Konfiguration von Denial of Service Prevention-Techniken (Security Suite) auf Stackable Switches der Serie Sx500

Ziel

Denial of Service (DoS)- oder Distributed Denial of Service (DDoS)-Angriffe schränken gültige Benutzer ein, das Netzwerk zu verwenden. Der Angreifer führt einen DOS-Angriff durch, indem er ein Netzwerk mit vielen unnötigen Anfragen überflutet, die die gesamte Bandbreite des Netzwerks beanspruchen. DoS-Angriffe können entweder das Netzwerk verlangsamen oder das Netzwerk mehrere Stunden lang komplett außer Betrieb setzen. Der DoS-Schutz ist das wichtigste Merkmal zur Verbesserung der Netzwerksicherheit. es erkennt den ungewöhnlichen Datenverkehr und filtert ihn.

In diesem Artikel wird die Konfiguration von Denial of Service für SicherheitsSuite-Einstellungen und verschiedene Techniken erläutert, die für Denial of Service Prevention verwendet werden.

Hinweis: Wenn der gewählte DoS-Schutz auf Systemebene und auf Schnittstellenebene definiert ist, können die Martial-Adressen, die SYN-Filterung, der SYN-Ratenschutz, die ICMP-Filterung und die IP-Fragment-Filterung bearbeitet und konfiguriert werden. Diese Konfigurationen werden auch in diesem Artikel erläutert.

Hinweis: Bevor die DoS-Prävention aktiviert wird, müssen alle Zugriffskontrolllisten (ACLs) oder alle erweiterten QoS-Richtlinien, die für den Port konfiguriert sind, deinstalliert werden. ACL und erweiterte QoS-Richtlinien sind nicht aktiv, sobald der DoS-Schutz auf dem Port aktiviert ist.

