Configuração da recusa de técnicas de prevenção do serviço (série da Segurança) em switch empilhável do Sx500 Series

Objetivo

A recusa de serviço (DoS) ou a recusa distribuída de ataques do serviço (DDoS) restringem os usuários válidos para usar a rede. O atacante executa um ataque DOS inundando uma rede com muitos pedidos desnecessários que pegam toda a largura de banda da rede. Os ataques DoS podem ou retardar uma rede, ou tome completamente para baixo uma rede por diversas horas. A proteção de DOS é os recursos principais para melhorar a segurança de rede; detecta o tráfego anormal e filtra-o.

Este artigo explica a configuração da recusa de serviço nos ajustes da série da Segurança e nas várias técnicas usados para a recusa da prevenção do serviço.

Nota: Se a prevenção DoS escolhida é prevenção do nível de sistema e do Relação-nível, a seguir os endereços marciais, a filtração SYN, da taxa SYN proteção, filtragem ICMP, e filtração do fragmento IP podem ser editados e configurado. Estas configurações são explicadas igualmente neste artigo.

Nota: Antes que a prevenção DoS esteja ativada, é necessário desatar todo o Access Control Lists (ACLs) ou todas as políticas de QoS avançadas que forem configurados à porta. O ACL e as políticas de QoS avançadas não são ativos uma vez que a proteção de DOS é permitida na porta.

Dispositivos aplicáveis

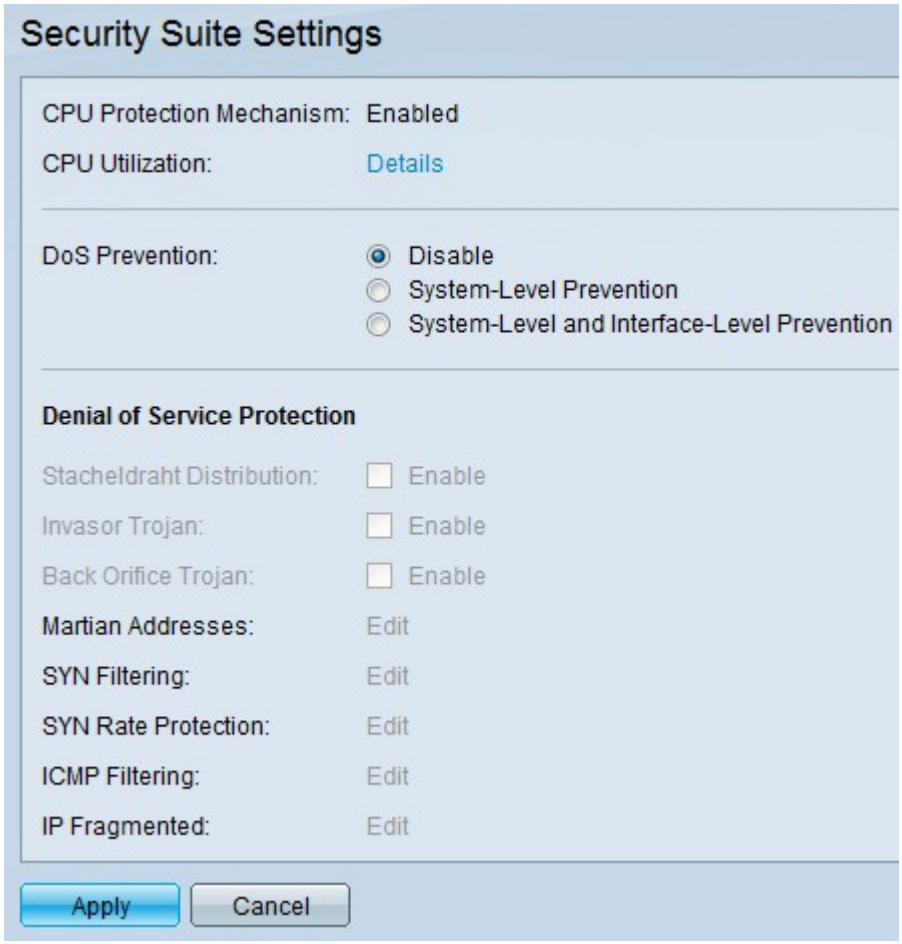
- Switch empilhável do Sx500 Series

Versão de software

- 1.3.0.62

Configuração da recusa de serviço em ajustes da série da Segurança

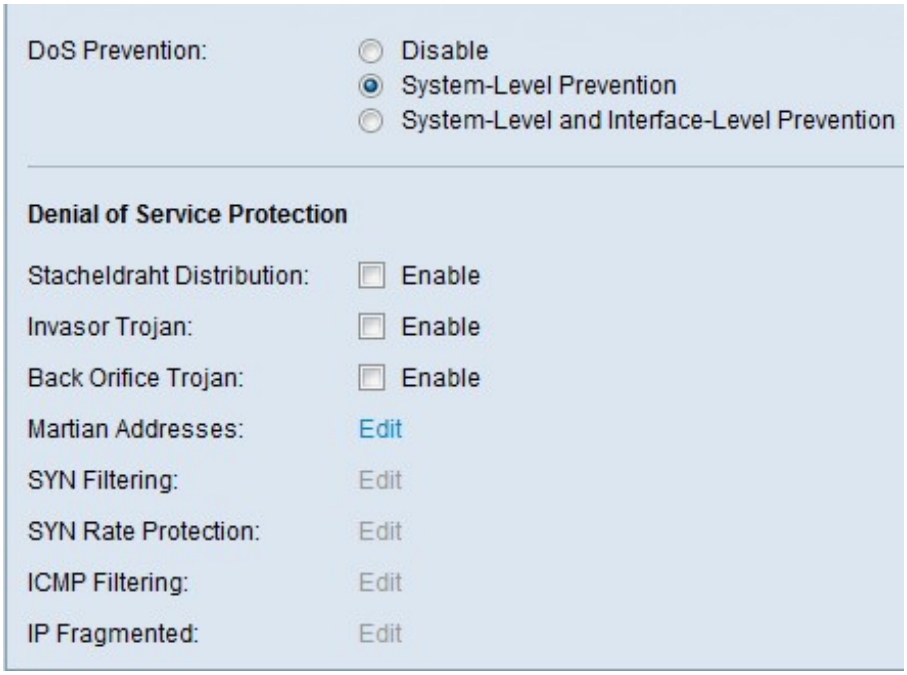
Etapa 1. Entre ao utilitário de configuração da Web, e escolha a **Segurança > a recusa de ajustes da série do > segurança da prevenção do serviço**. A página dos *ajustes da série da Segurança* abre:



- Mecanismo de proteção CPU — Isto é
- Habilitado. Isto indica que a ferramenta da conversão da Segurança (SCT) está permitida.
- Utilização CPU — Clique
- **Detalhes** ao lado da utilização CPU para ver a informação de utilização dos recursos do CPU.

Etapa 2. Clique o botão Appropriate Radio Button sob o campo da prevenção DoS.

- Desabilitação — Para desabilitar a prevenção DoS.
- Prevenção do nível de sistema — Isto impede ataques da distribuição de Stacheldraht, do Trojan de Invasor e do Trojan traseiro do orifício.
- Prevenção do nível de sistema e do Relação-nível — Isto impede ataques pela relação no interruptor.



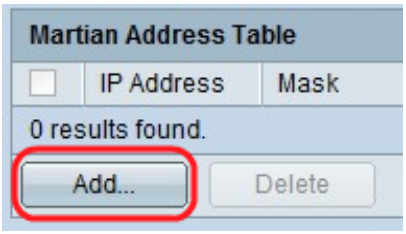
Etapa 3. Estas opções podem ser escolhidas para a recusa da proteção do serviço:

- Distribuição de Stacheldraht — Este é um exemplo do ataque de ddis onde o atacante usa um programa de cliente para conectar aos computadores dentro da rede. Aqueles computadores então mandam solicitações de login múltiplas ao servidor interno e começam um ataque de ddis.
- Trojan de Invasor — Se o computador é contaminado por este ataque, a porta TCP 2140 está usada para a atividade mal-intencionada.
- Trojan traseiro do orifício — Isto rejeita os pacotes de UDP que são usados para se comunicar com o server e o programa de cliente para o ataque DoS.

