A solução deve suportar NAT de Origem e NAT de Destino simultaneamente;

2.59.1.20. A solução deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

2.59.1.21. A solução deve suportar NAT64;

2.59.1.22. A solução deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

2.59.1.23. A solução deve possibilitar o envio de log para sistemas de monitoração externos, de forma segura, usando protocolo SSL, túneis IPSEC ou outro mecanismo de transporte de dados segura. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

2.59.1.24. A solução deve ter funcionalidade de Proteção anti-spoofing;

2.59.1.25. A solução deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

2.59.1.26. A solução deve suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados e deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;;

2.59.1.27. A solução deve deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.59.1.28. A solução deve ter suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

2.59.1.29. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

2.59.1.30. O modo de Alta-Disponibilidade deve possibilitar monitoração de falha de link;

2.59.1.31. A solução deve possibilitar o Controle, inspeção e descriptografia de SSL/TLS para tráfego de Saída (Outbound);

2.59.1.32. Não serão aceitas soluções baseadas em PCs de uso geral.

2.59.1.33. Os equipamentos devem ser novos, ou seja, de primeiro uso. 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*.

2.59.2. **Políticas**

2.59.2.1. A solução deve suportar controles por zonas de segurança;

2.59.2.2. A solução deve suportar controles de políticas por porta e protocolo;

2.59.2.3. A solução deve suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

2.59.2.4. A solução deve possibilitar a definição de Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.59.2.5. A solução deve possibilitar o controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

2.59.2.6. A solução deve possibilitar o Controle, inspeção e descriptografia de SSL/TLS, por política, para tráfego de saída (Outbound);

2.59.2.7. A solução deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

2.59.2.8. A solução deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

2.59.2.9. A solução deve ter suporte a objetos e regras IPV6;

2.59.2.10. A solução deve ter suporte a objetos e regras multicast;

2.59.2.11. A solução deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.59.3. **Controle de Aplicações**

2.59.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.59.3.2. A solução deve possibilitar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

2.59.3.3. A solução deve 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;

2.59.3.4. A solução deve 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;

2.59.3.5. A solução deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.59.3.6. A solução deve 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;

2.59.3.7. Para tráfego criptografado SSL/TLS, a solução deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

2.59.3.8. A solução 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. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

2.59.3.9. A solução deve identificar o uso de táticas evasivas via comunicações criptografadas;

2.59.3.10. A solução deve ser capaz de atualizar a base de assinaturas de aplicações automaticamente;

2.59.3.11. 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;

2.59.3.12. 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;

2.59.3.13. A solução deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

2.59.3.14. A solução deve permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias;

2.59.3.15. A solução deve permitir a atualização da base de assinaturas de aplicações;

2.59.3.16. A solução deve deve alertar o usuário quando uma aplicação for bloqueada;

2.59.3.17. A solução deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

2.59.3.18. A solução deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

2.59.3.19. A solução deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

2.59.3.20. A solução deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

2.59.3.21. A solução deve possibilitar a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

2.59.3.22. A solução deve possibilitar a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

2.59.3.23. A solução deve possibilitar a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

2.59.3.24. A solução deve possibilitar a inspeção do payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.59.3.25. A solução 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, A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

2.59.3.26. A solução deve possibilitar adicionar o controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

2.59.3.27. A solução deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao whatsapp mas bloquear a transferência de arquivos.

2.59.3.28. A solução deve possibilitar a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);Nível de risco da aplicação;

2.59.3.29. Possibilitar o bloqueio do tráfego de aplicações , integrado a base de Antivírus e Antimalware;

2.59.4. **Prevenção de ameaças**

2.59.4.1. Para proteção do ambiente contra ameaças, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

2.59.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

2.59.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

2.59.4.4. **IPS**

2.59.4.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

2.59.4.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

a) Análise de padrões de estado de conexões;

b) Análise de decodificação de protocolo;

c) Análise para detecção de anomalias de protocolo;

d) IP Defragmentation;

e) Remontagem de pacotes TCP;

f) Bloqueio de pacotes malformados;

g) Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

h) Detectar e bloquear a origem de port scans;

i) Possuir assinaturas para bloqueio de ataques de buffer overflow;

j) Deverá possibilitar a criação de assinaturas customizadas;

k) Suportar bloqueio de arquivos por tipo;

l) Identificar e bloquear comunicação com botnets;

m) Deve suportar várias técnicas de prevenção, incluindo Drop (Cliente, Servidor e ambos);

n) Deve suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);

o) Deve suportar a captura de pacotes (PCAP), por assinatura de IPS;

p) Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

q) Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis;

r) Rastreamento de vírus em pdf;

s) Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate, como: zip e gzip;

t) 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;

u) Deve permitir a inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção.

2.59.4.7. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

2.59.4.8. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.59.4.9. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

2.59.4.10. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.59.4.11. Deve permitir o bloqueio de vulnerabilidades;

2.59.4.12. Deve permitir o bloqueio de exploits conhecidos;

2.59.4.13. Deve incluir proteção contra ataques de negação de serviços;

2.59.4.14. Bloquear ataques efetuados por worms conhecidos;

2.59.4.15. Possuir assinaturas para bloqueio de ataques de buffer overflow;

2.59.4.16. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

2.59.4.17. 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;

2.59.4.18. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

2.59.4.19. 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;

2.59.4.20. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

2.59.4.21. Os eventos devem identificar o país de onde partiu a ameaça;

2.59.4.22. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

2.59.4.23. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

2.59.4.24. 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.

2.59.4.25. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

2.59.4.26. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

2.59.4.27. Possuir no mínimo 11.000 assinaturas de IPS;

2.59.4.28. A proteção deve possuir capacidade de análise da reputação de endereços IP, possuindo base própria de informações, gerada durante a filtragem dos ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;

2.59.4.29. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 5 (cinco) categorias, capaz de permitir seleção por categorização, elas devem atender as seguintes classificações: Sites Maliciosos Conhecidos, Sites de oferecem serviços de alto risco, Sites não verificados, Sites respeitáveis de mídia social e Sites seguros conhecidos e verificados; spam, reputation, malware, attacks, anonymous e abuse;

3. **GLOSSÁRIO**

**3DES:** Triple(3) Data Encryption Standard(Padrão de Criptografia de Dados Triplo).É um padrão de criptografia baseado em outro algoritmo de criptografia simétrica, o DES( Data Encryption Standard – Padrão de Cripto grafia de Dados) , desenvolvido pela IBM em 1974 e adotado como padrão em 1977. O 3DES usa 3 chaves de 64 bits,embora apenas 56 bits de cada chave são efetivamente usados, os outros 8 bits são usados para verificar paridade.

**802.1X:** É um padrão IEEE para controle de acesso à rede com base em portas; faz parte do grupo IEEE 802.1 de protocolos de redes de computadores. Provê um mecanismo de autenticação para dispositivos que desejam juntar-se a uma porta na LAN, seja estabelecendo uma conexão ponto-a-ponto ou prevenindo acesso para esta porta se a autenticação falhar. É usado para a maioria dos Access points(Pontos de Acesso) sem fio.

**Active Directory:** Diretório Ativo (tradução literal). *Active Directory* (AD) é um **serviço de diretório** desenvolvido pela Microsoft para redes Windows. Ele está incluído na maioria dos sistemas operacionais Windows Server como um conjunto de processos e serviços. Inicialmente, o Active Directory era responsável apenas pelo gerenciamento centralizado do domínio. No entanto, se tornou um título abrangente para uma ampla gama de serviços relacionados à identidade baseados em diretório.

**ADSL:** *Asymmetric Digital Subscriber Line* (Linha de Assinante Digital Assimétrica) É uma tecnologia de comunicação de dados que permite a transmissão de dados mais rápida em linhas telefônicas de cobre do que um modem de voz convencional. Em ADSL, a largura de banda e a taxa de bits são consideradas assimétricas, o que significa maior taxa em direção às instalações do cliente (download) do que o inverso (upload).

**AES:** O *Advanced Encryption Standard* (Padrão para Criptografia Avançada), também conhecido por seu nome original ***Rijndael*** , é uma especificação para a criptografia de dados eletrônicos estabelecida pelo Instituto Nacional de Padrões e Tecnologia dos EUA em 2001.

**Anti-Spyware:** Software dedicado a remover ou bloquear ***spyware***. Os programas anti-*spyware* podem combater o *spyware* de duas maneiras: Eles podem fornecer proteção em tempo real de maneira semelhante à proteção antivírus: eles verificam todos os dados de rede recebidos em busca de *spyware* e bloqueiam todas as ameaças detectadas, ou podem ser usados exclusivamente para detecção e remoção de software *spyware* que já foi instalado no computador. Esse tipo de *anti-spyware* geralmente pode ser configurado para fazer uma varredura regularmente.

**API Northbound**: API para o Norte. É uma peça chave da arquitetura **SDN** (*Software Defined Network – Rede definida por Software. **SD-WAN** é um tipo de SDN*). Ela é uma API que faz a comunicação entre o plano de gerenciamento e o plano de controle(partes da arquitetura SD-WAN), efetivamente permitindo que aplicações utilizadas por administradores de rede efetuem o controle e o monitoramento das funções da rede sem ter que ajustar os detalhes mais finos da comunicação.

**API RESTful**. É um tipo de API que fornece dados em um formato padronizado baseado em requisições HTTP. Por exemplo: As API das redes sociais, que permite que usuário se autentique em aplicações externas a elas, mas com as mesmas credenciais. Uma API Restful faz isso, fornecendo os dados da rede social para as aplicações, facilitando o cadastro e o acesso.

**API:** *Application Programming Interface*. É uma interface de computação que define as interações entre vários softwares. Ele define os tipos de chamadas ou solicitações que podem ser feitas, como fazê-las, os formatos de dados que devem ser usados, as convenções a seguir, etc. Ele também pode fornecer mecanismos de extensão para que os usuários possam estender a funcionalidade existente de várias maneiras e em vários graus. Uma API pode ser totalmente customizada, específica para um componente ou pode ser projetada com base em um padrão da indústria para garantir a interoperabilidade. Por meio da ocultação de informações, as APIs permitem a programação modular, que permite aos usuários usar a interface independentemente da implementação.

**Appliance**: geralmente é um dispositivo de hardware separado e dedicado com software integrado (firmware), especificamente projetado para fornecer um recurso de computação específico.

**Ataque Command and Control:** Ataque Comando e Controle. Um ataque de comando e controle (também chamado C2) usa código malicioso para obter acesso remoto - ou controle - sobre um computador. Utiliza um servidor C2 controlado pelo invasor para enviar comandos e receber dados roubados de máquinas comprometidas.

**AWS:** *Amazon Web Services (Amazon Serviços Web)* é uma subsidiária da Amazon que fornece plataforma de computação em nuvem sob demanda.

**Backbone:** *Espinha Dorsal.* No contexto de redes de computadores, o backbone, designa o esquema de ligações centrais de um sistema de redes mais amplo, tipicamente de elevado desempenho e com dimensões continentais.

**Backhaul**: Backhaul é a porção de uma rede de telecomunicações responsável por fazer a ligação entre o núcleo da rede, ou backbone, e as sub-redes periférica, ou rede de acesso.

**Banda KA:** É a parte do espectro eletromagnético, na faixa de micro-ondas, compreendida entre as frequências de 27 e 40Ghz. É utilizada na comunicação satelital.

**Banda KU**: É uma faixa de frequência utilizada nas comunicações satelitais que tem espectro de frequência, segundo o IEEE: 15.35 GHz até 17.25 GHz.

**BGP:** (*Border Gateway Protocol*) É um protocolo de roteamento, criado para uso nos roteadores principais da Internet.

**Bloqueio de Query (pesquisa) de DNS:** O bloqueio ou filtragem de *query* de DNS, é uma estratégia para dificultar a localização de domínios ou sites específicos na internet pelos usuários. Foi criado como um meio de bloquear e-mails de spam de endereços IP maliciosos conhecidos.

**Bot:** Um bot é um aplicativo de software que executa tarefas automatizadas pela Internet. [Normalmente, os bots realizam tarefas que são simples e repetitivas, muito mais rápido do que uma pessoa poderia. O uso mais extenso de bots é para rastreamento da web, em que um script automatizado busca, analisa e arquiva informações de servidores da web.

**Botnet:** Botnet são vários dispositivos conectados à Internet, cada um executando um ou mais ***bots***. Os botnets podem ser usados para realizar ataques de negação de serviço distribuído (DDoS), roubar dados, enviar spam e permitir que o invasor acesse o dispositivo e sua conexão. O proprietário pode controlar o botnet usando software de comando e controle (C&C).

***Broadcast:*** Em uma LAN, é uma transmissão para todos os nós da rede, simultaneamente.

**Browser Based:** A computação baseada em navegador é o uso de navegadores da web para realizar tarefas de computação. A computação na web foi descrita em 2000. A computação baseada em navegador complementa a computação em nuvem porque reduz a carga computacional do lado do servidor, geralmente usando serviços da web hospedados na nuvem.

**Buffer Overflow:** Estouro de Buffer. Em segurança da informação e programação, um estouro de buffer, ou saturação de buffer, é uma anomalia em que um programa, enquanto grava dados em um buffer, ultrapassa os limites do buffer e sobrescreve em localizações de memória adjacentes.

**CE:** *Customer Edge*(Borda do Cliente). É o roteador que está localizado na rede do cliente do serviço de telecomunicação, e que está diretamente conectado ao PE**.**

**CLI:** *Command-Line Interface*( interface de linha de comando). Uma interface de linha de comando processa comandos para um programa de computador na forma de linhas de texto. O programa que controla a interface é chamado de interpretador de linha de comando ou processador de linha de comando. Os sistemas operacionais implementam uma interface de linha de comando em um ***shell*** para acesso interativo às funções ou serviços do sistema operacional.

**Client Server:** Cliente Servidor. O modelo cliente-servidor é uma estrutura de aplicativo distribuída que particiona tarefas ou cargas de trabalho entre os provedores de um recurso ou serviço, chamados servidores, e solicitantes de serviços, chamados clientes. Frequentemente, clientes e servidores se comunicam em uma rede de computadores em hardware separado, mas tanto o cliente quanto o servidor podem residir no mesmo sistema. Um host de servidor executa um ou mais programas de servidor, que compartilham seus recursos com os clientes. Um cliente não compartilha nenhum de seus recursos, mas solicita conteúdo ou serviço de um servidor.

**Cloud:** *Nuvem.* A computação em nuvem é a disponibilidade sob demanda de recursos computacionais, especialmente armazenamento de dados (armazenamento em nuvem) e poder de computação, sem gerenciamento ativo direto pelo usuário. O termo é geralmente usado para descrever centros de dados disponíveis para muitos usuários na Internet. Nuvens grandes, predominantes hoje, muitas vezes têm funções distribuídas em vários locais a partir de servidores centrais.

**Cluster:** *Agrupamento*. Em computação, cluster é um conjunto de dispositivos conectados que funcionam juntos para que, em muitos aspectos, possam ser vistos como um único sistema.

**CPE:** *Customer Premises Equipment* ou *Customer Provided Equipment*. É um termo técnico muito utilizado por operadoras de telecomunicações e fornecedores de serviços de comunicação. significa "equipamento dentro das instalações do cliente". CPE é um termo genérico que está relacionado à tecnologia e depende do contexto aonde é utilizado. Por exemplo, para uma operadora de serviços celular o

**CPE** é o telefone celular, para uma empresa de telefonia o **CPE** pode ser o aparelho de telefone (para serviços de voz) ou o modem (para serviços de dados).Outros exemplos de **CPEs**: roteadores, cable modem, antenas etc. Qualquer equipamento que seja necessário para um cliente receber o serviço de comunicação é um CPE.

**Creepware:** Creepware é um software spyware que permite que hackers, predadores online e criminosos cibernéticos bisbilhotem o computador pessoal da vítima, tablet, laptop, desktop, smartphone ou outro dispositivo (como IoT - internet das coisas) que tenha conectividade com a Internet, geralmente uma webcam e um microfone. Muitas vezes o Creepware ignora firewalls, antivírus e outras contramedidas de segurança porque os usuários finais confiam em aplicativos para download (Apps) de lojas online em plataformas conhecidas e confiáveis. Houve centenas de milhões de downloads de Creepware e a maioria ainda não é detectada.

**CVE:** Common Vulnerabilities and Exposures (Vulnerabilidades e Exposições Comuns). O Common Vulnerabilities and Exposures (CVE) é um banco de dados que registra vulnerabilidades e exposições relacionadas a segurança da informação conhecidas publicamente. O sistema é mantido pela National Cybersecurity FFRDC, operado pela Mitre Corporation, com financiamento da National Cyber Security Division do Departamento de Segurança Interna dos Estados Unidos.

**DdoS:** *Distributed Denial-of-Service* (Negação de Serviço Distribuído) Ataque de negação de serviço distribuído ocorre quando vários sistemas inundam a largura de banda ou os recursos de um sistema direcionado, geralmente um ou mais servidores web. Um ataque DDoS usa mais de um endereço IP exclusivo ou máquinas, geralmente de milhares de hosts infectados com *malware*. Um ataque distribuído de negação de serviço normalmente envolve mais do que cerca de 3 a 5 nós em redes diferentes.

**Delay:** *Atraso*. O atraso da rede é uma característica de design e desempenho de uma rede de telecomunicações. Ele especifica a latência para que um bit de dados viaje pela rede de um ponto da conexão a outro. Normalmente é medido em múltiplos ou frações de segundo. O *delay* é função, entre outras coisas, do meio físico e da taxa de transferência do circuito de dados.

Depois que o servidor é autenticado com segurança para o cliente por meio de seu certificado CA e, opcionalmente, o cliente para o servidor, o servidor pode usar a conexão segura estabelecida ("túnel") para autenticar o cliente. Ele pode usar um protocolo de autenticação e infraestrutura existentes e amplamente implantados, incorporando mecanismos de senha legados e bancos de dados de autenticação, enquanto o túnel seguro fornece proteção contra espionagem e ataques . Observe que o nome do usuário nunca é transmitido em texto não criptografado, melhorando a privacidade.

**DHCP Relay:** Encaminhamento(de requisição) DHCP. Mecanismo utilizado para atribuição dinâmica de endereços IP e outros parâmetros de configuração de rede, quando o servidor DHCP não está na mesma rede dos dispositivos requisitantes. É configurado um agente DHCP relay no *gateway default*(normalmente o roteador) da rede, que recebe as requisições e encaminha para o servidor DHCP. Para fazer isso, o agente pega os pacotes enviados pelos clientes DHCP e transforma esses pacotes em um formato que o *gateway* possa encaminhá-los ao servidor.

