Security Suite-instellingen voor 3000 Series beheerde Switches

Doel

Security Suite op Cisco 300 Series Managed-Switches bieden bescherming tegen Denial of Service (DoS)-aanvallen. Sluit overstromingsnetwerken aan op vals verkeer, waardoor de bronnen van netwerkservers niet beschikbaar zijn of niet reageren op legitieme gebruikers. Over het algemeen zijn er twee typen DOS-aanvallen. Brute force DoS aanvallen overspoelen de server en gebruiken server- en netwerkbandbreedte. Systematische aanvallen manipuleren protocollen kwetsbaarheden zoals TCP SYN bericht aan crashsystemen. Dit artikel verklaart de instellingen die in Security Suite beschikbaar zijn op de 300 Series Managed-Switches.

Opmerking: Toegangscontrolelijsten (ACL's) en geavanceerd QoS-beleid zijn niet actief op een poort wanneer DoS-aanvalsbescherming is ingeschakeld.

Toepasselijke apparaten

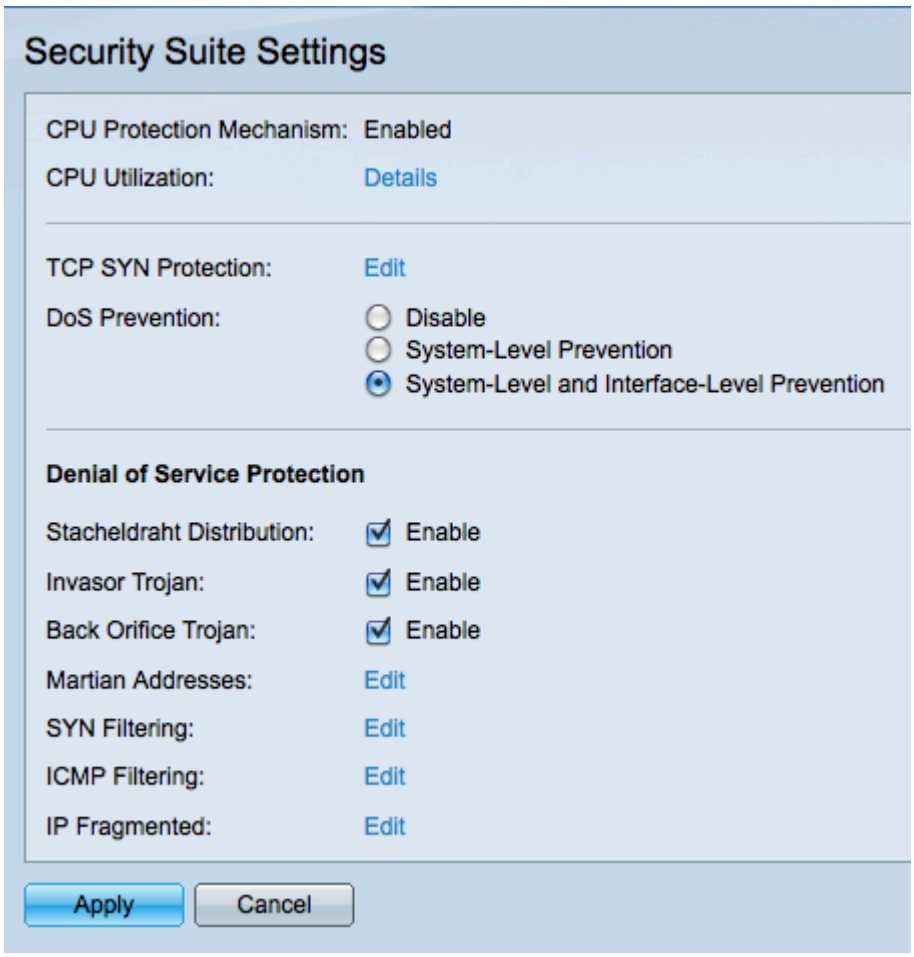
- SF/SG 300 Series beheerde Switches

Softwareversie

•1.3.0.62

Configuratie van 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:



Opmerking: CPU-beveiligingsmechanisme is standaard ingeschakeld voor 300 Series beheerde Switches en kan niet worden uitgeschakeld. De switch gebruikt Secure Core Technology (SCT), waardoor de switch beheer en protocolverkeer kan verwerken, ongeacht hoeveel totaal verkeer wordt ontvangen.

Stap 2. (Optioneel) Klik op **Details** in het veld CPU-gebruik om het CPU-gebruik te bekijken. Raadpleeg het artikel *CPU-gebruik op 200/300 Series beheerde Switches* voor meer informatie.

