CoPP auf Nexus Switches der Serie 7000

Inhalt

Einführung

In diesem Dokument wird beschrieben, was, wie und warum Control Plane Policing (CoPP) auf den Nexus Switches der Serie 7000 verwendet wird, darunter die Module der Serien F1, F2, M1 und M2 sowie die Linecards (LCs). Es enthält außerdem Best Practice-Richtlinien sowie Informationen zum Anpassen einer CoPP-Richtlinie.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der CLI des Nexus-Betriebssystems zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Nexus Switches der Serie 7000 mit Supervisor 1-Modul.

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.

Übersicht über CoPP auf Switches der Serie Nexus 7000

Für den Netzwerkbetrieb ist CoPP von entscheidender Bedeutung. Ein DoS-Angriff (Denial of Service) auf die Kontroll- und Verwaltungsebene, der entweder versehentlich oder böswillig verübt werden kann, führt in der Regel zu hohen Datenverkehrsraten, die zu einer übermäßigen CPU-Auslastung führen. Das Supervisor-Modul verbringt unangemessene Zeit mit der Verarbeitung der Pakete.

Beispiele für solche Angriffe:

- ICMP-Echo-Anfragen (Internet Control Message Protocol).
- Pakete, die mit **IP-Optionen** gesendet werden

Dies kann Folgendes bewirken:

- Verlust von Keepalive-Nachrichten und Aktualisierungen des Routing-Protokolls.
- Füllen von Paketwarteschlangen, was zu wahllosen Drops führt.
- Langsame oder nicht reagierende interaktive Sitzungen.

Angriffe können die Netzwerkstabilität und -verfügbarkeit überfordern und zu geschäftsschädigenden Netzwerkausfällen führen.

CoPP ist eine hardwarebasierte Funktion, die den Supervisor vor DoS-Angriffen schützt. Sie kontrolliert die Geschwindigkeit, mit der Pakete den Supervisor erreichen können. Die CoPP-Funktion ist wie eine Eingangs-QoS-Richtlinie modelliert, die an die spezielle Schnittstelle mit der Bezeichnung **Kontrollebene** angeschlossen ist. CoPP ist jedoch eine Sicherheitsfunktion und nicht Teil von QoS. Zum Schutz des Supervisors trennt CoPP Datenebenenpakete von den Kontrollebenenpaketen (Ausnahmelogik). Identifiziert DoS-Angriffspakete aus gültigen Paketen (Klassifizierung). CoPP ermöglicht die Klassifizierung dieser Pakete:

- Empfangen von Paketen
- Multicast-Pakete
- Ausnahmepakete
- Umleiten von Paketen
- Broadcast-MAC + Nicht-IP-Pakete
- Broadcast-MAC- und IP-Pakete (siehe Cisco Bug ID CSCub47533 - Pakete im L2-VLAN (kein SVI), die CoPP erreichen)
- Multicast-MAC + IP-Pakete
- Router MAC + Nicht-IP-Pakete
- ARP-Pakete

Nach der Klassifizierung eines Pakets kann das Paket auch markiert und verwendet werden, um je nach Pakettyp unterschiedliche Prioritäten zuzuweisen. Aktionen anpassen, übertreffen und verletzen (Senden, Verwerfen, Markieren) können festgelegt werden. Wenn keine Richtlinie an eine Klasse angefügt ist, wird eine Standardrichtlinie hinzugefügt, deren konforme Aktion verworfen wird. Glean-Pakete werden mit der Standardklasse geregelt. Eine Durchsatzrate, zwei Farben und zwei Durchsatzraten, drei Farbrichtlinien werden unterstützt.

Datenverkehr, der auf die CPU des Supervisor-Moduls trifft, kann über vier Pfade erfolgen:

1. In-Band-Schnittstellen (Port an der Vorderseite) für Datenverkehr, der über Line Cards gesendet wird.

2. Management-Schnittstelle (mgmt0) für den Verwaltungsdatenverkehr.

3. Für die Konsole verwendete CMP-Schnittstelle (Control and Monitoring Processor).

4. Switched Ethernet Out Band Channel (EOBC) zur Steuerung der Line Cards vom Supervisor-Modul und zum Austausch von Statusmeldungen.