**DHCP:** *Dynamic Host Configuration Protocol (P*rotocolo de Configuração Dinâmica de Hosts) É um protocolo de gerenciamento de rede usado em redes IP, por meio do qual um servidor DHCP atribui dinamicamente um endereço IP e outros parâmetros de configuração de rede a cada dispositivo na rede, para que possam se comunicar com outras redes IP redes.

**Diffie-Hellman Groups:** Os grupos Diffie-Hellman (DH) determinam a força da chave usada no processo de troca de chave. Números de grupo mais altos são mais seguros, mas requerem mais tempo para calcular a chave.

**Diffie-Hellman:** A troca de chaves de Diffie-Hellman é um método de criptografia específico para troca de chaves desenvolvido por Whitfield ***Diffie*** e Martin ***Hellman*** e publicado em 1976. Foi um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro do campo da criptografia. O método da troca de chaves de Diffie-Hellman permite que duas partes que não possuem conhecimento a priori de cada uma, compartilhem uma chave secreta sob um canal de comunicação inseguro.

**DiffServ:** *Differentiated services* (Serviços Diferenciados). É uma arquitetura de rede de computadores que especifica um mecanismo simples e escalonável para classificar e gerenciar o tráfego de rede e fornecer qualidade de serviço (QoS) em redes IP modernas. DiffServ pode, por exemplo, ser usado para fornecer baixa latência para tráfego de rede crítico, como voz ou streaming de mídia, enquanto fornece serviço simples de melhor esforço para serviços não críticos, como tráfego da web ou transferência de arquivos. DiffServ usa um ponto de código de serviços diferenciados de 6 bits (**DSCP** - *Differentiated Services Code Point*) no campo de serviços diferenciados de 8 bits (campo DS) no cabeçalho IP para fins de classificação de pacotes.

**DLP:** *DATA LOSS PREVENTION*(Prevenção contra Perda de Dados). A prevenção de perda de dados é uma tecnologia para detectar potenciais violações de dados / transmissões de filtração de dados e as impedir por meio do monitoramento, detectando e bloqueando dados confidenciais durante o uso (ações de endpoint), em movimento (tráfego de rede) e em repouso (armazenamento de dados) .Os termos "perda de dados" e "vazamento de dados" estão relacionados e costumam ser usados alternadamente. Os incidentes de perda de dados se transformam em incidentes de vazamento de dados nos casos em que a mídia que contém informações confidenciais é perdida e subsequentemente adquirida por uma parte não autorizada. No entanto, um vazamento de dados é possível sem perder os dados do lado de origem. Outros termos associados à prevenção de vazamento de dados são detecção e prevenção de vazamento de informações (*Information Leak Detection and Prevention* - ILDP), prevenção de vazamento de informações (*Information Leak Prevention* ILP), monitoramento e filtragem de conteúdo (*Content Monitoring and Filtering* - CMF), proteção e controle de informações (*Information Protection and Control* IPC) e sistema de prevenção de extrusão (*Extrusion Protection System* - EPS), em oposição a sistema de prevenção de intrusão.

**DNS Blacklist:** Lista Negra baseada no Sistema de Nomes de Domínio ou DNSBL é um serviço onde, com uma simples consulta DNS, os servidores de e-mail podem verificar se um endereço IP de envio está em uma lista negra de Endereços IP com reputação de enviar spam por e-mail. A maioria dos softwares de servidor de e-mail pode ser configurada para verificar uma ou mais dessas listas - normalmente rejeitando ou sinalizando mensagens se forem de um site listado. Um DNSBL é um mecanismo de software, em vez de uma lista ou política específica. Existem dezenas de DNSBLs, que usam uma ampla gama de critérios para a listagem e remoção de endereços. Isso pode incluir listar os endereços de computadores zumbis ou outras máquinas usadas para enviar spam, provedores de serviços de Internet (ISPs) que hospedam spammers voluntariamente ou aqueles que enviaram spam para um sistema *honeypot.*

**DNS:** *Domain Name System*( Sistema de Nome de Domínio). é um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada . Faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante. A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: resolução de nome.

**DNSSEC:** *Domain Name System Security Extensions*(Extensões de Segurança do DNS).As Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC) são um conjunto de especificações da IETF (Internet Engineering Task Force – Força Tarefa de Engenharia da Internet) para

proteger certos tipos de informações fornecidas pelo Sistema de Nomes de Domínio (DNS) conforme usado em redes de protocolo da Internet (IP). É um conjunto de extensões do DNS que fornecem aos clientes DNS (resolvedores) autenticação criptográfica de dados DNS, negação de existência autenticada e integridade de dados, mas não disponibilidade ou confidencialidade.

**Domain Controller:** Controlador de Domínio (DC). É um computador servidor que responde a solicitações de autenticação de segurança em um domínio de rede de computador. É um servidor em uma rede responsável por permitir o acesso do host aos recursos do domínio.

**Domínio de broadcast:** No contexto de uma LAN, dispositivos( hosts) conectados ao mesmo switch Ethernet são membros do mesmo domínio de *broadcast*. Além disso, qualquer host conectado ao mesmo conjunto de switches são membros do mesmo domínio de broadcast. Logicamente, são todos os dispositivos de uma rede que podem alcançar uns aos outros por um *broadcast.*

**Drop:** Em rede de computadores, é o descarte de um pacote de dados devido a sobrecarga no circuito, ou o encerramento intencional, mas não acordado, de uma conexão.

**Dropbox:** Dropbox é um serviço de hospedagem de arquivos operado pela empresa Dropbox, Inc

**EAP-GTC:** EAP Generic Token Card(EAP Cartão Token Genérico). É um método EAP criado pela Cisco como uma alternativa ao PEAP / EAP-MSCHAP . EAP-GTC carrega um desafio de texto do servidor de autenticação e uma resposta gerado por um token de segurança. O mecanismo de autenticação PEAP-GTC permite autenticação genérica para vários bancos de dados, bem como o uso de uma senha descartável.

**EAP-TLS:** EAP - Transport Layer Security é um padrão aberto IETF que usa o protocolo **TLS** e é bem suportado pelos fornecedores sem fio. EAP-TLS é o protocolo de autenticação EAP LAN sem fio padrão original. O EAP-TLS ainda é considerado um dos padrões EAP mais seguros disponíveis, embora o TLS forneça uma segurança forte apenas enquanto o usuário compreender os avisos potenciais sobre credenciais falsas e é universalmente suportado por todos os fabricantes de hardware e software de LAN sem fio.

**EAP-TTLS:** EAP Tunneled Transport Layer Security (EAP-TLS Tunelado) é um protocolo EAP que estende TLS.

**EAP:** *Extensible Authentication Protocol* (Protocolo de Autenticação Extensível) É uma estrutura de autenticação freqüentemente usada em conexões de rede e internet. EAP é uma estrutura de autenticação para fornecer o transporte e o uso de material e parâmetros gerados por métodos EAP. Existem muitos métodos definidos e existem vários métodos específicos de fornecedores e novas propostas. EAP não é um protocolo com fio; em vez disso, ele apenas define as informações da interface e os formatos. Cada protocolo que usa EAP define uma maneira de encapsular as mensagens EAP do usuário dentro das mensagens desse protocolo.

**FIN:** É uma *flag* TCP. A fase de encerramento da sessão TCP é um processo de quatro fases, em que cada interlocutor responsabiliza-se pelo encerramento do seu lado da ligação. Quando um deles pretende finalizar a sessão, envia um pacote com a *flag* **FIN** ativa.

**Firewall Stateful:** É um Firewall orientado a conexões, ou estados. Nesse tipo de Firewall, todo início de conexão é devidamente registrado (um novo estado é criado). Quando o pacote retorna, antes de iniciar o processo de avaliação das regras de acesso, o **firewall** verifica a tabela de estados, valida se há alguma conexão associada e, caso afirmativo, aceita a conexão, sem processar as regras. Do contrário, descarta o pacote.

**Firewall**: É  um elemento (software, software/hardware) de uma rede de computadores, na forma de , que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.

**Flag de recursão DNS:** É parte do cabeçalho das requisições e respostas DNS. Na requisição, indica quando um cliente deseja que o servidor DNS atue de forma recursiva quando não possuir o registro solicitado. Na resposta, indica que o servidor pode atuar como recursivo. Servidores DNS recursivos abertos(qualquer host da Internet pode fazer requisição a ele) podem ser vítimas de ataques tipo DdoS.

**Flag RST:** Quando um pacote TCP inesperado chega a um host, esse host geralmente responde enviando um pacote de Reset de volta na mesma conexão, com o flag RST ativado( 1). Isso indica ao computador receptor que o computador deve parar imediatamente de usar a conexão TCP; ele não deve enviar mais pacotes usando os números de identificação da conexão, chamados de portas, e descartar quaisquer pacotes adicionais que receber com cabeçalhos indicando que pertencem a essa conexão.

**Flag TCP:** Sinalizador TCP. Na conexão TCP, os sinalizadores são usados para indicar um determinado estado de conexão ou para fornecer algumas informações adicionais úteis, como solução de problemas ou para controlar o controle de uma determinada conexão. Os sinalizadores mais comumente usados são “SYN”, “ACK” e “FIN”.

**Gateway:** Um gateway de rede é um elemento de hardware ou software, que fornece interoperabilidade entre redes e contém dispositivos, como tradutores de protocolo. Um gateway de rede requer o estabelecimento de procedimentos mutuamente aceitáveis entre as redes que usam o gateway. Os gateways de rede, conhecidos como gateways de tradução de protocolo ou gateways de mapeamento, podem realizar conversões de protocolo para conectar redes com diferentes tecnologias de protocolo de rede Os *gateways* são distintos dos roteadores ou switches porque se comunicam usando mais de um protocolo para conectar várias redes e podem operar em qualquer uma das sete camadas Modelo OSI.