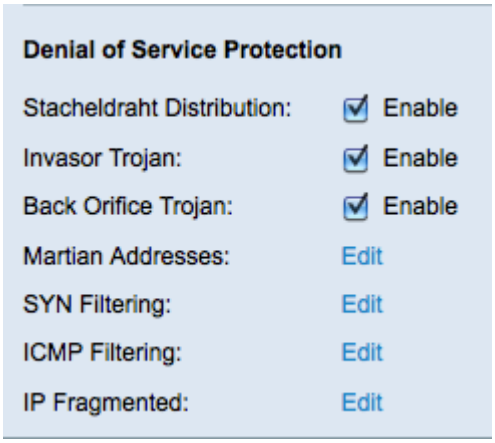
Stap 3. (Optioneel) Klik op **Bewerken** in het veld TCP-SYN-bescherming om de TCP-instellingen voor SYN-bescherming te bewerken. Raadpleeg het artikel *Synchronize (SYN) Filtering op de 300 Series Managed-Switches* voor meer informatie.

Stap 4. Klik in het veld DoS Prevention op de radioknop die overeenkomt met de methode van de DoS-preventie die u wilt gebruiken. De beschikbare opties zijn:

- Uitschakelen — DoS security optie uit. Als Uitschakelen is geselecteerd, slaat u over naar Stap 13.

- Systeem - Level-Prevention - hiermee kunnen DoS-beschermingsfuncties worden ingeschakeld die bescherming bieden tegen Invasor Trojan, distributie van Stacheldraden, Trojan aan de achterkant en martiaanse adressen.

- Systeem - Level-preventie en interface-level bescherming — Hiermee kunnen alle beveiligingsmaatregelen worden uitgevoerd die in het gebied Denial of Service Protection zijn gedefinieerd.



Stap 5. Controleer het aanvinkvakje **Enable** in het veld Distributie-Stachelpad om TCP-pakketten met een TCP-bronnummer 16660 af te wijzen.

Stap 6. Controleer het aanvinkvakje **Enable** in het veld Invasor Trojan om TCP-pakketten af te wijzen met een TCP-doelpoort van 2140 en een TCP-bronpoort van 1024.

Stap 7. Controleer het aanvinkvakje **Enable** in het veld Terug begin Troje om UDP-pakketten af te wijzen met een bestemming UDP-poort gelijk aan 31337 en een bron-UDP-poort van 1024.

Opmerking: Hoewel er honderden DOM-aanvallen zijn, worden de hierboven genoemde havens doorgaans geëxploiteerd voor boosaardige activiteiten. Ze worden echter ook gebruikt voor legitiem verkeer. Als u een apparaat hebt dat een van de bovengenoemde poorten gebruikt, wordt die informatie geblokkeerd.

Stap 8. Klik op **Bewerken** in het veld Martiaanse adressen om de tabel met Martiaanse adressen te bewerken. De Martiaanse Adressaten in tabel verwijderen van geselecteerde IP-adressen. U kunt de lijst met Martiaanse adressen bewerken door te verwijzen naar het artikel *Denial of Service (DoS) Martian Address Configuration op 300 Series Managed Switches*.

Opmerking: Stap 9-12 vereist dat systeemniveau en interfaceniveau-preventie worden gekozen in stap 4. Naar stap 13 als u een ander type DoS-preventie hebt gekozen.

Stap 9. Klik op **Bewerken** in het veld SYN-filtering om de beheerder toe te staan bepaalde TCP-poorten te blokkeren. Raadpleeg het artikel *Denial of Service (*DoS*) SYN-filtering op 300 Series beheerde Switches* om *de* SYN-*filtering te* configureren*.*

Stap 10. Klik op **Bewerken** in het veld SYN Rate Protection om het aantal ontvangen SYN-pakketten te beperken. Raadpleeg het artikel *SYN Rate Protection op 300 Series beheerde Switches* om deze *te* configureren.

Stap 1. Klik op **Bewerken** in het veld ICMP-filtering om toe te staan dat ICMP-pakketten uit bepaalde bronnen worden geblokkeerd. Om ICMP-filtering te configureren verwijst u naar het artikel *Internet Control Message Protocol (ICMP)-filtering op de 300 Series beheerde Switches.*

Stap 12. Klik op **Bewerken** in het veld IP Fragmented om gefragmenteerde IP-pakketten te blokkeren. Om IP-fragmentatie te configureren verwijst u naar het artikel *Denial of Service (DoS) IP-fragmentatie van 300 Series beheerde Switches*.

Stap 13. Klik op **Toepassen** om wijzigingen op te slaan of klik op **Annuleren** om uw wijzigingen te annuleren.