Konfigurationsbeispiel für Layer-2-Sicherheitsfunktionen in Cisco Catalyst Layer-3-Switches mit fester Konfiguration

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für einige der Layer-2-Sicherheitsfunktionen, wie Port-Sicherheit, DHCP-Snooping, dynamische ARP-Inspektion (Address Resolution Protocol) und IP Source Guard, die auf Cisco Catalyst Layer-3-Switches mit fester Konfiguration implementiert werden können.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Catalyst Switch der Serie 3750 mit Version 12.2(25)SEC2.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware-Komponenten verwendet werden:

- Cisco Catalyst Switches der Serie 3550
- Cisco Catalyst Switches der Serie 3560
- Cisco Catalyst Switches der Serie 3560-E
- Cisco Catalyst Switches der Serie 3750-E

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Ähnlich wie Router verfügen Layer-2- und Layer-3-Switches über eigene Set von Netzwerksicherheitsanforderungen. Switches sind anfällig für viele der gleichen Layer-3-Angriffe wie Router. Allerdings unterliegen Switches und Layer 2 des OSI-Referenzmodells im Allgemeinen auf unterschiedliche Weise Netzwerkangriffen. Dazu gehören:

- **Tabellenüberlauf für Content Addressable Memory (CAM)**Die Größe der Tabellen für den Content Addressable Memory (CAM) ist begrenzt. Wenn genügend Einträge in die CAM-Tabelle eingegeben wurden, bevor andere Einträge abgelaufen sind, füllt die CAM-Tabelle so weit aus, dass keine neuen Einträge mehr akzeptiert werden können. In der Regel überflutet ein Netzwerkeingriffe den Switch mit einer großen Anzahl ungültiger MAC-Adressen (Source Media Access Control), bis die CAM-Tabelle ausgefüllt ist. In diesem Fall flutet der Switch alle Ports mit eingehendem Datenverkehr, da er die Portnummer für eine bestimmte MAC-Adresse nicht in der CAM-Tabelle finden kann. Der Switch fungiert im Wesentlichen wie ein Hub. Wenn der Eindringling die Flut von ungültigen Quell-MAC-Adressen nicht aufrecht erhält, löst der Switch am Ende ältere MAC-Adresseinträge aus der CAM-Tabelle aus und beginnt wieder wie ein Switch zu agieren. Der Überlauf der CAM-Tabelle flutet nur den Datenverkehr innerhalb des lokalen VLAN, sodass der Eindringling nur den Datenverkehr innerhalb des lokalen VLANs sieht, mit dem er verbunden ist.Der Überlaufangriff der CAM-Tabelle kann durch Konfigurieren der Port-Sicherheit auf dem Switch abgeschwächt werden. Diese Option ermöglicht entweder die Angabe der MAC-Adressen an einem bestimmten Switch-Port oder die Angabe der Anzahl der MAC-Adressen, die von einem Switch-Port abgerufen werden können. Wenn eine ungültige MAC-Adresse auf dem Port erkannt wird, kann der Switch entweder die falsche MAC-Adresse blockieren oder den Port ausschalten. Die Spezifikation von MAC-Adressen auf Switch-Ports ist eine Lösung für eine Produktionsumgebung viel zu unkontrollierbar. Ein Grenzwert für die Anzahl der MAC-Adressen auf einem Switch-Port ist verwaltbar. Eine verwaltungstechnisch skalierbarere Lösung ist die Implementierung dynamischer Port-Sicherheit am Switch. Um die dynamische Port-Sicherheit zu

implementieren, geben Sie eine maximale Anzahl von MAC-Adressen an, die gelernt werden.