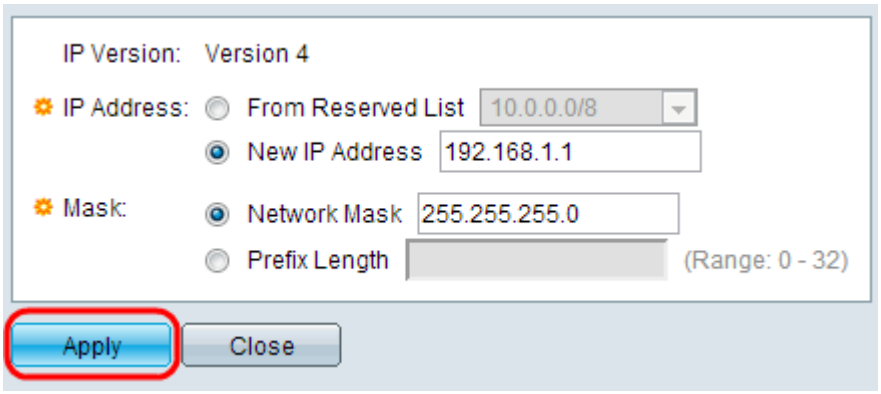
Configuração de endereços marcianos

Etapa 1. O clique **edita no** campo de endereços marciano então os *endereços que marcianos a* página abre. Os endereços marcianos indicam o endereço IP de Um ou Mais Servidores Cisco ICM NT que pode possivelmente ser a causa de um ataque na rede. Os pacotes que vêm destas redes são deixados cair.

Etapa 2. A verificação **inclui nos** endereços marcianos reservados e o clique **aplica-se** para adicionar os endereços marcianos reservados na lista da prevenção do nível de sistema.



Etapa 3. Para adicionar um clique marciano do endereço **adicionar**. A página dos *endereços de Marciano adicionar* é indicada. Incorpore estes parâmetros:



Etapa 4. No campo do endereço IP de Um ou Mais Servidores Cisco ICM NT incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT que necessidades de ser rejeitado.

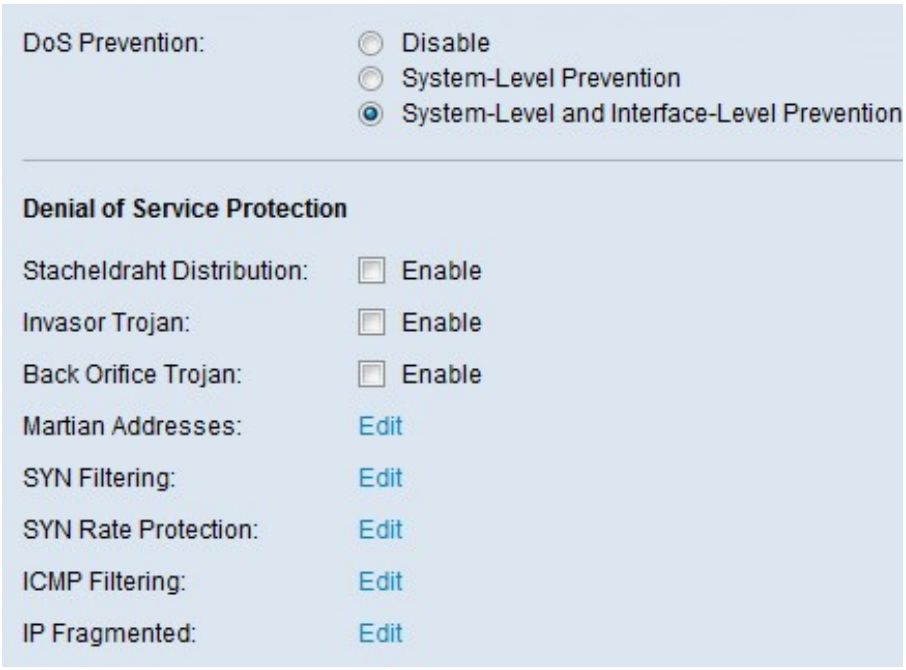
Etapa 5. A máscara do endereço IP de Um ou Mais Servidores Cisco ICM NT para indicar a escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT que devem ser rejeitados.