Anwendbare Geräte

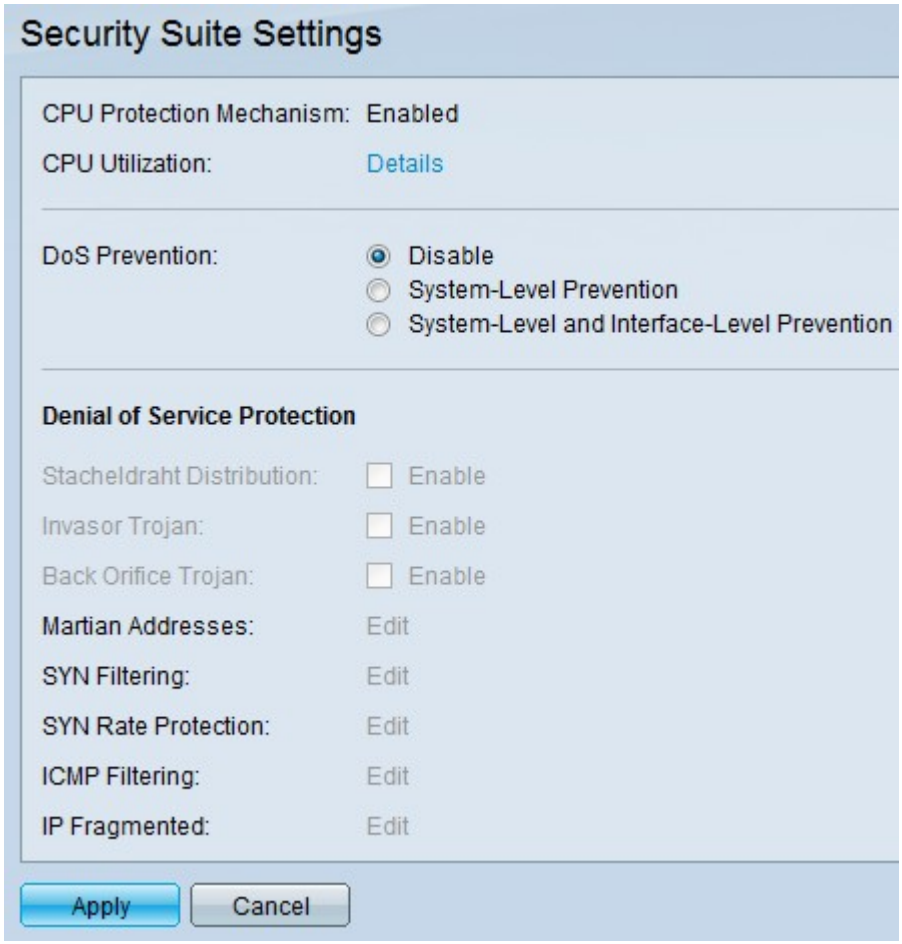
- Stackable Switches der Serie Sx500

Softwareversion

- 1,3 0,62

Konfiguration der Denial-of-Service-Einstellungen für die Security Suite

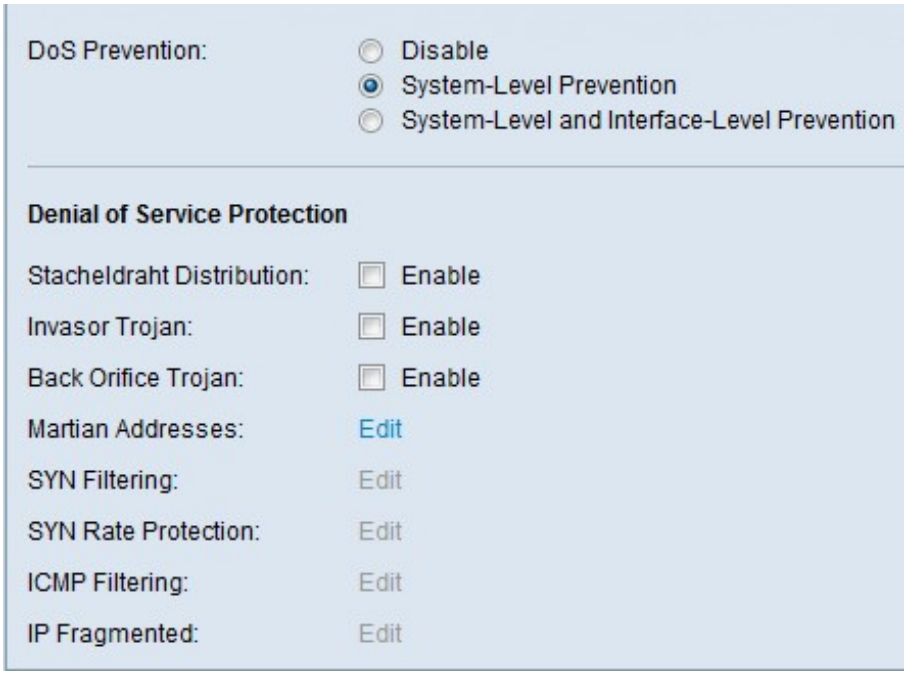
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Denial of Service Prevention > Security Suite Settings aus**. Die Seite *SicherheitsSuite-Einstellungen* wird geöffnet:



- CPU-Schutzmechanismus - Dies ist
- **Aktiviert**. Dies zeigt an, dass das Security Conversion Tool (SCT) aktiviert ist.
- CPU-Auslastung - Klicken Sie auf
- **Details** neben der CPU-Auslastung, um Informationen zur CPU-Ressourcenauslastung anzuzeigen.

Schritt 2: Klicken Sie im Feld "DoS Prevention" auf das entsprechende Optionsfeld.

- Disable (Deaktivieren) - So deaktivieren Sie die DoS-Prävention.
- Vorbeugung auf Systemebene - Diese Funktion verhindert Angriffe durch Stacheldraht Distribution, Invasor Trojan und Back Orioption Trojan.
- Schutz auf Systemebene und Schnittstellenebene - Diese Funktion verhindert Angriffe auf einzelne Schnittstellen des Switches.



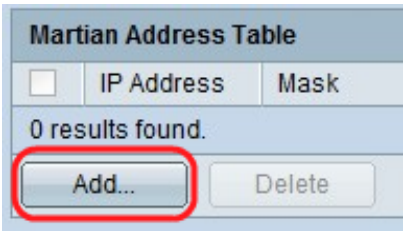
Schritt 3: Diese Optionen können für "Denial of Service Protection" ausgewählt werden:

- Stacheldraht-Verteilung - Dies ist ein Beispiel für einen DDoS-Angriff, bei dem der Angreifer ein Clientprogramm verwendet, um eine Verbindung zu den Computern im Netzwerk herzustellen. Diese Computer senden dann mehrere Anmeldeanfragen an den internen Server und starten einen DDoS-Angriff.
- Invasor Trojan (Invasor-Trojaner): Wenn der Computer von diesem Angriff infiziert ist, wird der TCP-Port 2140 für schädliche Aktivitäten verwendet. .
- Back Orioping Trojan (Trojaner für die Rückseite): Dieser Befehl verwirft UDP-Pakete, die zur Kommunikation mit dem Server- und Clientprogramm für DoS-Angriffe verwendet werden.

