Nexus 7000 TCAM-Bankeinschränkungen und Konfiguration der Bankkette

Inhalt

Einleitung

In diesem Dokument wird die Standardprogrammierung für die ACL-Funktionen (Access Control List-based) für die Ternary Content Addressable Memory (TCAM)-Banken des Nexus 7000 beschrieben. Außerdem wird erläutert, wie Ressourcen mithilfe der Funktion zur Verkettung von Banken zusammengefasst werden.

Problem

Bei der Erstimplementierung sind die ACL-Funktionen nicht über verschiedene TCAM-Banken hinweg programmiert. Dadurch werden die verfügbaren Einträge für jede Funktion auf 16.000 begrenzt. Für Kunden mit großen Zugriffskontrolllisten ist dies ein Problem. Die Verwendung der Bankenkettenfunktion löst dieses Problem, indem die Bankenbeschränkung aufgehoben wird. Wenn die Bankkette aktiviert ist, können bankübergreifende ACL-basierte Funktionen programmiert werden.

Beispiele für Fehlermeldungen:

```
ACLQOS-SLOT3-4-ACLQOS_OVER_THRESHOLD
Tcam 0 Bank 0's usage has reached its threshold

ACLMGR-3-ACLMGR_VERIFY_FAIL  Verify failed: client 8200016E,
Sufficient free entries are not available in TCAM bank
```

Lösung

- Wenn die Bankkette aktiviert ist, wirkt sich dies nur auf zukünftige Konfigurationen aus. Die aktuellen TCAM-Einträge werden nicht neu programmiert. Wenn eine neue ACL auf eine Schnittstelle angewendet wird, wird diese neue ACL über mehrere Banken hinweg

programmiert.

- Wenn die Bankkette aktiviert ist, wird die ACL über mehrere Banken hinweg programmiert (mit Ausnahme von Tunnel Decap und Control Plane Protection (CoPP)). (Siehe Abschnitt "Einschränkungen".) Wenn genügend Einträge in zwei TCAM Bank 0s vorhanden sind, wird die ACL aufgeteilt und in diese beiden Banken programmiert.
- Wenn die beiden TCAM Bank 0s nicht über genügend freie Einträge verfügen, wird die ACL-Regel für alle vier Banken programmiert.
- Wenn die Bankkettenfunktion aktiviert ist, wird sie auch dann über die beiden TCAM-Banknummern hinweg programmiert, wenn die ACL weniger Regeln als die freien Einträge einer einzigen Bank enthält.
- Wenn die Bankkette deaktiviert ist, werden die aktuellen TCAM-Einträge neu programmiert. Wenn die aktuelle ACL nicht in eine Bank passt, wird eine Fehlermeldung ausgegeben, und die Bankkette kann nicht deaktiviert werden.
- Während des In-Service-Software-Upgrades (ISSU) muss die Bankkette deaktiviert werden. Andernfalls schlägt das ISSU-Downgrade fehl.

Einschränkungen

- Wenn die Bankenkettenfunktion aktiviert ist, können die auf eine Schnittstelle und ein Verzeichnis angewendeten Richtlinien kombiniert werden. Eine der Richtlinien, für die Statistiken aktiviert sind, kann nicht zusammengeführt werden. Wenn die Bankkette aktiviert ist, kann die Funktion mit aktivierten Statistiken nicht gleichzeitig mit anderen Funktionen auf derselben Schnittstelle in derselben Richtung verwendet werden.

  Beispiel: Wenn in der RACL (Access Control List) des Eingangs-Routers an Ethernet2/1 Statistiken aktiviert sind, kann unter dieser Schnittstelle kein richtlinienbasiertes Routing (Policy Based Routing, PBR) konfiguriert werden.

- Zwei Richtlinien, deren Ergebnistypen unterschiedlich sind, können nicht zusammengeführt werden. Es gibt drei Ergebnistypen: ACL, Accounting und Quality of Service (QoS). Diese drei Ergebnistypen können nicht zusammengeführt werden. Funktionen unter dem ACL-Ergebnistyp: Port Access Control List (PACL), RACL, VLAN Access Control List (VACL), PBR, DHCP, Address Resolution Protocol (ARP), NetFlowFunktionen unter dem Ergebnistyp "Accounting": NetFlow einfachFunktionen unter dem QoS-Ergebnistyp: QoS
  Beispiel: RACL und QoS können unter einer Schnittstelle nicht gleichzeitig in derselben Richtung vorhanden sein, wenn die Bankkette aktiviert ist.

- Tunnel Decap und CoPP werden unter einer logischen Schnittstelle (Logical Interface, LIF) programmiert und können nicht zusammengeführt werden, da ihre Ergebnistypen unterschiedlich sind. Um die Beschränkung zu vermeiden, in der sie nicht gleichzeitig existieren können, werden sie in einer einzigen Bank aufbewahrt, selbst wenn die Bankenkette aktiviert ist. Wenn die rollenbasierte Zugriffskontrollliste (RBACL, Rollenbasierte Zugriffskontrollliste) aktiviert ist, wird der TCAM-Nachschlageschlüssel mithilfe der Tag-Nummer/Ziel-Sicherheitsgruppen-Tag-Nummer (SGT/DGT) erstellt. Die RBACL kann nicht mit anderen Ausgangsrichtlinien zusammengeführt werden, da die Bezeichnung so programmiert ist, dass sie statt der IPv4-Quellzieladressen SGT/DGT abruft. Wenn die Bankkette aktiviert ist, gelten die folgenden Regeln:

1. Wenn die RBACL unter Virtual Routing and Forwarding (VRF) aktiviert ist, können für diese Schnittstellen auf dieser VRF-Instanz keine anderen Ausgangs-Richtlinien konfiguriert werden.
2. Wenn die RBACL unter VLAN aktiviert ist, kann keine VLAN-Ausgangs-Richtlinie konfiguriert werden.

- Port + VLAN-Richtlinie: In der Hardware (HW) werden die Label für Port-Richtlinien und VLAN-Richtlinien unter einem Information Lifecycle Management (ILM)-Eintrag programmiert. Es kann nur ein Label für Port-Richtlinien und ein Label für VLAN-Richtlinien enthalten. Wenn die Bankkette aktiviert ist, können Port + VLAN-Richtlinien nicht unterstützt werden: Wenn eine Port-Richtlinie konfiguriert wird, kann keine Richtlinie unter dem VLAN/SVI konfiguriert werden, zu dem der Port gehört.Wenn eine VLAN/SVI-Richtlinie konfiguriert wird, kann für den zum VLAN gehörenden Port keine Richtlinie konfiguriert werden.

Beispiel einer Fehlermeldung:

```
ERROR: Resource-pooling is not supported with certain feature combinations
```

Konfiguration

config t

Ressourcen-Pooling für Hardwarezugriffslisten: Diese können nur über das Standard-VDC bereitgestellt werden.

Anzeigen von Hardware-Zugriffslisten-Ressourcen-Pooling

Anzeige des Status der internen Systemzugriffsliste

```
SITE1-AGG1(config)# hardware access-list resource pooling mod ?
<1-9>  Specify module number
SITE1-AGG1(config)# hardware access-list resource pooling mod 3
SITE1-AGG1(config)# show hardware access-list resource pooling
  Module 3 enabled
SITE1-AGG1# show system internal access-list status
Atomic ACL updates Enabled.
TCAM Default Result is Deny.
ACL Logging enabled.
Current LOU resource threshold: 5
```

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme