Beleid inzake standaardbesturingsplane voor Catalyst 6500/Sup2T en Catalyst 6880 configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft in detail welke soorten verkeer tegen standaardinstellingen van class-maps worden afgesloten, die deel uitmaken van de standaard Catalyst 6500 Sup2T/Catalyst 6880 CoPP-configuratie (controle van besturingsplane) die automatisch op het apparaat wordt ingesteld. Dit wordt ingesteld om te voorkomen dat de CPU's worden overbelast.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

CoPP is standaard ingeschakeld op Catalyst 6500/SUP2T- en Catalyst 6880-switches en is gebaseerd op een vooraf ingesteld sjabloon. Sommige class-map-configuraties hebben geen corresponderende matchverklaringen vanwege het feit dat ze verkeer niet opnemen in de MAC/IP Access Control List (ACL), maar eerder op interne uitzonderingen die worden gemarkeerd door de expediteur-motor wanneer het verkeer ontvangen is door de schakelaar en een beschikking voor verzenden wordt genomen.

Als een specifieke class-map moet worden toegevoegd / aangepast / verwijderd van het huidige CoPP-beleid, dan moet dit in de beleidskaartmodus gebeuren. Zie Catalyst 6500 release 15.0SY softwareconfiguratie Guide - Control Plane Monitoring (CoPP) voor de exacte syntaxis.

CoPP standaard uitzonderingsklassen hebben deze beschrijvingen:

Case	klassenaam	Beschrijving
Max. storing van transmissieeenheid (MTU)	class-copp-mtu-fail	Packet size is groter dan uitgaande interface MTU-grootte. Als het Don Fragment nie ingesteld is fragmentatie vereist. Als het bit Don Fragment is ingesteld, geeft het onbereikbare bericht van bestemming ICMP (Intern Control Message Protoco aan dat "fragmentatie noo en DF set" moet worden gegenereerd en naar de bron moet worden teruggestuurd. Referentie: RFC-791, RF 191
Tijd om te leven (TTL)-storing	class-copp-tl-fail	Packet TTL = 1 (voor IPv4 Hop Limit = 0 of 1 (voor IPv6) TTL = 0 (voor IPv4) kan in hardware onmiddellijk worden weggegooid aangezien de vorige hop pakket moet vernietigen wanneer TTL tot 0 wordt verlaagd. Hop Limit = 0 (voor IPv6) niet gelijk aan TTL = 0, omdat deze in RFC-2460 sectie 8.2 wordt vermeld "In tegenstelling tot IPv4, IPv6 knooppunten niet no zijn om maximale pakketlevensduur af te

Opties	class-copp-opties	dwingen. Dat is de reden het veld IPv4 Time to Live werd omgedoopt tot Hop Limit in IPv6". Dit betekent inkomend IPv6-pakket met Hop Limit = 0 is nog steeds geldig en het ICMP-bericht moet worden teruggestuurd Referentie: RFC-791, RFC 2460 Packet met opties (voor IPv4), Hop-by-hop uitbreidingsheader (voor IPv6). Bijvoorbeeld, de RFC-211 van de router, de strikte BronRoute, enz. De kopregels van de uitbreiding worden niet onderzocht of verwerkt door enige knoop langs het leveringspad van een pakket, tot het pakket het knooppunt (of elk van de reeks knooppunten in het geval van multicast) bereikt dat in het veld Bestemmingsadres van de IPv6-header wordt geïdentificeerd. De enige uitzondering is de kop van de opties van het Hop-bij-Hop, die informatie bevat door elk knooppunt moet worden onderzocht en verwerkt langs het leveringspad van een pakket, dat de bron- en doelknooppunten bevat. Hardware verwerking op optievelden wordt niet ondersteund, dat wil zeggen dat softwareverwerking/switching nodig zijn. Referentie: RFC-791/RFC 2460
FOUT BIJ DOORSTUREN (RPF) (Unicast)	class-copp-ucast-rpf-fail	Het pakket met de RPF-to wordt gefilterd. Vanwege beperkte middelen in de hardware kan de VPF-controle echter in bepaalde gevallen niet in hardware

RPF-fout (multicast)	class-copp-mcast-rpf-fail	worden uitgevoerd (dat w zeggen, meer dan 16 RP interfaces gekoppeld aan één IP). Wanneer dat gebeurt, wordt het pakket naar software verzonden voor een volledige contro van PDF. Het eerste RPF mislukte gegevenspakket (bedoeld voor een multicast groep) wordt naar software verzonden om het Protoc Onafhankelijke Multicast (PIM)-proces te starten. Zodra het proces wordt voltooid, wordt een aangewezen router/expediteur geselecteerd. Als het volgende pakket (dezelfd stroom) niet van de aangewezen router komt, veroorzaakt het een storin van RPF, en kan de hardware het meteen late vallen (om een aanval va de Staat van de Dienst (v de Staat) te voorkomen). Het eerste RPF-datapakk (bedoeld voor een multica groep) wordt naar de software verzonden om h PIM-Assemblee proces te starten. Zodra het proces wordt voltooid, wordt een aangewezen router/expediteur geselecteerd. Als het volgende pakket (dezelfd stroom) niet van de aangewezen router komt, veroorzaakt het een storin van RPF, en kan de hardware het meteen late vallen (om een DoS-aanv te voorkomen). Als de routingtabel echter wordt bijgewerkt, kan het nodig zijn om een nieuwe aangewezen router te kie (via PIM-waarschuwing),

