Configuração de técnicas de prevenção de negação de serviço (Security Suite) em switches empilháveis Sx500 Series

Objetivo

Os ataques de negação de serviço (DoS) ou negação de serviço distribuído (DDoS) restringem os usuários válidos a usar a rede. O invasor executa um ataque DOS inundando uma rede com muitas solicitações desnecessárias que ocupam toda a largura de banda da rede. Os ataques de DoS podem retardar uma rede ou desativar completamente uma rede por várias horas. A proteção do DoS é o principal recurso para melhorar a segurança da rede; ele detecta o tráfego anormal e o filtra.

Este artigo explica a configuração da negação de serviço nas configurações do Security Suite e várias técnicas usadas para a prevenção de negação de serviço.

Nota: Se a Prevenção de DoS escolhida for Nível de Sistema e Prevenção de Nível de Interface, os Endereços Marciais, a Filtragem SYN, a Proteção de Taxa SYN, a Filtragem ICMP e a Filtragem de Fragmentos IP poderão ser editados e configurados. Essas configurações também são explicadas neste artigo.

Note: Antes que a prevenção de DoS seja ativada, é necessário desvincular todas as Access Control Lists (ACLs) ou quaisquer políticas de QoS avançadas configuradas para a porta. A ACL e as políticas avançadas de QoS não estarão ativas quando a proteção DoS estiver ativada na porta.

