Índice

Introdução

Este documento fornece um exemplo de configuração de alguns dos recursos de segurança da Camada 2, como segurança de portas, snooping de DHCP, inspeção de ARP (Address Resolution Protocol) dinâmica e proteção de origem de IP que podem ser implementados em switches de configuração fixa da Camada 3 Cisco Catalyst.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Cisco Catalyst 3750 Series Switch com versão 12.2(25)SEC2.

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.

Produtos Relacionados

Esta configuração também pode ser utilizada com o seguinte hardware:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3560-E Series Switches

- Cisco Catalyst 3750-E Series Switch

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Similar ao Roteadores, mergulhe 2 e os switch de camada 3 têm seus próprios grupos de exigências de segurança de rede. O Switches é suscetível a muitos dos mesmos ataques da camada 3 que o Roteadores. Contudo, o Switches e mergulha 2 do OSI Reference Model geralmente, é sujeito aos ataques de rede em maneiras diferentes. Eles incluem:

- **Excesso da tabela do Content Addressable Memory (CAM)**As tabelas do Content Addressable Memory (CAM) são limitadas em tamanho. Se bastante entradas estão incorporadas na tabela CAM antes que outras entradas estejam expiradas, a tabela CAM enche-se até o ponto que nenhuma entrada nova pode ser aceitada. Tipicamente, um intruso da rede inunda o interruptor com um grande número endereços de controle de acesso de mídia (MAC) do origem inválida até a tabela CAM enche-se acima. Quando isso ocorre, o interruptor inunda todas as portas com o tráfego de entrada porque não pode encontrar o número de porta para um endereço MAC particular na tabela CAM. O interruptor, essencialmente, atua como um hub. Se o intruso não mantém a inundação de endereços do origem inválida MAC, o interruptor cronometra eventualmente para fora umas entradas de endereço MAC mais idosas da tabela CAM e começa a atuar outra vez como um interruptor. As inundações do excesso da tabela CAM somente traficam dentro do VLAN local assim que o intruso vê somente o tráfego dentro do VLAN local a que ou são conectados.O ataque do excesso da tabela CAM pode ser abrandado configurando a Segurança de portas no interruptor. Esta opção prevê a especificação dos endereços MAC em uma porta do switch particular ou a especificação do número de endereços MAC que podem ser aprendidos por uma porta de switch. Quando um endereço MAC inválido é detectado na porta, o interruptor pode obstruir o MAC address de ofensa ou fechar a porta. A especificação de endereços MAC em portas de switch é uma solução demasiado incontrolável distante para um ambiente de produção. Um limite do número de endereços MAC em uma porta de switch é manejável. Mais administrativamente uma solução escalável é a aplicação da Segurança de porta dinâmica no interruptor. A fim executar a Segurança de porta dinâmica, especifique um número máximo de endereço MAC que seja instruído.
- **Falsificação do endereço de controle de acesso de mídia (MAC)**Os ataques de falsificação do Media Access Control (MAC) envolvem o uso de um MAC address conhecido de um outro host tentar fazer o alvo comutar os quadros dianteiros destinados para o host remoto ao atacante da rede. Quando um único quadro é enviado com o endereço de Ethernet da fonte do outro host, o atacante da rede overwrites a entrada de tabela CAM de modo que os pacotes do interruptor para a frente destinados para o host ao atacante da rede. Até que o host envie o tráfego, não recebe nenhum tráfego. Quando o host manda o tráfego, a entrada de tabela CAM está reescrita uma vez mais de modo que se mova de volta à porta original.Use os recursos de segurança de porta para abrandar ataques de falsificação MAC. A Segurança de portas fornece a capacidade de especificar o MAC address do sistema conectado a uma porta particular. Isto igualmente fornece a capacidade para especificar uma

ação para tomar se uma violação de Segurança de portas ocorre.