Nur der über die In-Band-Schnittstelle gesendete Datenverkehr unterliegt CoPP, da dies der einzige Datenverkehr ist, der das Supervisor-Modul über die Weiterleitungs-Engines (FEs) auf den Linecards erreicht. Die Implementierung von CoPP in den Nexus-Switches der Serie 7000 erfolgt ausschließlich hardwarebasiert, d. h. CoPP wird nicht in der Software vom Supervisor-Modul durchgeführt. CoPP-Funktionalität (Richtlinienvergabe) wird auf jeder FE unabhängig implementiert. Wenn die verschiedenen Raten für die CoPP-Richtlinienzuordnung konfiguriert sind, muss die Anzahl der Linecards im System berücksichtigt werden.

Der gesamte vom Supervisor empfangene Datenverkehr beträgt N-mal X, wobei N für die Anzahl der FEs auf dem Nexus 7000-System und X für die zulässige Rate für die jeweilige Klasse steht. Die konfigurierten Policer-Werte gelten pro FE, und der aggregierte Datenverkehr, der die CPU trifft, ist die Summe des konformen und übertragenen Datenverkehrs auf allen FEs. Mit anderen Worten, Datenverkehr, der die CPU trifft, entspricht der konfigurierten konformen Rate multipliziert mit der Anzahl der FEs.

- N7K-M148GT-11/L LC hat 1 FE
- N7K-M148GS-11/L LC hat 1 FE
- N7K-M132XP-12/L LC hat 1 FE
- N7K-M108X2-12L LC hat 2 FE
- N7K-F248XP-15 LC hat 12 FE (SOC)
- N7K-M235XP-23L LC hat 2 FE
- N7K-M206FQ-23L LC hat 2 FE
- N7K-M202CF-23L LC hat 2 FE

Die CoPP-Konfiguration wird nur im Standard Virtual Device Context (VDC) implementiert. Die CoPP-Richtlinien gelten jedoch für alle VDCs. Für alle Linecards wird dieselbe globale Richtlinie angewendet. CoPP wendet die gemeinsame Nutzung von Ressourcen zwischen VDCs an, wenn die Ports der gleichen FEs zu unterschiedlichen VDCs gehören (M1- oder M2-Serie LC). Beispielsweise zählen Ports eines FE, selbst in unterschiedlichen VDCs, für denselben Grenzwert für CoPP.

Wenn dieselbe FE von verschiedenen VDCs gemeinsam genutzt wird und eine bestimmte Klasse von Kontrollebenen-Datenverkehr den Schwellenwert überschreitet, betrifft dies alle VDCs im gleichen FE. Es wird empfohlen, pro VDC einen FE zu reservieren, um die CoPP-Durchsetzung,

wenn möglich, zu isolieren.

Beim ersten Einschalten des Switches muss die Standardrichtlinie zum Schutz der **Kontrollebene** programmiert werden. CoPP stellt die Standardrichtlinien bereit, die als Teil der anfänglichen Startsequenz auf die **Steuerungsebene** angewendet werden.

Warum CoPP auf dem Nexus Switch der Serie 7000?

Der Nexus Switch der Serie 7000 wird als Aggregations- oder Core-Switch bereitgestellt. Es ist also das Ohr und das Gehirn des Netzwerks. Er übernimmt die maximale Auslastung im Netzwerk. Sie muss häufige Anfragen und Burst-Anfragen bearbeiten. Einige Anfragen sind:

- **Verarbeitung der Spanning Tree Bridge Protocol Data Unit (BPDU)** - Die Standardeinstellung ist alle zwei Sekunden.
- **First-Hop-Redundanz** - Dazu gehören Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) und Gateway Load Balancing Protocol (GLBP). Die Standardeinstellung ist alle drei Sekunden.
- **Adressenauflösung** - Dazu gehört Address Resolution Protocol/Neighbor-Discovery (ARP/ND), Forwarding Information Base (FIB)-GRENZE - Bis zu eine Anforderung pro Sekunde, pro Host, z. B. NIC-Teaming (Network Interface Controller).
- **Dynamic Host Control Protocol (DHCP)** - DHCP-Anfrage, Relay - Bis zu eine Anforderung pro Sekunde, pro Host.
- **Routing-Protokolle** für Layer 3 (L3).
- **Data Center Interconnect** - Overlay Transport Virtualization (OTV), Multiprotocol Label Switching (MPLS) und Virtual Private LAN Service (VPLS).