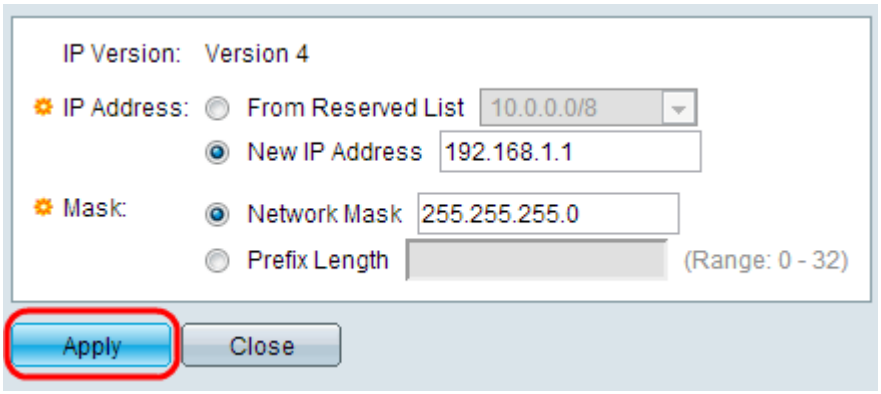
Konfiguration der Marsadressen

Schritt 1: Klicken Sie im Feld "Martian Addresses" auf **Edit** (**Bearbeiten**), und die Seite "*Martian Addresses"* wird geöffnet. Marsadressen geben die IP-Adresse an, die möglicherweise die Ursache eines Angriffs auf das Netzwerk sein kann. Pakete, die von diesen Netzwerken kommen, werden verworfen.

Schritt 2: Markieren Sie **Include** in the Reserved Martian Addresses (Eingeschränkte Marsadressen **einschließen** und klicken Sie auf **Apply**, um die reservierten Marsadressen in der Liste für den Schutz auf Systemebene hinzuzufügen.



Schritt 3: Um eine Marsadresse hinzuzufügen, klicken Sie auf **Hinzufügen**. Die Seite *Marsadressen hinzufügen* wird angezeigt. Geben Sie folgende Parameter ein:



Schritt 4: Geben Sie im Feld IP Address (IP-Adresse) die IP-Adresse ein, die abgelehnt werden muss.

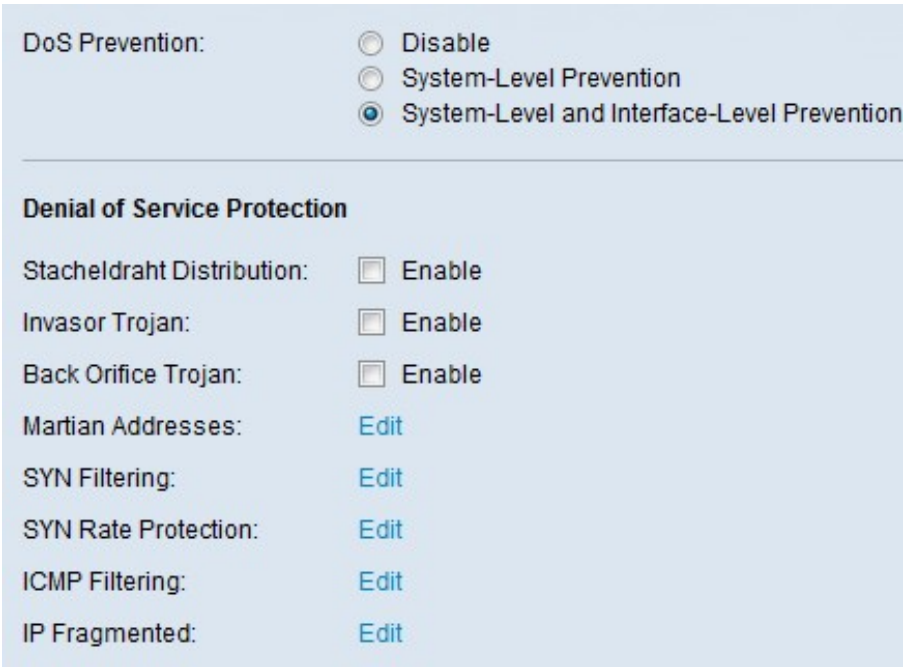
Schritt 5: Die Maske der IP-Adresse, um den IP-Adressbereich anzugeben, der abgelehnt werden soll.

