

ANEXO A

Questionamentos públicos para avaliar serviço de proteção Anti-DDoS distribuída em nuvem (versão prévia para Consulta Pública)

Todas as necessidades do Serpro precisam ser atendidas e operacionalizadas via console web sem a necessidade de acionamento do fabricante.

Necessidades	Expectativas e questões vinculadas	Atende? De que forma?
Publicação de uma rede /24 sem ação de mitigação	Desvio do tráfego de uma rede /24 para o centro de limpeza exclusivamente para fim de monitoração, análise e identificação das mitigações executadas caso os bloqueios estivessem ativos.	
Visualização do fluxo inspecionado e do fluxo em liberado	Dashboard com informações em tempo real das ações de bloqueio e liberação executadas com sumarização em gráficos em função tempo dos últimos 30 dias.	
Identificação das informações do fluxo malicioso	Dashboard com informações em tempo real dos fluxos maliciosos identificando a não conformidade e ação de contra-medida utilizada.	
Identificação dos IPs bloqueados	Dashboard com informações em tempo real dos IPs bloqueados com sumarização por rede protegida, tuneis GRE, tipo de anomalia e destinos IP.	
Identificação dos IPs liberados	Dashboard com informações em tempo real dos IPs liberados e qual o critério para tomada de decisão.	
Bloqueio explícito de um IP ou rede	Configuração de regra para bloqueio explícito de IP e rede, de origem e destino com monitoração em tempo real.	
Liberação explícita de um IP ou rede	Configuração de regra para liberação explícita de IP e rede, de origem e destino com monitoração em tempo real.	
Visualização dos critérios de identificação de fluxo malicioso	Dashboard em tempo real para visualização dos critérios de seleção do fluxo malicioso.	

Estatísticas do fluxo malicioso	Dashboard em tempo real para visualização dos quantitativos dos fluxos selecionados como maliciosos e seus tipos;	
Monitoração do fluxo em bypass	Dashboard em tempo real para visualização do tráfego explicitamente configurado nas listas de acesso e os critérios utilizado.	
Integração com SIEM	Disponibilizar mecanismo para integração com o SIEM do Serpro.	
Integração com Grafana	Disponibilizar mecanismo para integração do Grafana do Serpro.	
Ativação da proteção para um /32 sem interferir no restante do fluxo do /24	Possibilidade de realizar mitigação em um IP /32 específico sem tomar ações de mitigação nos outros IPs do tráfego da rede desviada.	
Visualização dos contra-medidas para bloqueio	Disponibilizar todas as contra-medidas ativas e inativas e os parâmetros de sensibilidade e ação de mitigação.	
DNS protection	Mecanismos de proteção DNS com análise da camada de aplicação.	
TCP dump com fluxo monitorado	Possibilidade de captura de tráfego nos POPs do serviço para análise no Wireshark.	