Dispositivos aplicáveis

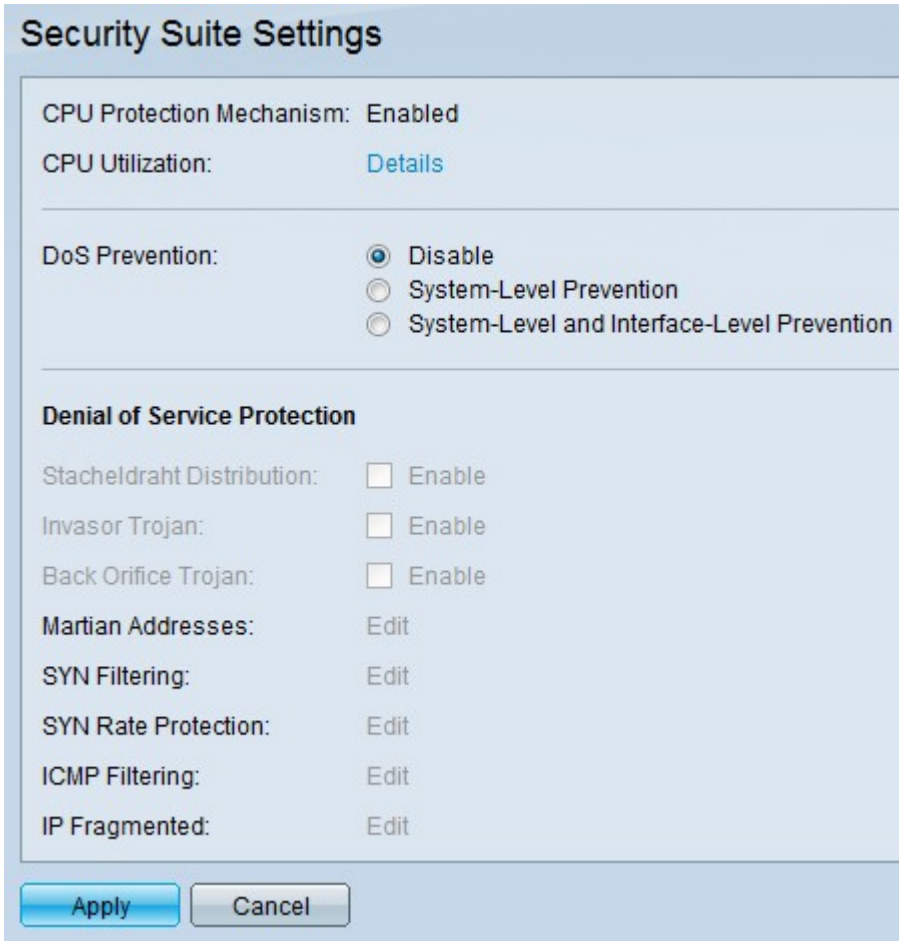
- Switches empilháveis Sx500 Series

Versão de software

- 1.3.0.62

Configuração de negação de serviço nas configurações do Security Suite

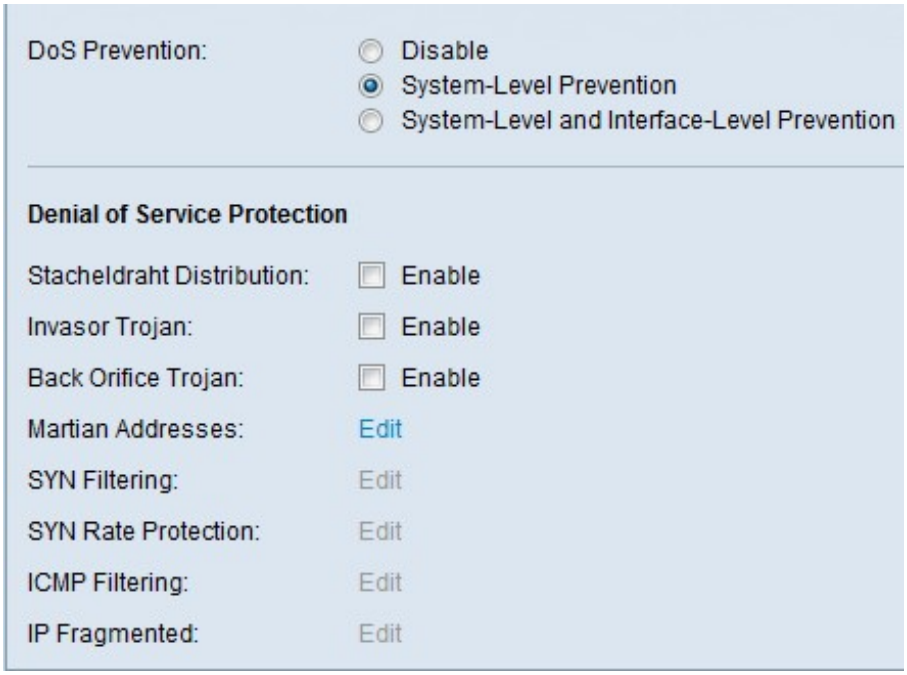
Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > Denial of Service Prevention > Security Suite Settings**. A página *Configurações do Security Suite* é aberta:



- Mecanismo de proteção da CPU — Este é o
- **Habilitado.** Isso indica que a Security Conversion Tool (SCT) está habilitada.
- Utilização da CPU — Clique
- **Detalhes** ao lado da utilização da CPU para ver as informações de utilização de recursos da CPU.

Etapa 2. Clique no botão de opção apropriado no campo Prevenção de DoS.

- Desabilitar — Para desabilitar a prevenção DoS.
- Prevenção em nível de sistema — evita ataques de Stacheldraht Distribution, Cavalo de Troia Invasor e Cavalo de Troia Back Orifice.
- Prevenção no nível do sistema e no nível da interface — evita ataques por interface no switch.



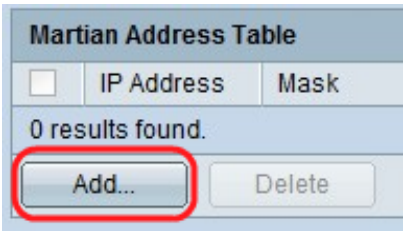
Etapa 3. Essas opções podem ser escolhidas para a proteção contra negação de serviço:

- Stacheldraht Distribution — Este é um exemplo de ataque de DDoS em que o invasor usa um programa cliente para se conectar aos computadores dentro da rede. Esses computadores enviam várias solicitações de login ao servidor interno e iniciam um ataque de DDoS.
- Cavalo de Troia Invasor — Se o computador está infectado por esse ataque, a porta TCP 2140 é usada para atividades mal-intencionadas. .
- Cavalo de Troia Back Orifice — Descarta os pacotes UDP usados para se comunicar com o servidor e o programa cliente para ataque DoS.

