Exemple de configuration de la stratégie de plan de contrôle par défaut sur Catalyst 6500/Sup2T et Catalyst 6880

Contenu

Introduction

Ce document décrit en détail quels types de trafic sont mis en correspondance avec les class-maps par défaut, qui font partie de la configuration Catalyst 6500 Sup2T / Catalyst 6880 CoPP (Control Plane Policing) par défaut qui est automatiquement configurée sur le périphérique. Ceci est configuré afin de protéger son processeur contre la surcharge.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

CoPP est activé par défaut sur les commutateurs Catalyst 6500 / SUP2T et Catalyst 6880 et repose sur un modèle préconfiguré. Certaines configurations de mappage de classe ne comportent pas d'instructions de correspondance correspondantes en raison du fait qu'elles capturent le trafic non pas sur la liste de contrôle d'accès MAC/IP (ACL), mais sur des exceptions internes qui sont signalées par le moteur de transfert lorsque le trafic est reçu par le commutateur et qu'une décision de transfert est prise.

Si un class-map spécifique doit être ajouté / modifié / supprimé de la stratégie CoPP actuelle, il doit être effectué à partir du mode de configuration en mode policy-map. Voir Guide de configuration du logiciel Catalyst 6500 version 15.0SY - Control Plane Policing (CoPP) pour la syntaxe exacte.

Les classes d'exception CoPP par défaut ont les descriptions suivantes :

Cas	class-map name	Description
Défaillance MTU (Maximum Transmission Unit)	class-copp-mtu-fail	La taille du paquet dépasse la taille MTU de l'interface sortante. Si le bit Ne pas fragmenter n'est pas défini, la fragmentation est requise. Si le bit Ne pas fragmenter est défini, le message ICMP (Internet Control Message Protocol) Destination Unreachable indique que la fragmentation requise et DF set est supposée être générée et renvoyée à la source. Référence: RFC-791, RFC-1191
Échec de durée de vie (TTL)	class-copp-ttl-fail	TTL du paquet = 1 (pour IPv4), limite de sauts = 0 ou 1 (pour IPv6) TTL = 0 (pour IPv4) peut être immédiatement ignoré dans le matériel, car le saut précédent est censé détruire le paquet lorsque TTL est décrémenté à 0. La limite de sauts = 0 (pour IPv6) est différente de TTL = 0, car il est indiqué dans la RFC-2460, section 8.2 que « Contrairement à IPv4, les noeuds IPv6 ne sont pas nécessaires pour appliquer la durée de vie maximale des paquets. C'est la raison pour laquelle le champ IPv4 Time to Live a été renommé Hop Limit dans IPv6 ». Cela signifie que le paquet IPv6 entrant avec la limite de sauts = 0 est toujours valide et que le message ICMP doit être renvoyé. Référence: RFC-791, RFC-2460
Options	class-copp-options	Paquet avec options (pour IPv4), en-tête d'extension saut par saut (pour IPv6). Par exemple, Router Alert RFC-2113, Strict Source Route, etc. Les en-têtes d'extension ne sont pas examinés ou traités par un noeud sur le chemin de livraison d'un paquet, jusqu'à ce que le paquet atteigne le noeud (ou

		chaque ensemble de noeuds dans le cas de multidiffusion) identifié dans le champ Adresse de destination de l'en-tête IPv6. La seule exception est l'en-tête Options de saut par saut, qui transporte des informations qui doivent être examinées et traitées par chaque noeud le long du chemin de livraison d'un paquet, qui inclut les noeuds source et de destination. Le traitement matériel sur les champs d'options n'est pas pris en charge, c'est-à-dire que le traitement/la commutation logiciel est nécessaire. Référence: RFC-791 / RFC-2460
Échec du transfert inverse du chemin (RPF) (monodiffusion)	class-copp-ucast-rpf-fail	Le contrôle RPF du paquet qui échoue est filtré. Cependant, en raison de ressources limitées dans le matériel, le contrôle RPF ne peut pas être effectué dans le matériel dans certains cas (c'est-à-dire plus de 16 interfaces RPF liées à une adresse IP). Dans ce cas, le paquet est envoyé au logiciel pour un contrôle RPF complet. Le premier paquet de données RPF défaillant (adressé à un groupe de multidiffusion) est envoyé au logiciel afin que le processus d'assertion PIM (Protocol Independent Multicast) démarre. Une fois le processus terminé, un routeur/redirecteur désigné est sélectionné. Si le paquet suivant (même flux) ne provient pas du routeur désigné, il déclenche une défaillance RPF et le matériel peut le déposer immédiatement (afin d'empêcher une attaque par déni de service).
Échec RPF (Multidiffusion)	class-copp-mcast-rpf-fail	Le premier paquet de données RPF défaillant (adressé à un groupe de multidiffusion) est envoyé au logiciel afin que le processus d'assertion PIM démarre. Une fois le processus terminé, un routeur/redirecteur désigné est sélectionné. Si le paquet suivant (même flux) ne provient pas du routeur désigné, il déclenche une défaillance RPF et le matériel peut le déposer immédiatement (afin d'empêcher une attaque DoS). Cependant, si la table de routage est mise à jour, il peut être nécessaire de choisir un nouveau routeur désigné (via PIM-assert), ce qui signifie que le paquet RPF défaillant doit atteindre le logiciel (pour que PIM-assert redémarre). Pour ce faire, une fuite