- IP-Version - Die unterstützte IP-Version. Derzeit ist nur IPv4 zulässig.
- Aus reservierter Liste: Wählen Sie eine bekannte IP-Adresse aus reservierter Liste aus.
- Neue IP-Adresse - Geben Sie eine IP-Adresse ein.
- Netzwerkmaske - Netzwerkmaske im Dezimalpunktformat.
- Präfixlänge - Präfix der IP-Adresse, um den Bereich der IP-Adressen festzulegen, für die der 'Denial of Service Prevention' aktiviert ist.

Schritt 6: Klicken Sie auf **Apply**, wodurch die Martian-Adresse in die Running Configuration-Datei geschrieben wird.

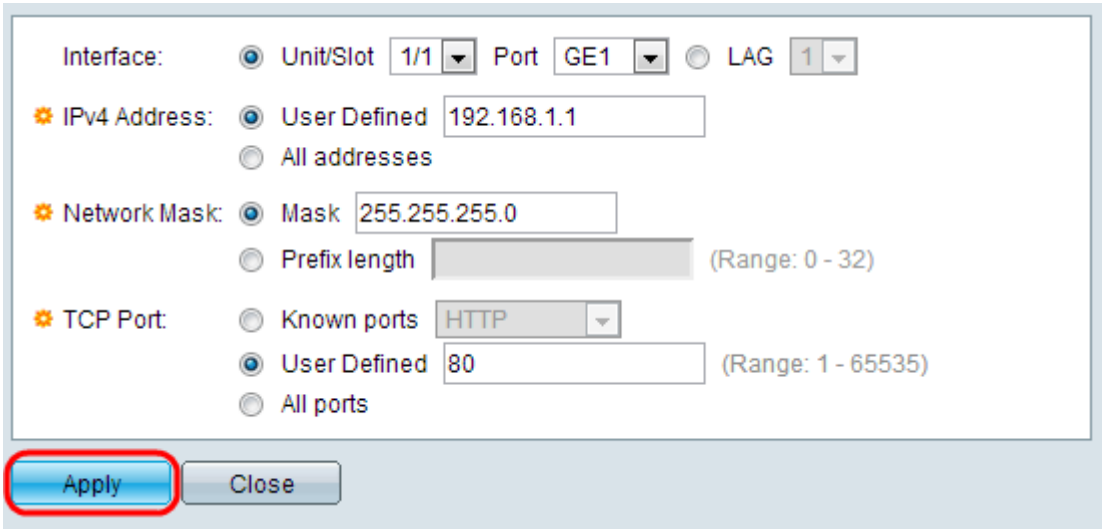
Konfiguration der SYN-Filterung

Die SYN-Filterung ermöglicht Netzwerkadministratoren, illegale TCP-Pakete mit SYN-Flag zu verwerfen. Die SYN-Portfilterung wird pro Port definiert.



Schritt 1: Um die SYN-Filterung zu konfigurieren, klicken Sie auf **Bearbeiten**, und die Seite *SYN-Filterung* wird geöffnet:

Schritt 2: Klicken Sie auf **Hinzufügen**. Die Seite *SYN-Filterung hinzufügen* wird angezeigt. Geben Sie die folgenden Parameter in die angezeigten Felder ein:

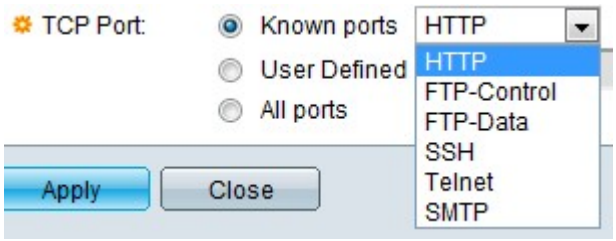


Schritt 3: Wählen Sie die Schnittstelle aus, auf der der Filter definiert werden soll.

Schritt 4: Klicken Sie auf **Benutzerdefiniert**, um eine IP-Adresse anzugeben, für die der Filter definiert ist, oder klicken Sie auf **Alle Adressen**.