- **Falsificação do Address Resolution Protocol (ARP)**O ARP é usado para traçar o endereçamento de IP aos endereços MAC em um segmento da rede de área local onde os anfitriões da mesma sub-rede residam. Normalmente, um host manda um pedido do ARP de transmissão encontrar o MAC address de um outro host com um endereço IP particular, e uma reação ARP vem do host cujo o endereço combina o pedido. O host de pedido põe em esconderijo então esta reação ARP. Dentro do protocolo ARP, uma outra disposição é feita para que os anfitriões executem respostas ARP espontâneas. As respostas ARP espontâneas são chamadas o ARP gratuito (GARP). O GARP pode ser explorado maliciosamente por um atacante ao spoof a identidade de um endereço IP de Um ou Mais Servidores Cisco ICM NT em um segmento de LAN. Isto é usado tipicamente ao spoof a identidade entre dois anfitriões ou todo o tráfego a e de um gateway padrão em um ataque “homem-em--médio”.Quando uma resposta ARP crafted, um atacante da rede pode fazer seu sistema parecer ser o host de destino procurado pelo remetente. A resposta de ARP faz com que o emissor armazene o endereço MAC do sistema do agressor no cache de ARP. Este MAC address é armazenado igualmente pelo interruptor em sua tabela CAM. Ao agir dessa forma, o agressor de rede inseriu o endereço MAC do seu próprio sistema na tabela CAM do switch e no cache de ARP do emissor. Isso permite que ele intercepte frames destinados ao host que está falsificando.Mantenha temporizadores no menu da configuração da interface pode ser usado para abrandar ataques de falsificação ARP ajustando o intervalo de tempo que uma entrada ficará no cache ARP. Contudo, mantenha temporizadores são sós insuficiente. A alteração do tempo de expiração do cache ARP em todos os sistemas finais é exigida assim como entradas de ARP estáticas. Uma outra solução que possa ser usada para abrandar a vária rede ARP-baseada explora, é o uso da espião DHCP junto com a inspeção ARP dinâmica. Estas características do catalizador validam pacotes ARP em uma rede e permitem a intercepção, registrando, e rejeitando dos pacotes ARP com endereço MAC inválido aos emperramentos do endereço IP de Um ou Mais Servidores Cisco ICM NT.A espião DHCP filtra confiou mensagens DHCP a fim fornecer a Segurança. Então, estas mensagens são usadas para construir e manter uma tabela de ligação da espião DHCP. A espião DHCP considera os mensagens DHCP que originam de toda a porta do USER-revestimento que não for uma porta de servidor DHCP como o não-confiável. De uma perspectiva da espião DHCP, estas portas não confiáveis do USER-revestimento não devem enviar o tipo de servidor DHCP respostas, tais como DHCPOFFER, DHCPACK, ou DHCPNAK. A tabela de ligação da espião DHCP contém o MAC address, o endereço IP de Um ou Mais Servidores Cisco ICM NT, o Lease Time, o tipo obrigatório, o número de VLAN, e a informação da relação que corresponde às interfaces não confiável locais de um interruptor. A tabela de ligação da espião DHCP não contém a informação sobre os anfitriões interconectados com uma relação confiada. Uma interface não confiável é uma relação configurada para receber mensagens fora da rede ou do Firewall. Uma relação confiada é uma relação que seja configurada para receber - somente mensagens de dentro da rede. A tabela de ligação da espião DHCP pode conter dinâmico e o endereço MAC estático aos emperramentos do endereço IP de Um ou Mais Servidores Cisco ICM NT.A inspeção ARP dinâmica determina a validez de um pacote ARP baseado no MAC address válido aos emperramentos do endereço IP de Um ou Mais Servidores Cisco ICM NT armazenados em um banco de dados da espião DHCP. Adicionalmente, a inspeção ARP dinâmica pode validar os pacotes ARP baseados no Access Control Lists (ACLs) dos configuráveis pelo usuário. Isto permite a inspeção dos pacotes ARP para os anfitriões que usam estaticamente endereços IP configurados. A inspeção ARP dinâmica permite o uso da porta per. e das listas