- Versão IP — A versão IP apoiada. Presentemente, somente o IPv4 é permitido.
- Da lista reservado — Escolha um endereço IP de Um ou Mais Servidores Cisco ICM NT conhecido da lista reservado.
- Endereço IP de Um ou Mais Servidores Cisco ICM NT novo — Incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT.
- Máscara de rede — Máscara de rede no formato do ponto decimal.
- Comprimento de prefixo — Prefixo do endereço IP de Um ou Mais Servidores Cisco ICM NT para definir a escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT para que a recusa da prevenção do serviço é permitida.

Etapa 6. O clique **aplica-se** que faz o endereço marciano a ser escrito ao arquivo de configuração running.

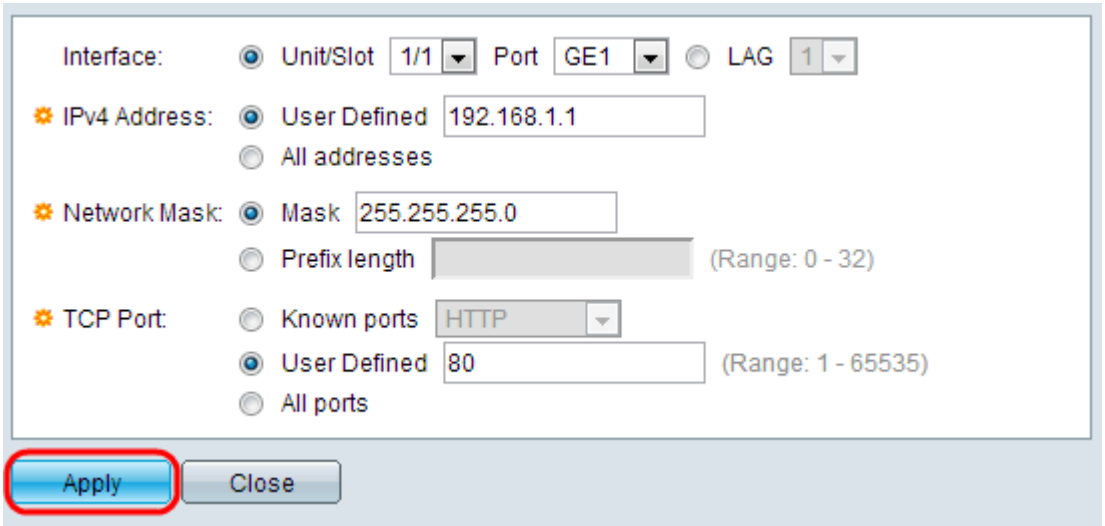
Configuração da filtração SYN

A filtração SYN permite que os administradores de rede deixem cair pacotes de TCP ilegais com bandeira SYN. A filtração da porta SYN é definida em uma base por porto.



Etapa1. Para configurar o clique de filtração SYN **edite** e a página de *filtração SYN* abre:

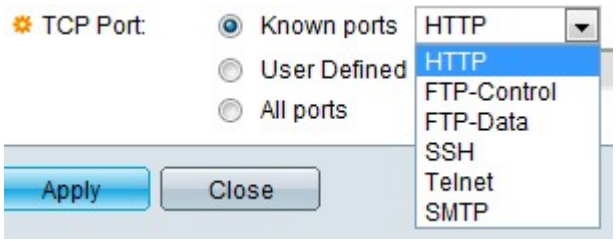
Etapa 2. O clique **adiciona**. A página de *filtração adicionar SYN* é mostrada. Incorpore estes parâmetros aos campos indicados:



Etapa 3. Escolha a relação em que o filtro precisa de ser definido.