Schritt 5: Die Netzwerkmaske, für die der Filter aktiviert ist. Klicken Sie auf **Prefix Length**, um die Länge anzugeben. Der Bereich liegt zwischen 0 und 32, oder klicken Sie auf **Mask**

(Maske), um die Subnetzmaske wie in der Notation mit Dezimalpunkten einzugeben.



Schritt 6: Klicken Sie auf den Ziel-TCP-Port, der gefiltert wird. Es gibt verschiedene Typen:

- Bekannte Ports - Wählen Sie einen Port aus der Liste aus.
- User Defined (Benutzerdefiniert) - Geben Sie die Portnummer ein.
- All Ports (Alle Ports): Klicken Sie, um anzuzeigen, dass alle Ports gefiltert sind.

Schritt 7: Klicken Sie auf **Apply**, wodurch die SYN-Filterung in die aktuelle Konfigurationsdatei geschrieben wird.

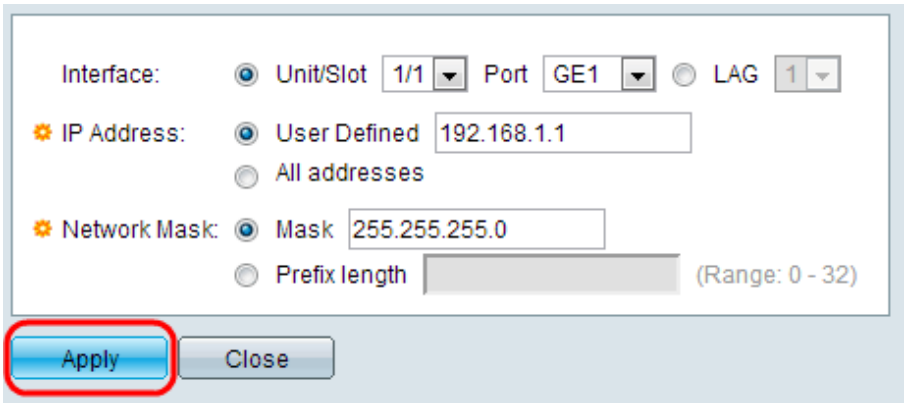
Konfiguration der ICMP-Filterung

Internet Control Message Protocol (ICMP) ist eines der wichtigsten Internetprotokolle. Es ist ein Netzwerkschichtprotokoll. ICMP wird von den Betriebssystemen verwendet, um Fehlermeldungen zu senden, um anzuzeigen, dass der angeforderte Dienst nicht verfügbar ist oder ein bestimmter Host nicht erreicht werden kann. Sie wird auch zum Senden von Diagnosemeldungen verwendet. ICMP kann nicht zum Austausch von Daten zwischen den Systemen verwendet werden. Sie werden in der Regel als Reaktion auf einige Fehler in den IP-Datagrammen generiert.

ICMP-Datenverkehr ist ein sehr kritischer Netzwerkverkehr, kann aber auch zu vielen Netzwerkproblemen führen, wenn er von einem böswilligen Angreifer gegen das Netzwerk verwendet wird. Dies macht eine strikte Filterung des ICMP-Datenverkehrs aus dem Internet erforderlich. Die Seite *ICMP-Filterung* ermöglicht das Filtern der ICMP-Pakete aus bestimmten Quellen. Dadurch wird die Netzwerkauslastung bei einem ICMP-Angriff minimiert.

Schritt 1: Zum Konfigurieren der ICMP-Filterung klicken Sie auf **Bearbeiten**, und die Seite *ICMP-Filterung* wird geöffnet.

Schritt 2: Klicken Sie auf **Hinzufügen**. Die Seite *ICMP-Filterung hinzufügen* wird angezeigt. Geben Sie die folgenden Parameter in die angezeigten Felder ein:



Schritt 3: Wählen Sie die Schnittstelle aus, auf der die ICMP-Filterung definiert ist.

Schritt 4: Geben Sie die IPv4-Adresse ein, für die die ICMP-Paketfilterung aktiviert ist, oder klicken Sie auf **Alle Adressen**, um ICMP-Pakete von allen Quelladressen zu blockieren. Wenn die IP-Adresse eingegeben wird, geben Sie entweder die Maske oder die Präfixlänge ein.