CoPP ist unerlässlich, um die CPU vor falsch konfigurierten Servern oder potenziellen DoS-Angriffen zu schützen, wodurch die CPU über ausreichend Zyklus verfügt, um kritische Nachrichten auf Kontrollebene zu verarbeiten.

Verarbeitung der Kontrollebene auf dem Nexus Switch der Serie 7000

Der Nexus Switch der Serie 7000 verfolgt einen verteilten Steuerungsebenenansatz. Er verfügt über einen Multicore auf jedem E/A-Modul sowie eine Multicore-Schnittstelle für die Switch-Kontrollebene im Supervisor-Modul. Es lagert intensive Aufgaben für die Zugriffskontrolllisten (ACL) und die FIB-Programmierung an die E/A-Modul-CPU aus. Es skaliert die Kontrollebenenkapazität mit der Anzahl der Linecards. Dadurch wird ein Engpass bei der Supervisor-CPU vermieden, der bei einem zentralisierten Ansatz zu beobachten ist. Hardware-Ratenlimitierungen und hardwarebasiertes CoPP schützen die Kontrollebene vor schädlichen oder schädlichen Aktivitäten.

CoPP Best Practices-Richtlinie

Die CoPP Best Practices Policy (BPP) wurde in Version 5.2 von Cisco NX-OS eingeführt. Die Ausgabe des Befehls **show running-config** zeigt den Inhalt des CoPP-BPP nicht an. Der Befehl **show run all** (Alle anzeigen) zeigt den Inhalt von CoPP BPP an.

```
-----------------------------------SNIP----------------------------------------
SITE1-AGG1# show run copp

!! Command: show running-config copp
!! Time: Mon Nov 5 22:21:04 2012

version 5.2(7)
copp profile strict


SITE1-AGG1# show run copp all

!! Command: show running-config copp all
!! Time: Mon Nov 5 22:21:15 2012

version 5.2(7)
------------------------------SNIP--------------------
control-plane
service-policy input copp-system-p-policy-strict
copp profile strict
```

CoPP bietet dem Benutzer vier Optionen für Standardrichtlinien:

- Strict
- Mittel
- leuchtend
- Dense (eingeführt in Version 6.0(1))

Wenn keine Option ausgewählt oder die Einrichtung übersprungen wird, wird eine strikte Richtlinienvergabe angewendet. Alle diese Optionen verwenden dieselben Klassenzuordnungen und Klassen, aber unterschiedliche Committed Information Rate (CIR)- und Burst Count (BC)-Werte für die Richtlinienvergabe. In Cisco NX-OS-Versionen vor 5.2.1 wurde der Befehl **setup** verwendet, um die Option zu ändern. In Cisco NX-OS 5.2.1 wurde das CoPP BPP um eine Erweiterung erweitert, sodass die Option ohne den Befehl **setup** geändert werden kann. Verwenden Sie den Befehl **copp profile**.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# copp profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

Verwenden Sie den Befehl **show copp profile <profile-type>**, um die standardmäßige CoPP-BPP-Konfiguration anzuzeigen. Verwenden Sie den Befehl **show copp status**, um zu überprüfen, ob die CoPP-Richtlinie korrekt angewendet wurde.

