Gigamon®

Inserção dinâmica de equipamentos de segurança online

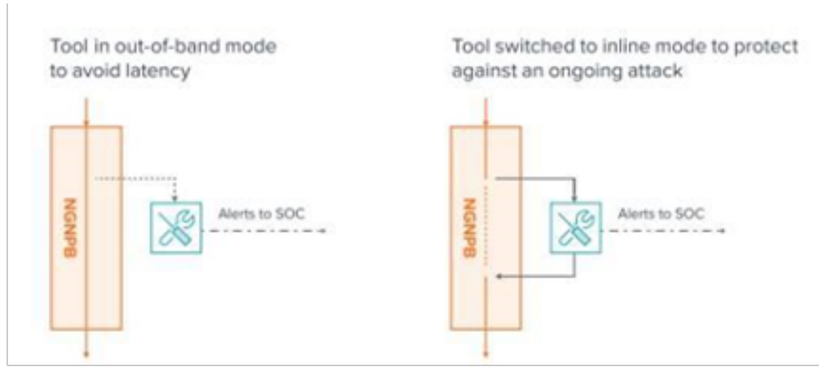
Problema

A implementação de ferramentas de segurança online, como IPS, WAF ou DDoS, pode ser problemática em muitas situações devido aos atrasos que podem introduzir, ao aumento do risco na continuidade dos negócios, à adição de mais equipamentos online, ou aos riscos para o negócio derivados de configurações incorretas da sonda que podem afetar todo o tráfego que passa por elas. Além disso, obrigar todo o tráfego online a passar por estes equipamentos de segurança vai exigir um projeto de maior dimensão e, consequentemente, de custo mais elevado, quando na realidade poderia ser corretamente dimensionado se apenas o tráfego suscetível de ser malicioso passasse por eles. A tudo isso, devemos adicionar a problemática de fornecer alta disponibilidade a esses equipamentos tão críticos, devido às assimetrias de tráfego e às diferentes capacidades das sondas.

Solução

Todos os equipamentos de segurança têm modos out-of-band, também chamados de monitor, nos quais analisam o tráfego com base numa cópia do mesmo sem a necessidade de estar online. Graças à integração que podemos realizar entre a sonda de segurança e o Network Packet Broker da Gigamon, através da API programável do FabricManager, seremos capazes de redirecionar o tráfego para a própria sonda que detetou o ataque offline de maneira dinâmica para que passe a estar online. Além disso, com a capacidade de aplicar filtros específicos nos níveis 2/3/4, uma vez detetado o ataque, temos a possibilidade de limitar o tráfego que se dirige à sonda pelo facto de ela estar online, e dimensioná-la de uma forma mais racional, com a consequente economia de custos. Uma vez mitigado o ataque, ou após um tempo razoável, podemos reverter automaticamente a situação e colocar novamente a sonda offline no modo de monitorização. Essas capacidades de inserção dinâmica somam-se às capacidades do NPB em resolver os problemas associados ao fornecimento de alta disponibilidade e escalabilidade a essas sondas.

Esquema



Licença

ILoad Balancing
Flow Mapping
Fabric Manager
Inline Bypass
Bypass HW