Esempio di configurazione di Control Plane predefinito su Catalyst 6500/Sup2T e Catalyst 6880

Sommario

Introduzione

Questo documento descrive in dettaglio i tipi di traffico che vengono confrontati con le mappe di classi predefinite, che fanno parte della configurazione predefinita di Catalyst 6500 Sup2T / Catalyst 6880 CoPP (Control Plane Policing) configurata automaticamente sul dispositivo. Questa opzione è configurata in modo da evitare l'overload della CPU.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Per impostazione predefinita, il protocollo CoPP è abilitato sugli switch Catalyst 6500 / SUP2T e Catalyst 6880 ed è basato su un modello preconfigurato. Alcune configurazioni di mappe di classi non dispongono di istruzioni match corrispondenti per il fatto che acquisiscono il traffico non sull'elenco di controllo di accesso (ACL) MAC/IP, ma piuttosto sulle eccezioni interne segnalate dal motore di inoltro quando il traffico viene ricevuto dallo switch e viene presa una decisione di inoltro.

Se è necessario aggiungere, modificare o rimuovere una specifica mappa di classi dalla regola CoPP corrente, è necessario eseguire tale operazione dalla modalità di configurazione nella modalità mappa delle policy. Per la sintassi esatta, vedere la guida alla configurazione del software Catalyst 6500 release 15.0SY - Control Plane Policing (CoPP).

Le classi di eccezione predefinite CoPP sono descritte come segue:

Case	nome mappa classi	Descrizione
Errore MTU (Maximum Transmission Unit)	class-copp-mtu-fail	Le dimensioni del pacchetto superano le dimensioni MTU dell'interfaccia in uscita. Se il bit "non frammentare" non è impostato, la frammentazione è necessaria. Se il bit "non frammentare" è impostato, il messaggio ICMP (Internet Control Message Protocol) "destinazione irraggiungibile" indica che la "frammentazione richiesta e DF impostato" deve essere generata e rinviata all'origine. Riferimento: RFC-791 - RFC-1191
Errore TTL (Time To Live)	class-copp-ttl-fail	TTL pacchetto = 1 (per IPv4), limite hop = 0 o 1 (per IPv6) TTL = 0 (per IPv4) può essere scartato immediatamente nell'hardware, in quanto l'hop precedente dovrebbe distruggere il pacchetto quando il valore TTL è ridotto a 0. Il limite hop = 0 (per IPv6) è diverso da TTL = 0 in quanto nella RFC-2460, sezione 8.2, è indicato che "A differenza di IPv4, i nodi IPv6 non sono necessari per applicare la durata massima del pacchetto. Per questo motivo, il campo Durata IPv4 è stato rinominato "Limite hop in IPv6". Il pacchetto IPv6 in ingresso con limite hop = 0 è ancora valido e il messaggio ICMP deve essere inviato nuovamente. Riferimento: RFC-791, RFC-2460
Opzioni	class-copp-options	Pacchetto con opzioni (per IPv4), intestazione Hop-by-Hop Extension (per IPv6).

		Ad esempio, Router Alert RFC-2113, Strict Source Route e così via. Le intestazioni di estensione non vengono esaminate o elaborate da alcun nodo lungo il percorso di recapito di un pacchetto finché il pacchetto non raggiunge il nodo (o ognuno dei nodi nel caso di multicast) identificato nel campo Indirizzo di destinazione dell'intestazione IPv6. L'unica eccezione è l'intestazione delle opzioni Hop-by-Hop, che riporta le informazioni che devono essere esaminate ed elaborate da ogni nodo del percorso di consegna di un pacchetto, inclusi i nodi di origine e destinazione. L'elaborazione hardware nei campi delle opzioni non è supportata, ovvero è necessaria l'elaborazione/commutazione software. Riferimento: RFC-791 / RFC-2460
Errore di Reverse Path Forwarding (RPF) (Unicast)	class-copp-ucast-rpf-fail	Il pacchetto che non supera il controllo RPF è filtrato. Tuttavia, a causa delle risorse limitate dell'hardware, in alcuni casi il controllo RPF non può essere eseguito nell'hardware (ossia, più di 16 interfacce RPF collegate a un IP). In questo caso, il pacchetto viene inviato al software per un controllo completo di RPF.
Errore RPF (Multicast)	class-copp-mcast-rpf-fail	Il primo pacchetto di dati RPF non riuscito (indirizzato a un gruppo multicast) viene inviato al software per avviare il processo di asserzione PIM (Protocol Independent Multicast). Al termine del processo, viene scelto un router/server d'inoltro designato. Se il pacchetto successivo (stesso flusso) non proviene dal router designato, si verifica un errore RPF e l'hardware può scaricarlo immediatamente (per evitare un attacco Denial of Service (DoS)). Il pacchetto dati del primo RPF non riuscito (indirizzato a un gruppo multicast) viene inviato al software per avviare il processo PIM-assert. Al termine del processo, viene scelto un router/server d'inoltro designato. Se il pacchetto successivo (stesso flusso) non proviene dal router designato, si verifica un errore RPF e l'hardware può eliminarlo immediatamente (per prevenire un attacco DoS). Tuttavia, se la tabella di routing viene aggiornata, potrebbe essere necessario

