

Configuratie van Denial of Service Prevention Techniques (Security Suite) op SX500 Series Stackable Switches

Doel

Denial of Service (DoS) of Distributed Denial of Service (DDoS)-aanvallen beperken de geldige gebruikers tot het gebruik van het netwerk. De aanvaller voert een DOS aanval uit door een netwerk met vele onnodige verzoeken te overspoelen die alle bandbreedte van het netwerk opnemen. Zijn aanvallen mogelijk om een netwerk te vertragen of een netwerk meerdere uren lang af te sluiten. Is de bescherming van een netwerk de belangrijkste functie om de netwerkbeveiliging te verbeteren? het detecteert het abnormale verkeer en filtert het .

Dit artikel legt de configuratie van de Klantenservice uit op Security Suite-instellingen en diverse technieken die worden gebruikt voor de voorkoming van servicedetectie.

N.B.: Als de gekozen DoS-preventie systeemniveau en interfaceniveau-preventie is, dan kunnen de militaire adressen, SYN-filtering, SYN-snelheidsbescherming, ICMP-filtering en IP-fragmentatie worden bewerkt en geconfigureerd. Deze configuraties worden ook in dit artikel uitgelegd.

Opmerking: Voordat de DoS-preventie is geactiveerd, moet u alle toegangscontrolelijsten (ACL's) of elk geavanceerd QoS-beleid dat op de poort is ingesteld, verwijderen. ACL en geavanceerd QoS-beleid zijn niet actief zodra de DoS-bescherming op de poort is ingeschakeld.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- 1.3.0.62

Configuratie van Service-ontkenning op Security Suite-instellingen

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Security > Denial of Service Prevention > Security Suite-instellingen**. De pagina *Instellingen Security Suite* wordt geopend:

Security Suite Settings

CPU Protection Mechanism: Enabled

CPU Utilization: [Details](#)

DoS Prevention: Disable
 System-Level Prevention
 System-Level and Interface-Level Prevention

Denial of Service Protection

Stacheldraht Distribution: Enable

Invasor Trojan: Enable

Back Orifice Trojan: Enable

Martian Addresses: [Edit](#)

SYN Filtering: [Edit](#)

SYN Rate Protection: [Edit](#)

ICMP Filtering: [Edit](#)

IP Fragmented: [Edit](#)

- CPU-beschermingsmechanisme — Dit is
- **Ingeschakeld.** Dit geeft aan dat het Security Conversion Tool (SCT) is ingeschakeld.
- CPU-gebruik — klik op
- **Details** naast het CPU-gebruik om de informatie over het gebruik van de CPU-bron te bekijken.

Stap 2. Klik op de gewenste radioknop onder het veld DoS Prevention.

- Uitschakelen - DoS-preventie uitschakelen.
- Voorkoming van systeemniveau — Dit voorkomt aanvallen door de distributie van Stacheldraden, Invasor Trojan en Back Orifice Trojan.
- Systeem-niveau en interface-niveau Preventie — Dit voorkomt aanvallen per interface op de schakelaar.

DoS Prevention: Disable
 System-Level Prevention
 System-Level and Interface-Level Prevention

Denial of Service Protection

Stacheldraht Distribution: Enable
Invasor Trojan: Enable
Back Orifice Trojan: Enable
Martian Addresses: [Edit](#)
SYN Filtering: [Edit](#)
SYN Rate Protection: [Edit](#)
ICMP Filtering: [Edit](#)
IP Fragmented: [Edit](#)

Stap 3. Deze opties kunnen worden gekozen voor Knippering of Servicebescherming:

- Stroomdistributie — Dit is een voorbeeld van DDoS-aanval waarbij de aanvaller een clientprogramma gebruikt om verbinding te maken met de computers binnen het netwerk. Deze computers verzenden dan meerdere inlogaanvragen naar de interne server en starten een DDoS-aanval.
- Invasor Trojan — Als de computer door deze aanval is geïnfecteerd, wordt de TCP poort 2140 gebruikt voor kwaadaardige activiteit.
- Terug begin Trojan — Dit vergooit UDP pakketten die worden gebruikt om met het server- en clientprogramma voor DoS-aanval te communiceren.