		périodique au mécanisme logiciel (par flux) pour le paquet défaillant RPF est disponible dans le matériel. Notez cependant que s'il y a une énorme quantité de flux, une fuite périodique peut être trop importante pour que le logiciel puisse gérer. Le CoPP matériel est toujours requis pour le paquet RPF multicast ayant échoué. Référence: RFC-3704, RFC-2362
Réécriture de paquet matériel non prise en charge	class-copp-unsupp-rewrite	Bien que le matériel puisse réécrire des paquets dans différents cas, certains cas ne peuvent tout simplement pas être effectués dans la conception matérielle actuelle. Et pour ceux-ci, le matériel envoie le paquet au logiciel.
Non-route ICMP Liste déroulante ICMP redirection ICMP	class-copp-icmp-redirect-unreachable	Paquets envoyés au logiciel pour la génération de messages ICMP. Par exemple, redirection ICMP, destination ICMP inaccessible (par exemple,. hôte inaccessible ou administrativement interdit). Référence: RFC-792 / RFC-2463
Réception CEF (Cisco Express Forwarding) (l'adresse IP de destination est l'adresse IP du routeur)	class-copp-receive	Si l'adresse IP de destination du paquet est l'une des adresses IP du routeur (qui atteint la contiguïté de réception CEF), le logiciel est censé traiter le contenu.
Glean CEF (l'adresse IP de destination appartient à l'un des réseaux du routeur)	class-copp-glean	Si l'adresse IP de destination du paquet appartient à l'un des réseaux du routeur, mais qu'elle n'est pas résolue (c'est-à-dire qu'elle ne figure pas dans la table FIB (Forwarding Information Base)), elle atteint la contiguïté du canal CEF, envoyée au logiciel où la procédure de résolution démarre. Pour IPv4, le même flux continue d'atteindre CEF glean jusqu'à ce que l'adresse soit résolue. Pour IPv6, une entrée FIB temporaire qui correspond à l'adresse IP de destination (et qui pointe à la place vers la contiguïté de suppression) est installée pendant la résolution. S'il ne peut pas être résolu dans la durée spécifiée, l'entrée FIB est supprimée (c'est-à-dire que le même flux commence à frapper à nouveau CEF glean).
Paquet destiné à la multidiffusion IP 224.0.0.0/4	class-copp-mcast-ip-control	Le paquet de contrôle doit être traité par le logiciel.

Paquet destiné à la multidiffusion IP FF::/8	class-copp-mcast-ipv6-control	Le paquet de contrôle doit être traité par le logiciel.
Paquet de multidiffusion qui doit être copié dans le logiciel	class-copp-mcast-copy	Dans certains cas, le paquet de multidiffusion doit être copié dans le logiciel pour une mise à jour d'état (le paquet est toujours un paquet matériel ponté sur le même VLAN). Par exemple, (*, G/m) a appuyé pour l'entrée en mode dense, commutation SPT à double rpf.
Paquet de multidiffusion manquant dans la table FIB	class-copp-mcast-punt	L'adresse IP de destination (IP de multidiffusion) est une erreur dans la table FIB. Le paquet est pointé vers le logiciel.
Source connectée directement (IPv4)	class-copp-ip-connected	Le trafic de multidiffusion provenant de sources directement connectées est envoyé au logiciel où un état de multidiffusion peut être créé (et installé dans le matériel).
Source connectée directement (IPv6)	class-copp-ipv6-connected	Le trafic de multidiffusion provenant de sources directement connectées est envoyé au logiciel où un état de multidiffusion peut être créé (et installé dans le matériel).
Paquet de diffusion	class-copp-broadcast	Les paquets de diffusion (par exemple, IP/Non-IP avec DMAC de diffusion et IP monodiffusion avec DMAC de multidiffusion) sont divulgués au logiciel.
Protocole inconnu (non pris en charge par) en termes de commutation matérielle	class-copp-inconnu-protocol	Le protocole non IP, tel qu'IPX (Internetwork Packet Exchange), etc., ne sera pas commuté au niveau matériel. Ils sont envoyés au logiciel et y sont transférés.
Trafic de données multidiffusion entrant via un port routé où PIM est désactivé	class-copp-mcast-v4-data-on-routedPort	Le trafic de données multidiffusion qui arrive par un port routé (où PIM est désactivé) est divulgué au logiciel. Cependant, il n'est pas nécessaire de les envoyer au logiciel pour qu'ils soient abandonnés.
Trafic de données multidiffusion entrant via un port routé où PIM est désactivé	class-copp-mcast-v6-data-on-routedPort	Le trafic de données multidiffusion qui arrive par un port routé (où PIM est désactivé) est divulgué au logiciel. Cependant, il n'est pas nécessaire de les envoyer au logiciel pour qu'ils soient abandonnés.
Redirection de la liste de	class-copp-ucast-ingress-acl-bridged	Le matériel dispose de 8 exceptions liées aux listes de contrôle d'accès définies par