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

Um den Unterschied zwischen zwei CoPP-BPPs anzuzeigen, verwenden Sie den Befehl **show copp diff profile <profile-type 1> profile <profile-type 2>:**

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
a '-' represents a line that has been removed.
-policy-map type control-plane copp-system-p-policy-strict
- class copp-system-p-class-critical
- set cos 7
- police cir 39600 kbps bc 250 ms conform transmit violate drop
- class copp-system-p-class-important
- set cos 6
- police cir 1060 kbps bc 1000 ms conform transmit violate drop
----------------------SNIP----------------------------------------
+policy-map type control-plane copp-system-p-policy-moderate
+ class copp-system-p-class-critical
+ set cos 7
+ police cir 39600 kbps bc 310 ms conform transmit violate drop
+ class copp-system-p-class-important
+ set cos 6
+ police cir 1060 kbps bc 1250 ms conform transmit violate drop
----------------------SNIP----------------------------------------
```

Anpassen einer CoPP-Richtlinie

Benutzer können eine benutzerdefinierte CoPP-Richtlinie erstellen. Klonen Sie das standardmäßige CoPP-BPP, und fügen Sie es an die **Kontrollebenen-**Schnittstelle an, da das CoPP-BPP schreibgeschützt ist.

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
^
% String is invalid, 'copp-system-p-policy-strict' is not an allowed string at
'^' marker.
```

Der Befehl **copp copy profile <profile-type> <prefix> [suffix]** erstellt einen Klon des CoPP BPP. Dies wird verwendet, um die Standardkonfigurationen zu ändern. Der Befehl **copp copy profile** ist ein Befehl **exec mode**. Benutzer können ein Präfix oder Suffix für die Zugriffsliste, Klassenzuordnungen und den Namen der Richtlinienzuordnung auswählen. Beispielsweise wird **copp-system-p-policy-strict in [prefix]copp-policy-strict[suffix]** geändert. Klonte Konfigurationen werden als Benutzerkonfigurationen behandelt und in der **Ausgabe "show run"** enthalten.

```
SITE1-AGG1# copp copy profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
prefix Prefix for the copied policy
suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
```

```
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

Mit den folgenden Befehlen können Sie Datenverkehr, der eine angegebene Permitted Information Rate (PIR) überschreitet und gegen diese verstößt, markieren:

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms ?
<CR>
conform Specify a conform action
pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir ?
<1-80000000000> Peak Information Rate in bps/kbps/mbps/gbps

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps ?
<CR>
<1-512000000> Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us
be Specify extended burst
conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform ?
drop Drop the packet
set-cos-transmit Set conform action cos val
set-dscp-transmit Set conform action dscp val
set-prec-transmit Set conform action precedence val
transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
SITE1-AGG1(config-pmap-c)#
```

Wenden Sie die angepasste CoPP-Richtlinie auf die **Kontrollebene** der globalen Schnittstelle an. Verwenden Sie den Befehl **show copp status**, um zu überprüfen, ob die CoPP-Richtlinie korrekt angewendet wurde.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

Anwenderbericht zu angepassten CoPP-Richtlinien

In diesem Abschnitt wird ein echtes Beispiel beschrieben, in dem der Kunde mehrere Überwachungsgeräte benötigt, um die lokalen Schnittstellen häufig pingen zu können. Probleme treten in diesem Szenario auf, wenn der Kunde die CoPP-Richtlinie ändern möchte, um Folgendes zu erreichen:

- Erhöhen Sie die CIR, sodass diese spezifischen Adressen das lokale Gerät pingen können und nicht gegen die Richtlinie verstoßen.

- Lassen Sie zu, dass die anderen IP-Adressen die Fähigkeit beibehalten, das lokale Gerät zu pingen, jedoch mit einer niedrigeren CIR für Fehlerbehebungszwecke.

