Exemplo de política de plano de controle padrão no Catalyst 6500/Sup2T e no Catalyst 6880 Configuration

Contents

Introduction

Este documento descreve em detalhes quais tipos de tráfego são comparados com os mapas de classe padrão, que fazem parte da configuração padrão do Catalyst 6500 Sup2T / Catalyst 6880 CoPP (Control Plane Policing) que é automaticamente configurada no dispositivo. Isso é configurado para proteger a CPU de sobrecarga.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Configurar

O CoPP é ativado por padrão nos switches Catalyst 6500 / SUP2T e Catalyst 6880 e é baseado em um modelo pré-configurado. Algumas configurações de mapa de classe não têm instruções correspondentes devido ao fato de capturarem tráfego não na ACL (Access Control List, lista de controle de acesso) MAC/IP, mas em exceções internas que são sinalizadas pelo mecanismo de encaminhamento quando o tráfego é recebido pelo switch e uma decisão de encaminhamento é tomada.

Se um mapa de classe específico precisar ser adicionado/modificado/removido da política atual de CoPP, ele deverá ser feito no modo de configuração no modo de mapa de política. Consulte o Guia de Configuração do Software Catalyst 6500 Release 15.0SY - Política de Plano de Controle (CoPP) para obter a sintaxe exata.

As classes de exceção padrão de CoPP têm estas descrições:

Caso	class-map name	Descrição
Falha de MTU (Unidade Máxima de Transmissão)	class-copp-mtu-fail	O tamanho do pacote excede o tamanho da MTU da interface de saída. Se o bit Don't Fragment não estiver definido, a fragmentação será necessária. Se o bit Não Fragmentar estiver definido, a mensagem Destino Inalcançável do Internet Control Message Protocol (ICMP) indica que "fragmentação necessária e DF definido" deve ser gerado e enviado de volta à origem. Referência: RFC-791, RFC-1191
Falha de TTL (Time To Live, tempo de vida útil)	class-copp-ttl-fail	TTL do pacote = 1 (para IPv4), Limite de saltos = 0 ou 1 (para IPv6) TTL = 0 (para IPv4) pode ser descartado no hardware imediatamente, pois o salto anterior deve destruir o pacote quando o TTL é reduzido para 0. Limite de saltos = 0 (para IPv6) é diferente de TTL = 0 porque é declarado em RFC-2460, seção 8.2 que "Diferentemente de IPv4, os nós IPv6 não são necessários para aplicar a duração máxima do pacote. Esse é o motivo pelo qual o campo Tempo de Vida do IPv4 foi renomeado como Limite de Saltos no IPv6". Isso significa que o pacote de entrada IPv6 com limite de salto = 0 ainda é válido e a mensagem ICMP deve ser enviada de volta. Referência: RFC-791, RFC-2460
Opções	class-copp-options	Pacote com opções (para IPv4), cabeçalho de extensão salto por salto (para IPv6). Por exemplo, Router Alert RFC-2113, Rota de origem estrita e assim por diante. Os cabeçalhos de extensão não são examinados ou processados por nenhum

		nó ao longo do caminho de entrega de um pacote, até que o pacote atinja o nó (ou cada um dos conjuntos de nós no caso de multicast) identificado no campo Endereço de destino do cabeçalho IPv6. A única exceção é o cabeçalho de opções de salto por salto, que transporta informações que devem ser examinadas e processadas por cada nó ao longo do caminho de entrega de um pacote, que inclui os nós origem e destino. O processamento de hardware em campos de opção não é suportado, ou seja, o processamento/comutação de software é necessário. Referência: RFC-791 / RFC-2460
Falha de Reverse Path Forwarding (RPF) (Unicast)	class-copp-ucast-rpf-fail	A verificação de RPF com falha do pacote é filtrada. No entanto, devido a recursos limitados no hardware, a verificação RPF não pode ser feita em hardware em certos casos (ou seja, mais de 16 interfaces RPF vinculadas a um IP). Quando isso acontece, o pacote é enviado ao software para uma verificação completa de RPF. O primeiro pacote de dados com falha de RPF (endereçado a um grupo multicast) é enviado ao software para que o processo de declaração de PIM (Protocol Independent Multicast) seja iniciado. Uma vez concluído o processo, um roteador/encaminhador designado é eleito. Se o próximo pacote (mesmo fluxo) não for proveniente do roteador designado, ele acionará uma falha de RPF e o hardware poderá descartá-lo imediatamente (para evitar um ataque de negação de serviço (DoS)).
Falha de RPF (Multicast)	class-copp-mcast-rpf-fail	O primeiro pacote de dados com falha de RPF (endereçado a um grupo multicast) é enviado ao software para que o processo de declaração de PIM seja iniciado. Uma vez concluído o processo, um roteador/encaminhador designado é eleito. Se o próximo pacote (mesmo fluxo) não for proveniente do roteador designado, ele acionará uma falha de RPF e o hardware poderá descartá-lo imediatamente (para evitar um ataque de DoS). No entanto, se a tabela de roteamento for atualizada, um novo roteador designado

