Configuration de déni de service des techniques de prévention (suite de Sécurité) sur des commutateurs empilables de gamme Sx500

Objectif

Les attaques du Déni de service (DOS) ou du Distributed Denial of Service (DDoS) limitent les utilisateurs valides pour utiliser le réseau. L'attaquant exécute une attaque DoS en inondant un réseau avec beaucoup de demandes inutiles qui prennent toute la bande passante du réseau. Les attaques DoS peuvent ou ralentir un réseau, ou prenez complètement vers le bas un réseau pendant plusieurs heures. La protection DOS est la fonction principale pour améliorer la sécurité des réseaux ; il détecte le trafic anormal et le filtre.

Cet article explique la configuration du Déni de service sur des configurations de suite de Sécurité et de diverses techniques utilisées pour la prévention de Déni de service.

Remarque: Si la prévention DOS choisie est prévention au niveau système et niveau de l'interface, alors les adresses, le filtrage de synchronisation, protection du débit martiaux de synchronisation, ICMP filtrant, et filtrage de fragment IP peuvent être édités et configurés. Ces configurations sont également expliquées en cet article.

Remarque: Avant que la prévention DOS soit lancée, il est nécessaire de défaire tout le Listes de contrôle d'accès (ACL) ou toutes les stratégies QoS avancées qui sont configurés au port. L'ACL et les stratégies QoS avancées ne sont pas en activité une fois que la protection DOS est activée sur le port.

Périphériques applicables

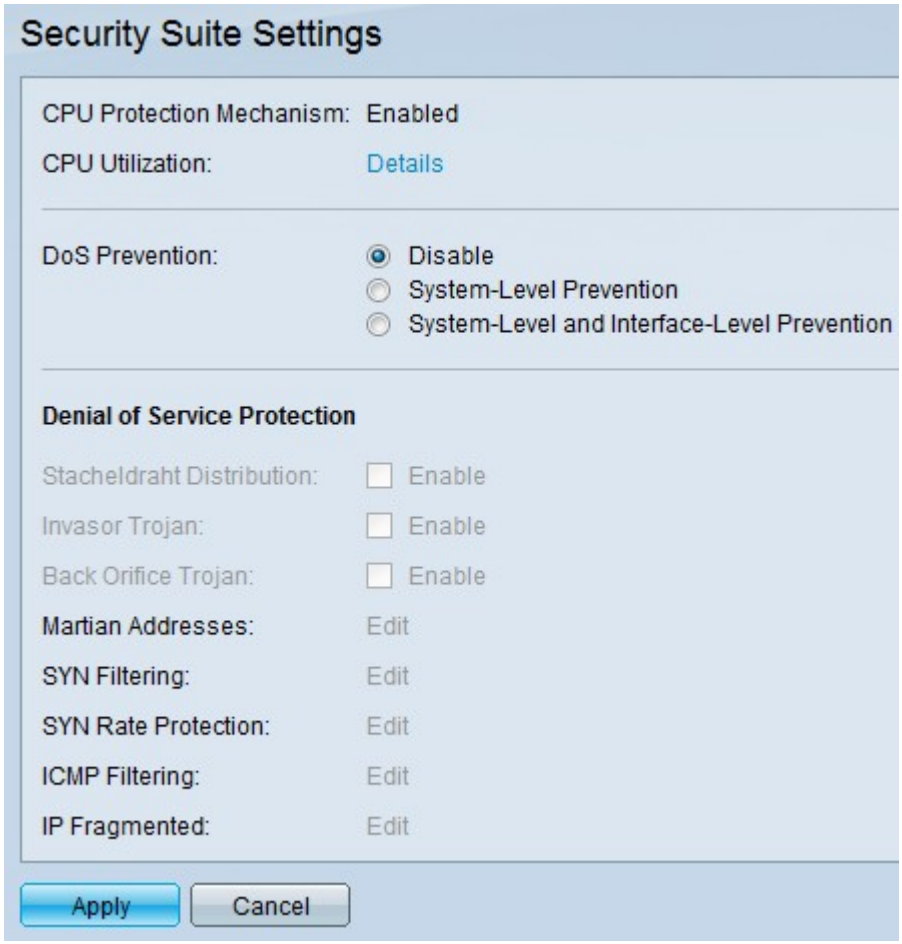
- Commutateurs empilables de gamme Sx500

