Opte pela política plana do controle no exemplo de configuração do catalizador 6500/Sup2T e do catalizador 6880

Índice

Introdução

Este documento descreve em detalhe que tipos de tráfego são combinados contra os mapas de classe do padrão, que são parte do Catalyst 6500 Sup2T do padrão/a configuração CoPP do catalizador 6880 (Policiamento do plano de controle) que é configurada automaticamente no dispositivo. Isto é configurado a fim proteger seu CPU do sobrecarregamento.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

CoPP é permitido à revelia no Catalyst 6500/SUP2T e nos Catalyst 6880 Switch e baseado em um molde preconfigured. Algumas configurações de mapa de classe não têm as instruções compatível correspondentes devido ao fato de que capturam o tráfego não no Access Control List MAC/IP (ACL), mas um pouco nas exceções internas que estão sinalizadas pelo Forwarding Engine quando o tráfego é recebido pelo interruptor e por uma decisão de encaminhamento tomados.

Se um mapa de classe específico precisa de ser adicionado/alterado/removido da política atual de CoPP, a seguir deve ser feita do modo de configuração no modo do mapa de política. Veja o manual de configuração do software da liberação 15.0SY do Catalyst 6500 - Policiamento do plano de controle (CoPP) para a sintaxe exata.

As classes da exceção do padrão de CoPP têm estas descrições:

Caso	nome do mapa de classe	Descrição
Falha da unidade de transmissão máxima (MTU)	classe-copp-MTU-falha	O tamanho do pacote excede o tamanho do MTU da interface enviada. Se o bit do Don't Fragment não é ajustado, a fragmentação está exigida. Se o bit do Don't Fragment é ajustado, o mensagem de destinatário inalcançável do Internet Control Message Protocol (ICMP) indica que a “fragmentação necessária e o DF se ajustar” estão supostos para ser gerados para trás e enviado à fonte. Referência: RFC-791, RFC-1191
Falha do Time to Live (TTL)	classe-copp-TTL-falha	Pacote TTL=1 (para o IPv4), limite do salto = 0 ou 1 (para o IPv6) O TTL = 0 (para o IPv4) pode ser rejeitado no hardware imediatamente enquanto o salto precedente está suposto para destruir o pacote quando o TTL está decrescido a 0. O limite do salto = 0 (para o IPv6) é diferente de TTL = 0 porque se indica no RFC-2460, a seção 8.2 que “ao contrário do IPv4, os Nós do IPv6 não são exigidos reforçar a vida do pacote máximo. Aquela é a razão que o campo do Time to Live do IPv4 foi rebatizado limite do salto em IPv6". Isto significa que o pacote entrante do IPv6 com limite do salto = 0 é ainda válido, e o mensagem ICMP deve ser enviado

		para trás. Referência: RFC-791, RFC-2460
Opções	classe-copp-opções	Pacote com opções (para o IPv4), cabeçalho de extensão do salto a salto (para o IPv6). Por exemplo, RFC-2113 da alerta de roteador, rota de origem restrita, e assim por diante. Os cabeçalhos de extensão não estão examinados nem estão processados por todo o nó ao longo do trajeto da entrega de um pacote, até que o pacote alcance o nó (ou cada um do grupo de Nós no ofmulticast do caso) identificado no campo de endereço de destino do encabeçamento theIPv6. A única exceção é o encabeçamento das opções do salto a salto, que leva a informação que deve ser examinada e processado por cada nó ao longo do trajeto da entrega de um pacote, que inclui os nós de origem e de destino. O hardware que processa em campos de opção não é apoiado, isso é processamento do software/interruptor é precisado. Referência: RFC-791/RFC-2460
Falha do encaminhamento de caminho reverso (RPF) (unicast)	classe-copp-ucast-RPF-falha	A verificação RPF de falha do pacote é filtrada. Contudo, devido aos recursos limitados no hardware, a verificação RPF não pode ser feita no hardware em certos casos (isto é, mais de 16 relações RPF ligadas a um IP). Quando isso acontece, o pacote está enviado ao software para uma verificação RPF completa. O primeiro pacote de dados falhado RPF (endereçado a um grupo de transmissão múltipla) é enviado ao software para que a transmissão múltipla independente de protocolo (PIM) - afirma o processo para começar. O processo é feito uma vez, um roteador designado/remetente é elegido. Se o próximo pacote (o mesmo fluxo) não vem do roteador designado, provoca uma falha de RPF, e o hardware pode deixá-lo

		cair imediatamente (a fim impedir um ataque de recusa de serviço (DOS)).
Falha de RPF (Multicast)	classe-copp-mcast-RPF-falha	O primeiro pacote de dados falhado RPF (endereçado a um grupo de transmissão múltipla) é enviado ao software para que o processo da PIM-afirmação comece. O processo é feito uma vez, um roteador designado/remetente é elegido. Se o próximo pacote (o mesmo fluxo) não vem do roteador designado, provoca uma falha de RPF, e o hardware pode deixá-lo cair imediatamente (a fim impedir um ataque DoS). Contudo, se a tabela de roteamento é atualizada, um roteador designado novo pôde precisar de ser escolhido (através de PIM-afirme), que significasse que o pacote falhado RPF precisa de alcançar o software (para que PIM-afirme comece outra vez). A fim fazer isso, um escape periódico ao mecanismo de software (pelo fluxo) para o pacote RPF-falhado está disponível no hardware. Note embora, se há uma quantia enorme dos fluxos então que um escape periódico pode ser demasiado para que o software segure. O hardware CoPP é exigido ainda para o pacote falhado RPF do Multicast. Referência: RFC-3704, RFC-2362
Reescrita de pacote de informação do hardware não apoiada	classe-copp-unsupp-reescrita	Quando o hardware puder reescrever pacotes em vários casos, alguns casos apenas não podem ser feitos no projeto de hardware atual. E para aqueles, o hardware envia o pacote ao software.
Nenhum-rota ICMP ACL-gota ICMP Redirecionamento de ICMP	classe-copp-ICMP-reorientar-inacessível	Os pacotes enviaram ao software para a geração de mensagens ICMP. Como o redirecionamento de ICMP, destino ICMP inacessível (por exemplo. host inalcançável ou proibido administrativamente). Referência: RFC-792/RFC-2463
O Cisco Express Forwarding (CEF)	classe-copp-receba	Se o IP de destino do pacote é um dos endereços IP de Um ou Mais

recebe (o IP de destino é o IP do roteador)		Servidores Cisco ICM NT do roteador (baterá o CEF recebem a adjacência), a seguir o software está suposto para processar o índice.
O CEF recolhe (o IP de destino pertence a uma da rede do roteador)	classe-copp-recolha	Se o IP de destino do pacote pertence a uma da rede do roteador, mas não é resolved (isto é, nenhuma batida na tabela do banco de informação de encaminhamento (FIB)), baterá a adjacência glean CEF, sendo enviado ao software aonde o procedimento de resolução obterá começado. Para o IPv4, o mesmo fluxo continua a bater o CEF recolhe até que o endereço esteja resolved. Para o IPv6, um provisório MENTE a entrada que combina o IP de destino (e os pontos para deixar cair pelo contrário a adjacência) obtém instalada durante a definição. Se não se pode resolver na duração especificada, a entrada MENTIR está removida (isto é, os mesmos começos do fluxo para bater o CEF recolhem outra vez).
Pacote destinado ao IP de transmissão múltipla 224.0.0.0/4	classe-copp-mcast-IP-controle	O pacote de controle precisa de ser processado pelo software.
Pacote destinado ao IP de transmissão múltipla FF::/8	class-copp-mcast-ipv6-control	O pacote de controle precisa de ser processado pelo software.
Pacote de transmissão múltipla que precisa de ser copiado ao software	classe-copp-mcast-cópia	Em alguns casos, o pacote de transmissão múltipla precisa de ser copiado ao software para uma atualização do estado (o pacote é ainda hardware construído uma ponte sobre no mesmo VLAN). Por exemplo, (*, G/m) batido para a entrada do modo denso, switchover duplo-RPF SPT.
Pacote de transmissão múltipla que obtém uma falta na tabela FIB	classe-copp-mcast-pontapé	O IP de destino (IP de transmissão múltipla) é uma falta na tabela FIB. O pacote punted ao software.
Fonte diretamente conectada (IPv4)	classe-copp-IP-conectado	O tráfego multicast das fontes diretamente conectadas é enviado

		ao software onde um estado do Multicast pode ser criado (e instalado no hardware).
Fonte diretamente conectada (IPv6)	class-copp-ipv6-connected	O tráfego multicast das fontes diretamente conectadas é enviado ao software onde um estado do Multicast pode ser criado (e instalado no hardware).
Pacote de transmissão	classe-copp-transmissão	Os pacotes de transmissão (por exemplo, IP/Non-IP com transmissão DMAC e unicast IP com Multicast DMAC) são escapados ao software.
Desconhecido do protocolo a (isto é, unsupported por) em termos do switching de hardware	classe-copp-desconhecido-protocolo	O protocolo não-IP, tal como Trocas de Pacote Entre Redes IPX (IPX) e assim por diante, não será hardware comutado. São enviados ao software e obtêm enviados lá.
Tráfego de dados de transmissão múltipla que entra através da porta roteada onde o PIM é desabilitado	class-copp-mcast-v4-data-on-routedPort	O tráfego de dados de transmissão múltipla que entra através de uma porta roteada (onde o PIM é desabilitado) é escapado ao software. Contudo, não é necessário enviá-los ao software assim que são deixados cair.
Tráfego de dados de transmissão múltipla que entra através da porta roteada onde o PIM é desabilitado	class-copp-mcast-v6-data-on-routedPort	O tráfego de dados de transmissão múltipla que entra através de uma porta roteada (onde o PIM é desabilitado) é escapado ao software. Contudo, não é necessário enviá-los ao software assim que são deixados cair.
O ingresso ACL reorienta para construir uma ponte sobre o pacote	classe-copp-ucast-ingresso-ACL-construído uma ponte sobre	O hardware tem 8 exceções ACL-relacionadas ajustadas pelo software através de um ACL para reorientar. Este relaciona-se aos pacotes do unicast construídos uma ponte sobre o ao CPU pelo ACL para o Ternary Content Addressable Memory (TCAM) relacionou razões.
A saída ACL reorienta para construir uma ponte sobre o pacote	classe-copp-ucast-saída-ACL-construído uma ponte sobre	O hardware tem 8 exceções ACL-relacionadas ajustadas pelo software através de um ACL para reorientar. Este relaciona-se aos pacotes do unicast construídos uma ponte sobre o ao CPU pelo ACL para o Ternary Content Addressable Memory (TCAM) relacionou razões.
O mcast ACL reorienta aos	classe-copp-mcast-ACL-construído uma ponte sobre	O hardware tem 8 exceções ACL-relacionadas ajustadas pelo

pacotes de Bridge ao CPU		software através de um ACL para reorientar. Este relaciona-se ao processamento do Multicast.
Ponte ACL ao CPU para o processamento do Server Load Balancing	classe-copp-SLB	O hardware tem 8 exceções ACL-relacionadas ajustadas pelo software através de um ACL para reorientar. Este relaciona-se a um hardware reorienta para uma decisão do Server Load Balancing (SLB).
O log ACL VACL reorienta	classe-copp-VACL-log	O hardware tem 8 exceções ACL-relacionadas ajustadas pelo software através de um ACL para reorientar. Este relaciona-se ao redirecionamento de pacote pelo VLAN Access Control List (VACL) ACL ao CPU para o Cisco IOS? finalidades de registro.
Espião DHCP	classe-copp-DHCP-espião	O DHCP snooped pacotes é reorientado ao CPU para o processamento de DHCP
A política MAC baseou a transmissão	classe-copp-MAC-pbf	A transmissão baseada política deve ser feita no CPU desde que o hardware não é capaz enviar neste caso pacotes.
controle de admissão de rede da IP-admissão	classe-copp-IP-admissão	A fim fornecer o acesso de rede baseado nas credenciais do antivirus do host, há uma validação da postura através de uma destas opções: (1) a relação L2 usará IP da porta de LAN (LPIP), onde os pacotes do Address Resolution Protocol (ARP) são reorientados que ao CPU, (2) a relação L3 usa IP do gateway (GWIP). Após a validação, há a autenticação (*). Para uma relação L2 é WebAuth, que executa a intercepção do pacote de HTTP e pôde igualmente executar a reorientação URL (*). Para a relação L3, é AuthProxy.
Inspeção ARP dinâmica	classe-copp-ARP-espião	A fim impedir o ataque (homem-em--médio) do envenenamento ARP, inspeção ARP dinâmica (igualmente conhecida como a inspeção ARP dinâmica (DAI)) valida as requisições ARP/respostas por quando os intercepta e processa então no CPU contra um do estes: (1) configurado pelo usuário ARP ACL (para anfitriões estaticamente configurados), (2) MAC address

		aos emperramentos do endereço IP de Um ou Mais Servidores Cisco ICM NT armazenados no base de dados confiado (isto é, emperramentos DHCP). Somente os pacotes ARP válidos são usados para atualizar o cache ARP local ou enviados para fora. O processo de validação exige a participação dos pacotes ARP CPU, que significa que o hardware CoPP está precisado a fim impedir um ataque DoS.
O ACL reorienta ao CPU para o WCCP	classe-copp-WCCP	Usado caso que o pacote/fluxo precisa de ser reorientado ao CPU para a decisão de encaminhamento do Protocolo de Comunicação de Cache da Web (WCCP).
O ACL reorienta ao CPU para a arquitetura da inserção do serviço (o SIA)	classe-copp-serviço-inserção	Usado caso que o pacote/fluxo precisa de ser reorientado ao CPU para a decisão SIA.
Descoberta da rede do IPv6	classe-copp-nd	A fim reorientar o pacote da descoberta da rede do IPv6 ao CPU para processar mais. Referência: RFC4861

Verificar

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

A fim verificar se havia um tráfego observado em alguns dos mapas de classe configurados de CoPP, incorpore o comando do **controle plano do mapa de política da mostra**.

Troubleshooting

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

Informações Relacionadas

- Cisco Catalyst 6500 Series Switch de proteção usando o Policiamento do plano de controle, a taxa do hardware que limitam, e as listas de controle de acesso
- Manual de configuração do software da liberação 15.0SY do Catalyst 6500 - Policiamento do plano de controle (CoPP)

- Suporte Técnico e Documentação - Cisco Systems