		scegliere un nuovo router designato (tramite PIM-assert), il che significa che il pacchetto RPF non riuscito deve raggiungere il software (per riavviare PIM-assert). A tale scopo, è disponibile nell'hardware una perdita periodica al meccanismo software (per flusso) per il pacchetto RPF non riuscito. Tuttavia, se si verifica una quantità enorme di flussi, una perdita periodica può essere eccessiva per la gestione del software. Il CoPP hardware è ancora richiesto per il pacchetto multicast RPF non riuscito. Riferimento: RFC-3704, RFC-2362
Riscrittura pacchetti hardware non supportata	class-copp-unsupp-rewrite	Sebbene l'hardware sia in grado di riscrivere i pacchetti in vari casi, alcuni casi non possono essere eseguiti nella progettazione hardware corrente. E per queste, l'hardware invia il pacchetto al software.
ICMP no-route ICMP acl-drop Reindirizzamento ICMP	class-copp-icmp-redirect-unreachable	Pacchetti inviati al software per la generazione di messaggi ICMP. Ad esempio, reindirizzamento ICMP, destinazione ICMP non raggiungibile (ad esempio,. non raggiungibile o proibito a livello amministrativo). Riferimento: RFC-792 / RFC-2463
Ricezione Cisco Express Forwarding (CEF) (l'IP di destinazione è l'IP del router)	class-copp-receive	Se l'IP di destinazione del pacchetto è uno degli indirizzi IP del router (colpirà l'adiacenza di ricezione CEF), il software deve elaborare il contenuto.
CEF glean (l'IP di destinazione appartiene a una rete del router)	class-copp-glean	Se l'IP di destinazione del pacchetto appartiene a una rete del router, ma non viene risolto (ossia, non viene rilevato alcun hit nella tabella FIB (Forwarding Information Base), il pacchetto incontrerà l'adiacenza dell'icona CEF, e verrà inviato al software da cui verrà avviata la procedura di risoluzione. Per l'IPv4, lo stesso flusso continua a raggiungere il margine CEF finché l'indirizzo non viene risolto. Per IPv6, durante la risoluzione viene installata una voce FIB temporanea che corrisponde all'IP di destinazione (e punta invece all'adiacenza di rilascio). Se non è possibile risolverlo nella durata specificata, la voce FIB viene rimossa, ovvero lo stesso flusso inizia a raggiungere di nuovo l'impostazione CEF lean.

Pacchetto destinato al multicast IP 224.0.0.0/4	class-copp-mcast-ip-control	Il pacchetto di controllo deve essere elaborato dal software.
Pacchetto destinato a IP multicast FF::/8	class-copp-mcast-ipv6-control	Il pacchetto di controllo deve essere elaborato dal software.
Pacchetto multicast da copiare nel software	class-copp-mcast-copy	In alcuni casi, il pacchetto multicast deve essere copiato sul software per un aggiornamento di stato (il pacchetto è ancora collegato all'hardware sulla stessa VLAN). Ad esempio, (*,G/m) premere per l'ingresso in modalità densa, switchover SPT dual-rpf.
Mancato riscontro del pacchetto multicast nella tabella FIB	class-copp-mcast-punt	L'IP di destinazione (IP multicast) non è presente nella tabella FIB. Il pacchetto viene inviato al software.
Origine con connessione diretta (IPv4)	class-copp-ip-connected	Il traffico multicast proveniente da origini direttamente connesse viene inviato al software dove è possibile creare (e installare nell'hardware) uno stato multicast.
Origine con connessione diretta (IPv6)	connesso a class-copp-ipv6	Il traffico multicast proveniente da origini direttamente connesse viene inviato al software dove è possibile creare (e installare nell'hardware) uno stato multicast.
Pacchetto broadcast	class-copp-broadcast	I pacchetti broadcast (ad esempio, IP/Non-IP con broadcast DMAC e IP unicast con Multicast DMAC) vengono trasmessi al software.
Protocollo sconosciuto a (ovvero non supportato da) in termini di commutazione hardware	class-copp-known-protocol	Il protocollo non IP, ad esempio IPX (Internetwork Packet Exchange) e così via, non verrà commutato dall'hardware. Vengono inviate al software e inoltrate lì.
Traffico dati multicast in entrata tramite porta instradata dove PIM è disabilitato	class-copp-mcast-v4-data-on-routed Port	Il traffico di dati multicast che arriva attraverso una porta instradata (dove PIM è disabilitato) viene perso verso il software. Tuttavia, non è necessario inviarli al software in modo che vengano eliminati.
Traffico dati multicast in entrata tramite porta instradata dove PIM è disabilitato	class-copp-mcast-v6-data-on-routedPort	Il traffico di dati multicast che arriva attraverso una porta indirizzata (dove PIM è disabilitato) viene perso nel software. Tuttavia, non è necessario inviarli al software in modo che vengano eliminati.
Reindirizzamento	class-copp-ucast-ingress-acl-bridged	L'hardware presenta 8 eccezioni relative