		betekent dat het RPF-pak niet heeft gefaald om de software te bereiken (om PIM-bericht opnieuw te starten). Om dat te doen, er een periodiek lek naar softwaremechanisme (pe flow) voor een PPF-mislu pakket beschikbaar in de hardware. Merk op dat als een grote hoeveelheid stromen is, een periodiek te veel kan zijn voor de software om deze aan te kunnen. De hardware Co is nog steeds vereist voor multicast RPF-pakket me fouten. Referentie: RFC-3704, RF 2362
Herschrijven van hardwarepakketten niet ondersteund	klasseoverschrijdend	Hoewel de hardware pakketten in verschillende gevallen kan herschrijven kunnen sommige gevallen eenvoudigweg niet worde gedaan in het huidige hardwareontwerp. En daarvoor stuurt de hardw het pakket naar software.
ICMP-on-route ICMP-toets ICMP-omleiding	class-copp-icmp-redirect onbereikbaar	Packets die naar software worden verzonden voor d productie van ICMP-berichten. Zoals ICMP redirect, ICMP bestemmi onbereikbaar (bijvoorbeel gastheer onbereikbaar of administratief verboden). Referentie: RFC-792/RFC 2463
Cisco Express Forwarding (CEF) ontvangt (bestemming IP is IP van router)	per klasse ontvangen	Als de bestemming van h pakket IP een van de IP adressen van de router is (zal CEF nabijheid ontvangen), dan moet de software de inhoud verwerken.
CEF-slang (bestemming IP behoort tot een van de netwerken van de router)	van klasse overhellende	Als de bestemming van h pakket tot één van het netwerk van de router behoort, maar het niet wo opgelost (dat wil zeggen, in de tabel Forwarding Information Base (FIB) wo

		geraakt, zal het de nabijh van de vraag om CEF worden verzonden naar software waar de resolutieprocedure zal worden begonnen. Voor IPv4 blijft dezelfde stroom CEF glean raken totdat het adres is opgelo Voor IPv6 wordt een tijde FIB-ingang die bij de bestemming IP (en punte om nabijheid te laten valle in plaats daarvan) tijdens resolutie geïnstalleerd. Al het niet kan worden opge in de gespecificeerde duu wordt de FIB-ingang verwijderd (dat wil zegge dezelfde stroom begint w CEF-legendarisch te rake
Packet voor multicast IP 224.0.0.0/4	class-copp-mcast-ip-control	Het bedieningspaneel mo door de software worden verwerkt.
Packet voor multicast IP-FF: 8/8	class-copp-mcast-ipv6-control	Het bedieningspaneel mo door de software worden verwerkt.
Multicastpakket dat naar de software moet worden gekopieerd	van klasse voorzien van een gepresteerde kopie	In sommige gevallen moe het multicast pakket naar software worden gekopie voor een update van de s (het pakket is nog hardwa overbrugd op hetzelfde VLAN). Bijvoorbeeld (*,G/ ingedrukt voor Dense Mo invoer, dual-rpf SPT-omschakeling.
Multicastpakket dat een fout in FIB-tabel krijgt	klas-copp-mcast-punt	Het bestemming IP (multicast IP) is een fout i de FIB-tabel. Het pakje is de software gezet.
Direct verbonden bron (IPv4)	met klasse-copp-ip verbonden	Multicastverkeer van rechtstreeks aangesloten bronnen wordt naar de software verzonden waar een multicaststatus kan worden gecreëerd (en in hardware kan worden geïnstalleerd).
Direct verbonden bron (IPv6)	met klasse copp-ipv6 verbonden	Multicastverkeer van rechtstreeks aangesloten bronnen wordt naar de software verzonden waar