Die Projektmappe wird im nächsten Beispiel veranschaulicht, nämlich eine benutzerdefinierte Richtlinie mit einer separaten Klassenzuordnung zu erstellen. Die separate Klassenzuordnung enthält die angegebenen IP-Adressen der Überwachungsgeräte, und die Klassenzuordnung verfügt über eine höhere CIR. Dadurch wird auch die ursprüngliche *Überwachung der* Klassenzuordnung beibehalten, die den ICMP-Datenverkehr für alle anderen IP-Adressen in einer niedrigeren CIR erfasst.

```
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
F340.13.19-Nexus7000-1(config)# copp copy profile strict prefix TAC_CHANGE
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# ip access-list TAC_CHANGE-copp-acl-specific-icmp
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo-reply
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# exit
F340.13.19-Nexus7000-1(config)# sho ip access-lists TAC_CHANGE-copp-acl-specific-
icmp IP access list TAC_CHANGE-copp-acl-specific-icmp
10 permit icmp 1.1.1.1/32 2.2.2.2/32 echo
20 permit icmp 1.1.1.1/32 2.2.2.2/32 echo-reply
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# class-map type control-plane match-any
TAC_CHANGE-copp-class-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)# match access-group name TAC_CHANGE-copp
-acl-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)#exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#policy-map type control-plane TAC_CHANGE-copp-
policy-strict
F340.13.19-Nexus7000-1(config-pmap)# class TAC_CHANGE-copp-class-specific-icmp
insert-before
TAC_CHANGE-copp-class-monitoring
F340.13.19-Nexus7000-1(config-pmap-c)# set cos 7
F340.13.19-Nexus7000-1(config-pmap-c)# police cir 5000 kbps bc 250 ms conform transmit
violate drop
F340.13.19-Nexus7000-1(config-pmap-c)# exit
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)# exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# control-plane
F340.13.19-Nexus7000-1(config-cp)# service-policy input TAC_CHANGE-copp-policy-strict
F340.13.19-Nexus7000-1(config-cp)# end
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# sho policy-map interface control-plane
Control Plane
```

```
service-policy input TAC_CHANGE-copp-policy-strict
<abbreviated output>
class-map TAC_CHANGE-copp-class-specific-icmp (match-any)
match access-group name TAC_CHANGE-copp-acl-specific-icmp
set cos 7
police cir 5000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/secclass-map TAC_CHANGE-copp-class-monitoring (match-any)
match access-group name TAC_CHANGE-copp-acl-icmp
match access-group name TAC_CHANGE-copp-acl-icmp6
match access-group name TAC_CHANGE-copp-acl-mpls-oam
match access-group name TAC_CHANGE-copp-acl-traceroute
match access-group name TAC_CHANGE-copp-acl-http-response
match access-group name TAC_CHANGE-copp-acl-smtp-response
match access-group name TAC_CHANGE-copp-acl-http6-response
match access-group name TAC_CHANGE-copp-acl-smtp6-response
set cos 1
police cir 130 kbps bc 1000 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
<abbreviated output>
```

CoPP-Datenstruktur

Die CoPP-BPP-Datenstruktur wird wie folgt aufgebaut:

- **ACL-Konfiguration**: IP-ACL und MAC-ACL.
- **Klassifizierungskonfiguration**: Klassenzuordnung mit IP-ACL oder MAC-ACL.
- **Policer-Konfiguration**: Festlegen von CIR, BC, konform und verletzende Maßnahmen Die Policer hat zwei Raten (CIR und BC) und zwei Farben (konform und verletzen).

```
mac access-list copp-system-p-acl-mac-fabricpath-isis
permit any 0180.c200.0015 0000.0000.0000
permit any 0180.c200.0014 0000.0000.0000

ip access-list copp-system-p-acl-bgp
permit tcp any gt 1024 any eq bgp
permit tcp any eq bgp any gt 1024

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-pim
<snip>
match access-group name copp-system-p-acl-mac-fabricpath-isis
policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-critical
set cos 7
police cir 5000 kbps bc 250 ms conform transmit violate drop
```

CoPP-Skalierungsfaktor

Die in Cisco NX-OS 6.0 eingeführte Skalierungsfaktorkonfiguration dient zur Skalierung der Überwachungsrate der angewendeten CoPP-Richtlinie für eine bestimmte Linecard. Dadurch wird die Policer-Rate für eine bestimmte Linecard erhöht oder verringert, die aktuelle CoPP-Richtlinie wird jedoch nicht geändert. Die Änderungen sind sofort wirksam, und eine erneute Anwendung der CoPP-Richtlinie ist nicht erforderlich.

```
scale factor option configured within control-plane interface:
Scale-factor <scale factor value> module <module number>
<scale factor value>: from 0.10 to 2.00
Scale factor is recommended when a chassis is loaded with both F2 and M
Series modules.
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# scale-factor ?
<whole>.<decimal> Specify scale factor value from 0.10 to 2.00

SITE1-AGG1(config-cp)# scale-factor 1.0 ?
module Module

SITE1-AGG1(config-cp)# scale-factor 1.0 module ?
<1-10> Specify module number

SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
Linecard Configuration:
-----------------------
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
```

```
Module 10: 1.00
```

CoPP-Überwachung und -Verwaltung

Mit Cisco NX-OS 5.1 kann pro CoPP-Klassenname ein Drop-Grenzwert konfiguriert werden, der bei Überschreitung des Schwellenwerts eine Syslog-Meldung auslöst. Der Befehl **protokolliert den Drop-Schwellwert <Anzahl verworfener Bytes> auf der Ebene <Protokollierungsebene>**.

