Konfigurationsbeispiel für Catalyst 6500/Sup2T und Catalyst 6880: Standardrichtlinie für die Kontrollebene

Inhalt

Einführung

In diesem Dokument wird detailliert beschrieben, welche Datenverkehrstypen mit Standard-Klassenzuordnungen abgeglichen werden, die Teil der automatisch auf dem Gerät konfigurierten Catalyst 6500 Sup2T/Catalyst 6880 CoPP-Standardkonfiguration (Control Plane Policing) sind. Dies wird konfiguriert, um die CPU vor Überlastung zu schützen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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.

Konfigurieren

CoPP ist auf Catalyst 6500/SUP2T- und Catalyst 6880-Switches standardmäßig aktiviert und basiert auf einer vorkonfigurierten Vorlage. Einige Klassenzuordnungs-Konfigurationen verfügen nicht über entsprechende Übereinstimmungsanweisungen, da sie Datenverkehr nicht in der MAC/IP Access Control List (ACL) erfassen, sondern über interne Ausnahmen, die von der Weiterleitungs-Engine signalisiert werden, wenn der Datenverkehr vom Switch empfangen wird und eine Weiterleitungsentscheidung getroffen wird.

Wenn eine bestimmte Klassenzuordnung aus der aktuellen CoPP-Richtlinie hinzugefügt, geändert oder entfernt werden muss, muss sie im Richtlinienzuweisungsmodus aus dem Konfigurationsmodus ausgeführt werden. Die genaue Syntax finden Sie im Catalyst 6500 Release 15.0SY Software Configuration Guide - Control Plane Policing (CoPP).

CoPP-Standardausnahmeklassen haben folgende Beschreibungen:

Fall	Klassenzuordnungsname	Beschreibung
Maximum Transmission Unit (MTU)-Ausfall	class-copp-mtu-fail	Die Paketgröße überschreitet die MTU-Größe der Ausgangsschnittstelle. Wenn das Bit Nicht fragmentieren nicht festgelegt ist, ist Fragmentierung erforderlich. Wenn das Don't Fragment-Bit festgelegt ist, zeigt die Meldung "Destination Unreachable" (ICMP), dass "fragmentation needed and DF set" generiert und an die Quelle zurückgesendet werden soll. Referenz: RFC-791, RFC-1191
TTL-Fehler (Time To Live)	class-copp-ttl-fail	Paket-TTL = 1 (für IPv4), Hop-Limit = 0 oder 1 (für IPv6) TTL = 0 (für IPv4) kann sofort in der Hardware verworfen werden, da der vorherige Hop das Paket zerstören soll, wenn TTL auf 0 reduziert wird. Der Hop Limit = 0 (für IPv6) unterscheidet sich von TTL = 0, da in RFC-2460, Abschnitt 8.2, angegeben wird, dass "Im Gegensatz zu IPv4 sind IPv6-Knoten nicht erforderlich, um die maximale Paketlebensdauer durchzusetzen. Aus diesem Grund wurde das Feld "IPv4 Time to Live" in "Hop Limit in IPv6" umbenannt. Das bedeutet, dass eingehendes IPv6-Paket mit Hop Limit = 0 noch gültig ist

		und die ICMP-Nachricht zurückgesendet werden sollte. Referenz: RFC-791, RFC-2460
Optionen	Klassenkopp-Optionen	Paket mit Optionen (für IPv4), Hop-by-Hop-Extension-Header (für IPv6). Beispiel: Router Alert RFC-2113, Strict Source Route usw. Extension-Header werden von keinem Knoten entlang des Delivery-Pfades eines Pakets geprüft oder verarbeitet, bis das Paket den Knoten (oder im Fall von Multicast jeder Satz von Knoten) erreicht, der im Feld Destination Address (Zieladresse) des IPv6-Headers angegeben ist. Die einzige Ausnahme ist der Header "Hop-by-Hop Options" (Hop-by-Hop-Optionen), der Informationen enthält, die von jedem Knoten entlang des Bereitstellungspfads eines Pakets geprüft und verarbeitet werden müssen, einschließlich der Quell- und Zielknoten. Die Hardwareverarbeitung in Optionsfeldern wird nicht unterstützt, d. h. die Softwareverarbeitung bzw. das Switching ist erforderlich. Referenz: RFC-791/RFC-2460
Reverse Path Forwarding (RPF)-Ausfall (Unicast)	class-copp-ucast-rpf-fail	Die RPF-Paketprüfung, die fehlschlägt, wird gefiltert. Aufgrund begrenzter Ressourcen in der Hardware kann die RPF-Prüfung jedoch in bestimmten Fällen nicht in der Hardware durchgeführt werden (d. h., mehr als 16 RPF-Schnittstellen, die mit einer IP verbunden sind). In diesem Fall wird das Paket zur vollständigen RPF-Prüfung an die Software gesendet. Das erste ausgefallene RPF-Datenpaket (das an eine Multicast-Gruppe adressiert ist) wird an die Software gesendet, damit der PIM-Assertierungsprozess (Protocol

		Independent Multicast) gestartet werden kann. Nach Abschluss des Vorgangs wird ein designierter Router/Forwarder ausgewählt. Wenn das nächste Paket (derselbe Fluss) nicht vom designierten Router stammt, löst es einen RPF-Ausfall aus, und die Hardware kann es sofort ablegen (um einen DoS-Angriff (Denial of Service) zu verhindern).
RPF-Fehler (Multicast)	class-copp-mcast-rpf-fail	Das erste ausgefallene RPF-Datenpaket (das an eine Multicast-Gruppe adressiert ist) wird an die Software gesendet, damit der PIM-Assert-Prozess gestartet werden kann. Nach Abschluss des Vorgangs wird ein designierter Router/Forwarder ausgewählt. Wenn das nächste Paket (derselbe Fluss) nicht vom designierten Router stammt, löst es einen RPF-Ausfall aus, und die Hardware kann es sofort ablegen (um einen DoS-Angriff zu verhindern). Wenn die Routing-Tabelle jedoch aktualisiert wird, muss ggf. ein neuer designierter Router (über PIM-assert) ausgewählt werden, d. h. das ausgefallene RPF-Paket muss die Software erreichen (damit PIM-assert erneut gestartet werden kann). Dazu steht in der Hardware ein periodisches Leck zum Softwaremechanismus (pro Datenstrom) für RPF-fehlgeschlagene Pakete zur Verfügung. Beachten Sie jedoch, dass ein periodisches Leck, wenn es eine große Menge an Flüssen gibt, für die Software zu viel sein kann, um es zu verarbeiten. Das Hardware-CoPP ist weiterhin für ein ausgefallenes Multicast-RPF-Paket erforderlich. Referenz: RFC-3704, RFC-2362
Hardware-Paketumschreibung wird nicht unterstützt	class-copp-unsupp-rewrite	Während Hardware in verschiedenen Fällen Pakete

		umschreiben kann, ist es in einigen Fällen im aktuellen Hardwaredesign nicht möglich. Für diese sendet die Hardware das Paket an die Software.
ICMP keine Route ICMP ACL-Drop ICMP-Umleitung	class-copp-icmp-redirect-unreachable	Pakete, die zur Generierung von ICMP-Nachrichten an die Software gesendet werden. Beispielsweise ICMP-Umleitung, ICMP-Ziel nicht erreichbar (z. B. Host nicht erreichbar oder administrativ untersagt). Referenz: RFC-792/RFC-2463
Cisco Express Forwarding (CEF) Receive (Ziel-IP ist die IP-Adresse des Routers)	class-copp-empfänger	Wenn die Ziel-IP-Adresse des Pakets eine der IP-Adressen des Routers ist (die CEF ReceiAdjacency (CEF-Empfangsadjazenz) aufruft, sollte die Software den Inhalt verarbeiten.
CEF Glean (Ziel-IP gehört zu einem Netzwerk des Routers)	Klasse-Kopp-Glean	Wenn die Ziel-IP-Adresse des Pakets zu einem Netzwerk des Routers gehört, dieses jedoch nicht aufgelöst wird (d. h. kein Treffer in der FIB-Tabelle (Forwarding Information Base)), wird CEF Glean Adjacency aufgerufen, die an Software gesendet wird, in der das Auflösungsverfahren gestartet wird. Bei IPv4 wird der gleiche Datenfluss weiterhin auf CEF Glean gedrückt, bis die Adresse aufgelöst ist. Bei IPv6 wird während der Auflösung ein temporärer FIB-Eintrag installiert, der mit der Ziel-IP-Adresse übereinstimmt (und stattdessen auf die Drop-Adjacency verweist). Wenn sie nicht innerhalb der angegebenen Dauer aufgelöst werden kann, wird der FIB-Eintrag entfernt (d. h. der gleiche Fluss beginnt erneut mit CEF Glean).
Paket für Multicast IP 224.0.0.0/4	class-copp-mcast-ip-control	Das Steuerungspaket muss von der Software verarbeitet werden.
Paket für Multicast IP FF:/8	class-copp-mcast-ipv6-control	Das Steuerungspaket muss von der Software verarbeitet werden.
Multicast-Paket, das in die Software kopiert werden muss	class-copp-mcast copy	In einigen Fällen muss das Multicast-Paket zur