contrôle d’accès entrante pour relier le paquet		le logiciel via une redirection de listes de contrôle d’accès. Celle-ci concerne les paquets de monodiffusion pontés au CPU par la liste de contrôle d'accès pour des raisons liées à la mémoire TCAM (Ternary Content Addressable Memory).
Redirection de la liste de contrôle d’accès de sortie pour relier le paquet	class-copp-ucast-egress-acl-bridged	Le matériel dispose de 8 exceptions liées aux listes de contrôle d’accès définies par le logiciel via une redirection de listes de contrôle d’accès. Celle-ci concerne les paquets de monodiffusion pontés au CPU par la liste de contrôle d'accès pour des raisons liées à la mémoire TCAM (Ternary Content Addressable Memory).
Redirection de la liste de contrôle d'accès de diffusion vers le processeur des paquets de pont	class-copp-mcast-acl-bridged	Le matériel dispose de 8 exceptions liées aux listes de contrôle d’accès définies par le logiciel via une redirection de listes de contrôle d’accès. Celle-ci concerne le traitement de multidiffusion.
Pont ACL vers CPU pour le traitement de l'équilibrage de charge du serveur	class-copp-slb	Le matériel dispose de 8 exceptions liées aux listes de contrôle d’accès définies par le logiciel via une redirection de listes de contrôle d’accès. Celle-ci concerne une redirection matérielle pour une décision d'équilibrage de charge de serveur (SLB).
Redirection du journal ACL VACL	class-copp-vacl-log	Le matériel dispose de 8 exceptions liées aux listes de contrôle d’accès définies par le logiciel via une redirection de listes de contrôle d’accès. Celle-ci se rapporte à la redirection de paquets par liste de contrôle d'accès VLAN (VACL) au CPU pour Cisco IOS ? de journalisation.
Surveillance DHCP	class-copp-dhcp-snooping	Les paquets de surveillance DHCP sont redirigés vers le processeur pour le traitement DHCP
Transfert basé sur la stratégie MAC	class-copp-mac-pbf	Le transfert basé sur des stratégies doit être effectué dans le processeur, car le matériel ne peut pas transférer les paquets dans ce cas.
Contrôle d'admission au réseau IP	class-copp-ip-admission	Afin de fournir un accès réseau basé sur les informations d'identification antivirus de l'hôte, il existe une validation de position via l'une des options suivantes : (1) L'interface L2 utilise le protocole LPIP (LAN Port IP), où les paquets ARP (Address Resolution Protocol) sont redirigés vers le processeur, (2) L'interface L3 utilise le protocole GWIP (Gateway IP). Après la validation, il y a l'authentification (*). Pour une interface L2, il s'agit de

		WebAuth, qui effectue l'interception de paquets HTTP et peut également effectuer la redirection d'URL (*). Pour l'interface L3, il s'agit de AuthProxy.
Inspection dynamique d'ARP	class-copp-arp-snooping	Afin d'empêcher l'attaque par empoisonnement ARP (man-in-the-Middle), l'inspection ARP dynamique (également connue sous le nom d'inspection ARP dynamique (DAI)) valide les requêtes/réponses ARP par lorsqu'elle les intercepte et les traite dans le processeur contre l'une de ces deux méthodes : (1) listes de contrôle d'accès ARP configurées par l'utilisateur (pour les hôtes configurés de manière statique), (2) liaisons d'adresse MAC à adresse IP stockées dans une base de données de confiance (c'est-à-dire des liaisons DHCP). Seuls les paquets ARP valides sont utilisés pour mettre à jour le cache ARP local ou le transférer. Le processus de validation nécessite l'implication du CPU des paquets ARP, ce qui signifie que le matériel CoPP est nécessaire pour empêcher une attaque DoS.
Redirection ACL vers CPU pour WCCP	class-copp-wccp	Utilisé au cas où le paquet/flux doit être redirigé vers le processeur pour la décision de transfert du protocole WCCP (Web Cache Communication Protocol).
Redirection de la liste de contrôle d'accès vers le processeur pour l'architecture d'insertion de service (SIA)	class-copp-service-insertion	Utilisé au cas où le paquet/flux doit être redirigé vers le processeur pour la décision SIA.
Détection de réseau IPv6	class-copp-nd	Afin de rediriger le paquet de découverte de réseau IPv6 vers le processeur pour qu'il traite davantage. Référence: RFC4861

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier si du trafic a été observé dans l'une des cartes-classes CoPP configurées, entrez la commande **show policy-map control-plane**.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Protection des commutateurs de la gamme Cisco Catalyst 6500 à l'aide de la réglementation du plan de contrôle, de la limitation du débit matériel et des listes de contrôle d'accès
- Guide de configuration du logiciel Catalyst 6500 version 15.0SY - Contrôle du plan de contrôle (CoPP)
- Support et documentation techniques - Cisco Systems