		pode precisar ser escolhido (através de PIM-assert), o que significa que o pacote com falha de RPF precisa acessar o software (para que PIM-assert comece novamente). Para fazer isso, um vazamento periódico para o mecanismo de software (por fluxo) para o pacote com falha de RPF está disponível no hardware. Entretanto, se houver uma grande quantidade de fluxos, um vazamento periódico pode ser muito alto para o software lidar. O CoPP de hardware ainda é necessário para o pacote com falha de RPF de multicast. Referência: RFC-3704, RFC-2362
Não há suporte para reescrita de pacote de hardware	class-copp-unsupp-rewrite	Embora o hardware possa reescrever pacotes em vários casos, alguns casos simplesmente não podem ser feitos no projeto de hardware atual. E para esses, o hardware envia o pacote para o software.
ICMP sem rota ICMP acl-drop redirecionamento ICMP	class-copp-icmp-redirect-unreachable	Pacotes enviados ao software para a geração de mensagens ICMP. Como redirecionamento ICMP, destino ICMP inalcançável (por exemplo, host inalcançável ou administrativamente proibido). Referência: RFC-792 / RFC-2463
Cisco Express Forwarding (CEF) recebido (o IP de destino é o IP do roteador)	class-copp-receive	Se o IP de destino do pacote for um dos endereços IP do roteador (atingirá a adjacência de recepção do CEF), então o software deve processar o conteúdo.
CEF glean (o IP de destino pertence a uma rede do roteador)	class-copp-glean	Se o IP de destino do pacote pertencer a uma rede do roteador, mas não for resolvido (ou seja, nenhum acerto na tabela da Base de Informações de Encaminhamento (FIB)), ele atingirá a adjacência de Glean do CEF, sendo enviado para o software onde o procedimento de resolução será iniciado. Para IPv4, o mesmo fluxo continua a atingir o CEF glean até que o endereço seja resolvido. Para IPv6, uma entrada FIB temporária que corresponde ao IP de destino (e, em vez disso, aponta para derivação da adjacência) é instalada durante a resolução. Se não puder ser resolvido na duração especificada, a entrada FIB será removida (ou seja, o mesmo fluxo começa a pressionar CEF glean novamente).
Pacote destinado	class-copp-mcast-ip-control	O pacote de controle precisa ser

ao multicast IP 224.0.0.0/4		processado pelo software.
Pacote destinado ao multicast IP FF::/8	class-copp-mcast-ipv6-control	O pacote de controle precisa ser processado pelo software.
Pacote multicast que precisa ser copiado para o software	class-copp-mcast-copy	Em alguns casos, o pacote multicast precisa ser copiado para o software para uma atualização de estado (o pacote ainda é hardware ligado na mesma VLAN). Por exemplo, (*,G/m) apertou para entrada de modo denso, switchover SPT de rpf duplo.
Pacote multicast com erro na tabela FIB	class-copp-mcast-punt	O IP de destino (IP multicast) é uma falha na tabela FIB. O pacote é direcionado ao software.
Fonte diretamente conectada (IPv4)	class-copp-ip-connected	O tráfego multicast de fontes diretamente conectadas é enviado para o software onde um estado multicast pode ser criado (e instalado no hardware).
Fonte diretamente conectada (IPv6)	class-copp-ipv6-connected	O tráfego multicast de fontes diretamente conectadas é enviado para o software onde um estado multicast pode ser criado (e instalado no hardware).
Pacote de transmissão	class-copp-broadcast	Os pacotes de broadcast (por exemplo, IP/Não-IP com DMAC de broadcast e IP unicast com DMAC de multicast) são vazados para o software.
Protocolo desconhecido para (ou seja, não suportado por) em termos de switching de hardware	class-copp-unknown-protocol	O protocolo não IP, como o Internetwork Packet Exchange (IPX) e assim por diante, não será comutado por hardware. Eles são enviados para o software e encaminhados para lá.
Tráfego de dados multicast entrando pela porta roteada onde o PIM está desabilitado	class-copp-mcast-v4-data-on-routedPort	O tráfego de dados multicast que chega através de uma porta roteada (onde o PIM está desabilitado) vaza para o software. No entanto, não é necessário enviá-los para o software para que sejam descartados.
Tráfego de dados multicast entrando pela porta roteada onde o PIM está desabilitado	class-copp-mcast-v6-data-on-routedPort	O tráfego de dados multicast que chega através de uma porta roteada (onde o PIM está desabilitado) vaza para o software. No entanto, não é necessário enviá-los para o software para que sejam descartados.
Redirecionamento da ACL de entrada para ligar o pacote	class-copp-ucast-ingress-acl-bridged	O hardware tem 8 exceções relacionadas à ACL definidas pelo software através de um redirecionamento da ACL. Este se refere aos pacotes unicast ligados à CPU pela ACL por razões relacionadas à TCAM (Ternary Content Addressable Memory).