		Statusaktualisierung in die Software kopiert werden (das Paket ist noch im selben VLAN Hardware-Bridge). Beispielsweise wird bei einem dichten Modus-Eintrag (*,G/m) ein Dual-RPF-SPT-Switchover ausgelöst.
Multicast-Paket verpasst FIB-Tabelle	class-copp-mcast-punt	Die Ziel-IP (Multicast-IP) ist in der FIB-Tabelle eine Fehlfunktion. Das Paket wird auf die Software beschränkt.
Direkt verbundene Quelle (IPv4)	class-copp-ip verbunden	Multicast-Datenverkehr von direkt verbundenen Quellen wird an die Software gesendet, in der ein Multicast-Status erstellt (und in der Hardware installiert) werden kann.
Direkt verbundene Quelle (IPv6)	class-copp-ipv6-connected	Multicast-Datenverkehr von direkt verbundenen Quellen wird an die Software gesendet, in der ein Multicast-Status erstellt (und in der Hardware installiert) werden kann.
Broadcast-Paket	Klassenfernübertragung	Broadcast-Pakete (z. B. IP/Non-IP mit Broadcast DMAC und IP-Unicast mit Multicast DMAC) werden an die Software übertragen.
Protokoll unbekannt (d. h. nicht unterstützt von) im Hinblick auf Hardware-Switching	class-copp-known-protocol	Nicht-IP-Protokoll, wie Internetwork Packet Exchange (IPX) usw., wird nicht hardwarevermittelt. Sie werden an die Software gesendet und dort weitergeleitet.
Multicast-Datenverkehr kommt über gerouteten Port ein, an dem PIM deaktiviert ist.	class-copp-mcast-v4-data-on-routedPort	Multicast-Datenverkehr, der über einen gerouteten Port eingeht (bei dem PIM deaktiviert ist), wird an die Software weitergeleitet. Es ist jedoch nicht notwendig, sie an die Software zu senden, damit sie fallen gelassen werden.
Multicast-Datenverkehr kommt über gerouteten Port ein, an dem PIM deaktiviert ist.	class-copp-mcast-v6-data-on-routedPort	Multicast-Datenverkehr, der über einen gerouteten Port eingeht (bei dem PIM deaktiviert ist), wird an die Software übertragen. Es ist jedoch nicht notwendig, sie an die Software zu senden, damit sie fallen gelassen werden.
Umleitung der Eingangs-ACL zur Bridge des Pakets	class-copp-ucast-ingress-acl-bridge	Die Hardware verfügt über 8 Ausnahmen im Zusammenhang

