Konfiguration der SYN-Filterung für verwaltete Switches der Serie 300 synchronisieren

Ziel

TCP ist ein Transportschichtprotokoll, das eine zuverlässige, geordnete Paketübermittlung ermöglicht und die Fehlererkennung sowie die erneute Übertragung von Daten ermöglicht, bis die Daten korrekt und vollständig empfangen wurden. Bevor der Client Daten sendet, fordert er eine Verbindung mit einem synchronisierten (SYN-)Paket zum Server an, um die Verbindung zu starten. Der Server sendet dann ein SYN- und Bestätigungspaket (ACK) an den Client, und der Client sendet ein ACK-Paket, um die Serverantwort zu bestätigen. Nach dieser Drei-Wege-Handshake-Verbindung zwischen Client und Server können Daten gesendet werden.

Ein SYN-Flood-Angriff tritt auf, wenn dieser TCP-Handshake in drei Richtungen unterbrochen wird. Ein bösartiger Client überflutet den Server mit SYN-Paketen, der Server antwortet mit SYN- und ACK-Paketen für alle bösartigen Client-Anfragen, aber der böswillige Client sendet keine ACK-Pakete zurück. Der Server wartet auf ein ACK-Paket, das einfach nicht ankommt, das die Ressourcen des Servers für berechtigte Benutzer nutzt und schließlich das Netzwerk ausschaltet. Die SYN-Filterung verhindert diese Angriffe. In diesem Artikel wird erläutert, wie Sie die SYN-Filterung für die Managed Switches der Serie 300 konfigurieren.

Anwendbare Geräte

·Managed Switches der Serie SF/SG 300

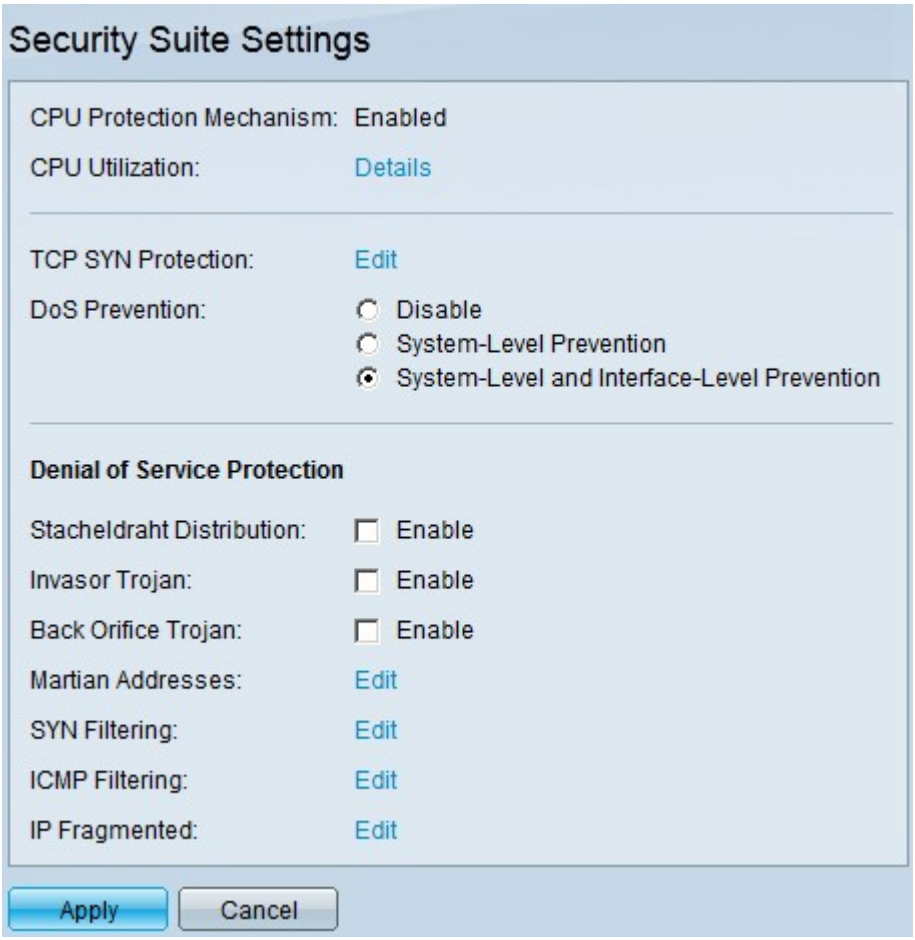
Softwareversion

·v1.2.7.76

Denial of Service Level Prevention aktivieren

Um die SYN-Filterung anwenden zu können, müssen Sie zunächst sicherstellen, dass der Switch die richtige 'Denial of Service'-Level-Prävention aufweist. In diesem Abschnitt wird erläutert, wie Sie die richtige Präventionsstufe für die Managed Switches der Serie 300 aktivieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Denial of Service Prevention > Security Suite Settings.** Die Seite *SicherheitsSuite-Einstellungen* wird geöffnet:



Schritt 2: Im Bereich der DoS-Prävention gibt es drei Ebenen der Prävention. Klicken Sie auf **Schutz auf Systemebene und Schnittstellenebene**. Auf dieser Ebene können Sie die SYN-Filterung konfigurieren.