Etapa 4. Clique **definido pelo utilizador** para dar um endereço IP de Um ou Mais Servidores Cisco ICM NT para que o filtro é definido ou para clicar **todos os endereços**.

Etapa 5. A máscara de rede para que o filtro é permitido. Clique o **comprimento de prefixo** a fim especificar o comprimento, sua escala é 0 a 32, ou clique a **máscara** para incorporar a máscara de sub-rede como ao dotted decimal notation.



Etapa 6. Clique a porta do TCP destino que está sendo filtrada. São dos tipos:

- Portas conhecidas — Escolha uma porta da lista.
- Definido pelo utilizador — Entre no número de porta.
- Todas as portas — Clique para indicar que todas as portas estão filtradas.

Etapa 7. O clique **aplica-se** que faz o SYN que filtra para ser escrito ao arquivo de configuração running.

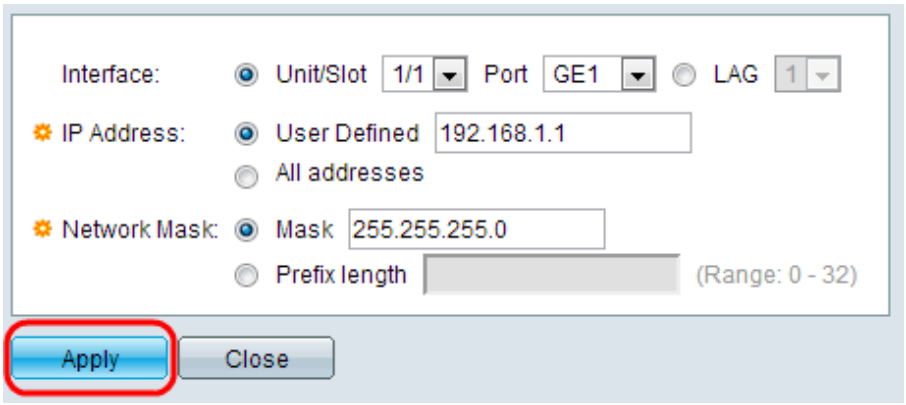
Configuração do filtragem ICMP

O Internet Control Message Protocol (ICMP) é um dos protocolos de internet os mais importantes. É um protocolo de camada de rede. O ICMP é usado pelos sistemas operacionais para enviar Mensagens de Erro para dizer que o serviço qual foi pedido não está disponível ou um host particular não pode ser alcançado. É usado igualmente para enviar mensagens de diagnóstico. O ICMP não pode ser usado aos dados de intercâmbio entre os sistemas. São gerados geralmente em resposta a alguns erros nas datagramas IP.

O tráfego ICMP é muito um tráfego de rede crítica mas pode igualmente conduzir a muitas questões de rede se é usado contra a rede por um atacante malicioso. Isto traz acima a necessidade para restritamente filtrar o tráfego ICMP que vem do Internet. A página do *filtragem ICMP* permite a filtração dos pacotes ICMP dos origens específica. Isto minimiza a carga na rede caso que se há qualquer ataque ICMP.

Etapa1. Para configurar o clique do filtragem ICMP **edite** e a página do *filtragem ICMP* abre.

Etapa 2. O clique **adiciona**. A página do *filtragem ICMP adicionar* é mostrada. Incorpore estes parâmetros aos campos indicados:



Etapa 3. Escolha a relação em que o filtragem ICMP é definido.

Etapa 4. Incorpore o endereço do IPv4 para que a filtração de pacote ICMP é permitida ou clique **todos os endereços** para obstruir pacotes ICMP de todos os endereços de origem. Se o endereço IP de Um ou Mais Servidores Cisco ICM NT é incorporado, incorpore a máscara ou o comprimento de prefixo.