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

Hier sehen Sie ein Beispiel für eine Syslog-Meldung:

```
%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class:
copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CoPP-Zähler

CoPP unterstützt dieselben QoS-Statistiken wie jede andere Schnittstelle. Es zeigt die Statistiken der Klassen, die die Service-Richtlinie für jedes E/A-Modul bilden, das CoPP unterstützt. Verwenden Sie den Befehl **show policy-map interface control-plane**, um die Statistiken für CoPP anzuzeigen.

> **Hinweis**: Alle Klassen sollten hinsichtlich verletzter Pakete überwacht werden.

```
SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
```

```
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms
module 1 :
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop

module 2 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop

module 3 :
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop

module 4 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

Um eine aggregierte Ansicht konformer und verletzter Zähler für alle Class-Map- und E/A-Module zu erhalten, verwenden Sie die **Steuerungsebene show policy-map interface | i** Befehl **"class|conform|violated"**.

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

Die **Klasse copp-class-l2-default und die Klasse-default** sollten überwacht werden, um sicherzustellen, dass selbst bei konformen Zählern keine hohen Erhöhungen auftreten.

Idealerweise müssen diese beiden Klassen niedrige Werte für konformierten Zähler und mindestens keine verletzte Zählererhöhung aufweisen.

ACL-Zähler

Der Befehl **statistics per entry** wird für die in der CoPP-Klassenzuordnung verwendete IP-ACL oder MAC-ACL nicht unterstützt. Bei Anwendung auf CoPP-IP-ACL oder MAC-ACL hat er keine Auswirkungen. (Es wird keine CLI-Überprüfung durch den CLI Parser durchgeführt.) Um die MAC-ACL- oder IP-ACL-Treffer von CoPP auf einem E/A-Modul anzuzeigen, verwenden Sie den Befehl **show system internal access-list input detail**.

