Beispiel für die ACL-Erfassung bei Nexus Switches der Serie 7000

Inhalt

Einführung

Die ACL-Erfassung (Access Control List) bietet Ihnen die Möglichkeit, Datenverkehr in einer Schnittstelle oder einem virtuellen VLAN selektiv zu erfassen. Wenn Sie die Erfassungsoption für eine ACL-Regel aktivieren, werden Pakete, die dieser Regel entsprechen, entweder aufgrund der angegebenen Zulassen- oder Ablehnungsaktion weitergeleitet oder verworfen und können zur weiteren Analyse auch in einen alternativen Ziel-Port kopiert werden. Eine ACL-Regel mit der Erfassungsoption kann angewendet werden:

1. In einem VLAN
2. In Eingangsrichtung an allen Schnittstellen
3. Ausgangs- und Layer-3-Schnittstellen

Diese Funktion wird von Nexus 7000 NX-OS 5.2 und höher unterstützt. Dieses Dokument enthält ein Beispiel als Kurzreferenz zur Konfiguration dieser Funktion.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Nexus 7000 mit Version 5.2.x und höher
- Linecard der Serie M1.

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.

Konventionen

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

ACL-Konfigurationsbeispiel

Im Folgenden finden Sie ein Beispiel für die Konfiguration der ACL-Erfassung, die auf ein VLAN angewendet wird, das auch als VACL-Erfassung (Virtual LAN Access Control List) bezeichnet wird. Zehn Gigabit-Sniffer sind möglicherweise nicht für alle Szenerien geeignet. Selektive Datenerfassung kann in solchen Szenarien besonders bei der Fehlerbehebung bei hohen Datenverkehrsmengen sehr nützlich sein.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

Sie können auch die Programmierung des Tternary Content Addressable Memory (TCAM) in der Zugriffsliste überprüfen. Diese Ausgabe gilt für das VLAN 500 für Modul 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------
```

```
Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

Einsprüche

1. Im System kann jeweils nur eine ACL-Aufzeichnungssitzung über Virtual Device Contexts (VDCs) hinweg aktiv sein.
2. Module der Nexus 7000 F1-Serie unterstützen die ACL-Erfassung nicht.
3. Die Module der Nexus 7000 F2-Serie unterstützen derzeit keine ACL-Erfassung. Dies ist jedoch möglicherweise in der Roadmap enthalten.
4. Die ACL-Erfassung auf Modulen der Nexus 7000 M2-Serie wird von Cisco NX-OS 6.1(1) und höher unterstützt.
5. Die ACL-Erfassung auf Modulen der Nexus 7000 M1-Serie wird von Cisco NX-OS 5.2(1) und höher unterstützt.
6. Die ACL-Erfassung ist nicht mit der ACL-Protokollierung kompatibel. Wenn Sie Zugriffskontrolllisten mit einem **log-**Schlüsselwort haben, funktionieren diese daher nicht, nachdem Sie die **Erfassung** der **Hardwarezugriffsliste** global eingegeben haben.
7. Aufgrund des Bugs CSCug20139 wird das Beispiel in diesem Dokument mit einer **Erfassungssitzung** pro ACE anstatt pro ACL dokumentiert, bis der Fehler behoben ist.

Zugehörige Informationen

- Cisco Nexus NX-OS Security Configuration Guide der Serie 7000, Version 6.x, Konfigurationsbeispiele für IP-Zugriffskontrolllisten
- Technischer Support und Dokumentation - Cisco Systems