Schritt 5: Die Netzwerkmaske, für die der Ratenschutz aktiviert ist. Wählen Sie das Format der Netzwerkmaske für die Quell-IP-Adresse aus, und klicken Sie auf eines der Felder.

- Maske: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske im Dezimalpunktformat ein.
- Klicken Sie auf **Prefix Length**, um die Länge anzugeben und die Anzahl der Bits einzugeben, die aus dem Quell-IP-Adressen-Präfix bestehen. Der Bereich liegt zwischen 0 und 32.

Schritt 6: Klicken Sie auf **Apply**, wodurch die ICMP-Filterung in die aktuelle Konfigurationsdatei geschrieben wird.

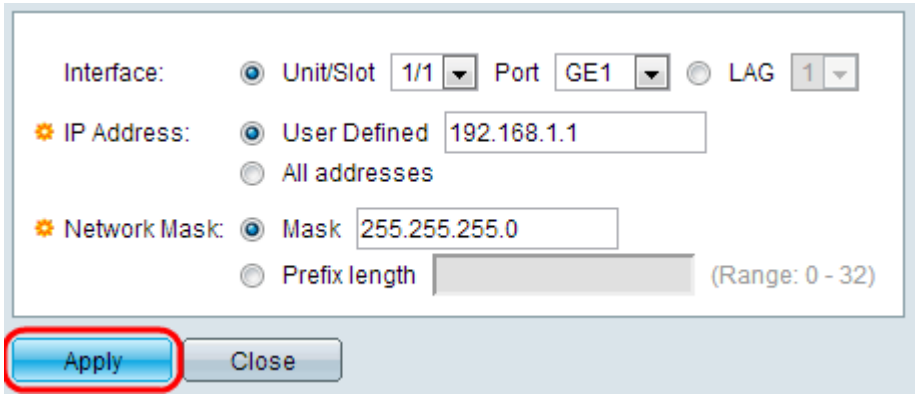
Konfiguration der IP-Fragmentfilterung

Alle Pakete haben eine MTU-Größe (Maximum Transmission Unit). MTU ist die Größe des größten Pakets, das ein Netzwerk übertragen kann. IP nutzt die Vorteile der Fragmentierung, sodass Pakete gebildet werden können, die über eine Verbindung mit einer kleineren MTU als der ursprünglichen Paketgröße übertragen werden können. Daher müssen Pakete, deren Größe größer als die zulässige MTU der Verbindung ist, in kleinere Pakete aufgeteilt werden, damit sie die Verbindung durchlaufen können.

Andererseits kann Fragmentierung auch viele Sicherheitsprobleme aufwerfen. Daher ist es notwendig, IP-Fragmente zu blockieren, da sie manchmal ein Grund für Systemkompromittierungen sein können.

Schritt 1: Um die IP-Fragmentfilterung zu konfigurieren, klicken Sie auf **Bearbeiten**, und die Seite *ICMP Fragments Filtering* wird geöffnet.

Schritt 2: Klicken Sie auf **Hinzufügen**. Die Seite *IP*-Fragmentfilterung *hinzufügen* wird angezeigt. Geben Sie die folgenden Parameter in die angezeigten Felder ein:



Schritt 3: Schnittstelle - Wählen Sie die Schnittstelle aus, auf der die IP-Fragmentierung definiert ist.

Schritt 4: IP-Adresse - Geben Sie die IP-Adresse ein, für die die IP-Fragmentierung aktiviert ist, oder klicken Sie auf **Alle Adressen**, um IP-fragmentierte Pakete von allen Quelladressen zu blockieren. Wenn die IP-Adresse eingegeben wird, geben Sie entweder die Maske oder die Präfixlänge ein.

Schritt 5: Network Mask (Netzwerkmaske): Die Netzwerkmaske, für die die IP-Fragmentierung blockiert wird. Wählen Sie das Format der Netzwerkmaske für die Quell-IP-Adresse aus, und klicken Sie auf eines der Felder.

- Maske: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske im Dezimalpunktformat ein.
- Klicken Sie auf **Prefix Length**, um die Länge anzugeben und die Anzahl der Bits einzugeben, die aus dem Quell-IP-Adressen-Präfix bestehen. Der Bereich liegt zwischen 0 und 32.

Schritt 6: Klicken Sie auf **Apply**, um die IP-Fragmentfilterung in die aktuelle Konfigurationsdatei zu schreiben.