Version de logiciel

- 1.3.0.62

Configuration de Déni de service sur des configurations de suite de Sécurité

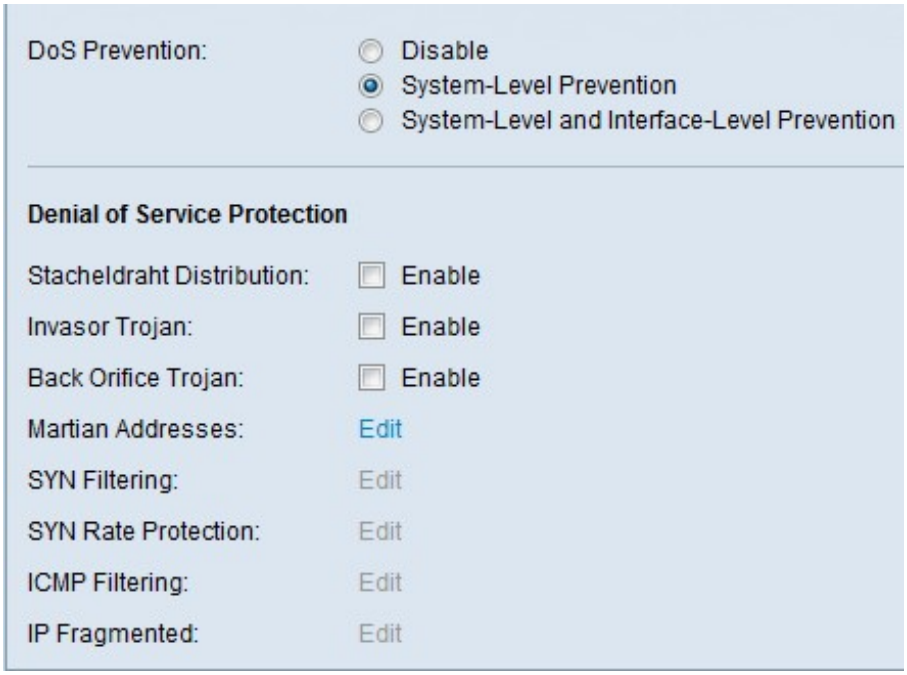
Étape 1. Ouvrez une session à l'utilitaire de configuration Web, et choisissez les **configurations de suite de Sécurité > de prévention > de Sécurité de Déni de service**. *La page Settings de suite de Sécurité* s'ouvre :



- Mécanisme de protection CPU — C'est
- **Activé**. Ceci indique que l'outil de conversion de Sécurité (SCT) est activé.
- Utilisation du processeur — Clic
- **Détails** près de l'utilisation du processeur pour visualiser les informations d'utilisation de ressource CPU.

Étape 2. Cliquez sur la case d'option appropriée sous le champ de prévention DOS.

- Débronchement — Pour désactiver la prévention DOS.
- Prévention au niveau système — Ceci empêche des attaques de la distribution de Stacheldraht, du cheval de Troie d'Invasor et du cheval de Troie arrière d'orifice.
- Prévention au niveau système et niveau de l'interface — Ceci empêche des attaques par interface sur le commutateur.



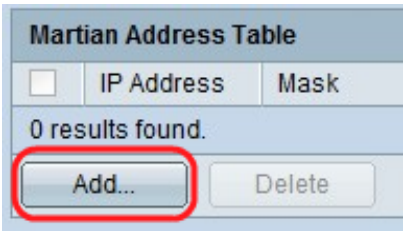
Étape 3. Ces options peuvent être choisies pour la protection de Déni de service :

- Distribution de Stacheldraht — C'est un exemple d'attaque DDoS où l'attaquant emploie un programme client pour se connecter aux ordinateurs à l'intérieur du réseau. Ces ordinateurs alors envoie de plusieurs demandes de procédure de connexion au serveur interne et commence une attaque DDoS.
- Cheval de Troie d'Invasor — Si l'ordinateur est infecté par cette attaque, le port TCP 2140 est utilisé pour l'action malveillante.
- Cheval de Troie arrière d'orifice — Ceci jette les paquets UDP qui sont utilisés pour communiquer avec le serveur et le programme client pour l'attaque DoS.

