Impostazioni di Security Suite sugli switch gestiti serie 300

Obiettivo

La Security Suite sugli switch gestiti Cisco serie 300 offre protezione dagli attacchi Denial of Service (DoS). Il servizio DoS attacca le reti flood con traffico falso, rendendo le risorse del server di rete non disponibili o non rispondenti agli utenti legittimi. In genere, esistono due tipi di attacchi DoS. Gli attacchi DoS di forza bruta invadono il server e consumano la larghezza di banda del server e della rete. Gli attacchi sistematici manipolano le vulnerabilità dei protocolli come il messaggio TCP SYN ai sistemi di crash. In questo documento vengono illustrate le impostazioni disponibili nella Security Suite sugli switch gestiti serie 300.

Nota: Gli Access Control Lists (ACLs) e i criteri QoS avanzati non sono attivi su una porta quando è abilitata la protezione da attacchi DoS.

Dispositivi interessati

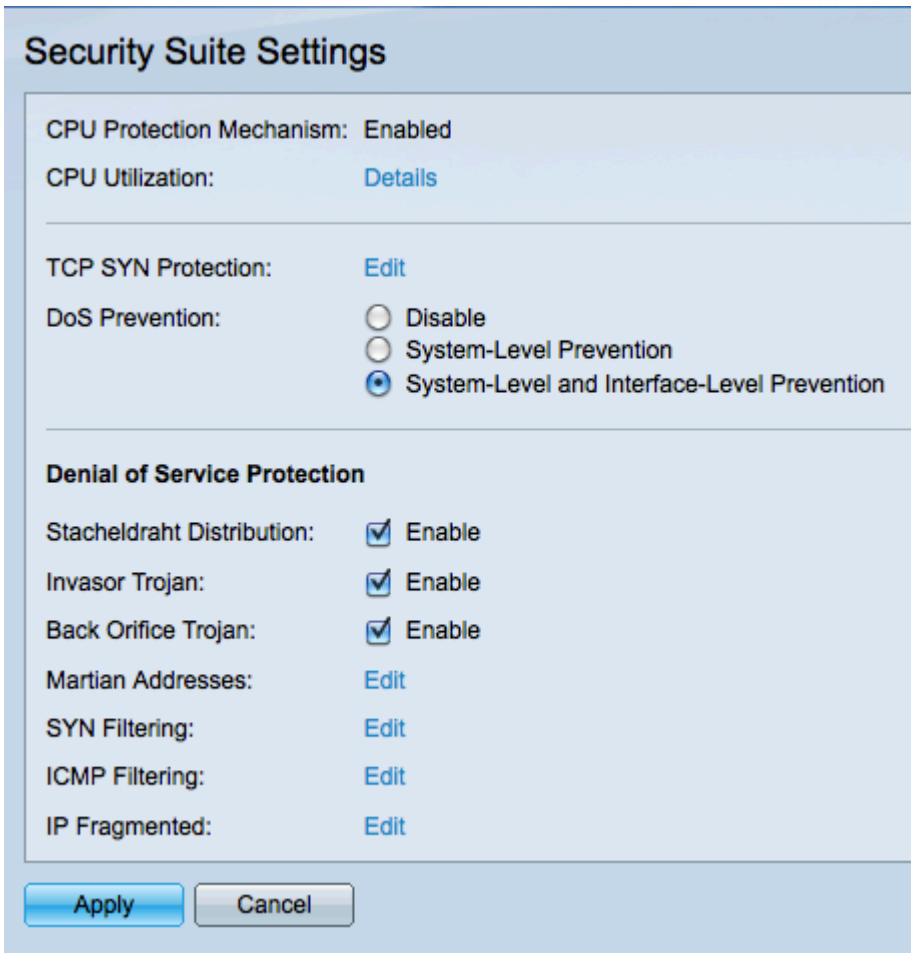
·SF/SG serie 300 Managed Switch

Versione del software

•1.3.0.62

Configurazione impostazioni suite di sicurezza

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Prevenzione della negazione del servizio > Impostazioni della suite di sicurezza**. Viene visualizzata la pagina *Security Suite Settings*:



Nota: Il meccanismo di protezione della CPU è abilitato per impostazione predefinita sugli switch gestiti serie 300 e non può essere disabilitato. Lo switch utilizza la tecnologia Secure Core (SCT), che consente di gestire la gestione e il traffico di protocollo indipendentemente dalla quantità di traffico totale ricevuto.

Passaggio 2. (Facoltativo) Fare clic su **Dettagli** nel campo Utilizzo CPU per visualizzare l'utilizzo della CPU. Per ulteriori informazioni, fare riferimento all'articolo *Utilizzo della CPU sugli switch gestiti serie 200/300*.