de controle de acesso VLAN (PACL) limitar pacotes ARP para endereços IP de Um ou Mais Servidores Cisco ICM NT específicos aos endereços específicos MAC.
- **Inanição do protocolo de configuração dinâmica host (DHCP)**Um ataque da inanição DHCP trabalha pela transmissão das requisições DHCP com endereços falsificado MAC. Se bastante pedidos são enviados, o atacante da rede pode esgotar o espaço de endereços disponível aos servidores DHCP por um período de tempo. O atacante da rede pode então estabelecer um servidor DHCP desonesto em seu sistema e responder às requisições DHCP novas dos clientes na rede. Com a colocação de um servidor DHCP desonesto na rede, um atacante da rede pode fornecer clientes os endereços e a outra informação de rede. Porque as respostas de DHCP incluem tipicamente o gateway padrão e a informação de servidor de DNS, o atacante da rede pode fornecer seu próprio sistema como o gateway padrão e o servidor DNS. Isto conduz a um ataque que envolva pessoas. Contudo, a exaustão de todos os endereços de DHCP não é exigida para introduzir um servidor DHCP desonesto.Os recursos adicionais nas Catalyst famílias de switch, tais como a espião DHCP, podem ser usados para ajudar a guardar contra um ataque da inanição DHCP. A espião DHCP é uns recursos de segurança que filtrem mensagens DHCP não confiáveis e construam e mantenham uma tabela de ligação da espião DHCP. A tabela de ligação contém a informação tal como o MAC address, o endereço IP de Um ou Mais Servidores Cisco ICM NT, o Lease Time, o tipo obrigatório, o número de VLAN e a informação da relação que corresponde às interfaces não confiável locais de um interruptor. As mensagens não confiáveis são aquelas recebidas fora da rede ou do Firewall. As interfaces de switch não confiáveis são umas que são configuradas para receber tais mensagens fora da rede ou do Firewall.Outras características do Catalyst Switch, tais como a proteção de origem de IP, podem fornecer a defesa adicional contra ataques tais como a inanição e a falsificação de IP DHCP. Similar à espião DHCP, a proteção de origem de IP é permitida em portas não confiáveis da camada 2. Todo o tráfego IP é obstruído inicialmente, à exceção dos pacotes DHCP capturados pelo processo da espião DHCP. Uma vez que um cliente recebe um endereço IP válido do servidor DHCP, um PACL está aplicado à porta. Isto restringe o tráfego do IP de cliente 2 aqueles endereços IP de origem configurados no emperramento. Todo o outro tráfego IP com um endereço de origem a não ser os endereços no emperramento é filtrado.

Configurar

Nesta seção, você é presentado com a informação para configurar a Segurança de portas, a espião DHCP, recursos de segurança dinâmicos da inspeção ARP e da proteção de origem de IP.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

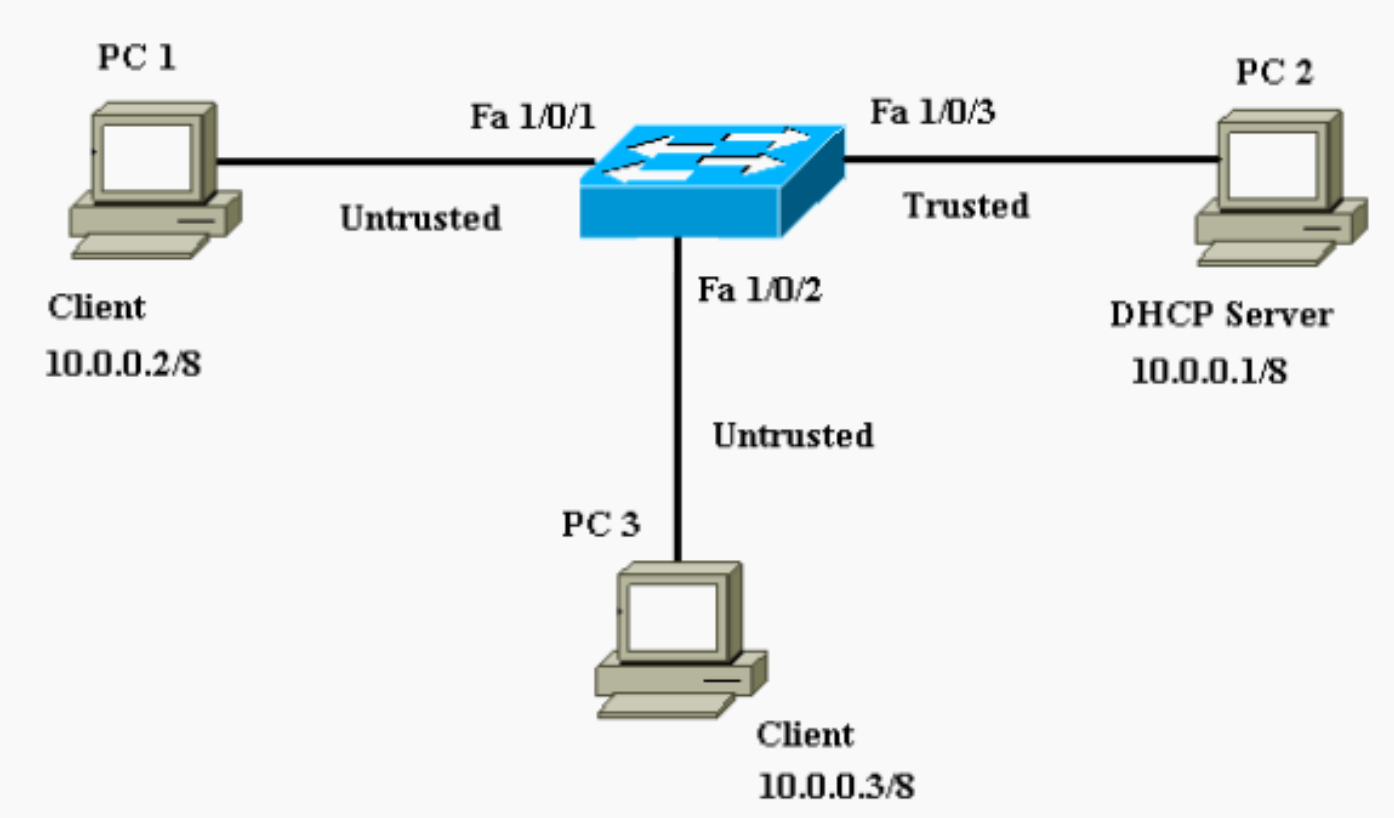
As configurações do Catalyst 3750 Switch contêm estes:

