A recusa da configuração de filtração do serviço (DoS) SYN no 300 Series controlou o Switches

Objetivo

Um ataque de recusa de serviço (DOS) inunda uma rede com o tráfego falso. Isto desenha recursos do servidor de rede longe dos usuários legítimos. Uma inundação de SYN visa o protocolo de TCP em particular. O protocolo de TCP exige três etapas funcionar. Primeiramente, um usuário envia seu endereço IP de Um ou Mais Servidores Cisco ICM NT ao server e pede uma conexão. Em seguida, o server responde ao pedido e espera uma confirmação. Finalmente, o usuário reconhece que o server abriu uma conexão. Um ataque SYN TCP usa endereços IP de Um ou Mais Servidores Cisco ICM NT múltiplos para pedir uma conexão, mas nunca envia um reconhecimento de volta ao server uma vez que uma conexão está aberta. Um server pode somente abrir uma quantidade limitada de conexões antes que comece deixar cair pedidos TCP, mesmo dos usuários legítimos.

O tráfego TCP é enviado em diversas portas virtuais. Estas portas são uma maneira para que o tráfego de rede seja rachado em grupos comuns. O filtro SYN pode ser configurado para obstruir o tráfego de uma porta virtual específica. Além, a filtração SYN é configurada em um real, em uma porta física ou em uma RETARDAÇÃO no interruptor. Este artigo explica como configurar o SYN que filtra no Switches controlado 300 Series.

Nota: Os filtros do Syn 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

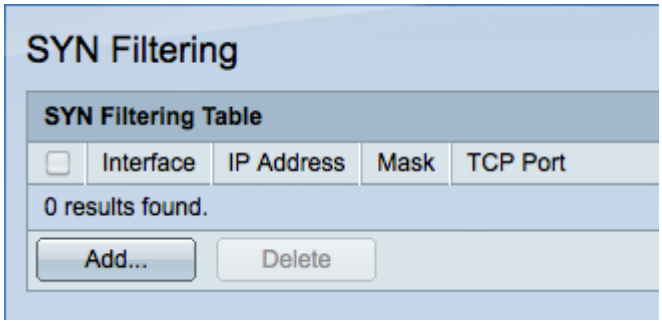
- Switches controlado 300 Series SF/SG

Versão de software

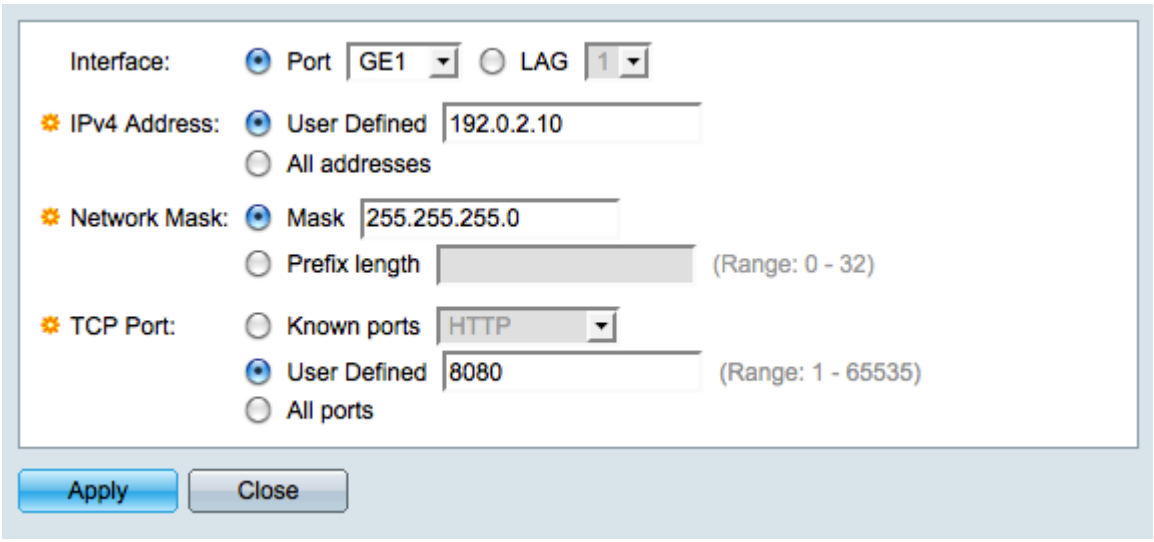
- v1.2.7.76

Configuração de filtração SYN

Etapa 1. Entre ao utilitário de configuração da Web e escolha a **Segurança > a recusa da prevenção do serviço > da filtração SYN**. A página de *filtração SYN* abre:



Etapa 2. O clique **adiciona** para adicionar um filtro novo SYN. O indicador de *filtração do Syn adicionar* aparece.



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 no campo de endereço do IPv4.

- Definido pelo utilizador — Incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT a ser filtrado para o tráfego TCP.

- Todos os endereços — Todos os endereços do IPv4 são filtrados para o tráfego TCP. Salte para pisar 6 se todos os endereços são escolhidos.

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. Clique o botão de rádio que corresponde com a porta TCP desejada a ser filtrada no campo de porta TCP. Estas são as portas virtuais que o tráfego de rede está dividido em.

- Portas conhecidas — Escolha uma porta TCP a ser filtrada da lista de drop-down conhecida das portas.

- Definido pelo utilizador — Entre em uma porta TCP a ser filtrada.

- Todas as portas — Todas as portas TCP são filtradas.

Etapa 7. O clique **aplica-se** para salvar suas mudanças e para clicar então **perto da** saída o indicador de *filtração do Syn adicionar*.