# Security Suite-Einstellungen auf Managed Switches der Serie 300

## Ziel

Die Security Suite der Cisco Managed Switches der Serie 300 bietet Schutz vor DoS-Angriffen (Denial of Service). DoS-Angriffe überfluten Netzwerke mit falschem Datenverkehr, wodurch Netzwerkserver-Ressourcen für berechtigte Benutzer nicht verfügbar oder nicht erreichbar sind. Im Allgemeinen gibt es zwei Arten von DoS-Angriffen. Brute Force-DoS-Angriffe überfluten den Server und belasten die Bandbreite von Servern und Netzwerk. Systematische Angriffe manipulieren Protokollschwachstellen wie TCP SYN-Nachrichten an Crash-Systeme. In diesem Artikel werden die in der Security Suite für die Managed Switches der Serie 300 verfügbaren Einstellungen erläutert.

**Hinweis:** Zugriffskontrolllisten (ACLs) und erweiterte QoS-Richtlinien sind auf einem Port nicht aktiv, wenn der Schutz vor DoS-Angriffen aktiviert ist.

## Anwendbare Geräte

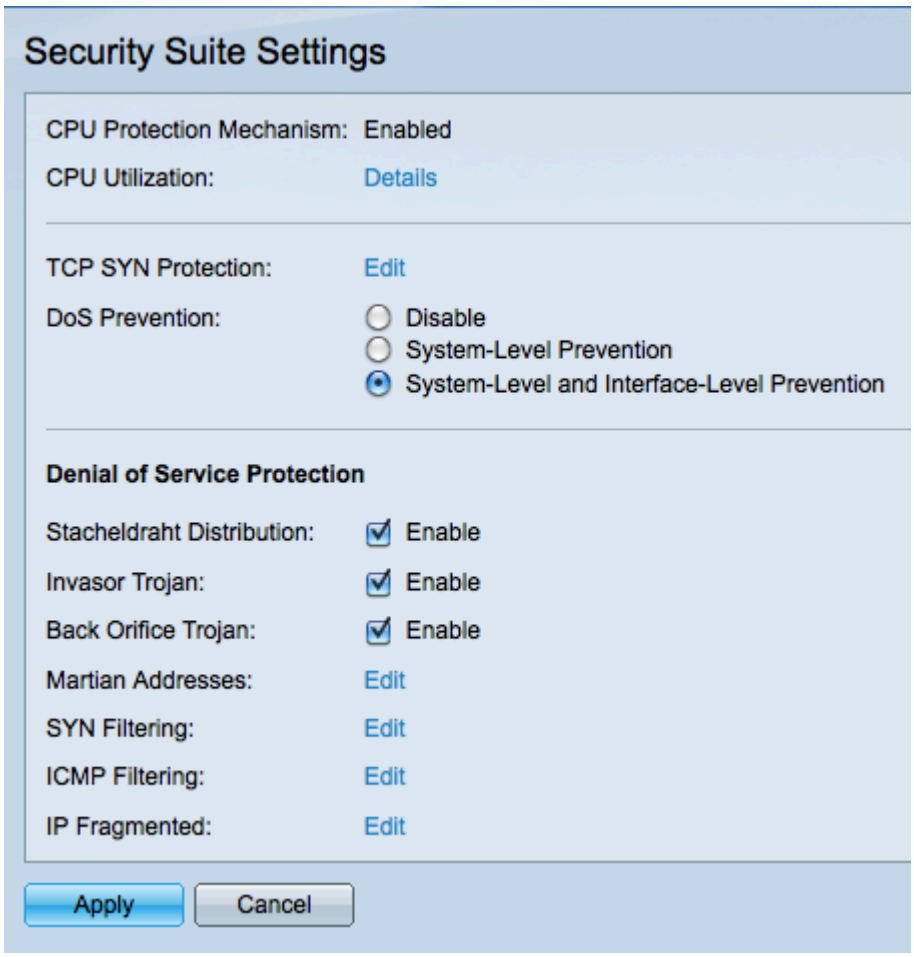
·Managed Switches der Serie SF/SG 300

## Softwareversion

·1.3.0.62

## Konfiguration der SicherheitsSuite-Einstellungen

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




**Hinweis:** Der CPU-Schutzmechanismus ist auf Managed Switches der Serie 300 standardmäßig aktiviert und kann nicht deaktiviert werden. Der Switch verwendet die Secure Core-Technologie (SCT), die es dem Switch ermöglicht, Management- und Protokolldatenverkehr unabhängig vom insgesamt empfangenen Datenverkehr zu verarbeiten.

Schritt 2: (Optional) Klicken Sie im Feld CPU Utilization (CPU-Auslastung) auf **Details**, um die CPU-Auslastung anzuzeigen. Weitere Informationen finden Sie im Artikel *CPU Utilization on 200/300 Series Managed Switches*.