- **MAC-Spoofing (Media Access Control)**Bei MAC-Spoofing-Angriffen (Media Access Control) wird eine bekannte MAC-Adresse eines anderen Hosts verwendet, um zu versuchen, den Ziel-Switch Frames, die für den Remote-Host bestimmt sind, an den Netzwerk-Angreifer weiterzuleiten. Wenn ein einzelner Frame mit der Quell-Ethernet-Adresse des anderen Hosts gesendet wird, überschreibt der Netzwerkangreifer den CAM-Tabelleneintrag, sodass der Switch Pakete, die für den Host bestimmt sind, an den Netzwerkangreifer weiterleitet. Bis der Host Datenverkehr sendet, empfängt er keinen Datenverkehr. Wenn der Host Datenverkehr sendet, wird der Eintrag der CAM-Tabelle erneut so geschrieben, dass er zum ursprünglichen Port zurückkehrt.Verwenden Sie die Funktion für die Port-Sicherheit, um MAC-Spoofing-Angriffe abzuwehren. Die Port-Sicherheit bietet die Möglichkeit, die MAC-Adresse des Systems anzugeben, das mit einem bestimmten Port verbunden ist. Dies bietet auch die Möglichkeit, eine Aktion festzulegen, die ausgeführt werden soll, wenn eine Verletzung der Port-Sicherheit auftritt.
- **ARP-Spoofing (Address Resolution Protocol)**ARP wird verwendet, um MAC-Adressen in einem LAN-Segment, in dem sich Hosts desselben Subnetzes befinden, die IP-Adressierung zuzuordnen. Normalerweise sendet ein Host eine Broadcast-ARP-Anfrage, um die MAC-Adresse eines anderen Hosts mit einer bestimmten IP-Adresse zu ermitteln. Eine ARP-Antwort stammt vom Host, dessen Adresse mit der Anfrage übereinstimmt. Der anfordernde Host zwischenspeichert diese ARP-Antwort anschließend. Im ARP-Protokoll ist eine weitere Bestimmung für Hosts vorgesehen, unangeforderte ARP-Antworten auszuführen. Die unerwünschten ARP-Antworten werden als Gratuitous ARP (GARP) bezeichnet. GARP kann von einem Angreifer böswillig ausgenutzt werden, um die Identität einer IP-Adresse in einem LAN-Segment zu verfälschen. Dies wird in der Regel verwendet, um die Identität zwischen zwei Hosts oder den gesamten Datenverkehr zu und von einem Standard-Gateway bei einem Man-in-the-Middle-Angriff zu verfälschen.Wenn eine ARP-Antwort erstellt wird, kann ein Netzwerkangreifer sein System als Ziel-Host erscheinen lassen, der vom Absender gesucht wird. Die ARP-Antwort veranlasst den Absender, die MAC-Adresse des Systems des Netzwerkangreifers im ARP-Cache zu speichern. Diese MAC-Adresse wird auch vom Switch in der CAM-Tabelle gespeichert. Auf diese Weise hat der Netzwerkangreifer die MAC-Adresse seines Systems sowohl in die Switch-CAM-Tabelle als auch in den ARP-Cache des Absenders eingefügt. Auf diese Weise kann der Netzwerkangreifer Frames abfangen, die für den Host bestimmt sind, den er Spoofing ausführt.Mit Hold-Down-Timern im Schnittstellenkonfigurationsmenü können ARP-Spoofing-Angriffe abgewehrt werden, indem die Dauer festgelegt wird, die ein Eintrag im ARP-Cache verbleibt. Die Hold-Down-Timer allein sind jedoch nicht ausreichend. Eine Modifizierung der ARP-Cache-Ablaufzeit auf allen Endsystemen ist ebenso erforderlich wie statische ARP-Einträge. Eine weitere Lösung, mit der verschiedene ARP-basierte Netzwerk-Exploits abgewehrt werden können, ist die Verwendung von DHCP-Snooping zusammen mit dynamischer ARP-Inspektion. Diese Catalyst-Funktionen validieren ARP-Pakete in einem Netzwerk und ermöglichen das Abfangen, Protokollieren und Verwerfen von ARP-Paketen mit ungültigen MAC-Adressen-zu-IP-Adressen-Bindings.DHCP-Snooping filtert vertrauenswürdige DHCP-Nachrichten, um die Sicherheit zu gewährleisten. Anschließend werden diese Meldungen verwendet, um eine Bindungstabelle für DHCP-Snooping zu erstellen und zu verwalten. DHCP-Snooping berücksichtigt DHCP-Meldungen, die von einem benutzerseitigen Port stammen, der kein DHCP-Serverport als nicht vertrauenswürdig gilt. Aus Sicht von DHCP-Snooping dürfen diese nicht vertrauenswürdigen, an Benutzer gerichteten Ports keine DHCP-Servertypantworten senden, z. B. DHCPOFFER, DHCPACK oder DHCPNAK. Die Bindungstabelle für DHCP-