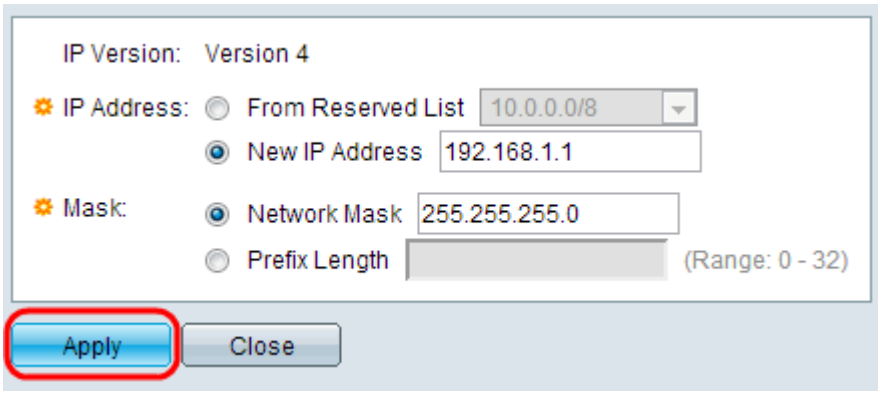
Configuração de endereços marcianos

Etapa 1. Clique em **Editar** no campo Endereços marcianos e a página *Endereços marcianos* será aberta. Os endereços marcianos indicam o endereço IP que pode ser a causa de um ataque na rede. Os pacotes que vêm dessas redes são descartados.

Etapa 2. Marque **Incluir** nos endereços marcianos reservados e clique em **Aplicar** para adicionar os endereços marcianos reservados na lista Prevenção de nível de sistema.



Etapa 3. Para adicionar um endereço marciano, clique em **Adicionar**. A página *Adicionar endereços marcianos* é exibida. Insira estes parâmetros:



Etapa 4. No campo Endereço IP, insira o endereço IP que precisa ser rejeitado.

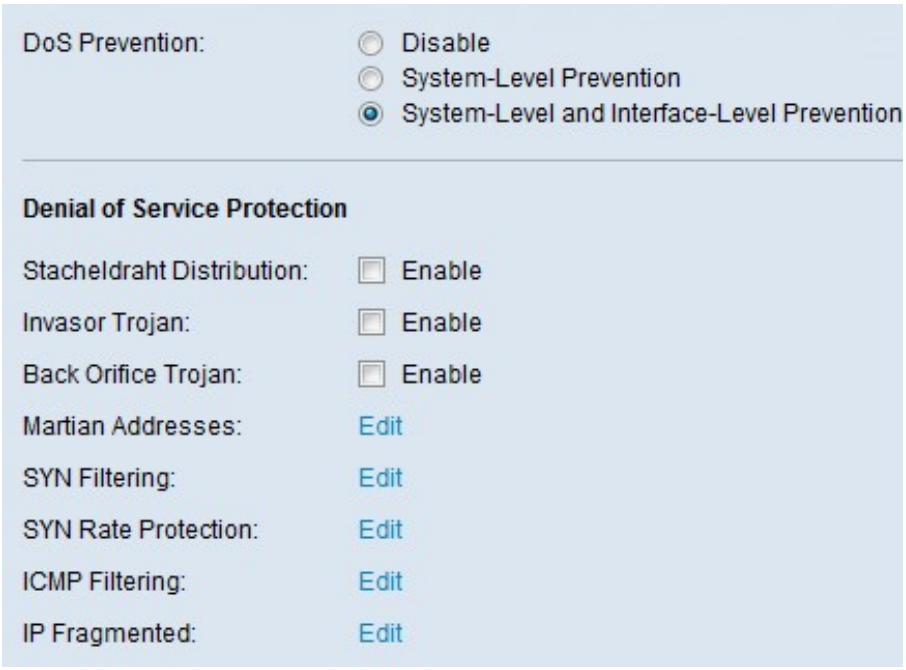
Etapa 5. A máscara do endereço IP para indicar o intervalo de endereços IP que devem ser rejeitados.

