

A recusa do IP do serviço (DoS) fragmenta a configuração de filtração no Switches controlado 300 Series

Objetivo

O tráfego de rede é enviado por meio dos pacotes múltiplos chamados datagramas. Cada método do transporte (Ethernet, Token Ring, etc.) tem um tamanho máximo da datagrama que possa segurar. Se a datagrama é demasiado grande para o método da transmissão, está rachada em fragmentos menores. Este processo é sabido como a fragmentação de IP. A maioria de tráfego de rede não tem que ser fragmentado. De fato, o tráfego que foi fragmentado pode ser usado como em um ataque de recusa de serviço (DOS). Um ataque DoS inunda uma rede com o tráfego falso e retarda ou para a rede. O Switches controlado 300 Series pode obstruir fragmentos IP, que diminui a vulnerabilidade de redes a um ataque DoS. Este artigo explica como configurar os *fragmentos IP que filtram* ajustes no Switches controlado 300 Series.

Nota: Os filtros do fragmento IP podem somente ser usados se a prevenção DoS é permitida. Refira os *ajustes da série da Segurança* do artigo no *Switches controlado 300 Series* para a ajuda.

Dispositivos aplicáveis

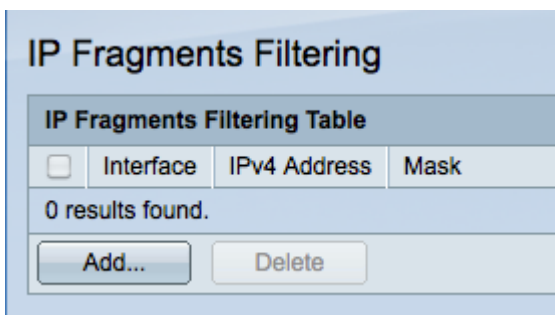
- Switches controlado 300 Series SF/SG

Versão de software

- 1.3.0.62

Adicionar o filtro dos fragmentos IP

Etapa 1. Entre ao utilitário de configuração da Web e escolha a **Segurança > a recusa da filtração da prevenção do serviço > dos fragmentos IP**. *Os fragmentos IP que filtram* a página abrem:



Etapa 2. O clique **adiciona** para adicionar um filtro novo dos fragmentos IP. *Os fragmentos IP adicionar que filtram* o indicador aparecem.

Interface: Port LAG

IP Address: User Defined All addresses

Network Mask: Mask Prefix length (Range: 0 - 32)

Apply Close

Etapa 3. Clique o botão de rádio que corresponde com a interface desejada no campo da relação. Este é o local físico que o filtro estará atribuído a.

- Porta — A porta física no interruptor. Escolha uma porta específica da lista de drop-down da porta.
- RETARDAÇÃO — Um grupo de portas que atua como uma porta única. Escolha uma RETARDAÇÃO específica da lista de drop-down da RETARDAÇÃO.

Etapa 4. Clique o botão de rádio que corresponde com o endereço desejado do IPv4 a ser filtrado no campo do endereço IP de Um ou Mais Servidores Cisco ICM NT.

- Definido pelo utilizador — Incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT a ser filtrado.
- Todos os endereços — Todos os endereços do IPv4 são filtrados.

Nota: Se você escolheu todos os endereços em etapa 4, salte para a etapa 6.

Etapa 5. Clique o botão de rádio que corresponde com o método usado para definir a máscara de sub-rede do endereço IP de Um ou Mais Servidores Cisco ICM NT no campo da máscara de rede.

- Máscara — Incorpore a máscara de rede ao campo da máscara de rede.
- Comprimento de prefixo — Incorpore o comprimento de prefixo (inteiro na escala de 0 a 32) ao campo do comprimento de prefixo.

Etapa 6. O clique **aplica-se** para salvar o muda e clica então **perto de fecha** os *fragmentos IP adicionar que filtram* o indicador.