- Segurança da porta
- Espião DHCP
- Inspeção ARP dinâmica
- Proteção de origem de IP

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

- O PC1 e o PC3 são clientes conectados ao interruptor.
- O PC2 é um servidor DHCP conectado ao interruptor.
- Todas as portas do interruptor estão no mesmo VLAN (VLAN1).
- O servidor DHCP é configurado para atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes baseados em seus endereços MAC.



Segurança da porta

Você pode usar os recursos de segurança de porta para limitar e identificar endereços MAC das estações permitidas alcançar a porta. Isto restringe a entrada a uma relação. Quando você atribui endereços MAC seguros a uma porta segura, a porta não envia pacotes com endereços de origem fora do grupo de endereços definidos. Se você limita o número de endereços MAC seguros a um e atribui um único endereço MAC seguro, a estação de trabalho anexada a essa porta está assegurada a largura de banda total da porta. Se uma porta está configurada enquanto uma porta segura e o número máximo de endereços MAC seguros estão alcançados, quando o MAC address de uma estação que tente alcançar a porta é diferente de alguns dos endereços MAC seguros identificados, uma violação de segurança ocorre. Também, se uma estação com um endereço MAC seguro configurado ou aprendido em uma porta segura tenta alcançar uma outra porta segura, uma violação é embandeirada. À revelia, a porta fechou quando o número máximo de endereços MAC seguros é excedido.

Nota: Quando um Catalyst 3750 Switch se junta a uma pilha, o interruptor novo recebe os endereços seguros configurados. Todos os endereços seguros dinâmicos são transferidos pelo membro de pilha novo dos outros membros de pilha.

Consulte as Diretrizes de Configuração para obter as diretrizes de configuração da segurança de portas.

Aqui, os recursos de segurança de porta são mostrados configurados nos FastEthernet 1/0/2 de

relação. À revelia, o número máximo de endereços MAC seguros para a relação é uma. Você pode emitir o **comando interface da Segurança de portas da mostra** a fim verificar o estado da Segurança de portas para uma relação.

