DDOS: Formas de contenção

Os ataques DDOS devem ser impedidos antes mesmo de causarem algum dano, porém pode ser necessário impedi-los após os mesmos já terem ocorrido. Essa é a fase de contenção do ataque. Vamos levar em consideração que a maioria dos ataques DDOS são internacionais, e que atacam sempre o roteador de borda das empresas, ou seja, aquele que executa a comunicação externa. Portanto, a contenção deve ocorrer da mesma forma, sempre o mais perto da fonte do ataque. Dentro deste parâmetro, é possível realizar algumas boas práticas para conter o ataque e impedir que muito dano seja causado.

Uma forma simples de contenção para ataques DDOS internacionais é dividir a máscara de rede em múltiplos de número menor, como uma máscara /22 em quatro máscaras de /24, por exemplo (A máscara /24 é a menor máscara que pode ser utilizada em um anúncio público). Após essa divisão, é feita uma solicitação para a operadora para que não sejam anunciados internacionalmente os IPs da máscara /24 específica que estavam na solicitação do ataque. Realizando esse procedimento, a rota que o ataque estava utilizando não será mais válida, impedindo o ataque. Apesar de todas as máquinas na faixa anterior continuarem funcionando internamente, as máquinas que foram divididas para o /24 alvo não terão mais conexão com sites internacionais. Podemos reabilitar a conexão dessas máquinas após a contenção do ataque.

Existe também o conceito de black hole (buraco negro), que impede pacotes na rede de forma automática. Ao utilizar o que é chamado de black hole community, após encontrar o IP que está sendo atacado ou o IP de onde está vindo o ataque, entramos em contato com a operadora de serviço para que a mesma aponte este IP para a interface Null0 do roteador, efetivamente derrubando todos os pacotes encaminhados.

É possível também configurar um dispositivo “gatilho” (Trigger), que irá ativar o black hole de forma remota. Assim, sendo detectado um ataque deste tipo na rede, este dispositivo atualizará as rotas dos outros roteadores de borda para o Null0. É inteligente criar diversos dispositivos “gatilhos” para ter redundância. Pode ser utilizado qualquer dispositivo que rode BGP (Border Gateway Protocol).

Podemos ter dois tipos de black hole filtering: Baseado em destino, que derruba todos os pacotes encaminhados para um certo IP ou faixa de IPs, e o baseado na fonte. Este verifica se o IP que consta no pacote recebido está listado na tabela de encaminhamento do roteador. Se não está, este também é derrubado.

Fontes:

https://www.cisco.com/c/dam/en\_us/about/security/intelligence/blackhole.pdf

https://www.he.net/adm/blackhole.html