**Gbps**: Gigabits por segundo. Medida de Taxa de transferência de um circuito de dados. No caso, representa taxas da ordem de bilhões de bits por segundo.

**GUI:** *Graphical User Interface*(Interface Gráfica de Usuário).É uma forma de interface de usuário que permite a interação com dispositivos eletrônicos por meio de ícones gráficos, em vez de interfaces de usuário baseadas em texto, rótulos de comandos digitados ou navegação de texto.

**Hash:** É o valor retornado por uma função *hash*. Também chamado de valor *hash*, código *hash*, ou simplesmente *hashes*. Uma função *hash* é qualquer função que pode ser usada para mapear dados de tamanho arbitrário para valores de tamanho fixo.

**Health Check:** Literalmente, “Verificação de Saúde”. No contexto de rede e serviço de comunicação de dados, é uma ferramenta de gestão da rede, usada para identificar e enviar alertas sobre problemas que afetam a disponibilidade ou funcionalidade dos serviços. Normalmente é o monitoramento da disponibilidade de serviços, funcionalidade de interfaces de rede, status de sistemas de hardware críticos, CPU, memória ou outras estatísticas para servidores e dispositivos em uma rede.

**Honeypot:** *Pote de Mel.* Na terminologia de computador, um *honeypot* é um mecanismo de segurança de computador configurado para detectar, desviar ou, de alguma maneira, neutralizar tentativas de uso não autorizado de sistemas de informação. Geralmente, um *honeypot* consiste em dados (por exemplo, em um site da rede) que parecem ser uma parte legítima do site que parece conter informações ou um recurso de valor para os invasores, mas na verdade são isolados e monitorados e permitem o bloquear o ataque ou analisar os atacantes.

**HTTPS**:*Hypertext Transfer Protocol Secure*(Protocolo Seguro de Transferência de Hypertexto) . É uma extensão do Hypertext Transfer Protocol (HTTP). Ele é usado para comunicação segura em uma rede de computadores e é amplamente utilizado na Internet. Em HTTPS, o protocolo de comunicação é criptografado usando Transport Layer Security (TLS) ou, anteriormente, Secure Sockets Layer (SSL). O protocolo é, portanto, também conhecido como HTTP sobre TLS ou HTTP sobre SSL.

***Hub-and-Spoke***: É uma topologia de rede formada por vários nós, que falam (*Spoke*), conversam entre si através de um nó central |(*Hub*).

**Hypervisor:** Um hypervisor, ou monitor de máquina virtual, é um software ou hardware que cria e roda máquinas virtuais (VMs). O computador no qual o hypervisor roda uma ou mais VMs é chamado de máquina hospedeira (host), e cada VM é chamada de máquina convidada (guest). O hypervisor se apresenta aos sistemas operacionais convidados como uma plataforma de virtualização e gerencia a execução dos sistemas operacionais convidados.

**ICMP flood:** Inundação ICMP. É um ataque de negação de serviço que utiliza pacotes ICMP (ping), que envia pacotes ICMP o mais rápido possível sem esperar por respostas. A maioria das implementações de ping exige que o usuário tenha privilégios para especificar a opção de inundação. É mais bem-sucedido se o invasor tiver mais largura de banda do que a vítima . O invasor espera que a vítima responda com pacotes ICMP de "resposta de eco", consumindo, assim, a largura de banda de saída e de entrada. Se o sistema de destino for lento o suficiente, é possível consumir o suficiente de seus ciclos de CPU para que o usuário perceba uma redução significativa.

**ICMP:** Internet Control Message Protocol(Protocolo de Mensagem de Controle Internet)É um protocolo de suporte no conjunto de protocolos da Internet. É usado por dispositivos de rede, incluindo roteadores, para enviar mensagens de erro e informações operacionais indicando sucesso ou falha ao se comunicar com outro endereço IP, por exemplo, um erro é indicado quando um serviço solicitado não está disponível ou que um host ou roteador não poderia ser alcançado. O ICMP difere dos protocolos de transporte, como TCP e UDP, porque não é normalmente usado para trocar dados entre sistemas, nem é regularmente empregado por aplicativos de rede do usuário final (com exceção de algumas ferramentas de diagnóstico como ping e traceroute).
**IDS:** *Intrusion Detection System(*Sistema de Detecção de Intrusão). É um dispositivo ou aplicativo de software que monitora uma rede ou sistemas em busca de atividades maliciosas ou violações de políticas. Qualquer atividade de intrusão ou violação é normalmente relatada a um administrador ou coletada centralmente usando um sistema de gerenciamento de informações e eventos de segurança (**SIEM**). Um sistema **SIEM** combina saídas de várias fontes e usa técnicas de filtragem de alarme para distinguir atividades maliciosas de alarmes falsos.

**IEEE:** *Institute of Electrical and Electronics Engineers*(Instituto de Engenheiros Elétricos e Eletrônicos). É uma associação profissional para engenharia eletrônica e engenharia elétrica (e disciplinas associadas) com sede nos EUA. Foi formado em 1963 a partir da fusão do *American Institute of Electrical Engineers* e do *Institute of Radio Engineers*. Entre outras atividades, desenvolve padrões globais em uma ampla gama de indústrias, incluindo: energia e energia, tecnologia de consumo e eletrônicos de consumo, biomédica e saúde, tecnologia de aprendizagem, tecnologia da informação e robótica, telecomunicações e automação residencial, transporte, nanotecnologia, garantia da informação e muito mais.

**IETF:** *Internet Engineering Task Force*( Força Tarefa de Engenharia da Internet) É uma organização de padrões abertos, que desenvolve e promove padrões voluntários da Internet, em particular os padrões que compõem o pacote de protocolos da Internet (TCP / IP). Não tem lista de membros formal ou requisitos de adesão. Todos os participantes e gerentes são voluntários, embora seu trabalho seja geralmente financiado por seus empregadores ou patrocinadores.

**IGMP:** *Internet Group Management Protocol*. É um protocolo participante do protocolo IP e sua função é controlar os membros de um grupo de multicast IP, gerenciando os grupos de multicast controlando a entrada e saída de hosts deles.

**IKE**( IKEv1 ou IKEv2)**:** *Internet Key Exchange* (Troca de Chaves Internet) É o protocolo usado para configurar uma associação de segurança (SA) no conjunto de protocolos IPsec. O IKE usa certificados X.509 para autenticação - pré-compartilhados ou distribuídos usando DNS (de preferência com *DNSSEC*) - e uma troca de chave Diffie-Hellman para configurar um segredo de sessão compartilhado do qual as chaves criptográficas são derivadas. Além disso, uma política de segurança para cada par que se conectará deve ser mantida manualmente.

**IP Defragmentation:** Defragmentação IP. Os protocolos de rede muitas vezes precisam transportar grandes blocos de dados que são completos em si mesmos, por exemplo, ao transferir um arquivo. O protocolo subjacente pode não ser capaz de lidar com esse tamanho de bloco (por exemplo, limitação do tamanho do pacote de rede), ou é baseado em fluxo como o TCP, que não conhece blocos de dados.Nesse caso, o protocolo de rede precisa lidar com os limites do bloco e (se necessário) distribuir os dados por vários pacotes, fragmentando-o. O receptor, por sua vez, precisa de um mecanismo pra remontar os blocos. Esse mecanismo é chamado de remontagem ou defragmentação.

**IP Spoofing:** Falsificação de IP. É a criação de pacotes de protocolo da Internet (IP) com um endereço IP de origem falso, com o objetivo de representar outro sistema
de computação.

**IPFIX:** *Internet Protocol Flow Information Export* (Protocolo Internet para Fluxo de Exportação de Informação) é um protocolo **IETF**(, assim como o nome do grupo de trabalho **IETF** que define o protocolo. Ele foi criado com base na necessidade de um padrão comum e universal de exportação para informações de fluxo de protocolo da Internet de roteadores, sondas e outros dispositivos que são usados por sistemas de mediação, sistemas de contabilidade / faturamento e sistemas de gerenciamento de rede para facilitar serviços como medição, contabilidade e cobrança. O padrão IPFIX define como as informações de fluxo de IP devem ser formatadas e transferidas de um exportador para um coletor. Anteriormente, muitas operadoras de rede de dados dependiam da tecnologia NetFlow de propriedade da Cisco Systems para exportar informações de fluxo de tráfego.

**IPS:** *Intrusion prevention Systems*(Sistemas de Prevenção de Intrusão). São dispositivos de segurança de rede que monitoram as atividades da rede ou do sistema em busca de atividades maliciosas. As principais funções dos sistemas de prevenção de intrusão são identificar atividades maliciosas, registrar informações sobre esta atividade, relatá-la e tentar bloqueá-la ou interrompê-la.

**IPSEC:** *IP Security Protocol*(Protocolo de Segurança IP )é um conjunto de protocolos de rede que autentica e criptografa os pacotes de dados para fornecer comunicação criptografada segura entre dois computadores em uma rede de IP. É usado em redes privadas virtuais (VPNs).

**IPV4:** É a quarta versão do protocolo da Internet (IP). É um dos principais protocolos de métodos de interconexão de redes, baseados em padrões na Internet e em outras redes comutadas por pacotes. IPv4 foi a primeira versão implantada para produção na SATNET em 1982 e na ARPANET em janeiro de 1983. Ele ainda roteia a maior parte do tráfego da Internet hoje, [1] apesar da implantação de um protocolo sucessor, o IPv6.

