

Configuration de la protection de la source IP sur les commutateurs empilables de la gamme Sx500

Objectif

La protection de la source IP est une fonction de sécurité qui peut être utilisée pour empêcher les attaques de trafic lorsqu'un hôte tente d'utiliser l'adresse IP d'un hôte voisin. Lorsque la protection de la source IP est activée, le commutateur transmet uniquement le trafic IP du client aux adresses IP contenues dans la base de données de liaison de surveillance DHCP. Si le paquet envoyé par un hôte correspond à une entrée de la base de données, le commutateur transfère le paquet. Si le paquet ne correspond pas à une entrée de la base de données, il est abandonné.

Dans un scénario en temps réel, l'une des manières d'utiliser la protection de la source IP consiste à empêcher les attaques de l'homme du milieu lorsqu'un tiers non fiable tente de se faire passer pour un utilisateur authentique. En fonction des adresses configurées dans la base de données de liaison de la protection de source IP, seul le trafic provenant du client avec cette adresse IP est autorisé et les autres paquets sont abandonnés.

Remarque : la surveillance DHCP doit être activée pour que la protection de la source IP fonctionne. Pour plus de détails sur l'activation de la surveillance DHCP, reportez-vous à l'article *Configuration de la surveillance DHCP sur les commutateurs empilables de la gamme SX500*. Il est également nécessaire de configurer la base de données de liaison pour spécifier les adresses IP autorisées. Pour plus d'informations à ce sujet, consultez l'article *Configuration de la base de données de liaison de surveillance DHCP sur les commutateurs empilables de la gamme SX500*.

Cet article explique comment configurer IP Source Guard sur les commutateurs empilables de la gamme Sx500.

Périphériques pertinents

Commutateurs Empilables · Sx500

Version du logiciel

•v 1.2.7.76

Configurer les paramètres de protection de la source IP

Activer globalement les paramètres de protection de la source IP

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > IP Source Guard > Properties**. La page *IP Source Guard Properties* s'ouvre :

Properties

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: Enable

Apply Cancel

Étape 2. Cochez la case **Activer** pour activer la protection de source IP globalement.

Properties

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: Enable

Apply Cancel

Étape 3. Cliquez sur **Apply** pour appliquer les paramètres.

Modifier les paramètres d'interface pour IP Source Guard

Si la protection de la source IP est activée sur un port ou un LAG non approuvé, les paquets DHCP transmis sont autorisés par la base de données de surveillance DHCP. Si l'adresse IP est activée avec un filtre, la transmission de paquets est autorisée comme suit :

- Trafic IPv4 : le trafic IPv4 associé à l'adresse IP source du port particulier est autorisé.
- Trafic non IPv4 — Tout le trafic non IPv4 est autorisé.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > IP Source Guard > Interface Settings**. La page *Paramètres d'interface* s'ouvre :

Interface Settings

DHCP Snooping must be enabled for IP Source Guard to operate. IP

Interface Settings Table

Filter: *Interface Type* equals to

	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Étape 2. Choisissez un type d'interface dans la liste déroulante Type d'interface et cliquez sur **Aller** dans le champ Filtre.

Le tableau des paramètres d'interface comprend les paramètres suivants.

- Interface : affiche l'interface à laquelle la protection de source IP est appliquée.
- IP Source Guard : indique si IP Source Guard est activé ou non.
- DHCP Snooping Trusted Interface — Indique s'il s'agit d'une interface de confiance DHCP ou non. Les interfaces de confiance ne peuvent recevoir le trafic que depuis le réseau. La protection de la source IP est généralement configurée sur les interfaces DHCP qui ne sont pas fiables. Une interface non fiable est une interface configurée de sorte qu'elle puisse recevoir des messages en dehors du réseau.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input checked="" type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Étape 3. Activez la case d'option correspondant à l'interface à modifier et cliquez sur **Modifier** en bas de la page. La fenêtre *Modifier les paramètres de l'interface* apparaît.

Interface: Unit/Slot Port LAG

IP Source Guard: Enabled

Étape 4. Cochez **Enable** dans le champ IP Source Guard pour activer IP Source Guard sur l'interface actuelle.

Interface: Unit/Slot Port LAG

IP Source Guard: Enabled

Étape 5. Cliquez sur Apply. Les modifications sont affichées.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input checked="" type="radio"/>	1	FE1	Yes	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Copier les paramètres d'interface pour la protection de la source IP

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > IP Source Guard > Interface Settings**. La page *Paramètres d'interface* s'ouvre :

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	Yes	No
<input checked="" type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Étape 2. Activez la case d'option correspondant à l'interface souhaitée et cliquez sur **Copy Settings**. La fenêtre *Copy Settings* s'affiche.

Copy configuration from entry 2 (FE2)

to: (Example: 1,3,5-10 or: FE1,FE3-FE5)

Étape 3. Entrez la ou les interfaces ou la ou les pages d'interfaces auxquelles l'entrée

sélectionnée doit être copiée et cliquez sur **Apply**. Les paramètres sont appliqués.