Prevenção de Quadros Jumbo ICMP nos Switches Gerenciados SG200/300 Series

Objetivo

O objetivo deste artigo é explicar por que os switches das séries SG200 e SG300 impedem alguns dos jumbo frames ICMP e permitem que outros jumbo frames passem sobre o Switch. Este artigo mostra quais são alguns dos problemas causados pelos jumbo frames ICMP. O artigo também explica o que é um ataque de negação de serviço (DoS) e como ele se relaciona aos quadros jumbo ICMP.

Dispositivos aplicáveis

SG200
SG300

Quadros jumbo ICMP sobre o switch

Veja a seguir uma explicação do que são quadros jumbo e por que os quadros jumbo ICMP não são permitidos nos switches das séries SG200 e SG300.

jumbo frames

O switch Gigabit Ethernet (séries SG200 e SG300) e o switch Fast Ethernet (switches da série SF200) suportam quadros jumbo. Os **Jumbo Frames** são quadros Ethernet estendidos que variam em tamanho desde os 1.518 bytes padrão até os 9.000 bytes. Assim, os quadros jumbo aumentam a velocidade de transferência de dados transportando mais dados por quadro, reduzindo a sobrecarga dos cabeçalhos.

ICMP (Internet Control Message Protocol)

O ICMP é um protocolo da camada de rede que faz parte do conjunto de protocolos da Internet que gera mensagens ICMP em resposta a erros no datagrama IP ou para fins de diagnóstico ou roteamento. Os erros ICMP são sempre reportados ao endereço IP origem do datagrama de origem. Embora esse protocolo seja muito importante para garantir a distribuição correta de dados, ele pode ser explorado por usuários mal-intencionados para realizar diferentes ataques de negação de serviço (DoS).

Os ataques de DoS tornam os recursos da rede e do servidor indisponíveis ou não respondem aos usuários legítimos por meio da inundação de redes com tráfego falso. Os ataques de DoS por força bruta consomem o servidor e a largura de banda da rede, inundando o servidor com tráfego intenso. A seguir estão tipos comuns de ataques DoS usando o ICMP.

·Ataque de Inundação de Ping ICMP — Em um ataque de Inundação de Ping ICMP, o ataque envia um grande número de pacotes de ping para o sistema de destino, geralmente usando o comando ping do host. Dessa forma, o sistema atacado não pode responder ao tráfego legítimo.

·Ataque ICMP Smurf — Um Ataque ICMP Smurf inunda a máquina vítima com pacotes de ping falsificados. Esses são pacotes modificados que contêm um endereço IP falsificado da vítima de destino. Isso causa um broadcast da informação incorreta para todos os hosts na rede local. Todos esses hosts respondem com uma resposta ao sistema de destino, que fica saturado com essas respostas.Se houver muitos hosts em redes usadas, a vítima será efetivamente falsificada por uma grande quantidade de tráfego.

Nota: IP Spoofing refere-se a um pacote IP com um endereço IP de origem forjado, com a finalidade de ocultar as informações do remetente.

·Ping of Death — Em um ataque de ping of death, o invasor envia à vítima um pacote ICMP echo request que é maior que o tamanho máximo do pacote IP de 65.536 bytes. Como o pacote de solicitação de eco ICMP recebido é maior que o tamanho normal do pacote IP, ele deve ser fragmentado. Como resultado disso, a vítima não consegue remontar os pacotes, de modo que o SO trava ou reinicializa.

·Ataque Nuke ICMP — nesse tipo de ataque, as nukes são enviadas à vítima por meio de um pacote ICMP com mensagens de destino inalcançável que são do tipo 3. O resultado desse ataque é que o sistema de destino interrompe as comunicações com as conexões existentes.

Nos switches das séries SG200 e SG300, a Prevenção de Negação de Serviço permite que os gerentes de rede configurem o bloqueio de determinados pacotes ICMP. Por padrão, alguns dos quadros ICMP jumbo são bloqueados porque muitos ataques de rede, como DoS, utilizam ICMP, portanto, por motivos de segurança, os firewalls desses switches bloqueiam os quadros ICMP jumbo. Isso faz com que a fragmentação ICMP necessária e a mensagem DF set não cheguem ao remetente. O remetente, portanto, não recebe nenhuma informação para enviar seus pacotes em um tamanho menor, nem recebe uma confirmação TCP de que seus pacotes foram bem-sucedidos. Subsequentemente, o remetente reenvia continuamente o quadro no mesmo tamanho grande, mas nunca chega ao destino, resultando em uma condição conhecida como "buraco negro".

Use o utilitário de configuração da Web para configurar quadros jumbo, escolha **Gerenciamento de porta > Configurações de porta** e escolha **Segurança > Prevenção de negação de serviço > Configurações do conjunto de segurança** para configurar a prevenção de DoS.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.