**IPV6:** É a versão mais recente do Protocolo da Internet (IP). IPv6 foi desenvolvido pela *Internet Engineering Task Force* (IETF) para lidar com o problema há muito antecipado de esgotamento de endereços IPv4.

**ISP:** *Internet Service Provider* ( Provedor de Serviços de Internet). Um provedor de serviços de Internet (ISP) é uma organização que fornece serviços para acessar, usar ou participar da Internet.

**Jitter:** É uma variação estatística do atraso na entrega de dados em uma rede, ou seja, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados. Observa-se ainda que uma variação de atraso elevada produz uma recepção não regular dos pacotes.

**LACP:** *Link Aggregation Control Protocol* ( Protocolo de Controle de Agregação de Link) Fornece um método para controlar o agrupamento de várias portas físicas juntas para formar um único canal lógico. O LACP permite que um dispositivo de rede negocie um agrupamento automático de links enviando pacotes LACP para o par (dispositivo conectado diretamente que também implementa LACP). O LACP é regulado pela norma IEEE 802.3.

**LAN:** *Local Area Network*. Rede de Abrangência Local ou Rede Local. Uma rede local é uma rede que interconecta computadores em uma área limitada, como uma residência, escola, laboratório, campus universitário ou prédio de escritórios.

**Latência:** No contexto da comunicação de dados, latência é o tempo de resposta a uma requisição de um dispositivo a outro em uma rede. Normalmente, para efeito de métrica de performance de rede, usa-se o tempo de resposta de requisições padrão de protocolos específicos para esse fim, como ICMP, TWAMP e OWAMP etc.

**LDAP:** O Lightweight Directory Access Protocol (Protocolo Leve de Acesso a Diretórios) é um protocolo aberto, independente de fornecedor, e padrão da indústria para acessar e manter serviços de informação de diretório distribuídos em uma rede IP. Os serviços de diretório desempenham um papel importante no desenvolvimento de aplicativos de intranet e Internet, permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicativos em toda a rede.

**Malware Point-of-Sale(POS Malware):** Malware de ponto de venda.É geralmente um tipo de software malicioso (malware) que é usado por cibercriminosos para direcionar pontos de venda (POS) e terminais de pagamento com a intenção de obter informações de cartão de crédito e débito. dados da faixa 1 ou faixa 2 e até mesmo o código CVV, por vários ataques man-in-the-middle(MITM), que é a interceptação do processamento no sistema de ponto de caixa de varejo de venda. A abordagem mais simples, ou mais evasiva, é a varredura de RAM(*RAM-Scraping - Radom Acces Memory Scraping*), acessando a memória do sistema e exportando as informações copiadas por meio de um *trojan* de acesso remoto (RAT), pois isso minimiza qualquer violação de software ou hardware, potencialmente sem deixar pegadas.

**Malware:** É qualquer software projetado intencionalmente para causar danos a um computador, servidor, cliente ou rede de computadores (em contraste, o software que causa danos não intencionais devido a alguma deficiência é normalmente descrito como um bug de software).

**Mbps**: Megabits por segundo. Medida de Taxa de transferência de um circuito de dados. No caso, representa taxas da ordem de milhões de bits por segundo.

**MD5:** Message-Digest algorithm 5(Algoritmo de Compilação de Mensagem 5) É um algoritmo de *hash* de 128 bits unidirecional desenvolvido pela RSA Data Security, Inc., usado por softwares com protocolo ponto-a-ponto (P2P), verificação de integridade e logins.

**MIB-II**: É a segunda versão da MIB. para uso com protocolos de gerenciamento de rede, em redes TCP / IP baseadas.
**MIB:** *Management Information Base*(Base de Informações de Gerenciamento) É um banco de dados usado para gerenciar as entidades em uma rede de comunicação. Mais frequentemente associado ao protocolo **SNMP** , o termo também é usado de forma mais genérica em contextos como no modelo de gerenciamento de rede OSI / ISO. Embora pretenda se referir à coleção completa de informações de gerenciamento disponíveis em uma entidade, é frequentemente usado para se referir a um subconjunto específico, mais corretamente referido como módulo MIB.

**Modelo OSI**: O Modelo ***OSI*** (***Open System Interconnection***) é um modelo de rede de computador, referência da ISO, dividido em camadas de funções, criado em 1971 e formalizado em 1983, com objetivo de ser um padrão, para protocolos de comunicação entre os mais diversos sistemas em uma rede local , garantindo a comunicação entre dois sistemas computacionais (*end-to-end*).

**MPLS**: *Multiprotocol Label Switching* (em português, "Comutação de Rótulos Multiprotocolo") é um mecanismo em redes de telecomunicações que direciona dados de um nó da rede para o próximo nó baseado em rótulos de menor caminho em vez de endereços de rede longos, evitando consultas complexas em uma tabela de roteamento.

**Multi-Tenant:** Múltiplos Inquilinos.O termo refere-se a aplicações com capacidade de "multilocação " (*multitenancy*) Trata-se de uma arquitetura de software na qual uma única instância do software é executada em um servidor e atende a vários locatários(inquilinos). Os sistemas projetados dessa maneira costumam ser chamados de compartilhados (em contraste com dedicados ou isolados). Um locatário é um grupo de usuários que compartilham um acesso comum com privilégios específicos para a instância do software. Com uma arquitetura *multitenant,* um aplicativo de software é projetado para fornecer a cada locatário um compartilhamento dedicado da instância - incluindo seus dados, configuração, gerenciamento de usuário, funcionalidade individual do locatário e propriedades não funcionais. A multilocação contrasta com arquiteturas de múltiplas instâncias, onde instâncias de software separadas operam em nome de diferentes locatários.

**NAT de Destino:** O NAT de destino altera o endereço de destino dos pacotes que passam pelo dispositivo que faz tradução. É usado principalmente para redirecionar pacotes de entrada com um endereço externo ou porta de destino para um endereço IP interno ou porta dentro da rede.

**NAT de Origem:** O NAT de origem é mais comumente usado para converter um endereço IP privado em um endereço público roteável . O NAT de origem altera o endereço de origem dos pacotes que estão saindo do dispositivo que faz a traduçã. É usado para permitir que hosts com endereços IP privados acessem uma rede pública. Permite que as conexões sejam iniciadas apenas para conexões de rede de saída - por exemplo, de uma rede privada para a Internet

**NAT dinâmico (*Many-to-Many*):** NAT Dinâmico(muitos para muitos). Em um NAT dinâmico, vários hosts com endereços IP privados podem compartilhar uma quantidade igual ou menor de endereços IP públicos, configurando um mapeamento muitos-para-muitos assimétrico. No NAT Dinâmico o número da porta não muda, apenas o endereço IP. O que significa que um único endereço IP público não pode ser compartilhado entre vários hosts internos ao mesmo tempo.

**NAT estático (1-to-1):** NAT estático(1-para-1) mapeia o tráfego de rede de um endereço IP externo estático para um endereço IP interno ou rede. Ele cria uma tradução estática de endereços reais para endereços mapeados. O NAT estático define um mapeamento um para um de uma sub-rede IP para outra sub-rede IP. O mapeamento inclui a tradução do endereço IP de destino em uma direção e a tradução do endereço IP de origem na direção reversa. NAT estático é **bidirecional.**

**NAT:** *Network Address Translation* (Tradução/Conversão de Endereço de Rede). É um método de remapeamento de um espaço de endereço IP em outro, modificando as informações de endereço de rede no cabeçalho IP dos pacotes enquanto eles estão em trânsito por um dispositivo

de roteamento de tráfego.

**NAT46:** NAT46 é um mecanismo de transição de IPv4 para IPv6 que fornece uma maneira para os nós finais IPv6 se comunicarem com os nós finais IPv4 e vice-versa. Isso é obtido usando uma combinação de tradução de endereço de rede e tradução de protocolo.

**NAT64:** NAT64 é um mecanismo de transição IPv6 que facilita a comunicação entre hosts IPv6 e IPv4 usando uma forma de conversão de endereço de rede (NAT).
O ***gateway*** NAT64 é um tradutor entre os protocolos IPv4 e IPv6, para a qual precisa de pelo menos um endereço IPv4 e um segmento de rede IPv6 compreendendo um espaço de endereço de 32 bits.

**NetFlow:** NetFlow é um recurso que foi introduzido nos roteadores Cisco por volta de 1996 que fornece a capacidade de coletar tráfego de rede IP conforme ele entra ou sai de uma interface. Ao analisar os dados fornecidos pelo NetFlow, um administrador de rede pode determinar coisas como a origem e o destino do tráfego, a classe de serviço e as causas do congestionamento.

**Netstream:** O NetStream é uma aplicação que coleta estatísticas de pacotes com base nos fluxos. Ele faz uma amostra do tráfego de entrada e saída em cada interface, classifica o tráfego de rede com base nos principais fatores dos pacotes (por exemplo, endereço IP de origem, endereço IP de destino, número de porta de origem e número de porta de destino) e filtros, bem como dados agregados. Os usuários podem personalizar modelos para classificar e coletar estatísticas sobre o tráfego da rede.

