Konfiguration der martianischen DoS-Adresse für Managed Switches der Serie 300

Ziel

Ein DoS-Angriff (Denial of Service) überflutet ein Netzwerk mit falschem Datenverkehr. Dadurch werden Netzwerkserverressourcen von legitimen Benutzern abgezogen. Der DoS-Schutz vor Angriffen blockiert den Eingang von Paketen innerhalb eines bestimmten IP-Adressbereichs. Marsadressen sind IP-Adressen, die vom Switch abgelehnt werden. Wenn ein Paket mit einer Marsadresse vom Switch empfangen wird, wird das Paket verworfen. Marsadressen werden nur im IPv4-Format unterstützt. In diesem Artikel wird erläutert, wie Sie Martian-Adressen auf einem Managed Switch der Serie 300 konfigurieren.

Hinweis: Martian-Adressen können nur verwendet werden, wenn DoS Prevention aktiviert ist. Hilfe finden Sie im Artikel *Security Suite Settings on 300 Series Managed Switches*.

Anwendbare Geräte

·Managed Switches der Serie SF/SG 300

Softwareversion

·1.3.0.62

Konfiguration der Martian-Adressen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Denial of Service Prevention > Martian Addresses (Sicherheit > Denial of Service Prevention > Martian Adressen)**. Die Seite *Martian Addresses* (Martische Adressen) wird geöffnet:

Schritt 2: (Optional) Aktivieren Sie **Include** in das Feld Reservierte Marsadressen, um die standardmäßig reservierten Marsadressen in die Martian-Adresstabelle aufzunehmen. Fahren Sie mit Schritt 4 fort, wenn Sie die reservierten Marsadressen nicht einschließen möchten.

Schritt 3: Klicken Sie auf **Apply**, um die standardmäßig reservierten Adressen in der Martian

Address Table anzuzeigen. Diese IP-Adressen werden von der Internet Assigned Numbers Authority nur für die besondere Verwendung reserviert. Die reservierten Marsadressen sind:

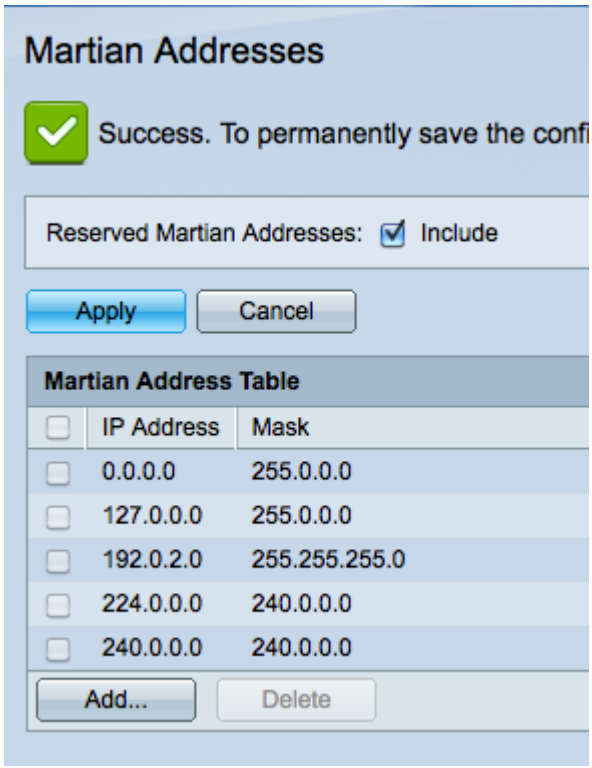
·0.0.0.0/8 — Der Adressbereich, der als Quelladresse verwendet wird, bis der Host eine eigene IP-Adresse erhält.

·127.0.0.0/8 — Adressbereich für Internet-Loopback, der für Netzwerktestzwecke verwendet wird.

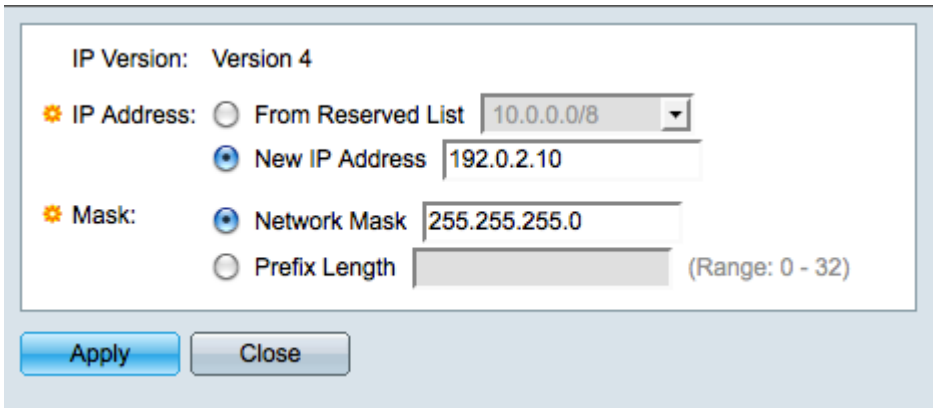
·192.0.2.0/24 — Der Adressbereich wird als TEST-NET-1 zugewiesen, um als Beispiele in Online-Dokumenten und -Beispielen verwendet zu werden.

·224.0.0.0/4 — Der Adressbereich ist für IPv4-Multicast reserviert. Wurde früher bei der Verwendung der klassischen Adressierung als Class D Address Space bezeichnet.

·240.0.0.0/4 — Der Adressbereich ist für die spätere Verwendung reserviert und wurde früher als Klasse E bezeichnet.



Schritt 4: Klicken Sie auf **Hinzufügen**, um eine neue Martian-Adresse hinzuzufügen. Das Fenster *Marsadressen hinzufügen* wird angezeigt.



Schritt 5: Klicken Sie im Feld IP-Adresse auf das Optionsfeld für die Ablehnung der

gewünschten IP-Adresse.

·Aus der Liste Reserviert - Wählen Sie eine IP-Adresse aus der Dropdown-Liste aus.

·Neue IP-Adresse: Geben Sie eine neue IP-Adresse ein, die der Martian Address Table (Martian-Adresstabelle) hinzugefügt werden soll.

Schritt 6: Klicken Sie auf das Optionsfeld, das der Methode entspricht, mit der die Subnetzmaske der Martian-Adresse im Maskenfeld definiert wird. Mit dem Maskenfeld können Sie einen Bereich von IP-Adressen gleichzeitig blockieren.

·Network Mask (Netzwerkmaske): Geben Sie die Netzwerkmaske in das Feld Network Maske (Netzwerkmaske) ein. Die Maske 255.255.255.255 bedeutet, dass nur die eingegebene IP-Adresse blockiert wird. Die Maske 255.0.0.0 bedeutet, dass auch alle IP-Adressen mit demselben ersten Oktett der eingegebenen IP-Adresse blockiert werden.

·Präfixlänge - Geben Sie die Präfixlänge (ganze Zahl im Bereich von 0 bis 32) im Feld Präfixlänge ein. Eine Präfixlänge von 32 bedeutet, dass nur die eingegebene IP-Adresse blockiert wird. Eine Präfixlänge von 8 bedeutet, dass auch alle IP-Adressen mit demselben ersten Oktett der eingegebenen IP-Adresse blockiert werden.

Schritt 7: Klicken Sie auf **Apply**, um die Marsadresse zu speichern, oder auf **Close**, um Ihre Änderungen zu stornieren.