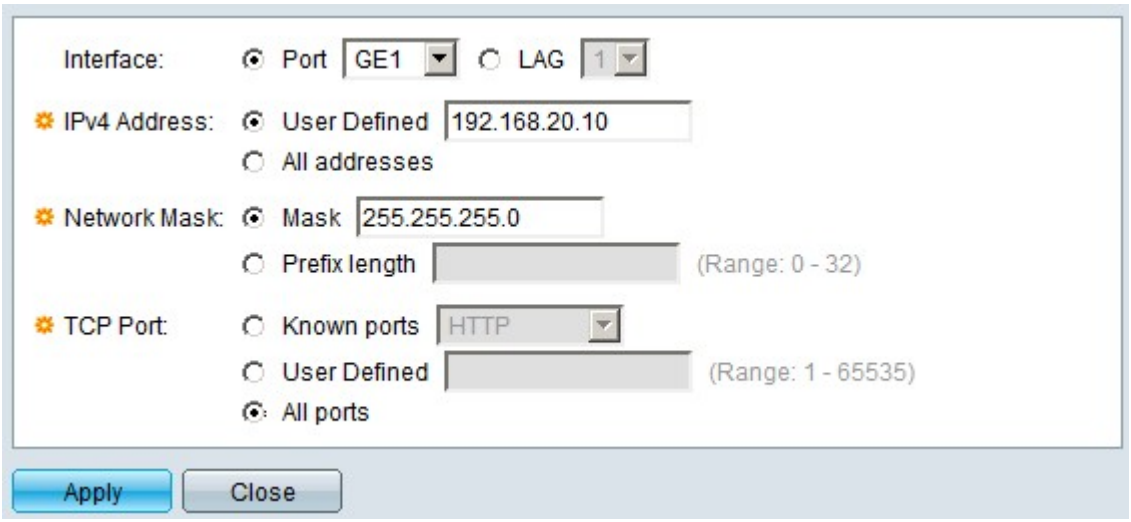
Schritt 3: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

TCP-SYN-Pakete filtern

In diesem Abschnitt wird erläutert, wie Sie die SYN-Filterung für die Managed Switches der Serie 300 konfigurieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Sicherheit > Denial of Service Prevention > SYN Filtering aus**. Die Seite *SYN-Filterung* wird geöffnet:

Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *SYN-Filterung hinzufügen* wird angezeigt:



Schritt 3: Klicken Sie im Feld Interface (Schnittstelle) auf das Optionsfeld einer der verfügbaren Schnittstellenoptionen:

·Port - Ermöglicht die Auswahl des Ports, von dem aus Sie SYN-Pakete aus der Dropdown-Liste "Port" filtern möchten.

·LAG: Ermöglicht die Auswahl der LAG, von der aus Sie SYN-Pakete filtern möchten, aus der Dropdown-Liste Link Aggregation Group (LAG). Eine LAG fasst mehrere Ports zu einem logischen Port zusammen.

Schritt 4: Klicken Sie im Feld IPv4 Address (IPv4-Adresse) auf das Optionsfeld einer der verfügbaren Optionen, um die IPv4-Adresse(n) zu definieren, aus der/denen SYN-Pakete gefiltert werden sollen:

·Benutzerdefiniert - Ermöglicht die Eingabe der IPv4-Adresse, für die der SYN-Paketfilter definiert ist.

·Alle Adressen - Diese Option filtert alle IPv4-Adressen für SYN-Pakete.

Schritt 5 Klicken Sie im Feld "Network Mask" (Netzwerkmaske) auf das Optionsfeld einer der verfügbaren Optionen, um die Netzwerkmaske der in Schritt 4 konfigurierten IP-Adresse einzugeben:

·Maske (Maske): Mit dieser Option können Sie die Subnetzmaske der IP-Adresse eingeben.

·Präfixlänge - Mit dieser Option können Sie die IP-Adresse der Subnetzmaske im Präfixformat eingeben.

Schritt 5: Klicken Sie im Feld TCP Port (TCP-Port) auf eine der verfügbaren Optionen, um die zu filterenden TCP-Ports zu bestimmen:

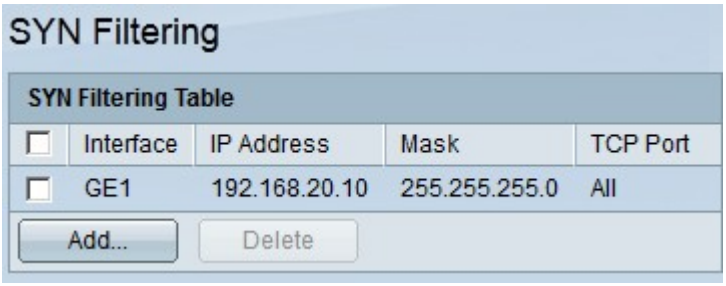
·Bekannte Ports - Mit dieser Option können Sie Ports aus der Dropdown-Liste "Bekannte Ports" auswählen. HTTP ist beispielsweise 80, TELNET 23.

·User Defined (Benutzerdefiniert) - Mit dieser Option können Sie die TCP-Portnummern eingeben, um zu filtern.

·Alle Ports - Diese Option filtert alle TCP-Ports.

Schritt 6: Klicken Sie auf **Apply**, um Ihre Konfiguration zu speichern. Die Änderungen werden

an der SYN-Filterungstabelle vorgenommen:



Schritt 7: (Optional) Um einen SYN-Filter zu löschen, aktivieren Sie in der SYN-Filtertabelle das Kontrollkästchen des SYN-Filters, den Sie löschen möchten. Klicken Sie anschließend auf **Löschen**.