**Network Prefix Translation (NPTv6 ou NAT66) :** *Tradução de Prefixo de Rede.* Quando um pacote IPv6 está indo de uma rede interna para a rede externa, a tradução de prefixo de rede de origem sem estado para IPv6 (NPTv6) mapeia o prefixo IPv6 do endereço de origem para um prefixo IPv6 de uma rede externa. Quando um pacote IPv6 está vindo da rede externa para a rede interna, o NPTv6 mapeia o prefixo IPv6 do endereço de destino para o prefixo IPv6 da rede interna. O NPTv6 usa um algoritmo para traduzir os endereços e não precisa manter o estado de cada nó ou de cada fluxo no tradutor. O NPTv6 também elimina a necessidade de recalcular a soma de verificação da camada de transporte.

**NGFW:** *Next-Generation Firewall* (Firewall de próxima geração). É uma parte da terceira geração de tecnologia de firewall, combinando um firewall tradicional com outras funções de filtragem de dispositivos de rede, como um firewall de aplicativo usando inspeção profunda de pacotes (DPI) , um sistema de prevenção de intrusão (IPS). Outras técnicas também podem ser empregadas, como inspeção de tráfego criptografado TLS / SSL, filtragem de site, gerenciamento de QoS / largura de banda, inspeção de antivírus etc.

**NOC:** *Network Operations Center*(Centro de Operações de Rede)Também conhecido como um "centro de gerenciamento de rede", é um ou mais locais a partir dos quais o monitoramento e controle de rede, ou gerenciamento de rede, é exercido. Os NOCs são implementados por organizações empresariais, serviços públicos, universidades, agências governamentais etc, que supervisionam ambientes de rede complexos que exigem alta disponibilidade. O pessoal do NOC é responsável por monitorar uma ou várias redes para certas condições que podem exigir atenção especial para evitar degradação do serviço. As organizações podem operar mais de um NOC, seja para gerenciar redes diferentes ou para fornecer redundância geográfica no caso de um local ficar indisponível.

**NTP:** *Network Time Protocol(Protocolo de Horário de Rede)*O NTP é um protocolo para sincronização dos relógios dos computadores. É utilizado para sincronização do relógio de um conjunto de computadores e dispositivos em redes de dados com latência variável. O NTP permite manter o relógio de um computador sincronizado com a hora sempre certa e com grande exatidão. O cliente pode, mas não precisa, ser autenticado por meio de um certificado PKI assinado pela CA para o servidor. Isso simplifica muito o procedimento de configuração, pois não é necessário um certificado em todos os clientes.

O IPsec inclui protocolos para estabelecer autenticação mútua entre agentes no início de uma sessão e negociação de chaves criptográficas para usar durante a sessão.

**On-premises:** *Nas Instalações*. O software instalado em computadores nas instalações da pessoa ou organização que usa o software, em vez de uma instalação remota, como um datacenter ou nuvem.

**ORQUESTRADOR:** É o elemento da arquitetura SD-WAN responsável programação de comportamentos automatizados, a fim de coordenar os elementos de hardware e software de rede necessários para oferecer suporte a aplicativos e serviços. A orquestração SD-WAN pode começar com pedidos de serviço ao cliente, gerados por tarefas manuais ou ações orientadas ao cliente, como o pedido de um serviço por meio de um site. O aplicativo ou serviço usaria a tecnologia de orquestração para fornecer o serviço. Isso pode exigir a configuração de camadas de rede virtual, virtualização baseada em servidor ou serviços de segurança, como um túnel criptografado.

**OSPF**: Open Shortest Path First. É um protocolo de roteamento para redes IP.

**OWAMP:** *One-Way Active Measurement Protocol* ( Protocolo de medição ativa bidirecional). O protocolo OWAMP faz parte de um conjunto de normas de medição conhecidas como IPPM (*IP Performance Metrics – Métricas de Perfomance IP*).O objetivo do protocolo é permitir a interoperabilidade dos equipamentos de rede no que diz respeito a forma de medir o tempo de propagação de mensagens entre origem e destino. Uma das motivações para o uso desse protocolo é a dificuldade de obter-se tais medições. Medições como o RTT (*Round Trip Time*) fornecem informação do tempo de ida e volta do tráfego, não possibilitando que seja identificada a direção em que algum tipo de congestionamento possa estar acontecendo, uma vez que o RTT fornece a soma dos dois tempos (ida e volta): assim, o RTT é uma medição *Two-Way*. Para possibilitar medições *One-Way*, o OWAMP baseia-se na existência de uma referência de tempo precisa nos dispositivos origem e destino dos pacotes de medição. Essa referência, em geral, é um GPS (*Global Positioning System*) ou o acesso a um servidor NTP primário de tempo.

**PAT:** *Port Address Translation* (Tradução de Endereço/número de Porta): É uma extensão da tradução de endereço de rede NAT que permite que vários dispositivos em uma LAN sejam mapeados para um único endereço IP público, a fim de conservar os endereços IP. O servidor que faz o NAT atribui a cada cliente um número de porta que é anexado ao endereço IP interno, dando a cada computador um endereço IP exclusivo, discriminado pelo número da porta.

**Payload:** *Carga útil*. Em computação e telecomunicações, a carga útil é a parte dos dados transmitidos que é a mensagem real pretendida. Cabeçalhos e metadados são enviados apenas para permitir a entrega de carga útil.

**PCAP:** *Packet Capture* (Captura de Pacote). É uma API para captura de tráfego de rede. É utilizada por softwares de monitoramento de rede.

**PCI:***Payment Card Industry.* O Padrão de segurança de dados do setor de cartões de pagamento é um padrão de segurança da informação para organizações que
lidam com cartões de crédito.

**PE:***Provider Edge*(Borda do Provedor). É o roteador que está localizado na rede do provedor de telecomunicação, e que está diretamente conectado ao CE(Customer Edge).

**PEAP:** Protected EAP(EAP Protegido). É um protocolo que encapsula o protocolo de autenticação extensível (EAP) em um túnel TLS (Transport Layer Security) criptografado e autenticado. O objetivo é corrigir deficiências no EAP; O EAP assumiu um canal de comunicação protegido, como aquele fornecido pela segurança física, portanto, não foram fornecidos recursos para proteção da conversa do EAP.

**Peer-to-Peer:** A computação ponto a ponto (P2P) é uma arquitetura de aplicativo distribuída que particiona tarefas ou cargas de trabalho entre pares. Os pares são participantes igualmente privilegiados e equipotentes na aplicação. Diz-se que eles formam uma rede ponto a ponto de nós.

**PIM-DM:** *Protocol Independent Multicast – Dense-Mode*( Protocolo de Multicast Independente – Modo Denso)O Modo Denso PIM (PIM-DM) usa roteamento multicast denso. Ele constrói implicitamente árvores de caminho mais curto inundando todo o domínio de tráfego multicast e, em seguida, podando os ramos da árvore onde não há receptores presentes. O PIM-DM é simples de implementar, mas geralmente tem propriedades de dimensionamento ruins.

**PIM-SM:** *Protocol Independent Multicast – Sparse-Mode*( Protocolo de Multicast Independente – Modo Esparso). É um protocolo para o roteamento eficiente de pacotes de Protocolo de Internet (IP) para grupos de multicast que podem abranger internets de área ampla e entre domínios. O protocolo é denominado independente de protocolo porque não depende de nenhum protocolo de roteamento unicast específico para descoberta de topologia, e modo esparso porque é adequado para grupos onde uma porcentagem muito baixa de nós (e seus roteadores) assinará a sessão multicast. Ao contrário dos protocolos de roteamento multicast de modo denso anteriores, que inundavam pacotes pela rede e, em seguida, removiam ramos onde não havia receptores, o PIM-SM constrói explicitamente uma árvore de cada remetente para os receptores no grupo multicast.

**PKI:** *Public Key Infrastructure***(** Infraestrutura de Chave Pública) É um conjunto de funções, políticas, hardware, software e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais e gerenciar criptografia de chave pública. O objetivo de uma PKI é facilitar a transferência eletrônica segura de informações para uma série de atividades de rede, como e-commerce, internet banking e e-mail confidencial.

**Policy-Based Forwarding:** *Encaminhamento Baseado em Políticas.* As regras permitem que o tráfego tome um caminho alternativo a partir do próximo salto especificado na tabela de rotas. Normalmente usadas para especificar uma interface de saída por motivos de segurança ou desempenho.

**Policy-Based Routing:** *Roteamento Baseado em Políticas* . Em rede de computadores, o roteamento baseado em políticas (PBR) é uma técnica usada para tomar decisões de roteamento com base nas políticas definidas pelo administrador da rede.

**Probe:** No contexto de rede e das comunicações de dados, probe é mecanismo para examinar, verificar a rede. Em geral, há dois tipos de probe de rede. Os primeiros são plug-ins de software que vêm integrados à ferramenta de monitoramento de rede. O segundo tipo é instalado separadamente no equipamento que você deseja monitorar. O principal trabalho de ambos os tipos de probes é falar com os dispositivos de rede e trazer os dados ao aplicativo de monitoramento de rede, em tempo real.

**Provedor de Identidade:** Um provedor de identidade é um serviço que cria, mantém e gerencia informações de identidade enquanto fornece serviços de autenticação para aplicativos confiáveis dentro de uma rede distribuída. Os provedores de identidade oferecem autenticação de usuário como um serviço. Aplicativos de terceiros confiáveis, como aplicativos da web, terceirizam a etapa de autenticação do usuário para um provedor de identidade confiável. Um provedor de identidade é um provedor confiável que permite que você use logon único para acessar outros sites. O logon único aumenta a usabilidade, reduzindo a fadiga da senha. Ele também fornece melhor segurança ao diminuir a superfície de ataque potencial. Os provedores de identidade podem facilitar as conexões entre os recursos de computação em nuvem e os usuários, diminuindo assim a necessidade de reautenticação dos usuários ao usar aplicativos móveis e de roaming.