Configuratie van martiaanse adressen

Stap 1. Klik op **Bewerken** in het veld Martiaanse adressen en vervolgens wordt de pagina *Martiaanse adressen* geopend. Martiaanse adressen geven het IP-adres aan dat mogelijk de oorzaak van een aanval op het netwerk kan zijn. Pakketten die uit deze netwerken komen, worden ingetrokken.

Martian Addresses

Reserved Martian Addresses: Include

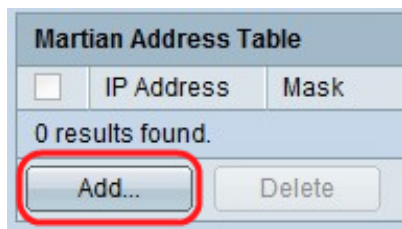
[Apply](#) [Cancel](#)

Martian Address Table

| <input type="checkbox"/> | IP Address | Mask |
|--------------------------|------------|------|
| 0 results found. | | |

[Add...](#) [Delete](#)

Stap 2. Controleer de **Optie** in de gereserveerde Marsadressen en klik op **Toepassen** om de Gereserveerde Martiaanse adressen aan de systeemlijst toe te voegen.



Stap 3. Als u een Martiaans adres wilt toevoegen, klikt u op **Toevoegen**. De pagina *Martistische adressen toevoegen* wordt weergegeven. Voer deze parameters in:

Stap 4. Voer in het veld IP-adres het IP-adres in dat moet worden afgewezen.

Stap 5. Het masker van IP-adres om het bereik van IP-adressen aan te geven dat moet worden afgewezen.

- IP-versie - De ondersteunde IP-versie. Op dit moment is alleen IPv4 toegestaan.
- Van gereserveerde Lijst - kies een bekend IP adres uit een gereserveerde lijst.
- Nieuw IP-adres - Voer een IP-adres in.
- Netwerkmasker - Netwerkmasker in decimale notatie met punten.
- Lengte prefixeren - Voorvoegsel van IP-adres om het bereik van IP-adressen te definiëren waarvoor de Denial of Service Prevention is ingeschakeld.

Stap 6. Klik op **Toepassen** om het Martiaanse adres in het configuratiebestand te laten schrijven.

Configuratie van SYN-filtering

Met SYN-filtering kunnen netwerkbeheerders illegale TCP-pakketten drogen met SYN-vlag. SYN-poortfiltering wordt gedefinieerd op basis van één poort.

DoS Prevention: Disable
 System-Level Prevention
 System-Level and Interface-Level Prevention

Denial of Service Protection

Stacheldraht Distribution: Enable

Invasor Trojan: Enable

Back Orifice Trojan: Enable

Martian Addresses: [Edit](#)

SYN Filtering: [Edit](#)

SYN Rate Protection: [Edit](#)

ICMP Filtering: [Edit](#)

IP Fragmented: [Edit](#)

Stap 1. Om het SYN-filtering te configureren klikt u op **Bewerken** en wordt de pagina *SYN-filtering* geopend:

SYN Filtering

SYN Filtering Table

| <input type="checkbox"/> | Interface | IP Address | Mask | TCP Port |
|--------------------------|-----------|------------|------|----------|
| 0 results found. | | | | |

[Add...](#) [Delete](#)

Stap 2. Klik op **Add**. De pagina *SYN-filtering* toevoegen wordt weergegeven. Voer deze parameters in de weergegeven velden in:

Interface: Unit/Slot LAG

Unit/Slot: Port: LAG:

IPv4 Address: User Defined
 All addresses

Network Mask: Mask
 Prefix length (Range: 0 - 32)

TCP Port: Known ports
 User Defined (Range: 1 - 65535)
 All ports

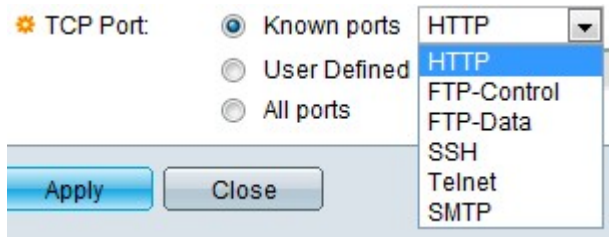
[Apply](#) [Close](#)

Stap 3. Kies de interface waarop het filter moet worden gedefinieerd.