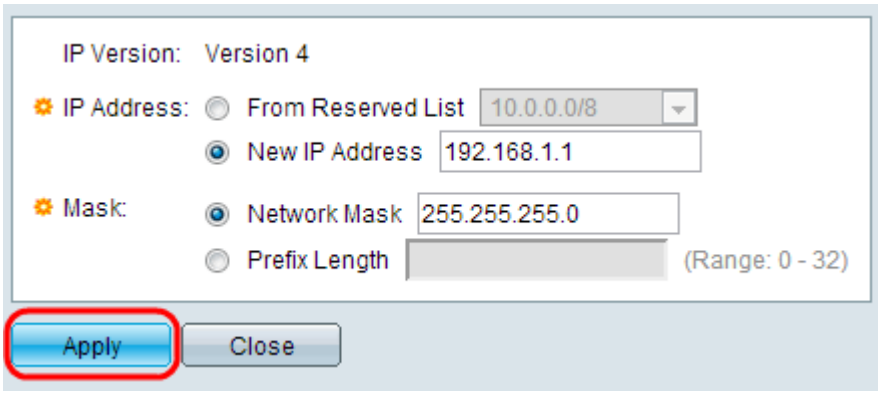
Configuration des adresses martiennes

Étape 1. Cliquez sur Edit dans la zone adresse martienne puis les *adresses martiennes que la* page s'ouvre. Les adresses martiennes indiquent l'adresse IP qui peut probablement être la cause d'une attaque sur le réseau. Des paquets qui proviennent ces réseaux sont lâchés.

Étape 2. Vérifiez **incluent** dans les adresses martiennes réservées et cliquent sur Apply pour ajouter les adresses martiennes réservées dans la liste au niveau système de prévention.



Étape 3. Pour ajouter une adresse martienne cliquez sur Add. La page *martienne d'adresses d'ajouter* est affichée. Entrez ces paramètres :



Étape 4. Dans le champ IP Address écrivez l'adresse IP qui les besoins d'être rejeté.

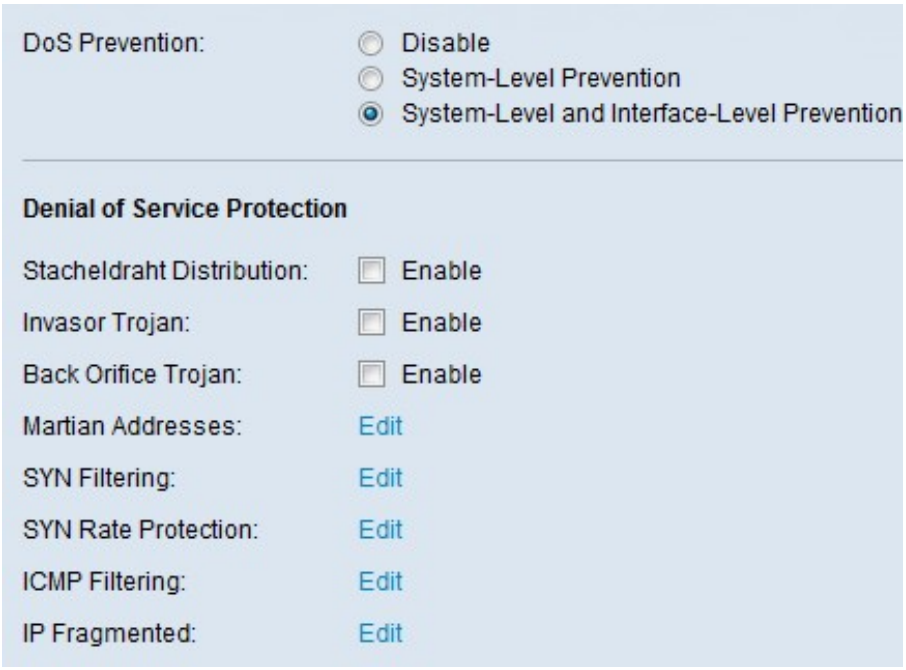
Étape 5. Le masque de l'adresse IP pour indiquer la plage des adresses IP qui devraient être rejetées.