**Proxy:** *Procurador, representante.* No contexto de rede de computadores, o proxy é um elemento de hardware e/ou software que atua como um intermediário para solicitações de clientes que buscam recursos de servidores que fornecem esses recursos. Um proxy, portanto, funciona em nome do cliente ao solicitar serviço, mascarando potencialmente a verdadeira origem da solicitação para o servidor de recursos.

**QoS:** *Quality of Service*(Qualidade de Serviço). No contexto das redes de computadores e outras redes de telecomunicações comutadas por pacotes, a qualidade do serviço se refere à priorização do tráfego e aos mecanismos de controle de reserva de recursos, e não à qualidade do serviço alcançada. Qualidade de serviço é a capacidade de fornecer diferentes prioridades a diferentes aplicativos, usuários ou fluxos de dados, ou de garantir um determinado nível de desempenho a um fluxo de dados.

**Radius:** *Remote Authentication Dial-In User Service(Serviço de Autenticação Remota de Usuário Discado)* é um protocolo de rede, operando na porta 1812,
que fornece gerenciamento centralizado de autenticação, autorização e contabilidade (Authentication, Authorization, and Accounting , ou AAA ou Triple A)
para usuários que se conectam e usam um serviço de rede.

**RAID1:** Redundant Array of Independent Disks ( Conjunto Redundante de Discos Independentes)É uma tecnologia de virtualização de armazenamento de dados que combina vários componentes de unidade de disco físico em uma ou mais unidades lógicas para fins de redundância de dados, melhoria de desempenho, ou ambos. Originalmente havia 5 níveis de redundância, o RAID1 especificamente faz apenas o espelhamento dos dados em duas ou mais unidades físicas.

**Rede TOR**: **Tor** é um software livre e de código aberto que proporciona a comunicação anônima e segura ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade. O nome é derivado de um acrônimo do projeto original do software chamado "The Onion Router"(O Roteador Cebola). O Tor direciona o tráfego da Internet por meio de uma rede sobreposta livre e de alcance mundial, consistindo de mais de sete mil retransmissores, para ocultar a localização e utilização do usuário de qualquer pessoa que realize vigilância de rede ou análise de tráfego. O uso do Tor dificulta o rastreamento da atividade da Internet para o usuário: isso inclui visitas a sites, postagens online, mensagens instantâneas e outras formas de comunicação. O uso pretendido do Tor é proteger a privacidade pessoal de seus usuários, bem como sua liberdade e capacidade de conduzir comunicação confidencial, mantendo suas atividades na Internet não monitoradas.

**RIP:** Routing Information Protocol. É um padrão para troca de informações entre os *gateways* e *hosts* de roteamento.

**SAML:** *Security Assertion Markup Language* (Linguagem de marcação para declaração de segurança) É um padrão aberto para troca de dados de autenticação e autorização entre as partes, em particular, entre um provedor de identidade e um provedor de serviços. SAML é uma linguagem de marcação baseada em **XML** para asserções de segurança (declarações que os provedores de serviço usam para tomar decisões de controle de acesso)

**SD-WAN**: Software Defined-Wide Area Network. Rede de longa distância definida por software.

**Serviço de Diretório:** Em computação, um serviço de diretório ou serviço de nomes mapeia os nomes dos recursos de rede para seus respectivos endereços de rede. É uma infraestrutura de informação compartilhada para localizar, gerenciar, administrar e organizar itens do dia a dia e recursos de rede, que podem incluir volumes, pastas, arquivos, impressoras, usuários, grupos, dispositivos, números de telefone e outros objetos. Um serviço de diretório é um componente crítico de um sistema operacional de rede. Um servidor de diretório ou servidor de nomes é um servidor que fornece esse serviço. Cada recurso da rede é considerado um objeto pelo servidor de diretório. As informações sobre um determinado recurso são armazenadas como uma coleção de atributos associados a esse recurso ou objeto.

**sFTP:** SSH File Transfer Protocol (Protocolo de transferência de arquivo sobre SSH) é um protocolo de rede que fornece acesso a arquivos, transferência e gerenciamento de arquivos em qualquer fluxo de dados confiável. Ele foi projetado pela Internet Engineering Task Force (IETF) como uma extensão do protocolo Secure Shell (SSH) versão 2.0 para fornecer recursos de transferência segura de arquivos. O IETF Internet Draft afirma que, embora esse protocolo seja descrito no contexto do protocolo SSH-2, ele pode ser usado em uma série de aplicações diferentes, como transferência segura de arquivos por Transport Layer Security (TLS) e transferência de informações de gerenciamento em aplicações VPN. Esse protocolo pressupõe que seja executado em um canal seguro, como SSH, que o servidor já tenha autenticado o cliente e que a identidade do usuário cliente esteja disponível para o protocolo.

**SHA-2**(inclui *SHA256, SHA384 e SHA512*). *Secure Hash Algorithm-2* (Padrão de Dispersão Seguro*). **SHA-2.*** SHA-2 é um conjunto de funções hash criptográficas projetadas pela NSA (*National Security Agency* - Agência de Segurança Nacional )dos EUA. SHA-2 inclui mudanças significativas de seu antecessor, SHA-1. A família SHA-2 é composta por seis funções hash com resumos (valores de hash) que são de 224, 256, 384 ou 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. A função hash SHA-2 é implementada em algumas aplicações de segurança e protocolos amplamente usados, incluindo TLS e SSL, SSH, e Ipsec. SHA-1 e SHA-2 são os algoritmos de hash seguros exigidos por lei para o uso em certas aplicações do governo dos EUA, incluindo o uso dentro de outros algoritmos e protocolos criptográficos, para a proteção da informação.

**SHA1(ou SHA-1):** *Secure Hash Algorithm* -1(Padrão de Dispersão Seguro*).* Em criptografia, SHA1 é uma função de dispersão criptográfica (ou função hash criptográfica).SHA-1 é a mais amplamente utilizada das funções de dispersão SHA existentes, sendo empregada em vários protocolos e aplicações incluindo TLS e SSL e Ipsec. SHA-1 produz um valor de dispersão de 160 bits (20 bytes) conhecido como resumo da mensagem. Um valor de dispersão SHA-1 é normalmente tratado como um número hexadecimal de 40 dígitos.

**Shell:** Em computação, um *shell* é uma interface de usuário para acesso aos serviços de um sistema operacional. Em geral, os *shells* do sistema operacional usam uma interface de linha de comando (CLI) ou uma interface gráfica de usuário (GUI), dependendo da função do computador e da operação específica. É chamado de shell ( concha )porque é a camada mais externa ao redor do sistema operacional.

**SIEM:** *Security Information and Event Management* (Segurança de informações e gerenciamento de eventos ) é uma subseção dentro do campo de segurança de computadores, onde produtos e serviços de software combinam gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Eles fornecem análise em tempo real de alertas de segurança gerados por aplicativos e hardware de rede. Os fornecedores vendem SIEM como software, como aparelhos ou como serviços gerenciados; esses produtos também são usados para registrar dados de segurança e gerar relatórios para fins de conformidade.

**SNMP:***Simple Network Management Protocol* (Protocolo Simples de Gerência de Rede) é um protocolo padrão da Internet para gerenciamento de dispositivos em redes IP.

**SNTP**: *Simple Network Time Protocol(Protocolo de Horário de Rede Simplificado)* O SNTP é uma versão simplificada do NTP, que não implementa alguns de seus algorítmos. O SNTP geralmente é utilizado quando há limitações de recursos de hardware, como por exemplo em dispositivos embarcados. Com o SNTP a exatidão alcançada no tempo é normalmente menor do que com o NTP.

**SpyWare:** *Spyware* descreve software com comportamento malicioso que visa coletar informações sobre uma pessoa ou organização e enviar tais informações a outra entidade de uma forma que prejudique o usuário; por exemplo, violando sua privacidade ou colocando em risco a segurança de seu dispositivo. Esse comportamento pode estar presente tanto em *malware* quanto em software legítimo. Os sites também podem se envolver em comportamentos de *spyware*, como rastreamento da web. Dispositivos de hardware também podem ser afetados.

**SSH:***Secure Shell (SSH)* é um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura.

**SSL: *Secure Socket Layer* . É** um protocolo de segurança. Ele cria um canal criptografado entre um servidor web e um navegador ,para garantir que todos os dados transmitidos sejam sigilosos e seguros.

**SSO:** Single Sign-on( Logon único). É um esquema de autenticação que permite a um usuário fazer logon com um único ID(identificador) e senha em qualquer um dos vários sistemas relacionados, mas independentes, aos quais ele tem acesso.

**SYN Flood:** (Inundação de SYN) É uma forma de ataque de negação de serviço em que um invasor inicia rapidamente uma conexão com um servidor sem finalizar a conexão. O servidor precisa gastar recursos esperando por conexões abertas pela metade, o que pode consumir recursos suficientes para fazer com que o sistema não responda ao tráfego legítimo. O pacote que o invasor envia é o pacote SYN, uma parte do ***handshake****( Um processo automatizado de negociação entre dois participantes de uma comunicação, feito por meio da troca de informações que estabelece os protocolos da conexão, realizado no início desta)* de três vias do TCP, usado para estabelecer uma conexão.

