5.6.2.137. 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;
5.6.2.138. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
5.6.2.139. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
5.6.2.140. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;
5.6.2.141. QoS e Traffic Shaping
5.6.2.142. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
5.6.2.143. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
5.6.2.144. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
5.6.2.145. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
5.6.2.146. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
5.6.2.147. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
5.6.2.148. O QoS deve possibilitar a definição de tráfego com banda garantida;
5.6.2.149. O QoS deve possibilitar a definição de tráfego com banda máxima;
5.6.2.150. O QoS deve possibilitar a definição de fila de prioridade;
5.6.2.151. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
5.6.2.152. Suportar modificação de valores DSCP para o Diffserv;
5.6.2.153. Suportar priorização de tráfego usando informação de Type of Service;
5.6.2.154. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
5.6.2.155. Filtro de Dados
5.6.2.156. Permitir a criação de filtros para arquivos e dados pré-definidos;
5.6.2.157. Os arquivos devem ser identificados por extensão e tipo;
5.6.2.158. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
5.6.2.159. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5.6.2.160. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5.6.2.161. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
5.6.2.162. Geo Localização
5.6.2.163. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
5.6.2.164. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
5.6.2.165. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
5.6.2.166. VPN
5.6.2.167. Suportar VPN Site-to-Site e Cliente-To-Site;
5.6.2.168. Suportar IPSec VPN;
5.6.2.169. Suportar SSL VPN;
5.6.2.170. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
5.6.2.171. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
5.6.2.172. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
5.6.2.173. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
5.6.2.174. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
5.6.2.175. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
5.6.2.176. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
5.6.2.177. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
5.6.2.178. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
5.6.2.179. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
5.6.2.180. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
5.6.2.181. Deverá manter uma conexão segura com o portal durante a sessão;
5.6.2.182. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
5.6.2.183. Deve suportar Auto-Discovery Virtual Private Network (ADVPN);
5.6.2.184. Deve suportar agregação de túneis IPSec;
5.6.2.185. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec;
5.6.2.186. A VPN IPSec deve suportar Forward Error Correction (FEC);
5.6.2.187. Deve suportar TLS 1.3 em VPN SSL;
5.6.2.188. SD-WAN
5.6.2.189. Deve implementar balanceamento de link por hash do IP de origem;
5.6.2.190. Deve implementar balanceamento de link por hash do IP de origem e destino;
5.6.2.191. 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.
5.6.2.192. Deve implementar balanceamento de link por custo configurado do link.
5.6.2.193. Deve suportar o balanceamento de, no mínimo, 256 links;
5.6.2.194. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec
5.6.2.195. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
5.6.2.196. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde
5.6.2.197. Deve suportar Zero-Touch Provisioning
5.6.2.198. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes
5.6.2.199. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado
5.6.2.200. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.
5.6.2.201. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS
5.6.2.202. Suportar UDP Hole Punching em arquitetura ADVPN
5.6.2.203. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado
5.6.2.204. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.
5.6.2.205. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN
5.6.2.206. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link
5.7. Instalação e Configuração – ITEM 7
5.7.1. As atividades de migração (se necessário), instalação e configuração dos equipamentos dos itens 1, 2, 3 e 4 deverão ser realizadas nas dependências do IGEPREV em Belém/PA e será inteiramente de responsabilidade da CONTRATADA, sem que comprometa o funcionamento dos sistemas, recursos ou outros equipamentos atualmente em operação;
5.7.2. O período mínimo o qual deve ser considerado para as atividades de instalação e configuração de todos os equipamentos é de 30 dias, isto é, a CONTRATADA deverá dispor de profissional(is) que ficará(ão) a disposição da CONTRATANTE durante este período de forma ON-SITE em horário comercial;
5.7.3. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem dos equipamentos até a energização dos mesmos;
5.7.4. Deverá ser fornecida documentação de toda a implementação e configuração da implantação dos equipamentos;
5.7.5. Ficará a critério do CONTRATANTE juntamente com a CONTRATADA definir o cronograma de atividades para a implantação dos equipamentos desde que atenda ao item 6.5.2;
5.8. Suporte Técnico Especializado – Item 8
5.8.1. Serviço de suporte técnico terá vigência de 12 (doze) meses, a partir da emissão do Termo de Recebimento dos equipamentos, com a possibilidade de ter a sua duração prorrogada por iguais e sucessivos períodos, conforme a lei 8.666/93.
5.8.2. O serviço deve contemplar manutenção e suporte técnico para os itens 1, 2, 3, 4 e 5.
5.8.3. A CONTRATADA deverá prestar serviço de manutenção e suporte técnico destinado a:
5.8.3.1. Restabelecimento de serviços interrompidos ou degradados;
5.8.3.2. Solução de problemas de configuração e falhas técnicas nos equipamentos;
5.8.3.3. Esclarecimentos de dúvidas sobre configurações e utilização dos equipamentos;
5.8.3.4. Implementação de novas funcionalidades.
5.8.3.5. Os serviços serão solicitados mediante a abertura de chamados a serem efetuados por técnicos do IGEPREV, via chamada telefônica local ou gratuita, e-mail ou website, em qualquer caso em português, a qualquer horário e em qualquer dia da semana (24x7), sem custos para a CONTRATANTE.
5.8.4. Não haverá limitação de quantidade de abertura de chamados para suporte.
5.8.5. O suporte deve estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nos 365 (trezentos e sessenta dias) do ano, sendo o Português Brasileiro o idioma de suporte técnico obrigatório.
5.8.6. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá a CONTRATADA fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços.
5.8.7. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.
5.8.8. O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.