- Versão IP — A versão IP suportada. Atualmente, somente IPv4 é permitido.
- Na lista reservada — Escolha um endereço IP conhecido na lista reservada.
- Novo endereço IP — insira um endereço IP.
- Máscara de rede — Máscara de rede no formato decimal com pontos.
- Comprimento do prefixo — Prefixo do endereço IP para definir o intervalo de endereços IP para os quais a Prevenção de negação de serviço está habilitada.

Etapa 6. Clique em **Apply**, que faz com que o endereço marciano seja gravado no arquivo Running Configuration (Configuração em execução).

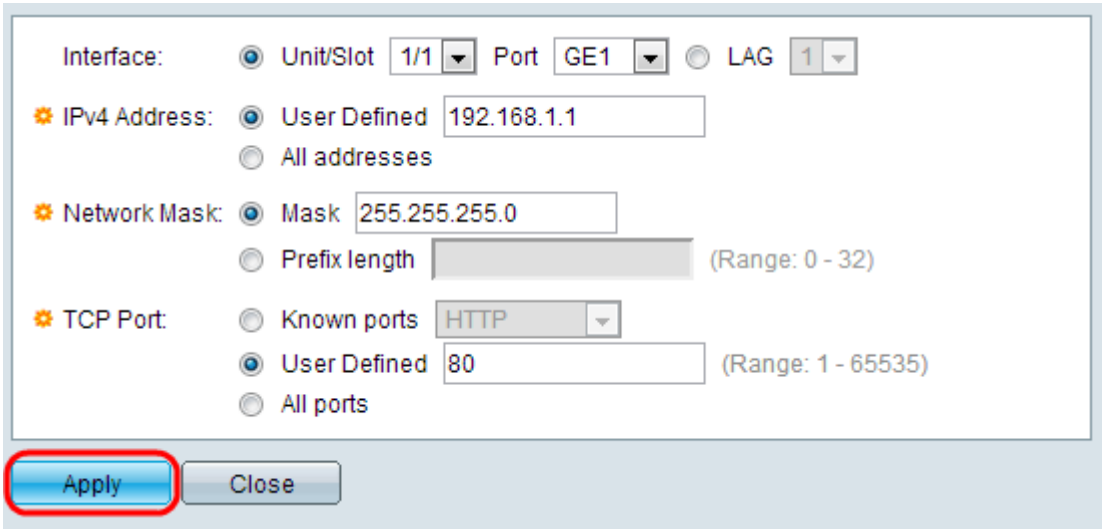
Configuração da filtragem SYN

A filtragem SYN permite que os administradores de rede descartem pacotes TCP ilegais com flag SYN. A filtragem de portas SYN é definida por porta.



Etapa 1. Para configurar a filtragem SYN, clique em **Editar** e a página *Filtragem SYN* será aberta:

Etapa 2. Clique em Add. A página *Adicionar filtragem SYN* é exibida. Insira estes parâmetros nos campos exibidos:

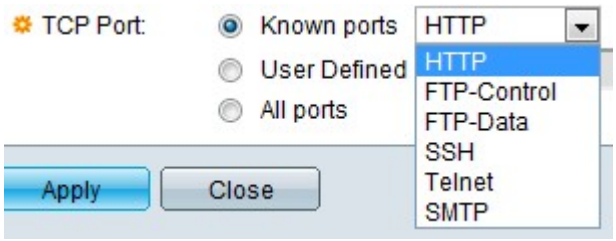


Etapa 3. Escolha a interface na qual o filtro precisa ser definido.

Etapa 4. Clique em **Definido pelo usuário** para fornecer um endereço IP para o qual o filtro está definido ou clique em **Todos os endereços**.

