Konfiguration der Port-Sicherheit auf Stackable Switches der Serie Sx500

Ziel

Die Port-Sicherheit kann mit dynamisch abgefragten und statischen MAC-Adressen verwendet werden, um den eingehenden Datenverkehr eines Ports zu begrenzen, da dadurch die MAC-Adressen begrenzt werden, die Datenverkehr an den Port senden dürfen. Wenn einem sicheren Port eine sichere MAC-Adresse zugewiesen ist, leitet der Port keinen eingehenden Datenverkehr für solche weiterleiten, die über Quell-MAC-Adressen verfügen, die nicht mit den definierten Adressen vergleichbar sind.

In diesem Dokument wird die Konfiguration der Port-Sicherheit auf Switches der Serie Sx500 erläutert.

Anwendbare Geräte

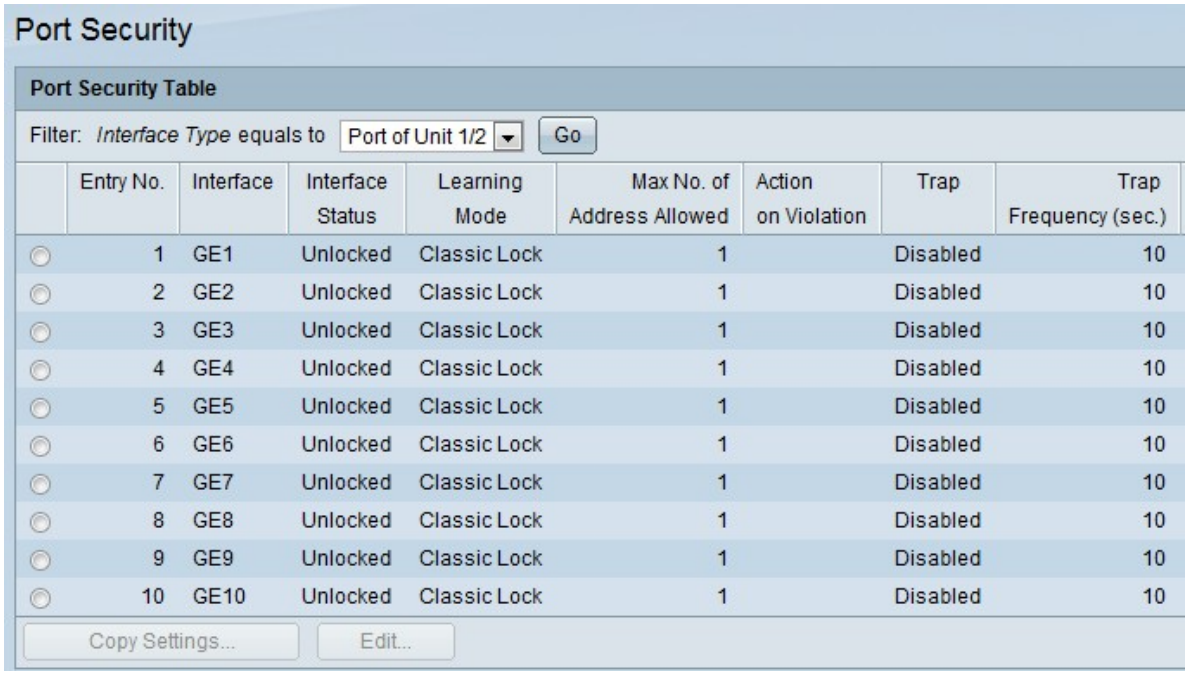
·Stackable Switches der Serie Sx500

Softwareversion

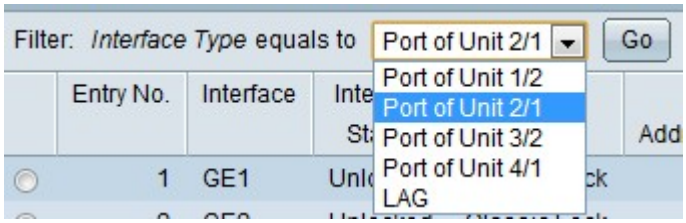
·v1.2.7.76

Konfiguration der Port-Sicherheit

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Port Security aus**. Die Seite *"Port Security"* wird geöffnet:



Schritt 2: Aus dem Filter: Wählen Sie in der Dropdown-Liste Interface Type (Schnittstellentyp) den Schnittstellentyp aus, für den das Paket erwartet wird.