		mit Zugriffskontrolllisten, die von der Software über eine ACL-Umleitung festgelegt werden. Dieser bezieht sich auf Unicast-Pakete, die aus Gründen, die sich auf den Ternary Content Addressable Memory (TCAM) beziehen, von der ACL an die CPU überbrückt werden.
Ausgangs-ACL-Umleitung zur Paketüberbrückung	class-copp-ucast-ausgang-acl-bridge	Die Hardware verfügt über 8 Ausnahmen im Zusammenhang mit Zugriffskontrolllisten, die von der Software über eine ACL-Umleitung festgelegt werden. Dieser bezieht sich auf Unicast-Pakete, die aus Gründen, die sich auf den Ternary Content Addressable Memory (TCAM) beziehen, von der ACL an die CPU überbrückt werden.
Multicast-ACL wird umgeleitet, um Pakete an CPU zu Bridge zu übertragen	class-copp-mcast-acl-bridge	Die Hardware verfügt über 8 Ausnahmen im Zusammenhang mit Zugriffskontrolllisten, die von der Software über eine ACL-Umleitung festgelegt werden. Diese betrifft die Multicast-Verarbeitung.
ACL-Bridge zur CPU für die Verarbeitung des Server-Lastenausgleichs	class-copp-slb	Die Hardware verfügt über 8 Ausnahmen im Zusammenhang mit Zugriffskontrolllisten, die von der Software über eine ACL-Umleitung festgelegt werden. Diese bezieht sich auf eine Hardware-Umleitung für eine Server Load Balancing (SLB)-Entscheidung.
ACL VACL Protokollumleitung	class-copp-vacl-log	Die Hardware verfügt über 8 Ausnahmen im Zusammenhang mit Zugriffskontrolllisten, die von der Software über eine ACL-Umleitung festgelegt werden. Dieser bezieht sich auf die Paketweiterleitung durch VLAN Access Control List (VACL) ACL an CPU für Cisco IOS? Protokollierungszwecke.
DHCP-Snooping	class-copp-dhcp-snooping	DHCP-Snooped-Pakete werden zur DHCP-Verarbeitung an die CPU umgeleitet
MAC Policy Based Forwarding	class-copp-mac-pbf	Die richtlinienbasierte Weiterleitung ist in der CPU durchzuführen, da die Hardware in diesem Fall keine Pakete

		weiterleiten kann.
IP-Zugangskontrolle für das Netzwerk	class-copp-ip-entry	Um den Netzwerkzugriff basierend auf den Antivirus-Anmeldeinformationen des Hosts bereitzustellen, wird eine Statusüberprüfung über eine der folgenden Optionen durchgeführt: (1) Die L2-Schnittstelle verwendet LAN-Port-IP (LPIP), bei dem ARP-Pakete (Address Resolution Protocol) an die CPU umgeleitet werden (2) Die L3-Schnittstelle verwendet Gateway-IP (GWIP). Nach der Validierung erfolgt die Authentifizierung (*). Für eine L2-Schnittstelle ist dies WebAuth, der HTTP-Paketabfangen durchführt und möglicherweise auch URL-Umleitung (*) durchführt. Für die L3-Schnittstelle ist dies AuthProxy.
Dynamische ARP-Inspektion	class-copp-arp-snooping	Um einen ARP-Poisoning-Angriff (Man-in-the-Middle-Angriff) zu verhindern, validiert eine dynamische ARP-Inspektion (auch bekannt als Dynamic ARP Inspection (DAI)) die ARP-Anfragen/-Antworten, bis sie abgefangen und anschließend in der CPU für eine der folgenden Aufgaben verarbeitet werden: (1) benutzerdefinierte ARP-ACLs (für statisch konfigurierte Hosts), (2) MAC-Adresse für IP-Adressen-Bindings, die in vertrauenswürdiger Datenbank gespeichert sind (d. h. DHCP-Bindings). Nur gültige ARP-Pakete werden zur Aktualisierung des lokalen ARP-Cache oder zur Weiterleitung an den Empfänger verwendet. Der Validierungsprozess erfordert eine CPU-Beteiligung von ARP-Paketen, d. h. Hardware-CoPP ist erforderlich, um einen DoS-Angriff zu verhindern.
ACL-Umleitung an CPU für WCCP	class-copp-wccp	Wird verwendet, wenn das Paket/der Datenfluss zur

		Weiterleitungsentscheidung an die CPU umgeleitet werden muss.
ACL-Umleitung an CPU für Service Insertion Architecture (SIA)	class-copp-service-Insertion	Wird verwendet, wenn das Paket/der Datenfluss zur SIA-Entscheidung an die CPU umgeleitet werden muss.
IPv6-Netzwerkerkennung	class-copp-nd	Um das IPv6-Netzwerkerkennungspaket zur weiteren Verarbeitung an die CPU umzuleiten. Referenz: RFC 4861

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um zu überprüfen, ob in einer der konfigurierten CoPP-Klassenzuordnungen Datenverkehr beobachtet wurde, geben Sie den Befehl **show policy-map control-plane (Richtlinienzuordnung anzeigen) ein**.

Fehlerbehebung

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

Zugehörige Informationen

- Schutz von Cisco Catalyst Switches der Serie 6500 mithilfe von Control Plane Policing, Hardware Rate Limiting und Zugriffskontrolllisten
- Catalyst 6500 Release 15.0SY Software Configuration Guide - Control Plane Policing (CoPP)
- Technischer Support und Dokumentation - Cisco Systems