Snooping enthält die MAC-Adresse, die IP-Adresse, die Leasingzeit, den Bindungstyp, die VLAN-Nummer und die Schnittstelleninformationen, die den lokalen nicht vertrauenswürdigen Schnittstellen eines Switches entsprechen. Die Bindungstabelle für DHCP-Snooping enthält keine Informationen über Hosts, die mit einer vertrauenswürdigen Schnittstelle verbunden sind. Eine nicht vertrauenswürdige Schnittstelle ist eine Schnittstelle, die für den Empfang von Nachrichten von außerhalb des Netzwerks oder der Firewall konfiguriert ist. Eine vertrauenswürdige Schnittstelle ist eine Schnittstelle, die so konfiguriert ist, dass sie nur Nachrichten aus dem Netzwerk empfängt. Die DHCP-Snooping-Bindungstabelle kann sowohl dynamische als auch statische MAC-Adressen für IP-Adressen-Bindings enthalten.Die dynamische ARP-Inspektion bestimmt die Gültigkeit eines ARP-Pakets auf der Grundlage der gültigen MAC-Adresse für IP-Adressen-Bindungen, die in einer DHCP-Snooping-Datenbank gespeichert sind. Darüber hinaus kann eine dynamische ARP-Inspektion ARP-Pakete anhand von benutzerdefinierten Zugriffskontrolllisten (ACLs) validieren. Dies ermöglicht die Überprüfung von ARP-Paketen für Hosts, die statisch konfigurierte IP-Adressen verwenden. Dynamische ARP-Inspektion ermöglicht die Verwendung von PACLs (Access Control Lists) pro Port und VLAN, um ARP-Pakete für bestimmte IP-Adressen auf bestimmte MAC-Adressen zu beschränken.

- **DHCP-Unterdrückung (Dynamic Host Configuration Protocol)**Ein DHCP-Hungerangriff sendet DHCP-Anfragen mit gefälschten MAC-Adressen. Wenn genügend Anfragen gesendet werden, kann der Netzwerkangreifer den Adressraum für die DHCP-Server für einen bestimmten Zeitraum ausschöpfen. Der Netzwerkangreifer kann dann einen nicht autorisierten DHCP-Server auf seinem System einrichten und auf neue DHCP-Anfragen von Clients im Netzwerk reagieren. Durch die Platzierung eines nicht autorisierten DHCP-Servers im Netzwerk kann ein Netzwerkangreifer Clients Adressen und andere Netzwerkinformationen bereitstellen. Da DHCP-Antworten normalerweise Standardgateway- und DNS-Serverinformationen enthalten, kann der Netzwerkangreifer sein eigenes System als Standard-Gateway und DNS-Server bereitstellen. Dies führt zu einem Man-in-the-Middle-Angriff. Allerdings ist nicht das Ausschöpfen aller DHCP-Adressen erforderlich, um einen nicht autorisierten DHCP-Server einzuführen.Zusätzliche Funktionen der Catalyst-Switches, wie z. B. DHCP-Snooping, können zum Schutz vor DHCP-Ausfällen verwendet werden. DHCP-Snooping ist eine Sicherheitsfunktion, die nicht vertrauenswürdige DHCP-Nachrichten filtert und eine DHCP-Snooping-Bindungstabelle erstellt und verwaltet. Die Bindungstabelle enthält Informationen wie die MAC-Adresse, die IP-Adresse, die Leasingzeit, den Bindungstyp, die VLAN-Nummer und die Schnittstelleninformationen, die den lokalen nicht vertrauenswürdigen Schnittstellen eines Switches entsprechen. Nicht vertrauenswürdige Nachrichten werden von außerhalb des Netzwerks oder der Firewall empfangen. Nicht vertrauenswürdige Switch-Schnittstellen sind solche, die so konfiguriert sind, dass sie solche Nachrichten von außerhalb des Netzwerks oder der Firewall empfangen.Andere Catalyst Switch-Funktionen wie IP Source Guard bieten zusätzlichen Schutz vor Angriffen wie DHCP-Ausfall und IP-Spoofing. Ähnlich wie beim DHCP-Snooping ist IP Source Guard auf nicht vertrauenswürdigen Layer-2-Ports aktiviert. Der gesamte IP-Datenverkehr wird anfänglich blockiert, mit Ausnahme der DHCP-Pakete, die vom DHCP-Snooping-Prozess erfasst werden. Sobald ein Client eine gültige IP-Adresse vom DHCP-Server erhält, wird eine PACL auf den Port angewendet. Dadurch wird der Client-IP-Datenverkehr auf die in der Bindung konfigurierten Quell-IP-Adressen beschränkt. Jeder andere IP-Datenverkehr mit einer anderen Quelladresse als den Adressen in der Bindung wird gefiltert.

Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der Funktionen Port Security, DHCP Snooping, Dynamic ARP Inspection und IP Source Guard.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

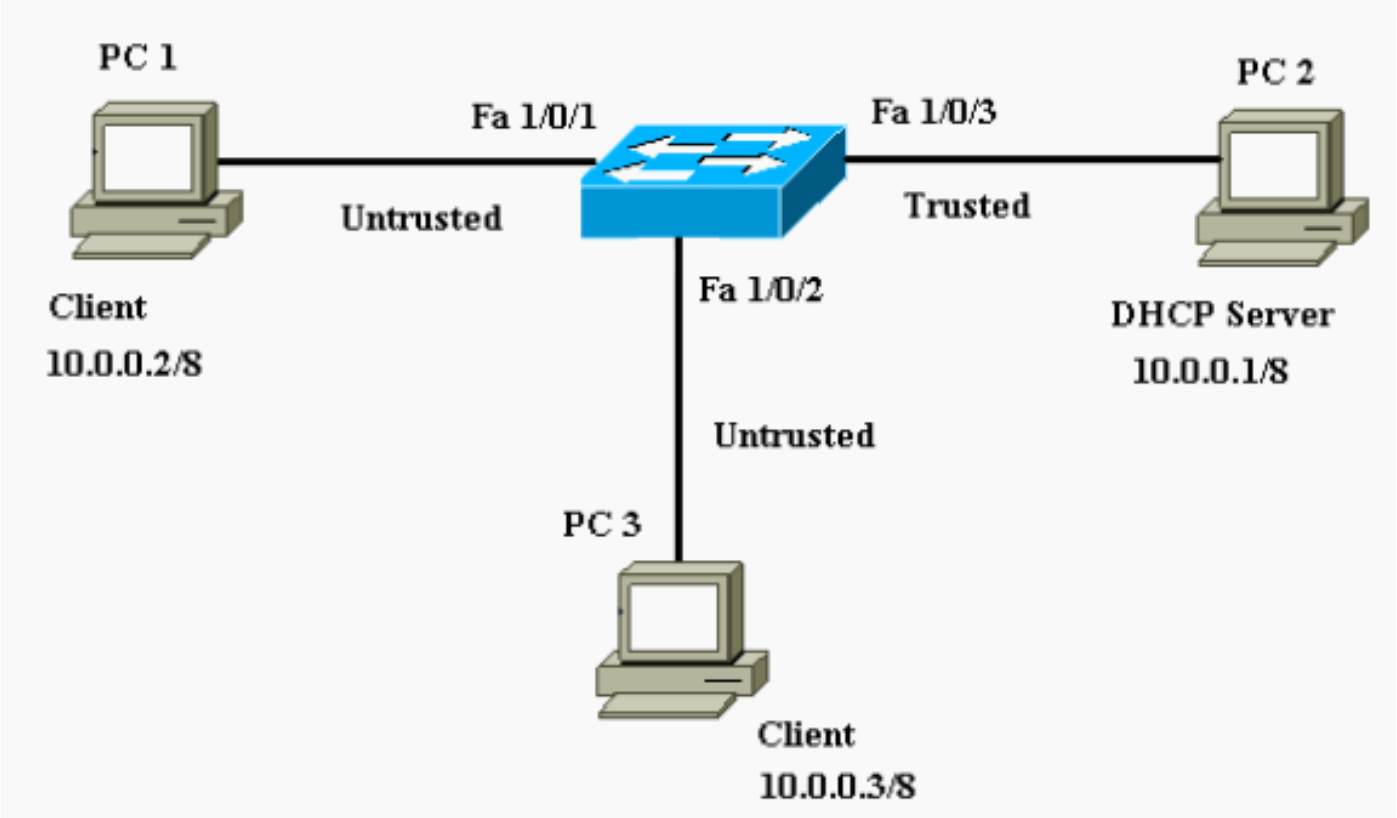
Die Konfigurationen des Catalyst 3750-Switches umfassen Folgendes:

- Port-Sicherheit
- DHCP-Snooping
- Dynamische ARP-Inspektion
- IP Source Guard

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

- PC 1 und PC 3 sind Clients, die mit dem Switch verbunden sind.
- PC 2 ist ein mit dem Switch verbundener DHCP-Server.
- Alle Ports des Switches befinden sich im gleichen VLAN (VLAN 1).
- Der DHCP-Server ist so konfiguriert, dass den Clients basierend auf ihren MAC-Adressen IP-Adressen zugewiesen werden.