- Version d'IP — La version d'IP prise en charge. Actuellement, on permet seulement l'ipv4.
- De la liste réservée — Choisissez une adresse IP connue de la liste réservée.
- Nouvelle adresse IP — Écrivez une adresse IP.
- Masque de réseau — Masque de réseau dans le format décimal séparé par des points.
- Longueur de préfixe — Préfixe de l'adresse IP pour définir la plage des adresses IP pour lesquelles la prévention de Déni de service est activée.

Étape 6. Cliquez sur Apply qui fait le discours martien à écrire au fichier de configuration en cours.

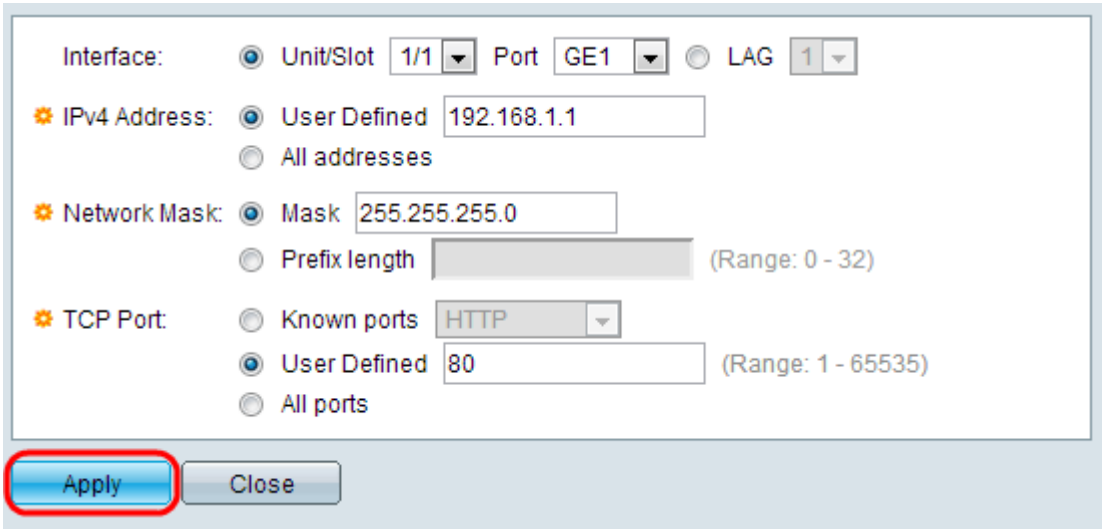
Configuration du filtrage de synchronisation

Le filtrage de synchronisation permet à des administrateurs réseau pour relâcher les paquets TCP illégaux avec l'indicateur de synchronisation. Le filtrage de port de synchronisation est défini sur une base de par-port.



Étape 1. Pour configurer le filtrage de synchronisation cliquez sur Edit et la page de *filtrage de synchronisation* s'ouvre :

Étape 2. Cliquez sur Add. La page de *filtrage de synchronisation d'ajouter* est affichée. Entrez ces paramètres dans les domaines affichés :

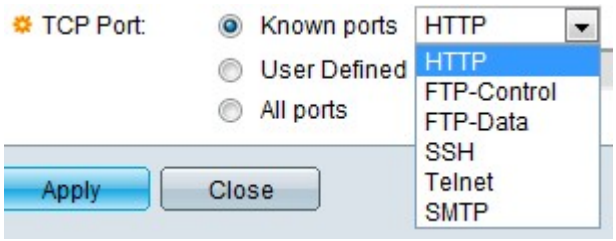


Étape 3. Choisissez l'interface sur laquelle le filtre doit être défini.

Étape 4. Cliquez sur **défini par l'utilisateur** pour donner une adresse IP pour laquelle le filtre est défini ou pour cliquer sur **toutes les adresses**.