segurança da porta

```
Cat3750#show port-security interface fastEthernet 1/0/2Port
Security              : DisabledPort Status                :
Secure-downViolation Mode             : ShutdownAging Time
: 0 minsAging Type                 : AbsoluteSecureStatic
Address Aging : DisabledMaximum MAC Addresses      : 1Total
MAC Addresses        : 0Configured MAC Addresses   : 0Sticky
MAC Addresses       : 0Last Source Address:Vlan   :
0000.0000.0000:0Security Violation Count   : 0!--- Default
port security configuration on the switch.Cat3750#conf tEnter
configuration commands, one per line.  End with
CNTL/Z.Cat3750(config)#interface fastEthernet
1/0/2Cat3750(config-if)#switchport port-security Command
rejected: FastEthernet1/0/2 is a dynamic port.!--- Port
security can only be configured on static access ports or
trunk ports.Cat3750(config-if)#switchport mode access!---
Sets the interface switchport mode as access. Cat3750(config-
if)#switchport port-security!--- Enables port security on the
interface. Cat3750(config-if)#switchport port-security mac-
address 0011.858D.9AF9!--- Sets the secure MAC address for
the interface.Cat3750(config-if)#switchport port-security
violation shutdown!--- Sets the violation mode to shutdown.
This is the default mode.Cat3750#!--- Connected a different
PC (PC 4) to the FastEthernet 1/0/2 port !--- to verify the
port security feature.00:22:51: %PM-4-ERR_DISABLE: psecure-
violation error detected on Fa1/0/2, putting Fa1/0/2 in err-
disable state00:22:51: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
0011.8565.4B75 on port FastEthernet1/0/2.00:22:52:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/2, changed state to down00:22:53: %LINK-3-
UPDOWN: Interface FastEthernet1/0/2, changed state to down!--
- Interface shuts down when a security violation is
detected.Cat3750#show interfaces fastEthernet
1/0/2FastEthernet1/0/2 is down, line protocol is down (err-
disabled)!--- Output Suppressed. !--- The port is shown
error-disabled. This verifies the configuration.!--- Note:
When a secure port is in the error-disabled state, !--- you
can bring it out of this state by entering !--- the
errdisable recovery cause psecure-violation global
configuration command, !--- or you can manually re-enable it
by entering the !--- shutdown and no shutdown interface
configuration commands.Cat3750#show port-security interface
fastEthernet 1/0/2Port Security              : EnabledPort
Status                : Secure-shutdownViolation Mode
: ShutdownAging Time                 : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC
Addresses      : 1Total MAC Addresses        : 1Configured
MAC Addresses   : 1Sticky MAC Addresses       : 0Last Source
Address:Vlan   : 0011.8565.4B75:1Security Violation Count   :
1
```

Nota: Os mesmos endereços MAC não devem ser configurados como seguro e o endereço MAC estático em portas diferentes de um interruptor.

Quando um telefone IP é conectado a um interruptor através do switchport configurado para a Voz VLAN, o telefone envia pacotes de CDP do sem etiqueta e pacotes de CDP etiquetados da

Voz. O MAC address do telefone IP é aprendido assim no PVID e no VVID. Se o número apropriado de endereços seguros não é configurado, você pode receber um Mensagem de Erro similar a esta mensagem:

```
Cat3750#show port-security interface fastEthernet 1/0/2Port Security              : DisabledPort Status
: Secure-downViolation Mode            : ShutdownAging Time                 : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC Addresses      : 1Total MAC Addresses        :
0Configured MAC Addresses   : 0Sticky MAC Addresses       : 0Last Source Address:Vlan   :
0000.0000.0000:0Security Violation Count   : 0!--- Default port security configuration on the
switch.Cat3750#conf tEnter configuration commands, one per line.  End with
CNTL/Z.Cat3750(config)#interface fastEthernet 1/0/2Cat3750(config-if)#switchport port-security Command
rejected: FastEthernet1/0/2 is a dynamic port.!--- Port security can only be configured on static access
ports or trunk ports.Cat3750(config-if)#switchport mode access!--- Sets the interface switchport mode as
access. Cat3750(config-if)#switchport port-security!--- Enables port security on the interface.
Cat3750(config-if)#switchport port-security mac-address 0011.858D.9AF9!--- Sets the secure MAC address
for the interface.Cat3750(config-if)#switchport port-security violation shutdown!--- Sets the violation
mode to shutdown. This is the default mode.Cat3750#!--- Connected a different PC (PC 4) to the
FastEthernet 1/0/2 port !--- to verify the port security feature.00:22:51: %PM-4-ERR_DISABLE: psecure-
violation error detected on Fa1/0/2, putting Fa1/0/2 in err-disable state00:22:51: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0011.8565.4B75 on port
FastEthernet1/0/2.00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/2, changed
state to down00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed state to down!--- Interface
shuts down when a security violation is detected.Cat3750#show interfaces fastEthernet
1/0/2FastEthernet1/0/2 is down, line protocol is down (err-disabled)!--- Output Suppressed. !--- The port
is shown error-disabled. This verifies the configuration.!--- Note: When a secure port is in the error-
disabled state, !--- you can bring it out of this state by entering !--- the errdisable recovery cause
psecure-violation global configuration command, !--- or you can manually re-enable it by entering the !--
- shutdown and no shutdown interface configuration commands.Cat3750#show port-security interface
fastEthernet 1/0/2Port Security              : EnabledPort Status                : Secure-
shutdownViolation Mode             : ShutdownAging Time                : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC Addresses      : 1Total MAC Addresses        :
1Configured MAC Addresses   : 1Sticky MAC Addresses       : 0Last Source Address:Vlan   :
0011.8565.4B75:1Security Violation Count   : 1
```

Você deve ajustar o máximo permitido endereços seguros na porta a dois (para o telefone IP) mais o número máximo de endereços seguros permitidos no acesso VLAN a fim resolver esta edição.

Consulte Configuração da Segurança de Portas para obter mais informações.

Espião DHCP

A espião DHCP atua como um Firewall entre host não confiável e servidores DHCP. Você usa a espião DHCP para diferenciar-se entre as interfaces não confiável conectadas ao utilizador final e as relações confiadas conectadas ao servidor DHCP ou a um outro interruptor. Quando um switch recebe um pacote em uma interface não confiável e a interface pertence a uma VLAN com snooping de DHCP habilitado, o switch compara o endereço MAC de origem e o endereço de hardware do cliente DHCP. Se os endereços combinam (o padrão), o interruptor para a frente o pacote. Se os endereços não combinam, o interruptor deixa cair o pacote. O interruptor deixa cair um pacote DHCP quando uma destas situações ocorre:

- Um pacote de um servidor DHCP, tal como um DHCPOFFER, pacote DHCPACK, DHCPNAK, ou DHCPLEASEQUERY, é recebido fora da rede ou do Firewall.
- Um pacote é recebido em uma interface não confiável, e o endereço MAC de origem e o endereço do hardware DHCP Client não combinam.
- O interruptor recebe um mensagem de transmissão DHCPRELEASE ou DHCPDECLINE que tenha um MAC address no banco de dados de ligação da espião DHCP, mas a informação

da relação no banco de dados de ligação não combina a relação em que a mensagem foi recebida.
- Um agente de transmissão de DHCP para a frente um pacote DHCP, que inclua um endereço IP de Um ou Mais Servidores Cisco ICM NT do agente de transmissão que não seja 0.0.0.0, ou o agente de transmissão para a frente um pacote que inclua a informação option-82 a uma porta não-confiável.

Consulte as Diretrizes de Configuração do Snooping de DCHP para obter as diretrizes de configuração do snooping de DHCP.

Nota: Para que a espião DHCP funcione corretamente, todos os servidores DHCP devem ser conectados ao interruptor através das relações confiadas.

Nota: Em uma pilha do interruptor com Catalyst 3750 Switch, a espião DHCP é controlada no mestre da pilha. Quando um interruptor novo se junta à pilha, o interruptor recebe a configuração da espião DHCP do mestre da pilha. Quando um membro deixa a pilha, todos os emperramentos da espião DHCP associaram com a idade do interruptor para fora.

Nota: A fim assegurar-se de que o Lease Time no banco de dados seja exato, Cisco recomenda que você permite e configura o NTP. Quando o NTP está configurado, o switch insere as alterações de ligação no arquivo de ligação somente quando o relógio do sistema do switch está sincronizado com o NTP.

Os servidores DHCP desonestos podem ser abrandados por características da espião DHCP. O comando **ip dhcp snooping** é executado para habilitar o DHCP globalmente no switch. Quando configuradas com espião DHCP, todas as portas no VLAN são não confiáveis para respostas DHCP. Aqui, somente a interface fastethernet 1/0/3 conectada ao servidor DHCP é configurada como confiado.

Espião DHCP

```
Cat3750#conf tEnter configuration commands, one per line.
End with CNTL/Z.Cat3750(config)#ip dhcp snooping!--- Enables
DHCP snooping on the switch. Cat3750(config)#ip dhcp snooping
vlan 1!--- DHCP snooping is not active until DHCP snooping is
enabled on a VLAN.Cat3750(config)#no ip dhcp snooping
information option!--- Disable the insertion and removal of
the option-82 field, if the !--- DHCP clients and the DHCP
server reside on the same IP network or
subnet.Cat3750(config)#interface fastEthernet
1/0/3Cat3750(config-if)#ip dhcp snooping trust!--- Configures
the interface connected to the DHCP server as
trusted.Cat3750#show ip dhcp snoopingSwitch DHCP snooping is
enabledDHCP snooping is configured on following
VLANs:1Insertion of option 82 is disabledOption 82 on
untrusted port is not allowedVerification of hwaddr field is
enabledInterface                    Trusted     Rate limit
(pps)------------------------     -------     ---------------
-FastEthernet1/0/3            yes         unlimited!---
Displays the DHCP snooping configuration for the
switch.Cat3750#show ip dhcp snooping bindingMacAddress
IpAddress        Lease(sec)  Type           VLAN  Interface--
---------------  --------------  ----------  -------------
----  --------------------00:11:85:A5:7B:F5     10.0.0.2
86391       dhcp-snooping  1
FastEtheret1/0/100:11:85:8D:9A:F9     10.0.0.3        86313
dhcp-snooping  1    FastEtheret1/0/2Total number of bindings:
2!--- Displays the DHCP snooping binding entries for the
```

```
switch.Cat3750#!--- DHCP server(s) connected to the untrusted
port will not be able !--- to assign IP addresses to the
clients.
```

Consulte Configuração de Recursos de DHCP para obter mais informações.

Inspeção ARP dinâmica

A inspeção ARP dinâmica é uns recursos de segurança que validem pacotes ARP em uma rede. Intercepta, logs, e rejeita pacotes ARP com as bindings do endereço IP-à-MAC inválidas. Esta capacidade protege a rede de determinados ataques que envolva pessoas.

A inspeção ARP dinâmica assegura-se de que somente as requisições ARP e as respostas válidas estejam retransmitidas. O interruptor executa estas atividades:

- Intercepta todas as requisições ARP e respostas em portas não-confiável
- Verifica que cada um destes pacotes interceptados tem uma binding do endereço IP-à-MAC válida antes que atualize o cache ARP local ou antes que ele para a frente o pacote ao destino apropriado
- Deixa cair pacotes ARP inválidos

A inspeção ARP dinâmica determina a validez de um pacote ARP baseado nas bindings do endereço IP-à-MAC válidas armazenadas em um banco de dados confiado, o banco de dados de ligação da espião DHCP. Este banco de dados está construído pela espião DHCP se a espião DHCP é permitida nos VLAN e no interruptor. Se o pacote ARP é recebido em uma relação confiada, o interruptor para a frente o pacote sem algumas verificações. Em interfaces não confiável, o interruptor para a frente o pacote somente se é válido.

Nos ambientes NON-DHCP, a inspeção ARP dinâmica pode validar pacotes ARP contra o configurado pelo usuário ARP ACL para anfitriões com estaticamente endereços IP configurados. Você pode executar o comando de configuração global **arp access-list** para definir uma ACL de ARP. O ARP ACL toma a precedência sobre entradas no banco de dados de ligação da espião DHCP. O interruptor usa ACL somente se você emite o comando global configuration **vlan do filtro da inspeção IP arp** a fim configurar os ACL. O interruptor compara primeiramente pacotes ARP ao configurado pelo usuário ARP ACL. Se o ARP ACL nega o pacote ARP, o interruptor igualmente nega o pacote mesmo se um emperramento válido existe no banco de dados povoado pela espião DHCP.

Consulte as Diretrizes de Configuração da Inspeção de ARP Dinâmica para obter as diretrizes de configuração da inspeção de ARP dinâmica.

O comando global configuration **vlan da inspeção IP arp** é emitido a fim permitir a inspeção ARP dinâmica em uma base do VLAN per. Aqui, somente a interface fastethernet 1/0/3 conectada ao servidor DHCP é configurada como confiado com o **comando trust da inspeção IP arp**. O snooping de DHCP deve ser habilitado para permitir os pacotes de ARP com endereços IP atribuídos dinamicamente. Consulte a seção Snooping de DHCP deste documento para obter informações de configuração do snooping de DHCP.

Inspeção ARP dinâmica

```
Cat3750#conf tEnter configuration commands, one per line.
End with CNTL/Z.Cat3750(config)#ip arp inspection vlan 1!---
Enables dynamic ARP inspection on the
VLAN.Cat3750(config)#interface fastEthernet
```

```
1/0/3Cat3750(config-if)#ip arp inspection trust!---
Configures the interface connected to the DHCP server as
trusted.Cat3750#show ip arp inspection vlan 1Source Mac
Validation      : DisabledDestination Mac Validation :
DisabledIP Address Validation      : Disabled Vlan
Configuration    Operation   ACL Match          Static ACL --
--     -------------    ---------   ---------          ------
----    1     Enabled          Active Vlan     ACL Logging
DHCP Logging ----     -----------      ------------    1
Deny             Deny!--- Verifies the dynamic ARP inspection
configuration.Cat3750#
```

Consulte Configurando a Inspeção de ARP Dinâmica para obter mais informações.

Proteção de origem de IP

A proteção de origem de IP é uns recursos de segurança que os filtros trafiquem baseado no banco de dados de ligação da espião DHCP e em emperramentos manualmente configurados do origem de IP a fim restringir o tráfego IP em interfaces de camada 2 NON-roteados. Você pode usar a proteção de origem de IP para impedir os ataques do tráfego causados quando um host tenta usar o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu vizinho. A proteção de origem de IP impede a falsificação IP/MAC.

Você pode permitir a proteção de origem de IP quando a espião DHCP é permitida em uma interface não confiável. Depois que a proteção de origem de IP é permitida em uma relação, o interruptor obstrui todo o tráfego IP recebido na relação, à exceção dos pacotes DHCP permitidos pela espião DHCP. Uma porta ACL é aplicada à relação. A porta ACL permite somente o tráfego IP com um endereço IP de origem na tabela de ligação do origem de IP e nega todo tráfego restante.

A tabela de ligação do origem de IP tem os emperramentos que são aprendidos pela espião DHCP ou configurados manualmente (emperramentos da fonte do IP Estático). Uma entrada nesta tabela tem um endereço IP de Um ou Mais Servidores Cisco ICM NT, seu MAC address associado, e seu número de VLAN associado. O interruptor usa a tabela de ligação do origem de IP somente quando a proteção de origem de IP é permitida.

Você pode configurar a proteção de origem de IP com a filtragem de endereços IP de origem ou com a filtragem de endereços IP e MAC de origem. Quando a proteção de origem de IP é permitida com esta opção, o tráfego IP está filtrado com base no endereço IP de origem. Do interruptor o tráfego IP para a frente quando o endereço IP de origem combinar uma entrada no banco de dados de ligação da espião DHCP ou um emperramento na tabela de ligação do origem de IP. Quando a proteção de origem de IP é permitida com esta opção, o tráfego IP está filtrado com base nos endereços IP e MAC da fonte. O interruptor trafica para a frente somente quando os endereços IP e MAC da fonte combinam uma entrada na tabela de ligação do origem de IP.

Nota: A proteção de origem de IP é apoiada somente em portas da camada 2, que inclui o acesso e as portas de tronco.

Consulte as Diretrizes de Configuração da Proteção de Origem de IP para obter as diretrizes de configuração da proteção de origem de IP.

Aqui, a proteção de origem de IP com filtragem de IP de origem é configurada na interface FastEthernet 1/0/1 com o comando **ip verify source**. Quando a proteção de origem de IP com filtragem de IP de origem é habilitada em uma VLAN, o snooping de DHCP deve ser habilitado na

VLAN de acesso à qual a interface pertence. Execute o comando **show ip verify source** para verificar a configuração da proteção de origem de IP no switch.

Proteção de origem de IP

```
Cat3750#conf tEnter configuration commands, one per line.
End with CNTL/Z.Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1!--- See the DHCP
Snooping section of this document for !--- DHCP snooping
configuration information.Cat3750(config)#interface
fastEthernet 1/0/1Cat3750(config-if)#ip verify source!---
Enables IP source guard with source IP filtering.Cat3750#show
ip verify sourceInterface  Filter-type  Filter-mode  IP-
address       Mac-address        Vlan---------  -----------
-----------  ---------------  -----------------  -----Fa1/0/1
ip           active       10.0.0.2
1!--- For VLAN 1, IP source guard with IP address filtering
is configured !--- on the interface and a binding exists on
the interface.Cat3750#
```

Consulte Entendendo a Proteção de Origem de IP para obter mais informações.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

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

Informações Relacionadas

- Protegendo redes com VLANs privados e listas de controle de acesso de VLAN
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems