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

ANEXO I - TERMO DE REFERÊNCIA

1. **ESPECIFICAÇÕES TÉCNICAS**

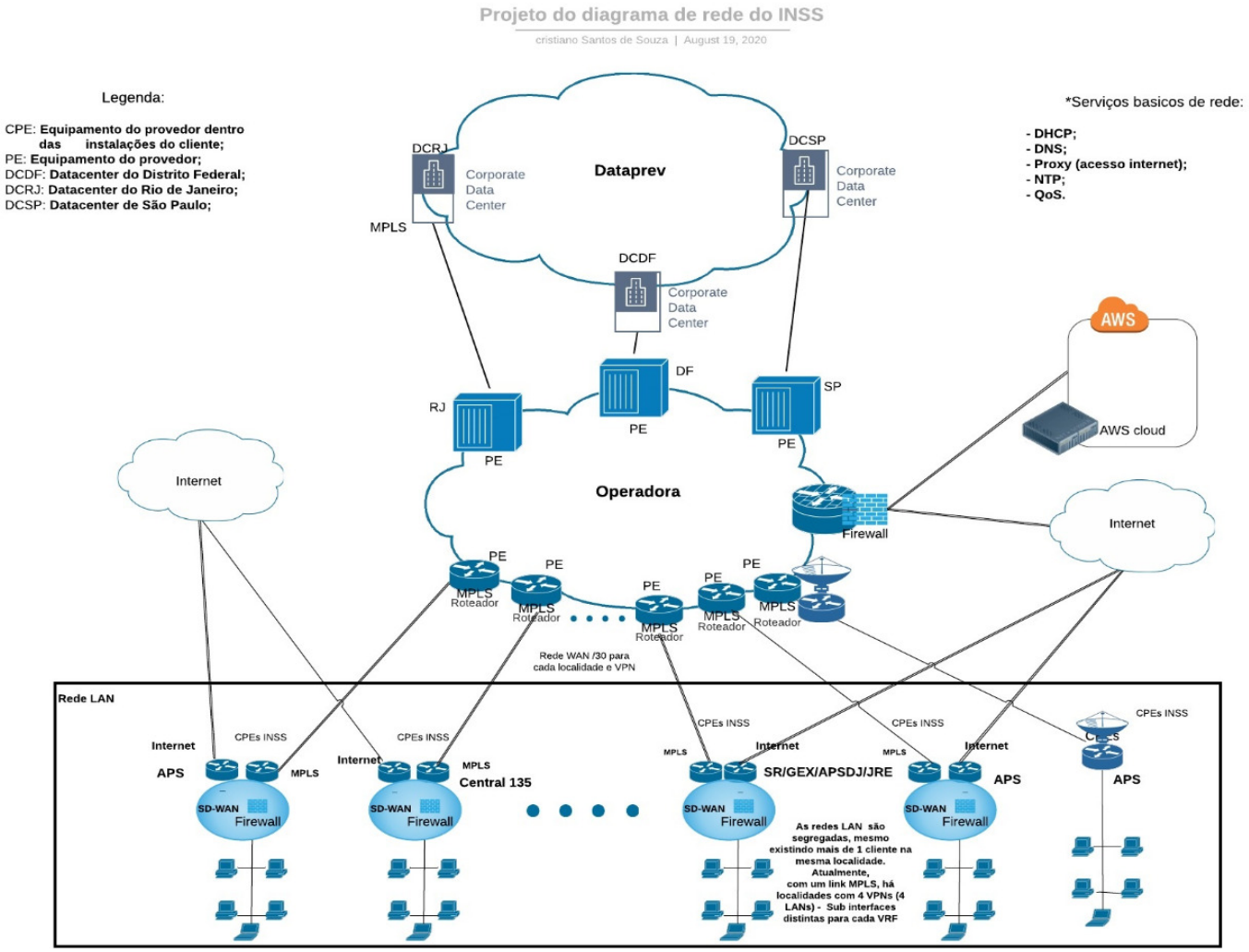
1.1. A CONTRATADA deve prover serviço de comunicação objetivando a interligação de endereços de interesse do CONTRATANTE situados em todo território nacional, além de acesso direto à Internet a partir desses endereços, contemplando:

a) Tecnologia VPN IP/MPLS para o tráfego de dados, voz e vídeo entre todos os endereços de interesses do CONTRATANTE;

b) Acesso à INTERNET através de circuito dedicado privativo;

1.2. 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

1.3. A topologia lógica proposta para a rede deverá ser a seguinte:



1.4. As unidades da CONTRATANTE foram divididas em grupos conforme a quantidade de pessoas e a capacidade de seus links, conforme disposto no 3.3.2 do Termo de Referência. Esses parâmetros serão utilizados para definir as capacidades mínimas dos equipamentos

SD-WAN, conforme disposto no item 1.65.2 deste documento.

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

1.6. 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.

1.7. 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 presente no item 4.10 do Termo de Referência.

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

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

1.10. Os concentradores receberão o tráfego MPLS 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.

1.11. Em cada concentrador deverá ser instalado um link Internet dedicado que funcionará para situações de contingenciamento e possivelmente em outras situações definidas no projeto executivo.

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

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

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

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

1.16. 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 unidades do Instituto ao ambiente de nuvem contratado pela CONTRATANTE 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.

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

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

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

1.20. 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.

1.21. 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.

1.22. 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).

1.23. A velocidade de todos os links com enlace satélite poderá ser entregue de forma assimétrica.

1.24. A CONTRATADA poderá entregar, nas unidades da rede de acesso, os links MPLS e Internet diretamente nos appliances SD-WAN.

1.25. Em situações normais, os tráfegos de sistemas e serviços corporativos, além dos tráfegos multimídia de telefonia IP e videoconferência devem ser encaminhados pela rede MPLS. Por outro lado, os serviços que estiverem publicados na Internet devem ser acessados diretamente sem a necessidade de utilização da rede MPLS.

1.26. Para as unidades da CONTRATADA poderá entregar os links MPLS e Internet 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.

1.27. Em situações de falha ou de uso intenso da rede MPLS, 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

1.28. Em situações de falha ou uso intenso dos links de internet dos endereços do CONTRATANTE, o tráfego deve ser encaminhado pela rede MPLS até os concentradores, e de lá enviado para a Internet.

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

1.30. 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, a 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.

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

1.32. 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.

1.33. Onde não for possível comprovadamente entregar acesso terrestre, será aceito acesso Satélite em banda Ka, e em alguns caso banda Ku, nas velocidades mínimas, dispostas no item 3.3.2 do Termo de Referência, 10 Mbps de download e 2 Mbps de upload para banda Ka e 2 Mbps de download e 1 Mbps de upload em banda Ku, e condições dispostas no item 3.3.2 do Termo de Referência e CIR de 100 % da banda, tanto de upload quanto de download

1.34. Caso não haja cobertura em banda Ka, será aceito acesso em banda Ku, nas velocidades, mínimas, de 2 Mbps para Download e 1 Mbps para Upload e CIR de 100 % da banda, tanto de upload quanto de download.

1.35. Serão aceitos no máximo 2,5 % , do total de acessos, em meio satelital.

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

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

1.38. Nos acessos satélite, as estações terrenas remotas deverão ser de pequeno porte, tipo VSAT.

1.39. Os acessos satélite deverão ser trocados para acessos terrestres, imediatamente, quando houver condições para tal.

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

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

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

1.43. Os appliances SD-WAN ou UTM em toda a rede devem ser do mesmo fabricante, para que a solução de gerência seja única e as configurações possam ser aplicadas em todos os dispositivos de forma unificada.

1.44. A 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.

1.45. As redes serão construídas por meio de circuitos de dados privativos e independentes, com velocidades ou largura de bandas simétricas 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.

1.46. 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.

1.47. 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.

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

1.49. 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, desde que atendam aos requisitos de performance e capacidade especificados neste Termo de Referência.

1.50. 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) quando o valor médio de utilização da banda (medido a cada cinco minutos) for menor ou igual à capacidade do canal contratado. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para a CONTRATANTE.

1.51. O equipamento CPE que receberá os canais de comunicação pode ser o mesmo equipamento aonde 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

1.52. Além das interfaces utilizadas para acesso a rede WAN (MPLS, Internet dedicada, 4G/5G/ADSL)o appliance SD WAN deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T), que serão utilizadas na rede interna do CONTRATANTE.

1.53. Deve ser possível implementar o CPE SD-WAN utilizando VRRP e realizar a recuperação de falhas através de um roteador compatível com esse protocolo.

1.54. **Acomodação dos equipamentos**

1.54.1. 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.

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

1.55. **Dupla abordagem**

1.55.1. A CONTRATADA deverá instalar os *links* MPLS e Internet com dupla abordagem de fibra óptica ~~em algumas unidades~~ nos endereços do CONTRATANTE dos grupos 1, 2 e 3 , conforme disposto no item 3.3.2.1 do Termo de Referência.

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

1.55.3. Os circuitos com dupla abordagem não poderão ser instalados no mesmo PE. Nos casos em que houverem limitação prediais nas unidades, serão aceitas, desde que devidamente justificado e autorizado plea Contratante, a utilização do mesmos encaminhamentos nesse acesso prediais.

1.55.4. 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.

1.56. **Domain Name System - DNS**

1.56.1. A solução deverá prover serviço de DNS Secundário que gerenciará a transferência dos registros de zona com o servidor de DNS primário da CONTRATANTE, ou conforme definido no projeto executivo, para que os endereços de Internet sejam resolvidos pela solução.

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

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

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

1.57. **Tunelamento e Criptografia**

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

1.57.2. 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”.

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

1.57.4. A solução SD-WAN deverá implementar túneis VPN IPSEC com capacidade de integração com equipamentos de outros fabricantes.

1.58. **Roteamento e Políticas**

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

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

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

1.58.4. 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.

1.58.5. A solução SD-WAN deverá suportar arquitetura VRF, onde o tráfego poderá ser segmentado com base em uma definição comum de VRFs em todos os sites.

1.58.6. Os CPE SD-WAN deverão ser entregues em alta disponibilidade (ativo/ativo e/ou ativo/passivo) nas unidades definidas no item 3.3.2.3 do Termo de Referência.

1.58.7. 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.

1.58.8. 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.

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

1.58.10. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas.

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

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

1.59.1. 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;

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

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

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

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

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

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

1.59.7. **MPLS - Muti Protocol Label Switching**

1.59.8. **Características gerais**

1.59.8.1. A solução deverá ser baseada em redes IPs Multisserviços, utilizando a tecnologia MPLS , com suporte a VPNs IP/MPLS, roteamento dinâmico e QoS (Quality of Services), com classes de serviço.

1.59.8.2. A solução suportará o tráfego de dados, voz e imagem, entre as unidades do CONTRATANTE, bem como de aplicações de Voz sobre IP – VoIP e Videoconferência IP, considerando os aspectos de segurança, confiabilidade e qualidade dos serviços.

1.59.8.3. Os equipamentos deverão ser dimensionados, fornecidos, instalados e configurados, pela CONTRATADA, garantindo-se o desempenho e os níveis de serviços definidos pela CONTRATANTE.

1.59.8.4. A solução deverá suportar Qualidade de Serviço (QoS) por meio da arquitetura DiffServ, incluindo DiffServ sobre MPLS.

1.59.9. **Backbone MPLS**

1.59.9.1. Deve permitir o isolamento total do tráfego e das tabelas de roteamento da CONTRATANTE e dos demais clientes da CONTRATADA utilizando tecnologia de VRFs criando uma VPN MPLS. Em função disso a CONTRATANTE poderá utilizar qualquer faixa de endereço privados IPv4 em sua estrutura de rede.

1.59.9.2. Deverá possuir capacidade de tráfego *multicast* em Ipv4 para que aplicações de voz e vídeo que utilizem esta tecnologia possam ser implementadas independentemente de qualquer configuração no *backbone*. Não será permitido o estabelecimento de túneis entre os roteadores para que o tráfego multicast seja encaminhado.

1.59.9.3. O backbone MPLS deve pertencer inteiramente a AS do mesmo grupo econômico.

1.59.10. **CONCENTRADORES MPLS**

1.59.10.1. A CONTRATADA deverá implantar 1 (um) concentrador da rede VPN IP/MPLS em cada um dos *datecenters* da DATAPREV, conforme endereços dispostos no item 3.3.2.4 do Termo de Referência.

1.59.10.2. A CONTRATADA deverá garantir a interconexão entre a rede VPN IP/MPLS do CONTRATANTE e a rede da DATAPREV.

1.59.10.3. 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.

1.59.10.4. A CONTRATADA deverá disponibilizar, em cada um dos concentradores, 1 circuito de acesso dedicado à Internet, conforme disposto no Grupo 10, Tabela 2, do item 3.3.2 do Termo de Referência.

1.59.11. **MPLS - Qualidade de Serviço (QoS)**

1.59.11.1. A solução da CONTRATADA deverá suportar a arquitetura Diffserv sobre redes MPLS;

1.59.11.2. De acordo com as prioridades e níveis de serviços definidos, os diferentes tipos de tráfego que serão encaminhados pela Rede do CONTRATANTE deverão ser classificados em classes de serviços (Diffserv) pela rede MPLS da CONTRATADA, conforme será definido no projeto executivo.

1.59.11.3. 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.

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

1.60. **CIRCUITO DEDICADO INTERNET**

1.60.1. 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.

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

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

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

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

1.61.1. **Características gerais**

1.61.1.1. 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.

1.61.1.2. 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.

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

1.61.1.4. 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.

1.61.1.5. 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.

1.61.1.6. 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 *pollings* a cada 5-minutos e de forma gráfica, dos serviços, de modo a permitir o acompanhamento e monitoração do estado global da rede.

1.61.1.7. 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.

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

1.61.1.9. 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.

1.61.1.10. 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.

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

1.61.1.12. 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.

1.61.1.13. 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.

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

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

1.61.1.16. 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 monitorado:

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

f) 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;

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

h) 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.*

1.61.1.17. 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.

1.61.1.18. 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.

1.61.1.19. 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.

1.61.1.20. 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.

1.61.1.21. 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.

1.61.1.22. 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.

1.61.1.23. 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.

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

1.61.1.25. 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 (ANSs) acordados.

1.61.1.26. 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 (ANS), e ter insumos para o planejamento de capacidade e a análise da efetividade da solução.

1.61.1.27. 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.

1.61.1.28. 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.

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

1.61.1.30. Sempre que os limites de desempenho dos equipamentos for ultrapassado, 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

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

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

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

1.61.2.2. 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.*

1.61.2.3. 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.

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

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

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

1.61.2.7. A gerência centralizada SD WAN/UTM deverá ser multi-tenant.

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

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

1.61.2.10. 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;

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

1.61.2.12. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC e suportar a comunicação com a API northbound do orquestrador. Essas comunicações deverão ser protegidas e criptografadas.

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

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

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

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

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

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

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

1.61.2.20. 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.

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

1.61.2.22. 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.

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

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

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

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

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

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

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

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

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

1.61.2.32. A solução de gerenciamento deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador.

1.61.2.33. A solução de gerência deve possuir "*wizard*" para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos.

1.61.2.34. A solução deve permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência.

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

1.61.2.36. A solução de gerenciamento deve possuir "wizard" para instalação de políticas e configurações dos dispositivos.

1.61.2.37. A solução deve permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração.

1.61.2.38. A solução deve permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos.

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

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

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

1.61.2.42. A solução deve permitir criar regras de NAT64 e NAT46 de forma centralizada.

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

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

1.61.2.45. 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.

1.61.2.46. 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.

1.62. **SEGURANÇA DA INFORMAÇÃO**

1.62.1. 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).

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

1.62.3. 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 Acordo de Nível de Serviço - ANS - acordado.

1.62.4. 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.

1.62.5. Os dispositivos disponibilizado pela CONTRATADA não poderão ter acesso via tecnologia sem fio. O acesso sem fio será desabilitado sempre que detectado e deverá assim permanecer ao longo da vigência do contrato.

1.62.6. 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.

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

1.62.8. 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.

1.62.9. 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.

1.62.10. 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 centralizadamente, armazenando-o por um período mínimo de 12 meses, para consulta futura, se necessário for. ***Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA***

1.62.11. A CONTRATADA deverá disponibilizar, para consulta on-line pelo prazo mínimo de 2 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***

1.62.12. 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.

1.62.13. 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.

1.63. **Serviços de Segurança da Informação**

1.63.1. **Características gerais**

1.63.1.1. 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).

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

1.63.1.3. 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.

1.63.1.4. 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.

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

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

1.63.1.7. 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***

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

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

1.63.1.10. 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.

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

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

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

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

1.63.4. 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.

1.63.4.1. 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:

1.63.4.2. 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.

1.63.4.3. Suportar mitigação automática de ataques, utilizando múltiplas técnicas como *WhiteLists*, *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.

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

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

1.63.4.6. 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-Control", 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.

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

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

1.63.4.9. 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.

1.63.4.10. Prover DNS BlackList; 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

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

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

1.63.4.13. 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.

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

1.63.4.15. 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.

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

1.63.4.17. 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;

1.63.4.18. 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.

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

1.63.4.20. 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.

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

1.63.4.22. 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;

1.63.4.23. 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;

1.63.4.24. 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;

1.63.4.25. 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.

1.64. **SD-WAN/UTM**

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

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

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

1.64.1.3. 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);

1.64.1.4. 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.

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

1.64.1.6. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo.