Stap 4. Klik op **Gebruiker gedefinieerd** om een IP-adres te geven waarvoor het filter is gedefinieerd of klik op **Alle adressen**.

Stap 5. Het netwerkmasker waarvoor het filter is ingeschakeld. Klik op **Prefixlengte** om de lengte te specificeren, is zijn bereik van 0 tot 32, of klik op **masker** om het subnetmasker in

te voeren zoals in decimale notatie met punten.



Stap 6. Klik op de doelpoort die wordt gefilterd. Het gaat om:

- Bekende poorten — Kies een poort in de lijst.
- Gebruikersnaam — Voer het poortnummer in.
- Alle poorten — Klik om aan te geven dat alle poorten worden gefilterd.

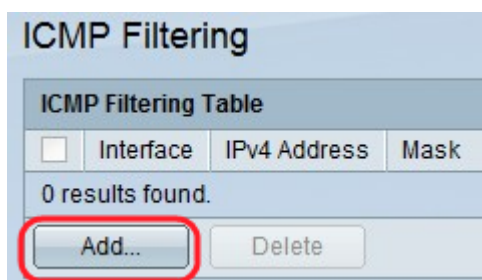
Stap 7. Klik op **Toepassen** waardoor het SYN-filtering op het actieve configuratiebestand moet worden geschreven.

Configuratie van ICMP-filtering

Internet Control Message Protocol (ICMP) is een van de belangrijkste internetprotocollen. Het is een protocol op de netwerklaag. ICMP wordt door de besturingssystemen gebruikt om foutmeldingen te verzenden om te weten te komen dat de gevraagde service niet beschikbaar is of dat een bepaalde host niet kan worden bereikt. Het wordt ook gebruikt om diagnostische boodschappen te versturen. Het ICMP kan niet worden gebruikt voor de uitwisseling van gegevens tussen de systemen. Ze worden meestal gegenereerd in antwoord op een aantal fouten in de IP-datagrammen.

ICMP-verkeer is een zeer kritisch netwerkverkeer, maar kan ook tot veel netwerkproblemen leiden als het tegen het netwerk wordt gebruikt door een kwaadaardige aanvaller. Dit brengt de noodzaak aan van het strikt filteren van het ICMP verkeer dat van het internet komt. Met de pagina *ICMP Filtering* kunt u de ICMP-pakketten uit bepaalde bronnen filteren. Dit minimaliseert de lading op het netwerk in het geval van een ICMP aanval.

Stap 1. Om ICMP-filtering te configureren klikt u op **Bewerken** en wordt de pagina *ICMP-filtering* geopend.



Stap 2. Klik op **Add**. De pagina *ICMP-filtering* toevoegen wordt weergegeven. Voer deze parameters in de weergegeven velden in:

Interface: Unit/Slot 1/1 Port GE1 LAG 1

IP Address: User Defined 192.168.1.1
 All addresses

Network Mask: Mask 255.255.255.0
 Prefix length (Range: 0 - 32)

Apply Close

Stap 3. Kies de interface waarop het ICMP-filtering is gedefinieerd.

Stap 4. Voer het IPv4-adres in waarvoor het ICMP-pakketfiltering is ingeschakeld of klik op **Alle adressen** om ICMP-pakketten van alle bronadressen te blokkeren. Als IP-adres is ingevoerd, voert u het masker of de voorvoegsellengte in.

Stap 5. Het netwerkmasker waarvoor de snelheidsbescherming is ingeschakeld. Kies het formaat van het netwerkmasker voor het IP-adres van de bron en klik op een van de velden.

- Makkelijk — Kies het type waarnaar het bron IP-adres hoort en voer het subnetmasker in in decimale indeling met punten in.
- Klik op **Prefixlengte** om de lengte te specificeren en het aantal bits in te voeren dat uit het bron IP-adresprefix bestaat, is de bereik van 0 tot 32.