Etapa 5. A máscara de rede para a qual o filtro está ativado. Clique em **Comprimento do prefixo** para especificar o comprimento, seu intervalo é de 0 a 32 ou clique em **Máscara**

para inserir a máscara de sub-rede como em notação decimal pontuada.



Etapa 6. Clique na porta TCP de destino sendo filtrada. Eles são dos tipos:

- Portas conhecidas — Escolha uma porta na lista.
- Definido pelo usuário — Insira o número da porta.
- Todas as portas — Clique para indicar que todas as portas estão filtradas.

Passo 7. Clique em **Apply**, que faz com que a filtragem SYN seja gravada no arquivo de configuração atual.

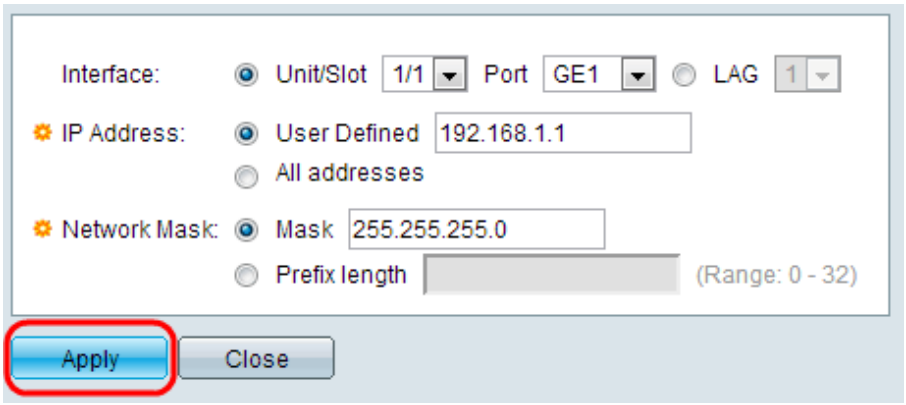
Configuração de filtragem ICMP

O Internet Control Message Protocol (ICMP) é um dos protocolos de Internet mais importantes. É um protocolo da camada de rede. O ICMP é usado pelos sistemas operacionais para enviar mensagens de erro para informar que o serviço solicitado não está disponível ou que um host específico não pode ser alcançado. Também é usado para enviar mensagens de diagnóstico. O ICMP não pode ser usado para trocar dados entre os sistemas. Geralmente são gerados em resposta a alguns erros nos datagramas IP.

O tráfego ICMP é um tráfego de rede muito crítico, mas também pode levar a muitos problemas de rede se for usado contra a rede por um invasor mal-intencionado. Isso traz à tona a necessidade de filtrar rigorosamente o tráfego ICMP que vem da Internet. A página *Filtragem ICMP* permite a filtragem de pacotes ICMP de fontes específicas. Isso minimiza a carga na rede caso haja algum ataque ICMP.

Etapa 1. Para configurar a Filtragem ICMP, clique em **Editar** e a página *Filtragem ICMP* será aberta.

Etapa 2. Clique em Add. A página *Adicionar filtragem ICMP* é exibida. Insira estes parâmetros nos campos exibidos:



Etapa 3. Escolha a interface na qual a filtragem ICMP está definida.

Etapa 4. Insira o endereço IPv4 para o qual a filtragem de pacotes ICMP está habilitada ou clique em **Todos os endereços** para bloquear pacotes ICMP de todos os endereços de origem. Se o endereço IP for inserido, insira a máscara ou o comprimento do prefixo.

Etapa 5. A máscara de rede para a qual a proteção de taxa está ativada. Escolha o formato da máscara de rede para o endereço IP de origem e clique em um dos campos.

- Máscara — Escolha a sub-rede à qual o endereço IP de origem pertence e insira a máscara de sub-rede no formato decimal pontuado.
- Clique em **Prefix Length** para especificar o comprimento e digitar o número de bits que consiste no prefixo do endereço IP de origem; seu intervalo é de 0 a 32.