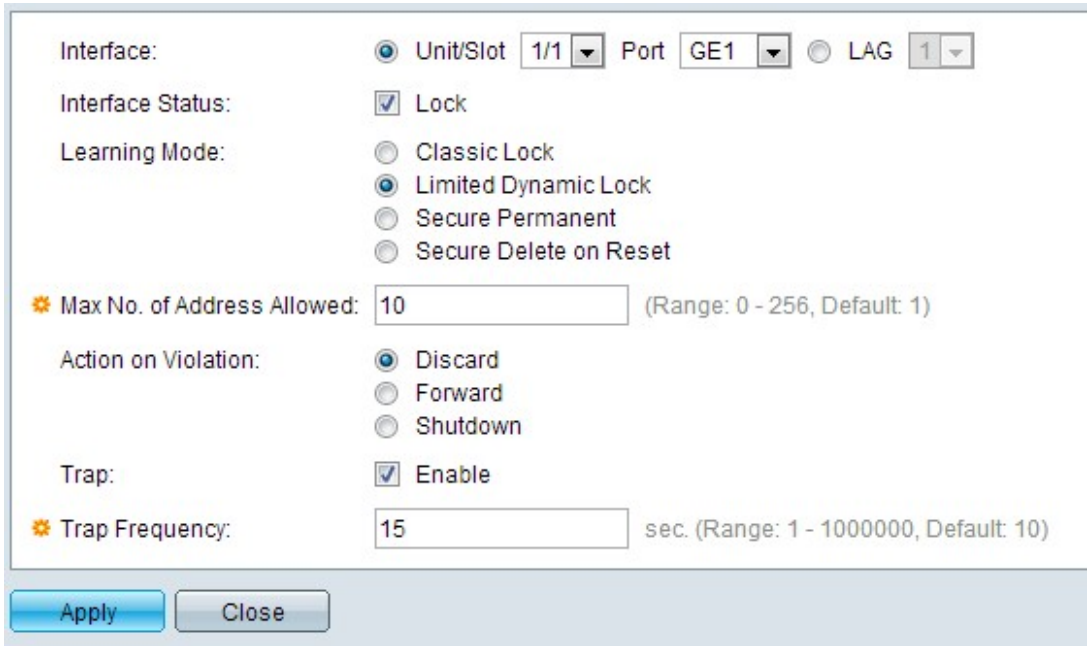
Schritt 3: Klicken Sie auf **Los**, um den Status der Schnittstellen anzuzeigen.

Schritt 4: Klicken Sie auf die zu ändernde Schnittstelle, und klicken Sie auf **Bearbeiten**. Das Fenster *Edit Port Security Interface Settings (Einstellungen für die Port-Sicherheitsschnittstelle bearbeiten*) wird angezeigt.

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
1	GE1	Unlocked	Classic Lock	1		Disabled	10
2	GE2	Unlocked	Classic Lock	1		Disabled	10
3	GE3	Unlocked	Classic Lock	1		Disabled	10
4	GE4	Unlocked	Classic Lock	1		Disabled	10
5	GE5	Unlocked	Classic Lock	1		Disabled	10
6	GE6	Unlocked	Classic Lock	1		Disabled	10
7	GE7	Unlocked	Classic Lock	1		Disabled	10
8	GE8	Unlocked	Classic Lock	1		Disabled	10
9	GE9	Unlocked	Classic Lock	1		Disabled	10
10	GE10	Unlocked	Classic Lock	1		Disabled	10

Copy Settings... Edit...

Schritt 5: (Optional) Zum Ändern der von Ihnen konfigurierten Schnittstelle klicken Sie im Feld *Schnittstelle* auf das gewünschte Optionsfeld und wählen die gewünschte Schnittstelle aus der Dropdown-Liste aus.



·Einheit/Steckplatz - Wählen Sie aus den Dropdown-Listen Einheit/Steckplatz die entsprechende Einheit/Steckplatz aus. Die Einheit identifiziert, ob der Switch aktiv ist oder ein Stack-Element vorhanden ist. Der Steckplatz identifiziert, welcher Switch an welchen Steckplatz angeschlossen ist (Steckplatz 1 ist SF500 und Steckplatz 2 ist SG500). Wenn Sie mit den verwendeten Begriffen nicht vertraut sind, lesen Sie Cisco Business: Glossar neuer Begriffe.

· Port - Wählen Sie in der Dropdown-Liste "Port" den gewünschten Port aus, den Sie konfigurieren möchten.

·LAG: Wählen Sie die LAG aus der LAG-Dropdown-Liste aus. Eine Link Aggregate Group (LAG) dient zum Verbinden mehrerer Ports. LAGs vervielfachen die Bandbreite, erhöhen die Portflexibilität und bieten Verbindungsredundanz zwischen zwei Geräten, um die Port-Nutzung zu optimieren.

Schritt 6: (Optional) Um den Port sofort zu sperren und keine neuen MAC-Adressen zu erhalten, aktivieren Sie im Feld *Schnittstellenstatus* Sperren.

Zeitgeber: Wenn Sperren aktiviert ist, fahren Sie mit Schritt 9 fort.

Schritt 7: Klicken Sie im Feld "*Learning Mode*" auf das Optionsfeld, das der gewünschten Art der erforderlichen Portsperrung entspricht. Es gibt vier Optionen.

·Klassische Sperre - Sperrt den Port sofort ohne Rücksicht auf die Anzahl der Adressen, die bereits gelernt wurden. Der Port erkennt keine neuen MAC-Adressen. Die erlernten Adressen können nicht neu erlernt oder gealtert werden.

·Eingeschränkte dynamische Sperrung - Sperrt den Port, entfernt die aktuellen dynamischen MAC-Adressen für den Port und anschließend lernt der Port Adressen bis zum maximalen Grenzwert. Der Port kann neu erlernt und gealtert werden.

·Secure Permanent - Die aktuelle dynamische MAC-Adresse, die sich auf den Port bezieht, wird beibehalten und die maximale Anzahl zulässiger Adressen auf dem Port ermittelt. Dies wird durch das Feld *Max No. of Address Allowed (Max. Anzahl zulässiger Adressen)* festgelegt. Releasing und Altern sind aktiviert.

·Sichere Löschung bei Zurücksetzen - Nach dem Zurücksetzen des Ports wird die aktuelle dynamische MAC-Adresse gelöscht. MAC-Adressen können basierend auf der Anzahl zulässiger Adressen auf dem Port abgerufen werden. Dies wird durch das Feld *Max No. of Address Allowed (Max. Anzahl zulässiger Adressen)* festgelegt. Releasing und Altern sind deaktiviert.

Schritt 8: Wenn in Schritt 7 nicht auf die klassische Sperre geklickt wird, geben Sie die maximale Anzahl von MAC-Adressen ein, die auf einem Port gelernt werden können, wenn auf den Modus "Eingeschränkte dynamische Sperrung" geklickt wird. Die Zahl 0 gibt an, dass auf der Schnittstelle nur statische Adressen unterstützt werden.

Schritt 9: Wenn Sperren in Schritt 6 aktiviert ist, klicken Sie im Feld *Aktion bei Verletzung* auf ein Optionsfeld, um die Aktion auszuwählen, die für die Pakete ausgeführt werden soll, die am gesperrten Port empfangen werden.

·Verwerfen - Verwirft Pakete von einer beliebigen unbekannten Quelle.

·Forward (Weiterleiten): Leitet Pakete von einer unbekannten Quelle weiter, ohne die MAC-Adresse zu kennen.

·Herunterfahren - Verwirft Pakete von einer beliebigen unbekannten Quelle und der Port wird heruntergefahren. Dieser Port wird so lange heruntergefahren, bis er neu aktiviert oder der Switch neu gestartet wird.

Schritt 10: (Optional) Um Traps zu aktivieren, wenn ein gesperrter Port ein Paket empfängt, aktivieren Sie im *Trap*-Feld Aktivieren. Sie gilt für Sperrverletzungen. Bei Classic Lock ist

dies eine beliebige neue Adresse. Bei einer eingeschränkten dynamischen Sperrung handelt es sich um eine neue Adresse, die die Anzahl der zulässigen Adressen überschreitet.

Zeitgeber: Wenn unter Schritt 10 die Option Enable (Aktivieren) nicht aktiviert ist, fahren Sie mit Schritt 12 fort.

Schritt 11: Geben Sie die Mindestzeit in Sekunden ein, die zwischen den Traps im Feld *Trap Frequency (Trap-Frequenz)* verläuft.

Schritt 12: Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen.

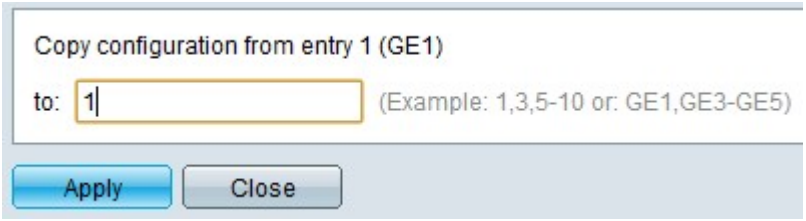
Kopiereinstellungen

Schritt 1: Klicken Sie auf die zu ändernde Schnittstelle, und klicken Sie auf **Copy Settings**. Das Fenster *Kopiereinstellungen* wird angezeigt.

	Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
◉	1	GE1	Unlocked	Classic Lock	1		Disabled	10
○	2	GE2	Unlocked	Classic Lock	1		Disabled	10
○	3	GE3	Unlocked	Classic Lock	1		Disabled	10
○	4	GE4	Unlocked	Classic Lock	1		Disabled	10
○	5	GE5	Unlocked	Classic Lock	1		Disabled	10
○	6	GE6	Unlocked	Classic Lock	1		Disabled	10
○	7	GE7	Unlocked	Classic Lock	1		Disabled	10
○	8	GE8	Unlocked	Classic Lock	1		Disabled	10
○	9	GE9	Unlocked	Classic Lock	1		Disabled	10
○	10	GE10	Unlocked	Classic Lock	1		Disabled	10

Copy Settings... Edit...

Schritt 2: Geben Sie die Schnittstelle bzw. den Bereich bzw. die Schnittstellen ein, auf die bzw. die die Konfiguration in das angegebene Feld kopiert werden muss.



Schritt 3: Klicken Sie auf **Apply**, um die Port-Sicherheit zu ändern und die aktuelle Konfigurationsdatei zu aktualisieren.