Hier ein Beispiel:

```
!! 0180.c200.0041 is the destination MAC used for FabricPath IS-IS

SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

Best Practices für die CoPP-Konfiguration

Hier einige Best Practice-Empfehlungen für die CoPP-Konfiguration:

- Verwenden Sie standardmäßig den strikten CoPP-Modus.
- Ein dichtes CoPP-Profil wird empfohlen, wenn das Chassis vollständig mit Modulen der F2-Serie ausgestattet ist oder mehr Module der F2-Serie als andere E/A-Module enthält.
- Es wird nicht empfohlen, CoPP zu deaktivieren. Passen Sie die CoPP-Standardeinstellung

nach Bedarf an.

- Überwachung unbeabsichtigter Datenverluste und Hinzufügen oder Ändern der CoPP-Standardrichtlinie entsprechend dem erwarteten Datenverkehr
- Je nach Anzahl der FEs im Chassis können die CIR- und BC-Einstellungen für CoPP erhöht oder reduziert werden. Dies hängt auch von der Rolle der Geräte im Netzwerk, den ausgeführten Protokollen usw. ab.
- Da sich die Datenverkehrsmuster in einem **Rechenzentrum** ständig ändern, ist die Anpassung einer CoPP ein konstanter Prozess.
- CoPP und VDC: Alle Ports desselben FE müssen demselben VDC angehören, was für einen LC der F2-Serie einfach ist, für eine M2- oder M108 LC jedoch nicht so einfach. Dies liegt daran, dass die gemeinsame Nutzung von CoPP-Ressourcen zwischen VDCs erfolgt, wenn die Ports desselben FE verschiedenen VDCs angehören (M1-Serie oder LC der M2-Serie). Die Ports eines FEs, selbst in verschiedenen VDCs, werden für dieselbe CoPP-Schwelle berechnet.
- Die Konfiguration des Skalierungsfaktors wird empfohlen, wenn ein Chassis mit Modulen der F2- und der M-Serie geladen wird.

Best Practices für die CoPP-Überwachung

Hier einige Best Practice-Empfehlungen für die CoPP-Überwachung:

- Konfigurieren Sie einen Syslog-Meldungsgrenzwert für CoPP (Cisco NX-OS Release 5.1), um die durch CoPP erzwungenen Datenverluste zu überwachen.
- Syslog-Meldungen werden generiert, wenn Verwerfen innerhalb einer Verkehrsklasse den benutzerdefinierten Grenzwert überschreitet.
- Der Protokollierungsschwellenwert und die Protokollierungsebene können innerhalb jeder Verkehrsklasse mithilfe des **Protokollierungsabfallschwellenwerts <Paketanzahl> auf der Ebene <Ebene>** angepasst werden.
- Da die Option "statistics per entry" für CoPP MAC ACL oder IP ACL nicht unterstützt wird, verwenden Sie den Befehl **show system internal access-list input** command, um Zugriffskontrolleinträge (ACE)-Treffer zu überwachen.
- Der Befehl **class copp-class-l2-default und class-default** sollte überwacht werden, um sicherzustellen, dass selbst bei konformen Zählern keine hohen Erhöhungen auftreten.
- Alle Klassen sollten hinsichtlich verletzter Pakete überwacht werden.
- Da **copp-klassenkritisch** sehr wichtig ist, aber eine **verletzende** Richtlinie hat, empfiehlt es sich, die Geschwindigkeit konformer Pakete zu überwachen, um frühzeitig einen Hinweis zu

erhalten, wenn die Klasse in der Nähe des Zeitpunkts beginnt, an dem sie die Verletzung auslöst. Wenn der verletzte Zähler für diese Klasse zunimmt, bedeutet dies nicht unbedingt eine rote Warnung. Vielmehr bedeutet dies, dass diese Situation kurzfristig untersucht werden muss.

- Verwenden Sie den Befehl **copp profile strict** nach jeder Codeaktualisierung für Cisco NX-OS oder zumindest nach jeder größeren Codeaktualisierung für Cisco NX-OS. Wenn eine CoPP-Änderung zuvor abgeschlossen wurde, muss sie erneut angewendet werden.

Schlussfolgerungen

- CoPP ist eine hardwarebasierte Funktion, die den Supervisor vor DoS-Angriffen schützt.
- LCs der Serien M1, F2 und M2 unterstützen CoPP. LCs der F1-Serie unterstützen CoPP nicht.
- Die CoPP-Konfiguration ähnelt MQC (Modular QoS CLI).
- Die CoPP-Konfiguration und -Überwachung wird nur in einem Standard-VDC durchgeführt.
- CoPP-Standardoptionen können mit strikten, moderaten, leichen und dichten Optionen verwendet werden.
- Kopieren von CoPP BPP in benutzerdefinierte CoPP-Regeln, um bestimmte Netzwerkanforderungen zu erfüllen
- CoPP-Zähler (konform und verletzt in Byte pro Klassenzuordnung) werden mit dem Befehl **show policy-map interface control-plane** angezeigt.
- Der von der CPU des Supervisor-Moduls empfangene Datenverkehr entspricht der Gesamtzahl der FEs, die dem zulässigen Durchsatz entspricht.
- Versuchen Sie, gemeinsame Ports eines FEs über verschiedene VDCs zu vermeiden.
- Befolgen Sie die Best Practices von CoPP, um die Funktionen erfolgreich zu implementieren und zu überwachen.

Nicht unterstützte Funktionen

Diese Funktionen werden nicht unterstützt:

- Verteilte Aggregation Policing.
- Microflow Policing.
- Überwachung von Ausgangsausnahmen.

- CoPP-Unterstützung für BPDU über einen dot1q-Tunnel-Port (QinQ): Cisco Discovery Protocol (CDP), DOT1x, Spanning Tree Protocol (STP) und VLAN Trunk Protocol (VTP).