

Itens/Descrição do Requisito	Atende/ Não Atende/ Atende Parcial	Observação
2.1.9.4. A Contratada deverá possuir centros de limpeza no Brasil, e nos continentes América do Norte, Europa e Ásia. Todos devem tratar ataques originados fora do Brasil em centros de limpeza mais próximos à origem dos ataques;		
2.1.9.4.1. A Contratada deve possuir, ao menos, 1 (um) Centro de Limpeza em cada uma das regiões anteriormente citadas;		
2.1.9.4.2. No Brasil, a Contratada deverá possuir, ao menos 5 (cinco) Centros de Limpeza, sendo um centro de limpeza por região geográfica (Sul, Sudeste, Centro-Oeste, Nordeste e Norte);		
2.1.9.4.3. Nos demais continentes, a Contratada deve possuir ao menos 15 (quinze) centros de limpeza espalhados nas regiões mencionadas anteriormente, atingindo assim o objetivo de proteção contra negação de serviço de forma globalmente distribuída, além da distribuição de proteção em uma infraestrutura nacional;		
2.1.10.2. O acionamento do desvio de tráfego para os centros de limpeza deve ser disponibilizado através de publicação de rotas via BGP, e também por túneis GRE via console de gerenciamento WEB publicada na Internet;		
2.1.10.4. O serviço deve permitir a configuração de endereço IP e grupos de IPs para a mitigação do tráfego, possibilitando que apenas o tráfego de aplicações desejadas seja inspecionado no centro de limpeza, evitando assim que seja feita a mitigação do tráfego de aplicações que não devem ser inspecionados;		
2.1.10.6. O serviço deve suportar, no mínimo, os modos operacionais abaixo:		
2.1.10.6.1. Passivo: Detecção completa de ataques, sem bloqueio;		
2.1.10.6.2. Ativo: Detecção completa de ataques, interceptação e bloqueio;		
2.1.10.11. O serviço deve detectar, identificar e mitigar ameaças em tempo real em seus Scrubbing Centers e entregar o tráfego legítimo ao Serpro;		
2.1.11.6. O serviço deve implementar listas de acesso (accesslist) e listas de bloqueio (blocklist) via console de gerência WEB;		
2.1.11.10. Os parâmetros de proteção do serviço em nuvem listados devem ser editáveis sem restrições via console de gerência WEB, com acesso administrativo para edição e aplicação imediata pela equipe técnica do Serpro:		
2.1.11.10.1. Endereço IP/máscara submetido às proteções do serviço;		
2.1.11.10.2. Listas de bloqueio de:		

2.1.11.10.2.1. IPs;		
2.1.11.10.2.2. Portas de serviço TCP e UDP;		
2.1.11.10.2.3. Protocolos TCP, UDP e ICMP;		
2.1.11.10.3. Lista de acesso de:		
2.1.11.10.3.1. IPs;		
2.1.11.10.3.2. Portas de serviço TCP e UDP;		
2.1.11.10.3.3. Protocolos TCP, UDP e ICMP;		
2.1.11.12. O serviço deve suportar mecanismos de mitigação baseados em:		
2.1.11.12.1. Bloqueio por IP, protocolo, socket TCP e localização geográfica do ponto de acesso e operação à rede do serviço contratado;		
2.1.11.12.2. Liberação por IP, protocolo, socket TCP e localização geográfica do ponto de acesso e operação à rede do serviço contratado;		
2.1.11.12.3. Lista de reputação de IPs maliciosos detectados, atualizados e fornecidos pela fabricante do serviço contratado;		
2.1.11.12.4. Limite da quantidade de tráfego em pacotes e bytes por segundo de uma determinada origem IP;		
2.1.11.12.5. Limite da quantidade de tráfego em pacotes e bytes por segundo de uma determinada região do globo terrestre;		
2.1.11.12.6. No estabelecimento das conexões criptografadas em HTTPS;		
2.1.11.12.7. Ataques de baixa velocidade;		