1.64.1.7. 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.

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

1.64.1.9. 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.

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

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

1.64.1.12. 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.

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

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

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

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

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

1.64.1.18. A solução deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões.

1.64.1.19. 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.

1.64.1.20. 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.

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

1.64.1.22. 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.

1.64.1.23. 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.

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

1.64.1.25. 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;

1.64.1.26. 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.

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

1.64.1.28. 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).

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

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

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

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

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

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

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

1.64.1.36. Deve suportar balanceamento de tráfego por sessão e pacote.

1.64.1.37. 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.

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

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

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

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

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

1.64.1.43. O dispositivo SD-WAN deverá suportar vários links de acesso, como MPLS, Internet dedicada.

1.64.1.44. 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.

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

1.64.1.46. 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 HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência).

1.64.1.47. 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).

1.64.1.48. Os equipamentos SDWAN/UTM funcionarão em regime de alta disponibilidade, para os enlaces dos grupos 1, 2, 3 e 10, conforme disposto no item 3.3.2.3 Termo de Referência, devem suportar as seguintes configurações de cluster:

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

b) Distribuição de carga, através do modo Ativo/Ativo, com opção de distribuição de carga igualitária (50-50) e modo pivot (70-30):

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.

1.64.1.49. 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.

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

1.64.2.1. *Equipamento SD-WAN/UTM Tipo 1* - Instalação nos enlaces dos grupos 6, 7, 8 e 9, conforme classificação de grupos disposta no item ~~3.2.3~~ 3.3.2 do Termo de Referência

a) *Throughput de, no mínimo, 750 Mbps com a funcionalidade de UTM/Firewall;*

b) *Throughput de, no mínimo, 220 Mbps de VPN IPSec;*

c) *Throughput de, no mínimo, 400 Mbps de IPS;*

d) *Throughput de, no mínimo,* 60 *Mbps de NGFW ;*

e) *Throughput de, no mínimo,* 60 *Mbps de Threat Prevention;*

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

g) *Suportar no mínimo 33 Mbps de throughput de Inspeção SSL;*

h) *Possuir ao menos 5 interfaces 1 GE RJ45;*

i) Suportar, no mínimo, 11.000 (onze mil) conexões por segundo;

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

1.64.2.2. 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, 3 Gbps com a funcionalidade de UTM/Firewall;

b) Throughput de, no mínimo, 600 Mbps de VPN IPSec;

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

d) *Throughput de, no mínimo, 400 Mbps de NGFW ;*

e) *Throughput de, no mínimo,* 100 *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 220 Mbps de throughput de Inspeção SSL;

h) Possuir ao menos 6 interfaces 1 GE RJ45;

i) Possuir armazenamento de no mínimo de 200GB;

j) Possuir fonte de alimentação interna e redundante;

k) Suportar, no mínimo, 20.000 (vinte mil) conexões por segundo;

l) Suportar, no mínimo,, 400.000 (quatrocentos mil) de conexões simultâneas;

1.64.2.3. Equipamento SD-WAN/UTM Tipo 3 – Instalação nos enlaces dos grupos 1 e 9, conforme classificação de grupos disposta no item 3.3.2 do Termo de Referência.

a) *Throughput de, no mínimo, 11 Gbps com a funcionalidade de UTM/Firewall;*

b) *Throughput de, no mínimo, 1.3 Gbps de VPN IPSec;*

c) *Throughput de, no mínimo, 3 Gbps de IPS;*

d) *Throughput de, no mínimo, 860 Gbps de NGFW ;*

e) *Throughput de, no mínimo,* 710 *Mbps de Threat Prevention;*

f) *Estar licenciado para, ou suportar sem o uso de licença, 10.000 (dez mil) túneis de VPN IPSEC Site-to-Site simultâneos;*

g) *Suportar no mínimo 800 Mbps de throughput de Inspeção SSL;*

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 com 2 (dois) discos em RAID1, por equipamento, pois a falha do disco, se único, ocasionará indisponibilidade da solução bem como os dados de log nele existentes;*

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

l) Suportar, no mínimo, 68.000 (sessenta e oito mil) conexões por segundo;

m) Suportar, no mínimo, 1.200.000 (um milhão e duzentos mil) de conexões simultâneas.

1.65. **VPN - Virtual Private Network**

1.65.1. **Características gerais**

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

1.65.1.2. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard).

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

1.65.1.4. 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.