Stap 6. Klik op **Toepassen** waardoor de ICMP-filtering op het actieve configuratiebestand moet worden geschreven.

Configuratie van IP-fragmentatie

Alle pakketten hebben een maximale grootte van de Transmission Unit (MTU). MTU is de grootte van het grootste pakket dat een netwerk kan verzenden. IP maakt gebruik van fragmentatie zodat pakketten kunnen worden gevormd die door een verbinding met een kleinere MTU kunnen bewegen dan de oorspronkelijke pakketgrootte. Daarom moeten pakketten waarvan de afmetingen groter zijn dan de toelaatbare MTU van de verbinding in kleinere pakketten worden verdeeld om ze door de verbinding te kunnen verplaatsen.

Aan de andere kant kan fragmentatie ook veel veiligheidsproblemen opleveren. Het wordt dus nodig om IP-fragmenten te blokkeren, omdat deze soms een reden kunnen zijn voor een systeemcompromis.

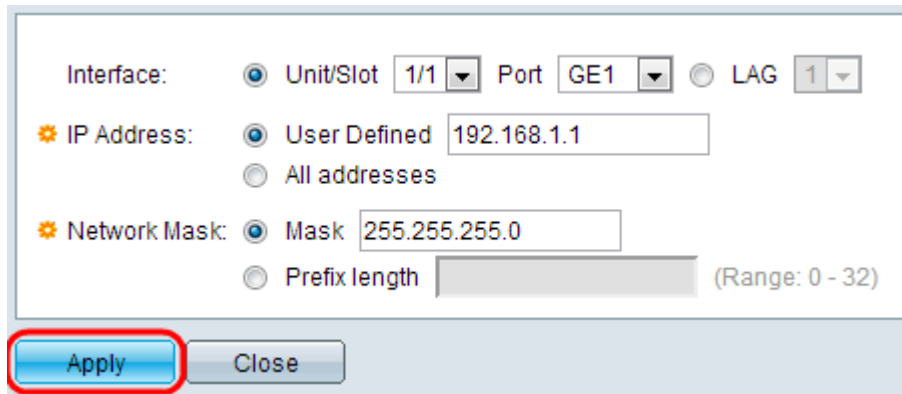
Stap 1. Om IP-fragmentaties te configureren klikt u op **Bewerken** en wordt de pagina *ICMP-fragmenten* geopend.

IP Fragments Filtering

| IP Fragments Filtering Table | | | |
|------------------------------|-----------|--------------|------|
| <input type="checkbox"/> | Interface | IPv4 Address | Mask |
| 0 results found. | | | |

Add... Delete

Stap 2. Klik op **Add**. De pagina *IP-fragmentatie toevoegen* wordt weergegeven. Voer deze parameters in de weergegeven velden in:



Interface: Unit/Slot 1/1 Port GE1 LAG 1

IP Address: User Defined 192.168.1.1
 All addresses

Network Mask: Mask 255.255.255.0
 Prefix length (Range: 0 - 32)

Apply Close

Stap 3. Interface - Kies de interface waarop de IP-fragmentatie is gedefinieerd.

Stap 4. IP-adres - Voer het IP-adres in waarvoor de IP-fragmentatie is ingeschakeld of klik op **Alle adressen** om IP-gefragmenteerde pakketten van alle bronadressen te blokkeren. Als IP-adres is ingevoerd, voert u het masker of de voorvoegsellengte in.

Stap 5. Netwerkmasker — het netwerkmasker waarvoor de IP-fragmentatie is geblokkeerd. Kies het formaat van het netwerkmasker voor het IP-adres van de bron en klik op een van de velden.

- Makkelijk — Kies het type waarnaar het bron IP-adres hoort en voer het subnetmasker in in decimale indeling met punten in.
- Klik op **Prefixlengte** om de lengte te specificeren en het aantal bits in te voeren dat uit het bron IP-adresprefix bestaat, is de bereik van 0 tot 32.

Stap 6. Klik op **Toepassen** om de IP-fragmentatie te maken die naar het actieve configuratiebestand moet worden geschreven.