Breedtepakje	klassenradio en televisie	een multicaststatus kan worden gecreëerd (en in hardware kan worden geïnstalleerd). Broadcast-pakketten (bijvoorbeeld IP/niet-IP m broadcast DMAC- en IP-unicast met Multicast DM worden naar de software gelekt.
Protocol onbekend aan (d.w.z. niet ondersteund door) in termen van hardware-switching	class-copp-onbekende-protocol	Het niet-IP protocol, zoals Internetwork Packet Exchange (IPX) enzovoor zal niet via hardware wor geschakeld. Ze worden n software gestuurd en naa daar doorgestuurd.
Multicast voor gegevensverkeer dat binnenkomt via een routepoort waar PIM is uitgeschakeld	class-copp-mcast-v4-data-on-routedPort	Multicast voor gegevensverkeer dat doo een routepoort komt (waa PIM wordt uitgeschakeld) wordt naar de software gelekt. Het is echter niet nodig ze naar de software sturen, zodat ze worden ingetrokken.
Multicast voor gegevensverkeer dat binnenkomt via een routepoort waar PIM is uitgeschakeld	class-copp-mcast-v6-data-on-routedPort	Multicast voor gegevensverkeer dat binnenkomt door een routepoort (waar PIM wor uitgeschakeld) wordt naa software gelekt. Het is ec niet nodig ze naar de software te sturen, zodat worden ingetrokken.
Verplaats ACL-richting om het pakket te overbruggen	met een loopbrug van klasse	De hardware heeft 8 ACL gerelateerde uitzondering die door de software via e ACL-omleiding zijn ingest Deze heeft betrekking op pakketten die door ACL a de CPU zijn gekoppeld vo Ternary Content Adressa Memory (TCAM)-gerelateerde redenen.
Druk ACL-omleiding om het pakket te overbruggen	met een loopbrug van klasse	De hardware heeft 8 ACL gerelateerde uitzondering die door de software via e ACL-omleiding zijn ingest Deze heeft betrekking op pakketten die door ACL a de CPU zijn gekoppeld vo Ternary Content Adressa

Mcast ACL-omleiding naar bridge-pakketten naar CPU's	met een klasse-kops-gekkeld-acl-bruin	Memory (TCAM)-gerelateerde redenen. De hardware heeft 8 ACL gerelateerde uitzondering die door de software via e ACL-omleiding zijn ingest Deze heeft betrekking op multicast verwerking.
ACL-brug naar CPU voor taakverdeling voor servers	klasblok	De hardware heeft 8 ACL gerelateerde uitzondering die door de software via e ACL-omleiding zijn ingest Deze heeft betrekking op een hardware-redirect vo een SLB-beslissing (Serv Taakverdeling).
ACL-logbestand omleiden	klassenbestand	De hardware heeft 8 ACL gerelateerde uitzondering die door de software via e ACL-omleiding zijn ingest Deze heeft betrekking op pakketomleiding door VL Access Control List (VAC naar CPU voor Cisco IOS houtkap.
DHCP-snooping	klas-copp-dhcp-snooping	DHCP-pakketten worden opnieuw naar de CPU vo DHCP-verwerking gericht
Op MAC-beleid gebaseerde doorsturen	class-copp-mac-pbf	Op beleid gebaseerde doorsturen moet in de CP worden uitgevoerd omdat hardware in dit geval niet staat is pakketten door te sturen.
IP-toegangsnetwerktoegangscontrole	klassebekentenis	Om netwerktoegang te bieden op basis van de antivirusreferenties van d host, is er posture validati via een van deze opties: (De L2-interface zal LAN P IP (LPIP) gebruiken, waa pakketten voor adresresolutie (ARP) wor omgeleid naar de CPU, (2 De L3-interface gebruikt Gateway IP (GWIP). Na d validatie is er de authenticatie (*). Voor een interface is het WebAuth, HTTP pakje interceptie uitvoert en ook URL redirectie (*) kan uitvoere Voor de L3 interface is he

		AuthProxy.
Dynamische ARP-inspectie	klas-copp-arp-snooping	Om ARP-vergiftiging (ma in-the-middle) te voorkom bevestigt dynamische AR inspectie (ook wel bekend als Dynamic ARP Inspect (DAI)) de ARP-verzoeken/antwoorden op het moment dat deze wor onderschept en verwerkt vervolgens in de CPU teg een van de volgende manieren: (1) door gebrui ingesteld ARP ACL's (voo statelijk geconfigureerd hosts), (2) MAC-adres na IP-adresbindingen die zijn opgeslagen in een vertrouwde database (d.w DHCP-verbindingen). Alle geldige ARP pakketten worden gebruikt om het lokale ARP cache bij te werken of om door te stur Het validatieproces vereis betrokkenheid van ARP-pakketten CPU, wat betek dat hardware-CoPP nodig om een DoS-aanval te voorkomen.
ACL-omleiding naar CPU voor WCCP	class-copp-wcp	Gebruikt voor het geval d het pakket/de flow moet worden omgeleid naar de CPU voor de beschikking voor webcaches met betrekking tot het communicatieprotocol (WCCP).
ACL-richting (opnieuw) naar CPU voor serviceaanpassingsarchitectuur (SIA)	plaatsing van klasse-copp-service	Gebruikt voor het geval d het pakket/de stroom moe worden omgeleid naar de CPU voor een SIA-beslissing.
IPv6-netwerkontdekking	klas-copp-nd	Om het IPv6-pakket voor netwerkdetectie opnieuw richten op de CPU's, zoda deze verder kunnen word verwerkt. Referentie: RFC4861

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Om te controleren of er verkeer was waargenomen in een van de geconfigureerde CoPP-class-maps, voert u de opdracht **besturing-vlak met** de **show policy-map in**.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco Catalyst 6500 Series-switches beveiligen met controle van het besturingsplane, hardwaresnelheidsbeperking en toegangscontrolelijsten
- Catalyst 6500 release 15.0SY software Configuration Guide - Control of Plane Policing (CoPP)
- Technische ondersteuning en documentatie – Cisco Systems