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

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

1.65.1.7. A solução deve possuir interoperabilidade com no mínimo os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWal

1.65.2. VPN Corporativa

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

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

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

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

1.65.2.5. Suporte a autenticação multifator integrado.

1.65.2.6. Suportar conexões VPN SSL e IPSec Client-to-site e site-to-site.

1.65.2.7. 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.

1.65.2.8. Para VPN SSL deverá suportar:

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

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

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

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

1.65.2.11. 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.

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

1.65.2.13. O software cliente VPN deverá ser compatível com os seguintes sistemas operacionais: Windows x, y z, Linux e MacOS.

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

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

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

1.65.2.17. Deverá possuir roteamento dos protocolos IPv4 e IPv6.

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

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

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

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

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

1.66. **Filtro de dados**

1.66.1. 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).

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

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

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

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

1.67.1. 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);

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

1.67.3. 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;

1.67.4. 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;

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

1.67.6. 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;

1.67.7. 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;

1.67.8. Atualizar a base de assinaturas de aplicações automaticamente;

1.67.9. 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.

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

1.67.11. 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.

1.67.12. 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.

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

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

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

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

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

1.67.18. 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;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.67.33. **Identificação de usuários**

1.67.33.1. 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;

1.67.33.2. 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;

1.67.33.3. 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;

1.67.33.4. 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;

1.67.33.5. 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;

1.67.33.6. 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;

1.67.33.7. 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);

1.67.33.8. 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;

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

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

1.67.33.11. 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;

1.67.33.12. A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;

1.67.33.13. 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);

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

1.67.33.15. 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;

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

1.67.33.17. 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;

1.67.33.18. 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;

1.68. **UTM**

1.68.1. **Características gerais**

1.68.1.1. 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).

1.68.1.2. 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.

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

1.68.1.4. 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.

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

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

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

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

1.68.1.9. 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;

1.68.1.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

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

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

1.68.1.13. A solução deve suportar NAT dinâmico (Many-to-Many);

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

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

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

1.68.1.17. A solução deve suportar NAT de Origem;

1.68.1.18. A solução deve suportar NAT de Destino;

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

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

1.68.1.21. A solução deve suportar NAT64;

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

1.68.1.23. A solução deve possibilitar o envio de log para sistemas de monitoração externos, inclusive via protocolo SSL. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

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

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

1.68.1.26. 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;;

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

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

1.68.1.29. 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;

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

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

1.68.1.32. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

1.68.1.33. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. 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*.

1.68.2. **Políticas**

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

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

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

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

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

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

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

1.68.2.8. 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;

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

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

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

1.68.2.12. A solução deve suportar offload de certificado em inspeção de conexões SSL

1.68.3. **Controle de Aplicações**

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

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

1.68.3.3. 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;

1.68.3.4. 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;

1.68.3.5. 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;

1.68.3.6. 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;

1.68.3.7. Para tráfego criptografado SSL, a solução devedeve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.68.3.8. 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;

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

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

1.68.3.11. 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;

1.68.3.12. 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;

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

1.68.3.14. A solução deve permitir, nativamente, a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

1.68.3.15. A solução deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

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

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

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

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

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

1.68.3.21. 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);

1.68.3.22. 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;

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

1.68.3.24. 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;

1.68.3.25. 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;

1.68.3.26. 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;

1.68.3.27. 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.

1.68.3.28. 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;

1.68.3.29. Possibilitar o bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

1.68.4. **Prevenção de ameaças**

1.68.4.1. 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;

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

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

1.68.4.4. IPS

1.68.4.5. 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;

1.68.4.6. 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.

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

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

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

1.68.4.10. 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;

1.68.4.11. Deve permitir o bloqueio de vulnerabilidades;

1.68.4.12. Deve permitir o bloqueio de exploits conhecidos;

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

1.68.4.14. Bloquear ataques efetuados por worms conhecidos;

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

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

1.68.4.17. 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;

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

1.68.4.19. 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;

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

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

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

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

1.68.4.24. 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.

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

1.68.4.26. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

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

1.68.4.28. Possuir no mínimo 21.000 assinaturas de IPS;

1.68.4.29. 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;

1.68.4.30. 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;

Integrante **Requisitante** Documento assinado eletronicamente XXXXXXXX **Matrícula/SIAPE: XXXXXX**	**Integrante** **Técnico** Documento assinado eletronicamente XXXXXXXXXXX **Matrícula/SIAPE: XXXXXX**	**Integrante** **Administrativo** Documento assinado eletronicamente XXXXXXXXXX **Matrícula/SIAPE: XXXXX**