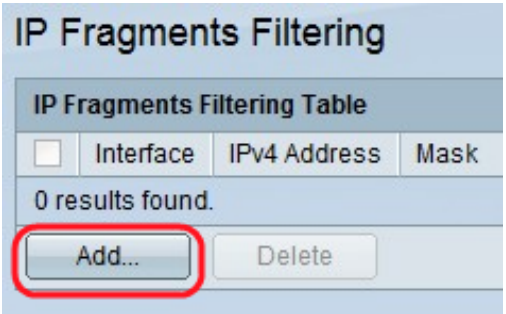
Etapa 6. Clique em **Apply**, que faz com que a filtragem ICMP seja gravada no arquivo de configuração atual.

Configuração da filtragem de fragmentos IP

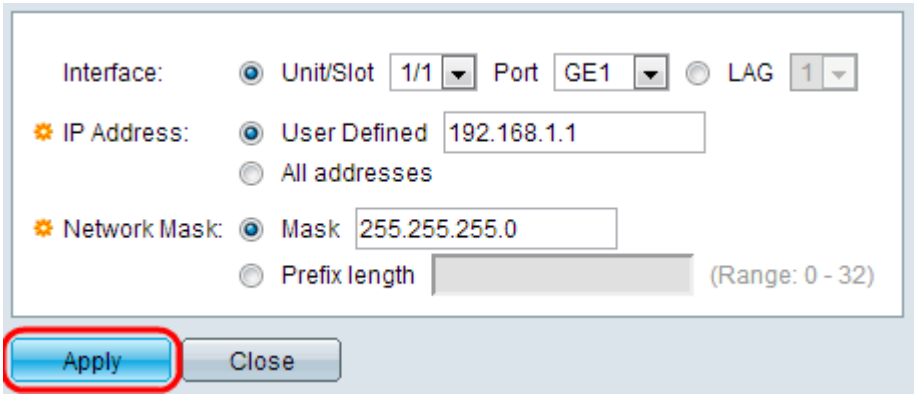
Todos os pacotes têm um tamanho de Unidade de Transmissão Máxima (MTU - Maximum Transmission Unit). MTU sendo o tamanho do maior pacote que uma rede pode transmitir. O IP tira a vantagem da fragmentação para que os pacotes possam ser formados, o que pode atravessar um link com uma MTU menor do que o tamanho do pacote original. Portanto, os pacotes cujos tamanhos sejam maiores que o MTU permitido do enlace devem ser divididos em pacotes menores para permitir que atravessem o enlace.

Por outro lado, a fragmentação também pode colocar muitos problemas de segurança. Assim, torna-se necessário bloquear fragmentos de IP, já que, às vezes, eles podem ser motivo de comprometimento do sistema.

Etapa 1. Para configurar a filtragem de fragmentos IP, clique em **Editar** e a página *Filtragem de Fragmentos ICMP* será aberta.



Etapa 2. Clique em Add. A página *Add IP Fragment Filtering* é exibida. Insira estes parâmetros nos campos exibidos:



Etapa 3. Interface — Escolha a interface na qual a fragmentação de IP é definida.

Etapa 4. IP Address — (Endereço IP) Insira o endereço IP para o qual a fragmentação de IP está habilitada ou clique em **All Addresses (Todos os endereços)** para bloquear os pacotes fragmentados de IP de todos os endereços de origem. Se o endereço IP for inserido, insira a máscara ou o comprimento do prefixo.

Etapa 5. Máscara de rede — A máscara de rede para a qual a fragmentação de IP está bloqueada. Escolha o formato da máscara de rede para o endereço IP de origem e clique em um dos campos.

- Máscara — Escolha a sub-rede à qual o endereço IP de origem pertence e insira a máscara de sub-rede no formato decimal pontuado.
- Clique em **Prefix Length** para especificar o comprimento e digitar o número de bits que consiste no prefixo do endereço IP de origem; seu intervalo é de 0 a 32.

Etapa 6. Clique em **Apply** para fazer com que a filtragem de fragmentos IP seja gravada no arquivo de configuração atual.