ACL in ingresso per il bridging del pacchetto		agli ACL impostate dal software tramite un reindirizzamento ACL. Questo riguarda i pacchetti unicast collegati alla CPU dall'ACL per motivi correlati al TCAM (Ternary Content Addressable Memory).
Esci dal reindirizzamento ACL per creare il bridge del pacchetto	class-copp-ucast-exit-acl-bridged	L'hardware presenta 8 eccezioni relative agli ACL impostate dal software tramite un reindirizzamento ACL. Questo riguarda i pacchetti unicast collegati alla CPU dall'ACL per motivi correlati al TCAM (Ternary Content Addressable Memory).
Mcast - Reindirizzamento ACL a bridge di pacchetti sulla CPU	class-copp-mcast-acl-bridged	L'hardware presenta 8 eccezioni relative agli ACL impostate dal software tramite un reindirizzamento ACL. Questo riguarda l'elaborazione multicast.
Adattatore ACL alla CPU per elaborazione bilanciamento carico server	class-copp-slb	L'hardware presenta 8 eccezioni relative agli ACL impostate dal software tramite un reindirizzamento ACL. Questo riguarda un reindirizzamento hardware per una decisione SLB (Server Load Balancing).
Reindirizzamento log VACL ACL	class-copp-vacl-log	L'hardware presenta 8 eccezioni relative agli ACL impostate dal software tramite un reindirizzamento ACL. Questo articolo è relativo al reindirizzamento dei pacchetti tramite ACL VLAN (Access Control List, VACL) sulla CPU per Cisco IOS? scopo di registrazione.
snooping DHCP	class-copp-dhcp-snooping	I pacchetti snooped DHCP vengono reindirizzati alla CPU per l'elaborazione DHCP
Inoltro basato su criteri MAC	class-copp-mac-pbf	L'inoltro basato su criteri deve essere eseguito nella CPU perché l'hardware non è in grado di inoltrare i pacchetti in questo caso.
Controllo dell'ingresso in rete con ingresso IP	class-copp-ip-ammissione	Per consentire l'accesso alla rete in base alle credenziali antivirus dell'host, è necessario eseguire la convalida della postura tramite una delle opzioni seguenti: (1) L'interfaccia L2 utilizzerà la porta LAN IP (LPIP), dove i pacchetti Address Resolution Protocol (ARP) vengono reindirizzati alla CPU, (2) L'interfaccia L3 utilizza il gateway IP (GWIP). Dopo la convalida viene eseguita l'autenticazione (*). Per un'interfaccia L2 è WebAuth, che esegue l'intercettazione dei pacchetti HTTP e può inoltre eseguire il reindirizzamento dell'URL (*). Per l'interfaccia L3, è AuthProxy.
Ispezione ARP dinamica	class-copp-arp-snooping	Per prevenire l'avvelenamento ARP (man-in-the-middle), l'ispezione ARP dinamica (nota anche come DAI (Dynamic ARP

		Inspection) convalida le richieste/risposte ARP in base a quando intercetta e quindi le elabora nella CPU in base a una delle seguenti: (1) ACL ARP configurati dall'utente (per host configurati staticamente), (2) binding da indirizzo MAC a indirizzo IP archiviati in database attendibili (ovvero binding DHCP). Per aggiornare la cache ARP locale o inoltrarla vengono utilizzati solo pacchetti ARP validi. Il processo di convalida richiede il coinvolgimento della CPU nei pacchetti ARP, il che significa che il CoPP hardware è necessario per prevenire un attacco DoS.
Reindirizzamento ACL alla CPU per WCCP	class-copp-wccp	Utilizzato nel caso in cui il pacchetto/flusso debba essere reindirizzato alla CPU per la decisione di inoltro WCCP (Web Cache Communication Protocol).
Reindirizzamento ACL alla CPU per Service Insertion Architecture (SIA)	class-copp-service-insertion	Utilizzato nel caso in cui il pacchetto/flusso debba essere reindirizzato alla CPU per la decisione SIA.
Individuazione rete IPv6	class-copp-end	Per reindirizzare il pacchetto IPv6 Network Discovery alla CPU e continuare l'elaborazione. Riferimento: RFC 4861

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare la presenza di traffico in una delle mappe di classe CoPP configurate, immettere il comando **show policy-map control-plane**.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Protezione degli switch Cisco Catalyst serie 6500 tramite Control Plane Policing, limitazione della velocità hardware e Access-Control Lists

- Guida alla configurazione del software Catalyst 6500 release 15.0SY - Control Plane Policing (CoPP)
- Documentazione e supporto tecnico – Cisco Systems