2.1.11.12.8. Pacotes malformados;		
2.1.11.12.9. Identificação e validação de acessos com origens forjadas;		
2.1.11.12.10. Bloqueio de pacotes por conexão TCP;		
2.1.11.12.11. Bloqueio de datagramas por fluxo UDP;		
2.1.11.12.12. Bloqueio e mitigação de ataques nos roteadores mais próximos da origem do ataque;		
2.1.11.12.13. Regras de detecção e mitigação específicas para os determinadas pontos de operação do globo terrestre;		
2.1.11.12.13.1. Os parâmetros de detecção e mitigação devem ser editáveis via gerência Web, com acesso administrativo e aplicação imediata pela equipe técnica do Serpro.		
2.1.11.15. O serviço deve possuir mecanismos necessários para a mitigação de ataques DDoS, sejam eles baseados em volume, em protocolos de rede (camadas 3 e 4) e em nível básico de aplicação, considerando no mínimo a seguinte lista (não exaustiva):		
2.1.11.15.1. SYN Flood;		
2.1.11.15.2. ACK Flood;		
2.1.11.15.3. UDP Flood;		
2.1.11.15.4. ICMP Flood;		
2.1.11.15.8. DNS Query Flood;		
2.1.11.15.14. Amplificação:		
2.1.11.15.14.1. DNS;		

2.1.11.15.16. SYN+UDP ou ICMP+UDP (Mixed);		
2.1.12. Interface de Gerência Web, Monitoração e Logs		
2.1.12.1. O serviço deve prover console de gerência Web que forneça acesso a todos os serviços disponíveis, como a detecção de DDoS, visualização de tráfego, política e mitigação;		
2.1.12.2. O serviço deve possuir um Dashboard que faça sumarização dos ataques em tempo real;		
2.1.12.3. O serviço deve permitir a utilização de usuários com perfis de acesso de somente leitura e administrativo;		
2.1.12.3.1. 1. Deverá possibilitar a integração com Login Único do Serpro com autenticação através de SSO (Single Sign-On) compatível com OpenID Connect 1.0 ou SAML 2.0, implementando as recomendações do protocolo OAuth.		
2.1.12.3.2.2. A solução deve permitir a integração com Login Único do Serpro, com autenticação através de Federação SSO (Single Sign-On) compatível com ao menos um dos seguintes protocolos, em ordem de prioridade:		
2.1.12.3.2.1. OpenID Connect 1.0 com implementação de Authorization Code Flow. Caso a Solução necessite utilizar Client público, deverá ser implementada a extensão "Proof Key for Code Exchange" (PKCE);		
2.1.12.3.2.2. SAML 2.0 com implementação de assinatura e criptografia do payload SAML.		
2.1.12.4. O serviço deve mostrar o número de ataques e os endereços IPs que participam do ataque;		
2.1.12.5. O serviço deve disponibilizar via interface de gerência WEB informações pós-incidente com o mínimo de 30 dias consecutivos contendo as informações:		
2.1.12.5.1. Eventos registrados;		
2.1.12.5.2. Vetores de ataque;		
2.1.12.5.3. Origens do ataque identificados;		
2.1.12.5.4. Destino do ataque identificados;		

2.1.12.5.5. Tráfego bloqueado e liberado;		
2.1.12.5.6. Regras de acesso e bloqueio acionadas;		
2.1.12.5.7. Bloqueios por pontos de operação do serviço;		
2.1.12.5.8. Critério de identificação do fluxo malicioso;		
2.1.12.5.9. Estatísticas do fluxo malicioso;		
2.1.12.5.10. Monitoração do fluxo nas listas de acesso;		
2.1.12.6. Integração com Grafana versão 11 ou superior hospedado na rede Serpro sem necessidade de scripts e rotinas paralelas;		
2.1.12.7. Capacidade de realizar captura de tráfego em tempo real nos pontos de operação e acesso ao serviço nos padrões do Wireshark (PCAP) via console de gerência WEB;		
2.1.12.8. O serviço deve possuir interface intuitiva, com a capacidade de trabalhar com políticas distintas para diferentes redes protegidas;		
2.1.12.8.1. As políticas devem ser aplicadas por segmento de rede, de forma que cada segmento de rede possa ter uma política distinta;		
2.1.12.9. O serviço deve prover interface de gerência Web que suporte no mínimo os navegadores Mozilla Firefox ESR 45128.8 e Google Chrome versão 138, Microsoft Edge 125.0.2535.85, Safari 16 e superiores;		
2.1.12.10. O serviço deve ter capacidade de analisar eventos com atraso máximo de 1 (um) minuto e opção de geração relatórios durante a avaliação do tráfego;		
2.1.12.11. O serviço deve possuir dashboard com gráficos estatísticos da disponibilidade do serviço;		
2.1.12.12. O serviço deve suportar os registros das operações do sistema e das ações de início e término de sessão (login);		
2.1.12.13. O serviço deve possuir uma trilha de auditoria para que as alterações de configurações sejam mostradas quando necessário, informando quando foram executadas e por qual usuário.		