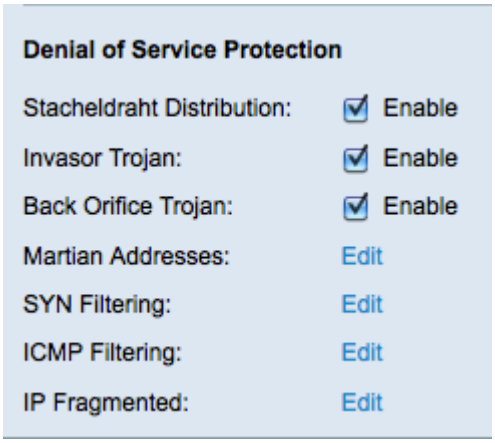
Passaggio 3. (Facoltativo) Fare clic su **Edit** nel campo TCP SYN Protection per modificare le impostazioni di TCP SYN Protection. Per ulteriori informazioni, fare riferimento all'articolo *Configurazione del filtro di sincronizzazione (SYN)* sugli *switch gestiti serie 300*.

Passaggio 4. Nel campo Prevenzione DoS, fare clic sul pulsante di opzione corrispondente al metodo di prevenzione DoS che si desidera utilizzare. Le opzioni disponibili sono:

·Disabilita: disabilita la funzione di protezione DoS. Se si sceglie Disabilita, andare al passo 13.

·Sistema - Prevenzione del livello - Abilita le funzioni di protezione DoS che proteggono da Invasor Trojan, Distribuzione Stacheldraht, Back Orifice Trojan e indirizzi marziani.

·Sistema - Protezione a livello di interfaccia e prevenzione - Attiva tutte le misure di sicurezza definite nell'area di protezione da attacchi Denial of Service.



Passaggio 5. Selezionare la casella di controllo **Abilita** nel campo Distribuzione stringhe per eliminare i pacchetti TCP con un numero di porta TCP di origine pari a 16660.

Passaggio 6. Selezionare la casella di controllo **Abilita** nel campo Trojan Invasor per ignorare i pacchetti TCP con una porta TCP di destinazione di 2140 e una porta TCP di origine di 1024.

Passaggio 7. Selezionare la casella di controllo **Enable** nel campo Back Orifizio Trojan per ignorare i pacchetti UDP con una porta UDP di destinazione uguale a 31337 e una porta UDP di origine pari a 1024.

Nota: Sebbene vi siano centinaia di attacchi DoS, le porte menzionate in precedenza vengono comunemente sfruttate per attività dannose. Tuttavia, sono anche utilizzati per il traffico legittimo. Se si dispone di un dispositivo che utilizza una qualsiasi delle porte indicate, tali informazioni verranno bloccate.

Passaggio 8. Fare clic su **Modifica** nel campo Indirizzi marziani per modificare la tabella Indirizzi marziani. La tabella Indirizzi di Marziani ignora i pacchetti da determinati indirizzi IP. Per modificare l'elenco di indirizzi Marziani, fare riferimento all'articolo *Configurazione degli indirizzi Marziani Denial of Service (DoS) sugli switch gestiti serie 300*.

Nota: I passaggi da 9 a 12 richiedono la selezione di Prevenzione a livello di sistema e di interfaccia nel passaggio 4. Se è stato scelto un altro tipo di prevenzione DoS, passare al passaggio 13.

Passaggio 9. Fare clic su **Modifica** nel campo Filtro SYN per consentire all'amministratore di bloccare alcune porte TCP. Per configurare il filtro SYN, fare riferimento all'articolo *Configurazione del filtro SYN Denial of Service (DoS) sugli switch gestiti serie 300.*

Passaggio 10. Fare clic su **Edit** nel campo SYN Rate Protection per limitare il numero di pacchetti SYN ricevuti. Per configurare SYN Rate Protection, fare riferimento all'articolo *SYN Rate Protection sugli switch gestiti serie 300*.

Passaggio 11. Fare clic su **Modifica** nel campo Filtro ICMP per consentire il blocco dei pacchetti ICMP da determinate origini. Per configurare il filtro ICMP, fare riferimento all'articolo *Configurazione del filtro ICMP (Internet Control Message Protocol) sugli switch gestiti serie 300.*

Passaggio 12. Per bloccare i pacchetti IP frammentati, fare clic su **Modifica** nel campo IP frammentato. Per configurare il filtro dei frammenti IP, fare riferimento all'articolo *Configurazione del filtro dei frammenti IP DoS (Denial of Service) sugli switch gestiti serie 300*.

Passaggio 13. Fare clic su **Applica** per salvare le modifiche o su **Annulla** per annullarle.