Étape 5. Le masque de réseau pour lequel le filtre est activé. Cliquez sur la **longueur de préfixe** afin de spécifier la longueur, sa plage est de 0 à 32, ou cliquez sur le **masque** pour

écrire le masque de sous-réseau comme dans le dotted decimal notation.



Étape 6. Cliquez sur le port TCP de destination étant filtré. Ils sont des types :

- Ports connus — Choisissez un port de la liste.
- Défini par l'utilisateur — Introduisez le numéro de port.
- Tous les ports — Cliquez sur pour indiquer que tous les ports sont filtrés.

Étape 7. Cliquez sur Apply qui fait la synchronisation filtrant pour être écrit au fichier de configuration en cours.

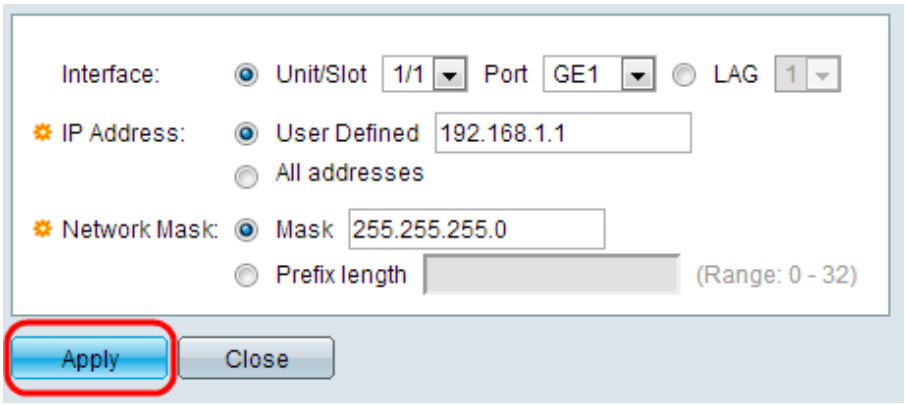
Configuration du filtrage d'ICMP

Le Protocole ICMP (Internet Control Message Protocol) est l'un des Internets Protocol les plus importants. C'est un protocole de couche réseau. L'ICMP est utilisé par les systèmes d'exploitation pour envoyer des messages d'erreur pour indiquer que le service ce qui a été demandé n'est pas disponible ou un hôte spécifique ne peut pas être atteint. Il est également utilisé pour envoyer les messages de diagnostic. L'ICMP ne peut pas être utilisé aux données d'échange entre les systèmes. Ils sont habituellement générés en réponse à quelques erreurs dans les datagrammes IP.

Le trafic d'ICMP est un trafic réseau très essentiel mais il peut également mener à beaucoup de problèmes de réseau s'il est utilisé contre le réseau par un attaquant malveillant. Ceci évoque le besoin de filtrer strictement le trafic d'ICMP qui provient l'Internet. La page de *filtrage d'ICMP* active le filtrage des paquets d'ICMP des sources particulières. Ceci réduirait le chargement sur le réseau au cas où s'il y a n'importe quelle attaque d'ICMP.

Étape 1. Pour configurer le filtrage d'ICMP cliquez sur Edit et la page de *filtrage d'ICMP* s'ouvre.

Étape 2. Cliquez sur Add. La page de *filtrage d'ICMP d'ajouter* est affichée. Entrez ces paramètres dans les domaines affichés :



Étape 3. Choisissez l'interface sur laquelle le filtrage d'ICMP est défini.

Étape 4. Entrez dans l'ipv4 addres pour lequel le filtrage des paquets d'ICMP est activé ou cliquez sur **toutes les adresses** pour bloquer des paquets d'ICMP de toutes les adresses sources. Si l'adresse IP est écrite, écrivez le masque ou la longueur de préfixe.

Étape 5. Le masque de réseau pour lequel la protection de débit est activée. Choisissez le format du masque de réseau pour l'adresse IP source et cliquez sur un des champs.

- Masque — Choisissez le sous-réseau auquel l'adresse IP source appartient à et écrivez le masque de sous-réseau dans le format décimal séparé par des points.
- Cliquez sur la **longueur de préfixe** afin de spécifier la longueur et écrire le nombre de bits qui comprend le préfixe d'adresse IP source, sa plage est de 0 à 32.