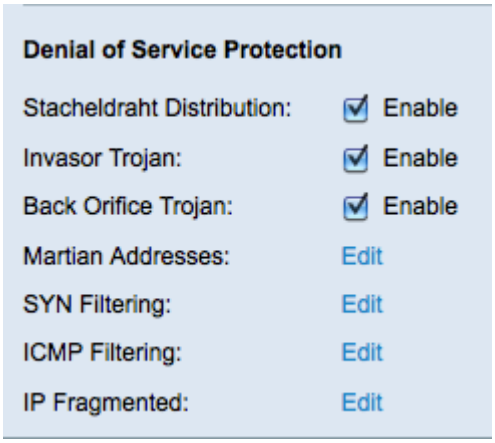
Schritt 3: (Optional) Klicken Sie im Feld TCP-SYN-Schutz auf **Bearbeiten**, um die TCP-SYN-Schutzeinstellungen zu bearbeiten. Weitere Informationen finden Sie im Artikel *Konfiguration der SYN-Filterung für verwaltete Switches der Serie 300*.

Schritt 4: Klicken Sie im Feld DoS Prevention (DoS-Prävention) auf das Optionsfeld, das der Methode der DoS-Prävention entspricht, die Sie verwenden möchten. Folgende Optionen stehen zur Verfügung:

·Disable (Deaktivieren) - DoS-Schutzfunktion deaktivieren Wenn Disable (Deaktivieren) ausgewählt ist, fahren Sie mit Schritt 13 fort.

·System - Level-Prevention - Aktiviert DoS-Schutzfunktionen zum Schutz vor Invasor-Trojanern, Stacheldraht-Distribution, Back-Orioper-Trojanern und Martian-Adressen.

·Schutz auf Systemebene und Schnittstellenebene - Aktiviert alle im Bereich "Denial of Service Protection" definierten Sicherheitsmaßnahmen.




Schritt 5: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Stacheldraht-Verteilung, um TCP-Pakete mit der Quell-TCP-Portnummer 1660 zu verwerfen.

Schritt 6: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Invasor Trojan, um TCP-Pakete mit dem Ziel-TCP-Port 2140 und dem Quell-TCP-Port 1024 zu verwerfen.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Enable (Aktivieren**) im Feld "Back Oriented Trojan", um UDP-Pakete mit einem Ziel-UDP-Port 31337 und einem Quell-UDP-Port 1024 zu verwerfen.

**Hinweis:** Obwohl es Hunderte von DoS-Angriffen gibt, werden die oben genannten Ports häufig für schädliche Aktivitäten ausgenutzt. Sie werden jedoch auch für legitimen Datenverkehr verwendet.  Wenn ein Gerät einen der oben genannten Ports verwendet, werden diese Informationen blockiert.

Schritt 8: Klicken Sie im Feld "Martische Adressen" auf **Bearbeiten**, um die Tabelle für Marsadressen zu bearbeiten. Die Martian Addresses Table verwirft Pakete von ausgewählten IP-Adressen. Informationen zum Bearbeiten der Liste der Marsadressen finden Sie im Artikel *"Denial of Service (DoS) Martian Address Configuration on 300 Series Managed Switches"*.

**Hinweis:** Für die Schritte 9-12 muss in Schritt 4 der Schutz auf Systemebene und Schnittstellenebene ausgewählt werden. Fahren Sie mit Schritt 13 fort, wenn Sie einen anderen DoS-Präventionstyp gewählt haben.

Schritt 9: Klicken Sie im Feld SYN-Filterung auf **Bearbeiten**, damit der Administrator bestimmte TCP-Ports blockieren kann. Informationen zum Konfigurieren der SYN-Filterung finden Sie im Artikel *Konfiguration der DoS-SYN-Filterung für verwaltete Switches der Serie 300.*

Schritt 10: Klicken Sie im Feld SYN Rate Protection (SYN-Ratenschutz) auf **Edit (Bearbeiten** ), um die Anzahl der empfangenen SYN-Pakete zu begrenzen. Informationen zum Konfigurieren des SYN-Ratenschutzes finden Sie im Artikel *SYN Rate Protection für Managed Switches der Serie 300*.

Schritt 11: Klicken Sie im Feld ICMP-Filterung auf **Bearbeiten**, um die Blockierung von ICMP-Paketen bestimmter Quellen zuzulassen. Informationen zum Konfigurieren der ICMP-Filterung finden Sie im Artikel *Konfiguration der ICMP-Filterung für Managed Switches der Serie 300.*

Schritt 12: Klicken Sie im Feld IP Fragmentierte IP-Pakete auf **Bearbeiten**, um fragmentierte IP-Pakete zu blockieren. Informationen zum Konfigurieren der IP-Fragmentfilterung finden

Sie im Artikel *Konfiguration der IP-Fragmentierungsfilterung für Managed Switches der Serie 300 (DoS)*.

Schritt 13: Klicken Sie auf **Apply**, um die Änderungen zu speichern, oder auf **Cancel (Abbrechen),** um die Änderungen abzubrechen.