

Configurazione del database di binding IP Source Guard sugli switch impilabili della serie Sx500

Obiettivo

IP Source Guard è una funzione di sicurezza che può essere utilizzata per prevenire gli attacchi al traffico causati quando un host tenta di utilizzare l'indirizzo IP di un host adiacente. Quando IP Source Guard è abilitato, lo switch trasmette il traffico IP dei client solo agli indirizzi IP contenuti nel database DHCP Snooping Binding. Se il pacchetto inviato da un host corrisponde a una voce del database, lo switch inoltra il pacchetto. Se il pacchetto non corrisponde a una voce del database, viene scartato.

In uno scenario in tempo reale, uno dei modi in cui viene utilizzato IP Source Guard è quello di contribuire a prevenire attacchi man-in-the-middle in cui una terza parte non attendibile tenta di mascherarsi come utente autentico. In base agli indirizzi configurati nel database di binding di IP Source Guard, viene consentito solo il traffico proveniente dal client con tale indirizzo IP e gli altri pacchetti vengono scartati.

Nota: lo snooping DHCP deve essere abilitato affinché IP Source Guard funzioni. Per ulteriori informazioni su come abilitare lo snooping DHCP, consultare l'articolo [DHCP Snooping Binding Database Configuration sugli switch impilabili serie Sx500](#). È inoltre necessario configurare il database di binding per specificare gli indirizzi IP consentiti.

Questo articolo spiega come configurare il binding database per IP source guard sugli switch serie Sx500 impilabili.

Dispositivi interessati

·Switch Stack Serie Sx500

Versione del software

·v1.2.7.76

Configurazione del database di binding di IP Source Guard

Database di associazione

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > IP Source Guard > Binding Database**. Viene visualizzata la pagina *Database di associazione*:

Binding Database

Supported IP Format: Version 4

TCAM Resources Consumed:

✱ Insert Inactive: Retry Frequency Sec. (Range: 10 - 600, Default: 60)
 Never

Binding Database Table (DHCP Snooping Binding Database Table)

Filter: VLAN ID equals to (Range: 1 - 4094)
 MAC Address equals to
 IP Address equals to
 Interface equals to Unit/Slot Port LAG

VLAN ID	MAC Address	IP Address	Interface	Status	Type	Reason
0 results found.						

Passaggio 2. Fare clic sulla voce appropriata tra le seguenti opzioni nel campo Inserisci inattivo per scegliere la frequenza con cui le voci inattive devono essere rese attive dal parametro. Il database di binding snooping DHCP utilizza TCAM (Ternary Content Addressable Memory) per la gestione del database.

- Frequenza di ripetizione: fornisce la frequenza di controllo delle risorse TCAM. Il valore predefinito è 60.

- Mai - Non tentare mai di attivare gli indirizzi inattivi.

Passaggio 3. Fare clic su **Apply** per aggiornare il file di configurazione in esecuzione.

Aggiungi voce di database di binding

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Configurazione IP > DHCP > DHCP Snooping Binding Database** che apre la pagina *DHCP Snooping Binding Database*.

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: VLAN ID equals to (Range: 1 - 4094)
 MAC Address equals to
 IP Address equals to
 Interface equals to Unit/Slot Port LAG

<input type="checkbox"/>	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	
							Status	Reason
0 results found.								

Passaggio 2. Fare clic su **Add** per immettere le voci nella pagina *Add DHCP Snooping Entry*

(Aggiungi voce snooping DHCP).

Supported IP Format: Version 4

VLAN ID: 1

MAC Address: 00b0d086d6f7

IP Address: 192.0.2.2

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

Type: Dynamic Static

Lease Time: Infinite User Defined 3456 Sec. (Range: 10 - 4294967294, Default: Infinite)

Apply Close

Passaggio 3. Selezionare l'ID VLAN dall'elenco a discesa in cui è previsto il pacchetto nel campo VLAN ID.

Passaggio 4. Inserire l'indirizzo MAC da associare nel campo Indirizzo MAC.

Passaggio 5. Inserire l'indirizzo IP da associare nel campo Indirizzo IP.

Passaggio 6. Scegliere l'interfaccia dall'elenco a discesa Interfaccia per visualizzare le porte o i LAG su cui è previsto il pacchetto.

Type: Dynamic Static

Lease Time: Infinite User Defined 3456

Passaggio 7. Fare clic sul tipo per indicare se la voce è Dinamica o Statica nel campo Tipo.

·Dinamico: l'ingresso ha una durata di leasing limitata.

·Statico: la voce è configurata in modo statico.

Passo 8: inserire la durata del leasing nel campo Durata leasing. Se la voce è dinamica, immettere la durata del periodo di tempo in cui la voce rimarrà attiva. Se il lease non è disponibile, fare clic su **Infinito**.

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: VLAN ID equals to 4 (Range: 1 - 4094)
 MAC Address equals to 00b0d086d6f7
 IP Address equals to 192.0.2.2
 Interface equals to Unit/Slot 1/1 Port GE1 LAG 1

VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	Status	Reason
1	00:b0:d0:86:d6:f7	192.0.2.2	GE1/1/1	Dynamic	3456	Inactive	No Snoop VLAN	

Add... Delete Clear Dynamic

Nel campo Motivo viene visualizzato il motivo per cui l'interfaccia non è attiva. I motivi possono essere i seguenti:

·Nessun problema: l'interfaccia è attiva.

·No Snoop VLAN: lo snooping DHCP non è abilitato sulla VLAN.

·Porta attendibile: la porta è attendibile.

·Problema di risorse: le risorse TCAM vengono utilizzate.

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: VLAN ID equals to (Range: 1 - 4094)

MAC Address equals to

IP Address equals to

Interface equals to Unit/Slot Port LAG

	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	
							Status	Reason
<input type="checkbox"/>	1	00:b0:d0:86:d6:f7	192.0.2.2	GE1/1/1	Dynamic	3456	Inactive	No Snoop VLAN

Passaggio 9. Per visualizzare un subset delle voci, immettere i criteri di ricerca appropriati nella tabella del database di associazione e fare clic su **Vai**. Le caselle di controllo dei filtri vengono utilizzate per filtrare una determinata voce dalla tabella del database di binding DHCP.

Passaggio 10. (Facoltativo) Per rimuovere i valori immessi e immettere nuovi valori, fare clic su **Cancella dinamico**.

Passaggio 11. Fare clic su **Apply** (Applica) per aggiornare il file di configurazione in esecuzione.