Etapa 5. A máscara de rede para que a proteção da taxa é permitida. Escolha o formato da máscara de rede para o endereço IP de origem e clique um dos campos.

- Máscara — Escolha a sub-rede a que o endereço IP de origem pertence a e incorpore a máscara de sub-rede ao formato do ponto decimal.
- Clique o **comprimento de prefixo** a fim especificar o comprimento e para incorporar o número de bit que consiste no prefixo do endereço IP de origem, sua escala é 0 a 32.

Etapa 6. O clique **aplica-se** que faz o filtragem ICMP a ser escrito ao arquivo de configuração running.

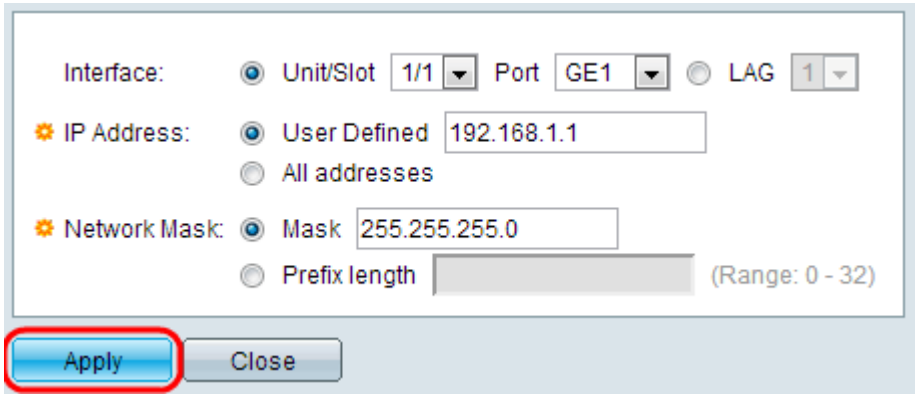
Configuração da filtração dos fragmentos IP

Todos os pacotes têm um tamanho da unidade de transmissão máxima (MTU). MTU que é o tamanho do pacote o maior que uma rede pode transmitir. O IP toma a vantagem da fragmentação de modo que os pacotes possam ser formados que podem atravessar através de um link com um MTU menor do que o tamanho de pacote original. Consequentemente, os pacotes cujos os tamanhos são maiores do que o MTU permissível do link devem ser divididos em pacotes menores para permitir que atravessem através do link.

Por outro lado, a fragmentação pode igualmente levantar muitos problemas de segurança. Assim torna-se necessário obstruir fragmentos IP enquanto às vezes podem ser uma razão para o acordo do sistema.

Etapa1. Para configurar os fragmentos IP que filtram o clique **edite** e os *fragmentos ICMP que filtram a* página abrem.

Etapa 2. O clique **adiciona**. *O fragmento IP adicionar que filtra a* página é mostrado. Incorpore estes parâmetros aos campos indicados:



Etapa 3. Relação — Escolha a relação em que a fragmentação de IP é definida.

Etapa 4. Endereço IP de Um ou Mais Servidores Cisco ICM NT — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para que a fragmentação de IP é permitida ou clique **todos os endereços** para obstruir pacotes fragmentados IP de todos os endereços de origem. Se o endereço IP de Um ou Mais Servidores Cisco ICM NT é incorporado, incorpore a máscara ou o comprimento de prefixo.

Etapa 5. Máscara de rede — A máscara de rede para que a fragmentação de IP é obstruída. Escolha o formato da máscara de rede para o endereço IP de origem e clique um dos campos.

- Máscara — Escolha a sub-rede a que o endereço IP de origem pertence a e incorpore a máscara de sub-rede ao formato do ponto decimal.
- Clique o **comprimento de prefixo** a fim especificar o comprimento e para incorporar o número de bit que consiste no prefixo do endereço IP de origem, sua escala é 0 a 32.

Etapa 6. O clique **aplica-se** para fazer os fragmentos IP que filtram para ser escrito ao arquivo de configuração running.