**Tag:** *Marca*. Em sistemas de informação, uma marca é uma palavra-chave ou termo atribuído a uma informação (como um marcador da Internet, imagem digital, registro de banco de dados ou arquivo de computador). Ajuda a descrever um item e permite que ele seja encontrado novamente navegando ou pesquisando na estrutura onde a informação está.

**TCP CONNECT:** Técnica utilizada para verificação do estado das portas TCP de um host.

**TCP/IP** . Também chamado de pilha de protocolos TCP/IP, é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (*Transmission Control Protocol* - Protocolo de Controle de Transmissão) e o IP (*Internet Protocol* – Protocolo de Internet). O conjunto de protocolos pode ser visto como um modelo de camadas , onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior.

**Threat Prevention**: Prevenção de Ameaça. Mecanismo ou procedimentos para prevenir, detectar e tratar ameaças à rede, tais como malwares, vírus, ataques, acessos indevidos etc

**Throughput:** *Taxa de transferência*. Em redes de comunicação, *throughput* é a quantidade de dados transferidos de um ponto a outro da rede, a quantidade de dados processados ou que passam por um nó da rede, em um determinado espaço de tempo, tendo como unidades básicas

de medidas o Kbps (Kilobits por segundo), Mbps (Megabits por segundo) e o Gbps (Gigabits por segundo). O *throughput* pode ser traduzido como a taxa de transferência efetiva de um sistema. Essa taxa menor que a taxa de entrada devido às perdas e atrasos no sistema.

**TLS:***Transport Layer Security*(Segurança de Camada de Transporte) é um protocolo criptográfico projetado para fornecer segurança de comunicações em uma rede de computadores. Várias versões dos protocolos são amplamente utilizadas em aplicativos como navegação na web, e-mail, mensagens instantâneas e voz sobre IP (VoIP). Os sites podem usar TLS para proteger todas as comunicações entre seus servidores e navegadores da web.

**Token:** um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB.

**Traffic Shaping:** Modelagem de Tráfego. A modelagem de tráfego é uma técnica de gerenciamento de largura de banda usada em redes de computadores que atrasa alguns ou todos os datagramas para colocá-los em conformidade com um perfil de tráfego desejado. A modelagem de tráfego é usada para otimizar ou garantir o desempenho, melhorar a latência ou aumentar a largura de banda utilizável para alguns tipos de pacotes, atrasando outros tipos.

**Traffic shaping:** Modelamento de Tráfego: É uma técnica de gerenciamento de largura de banda usada em redes de computadores, que atrasa os pacotes para colocá-los em conformidade com um perfil de tráfego desejado. A modelagem de tráfego é usada para otimizar ou garantir o desempenho, melhorar a latência ou aumentar a largura de banda utilizável para alguns tipos de pacotes, atrasando outros tipos.

**Trojan de Acesso Remoto:** *RAT(Remote Access Trojan).* Um trojan de acesso remoto (às vezes chamado de *creepware* ) é um tipo de malware que controla um sistema por meio de uma conexão de rede remota. Embora o compartilhamento de área de trabalho e a administração remota tenham muitos usos legais, "RAT" denota atividade criminosa ou maliciosa. Um RAT é normalmente instalado sem o conhecimento da vítima, geralmente como carga útil de um cavalo de Tróia, e tentará ocultar sua operação da vítima e de software de segurança e outro software antivírus.

**Trojan:** Na computação, um cavalo de Tróia, ou trojan, é qualquer *malware* que engana os usuários sobre sua verdadeira intenção. O termo é derivado da história da Grécia Antiga do enganador Cavalo, presente dos gregos, que levou à queda da cidade de Tróia.

**TWAMP:** *Two-Way Active Measurement Protocol*( Protocolo de medição ativa bidirecional) O protocolo TWAMP é um processo de monitoramento que se baseia no *One-Way Active Measurement Protocol* (OWAMP) com a adição da medição de performance de ida e volta e métricas *two-way*(bidirecional) para redes baseadas em IP. TWAMP traz um método flexível para medição precisa de performances unidirecional entre dois *endpoints* (Ponta, final, ponto terminal. Neste contexto, as duas pontas de uma conexão TCP) que tenham suporte para TWAMP, independente do tipo de dispositivo ou vendedor.

**UDP Flood:** Inundação UDP. É um ataque de negação de serviço volumétrico que usa o protocolo UDP, um protocolo sem sessão / conexão. Usar o UDP para ataques de negação de serviço não é tão direto quanto com TCP. No entanto, um ataque de inundação UDP pode ser iniciado enviando um grande número de pacotes UDP para portas aleatórias em um host remoto. Como resultado, o host remoto, verificar se o aplicativo está escutando nessa porta. Ao ver que nenhum aplicativo está escuntando, ele responde com um pacote de destino ICMP inacessível. Assim, para um grande número de pacotes UDP, o sistema vitimado será forçado a enviar muitos pacotes ICMP, eventualmente tornando-o inacessível para outros clientes. O invasor também podem falsificar o endereço IP dos pacotes UDP, garantindo que os pacotes de retorno ICMP em excesso não os alcancem, e anonimizando seus locais de rede. A maioria dos sistemas operacionais atenua essa parte do ataque, limitando a taxa de envio das respostas ICMP.

**UDP:** User Datagram Protocol ( Protocolo de Datagrama do Usuário ). É um dos membros principais do conjunto de protocolos da Internet. Com o UDP, os aplicativos de computador podem enviar mensagens, neste caso chamadas de datagramas, para outros hosts em uma rede de protocolo da Internet (IP). Comunicações anteriores não são necessárias para configurar canais de comunicação ou caminhos de dados. UDP usa um modelo de comunicação sem conexão simples com um mínimo de mecanismos de protocolo

**URL:** *Uniform Resource Locator* ( Localizador Uniforme de Recursos) , coloquialmente denominado endereço da web, é uma referência a um recurso da web que especifica sua localização em uma rede de computadores e um mecanismo para recuperá-lo.

**UTM:***Unified Threat Management*(Gerenciamento Unificado de Ameaças). O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede.

**VLAN:** *Virtual LAN*( LAN Virtual). Uma VLAN é qualquer domínio de *broadcast* particionado e isolado em uma rede de computadores na camada de enlace de dados (camada OSI 2). Neste contexto, virtual se refere a uma rede física, material, mapeada para uma rede lógica. Desta forma, em uma mesma rede física, é possível criar várias VLANs agregando dispositivos que não estejam fisicamente em um mesmo segmento de rede.

**VM:***Virtual Machine*(Máquina Virtual). É uma emulação de um sistema de computador. As máquinas virtuais são baseadas em arquiteturas de computador e fornecem a funcionalidade de um computador físico. Suas implementações podem envolver hardware especializado, software ou uma combinação deles.

**VPN:** *Virtual Private Network*(Rede Privada Virtual). É uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando Em resumo, cria uma conexão segura e criptografada, que pode ser considerada como um túnel. Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem
a confidencialidade , autenticidade e integridade necessárias para garantir a privacidade das comunicações requeridas.

**VRF**: *Virtual Routing and Forwarding*(Roteamento e Encaminhamento Virtual). Mecanismo que permite o uso de várias tabelas de roteamento em um único roteador. Pode trazer tanto a segurança, quanto os benefícios de eficiência , pois possibilita a execução de várias redes lógicas com espaços de endereços inteiramente separados, sem a necessidade de vários equipamentos de rede.

**VRRP:** *Virtual Router Redundancy Protocol* .É um protocolo tolerante a falhas, que permite que vários roteadores sejam agrupados em um roteador virtual, também chamado de grupo de backup VRRP. Em circunstâncias normais, o roteador *Master* no grupo de backup VRRP funciona como um gateway padrão e fornece serviços de acesso aos usuários. Se o roteador *Master* falhar, o VRRP elege um roteador de *backup* do grupo de backup VRRP para fornecer serviços de acesso aos usuários.

**VSAT:** *Very Small Aperture Terminal* (Terminal de Diâmetro Muito Pequeno) é uma estação terrestre de comunicação bi-direcional via satélite, com uma antena parabólica menor do que 3 metros. A maioria das antenas VSAT variam desde 75 cm a 1,2 m.

**Wizard:** É um assistente de software ou assistente de configuração, um tipo de interface de usuário que apresenta uma sequência de caixas de diálogo que o conduzem por uma série de etapas bem definidas. Tarefas complexas, executadas com pouca frequência ou desconhecidas podem ser mais fáceis de executar usando um assistente.

**Worm:** Worm é um malware autônomo que se replica para se espalhar para outros computadores. Ele geralmente usa uma rede de computadores para se espalhar, contando com falhas de segurança no computador de destino para acessá-lo. Ele usará esta máquina como um host para verificar e infectar outros computadores. Quando esses novos computadores invadidos por *worm* forem controlados, o worm continuará a verificar e infectar outros computadores usando esses computadores como hosts, e esse comportamento continuará. Os *worms* quase sempre causam pelo menos algum dano à rede, mesmo que apenas por
consumir largura de banda.

**XML:** *Extensible Markup Language* (Linguagem de Marcação Extensível) é uma linguagem de marcação que define um conjunto de regras para codificação de documentos em um formato que pode ser lido por humanos e por computadores. A Especificação XML 1.0 do World Wide Web Consortium(Consórcio WWW) de 1998 e várias outras especificações relacionadas - todas elas padrões abertos gratuitos - definem XML. Os objetivos de design do XML enfatizam a simplicidade, generalidade e usabilidade na Internet.