Redirecionamento de ACL de saída para ligar o pacote	class-copp-ucast-egress-acl-bridged	O hardware tem 8 exceções relacionadas à ACL definidas pelo software através de um redirecionamento da ACL. Este se refere aos pacotes unicast ligados à CPU pela ACL por razões relacionadas à TCAM (Ternary Content Addressable Memory).
Redirecionamento de ACL de transmissão para pacotes de ponte para CPU	class-copp-mcast-acl-bridged	O hardware tem 8 exceções relacionadas à ACL definidas pelo software através de um redirecionamento da ACL. Esta é relacionada ao processamento multicast.
Bridge ACL para CPU para processamento de balanceamento de carga do servidor	class-copp-slb	O hardware tem 8 exceções relacionadas à ACL definidas pelo software através de um redirecionamento da ACL. Este se refere a um redirecionamento de hardware para uma decisão de SLB (Server Load Balancing [balanceamento de carga do servidor]).
Redirecionamento de log da ACL	class-copp-vacl-log	O hardware tem 8 exceções relacionadas à ACL definidas pelo software através de um redirecionamento da ACL. Esta se refere ao redirecionamento de pacotes pela ACL da VLAN Access Control List (VACL) para a CPU do Cisco IOS? de registro.
Rastreamento de DHCP	class-copp-dhcp-snooping	Os pacotes rastreados por DHCP são redirecionados para a CPU para processamento de DHCP
Encaminhamento baseado em política MAC	class-copp-mac-pbf	O encaminhamento baseado em política deve ser feito na CPU, pois o hardware não é capaz de encaminhar pacotes nesse caso.
Controle de admissão de rede de admissão de IP	class-copp-ip-negotiation	Para fornecer acesso à rede com base nas credenciais antivírus do host, há validação de postura através de uma destas opções: (1) A interface L2 usará o IP da porta LAN (LPIP), onde os pacotes do Protocolo de Resolução de Endereços (ARP) são redirecionados para a CPU, (2) A interface L3 usa o IP do Gateway (GWIP). Após a validação, há a autenticação (*). Para uma interface L2, é o WebAuth, que executa a interceptação de pacotes HTTP e também pode executar o redirecionamento de URL (*). Para a interface L3, é AuthProxy.
Inspeção ARP dinâmica	class-copp-arp-snooping	Para evitar um ataque de envenenamento ARP (man-in-the-middle), a inspeção dinâmica ARP (também conhecida como Dynamic ARP Inspection (DAI)) valida as solicitações/respostas ARP quando

		intercepta e as processa na CPU contra uma destas: (1) ACLs ARP configuradas pelo usuário (para hosts configurados estaticamente), (2) vínculos de endereço MAC para endereço IP armazenados em um banco de dados confiável (ou seja, vínculos DHCP). Somente pacotes ARP válidos são usados para atualizar o cache ARP local ou encaminhados. O processo de validação requer o envolvimento da CPU dos pacotes ARP, o que significa que o CoPP de hardware é necessário para evitar um ataque de DoS.
ACL redireciona para CPU para WCCP	class-copp-wccp	Usado caso o pacote/fluxo precise ser redirecionado para a CPU para a decisão de encaminhamento do Web Cache Communication Protocol (WCCP).
A ACL redireciona para a CPU para a arquitetura de inserção de serviços (SIA)	class-copp-service-insert	Usado caso o pacote/fluxo precise ser redirecionado para a CPU para decisão de SIA.
Descoberta de rede IPv6	class-copp-nd	Para redirecionar o pacote de descoberta de rede IPv6 para a CPU para continuar o processo. Referência: RFC4861

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar se havia tráfego observado em qualquer um dos mapas de classe CoPP configurados, insira o comando **show policy-map control-plane**.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Proteção dos switches Cisco Catalyst 6500 Series usando políticas de plano de controle, limitação da taxa de hardware e listas de controle de acesso
- Guia de configuração do software Catalyst 6500 versão 15.0SY - Política de plano de controle (CoPP)
- Suporte Técnico e Documentação - Cisco Systems