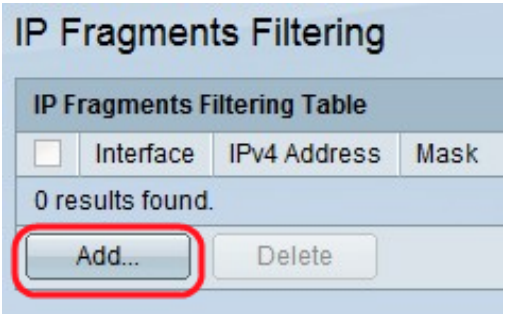
Étape 6. Cliquez sur Apply qui fait l'ICMP filtrant pour être écrit au fichier de configuration en cours.

Configuration du filtrage de fragments IP

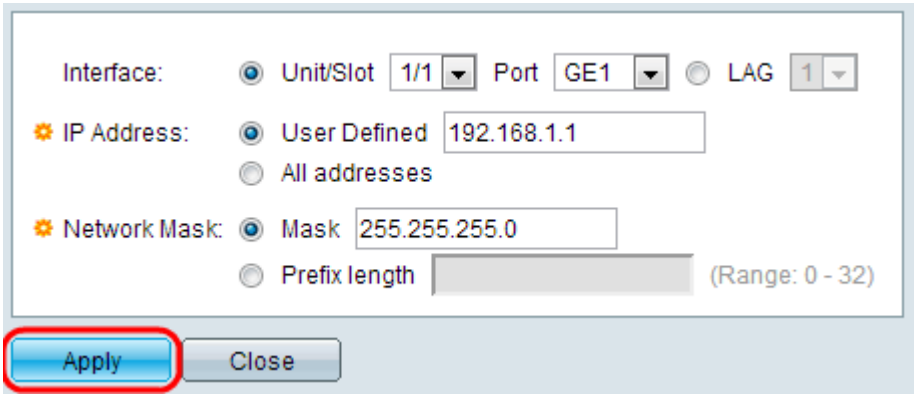
Tous les paquets ont une taille de Maximum Transmission Unit (MTU). MTU étant la taille du plus grand paquet qu'un réseau peut transmettre. L'IP profite de fragmentation de sorte qu'on puisse former des paquets qui peuvent traverser par un lien avec un plus petit MTU que la taille de paquet d'origine. Par conséquent, des paquets dont les tailles sont plus grandes que le MTU permis du lien doivent être divisés en plus petits paquets pour leur permettre pour traverser par le lien.

D'autre part, la fragmentation peut également poser beaucoup de problèmes de Sécurité. Ainsi il devient nécessaire de bloquer des fragments IP pendant que parfois ils peuvent être une raison pour la compromission de système.

Étape 1. Pour configurer le filtrage de fragments IP cliquez sur Edit et les *fragments d'ICMP filtrant la* page s'ouvre.



Étape 2. Cliquez sur Add. *Le fragment IP d'ajouter filtrant la* page est affiché. Entrez ces paramètres dans les domaines affichés :



Étape 3. Interface — Choisissez l'interface sur laquelle la fragmentation IP est définie.

Étape 4. Adresse IP — Écrivez l'adresse IP pour laquelle la fragmentation IP est activée ou cliquez sur **toutes les adresses** pour bloquer les paquets fragmentés par IP de toutes les adresses sources. Si l'adresse IP est écrite, écrivez le masque ou la longueur de préfixe.

Étape 5. Masque de réseau — Le masque de réseau pour lequel la fragmentation IP est bloquée. Choisissez le format du masque de réseau pour l'adresse IP source et cliquez sur un des champs.

- Masque — Choisissez le sous-réseau auquel l'adresse IP source appartient à et écrivez le masque de sous-réseau dans le format décimal séparé par des points.
- Cliquez sur la **longueur de préfixe** afin de spécifier la longueur et écrire le nombre de bits qui comprend le préfixe d'adresse IP source, sa plage est de 0 à 32.

Étape 6. Cliquez sur Apply **pour faire les fragments IP filtrant pour être écrit au fichier de configuration en cours.**