Port-Sicherheit

Sie können die Funktion für die Port-Sicherheit verwenden, um MAC-Adressen der Stationen zu begrenzen und zu identifizieren, die auf den Port zugreifen dürfen. Dadurch wird die Eingabe auf

eine Schnittstelle beschränkt. Wenn Sie einem sicheren Port sichere MAC-Adressen zuweisen, leitet der Port keine Pakete mit Quelladressen außerhalb der Gruppe definierter Adressen weiter. Wenn Sie die Anzahl sicherer MAC-Adressen auf eine begrenzen und eine einzige sichere MAC-Adresse zuweisen, wird der an diesen Port angeschlossenen Workstation die volle Bandbreite des Ports zugesichert. Wenn ein Port als sicherer Port konfiguriert ist und die maximale Anzahl an sicheren MAC-Adressen erreicht wird, wenn sich die MAC-Adresse einer Station, die versucht, auf den Port zuzugreifen, von einer der identifizierten sicheren MAC-Adressen unterscheidet, tritt eine Sicherheitsverletzung auf. Wenn eine Station mit einer sicheren MAC-Adresse, die auf einem sicheren Port konfiguriert oder abgerufen wurde, versucht, auf einen anderen sicheren Port zuzugreifen, wird eine Verletzung markiert. Standardmäßig wird der Port deaktiviert, wenn die maximale Anzahl an sicheren MAC-Adressen überschritten wird.

Hinweis: Wenn ein Catalyst Switch der Serie 3750 einem Stack beitritt, erhält der neue Switch die konfigurierten sicheren Adressen. Alle dynamischen sicheren Adressen werden vom neuen Stack-Element von den anderen Stack-Elementen heruntergeladen.

Richtlinien zur Konfiguration der Port-Sicherheit finden Sie in den Konfigurationsrichtlinien.

Hier wird die Port-Sicherheitsfunktion für die FastEthernet 1/0/2-Schnittstelle konfiguriert angezeigt. Standardmäßig ist die maximale Anzahl sicherer MAC-Adressen für die Schnittstelle eine. Sie können den Befehl **show port-security interface** eingeben, um den Portsicherheitsstatus einer Schnittstelle zu überprüfen.

Port-Sicherheit

```
Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
!--- Default port security configuration on the switch.
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#interface fastEthernet 1/0/2
Cat3750(config-if)#switchport port-security
Command rejected: FastEthernet1/0/2 is a dynamic port.
!--- Port security can only be configured on static
access ports or trunk ports. Cat3750(config-
if)#switchport mode access
!--- Sets the interface switchport mode as access.
Cat3750(config-if)#switchport port-security
!--- Enables port security on the interface.
Cat3750(config-if)#switchport port-security mac-address
0011.858D.9AF9
!--- Sets the secure MAC address for the interface.
Cat3750(config-if)#switchport port-security violation
shutdown
!--- Sets the violation mode to shutdown. This is the
default mode. Cat3750# !--- Connected a different PC (PC
```

```
4) to the FastEthernet 1/0/2 port !--- to verify the
port security feature. 00:22:51: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa1/0/2, putting
Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet1/0/2, changed state to down
00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2,
changed state to down !--- Interface shuts down when a
security violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2
FastEthernet1/0/2 is down, line protocol is down (err-
disabled)
!--- Output Suppressed. !--- The port is shown error-
disabled. This verifies the configuration. !--- Note:
When a secure port is in the error-disabled state, !---
you can bring it out of this state by entering !--- the
errdisable recovery cause psecure-violation global
configuration command, !--- or you can manually re-
enable it by entering the !--- shutdown and no shutdown
interface configuration commands.


Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0011.8565.4B75:1
Security Violation Count   : 1
```

Hinweis: Dieselben MAC-Adressen sollten nicht als sichere und statische MAC-Adresse auf verschiedenen Ports eines Switches konfiguriert werden.

Wenn ein IP-Telefon über den für das Sprach-VLAN konfigurierten Switch-Port mit einem Switch verbunden ist, sendet das Telefon nicht getaggte CDP-Pakete und getaggte Sprach-CDP-Pakete. Die MAC-Adresse des IP-Telefons wird also sowohl auf der PVID als auch auf der VVID erfasst. Wenn die entsprechende Anzahl an sicheren Adressen nicht konfiguriert ist, wird eine Fehlermeldung ähnlich der folgenden Meldung angezeigt:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

Um dieses Problem zu beheben, müssen Sie die maximal zulässige Anzahl sicherer Adressen am Port auf zwei (für IP-Telefon) plus die maximal zulässige Anzahl sicherer Adressen für das Zugriffs-VLAN festlegen.

Weitere Informationen finden Sie unter Konfigurieren der Port-Sicherheit.

DHCP-Snooping

DHCP-Snooping fungiert als Firewall zwischen nicht vertrauenswürdigen Hosts und DHCP-Servern. Mit DHCP-Snooping können Sie zwischen nicht vertrauenswürdigen Schnittstellen, die mit dem Endbenutzer verbunden sind, und vertrauenswürdigen Schnittstellen, die mit dem DHCP-Server oder einem anderen Switch verbunden sind, unterscheiden. Wenn ein Switch ein Paket an einer nicht vertrauenswürdigen Schnittstelle empfängt und die Schnittstelle zu einem VLAN gehört, für das DHCP-Snooping aktiviert ist, vergleicht der Switch die Quell-MAC-Adresse mit der DHCP-Client-Hardwareadresse. Wenn die Adressen übereinstimmen (die Standardadresse), leitet der Switch das Paket weiter. Wenn die Adressen nicht übereinstimmen, verwirft der Switch das Paket. Der Switch verwirft ein DHCP-Paket, wenn eine der folgenden Situationen eintritt:

- Ein Paket von einem DHCP-Server, z. B. ein DHCPOFFER-, DHCPACK-, DHCPNAK- oder DHCPLEASEQUERY-Paket, wird von außerhalb des Netzwerks oder der Firewall empfangen.
- Ein Paket wird auf einer nicht vertrauenswürdigen Schnittstelle empfangen, und die Quell-MAC-Adresse und die DHCP-Client-Hardwareadresse stimmen nicht überein.
- Der Switch empfängt eine DHCPRELEASE- oder DHCPDECLINE-Broadcast-Nachricht mit einer MAC-Adresse in der DHCP-Snooping-Bindungsdatenbank, aber die Schnittstelleninformationen in der Bindungsdatenbank stimmen nicht mit der Schnittstelle überein, auf der die Nachricht empfangen wurde.
- Ein DHCP Relay Agent leitet ein DHCP-Paket weiter, das eine Relay-Agent-IP-Adresse ohne 0.0.0.0 enthält, oder der Relay Agent leitet ein Paket mit Option-82-Informationen an einen nicht vertrauenswürdigen Port weiter.

Richtlinien zur Konfiguration von DHCP-Snooping finden Sie in den DHCP Snooping-Konfigurationsrichtlinien.

Hinweis: Damit DHCP-Snooping ordnungsgemäß funktioniert, müssen alle DHCP-Server über vertrauenswürdige Schnittstellen mit dem Switch verbunden sein.

Hinweis: In einem Switch-Stack mit Catalyst 3750-Switches wird DHCP-Snooping auf dem Stack-Master verwaltet. Wenn ein neuer Switch dem Stack beitritt, erhält der Switch die DHCP-Snooping-Konfiguration vom Stack-Master. Wenn ein Mitglied den Stack verlässt, werden alle dem Switch zugeordneten DHCP-Snooping-Bindings veraltet.

Hinweis: Um sicherzustellen, dass die Lease-Zeit in der Datenbank korrekt ist, empfiehlt Cisco die Aktivierung und Konfiguration von NTP. Wenn NTP konfiguriert ist, schreibt der Switch Bindungsänderungen nur dann in die Bindungsdatei, wenn die Systemuhr des Switches mit NTP synchronisiert wird.

Nicht autorisierte DHCP-Server können durch DHCP-Snooping-Funktionen abgeschwächt werden. Der Befehl **ip dhcp snooping** wird ausgegeben, um DHCP global auf dem Switch zu aktivieren. Bei der Konfiguration mit DHCP-Snooping sind alle Ports im VLAN für DHCP-Antworten nicht vertrauenswürdig. Hier wird nur die mit dem DHCP-Server verbundene FastEthernet-Schnittstelle 1/0/3 als vertrauenswürdig konfiguriert.

DHCP-Snooping

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1
!--- DHCP snooping is not active until DHCP snooping is
```

```
enabled on a VLAN. Cat3750(config)#no ip dhcp snooping
information option
!--- Disable the insertion and removal of the option-82
field, if the !--- DHCP clients and the DHCP server
reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit
(pps)
------------------------     -------     ---------------
-
FastEthernet1/0/3            yes         unlimited
!--- Displays the DHCP snooping configuration for the
switch. Cat3750#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
VLAN  Interface
------------------  ---------------  ----------  -------
------  ----  --------------------
00:11:85:A5:7B:F5     10.0.0.2        86391       dhcp-
snooping  1    FastEtheret1/0/1
00:11:85:8D:9A:F9     10.0.0.3        86313       dhcp-
snooping  1    FastEtheret1/0/2
Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

Weitere Informationen finden Sie unter Konfigurieren von DHCP-Funktionen.

Dynamische ARP-Inspektion

Dynamic ARP Inspection ist eine Sicherheitsfunktion, die ARP-Pakete in einem Netzwerk validiert. Er fängt ARP-Pakete mit ungültigen IP-zu-MAC-Adressen-Bindings ab, protokolliert und verwirft sie. Diese Funktion schützt das Netzwerk vor bestimmten Man-in-the-Middle-Angriffen.

Dynamische ARP-Inspektion stellt sicher, dass nur gültige ARP-Anfragen und -Antworten weitergeleitet werden. Der Switch führt diese Aktivitäten aus:

- Abfangen aller ARP-Anfragen und -Antworten an nicht vertrauenswürdigen Ports
- Vergewissert sich, dass jedes dieser abgefangenen Pakete über eine gültige IP-zu-MAC-Adressbindung verfügt, bevor es den lokalen ARP-Cache aktualisiert oder das Paket an das entsprechende Ziel weiterleitet
- Löscht ungültige ARP-Pakete

Die dynamische ARP-Inspektion bestimmt die Gültigkeit eines ARP-Pakets auf der Grundlage gültiger IP-zu-MAC-Adressen-Bindings, die in einer vertrauenswürdigen Datenbank, der DHCP-Snooping-Bindungsdatenbank, gespeichert sind. Diese Datenbank wird durch DHCP-Snooping erstellt, wenn DHCP-Snooping auf den VLANs und auf dem Switch aktiviert ist. Wenn das ARP-Paket auf einer vertrauenswürdigen Schnittstelle empfangen wird, leitet der Switch das Paket

ohne Überprüfungen weiter. Auf nicht vertrauenswürdigen Schnittstellen leitet der Switch das Paket nur weiter, wenn es gültig ist.

In Nicht-DHCP-Umgebungen kann die dynamische ARP-Prüfung ARP-Pakete für Hosts mit statisch konfigurierten IP-Adressen mit benutzerdefinierten ARP-ACLs abgleichen. Sie können den globalen Konfigurationsbefehl **arp access-list** ausgeben, um eine ARP-ACL zu definieren. ARP-ACLs haben Vorrang vor Einträgen in der DHCP-Snooping-Binding-Datenbank. Der Switch verwendet ACLs nur, wenn Sie den globalen Konfigurationsbefehl **ip arp Inspection Filter vlan** ausstellen, um die ACLs zu konfigurieren. Der Switch vergleicht zuerst ARP-Pakete mit benutzerdefinierten ARP-ACLs. Wenn die ARP-ACL das ARP-Paket verweigert, verweigert der Switch das Paket auch dann, wenn in der durch DHCP-Snooping belegten Datenbank eine gültige Bindung vorhanden ist.

Richtlinien zum Konfigurieren einer dynamischen ARP-Inspektion finden Sie in den Konfigurationsrichtlinien für die dynamische ARP-Inspektion unter Dynamic ARP Inspection (Dynamische ARP-Inspektion).

Der Befehl **ip arp Inspection vlan** global configuration ermöglicht eine dynamische ARP-Inspektion auf VLAN-Basis. Hier wird nur die mit dem DHCP-Server verbundene FastEthernet-Schnittstelle 1/0/3 mit dem Befehl **ip arp Inspection trust** als vertrauenswürdig konfiguriert. DHCP-Snooping muss aktiviert werden, um ARP-Pakete mit dynamisch zugewiesenen IP-Adressen zuzulassen. Informationen zur DHCP Snooping-Konfiguration finden Sie im Abschnitt DHCP Snooping dieses Dokuments.

Dynamische ARP-Inspektion

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1
!--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match
Static ACL
 ----     -------------    ---------   ---------
----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
!--- Verifies the dynamic ARP inspection configuration.
Cat3750#
```

Weitere Informationen finden Sie unter Konfigurieren der dynamischen ARP-Prüfung.

IP Source Guard

IP Source Guard ist eine Sicherheitsfunktion, die Datenverkehr basierend auf der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierten IP-Quellbindungen filtert, um den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen einzuschränken. Sie können IP Source Guard verwenden, um Datenverkehrsangriffe zu verhindern, die entstehen, wenn ein Host versucht, die IP-Adresse seines Nachbarn zu verwenden. IP Source Guard verhindert IP/MAC Spoofing.

Sie können IP Source Guard aktivieren, wenn DHCP-Snooping auf einer nicht vertrauenswürdigen Schnittstelle aktiviert ist. Wenn IP Source Guard auf einer Schnittstelle aktiviert ist, blockiert der Switch den gesamten auf der Schnittstelle empfangenen IP-Datenverkehr, mit Ausnahme der DHCP-Pakete, die durch DHCP-Snooping zugelassen sind. Auf die Schnittstelle wird eine Port-ACL angewendet. Die Port-ACL lässt nur IP-Datenverkehr mit einer Quell-IP-Adresse in der IP-Quellbindungstabelle zu und verweigert den gesamten anderen Datenverkehr.

Die IP-Quellbindungstabelle enthält Bindungen, die vom DHCP-Snooping abgerufen werden oder manuell konfiguriert werden (statische IP-Quellbindungen). Ein Eintrag in dieser Tabelle hat eine IP-Adresse, die zugeordnete MAC-Adresse und die zugehörige VLAN-Nummer. Der Switch verwendet die IP-Quellbindungstabelle nur, wenn IP Source Guard aktiviert ist.

Sie können IP Source Guard mit IP-Adressfilterung der Quelle oder mit IP- und MAC-Adressfilterung konfigurieren. Wenn IP Source Guard mit dieser Option aktiviert ist, wird der IP-Datenverkehr basierend auf der Quell-IP-Adresse gefiltert. Der Switch leitet IP-Datenverkehr weiter, wenn die Quell-IP-Adresse mit einem Eintrag in der DHCP-Snooping-Binding-Datenbank oder einer Bindung in der IP-Quellbindungstabelle übereinstimmt. Wenn IP Source Guard mit dieser Option aktiviert ist, wird der IP-Datenverkehr basierend auf den Quell-IP- und MAC-Adressen gefiltert. Der Switch leitet Datenverkehr nur weiter, wenn die Quell-IP- und MAC-Adressen mit einem Eintrag in der IP-Quellbindungstabelle übereinstimmen.

Hinweis: IP Source Guard wird nur auf Layer-2-Ports unterstützt, die Zugriffs- und Trunk-Ports enthalten.

Richtlinien zur Konfiguration von IP Source Guard finden Sie in den Konfigurationsrichtlinien des IP Source Guard.

Hier wird IP Source Guard mit IP-Quellfilterung auf der FastEthernet 1/0/1-Schnittstelle mit dem Befehl **ip verify source** konfiguriert. Wenn IP Source Guard mit IP-Quellfilterung in einem VLAN aktiviert ist, muss DHCP-Snooping im Zugriffs-VLAN aktiviert werden, zu dem die Schnittstelle gehört. Geben Sie den Befehl **show ip verify source** ein, um die Konfiguration des IP Source Guard auf dem Switch zu überprüfen.

IP Source Guard

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1
!--- See the DHCP Snooping section of this document for
!--- DHCP snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source
!--- Enables IP source guard with source IP filtering.
Cat3750#show ip verify source
Interface  Filter-type  Filter-mode  IP-address
Mac-address        Vlan
```

```
---------  -----------  -----------  ---------------  --
---------------  -----
Fa1/0/1    ip           active       10.0.0.2
1
!--- For VLAN 1, IP source guard with IP address
filtering is configured !--- on the interface and a
binding exists on the interface. Cat3750#
```

Weitere Informationen finden Sie unter Understanding IP Source Guard.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Sicherung von Netzwerken mit privaten VLANs und VLAN-Zugriffskontrolllisten
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems