Usar o Guia de Fortalecimento do Cisco IOS XE

Contents

Introdução

Este documento descreve informações para proteger os dispositivos do sistema Cisco IOS® XE, o que aumenta a segurança geral da documentação da rede.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estruturado em torno dos três planos nos quais as funções de um dispositivo de rede podem ser categorizadas, este documento fornece uma visão geral de cada recurso incluído e referências a itens relacionados.

Os três planos funcionais de uma rede; plano de gerenciamento, plano de controle e plano de dados, cada um fornece uma funcionalidade diferente que precisa ser protegida.

1. Plano de gerenciamento - O plano de gerenciamento gerencia o tráfego que é enviado para o dispositivo Cisco IOS XE e é composto de aplicativos e protocolos como Secure Shell (SSH) e Simple Network Management Protocol (SNMP).
2. Plano de controle – O plano de controle de um dispositivo de rede processa o tráfego essencial para manter a funcionalidade da infraestrutura de rede. O plano do controle consiste em aplicações e em protocolos entre dispositivos de rede, que inclui o Border Gateway Protocol (BGP), assim como os protocolos Interior Gateway Protocols (IGP) como o Enhanced Interior Gateway Routing Protocol (EIGRP) e o Open Shortest Path First (OSPF).
3. Plano de dados – O plano de dados encaminha os dados através de um dispositivo de rede. O plano de dados não inclui o tráfego enviado para o dispositivo Cisco IOS XE local.

   A cobertura dos recursos de segurança neste documento fornece frequentemente bastante detalhes para que você configure a característica. Contudo, nos casos onde não faz, a característica é explicada de tal maneira que você pode avaliar se a atenção adicional à característica está exigida. Sempre que possível e apropriado, este documento contém as recomendações que, se executadas, ajudam a fixar a rede.

Fixe operações

As operações de rede seguras são um assunto substancial. Embora a maior parte deste documento seja dedicada à configuração segura de um dispositivo Cisco IOS XE, as configurações sozinhas não protegem completamente uma rede. Os procedimentos operacionais no uso na rede contribuem tanto quanto à segurança quanto a configuração dos dispositivos subjacentes.

Estes assuntos contêm as recomendações operacionais que você é recomendado executar. Estes assuntos destacam áreas crítica específicas das operações de rede e não são detalhados.

Monitore Recomendações de Segurança da Cisco e respostas

A equipe da resposta de incidentes de segurança de produto Cisco (PSIRT) cria e mantém as publicações, referidas geralmente como informativos psirt, para edições relacionadas à segurança nos produtos da Cisco. O método usado para uma comunicação de edições menos severas é a resposta do Cisco Security. As recomendações e respostas de segurança estão disponíveis em Recomendações e respostas de segurança da Cisco

Informações adicionais sobre esses veículos de comunicação estão disponíveis na Política de Vulnerabilidade de Segurança da Cisco

A fim manter uma rede segura, você precisa de estar ciente das Recomendações de Segurança da Cisco e das respostas que foram liberadas. Você precisa de ter o conhecimento de uma vulnerabilidade antes que a ameaça que possa levantar a uma rede possa ser avaliada. Consulte Triagem de riscos para anúncios de vulnerabilidade de segurança para obter assistência neste processo de avaliação.

Entrega de Autenticação, Autorização e Relatório

A estrutura de autenticação, autorização e contabilização (AAA) é fundamental para proteger os dispositivos de rede. A estrutura AAA fornece a autenticação das sessões de gerenciamento e pode igualmente limitar usuários a comandos específico, definidos pelos administradores e aos comandos all do registro inscritos por todos os usuários. Consulte a seção Autenticação, autorização e contabilização deste documento para obter mais informações sobre como utilizar a estrutura de AAA.

Centralize a coleção e a monitoração do registro

Para obter conhecimento sobre eventos atuais, emergentes e históricos relacionados a incidentes de segurança, sua empresa deve ter uma estratégia unificada para registro e correlação de eventos. Esta estratégia deve entregar o registo de todos os dispositivos de rede e usar capacidades pré-embaladas e customizáveis da correlação.

Depois que o registo centralizado é executado, você deve desenvolver uma aproximação

estruturada para registrar o seguimento da análise e do incidente. Baseado nas necessidades de sua organização, esta aproximação pode variar de uma revisão diligente simples dos dados de registro a análise baseado em regras avançada.

Consulte a seção Logging Best Practices deste documento para obter mais informações sobre como implementar o registro em dispositivos de rede Cisco IOS XE.

Use protocolos seguros quando possível

Muitos protocolos são usados a fim levar dados de gerenciamento de redes sensíveis. Você deve usar protocolos seguros sempre que possível. Uma escolha segura do protocolo inclui o uso do SSH em vez do telnet de modo que os dados de autenticação e a informação de gerenciamento sejam cifrados. Além, você deve usar protocolos de transferência de arquivo seguros quando você copia dados de configuração. Um exemplo é o uso do protocolo da cópia segura (SCP) no lugar do FTP ou do TFTP.

Consulte a seção Secure Interative Management Sessions deste documento para obter mais informações sobre o gerenciamento seguro de dispositivos Cisco IOS XE.

Ganhe a visibilidade do tráfego com NetFlow

O NetFlow permite-o de monitorar fluxos de tráfego na rede. Pretendeu originalmente exportar a informação de tráfego para aplicativos de gerenciamento de rede, NetFlow pode igualmente ser usado a fim mostrar a informação de fluxo em um roteador. Esta capacidade permite que você considere que tráfego atravessa a rede no tempo real. Apesar da informação de fluxo ser exportada para um coletor remoto, é recomendado configurar dispositivos de rede para o NetFlow de modo que possa ser usado de forma reativa, se necessário.

Mais informações sobre esse recurso estão disponíveis na seção Identificação de tráfego e Traceback deste documento e no Cisco IOS NetFlow (somente usuários registrados).

Gerenciamento de configuração

O gerenciamento de configuração é um processo pelo qual as alterações de configuração são propostas, revistas, aprovadas, e distribuídas. Dentro do contexto de uma configuração de dispositivo Cisco IOS XE, dois aspectos adicionais do gerenciamento de configuração são críticos: arquivamento de configuração e segurança.

Você pode usar arquivos de configuração para rolar para trás as mudanças que são feitas aos dispositivos de rede. Em um contexto de segurança, os arquivos de configuração podem igualmente ser usados a fim determinar que alterações de segurança foram feitas e quando estas mudanças ocorreram. Conjuntamente com dados de registro AAA, esta informação pode ajudar no exame de segurança dos dispositivos de rede.

A configuração de um dispositivo Cisco IOS XE contém muitos detalhes confidenciais. Os nomes de usuário, as senhas, e os índices de lista de controle de acesso são exemplos deste tipo de

informação. O repositório que você usa para arquivar as configurações do dispositivo Cisco IOS XE precisa ser protegido. O acesso incerto a esta informação pode minar a segurança da toda a rede.

Plano de gerenciamento

O plano de gerenciamento consiste nas funções que conseguem os objetivos da gestão da rede.

Isso inclui as sessões interativas de gerenciamento que usam o SSH e a coleta de estatísticas com SNMP ou NetFlow. Quando você considera a segurança de um dispositivo de rede, é crítico que o plano de gerenciamento esteja protegido. Se um incidente de segurança pode minar as funções do plano de gerenciamento, pode ser impossível para você recuperar ou estabilizar a rede.

Estas seções detalham os recursos e as configurações de segurança disponíveis no software Cisco IOS XE que ajuda a fortificar o plano de gerenciamento.

Plano de gerenciamento geral de endurecimento

O plano de gerenciamento é usado a fim alcançar, configurar, e controlar um dispositivo, assim como monitora suas operações e a rede em que é distribuído. O plano de gerenciamento é o plano que recebe e envia o tráfego para operações destas funções. Você deve proteger o plano de gerenciamento e o plano de controle de um dispositivo, pois as operações do plano de controle afetam diretamente as operações do plano de gerenciamento. Esta lista de protocolos é usada pelo plano de gerenciamento:

1. Protocolo simples de gestão de rede
2. Telnet
3. Protocolo secure shell
4. Protocolo de transferência de arquivo
5. Hyper Text Transfer Protocol / Secure Hyper Text Transfer Protocol
6. Protocolo trivial file transfer
7. Protocolo da cópia segura
8. TACACS+
9. RADIUS
10. Netflow
11. Protocolo de tempo de rede
12. Syslog

    As etapas devem ser tomadas para assegurar a sobrevivência da gestão e para controlar planos durante incidentes de segurança. Se um destes planos é explorado com sucesso, todos os planos podem ser comprometidos.

Gerenciamento de senha

Acesso do controle das senhas aos recursos ou aos dispositivos. Isso é feito por meio da

definição de uma senha ou segredo que é usado para autenticar solicitações. Quando um pedido é recebido para o acesso a um recurso ou a um dispositivo, o pedido está desafiado para a verificação da senha e da identidade, e o acesso pode ser concedido, negado, ou limitado baseado no resultado. Como um melhor prática da segurança, as senhas devem ser controladas com um TACACS+ ou um servidor de autenticação RADIUS. No entanto, observe que uma senha configurada localmente para acesso privilegiado ainda é necessária, em caso de falha dos serviços TACACS+ ou RADIUS. Um dispositivo pode igualmente ter a outra informação de senha atual dentro de sua configuração, tal como uma chave NTP, a chave da série de comunidade SNMP, ou do protocolo de roteamento.

O comando enable secret é usado para definir a senha que concede acesso administrativo privilegiado ao sistema Cisco IOS XE. O comando enable secret deve ser usado, ao invés do comando enable password mais veho. O comando enable password usa um algoritmo de criptografia fraco.

Se nenhum permita o segredo é ajustado e uma senha está configurada para a linha tty do console, a senha de console pode ser usada a fim de receber o acesso privilegiado, mesmo de uma sessão virtual remota (vty) tty. Esta ação é quase certamente indesejável e é uma outra razão para assegurar a configuração de habilitar segredo.

O comando de configuração global service password-encryption direciona o Cisco IOS XE Software para criptografar as senhas, os segredos do Challenge Handshake Authentication Protocol (CHAP) e dados semelhantes que são salvos em seu arquivo de configuração. Tal criptografia é útil a fim impedir observadores ocasionais das senhas da leitura, como quando olham a tela sobre o agrupamento de um administrador. No entanto, o algoritmo usado pelo comando service password-encryption é uma cifra Vigen re simples. O algoritmo não é projetado para proteger arquivos de configuração contra a análise séria mesmo por atacantes leve sofisticados e não deve ser usado por esse motivo. Qualquer arquivo de configuração do Cisco IOS XE que contenha senhas criptografadas deve ser tratado com o mesmo cuidado que é usado para uma lista de texto claro dessas mesmas senhas.

Quando este algoritmo de criptografia fraco não for usado pelo comando enable secret, está usado pelo comando global configuration da senha da possibilidade, assim como pelo comando password line configuration. As senhas deste tipo devem ser eliminadas e o comando enable secret ou a característica aumentada da segurança de senha precisam de ser usados.

O comando enable secret e o recurso Enhanced Password Security usam o Message Digest 5 (MD5) para executar o hash da senha. Este algoritmo teve a revisão pública considerável e não é sabido para ser reversível. Contudo, o algoritmo é sujeito aos ataques do dicionário. Em um ataque do dicionário, um atacante tenta cada palavra em um dicionário ou a outra lista de senhas do candidato a fim de encontrar uma combinação. Conseqüentemente, os arquivos de configuração devem firmemente ser armazenados e somente compartilhado com os indivíduos confiados.

Segurança de senha aumentada

O recurso Enhanced Password Security, que tem funcionado desde a primeira versão do Cisco

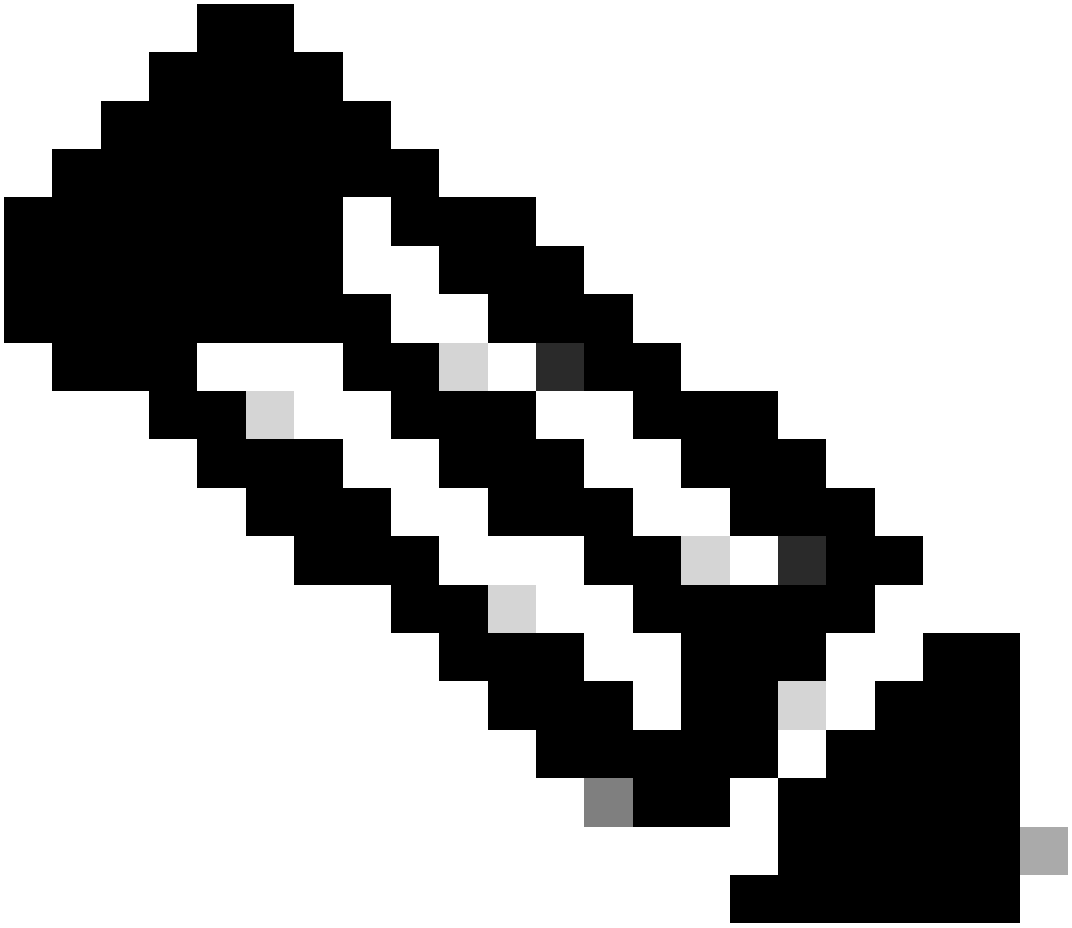
IOS XE Software Release 16.6.4, permite que um administrador configure o hash MD5 de senhas para o comando username. Antes desta característica, havia dois tipos de senhas: Tipo 0, que é uma senha de texto claro, e Tipo 7, que usa o algoritmo da cifra Vigen re. A característica aumentada da segurança de senha não pode ser usada com protocolos que exigem a senha de texto claro ser recuperável, como o CHAP.

A fim cifrar uma senha do usuário com hashing MD5, emita o comando global configuration do username secreto.

username <name> secret <password>

Fechamento da nova tentativa da senha de login

O recurso Bloqueio de Nova Tentativa de Senha de Login, que tem funcionado desde a primeira versão do Cisco IOS XE Software Release 16.6.4, permite bloquear uma conta de usuário local após um número configurado de tentativas de login malsucedidas. Uma vez que um usuário é fechado para fora, sua conta é fechada até que você a destrave. Um usuário autorizado que seja configurado com nível de privilégio 15 não pode ser fechado para fora com esta característica. O número de usuários com nível de privilégio 15 deve ser mantido a um mínimo.



Observação: os usuários autorizados podem se bloquear em um dispositivo se o número de tentativas de login malsucedidas for atingido. Adicionalmente, um usuário malicioso pode criar uma recusa da condição do serviço (DoS) com as tentativas repetidas de autenticar com um nome de usuário válido.

Este exemplo mostra como permitir a característica do fechamento da nova tentativa da senha de login:

aaa new-model aaa local authentication attempts max-fail <max-attempts> aaa authentication login default local

username <name> secret <password>

Esta característica igualmente aplica-se aos métodos de autenticação tais como a CHAP e o protocolo password authentication (PAP).

Recuperação de Senha Sem Serviço

No Cisco IOS XE Software Release 16.6.4 e posterior, o recurso No Service Password-Recovery não permite que qualquer pessoa com acesso de console acesse inseguramente a configuração do dispositivo e limpe a senha. Igualmente não permite que os usuários maliciosos mudem o valor do registro de configuração e o acesso NVRAM.

recuperação de senha sem serviço

O software Cisco IOS XE fornece um procedimento de recuperação de senha que depende do acesso ao ROM Monitor Mode (ROMMON) e usa a tecla Break durante a inicialização do sistema. No ROMMON, o software do dispositivo pode ser recarregado para solicitar uma nova configuração do sistema que inclua uma nova senha.

O procedimento de recuperação da senha atual permite qualquer um com acesso de console de alcançar o dispositivo e sua rede. O recurso No Service Password-Recovery impede a conclusão da sequência de tecla Break e a entrada do ROMMON durante a inicialização do sistema.

Se nenhuma recuperação de senha do serviço é permitida em um dispositivo, recomenda-se que uma cópia autônoma da configuração de dispositivo salvar e que uma configuração que arquiva a solução esteja executada. Se for necessário recuperar a senha de um dispositivo Cisco IOS XE depois que esse recurso for habilitado, toda a configuração será excluída.

Desabilite serviços não utilizados

Como uma melhor prática da segurança, todo o serviço desnecessário deve ser deficiente. Esses serviços desnecessários, especialmente os que usam o UDP (User Datagram Protocol), são utilizados com pouca frequência para fins legítimos, mas podem ser usados para iniciar o DoS e outros ataques que, de outra forma, seriam impedidos pela filtragem de pacotes.

Os serviços pequenos TCP e UDP devem ser deficientes. Estes serviços incluem:

1. eco (número de porta 7)
2. rejeite (número de porta 9)
3. dia (número de porta 13)
4. chargen (número de porta 19)

   Embora o abuso dos serviços pequenos possa ser evitado ou feito menos perigoso por listas de acesso anti-falsificação, os serviços devem ser deficientes em todo o dispositivo acessível dentro da rede. Os serviços pequenos são desativados por padrão no Cisco IOS XE Software Releases 16.6.4 e posteriores. No software anterior, o no service tcp-small-servers e no service udp-small-servers comandos de configuração global podem ser emitidos a fim de desabilitá-los.

   Esta é uma lista de serviços adicional que devem ser deficientes se não no uso:
5. Não emita o no ip fingercomando global configuration a fim de desabilitar o serviço Finger. As versões do Cisco IOS XE Software posteriores à 16.1 desabilitam esse serviço por padrão.
6. Emita o comando global configuration do no ip bootp server a fim desabilitar o protocolo de bootstrap (BOOTP). As versões do Cisco IOS XE Software posteriores à 16.1 desabilitam

esse serviço por padrão.

7. No Cisco IOS XE Software Release 16.6.4 e posterior, execute o comando ip dhcp bootp ignore no modo de configuração global para desabilitar o BOOTP. Isto deixa serviços do protocolo de configuração dinâmica host (DHCP) habilitados.
8. Os serviços DHCP podem ser deficientes se os serviços da transmissão de DHCP não forem exigidos. Emita o comando no service dhcp no modo de configuração global.
9. Não emita nenhum comando mop enabled no modo de configuração da interface a fim desabilitar o serviço de Protocolo de Manutenção de Operação (MOP).
10. Emita o no ip domain-lookup comando de configuração global a fim desabilitar serviços da resolução do Domain Name System (DNS).
11. Emita o no service pad command no modo de configuração global a fim desabilitar o serviço pacote de montagem/desmontagem (PAD), o qual é usado para as redes X.25.
12. O servidor HTTP pode ser desativado com o comando no ip http server modo de configuração global, e o servidor Secure HTTP (HTTPS) pode ser desativado com o comando de configuração global no ip http secure-server.
13. A menos que os dispositivos Cisco IOS XE recuperem configurações da rede durante a inicialização, o comando de configuração global no service config deve ser usado. Isso evita que o dispositivo Cisco IOS XE tente localizar um arquivo de configuração na rede com TFTP.
14. O protocolo cisco discovery (CDP) é um protocolo de rede usado a fim de descobrir outros dispositivos permitidos CDP para a adjacência vizinha e a topologia de rede. O CDP pode ser usado por sistemas de gerenciamento de rede (NMS) ou durante o Troubleshooting. O CDP deve ser deficiente em todas as relações que são conectadas às redes não confiáveis. Isto é realizado com o comando interface do no cdp enable. Alternativamente, o CDP pode ser desabilitada globalmente com o comando de configuração global do no cdp run. Note que o CDP pode ser usado por um usuário malicioso para o reconhecimento e o traço da rede.
15. O protocolo de descoberta da camada de enlace (LLDP) é um protocolo de IEEE definido em 802.1AB. LLDP é similar ao CDP. Contudo, este protocolo permite a interoperabilidade entre os outros dispositivos que não apoiam o CDP. LLDP deve ser tratado da mesma forma como o CDP e desabilitado em todas as relações que conectam às redes não confiáveis. A fim realizar isto, emita o no lldp transmit e no lldp receive comandos configuração de interface. Emita o comando no lldp run global configuration a fim de desabilitar o LLDP global. LLDP pode igualmente ser usado por um usuário malicioso para o reconhecimento e o traço da rede.
16. Para switches que suportam inicialização a partir do sdflash, a segurança pode ser melhorada com a inicialização a partir do flash e desabilitar o sdflash com o comando de configuração no sdflash.

EXEC timeout

A fim de ajustar o intervalo o intérprete do comando exec espera a entrada de usuário antes que termine uma sessão, emita o comando exec-timeout linha de configuração. O comando exec-timeout deve ser usado a fim de terminar sessões nas linhas vty ou tty que são deixadas inativas. Por padrão, as sessões são desconectadas após dez minutos de inatividade.

line con 0

exec-timeout <minutos> [segundos]

line vty 0 4

exec-timeout <minutos> [segundos]

Keepalives para sessões de TCP

Os comandos de configuração global service tcp-keepalives-in e service tcp-keepalives-out permitem que um dispositivo envie keepalives de TCP para sessões TCP. Esta configuração deve ser usada a fim permitir manutenções de atividade TCP em conexões de entrada ao dispositivo e às conexões externas do dispositivo. Isso garante que o dispositivo na extremidade remota da conexão ainda esteja acessível e que as conexões semiabertas ou órfãs sejam removidas do dispositivo Cisco IOS XE local.

serviço tcp-keepalives-in

service tcp-keepalives-out

Uso da interface de gerenciamento

O plano de gerenciamento de um dispositivo é em-faixa ou fora da banda alcançado em um exame ou no Logical Management Interface. Idealmente, ambos os gerenciamentos de acesso em-banda e fora de banda existem para cada dispositivo de rede de modo que o plano de gerenciamento possa ser alcançado durante paradas de rede.

Uma das relações as mais comuns usadas para o acesso em-faixa a um dispositivo é a interface lógica de loopback. As interfaces de loopback são sempre acima, visto que as interfaces física podem mudar o estado, e a relação podem ser potencialmente não acessíveis. Recomenda-se adicionar uma interface de loopback a cada dispositivo como uma interface de gerenciamento e isso seja usado exclusivamente para o plano de gerenciamento. Isto permite que o administrador aplique políticas durante todo a rede para o plano de gerenciamento. Uma vez que a interface de loopback é configurada em um dispositivo, pode ser usada por protocolos do plano de gerenciamento, tais como o SSH, o SNMP, e o syslog, a fim de enviar e receber tráfego.

interface Loopback0

endereço ip 192.168.1.1 255.255.255.0

Notificações do ponto inicial da memória

A Notificação de Limite de Memória do recurso, adicionada ao Cisco IOS XE Software Release 16.6.4, permite que você reduza as condições de memória baixa em um dispositivo. Esse recurso usa dois métodos para realizar isso: Notificação de limite de memória e Reserva de memória.

A notificação do ponto inicial da memória gera um mensagem de registro a fim indicar que a

memória livre em um dispositivo caiu mais baixo do que o limiar configurado. Este exemplo de configuração mostra como permitir esta característica com o comando global configuration memory free low-watermark. Isto permite um dispositivo de gerar uma notificação quando a memória livre disponível cai mais baixo do que o limiar especificado, e outra vez quando a memória livre disponível aumentar cinco por cento a mais alto do que o limiar especificado.

memory free low-watermark processor <threshold>

memory free low-watermark io <threshold>

A reserva da memória é usada de modo que a memória suficiente esteja disponível para notificações críticas. Este exemplo de configuração demonstra como habilitar esta característica. Isto assegura que os processos de gerenciamento continuem a funcionar quando a memória do dispositivo é esgotada.

memory reserve critical <value>

Notificação do limiar CPU

Introduzido no Cisco IOS XE Software Release 16.6.4, o recurso de Notificação de Limite de CPU permite que você detecte e seja notificado quando a carga de CPU em um dispositivo cruza um limite configurado. Quando o ponto inicial é cruzado, o dispositivo gera e envia um mensagem de armadilha de SNMP. Dois métodos de limite de utilização de CPU são suportados no software Cisco IOS XE: Limite de elevação e Limite de queda.

Este exemplo de configuração mostra como permitir os limiares de elevação e de queda que provocam um mensagem de notificação do limiar de CPU:

snmp-server enable traps cpu threshold

snmp-server host <host-address> <community-string> cpu

tipo de limite de cpu de processo <tipo> aumento <porcentagem> intervalo <segundos> [queda <porcentagem> intervalo <segundos>]

process cpu statistics limit entry-percentage <number> [size <seconds>]

Protocolo de tempo de rede

O protocolo Network Time Protocol (NTP) é um não serviço especialmente perigoso, mas todo o serviço unneeded pode representar um vetor do ataque. Se o NTP é usado, é importante configurar explicitamente um origem de tempo confiado e usar a autenticação apropriada. Um tempo preciso e confiável é necessário para fins de syslog, como durante investigações forenses de ataques potenciais, bem como para conectividade de VPN bem-sucedida que depende de certificados para autenticação da Fase 1.

1. Fuso horário do NTP – Quando você configura o NTP, o fuso horário precisa ser configurado para que os carimbos de hora possam ser correlacionados com precisão. Geralmente, existem duas abordagens para configurar o fuso horário para dispositivos em

uma rede com presença global. Um método é configurar todos os dispositivos de rede com o tempo universal coordenado (UTC) (previamente horário de Greenwich (GMT)). A outra aproximação é configurar dispositivos de rede com o fuso horário local. Mais informações sobre esse recurso podem ser encontradas no fuso horário do relógio na documentação do produto Cisco.

2. Autenticação NTP – Se você configurar a autenticação NTP, ela garante que as mensagens NTP sejam trocadas entre pares NTP confiáveis.

   Exemplo de configuração que usa autenticação NTP:

   Cliente:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

   (config)#ntp servidor 172.16.1.5 chave 5 Servidor:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

Limitar o acesso à rede com ACLs para infraestrutura

Planejado para impedir uma comunicação direta desautorizada aos dispositivos de rede, as lista de controle de acesso da infra-estrutura (iACLs) são um dos controles de segurança os mais críticos que podem ser executados nas redes. A infra-estrutura ACL leverage a ideia que quase todo o tráfego de rede atravessa a rede e não está destinado à rede própria.

Uma iACL é criada e aplicada para especificar as conexões de hosts ou redes que precisam ter permissão para acessar os dispositivos de rede. Os exemplos comuns destes tipos de conexão são eBGP, SSH, e SNMP. Depois que as conexões exigidas foram permitidas, todo tráfego restante à infra-estrutura está negado explicitamente. Todo o tráfego de trânsito que cruza a rede e não é destinado aos dispositivos de infra-estrutura é permitido então explicitamente.

As proteções fornecidas por iACLs são relevantes à gestão e controlam planos. A aplicação dos iACLs pode ser facilitada com o uso do endereçamento distinto para dispositivos da infra-estrutura de rede. Refira uma aproximação orientada segurança ao endereçamento de IP para obter mais informações sobre das implicações de segurança do endereçamento de IP.

Esta configuração do iACL do exemplo ilustra a estrutura que deve ser usada como um ponto de início quando você começa o processo de implementação do iACL:

```
ip access-list extended ACL-INFRASTRUCTURE-IN

— Permitir as conexões necessárias para protocolos de roteamento e gerenciamento de rede

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179

permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>

permit tcp host <trusted-management-stations> any eq 22

permit udp host <trusted-netmgmt-servers> any eq 161

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny ip any <infrastructure-address-space> <wildcard-mask>

— Autorizar o tráfego em trânsito

permit ip any any
```

Uma vez que criado, o iACL deve ser aplicado a todas as relações que enfrentam dispositivos da NON-infra-estrutura. Isto inclui as relações que conectam a outros organizações, segmentos do acesso remoto, segmentos do usuário, e segmentos nos centros de dados.

Consulte Protecting Your Core: Infrastructure Protection Access Control Lists para obter mais informações sobre ACLs de infraestrutura.

Filtração do pacote ICMP

O Internet Control Message Protocol (ICMP) é projetado como um protocolo de controle de IP. Como tal, as mensagens que transporta podem ter ramificação de grande envergadura ao TCP e aos protocolos IP em geral. Quando as ferramentas de Troubleshooting da rede executarem o ping e traceroute use o ICMP, a conectividade externa do ICMP é raramente necessária para a operação apropriada de uma rede.

O software Cisco IOS XE fornece funcionalidade para filtrar especificamente mensagens ICMP por nome ou tipo e código. Este exemplo ACL, o qual deve ser usado com as entradas de controle de acesso (ACE) dos exemplos anteriores, permite a execução do ping das estações de gerenciamento e dos servidores NMS confiados e obstrui todos pacotes ICMP restantes:

```
ip access-list extended ACL-INFRASTRUCTURE-IN

— Permitir eco ICMP (ping) de estações de gerenciamento e servidores confiáveis

permit icmp host <trusted-management-stations> any echo

permit icmp host <trusted-netmgmt-servers> any echo

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny ip any <infrastructure-address-space> <wildcard-mask>
```

— Autorizar o tráfego em trânsito

permit ip any any

Filtre fragmentos IP

O processo de filtragem de pacotes IP fragmentados pode representar um desafio para os dispositivos de segurança. Isto é porque a informação da camada 4 que é usada a fim de filtrar o TCP e os pacotes de UDP está presente somente no fragmento inicial. O software Cisco IOS XE usa um método específico para verificar fragmentos não iniciais em relação às listas de acesso configuradas. O software Cisco IOS XE avalia esses fragmentos não iniciais em relação à ACL e ignora qualquer informação de filtragem da Camada 4. Isto faz com que os fragmentos não iniciais sejam avaliados unicamente na camada 3 parcelas de todo o ACE configurado.

Neste exemplo de configuração, se um pacote de TCP destinado a 192.168.1.1 na porta 22 é fragmentads no trânsito, o fragmento inicial é deixado cair como esperado pelo segundo ACE baseado na informação da camada 4 dentro do pacote. Contudo, os fragmentos (não-iniciais) todos os restantes são permitidos pelo primeiro ACE baseado completamente na informação da camada 3 no pacote e no ACE. O cenário é mostrado nesta configuração:

ip access-list extended ACL-FRAGMENT-EXAMPLE

permit tcp any host 192.168.1.1 eq 80

deny tcp any host 192.168.1.1 eq 22

Devido à natureza não intuitiva do fragmento que segura, os fragmentos IP frequentemente são permitidos inadvertidamente por ACL. A fragmentação é frequentemente usada nas tentativas de iludir a detecção pelo Intrusion Detection Systems. É por estas razões que os fragmentos IP são usados frequentemente nos ataques, e porque devem explicitamente ser filtrados na parte superior de todos os iACLs configurados. Este exemplo ACL inclui a filtração detalhada de fragmentos IP. A funcionalidade deste exemplo deve ser usada conjuntamente com a funcionalidade dos exemplos anteriores.

ip access-list extended ACL-INFRASTRUCTURE-IN

— Negue fragmentos IP que usam ACEs específicas de protocolo para ajudar na

— classificação do tráfego de ataque

deny tcp any any fragments

deny udp any any fragments

deny icmp any any fragmentos

deny ip any any fragments

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny ip any <infrastructure-address-space> <wildcard-mask>

— Autorizar o tráfego em trânsito

permit ip any any

Consulte Listas de controle de acesso e fragmentos IP para obter mais informações sobre como a ACL lida com pacotes IP fragmentados.

Apoio ACL para opções IP de filtração

O Cisco IOS XE Software Release 16.6.4 adicionou suporte para o uso de ACLs para filtrar pacotes IP com base nas opções IP que estão contidas no pacote. As opções IP apresentam um desafio da segurança para dispositivos de rede porque estas opções devem ser processadas como pacotes da exceção. Isto exige um nível do esforço da CPU que não é exigido para os pacotes típicos que atravessam a rede. A presença de opções IP dentro de um pacote pode igualmente indicar uma tentativa de subverter controles de segurança na rede ou de alterar de outra maneira as características do trânsito de um pacote. É por estas razões que os pacotes com opções IP devem ser filtrados na borda da rede.

Este exemplo deve ser usado com os ACE dos exemplos anteriores a fim de incluir a filtração completa dos pacotes IP que contêm opções IP:

ip access-list extended ACL-INFRASTRUCTURE-IN

— Negar pacotes IP que contenham opções IP

deny ip any any option-options

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny ip any <infrastructure-address-space> <wildcard-mask>

— Autorizar o tráfego em trânsito

permit ip any any

Suporte à ACL para filtrar o valor TTL

O Cisco IOS XE Software Release 16.6.4 adicionou suporte ACL para filtrar pacotes IP com base no valor Time to Live (TTL). O valor TTL de um IP datagrams é decrescido por cada dispositivo de rede como fluxos de pacote de informação da fonte ao destino. Embora os valores iniciais variem pelo sistema operacional, quando o TTL de um pacote alcança zero, o pacote deve ser deixado cair. O dispositivo que diminui o TTL para zero e, portanto, descarta o pacote, é necessário para gerar e enviar uma mensagem de tempo excedido do ICMP para a origem do pacote.

A geração e a transmissão destas mensagens são um processo da exceção. Os roteadores podem realizar essa função quando o número de pacotes IP com vencimento próximo é baixo, mas se o número de pacotes com vencimento próximo for alto, a geração e a transmissão dessas

mensagens podem consumir todos os recursos disponíveis da CPU. Isto apresenta um vetor do ataque DoS. Por isso, os dispositivos precisam ser protegidos contra ataques de DoS que utilizam uma alta taxa de pacotes IP com vencimento próximo.

Recomenda-se que as organizações filtrem os pacotes IP com baixos valores TTL na borda da rede. Os pacotes de filtragem completos com os valores TTL insuficientes para atravessar a rede abrandam a ameaça dos ataques dos estabelecimentos de base TTL.

Neste exemplo, a ACL filtra pacotes com valores TTL inferiores a seis. Isto fornece a proteção contra ataques da expiração TTL para redes de até cinco saltos na largura.

ip access-list extended ACL-INFRASTRUCTURE-IN

— Negar pacotes IP com valores TTL insuficientes para atravessar a rede

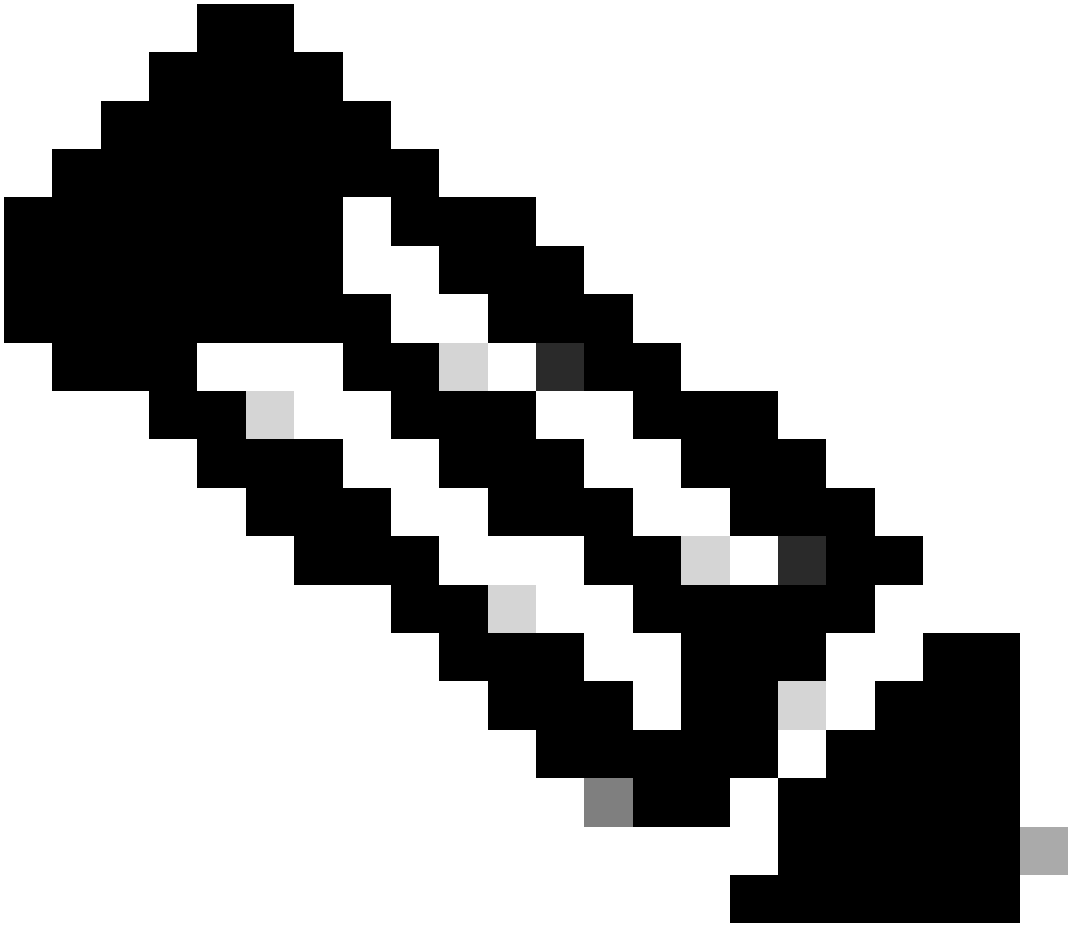
deny ip any any ttl lt 6

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny ip any **<infrastructure-address-space> <mask>**

— Autorizar o tráfego em trânsito

permit ip any any



Observação: Alguns protocolos fazem uso legítimo de pacotes com valores TTL baixos. O eBGP é um desses protocolos. Refira a identificação e a mitigação do ataque da expiração TTL para obter mais informações sobre mitigar ataques de expiração-estabelecimentos de bases TTL.

Proteger as sessões interativas de gerenciamento

As sessões de gerenciamento aos dispositivos permitem a capacidade para ver e recolher a informação sobre um dispositivo e suas operações. Se esta informação é divulgada a um usuário malicioso, o dispositivo pode transformar-se o alvo de um ataque, comprometido, e usado a fim de executar ataques adicionais. Qualquer um com acesso de privilegiado a um dispositivo tem a capacidade para o controle administrativo completo desse dispositivo. É essencial proteger as sessões de gerenciamento para evitar a divulgação de informações e o acesso não autorizado.

Proteção do plano de gerenciamento

No Cisco IOS XE Software Release 16.6.4 e posterior, o recurso Management Plane Protection (MPP) permite que um administrador restrinja em quais interfaces o tráfego de gerenciamento pode ser recebido por um dispositivo. Isto permite ao administrador o controle adicional sobre um dispositivo e como o dispositivo é alcançado.

Este exemplo mostra como ativar o MPP para permitir apenas o SSH e o HTTPS na interface GigabitEthernet0/1:

host de plano de controle

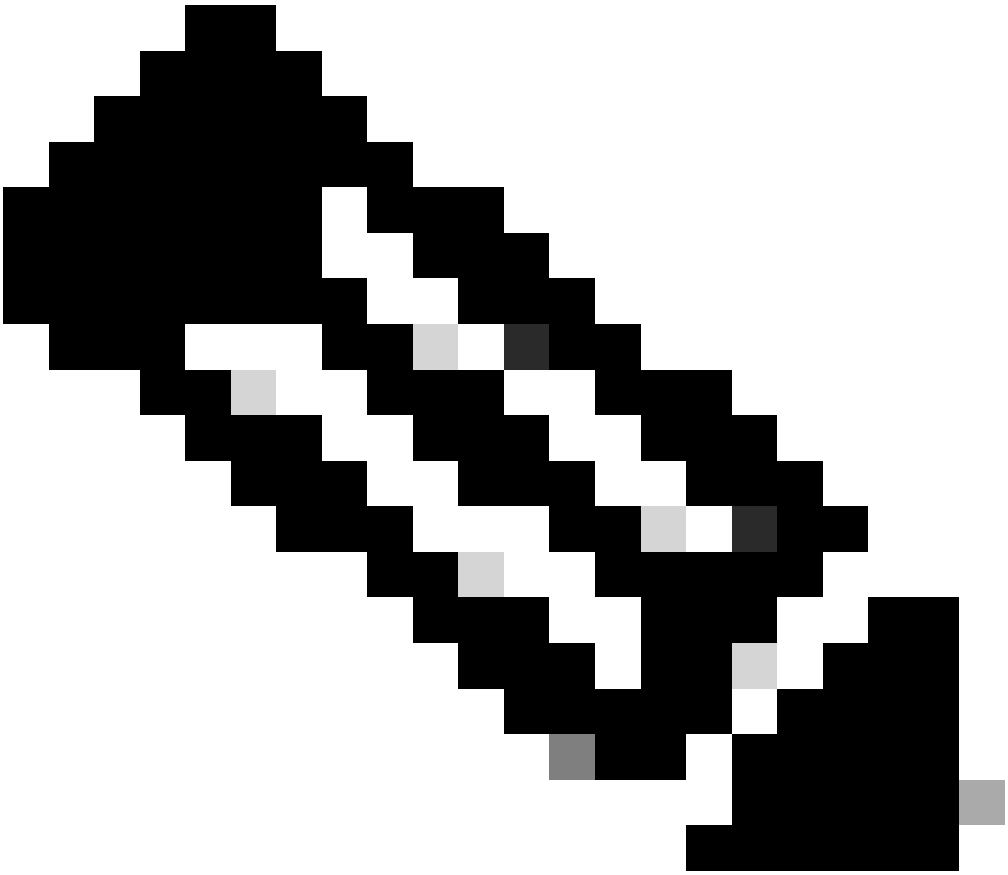
management-interface GigabitEthernet 0/1 allow ssh https

Controle a proteção plana

A Proteção do Plano de Controle (CPPr - Control Plane Protection) baseia-se na funcionalidade da Vigilância do Plano de Controle para restringir e policiar o tráfego do plano de controle que é destinado ao processador de rota do dispositivo IOS-XE. O CPPr divide o plano de controle em categorias separadas de plano de controle conhecidas como subinterfaces. Existem três subinterfaces de plano de controle: Host, Trânsito e CEF-Exceção. Além disso, CPPr inclui estes recursos de proteção adicionais do plano do controle:

1. Recurso Port-Filtering – Este recurso permite a fiscalização ou o descarte de pacotes enviados para portas TCP e UDP fechadas ou não audíveis.
2. Recurso Queue-Threshold Policy – Este recurso limita o número de pacotes de um protocolo especificado que são permitidos na fila de entrada IP do plano de controle.

   O CPPr permite que um administrador classifique, fiscalize e restrinja o tráfego enviado a um dispositivo para fins de gerenciamento com a subinterface do host. Os exemplos de pacotes que são classificados para a categoria da subinterface do host incluem o tráfego de gerenciamento tal como o SSH ou o telnet e os protocolos de roteamento.



Observação: CPPr não suporta IPv6 e é restrito ao caminho de entrada IPv4.

Consulte Política de Plano de Controle para obter mais informações sobre o recurso Cisco CPPr.

Criptografar as sessões de gerenciamento

Como as informações podem ser divulgadas em uma sessão interativa de gerenciamento, esse tráfego deve ser criptografado para que um usuário mal-intencionado não possa acessar os dados transmitidos. A criptografia de tráfego permite uma conexão segura de acesso remoto com o dispositivo. Se o tráfego para uma sessão de gerenciamento é enviado sobre a rede na minuta, um atacante pode obter informações sensíveis sobre o dispositivo e a rede.

Um administrador pode estabelecer uma conexão de gerenciamento de acesso remoto criptografado e seguro para um dispositivo com os recursos SSH ou HTTPS. O software Cisco IOS XE suporta SSH versão 2.0 (SSHv2) e HTTPS que usa Secure Sockets Layer (SSL) e Transport Layer Security (TLS) para autenticação e criptografia de dados.

O software Cisco IOS XE também suporta o Secure Copy Protocol (SCP), que permite uma conexão criptografada e segura para copiar configurações de dispositivo ou imagens de software.

O SCP confia no SSH.

Este exemplo de configuração ativa o SSH em um dispositivo Cisco IOS XE:

```
ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

line vty 0 4

transport input ssh
```

Este exemplo de configuração permite serviços SCP:

```
ip scp server enable
```

Este é um exemplo de configuração para serviços HTTPS:

```
crypto key generate rsa modulus 2048

ip http secure-server
```

SSHv2

O recurso SSHv2 foi introduzido no Cisco IOS XE na primeira versão 16.6.4 que permite que um usuário configure o SSHv2. O SSH é executado sobre uma camada de transporte confiável e oferece recursos eficazes de autenticação e criptografia. O único transporte confiável que é definido para o SSH é TCP. O SSH fornece meios para alcançar firmemente e executar firmemente comandos em um outro computador ou dispositivo sobre uma rede. A característica do protocolo da cópia segura (SCP) que é em túnel sobre o SSH permite a transferência segura dos arquivos.

Se o comando ip ssh version 2 não estiver explicitamente configurado, o Cisco IOS XE ativará o SSH Version 1.99. O SSH versão 1.99 permite as conexões SSHv1 e SSHv2. O SSHv1 é considerado inseguro e pode ter efeitos adversos no sistema. Se o SSH estiver habilitado, é recomendável desabilitar o SSHv1 usando o comando ip ssh version 2.

Esta configuração de exemplo habilita SSHv2 (com SSHv1 desabilitado) em um dispositivo Cisco IOS XE:

```
hostname router

ip domain-name example.com

crypto key generate rsa modulus 2048
```

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

ip ssh version 2

line vty 0 4

transport input ssh

Refira o apoio da versão 2 do Secure Shell para obter mais informações sobre do uso de SSHv2.

Realces SSHv2 para chaves RSA

O Cisco IOS XE SSHv2 suporta métodos de autenticação baseados em senha e interativos por teclado. Os realces SSHv2 para a característica de chaves RSA igualmente apoiam a autenticação da chave pública dos RSA-estabelecimentos de bases para o cliente e servidor.

Para a autenticação de usuário, a autenticação baseada em RSA usa pares associados privado/chave pública associada com cada usuário para a autenticação. O usuário deve gerar um par de chave privada/pública no cliente e configurar uma chave pública no servidor SSH Cisco IOS XE para concluir a autenticação.

Um usuário SSH que tenta estabelecer as credenciais fornece uma assinatura criptografada com a chave privada. A assinatura e a chave pública do usuário são enviadas ao servidor de SSH para a autenticação. O servidor de SSH computa uma mistura sobre a chave pública fornecida pelo usuário. O hash é usado para determinar se o servidor tem uma entrada correspondente. Se uma correspondência for encontrada, a verificação de mensagem baseada em RSA será realizada com a chave pública. Daqui, o usuário é autenticado ou o acesso negado é baseado na assinatura criptografada.

Para autenticação de servidor, o cliente SSH Cisco IOS XE deve atribuir uma chave de host para cada servidor. Quando o cliente tenta estabelecer uma sessão SSH com um servidor, recebe a assinatura do server como parte da mensagem das trocas de chave. Se o sinalizador estrito de verificação de chave de host estiver ativado no cliente, o cliente verificará se tem a entrada de chave de host que corresponde ao servidor pré-configurado. Se uma correspondência for encontrada, o cliente tentará validar a assinatura com a chave de host do servidor. Se o servidor for autenticado com êxito, o estabelecimento da sessão continuará; caso contrário, ele será encerrado e exibirá uma mensagem de falha de autenticação de servidor.

Esta configuração de exemplo permite o uso de chaves RSA com SSHv2 em um dispositivo Cisco IOS XE:

Configurar um nome de host para o dispositivo

hostname router

Configurar um nome de domínio

ip domain-name example.com

Ative o servidor SSH para autenticação local e remota no roteador que usa

o comando "crypto key generate".

Para a versão 2 do SSH, o tamanho do módulo deve ser de pelo menos 768 bits

crypto key generate rsa usage-keys label sshkeys modulus 2048

Especifique o nome do par de chaves RSA (neste caso, "sshkeys") a ser usado para SSH

ip ssh rsa keypair-name sshkeys

Configure um tempo limite de ssh (em segundos).

A próxima saída habilita um tempo limite de 120 segundos para conexões SSH.

ip ssh time-out 120

Configure um limite de cinco tentativas de autenticação.

ip ssh authentication-retries 5

Configure a versão 2 do SSH.

ip ssh version 2

Refira a realces da versão 2 do Secure Shell para chaves RSA para mais informações sobre do uso de chaves RSA com SSHv2.

Esta configuração de exemplo permite que o servidor Cisco IOS XE SSH execute a autenticação de usuário baseada em RSA. A autenticação de usuário é bem sucedida se a chave pública RSA armazenada no servidor é verificada com os pares de chave públicos ou privados armazenado no cliente.

Configure um nome de host para o dispositivo.

hostname router

Configure um nome de domínio.

ip domain name cisco.com

Gere pares de chaves RSA que usem um módulo de 2048 bits.

crypto key generate rsa modulus 2048

Configure chaves SSH-RSA para autenticação de usuário e servidor no servidor SSH.

ip ssh pubkey-chain

Configurar o nome de usuário SSH.

Configure chaves SSH-RSA para autenticação de usuário e servidor no servidor SSH.

ip ssh pubkey-chain

Configurar o nome de usuário SSH.

username ssh-user

Especifique a chave pública RSA do peer remoto.

Você deve configurar o comando key-string

(seguido pela chave pública RSA do peer remoto) ou pelo comando

comando key-hash (seguido pelo tipo e versão da chave SSH).

Consulte Configuração do Servidor SSH Cisco IOS XE para Executar Autenticação de Usuário Baseado em RSA para obter mais informações sobre o uso de chaves RSA com SSHv2.

Esta configuração de exemplo permite que o cliente SSH Cisco IOS XE execute a autenticação de servidor baseada em RSA.

hostname router

ip domain-name cisco.com

Gere pares de chaves RSA.

crypto key generate rsa

Configure chaves SSH-RSA para autenticação de usuário e servidor no servidor SSH.

ip ssh pubkey-chain

Ative o servidor SSH para autenticação de chave pública no roteador.

server SSH-server-name

Especifique a chave pública RSA do par remoto.

Você deve configurar o comando key-string

(seguido pela chave pública RSA do peer remoto) ou thea

comando key-hash <key-type> <key-name> (seguido pela chave SSH

tipo e versão).

Assegure-se de que a autenticação do servidor ocorra - A conexão é

terminada em caso de falha.

ip ssh stricthostkeycheck

Consulte Configuração do Cisco IOS XE SSH Client para Executar Autenticação de Servidor Baseado em RSA para obter mais informações sobre o uso de chaves RSA com SSHv2.

Console e Portas AUX

Nos dispositivos Cisco IOS XE, as portas de console e auxiliares (AUX) são linhas assíncronas que podem ser usadas para acesso local e remoto a um dispositivo. Você deve estar ciente de que as portas de console nos dispositivos Cisco têm privilégios especiais. Em particular, estes privilégios permitem que um administrador execute o procedimento de recuperação de senha. A fim de executar a recuperação de senha, um atacante não-autenticado precisaria de ter o acesso à porta de Console e à capacidade para interromper a potência ao dispositivo ou fazer com que o dispositivo cause um crash.

Todo o método usado a fim de alcançar a porta de Console de um dispositivo deve ser fixado de um modo que seja igual à segurança que é reforçada para o acesso de privilegiado a um dispositivo. Os métodos usados para acesso seguro deve incluir o uso do AAA, do EXEC-intervalo, e das senhas de modem se um modem é anexado ao console.

Se a recuperação de senha não for necessária, um administrador pode remover a capacidade de executar o procedimento de recuperação de senha que usa o comando de configuração global no service password-recovery; no entanto, uma vez que o comando no service password-recovery tenha sido habilitado, um administrador não pode mais executar a recuperação de senha em um dispositivo.

Na maioria das situações, a porta AUX de um dispositivo deve ser desativada para evitar o acesso não autorizado. Uma porta AUX pode ser desativada com estes comandos:

line aux 0

transport input none

transport output none

no exec exec-timeout 0 1

sem senha

Control vty e tty Lines

As sessões interativas de gerenciamento no software Cisco IOS XE usam um tty ou um tty virtual (vty). Um tty é uma linha assíncrona local a que um terminal pode ser anexado para o acesso

local ao dispositivo ou a um modem para o acesso de discagem a um dispositivo. Note que os ttys podem ser usados para conexões às portas de Console dos outros dispositivos. Esta função permite que um dispositivo com linhas tty atue como um servidor de console onde as conexões possam ser estabelecidas através da rede às portas de Console de dispositivo conectadas às linhas tty. As linhas tty para estas conexões reversas sobre a rede devem igualmente ser controladas.

Uma linha vty é usada para todas conexões restantes da rede remota apoiadas pelo dispositivo, apesar do protocolo (o SSH, o SCP, ou o telnet são exemplos). A fim de assegurar que um dispositivo possa ser alcançado através de uma sessão de gerenciamento local ou remota, os controles apropriados devem ser reforçados em linhas vty e tty. Os dispositivos Cisco IOS XE têm um número limitado de linhas vty; o número de linhas disponíveis pode ser determinado com o comando EXEC show line. Quando todas as linhas vty estão em uso, novas sessões de gerenciamento não podem ser estabelecidas, o que cria uma condição de DoS para acesso ao dispositivo.

O formulário mais simples de controle de acesso a um vty ou do tty de um dispositivo é com o uso da autenticação em todas as linhas apesar do lugar do dispositivo dentro da rede. Isto é crítico para linhas vty porque são acessíveis através da rede. Uma linha tty conectada a um modem usado para acesso remoto ao dispositivo ou uma linha tty conectada à porta do console de outros dispositivos também pode ser acessada pela rede. Outras formas de controles de acesso vty e tty podem ser aplicadas com os comandos transport input ou access-class, com o uso dos recursos CoPP e CPPr, ou se você aplicar listas de acesso às interfaces no dispositivo.

A autenticação pode ser aplicada com o uso de AAA, que é o método recomendado para acesso autenticado a um dispositivo, com o uso do banco de dados de usuário local, ou por autenticação de senha simples configurada diretamente na linha vty ou tty.

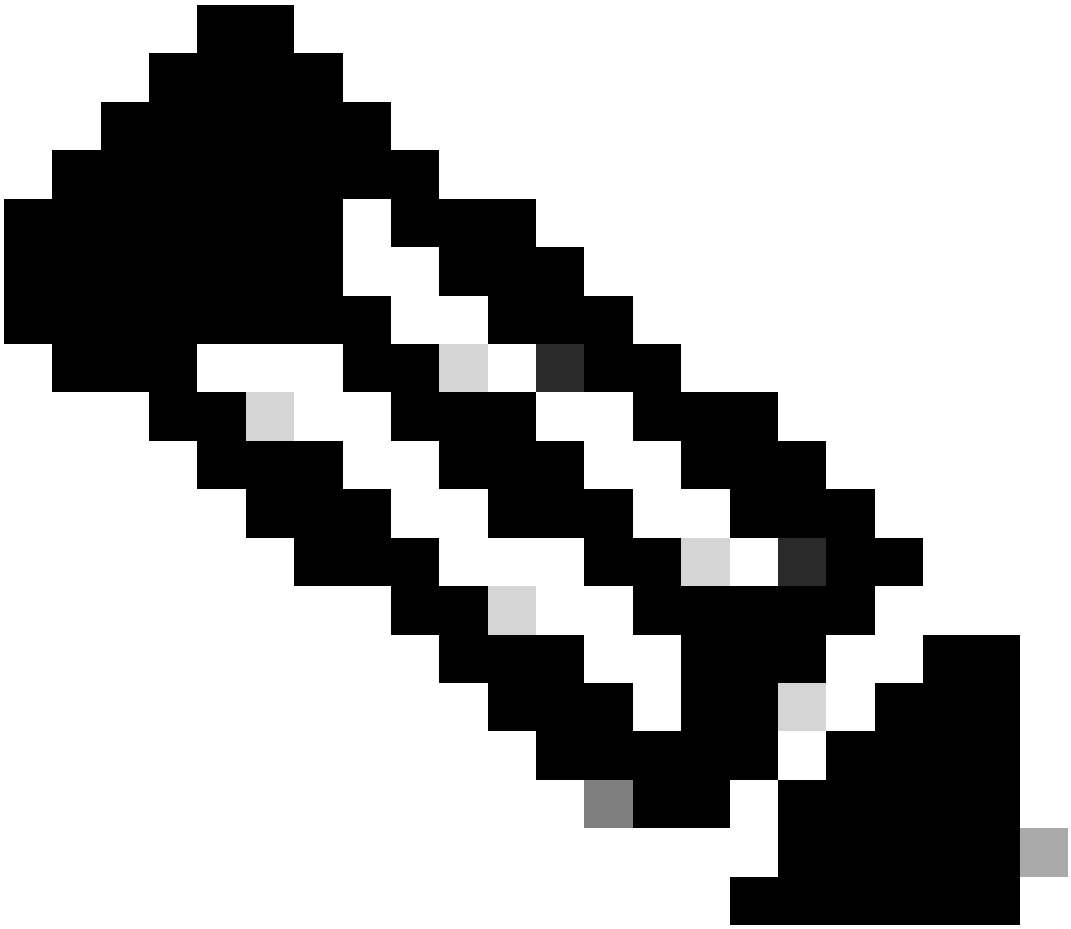
O comando exec-timeout deve ser usado a fim de terminar sessões nas linhas vty ou tty que são deixadas inativas. O comando service tcp-keepalives-in também deve ser usado para ativar o TCP keepalives nas conexões de entrada com o dispositivo. Isso garante que o dispositivo na extremidade remota da conexão ainda esteja acessível e que as conexões semiabertas ou órfãs sejam removidas do dispositivo IOS-XE local.

Controle o transporte para linhas vty e tty

Um vty e um tty podem ser configurados para aceitar apenas conexões de gerenciamento de acesso remoto criptografadas e seguras para o dispositivo ou através do dispositivo se ele for usado como um servidor de console. Esta seção endereça ttys porque tais linhas podem ser conectadas às portas de Console nos outros dispositivos, que permitem que o tty seja acessível sobre a rede. Em um esforço para impedir a divulgação de informações ou o acesso não autorizado aos dados que são transmitidos entre o administrador e o dispositivo, o transport input ssh pode ser usado em vez dos protocolos de texto claro, como Telnet e rlogin. A configuração transport input none pode ser ativada em um tty, o que, na verdade, desativa o uso da linha tty para conexões de console reverso.

As linhas vty e tty permitem que um administrador conecte aos outros dispositivos. A fim de limitar

o tipo de transporte que um administrador pode usar para conexões de saída, use o comando configuração da linha de saída do transporte. Se as conexões de saída não forem necessárias, a saída de transporte none poderá ser usada. No entanto, se as conexões de saída forem permitidas, um método de acesso remoto criptografado e seguro para a conexão poderá ser imposto por meio do uso do SSH de saída de transporte.



> Observação: o IPSec pode ser usado para conexões de acesso remoto criptografadas e seguras a um dispositivo, se suportado. Se você usa o IPSec, igualmente adiciona a carga adicional de CPU adicional ao dispositivo. Contudo, o SSH deve ainda ser reforçado como o transporte mesmo quando o IPSec é usado.

Banners de advertência

Em algumas jurisdições, talvez seja impossível processar e ilegal monitorar usuários mal-intencionados, a menos que tenham sido notificados de que não têm permissão para usar o sistema. Um método para fornecer essa notificação é colocar essas informações em uma mensagem de banner configurada com o comando banner login do software Cisco IOS XE.

Os requisitos de notificação legal são complexos, variam de acordo com a jurisdição e a situação e podem ser discutidos com o advogado. Mesmo dentro das jurisdições, as opiniões legais podem diferir. Em colaboração com o conselho, uma bandeira pode fornecer algum ou toda a esta informação:

1. Observe que o sistema deve ser registrado em ou usada especificamente somente por pessoais autorizados e talvez por informação sobre quem pode autorizar o uso.
2. Observe que toda a utilização não autorizada do sistema é ilegal e pode ser sujeita a civil e às penalidades criminal.
3. Observe que todo o uso do sistema pode ser registrado ou monitorado sem aviso futuro e que os log resultante podem ser usados como a evidência no tribunal.
4. Observações específicas exigidas por leis local.

   Do ponto de vista da segurança, e não do ponto de vista legal, um banner de login não pode conter nenhuma informação específica sobre o nome, o modelo, o software ou a propriedade do roteador. Esta informação pode ser abusada por usuários maliciosos.

Autenticação, autorização e contabilidade

A estrutura de autenticação, autorização e contabilização (AAA) é fundamental para proteger o acesso interativo aos dispositivos de rede. A estrutura AAA fornece um ambiente altamente configurável que pode ser personalizado de acordo com as necessidades da rede.

Autenticação TACACS+

O TACACS+ é um protocolo de autenticação que os dispositivos Cisco IOS XE podem usar para autenticação de usuários de gerenciamento contra um servidor AAA remoto. Esses usuários de gerenciamento podem acessar o dispositivo IOS-XE via SSH, HTTPS, telnet ou HTTP.

A autenticação TACACS+, ou mais geralmente a autenticação de AAA, fornecem a capacidade para usar o usuário individual esclarecem cada administrador de rede. Quando você não depende de uma única senha compartilhada, a segurança da rede é aumentada e sua responsabilidade é reforçada.

O RADIUS é um protocolo semelhante em propósito ao TACACS+; no entanto, ele somente criptografa a senha enviada pela rede. Por outro lado, o TACACS+ criptografa toda a carga TCP, que inclui o nome de usuário e a senha. Por esse motivo, o TACACS+ pode ser usado de preferência ao RADIUS quando o TACACS+ é suportado pelo servidor AAA. Refira a comparação de TACACS+ e RADIUS para uma comparação mais detalhada destes dois protocolos.

A autenticação TACACS+ pode ser habilitada em um dispositivo Cisco IOS XE com uma configuração semelhante a este exemplo:

aaa new-model

aaa authentication login default group tacacs+

tacacs server <server_name>

address ipv4 <tacacs_server_ip_address>

Key <key>

A configuração precedente pode ser usada como um ponto de início para um molde organização-específico da autenticação de AAA.

Uma lista de métodos é uma lista sequencial que descreve os métodos de autenticação a serem consultados para autenticar um usuário. As listas de métodos permitem designar um ou mais protocolos de segurança a serem usados para autenticação e, assim, garantir um sistema de backup para autenticação, em caso de falha do método inicial. O software Cisco IOS XE usa o primeiro método listado que aceita ou rejeita com êxito um usuário. Os métodos subseqüentes são tentados somente nos casos onde uns métodos mais adiantados falham devido à indisponibilidade ou à configuração incorreta do servidor.

Refira a listas de método nomeadas para a autenticação para obter mais informações sobre da configuração de listas de método nomeadas.

Reserva da autenticação

Se todos os servidores TACACS+ configurados ficarem indisponíveis, um dispositivo Cisco IOS XE poderá confiar em protocolos de autenticação secundários. As configurações típicas incluem o uso do local ou permitem a autenticação se todos os server configurados TACACS+ são não disponíveis.

A lista completa das opções para a autenticação do em-dispositivo inclui permite, local, e linha. Cada um destas opções tem vantagens. O uso o segredo de ativação é preferencial, pois o segredo recebe o hash com um algoritmo unidirecional inerentemente mais seguro do que o algoritmo de criptografia usado com as senhas tipo 7 para autenticação de linha ou local.

No entanto, nas versões do Cisco IOS XE Software que suportam o uso de senhas secretas para usuários definidos localmente, o fallback para autenticação local pode ser desejável. Isto permite para um usuário definido localmente ser criado para um ou vários administradores de rede. Se o TACACS+ deve se tornar completamente não disponível, cada administrador pode usar seu nome de usuário local e senha. Embora essa ação reforce a responsabilidade dos administradores de rede em interrupções do TACACS+, ela aumenta significativamente a carga administrativa, pois as contas de usuário local em todos os dispositivos de rede devem ser mantidas.

Este exemplo de configuração se baseia no exemplo de autenticação TACACS+ anterior para incluir a autenticação de fallback na senha configurada localmente com o comando enable secret:

enable secret <password>

aaa new-model

aaa authentication login default group tacacs+ enable

tacacs server <server_name>

address ipv4 <tacacs_server_ip_address>

Key <key>

Refira a configurar a autenticação para obter mais informações sobre do uso da autenticação da reserva com AAA.

Uso de senhas tipo 7

Originalmente criadas para permitir a descriptografia rápida de senhas armazenadas, as senhas tipo 7 não são uma forma segura de armazenamento de senhas. Há muitas ferramentas disponíveis que podem facilmente decifrar estas senhas. O uso de senhas Tipo 7 pode ser evitado a menos que seja exigido por um recurso que esteja em uso no dispositivo Cisco IOS XE.

O tipo 9 (criptografar) pode ser usado sempre que possível:

username <username> privilege 15 algorithm-type scrypt secret <secret>

A remoção das senhas deste tipo pode ser facilitada com a autenticação de AAA e o uso da característica aumentada da segurança de senha, que permite que as senhas secundárias sejam usadas com usuários que são definidos localmente através do comando global configuration username. Se você não pode prevenir completamente uso de senhas tipo 7, considere estas senhas confundidas, não cifradas.

Consulte a seção Blindagem geral do plano de gerenciamento deste documento para obter mais informações sobre a remoção de senhas tipo 7.

Autorização do comando TACACS+

O comando authorization com TACACS+ e AAA fornece um mecanismo que permita ou nega cada comando que é incorporado por um usuário administrativo. Quando o usuário insere comandos EXEC, o Cisco IOS XE envia cada comando para o servidor AAA configurado. O servidor AAA usa então as políticas configuradas para permitir ou negar o comando para este usuário particular.

Esta configuração pode ser adicionada ao exemplo precedente da autenticação de AAA a fim executar o comando authorization:

aaa authorization exec default group tacacs+ none

aaa authorization commands 0 default group tacacs+ none

aaa authorization commands 1 default group tacacs+ none

aaa authorization command 15 default group tacacs+ none

Refira a configurar a autorização para obter mais informações sobre do comando authorization.

Contabilidade do comando TACACS+

Quando configurado, a contabilidade do comando aaa envia a informação sobre cada comando EXEC que é inscrito nos servidores configurados TACACS+. As informações enviadas ao servidor TACACS+ incluem o comando executado, a data em que foi executado e o nome de usuário da pessoa que inseriu o comando. A contabilização do comando não é compatível com o RADIUS.

Este exemplo de configuração permite o comando aaa que esclarece os comandos EXEC inscritos nos níveis de privilégio zero, um, e 15. Construções desta configuração em cima dos exemplos anteriores que incluem a configuração dos servidores de TACACS.

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 0 default start-stop group tacacs+

aaa accounting commands 1 default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

Consulte Configuração da contabilização para obter mais informações sobre a configuração da contabilização AAA.

Servidores AAA redundantes

Os servidores AAA que são aproveitados em um ambiente podem ser redundantes e implantados de maneira tolerante a falhas. Isto ajuda a assegurar-se de que o acesso de gerenciamento interativo, tal como o SSH, seja possível se um servidor AAA é não disponível.

Ao projetar ou implementar uma solução de servidor AAA redundante, lembre-se destas considerações:

1. Disponibilidade dos servidores AAA durante falhas da rede potencial
2. Colocação geográfica dispersada dos servidores AAA
3. Carregar em servidores AAA individuais em condições de estado estacionário e de falha
4. Latência da rede entre servidores do acesso de rede e servidores AAA
5. Sincronização das bases de dados do servidor AAA

Consulte para distribuir os server do controle de acesso para mais informação.

Fortalecer o Simple Network Management Protocol

Esta seção destaca vários métodos que podem ser usados para proteger a implantação do SNMP em dispositivos IOS-XE. É fundamental que o SNMP seja protegido corretamente para resguardar a confidencialidade, integridade e disponibilidade dos dados de rede e dos dispositivos de rede em que esses dados transitam. O SNMP fornece-o uma riqueza de informação na saúde dos dispositivos de rede. Essas informações podem ser protegidas de usuários mal-intencionados que desejam aproveitar esses dados para realizar ataques contra a rede.

Strings de comunidade SNMP

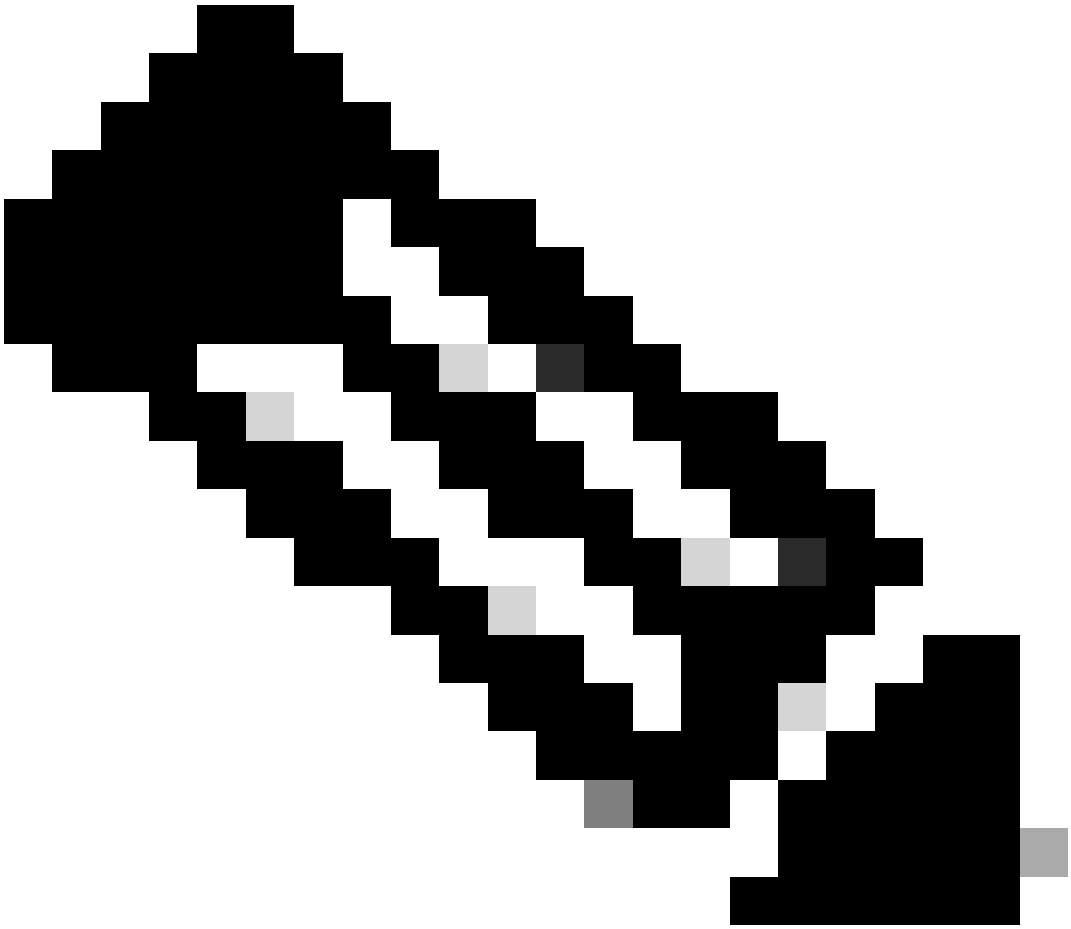
As strings de comunidade são senhas que são aplicadas a um dispositivo IOS-XE para restringir o acesso, somente leitura e leitura-gravação, aos dados SNMP no dispositivo. Essas strings de comunidade, como todas as senhas, podem ser cuidadosamente escolhidas para garantir que não sejam triviais. As strings de comunidade podem ser alteradas em intervalos regulares e de acordo com as políticas de segurança de rede.

Por exemplo, as strings podem ser alteradas quando um administrador de rede muda de função ou sai da empresa.

Estas linhas de configuração configuram uma série de comunidade somente leitura e SOMENTE LEITURA e uma série de comunidade de leitura/gravação de DE LEITURA/GRAVAÇÃO:

snmp-server community READONLY RO

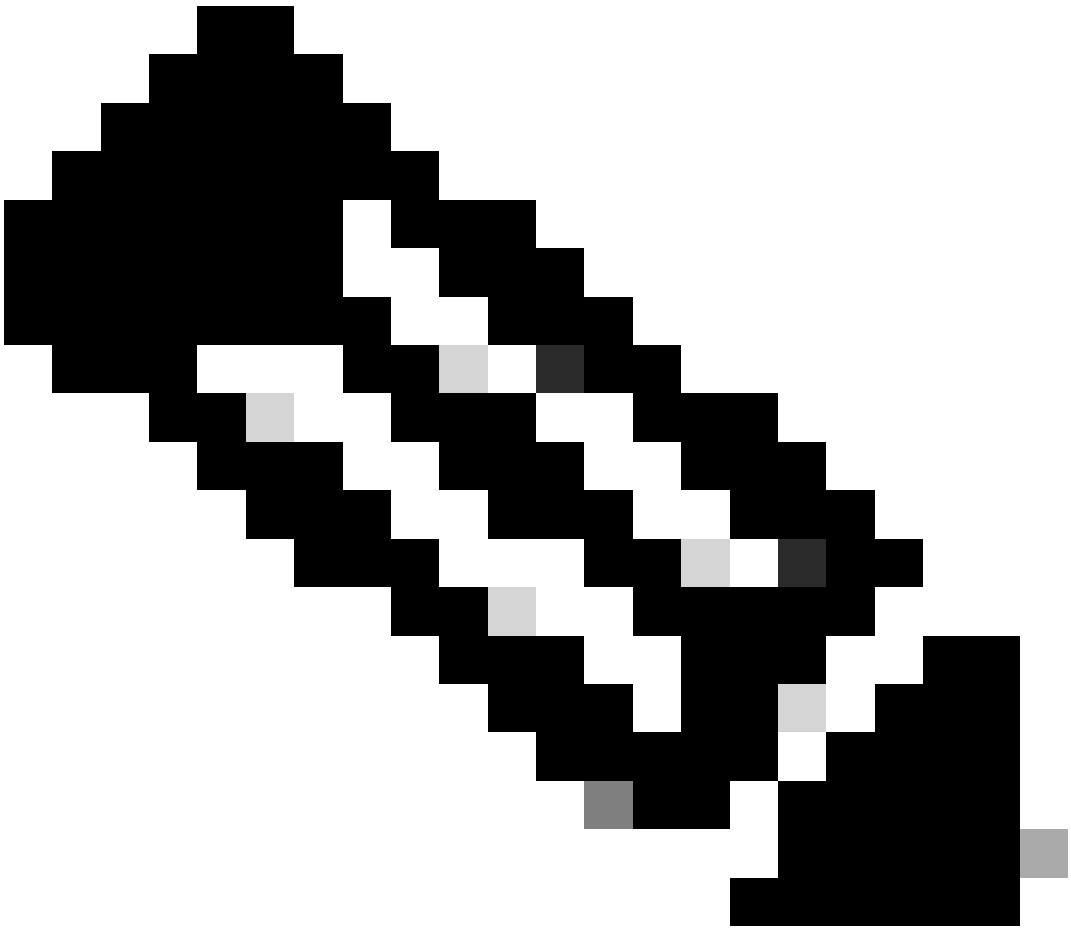
snmp-server community READWRITE RW



Observação: os exemplos de string de comunidade anteriores foram escolhidos para explicar claramente o uso dessas strings. Para ambientes de produção, as strings de comunidade podem ser escolhidas com cuidado e podem consistir em uma série de símbolos alfabéticos, numéricos e não alfanuméricos. Refira a recomendações para criar senhas elaboradas para obter mais informações sobre da seleção de senhas não-triviais.

Séries de comunidade snmp com ACL

Além da sequência de comunidade, pode ser aplicada uma ACL que restringe ainda mais o acesso SNMP a um grupo selecionado de endereços IP de origem. Essa configuração restringe o acesso somente leitura SNMP aos dispositivos de host final que residem no espaço de endereço 192.168.100.0/24 e restringe o acesso de leitura/gravação SNMP apenas ao dispositivo de host final em 192.168.100.1.



Observação: os dispositivos permitidos por essas ACLs exigem a sequência de comunidade apropriada para acessar as informações SNMP solicitadas.

access-list 98 permit 192.168.100.0 0.0.0.255

access-list 99 permit 192.168.100.1

snmp-server community READONLY RO 98

snmp-server community READWRITE RW 99

Consulte snmp-server community na Referência de Comandos de Gerenciamento de Rede do Cisco IOS XE para obter mais informações sobre esse recurso.

Infra-estrutura ACL

As ACLs de infraestrutura (iACLs) podem ser implantadas para garantir que somente os hosts finais com endereços IP confiáveis possam enviar o tráfego SNMP para um dispositivo IOS-XE. Um iACL pode conter uma política que nega pacotes SNMP não autorizados na porta UDP 161.

Consulte a seção Limitar o Acesso à Rede com ACLs de Infraestrutura deste documento para obter mais informações sobre o uso de iACLs.

SNMP Views

Os SNMP Views são uns recursos de segurança que possam permitir ou negar o acesso a determinado SNMP MIB. Depois que uma exibição é criada e aplicada a uma sequência de comunidade com os comandos de configuração global snmp-server community string view, se você acessar os dados da MIB, ficará restrito às permissões definidas pela exibição. Quando apropriado, é recomendado usar visualizações para limitar usuários do SNMP aos dados que exigem.

Este exemplo de configuração restringe o acesso SNMP com o string de comunidade LIMITADO aos dados MIB que estão situados no grupo de sistema:

snmp-server view <view_name> <mib_view_family_name> [include/exclude]

snmp-server community <community_string>view <view_name> RO

Refira aconfigurar o apoio SNMP para mais informação.

SNMP Versão 3

O SNMP versão 3 (SNMPv3) é definido pelo RFC3410 , pelo RFC3411 , pelo RFC3412 , pelo RFC3413 , pelo RFC3414 , e pelo RFC3415 e é um protocolo baseando em padrões interoperáveis para o gerenciamento de rede. O SNMPv3 fornece acesso seguro aos dispositivos, pois autentica e facultativamente criptografa pacotes na rede. Quando compatível, o SNMPv3 pode ser usado para adicionar outra camada de segurança ao implantar o SNMP. O SNMPv3 consiste em três opções de configuração preliminares:

1. no auth - Este modo não requer nenhuma autenticação nem criptografia de pacotes SNMP.
2. auth - Este modo requer autenticação do pacote SNMP sem criptografia.

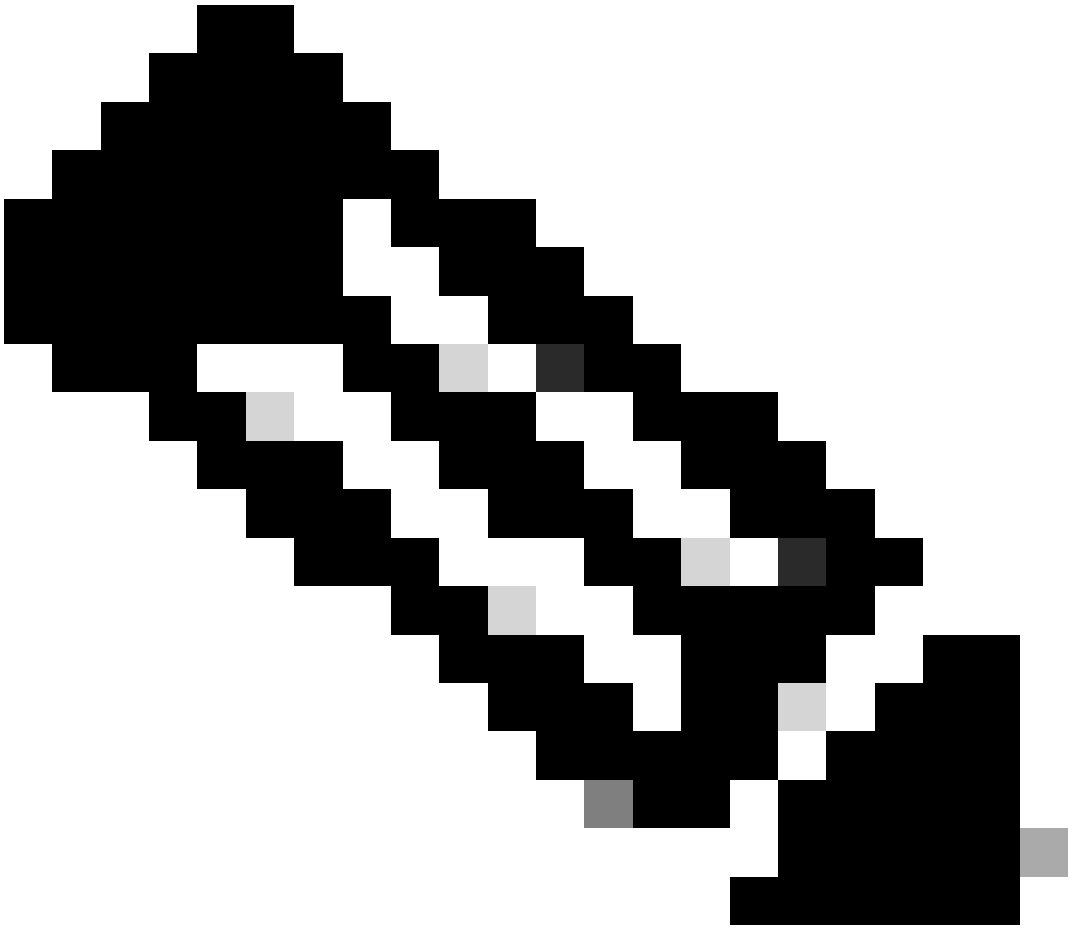
3. priv - Este modo requer autenticação e criptografia (privacidade) de cada pacote SNMP.

   Um ID de mecanismo autoritativo deve existir para usar a autenticação ou criptografia dos mecanismos de segurança SNMPv3 - para manipular pacotes SNMP; por padrão, o ID do mecanismo é gerado localmente. O Engine ID pode ser indicado com o comando show snmp engineID segundo as indicações deste exemplo:

   router#show snmp engineID

EngineID SNMP local: 800000090300000152BD35496

Porta de endereço IP da ID do mecanismo remoto



Observação: se o engineID for alterado, todas as contas de usuário SNMP deverão ser reconfiguradas.

A próxima etapa é configurar um grupo SNMPv3. Este comando configura um dispositivo Cisco

IOS XE para SNMPv3 com um grupo de servidor SNMP AUTHGROUP e habilita somente a autenticação para este grupo com a palavra-chave auth:

snmp-server group AUTHGROUP v3 auth

Este comando configura um dispositivo Cisco IOS XE para SNMPv3 com um grupo de servidores SNMP.

PRIVGROUP e habilita a autenticação e a criptografia para esse grupo com a palavra-chave privada:

snmp-server group PRIVGROUP v3 priv

Este comando configura SNMPv3 um usuário snmpv3user com uma senha da autenticação md5 do authpassword e uma senha da criptografia 3DES do privpassword:

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des privpassword

Esteja ciente de que os comandos de configuração snmp-server user não são exibidos na saída de configuração do dispositivo conforme exigido pelo RFC 3414; portanto, a senha do usuário não é visível na configuração. A fim de ver os usuários configurados, inscreva o comando show snmp user segundo as indicações deste exemplo:

router#show snmp user

Nome de usuário: snmpv3user ID do mecanismo: 80000090300000152BD35496

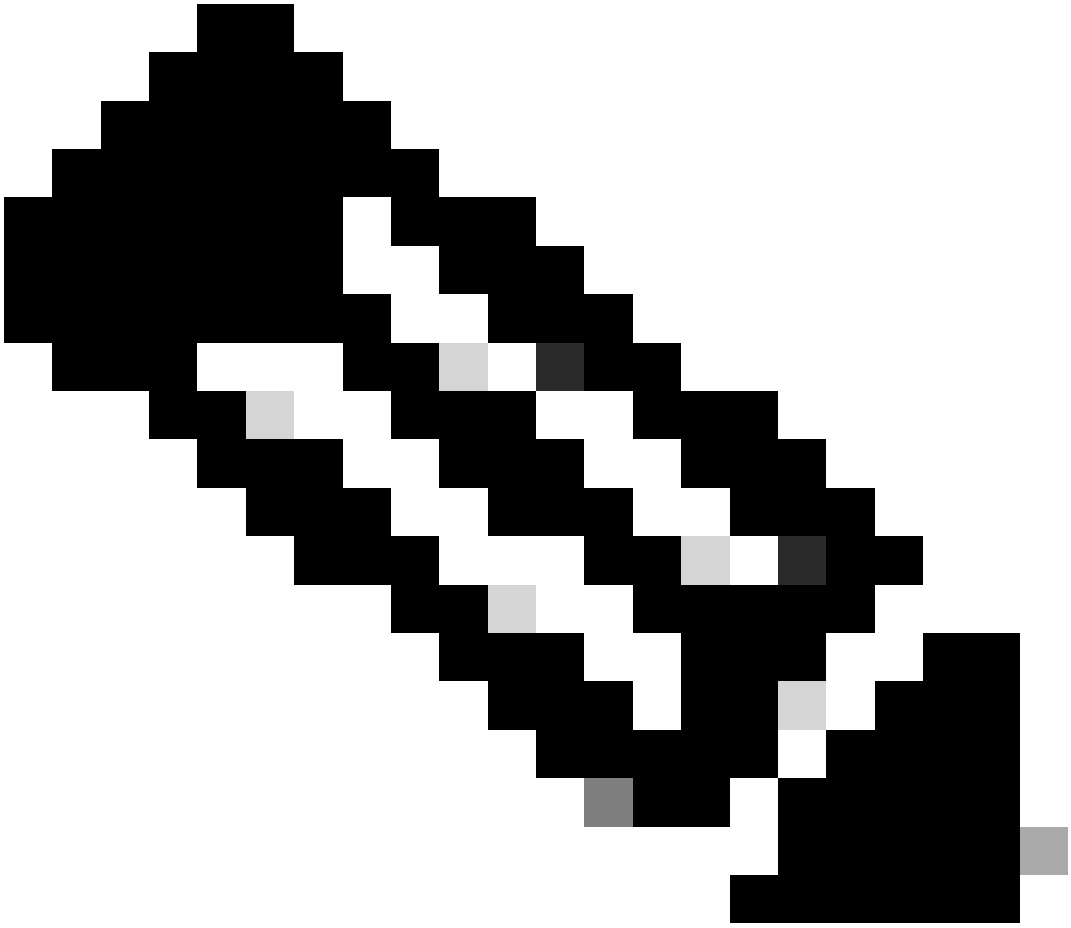
storage-type: nonvolatile ative

Protocolo de autenticação: MD5
Protocolo de privacidade: 3DES
Nome do grupo: PRIVGROUP

Refira a configurar o suporte SNMP para obter mais informações sobre desta característica.

Proteção do plano de gerenciamento

O recurso Management Plane Protection (MPP) no software Cisco IOS XE pode ser usado para ajudar a proteger o SNMP, pois restringe as interfaces através das quais o tráfego SNMP pode terminar no dispositivo. A característica PMP (produção máxima possível) permite que um administrador designe umas ou várias relações como interfaces de gerenciamento. O tráfego de gerenciamento é permitido para entrar em um dispositivo somente através destas interfaces de gerenciamento. Depois que a PMP (produção máxima possível) é permitida, nenhumas relações a não ser que as interfaces de gerenciamento designadas aceitem o tráfego de gerenciamento de rede que é destinado ao dispositivo.



Observação: o MPP é um subconjunto do recurso CPPr e requer uma versão do IOS que suporte CPPr. Refira a compreendendo a proteção plana do controle para obter mais informações sobre de CPPr.

Neste exemplo, a PMP (produção máxima possível) é usada a fim de restringir o acesso SNMP e SSH somente à relação do FastEthernet0/0:

host de plano de controle

management-interface FastEthernet0/0 allow ssh snmp

Refira ao guia dos recursos de proteção do plano de gerenciamento para mais informação.

Melhores práticas de registo

O registro de eventos oferece visibilidade da operação de um dispositivo Cisco IOS XE e da rede na qual ele está implantado. O software Cisco IOS XE fornece várias opções de registro flexíveis

que podem ajudar a alcançar os objetivos de gerenciamento de rede e visibilidade de uma organização.

Estas seções fornecem algumas práticas recomendadas básicas de registro que podem ajudar um administrador a aproveitar com sucesso o registro e minimizar o impacto do registro em um dispositivo Cisco IOS XE.

Envie registros a um local central

É recomendado enviar a informação de registro a um servidor de SYSLOG remoto. Isso possibilita a correlação e a auditoria de eventos de segurança e de rede entre dispositivos de rede com mais eficiência. Esteja ciente de que as mensagens de syslog são transmitidas de forma não confiável pelo UDP e em texto claro. Por esse motivo, qualquer proteção que uma rede oferece ao tráfego de gerenciamento (por exemplo, criptografia ou acesso fora de banda) pode ser estendida para incluir o tráfego de syslog.

Este exemplo de configuração configura um dispositivo Cisco IOS XE para enviar informações de registro a um servidor syslog remoto:

logging host <ip-address>

Consulte Identificação de Incidentes Usando Firewall e Eventos Syslog do Roteador IOS-XE para obter mais informações sobre correlação de logs.

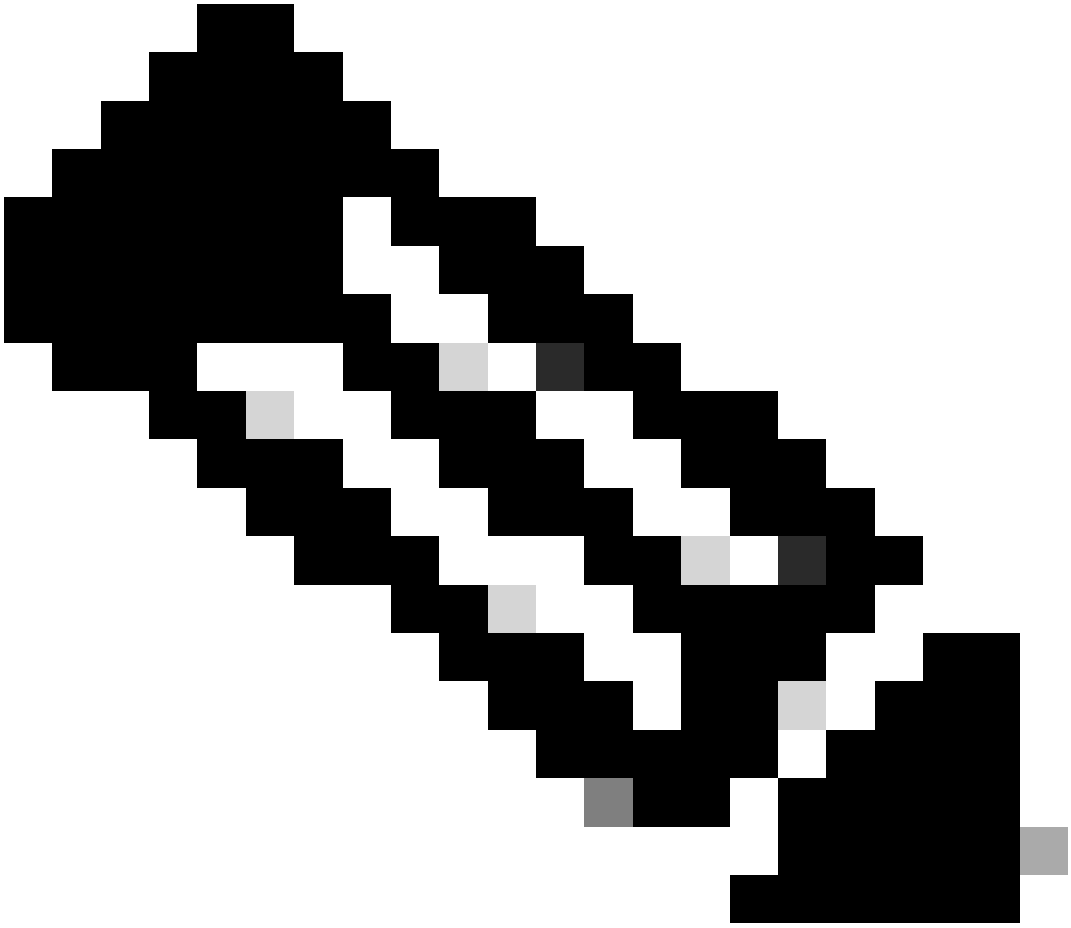
O recurso Logging to Local Nonvolatile Storage (ATA Disk) permite que as mensagens de registro do sistema sejam salvas em um disco flash ATA (Advanced Technology Attachment, tecnologia avançada de conexão). As mensagens salvas em uma movimentação ATA persistem depois que um roteador é recarregado.

Essas linhas de configuração configuram 134.217.728 bytes (128 MB) de mensagens de registro no diretório syslog da flash ATA (disk0) e especificam um tamanho de arquivo de 16.384 bytes:

registro colocado em buffer.

logging persistent url disk0:/syslog size 134217728 filesize 16384

Antes que as mensagens de registro sejam gravadas em um arquivo no disco ATA, o software Cisco IOS XE verifica se há espaço em disco suficiente. Se não, o arquivo o mais velho das mensagens de registro (pelo timestamp) é suprimido, e o arquivo atual é salvo. O formato do nome do arquivo é log_month:day:year::time.



Observação: uma unidade flash ATA tem espaço em disco limitado e, portanto, precisa ser mantida para evitar um excesso de dados armazenados.

Este exemplo mostra como copiar mensagens de registro do disco ATA flash do roteador para um disco externo no servidor FTP 192.168.1.129, como parte dos procedimentos de manutenção:

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

Consulte Logging to Local Nonvolatile Storage para obter mais informações sobre este recurso.

Nível de registro

A cada mensagem de registro gerada por um dispositivo Cisco IOS XE é atribuída uma das oito severidades que vão do nível 0, Emergências, até o nível 7, Depuração. A menos que seja especificamente necessário, você deve evitar o registro no nível 7. O registro no nível 7 produz uma carga elevada da CPU no dispositivo, o que pode levar à instabilidade do dispositivo e da rede.

O comando de configuração global logging trap é usado para especificar quais mensagens de registro são enviadas aos servidores syslog remotos. O nível especificado indica a mais baixa mensagem da severidade que é enviada. Para o registo protegido, o comando logging buffered level é usado.

Este exemplo de configuração limita os mensagens de registro que são enviados aos servidores de SYSLOG remotos e ao buffer de registro local às gravidades 6 (informativo) com 0 (emergências):

logging trap 6

logging buffered 6

Não registre para consolar ou sessões de monitor

Com o software Cisco IOS XE, é possível enviar mensagens de registro para monitorar sessões - as sessões de monitoramento são sessões de gerenciamento interativas nas quais o comando EXEC terminal monitor foi emitido - e para o console. No entanto, isso pode elevar a carga da CPU de um dispositivo IOS-XE e, portanto, não é recomendado. Em vez disso, recomendamos enviar a informação de registro para o buffer de registro local, que pode ser exibido por meio do comando show logging.

Use os comandos de configuração global no logging console e no logging monitor para desabilitar o registro para o console e para as sessões de monitoramento. Este exemplo de configuração mostra o uso destes comandos:

no logging console

no logging monitor

Consulte Referência de Comandos de Gerenciamento de Rede do Cisco IOS XE para obter mais informações sobre comandos de configuração global.

Use o registo protegido

O software Cisco IOS XE suporta o uso de um buffer de registro local para que um administrador possa visualizar mensagens de registro geradas localmente. O uso do registo protegido é altamente recomendado contra o registo ao console ou às sessões de monitor.

Há duas opções de configuração que são relevantes ao configurar o registro em buffer: o tamanho do buffer de registro e a severidade da mensagem que é armazenada no buffer. O tamanho do logging buffer é configurado com o comando global configuration que registra o tamanho protegido. A menor gravidade incluída no buffer é configurada com o comando logging buffered severity. Um administrador pode ver os índices do logging buffer através do comando show logging exec.

Este exemplo de configuração inclui a configuração de um buffer de registro de 16384 bytes, bem como uma gravidade de 6, informativa, que indica que as mensagens nos níveis de 0

(emergências) a 6 (informativas) são armazenadas:

logging buffered 16384 6

Consulte Cisco IOS XE Setting the Message Display Destination Device para obter mais informações sobre o registro em buffer.

Configurar a interface de origem de registo

Para fornecer um nível maior de consistência ao coletar e revisar mensagens de registro, é recomendável configurar estaticamente uma interface de origem de registro.

Realizado através do comando de interface logging source-interface, configurar estaticamente uma interface de origem de registro garante que o mesmo endereço IP apareça em todas as mensagens de registro enviadas de um dispositivo Cisco IOS individual. Para a estabilidade adicionada, é recomendado usar uma interface de loopback como a fonte de registo.

Este exemplo de configuração ilustra o uso do comando de configuração global de interface logging source-interface para especificar que o endereço IP da interface de loopback 0 seja usado para todas as mensagens de registro:

logging source-interface Loopback 0

Consulte o Cisco IOS XE Embedded Syslog Manager para obter mais informações.

Configurar data/hora de registro

A configuração de data/hora de registro ajuda-o a correlacionar eventos através dos dispositivos de rede. É importante executar uma configuração correta e consistente de data/hora de registro assegurar-se de que você possa correlacionar dados de registo. Os timestamps de registro podem ser configurados para incluir a data e a hora com precisão de milissegundos e para incluir o fuso horário em uso no dispositivo.

Este exemplo inclui a configuração de data/hora de registro com precisão do milissegundo dentro da zona do tempo universal coordenada (UTC):

service timestamps log datetime msec show-timezone

Se você prefere não registrar as épocas UTC relativas, você pode configurar um fuso horário local específico e configurá-lo que a informação esta presente na mensagens do log gerada. Este exemplo mostra uma configuração de dispositivo para a zona do horário padrão do pacífico (PST):

clock timezone PST -8

service timestamps log datetime msec localtime show-timezone

Gerenciamento de configuração do software Cisco IOS XE

O software Cisco IOS XE inclui vários recursos que podem permitir uma forma de gerenciamento de configuração em um dispositivo Cisco IOS XE. Tais características incluem a funcionalidade para arquivar as configurações e ao rollback a configuração a uma versão anterior assim como para criar um registro da mudança de configuração detalhada.

Substituir configuração e configuração Rollback

No Cisco IOS XE Software Release 16.6.4 e posterior, os recursos Substituição de Configuração e Reversão de Configuração permitem arquivar a configuração do dispositivo Cisco IOS XE no dispositivo. Armazenadas manual ou automaticamente, as configurações neste arquivo podem ser usadas para substituir a configuração em execução atual com o comando de nome do arquivo configure replace. Isto é em contraste com o copiar nome de arquivo comando running-config. O comando configurar substituir nome de arquivo substitui a configuração running ao contrário da fusão executada pelo comando copy.

É recomendado habilitar esse recurso em todos os dispositivos Cisco IOS XE na rede. Uma vez ativada, um administrador pode fazer com que a configuração atual em execução seja adicionada ao arquivo com o comando EXEC privilegiado archive config. As configurações arquivadas podem ser visualizadas com o comando EXEC show archive.

Este exemplo ilustra a configuração de arquivo da configuração automática. Ele também instrui o dispositivo Cisco IOS XE a armazenar configurações arquivadas como arquivos chamados archived-config-N no sistema de arquivos disk0:, manter um máximo de 14 backups e arquivar uma vez por dia (1440 minutos) e quando um administrador executar o comando EXEC write memory.

arquivo

path disk0:archived-config

máximo 14

time-period 1440

Embora a funcionalidade de arquivamento de configuração possa armazenar até 14 configurações de backup, você deve considerar os requisitos de espaço antes de usar o comando maximum.

Configuração Exclusiva de Alteração de Acesso

Adicionado ao Cisco IOS XE Software Release 16.6.4, o recurso Exclusive Configuration Change Access garante que apenas um administrador faça alterações de configuração em um dispositivo Cisco IOS XE em um determinado momento. Esta característica ajuda a eliminar o impacto indesejado das mudanças simultâneas feitas aos componentes da configuração relacionada. Este recurso é configurado com o comando de configuração global modo de configuração exclusivo e opera em um de dois modos: automático e manual. No auto-MODE, a configuração trava automaticamente quando um administrador emite o comando exec do terminal configurar. No modo manual, o administrador usa o comando configure terminal lock para bloquear a

configuração quando entra no modo de configuração.

Este exemplo ilustra a configuração desta característica para o travamento da configuração automática:

modo de configuração exclusivo

Software Cisco assinado Digital

Adicionado no Cisco IOS XE Software Release 16.1 e superior, o recurso Digital Signed Cisco Software facilita o uso do Cisco IOS XE Software que é digitalmente assinado e, portanto, confiável, com o uso de criptografia assimétrica segura (chave pública).

Uma imagem digital assinada leva (com uma chave privada) uma mistura criptografada dse. Após a verificação, o dispositivo descriptografa o hash com a chave pública correspondente das chaves encontradas no armazenamento de chaves e também calcula seu próprio hash da imagem. Se a mistura decifrada combina a mistura calculada da imagem, a imagem não foi alterada e pode ser confiada.

As chaves Digitais do software Cisco são identificadas pelo tipo e pela versão da chave. Uma chave pode ser especial, uma produção, ou um tipo chave do derrubamento. A produção e os tipos chaves especiais têm uma versão chave associada que incremente alfabeticamente sempre que a chave é revogada e substituída. Tanto as imagens ROMMON como as imagens regulares do Cisco IOS XE são assinadas com uma chave especial ou de produção quando você usa o recurso Software Cisco Digitally Signed. A imagem ROMMON pode ser atualizada e deve ser assinada com a mesma chave que a imagem especial ou de produção carregada.

Esse comando verifica a integridade da imagem isr4300-universalk9.16.06.04.SPA.bin na memória flash com as chaves no armazenamento de chaves do dispositivo:

show software authentication file bootflash:isr4300-universalk9.16.06.04.SPA.bin

Refira ao software Cisco Digital Assinado para obter mais informações sobre esta característica.

Uma nova imagem (isr4300-universalk9.16.10.03.SPA.bin) pode então ser copiada para a flash a ser carregada e a assinatura da imagem é verificada com a chave especial recém-adicionada

copy /verify tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin flash:

Notificação e registo da alteração de configuração

O recurso Notificação e registro de alteração de configuração, adicionado ao Cisco IOS XE Software Release 16.6.4, permite registrar as alterações de configuração feitas em um dispositivo Cisco IOS XE. O registro é mantido no dispositivo Cisco IOS XE e contém as informações de usuário do indivíduo que fez a alteração, o comando de configuração inserido e a hora em que a alteração foi feita. Essa funcionalidade é ativada com o comando de modo de configuração logging enable configuration change logger. Os comandos opcionais hide keys e logging size são usados para melhorar a configuração padrão porque impedem o registro de dados de senha e

aumentam o comprimento do registro de alterações.

Você é recomendado habilitar essa funcionalidade para que o histórico de alteração de configuração de um dispositivo Cisco IOS XE possa ser mais facilmente entendido. Além disso, é recomendável usar o comando de configuração notify syslog para ativar a geração de mensagens syslog, quando uma alteração de configuração é feita.

arquivo

log config

logging enable

logging size 200

teclas de ocultação

notifique o syslog

Após a notificação e os recursos de registro da alteração de configuração serem habilitados, a configuração do log de arquivo do privileged exec command show pode ser usado a fim ver o registro da configuração.

Controle o plano

As funções do plano de controle consistem em protocolos e processos que se comunicam entre dispositivos de rede para migrar os dados da origem para o destino. Isto inclui protocolos de roteamento como o Border Gateway Protocol, além de protocolos como o ICMP e o Resource Reservation Protocol (RSVP).

É importante que os eventos nos planos da gestão e dos dados não afetem adversamente o plano do controle. Quando um evento de plano de dados, como um ataque de DoS, afeta o plano de controle, toda a rede pode se tornar instável. Essas informações sobre os recursos e as configurações do software Cisco IOS XE podem ajudar a garantir a resiliência do plano de controle.

Endurecimento plano do controle geral

A proteção do plano do controle de um dispositivo de rede é crítica porque o plano do controle se assegura de que os planos da gestão e dos dados sejam mantidos e operacionais. Se o plano do controle era se tornar instável durante um incidente de segurança, pode ser impossível para você recuperar a estabilidade da rede.

Em muitos casos, é possível desativar o recebimento e a transmissão de certos tipos de mensagens em uma interface, para minimizar a quantidade de carga da CPU necessária para processar pacotes desnecessários.

Redirecionamentos de IP ICMP

Uma mensagem do redirecionamento de ICMP pode ser gerada por um roteador quando um pacote é recebido e transmitido na mesma relação. Nesta situação, o roteador encaminha o pacote e envia uma mensagem do redirecionamento de ICMP de volta ao remetente do pacote original. Este comportamento permite que o remetente contorneie o roteador e encaminhe pacotes futuros diretamente ao destino (ou a um roteador mais perto do destino). Em uma rede IP de funcionamento correto, um roteador envia reorienta somente aos anfitriões em suas próprias sub-redes local. Em outras palavras, os redirecionamentos de ICMP nunca podem ir além de um limite de Camada 3.

Há dois tipos de mensagens de redirecionamento ICMP: redirecionar para um endereço de host e redirecionar para uma sub-rede inteira. Um usuário mal-intencionado pode explorar a capacidade do roteador de enviar redirecionamentos de ICMP por meio do envio contínuo de pacotes ao roteador, o que força o roteador a responder com mensagens de redirecionamento de ICMP e resulta em um impacto adverso na CPU e no desempenho do roteador. A fim de impedir que o roteador envie redirecionamentos de ICMP, use o comando interface configuration do no ip redirects.

ICMP não alcançável

Filtrar com uma lista de acessos da relação induz a transmissão dos mensagens que não chega a seu destino do ICMP de volta à fonte do tráfego filtrado. A geração dessas mensagens pode aumentar a utilização da CPU no dispositivo. No Cisco IOS XE Software, a geração de ICMP inalcançável é limitada a um pacote a cada 500 milissegundos por padrão. A geração de mensagens inacessíveis de ICMP pode ser desativada com o comando de configuração de interface no ip unreachable. O limite de taxas inacessíveis de ICMP pode ser alterado em relação ao padrão com o comando de configuração global ip icmp rate-limit unreachable interval-in-ms.

Proxy ARP

O proxy ARP é a técnica em qual dispositivo, geralmente um roteador, as requisições ARP das respostas que são pretendidas para um outro dispositivo. Ao fingir sua identidade, o roteador aceita a responsabilidade pelo roteamento de pacotes para o destino real. O Proxy ARP pode ajudar máquinas em uma sub-rede a alcançar sub-redes remotas sem configurar o roteamento ou um gateway padrão. O proxy ARP é definido no RFC 1027.

Há várias desvantagens na utilização do proxy ARP. Isso pode resultar em um aumento no volume de tráfego ARP no segmento de rede e no esgotamento de recursos, além de ataques man-in-the-middle. O proxy ARP apresenta um vetor do ataque do esgotamento de recurso porque cada requisição ARP proxied consome uma quantidade pequena de memória. Um invasor pode esgotar toda a memória disponível, se enviar um grande número de solicitações ARP.

Os ataques man-in-the-middle permitem que um host na rede falsifique o endereço MAC do roteador, o que faz com que hosts inocentes enviem o tráfego para o invasor. O proxy ARP pode ser desativado com o comando de configuração de interface no ip proxy-arp.

Consulte Habilitação e Desabilitação do Proxy ARP para obter mais informações sobre esta característica.

Mensagens de controle de NTP

As consultas de mensagem de controle de NTP são funções do NTP que auxiliam nas funções de gerenciamento de rede (NM) antes que NMs melhores sejam criados e utilizados. A menos que sua organização ainda esteja usando NTP para funções NM, as Melhores formas de aprendizado de segurança de rede são desativá-las completamente. Se você os estiver usando, eles poderão ser um serviço de tipo somente de rede interna bloqueado pelo firewall ou outro dispositivo externo. Eles foram até mesmo removidos de todas as versões do IOS e do IOS-XE, exceto as versões padrão, já que o IOS-XR e o NX-OS não os suportam.

Se você optar por desativar esse recurso, o comando será

```
Router (config)# no ntp allow mode control
```

Esse comando então aparece na configuração atual como no ntp allow mode control 0. Ao fazer isso, você desativou as mensagens de controle do NTP no dispositivo e protegeu o dispositivo contra ataques.

Limitar o impacto do tráfego do plano de controle na CPU

A proteção do plano do controle é crítica. Porque o desempenho do aplicativo e a experiência de usuário final podem sofrer sem a presença de dados e de tráfego de gerenciamento, a sobrevivência do plano do controle assegura-se de que outros dois planos sejam mantidos e operacionais.

Entender o tráfego do plano de controle

Para proteger corretamente o plano de controle do dispositivo Cisco IOS XE, é essencial entender os tipos de tráfego que são comutados por processo pela CPU. O tráfego comutado do processo consiste normalmente em dois tipos de tráfego diferentes. O primeiro tipo de tráfego é direcionado para o dispositivo Cisco IOS XE e deve ser manipulado diretamente pela CPU do dispositivo Cisco IOS XE. Esse tráfego consiste na categoria Recebimento de tráfego de adjacências. Esse tráfego contém uma entrada na tabela Cisco Express Forwarding (CEF) em que o próximo salto do roteador é o próprio dispositivo, o que é indicado pelo termo receive na saída da CLI show ip cef . Essa indicação é o caso de qualquer endereço IP que exija tratamento direto pela CPU do dispositivo Cisco IOS XE, que inclui endereços IP da interface, espaço de endereço multicast e espaço de endereço de broadcast.

O segundo tipo de tráfego que é tratado pela CPU é o tráfego plano de dados - tráfego com um destino além do próprio dispositivo Cisco IOS XE - que requer processamento especial pela CPU. Embora não seja uma lista exaustiva de CPUs que impactam o tráfego do plano de dados, esses tipos de tráfego são comutados por processo e, portanto, podem afetar a operação do plano de controle:

1. Access Control List logging – O tráfego de registro da ACL consiste em todos os pacotes gerados devido a uma correspondência (permissão ou negação) de uma ACE em que a palavra-chave log é usada.

2. Unicast Reverse Path Forwarding (Unicast RPF) – O Unicast RPF, usado em conjunto com uma ACL, pode resultar no switching de processos de determinados pacotes.
3. Opções de IP – Todos os pacotes IP com opções incluídas devem ser processados pela CPU.
4. Fragmentação – Qualquer pacote IP que exija fragmentação deve ser passado para a CPU para processamento.
5. Expiração Time-to-Live (TTL) – Os pacotes que têm um valor TTL menor ou igual a um exigem o envio de mensagens Internet Control Message Protocol Time Exceeded (ICMP Tipo 11, Código 0), o que resulta no processamento da CPU.
6. Inacessíveis de ICMP – Os pacotes que resultam em mensagens inacessíveis de ICMP devido ao roteamento, à MTU ou à filtragem são processados pela CPU.
7. Tráfego que exige uma solicitação ARP – Os destinos para os quais não existe uma entrada ARP exigem processamento pela CPU.
8. Tráfego não IP – Todo o tráfego não IP é processado pela CPU.

   Esta lista detalha vários métodos para determinar quais tipos de tráfego são processados pela CPU do dispositivo Cisco IOS XE:
9. O comando show ip cef fornece a informação do salto seguinte para cada prefixo IP que é contido na tabela de CEF. Como indicado anteriormente, as entradas que contêm recepção como o próximo salto são consideradas adjacências de recepção e indicam que o tráfego deve ser enviado diretamente para a CPU.
10. O comando show interface switching fornece informações sobre o número de pacotes comutados por processo por um dispositivo.
11. O comando show ip traffic fornece informações sobre o número de pacotes IP: com um destino local (ou seja, tráfego de adjacência de recebimento) com opções que exigem fragmentação que são enviadas para o espaço de endereço de broadcast que são enviadas para o espaço de endereço de multicast.
12. Receba o tráfego da adjacência pode ser identificado com o uso do comando show ip cache flow. Todos os fluxos destinados ao dispositivo Cisco IOS XE têm uma interface de destino (DstIf) local.
13. O policiamento do plano de controle pode ser usado para identificar o tipo e a taxa de tráfego que alcança o plano de controle do dispositivo Cisco IOS XE. As políticas de plano de controle podem ser executadas por meio da utilização de ACLs de classificação granular, logging e por meio da utlização do comando show policy-map control-plane .

Infra-estrutura ACL

A infra-estrutura ACL (iACLs) limita uma comunicação externa aos dispositivos da rede.

As ACLs para infraestrutura são discutidas amplamente na seção Limitar o acesso à rede com ACLs para infraestrutura deste documento.

É recomendável implementar iACLs para proteger o plano de controle de todos os dispositivos de rede.

ACLs de Recebimento

O rACL protege o dispositivo do tráfego prejudicial antes do tráfego impacta o processador de rotas. Receba ACL são projetados proteger somente o dispositivo em que é configurado e o tráfego de trânsito não é afetado por um rACL. Como resultado, o endereço IP de destino any usado nas entradas ACL do exemplo refere-se apenas aos endereços IP físicos ou virtuais do roteador. As ACLs de recepção também são consideradas uma prática recomendada de segurança de rede e podem ser consideradas como um acréscimo de longo prazo à boa segurança de rede.

Este é o trajeto ACL da recepção que é escrito para permitir o tráfego SSH (porta TCP 22) dos host confiável na rede 192.168.100.0/24:

— Permitir SSH de hosts confiáveis permitidos para o dispositivo.

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22

— Negue SSH de todas as outras fontes para o RP.

access-list 151 deny tcp any any eq 22

— Permita todo o tráfego restante para o dispositivo.

— de acordo com a política e as configurações de segurança.

access-list 151 permit ip any any

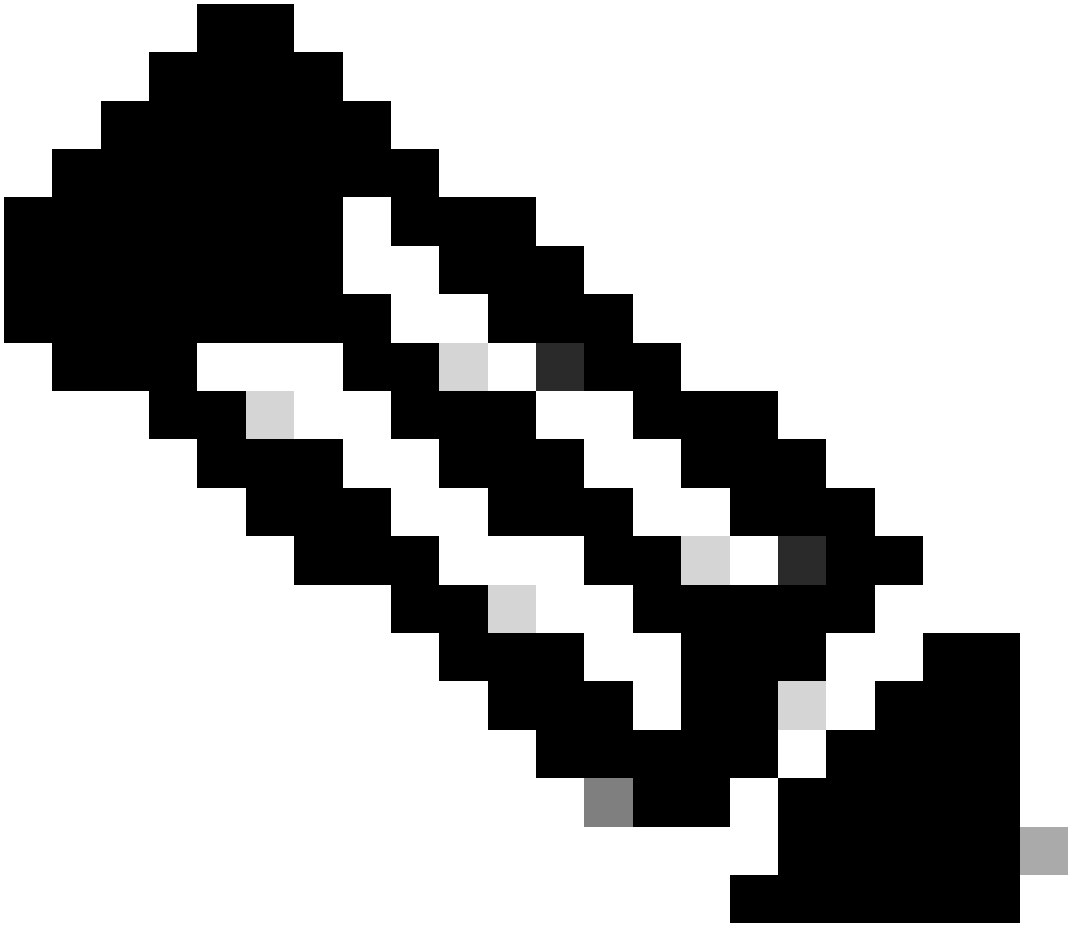
— Aplique essa lista de acesso ao caminho de recebimento.

ip receive access-list 151

Consulte Listas de Controle de Acesso para ajudar a identificar e permitir o tráfego legítimo para um dispositivo e negar todos os pacotes indesejados.

CoPP

O recurso CoPP também pode ser usado para restringir os pacotes IP destinados ao dispositivo de infraestrutura. Neste exemplo, somente o tráfego SSH de hosts confiáveis tem permissão para acessar a CPU do dispositivo Cisco IOS XE.



Observação: o descarte de tráfego de endereços IP desconhecidos ou não confiáveis pode impedir que os hosts com endereços IP atribuídos dinamicamente se conectem ao dispositivo Cisco IOS XE.

access-list 152 deny tcp <trusted-addresses> <mask> any eq 2

access-list 152 permit tcp any any eq 2

access-list 152 deny ip any any

class-map match-all COPP-KNOWN-UNDESIRABLE match access-group 152

policy-map COPP-INPUT-POLICY class COPP-KNOWN-UNDESIRABLE drop

control-plane service-policy input COPP-INPUT-POLICY

No exemplo anterior do CoPP, as entradas da ACL correspondentes aos pacotes não autorizados com a ação de permissão resultam em um descarte desses pacotes pela função policy-map drop,

enquanto os pacotes correspondentes à ação de negação não são afetados pela função policy-map drop.

O CoPP está disponível na versão do software Cisco IOS XE.

Consulte Política de Plano de Controle para obter mais informações sobre a configuração e o uso do recurso CoPP.

Controle a proteção plana

A Proteção do Plano de Controle (CPPr - Control Plane Protection), introduzida no Cisco IOS XE Software Release 16.6.4, pode ser usada para restringir ou policiar o tráfego plano de controle que é destinado à CPU do dispositivo Cisco IOS XE. Quando similar a CoPP, CPPr tem a capacidade para restringir o tráfego com granularidade mais fina. CPPr divide o plano agregado do controle em três categorias separadas do plano do controle conhecidas como subinterfaces. Subinterfaces existe para categorias de tráfego do host, do trânsito, e da CEF-Exceção. Além disso, CPPr inclui estes recursos de proteção de planos de controle:

1. Recurso Port-Filtering – Esse recurso permite a fiscalização e o descarte de pacotes enviados para portas TCP ou UDP fechadas ou não audíveis.
2. Recurso Queue-Thresholding – Esse recurso limita o número de pacotes de um protocolo especificado que são permitidos na fila de entrada IP do plano de controle.

   Refira a proteção e a compreensão do plano do controle da proteção plana do controle (CPPr) para obter mais informações sobre da configuração e do uso da característica de CPPr.

Limitadores da taxa do hardware

Específico da plataforma do apoio do Supervisor Engine 32 e do Supervisor Engine 720 do Cisco Catalyst 6500 Series, limitadores com base em hardware da taxa (HWRLs) para cenários de comunicação de rede especiais. Estes limitadores da taxa do hardware são referidos como limitadores da taxa do especial-caso porque cobrem um grupo predefinido específico de IPv4, de IPv6, de unicast, e de encenações DoS do multicast. Os HWRLs podem proteger o dispositivo Cisco IOS XE de uma variedade de ataques que exigem que os pacotes sejam processados pela CPU.

Proteger o BGP

O Border Gateway Protocol (BGP) é a fundação do roteamento da Internet. Como tal, qualquer empresa com requisitos de conectividade mais que modestos geralmente usa o BGP. Muitas vezes, o BGP é alvo de invasores devido à sua onipresença e à natureza simples e segura das configurações do BGP em empresas de porte menor. Contudo, há muitos recursos de segurança BGP-específicos que podem ser entregues para aumentar a segurança de uma configuração de BGP.

Isto fornece uma vista geral dos recursos de segurança os mais importantes BGP. Onde

apropriado, as recomendações de configuração são feitas.

As proteções de segurança dos TTL-estabelecimentos de bases

Cada pacote IP contem um campo 1-byte conhecido como o Time to Live (TTL). Cada dispositivo que um pacote IP atravessa decresce o valor por um. O valor inicial varia pelo sistema operacional e varia tipicamente de 64 a 255. Um pacote é deixado cair quando seu valor TTL alcança zero.

Conhecida como Generalized TTL-based Security Mecanismo (GTSM) e BGP TTL Security Hack (BTSH), uma proteção de segurança baseada em TTL aproveita o valor TTL dos pacotes IP para garantir que os pacotes BGP recebidos sejam de um par conectado diretamente. Esse recurso frequentemente requer coordenação de roteadores de peering; no entanto, uma vez ativado, ele pode derrotar completamente muitos ataques baseados em TCP contra o BGP.

O GTSM para BGP é ativado com a opção ttl-security para o comando de configuração de roteador do BGP neighbor. Este exemplo ilustra a configuração desta característica:

router bgp <asn>

neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> ttl-security hops <hop-count>

Enquanto os pacotes BGP são recebidos, o valor TTL está verificado e deve ser superior ou igual a 255 menos o contagem de saltos especificado.

Autenticação do bgp peer com MD5

A autenticação de pares com MD5 cria um resumo MD5 de cada pacote enviado como parte de uma sessão BGP. Especificamente, as parcelas do IP e dos cabeçalhos de TCP, o payload de TCP, e uma chave secreta são usados a fim gerar o resumo.

O resumo criado é armazenado então no tipo 19 da opção de TCP, que foi criado especificamente por esse motivo pelo RFC 2385. O alto-falante receptor do BGP usa o mesmo algoritmo e a mesma chave secreta para regenerar o resumo da mensagem. Se os resumos recebidos e computados não são idênticos, o pacote está rejeitado

A autenticação de pares com MD5 é configurada com a opção password para o comando de configuração de roteador do BGP neighbor. O uso deste comando é ilustrado como segue:

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> password <secret>

Refira a autenticação do roteador vizinho para obter mais informações sobre da autenticação do bgp peer com MD5.

Configurar os prefixos máximos

Os prefixos BGP são armazenados por um roteador na memória. Quanto mais prefixos um roteador deve manter, mais memória o BGP deve consumir. Em algumas configurações, um subconjunto de todos os prefixos da Internet pode ser armazenado, como em configurações que utilizam apenas uma rota padrão ou rotas para as redes de usuário de um provedor.

A fim de impedir a exaustão da memória, é importante configurar o número máximo de prefixos aceitos em uma base por peer. Recomenda-se que um limite esteja configurado para cada BGP peer.

Quando você configura esse recurso com o comando de configuração do roteador neighbor maximum-prefix BGP, um argumento é necessário: o número máximo de prefixos que são aceitos antes que um peer seja desligado. Opcionalmente, um número de 1 a 100 pode igualmente ser incorporado. Este número representa a porcentagem do valor máximo dos prefixos em que ponto um mensagem de registro é enviado.

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>

Refira a configurar os recursos de prefixo máximo BGP para obter mais informações sobre os prefixos máximos por peer.

Filtrar os prefixos BGP com listas de prefixos

As listas de prefixo permitem um administrador de rede aceitar ou rejeitar os prefixos específicos enviados ou recebidos através do BGP. As listas de prefixo podem ser usadas sempre que possível para garantir que o tráfego de rede seja enviado pelos caminhos pretendidos. As listas de prefixo podem ser aplicadas a cada peer do eBGP nas direções de entrada e saída.

As listas de prefixo configuradas limitam os prefixos que são enviados ou recebidos àqueles permitidos especificamente pela política de roteamento de uma rede. Se isso não for viável devido ao grande número de prefixos recebidos, uma lista de prefixos pode ser configurada para bloquear especificamente prefixos inválidos conhecidos. Estes prefixos ruins conhecidos incluem o espaço de endereços IP e as redes não localizadas que são reservadas para interno ou propósitos testando pelo RFC 3330. As listas de prefixos de saída podem ser configuradas para permitir especificamente apenas os prefixos que uma organização pretende anunciar.

Este exemplo de configuração usa listas de prefixo para limitar as rotas que são instruídas e anunciadas. Especificamente, somente uma rota padrão de entrada é permitida de prefixo BGP-PL-INBOUND, e o prefixo 192.168.2.0/24 é a única rota permitida anunciada por BGP-PL-OUTBOUND.

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0

ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24

router bgp <asn>

neighbor <ip-address> prefix-list BGP-PL-INBOUND in

neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out

Consulte Filtragem de rota de saída baseada em prefixo para obter uma cobertura completa da filtragem de prefixo BGP.

Filtrar os prefixos de BGP com listas de acesso do caminho para o sistema autônomo

As listas de acessos do trajeto do sistema autônomo BGP permitem que o usuário filtre os prefixos recebidos e anunciados baseados no atributo do Como-PATH de um prefixo. Este recurso pode ser usado em conjunto com as listas de prefixos para estabelecer um conjunto robusto de filtros.

Este exemplo de configuração usa as listas de acesso de caminho AS para restringir os prefixos de entrada aos originados pelo AS remoto e os prefixos de saída aos originados pelo sistema autônomo local. Os prefixos que são originados de todos os sistemas autônomos restantes são filtrados e não instalados na tabela de roteamento.

ip as-path access-list 1 permit

ip as-path access-list 2 permit

router bgp <asn>

neighbor <ip-address> remote-as 65501

neighbor <ip-address> filter-list 1 in

neighbor <ip-address> filter-list 2 out

Proteger os Interior Gateway Protocols

A capacidade de uma rede envia corretamente o tráfego e recupera-o das alterações de topologia ou as falhas são dependentes de um visualização precisa da topologia. Muitas vezes, você pode executar um Interior Gateway Protocol (IGP) para fornecer essa visualização. Por padrão, os IGP são dinâmicos e descobrem os roteadores adicionais que se comunicam com o IGP particular no uso. Os IGP igualmente descobrem as rotas que podem ser usadas durante uma falha do link de rede.

Estas subseções fornecem uma vista geral dos recursos de segurança os mais importantes IGP.

As recomendações e os exemplos que cobrem a versão 2 do protocolo de informação de roteamento protocolo de informação de roteamento (RIPv2), o protocolo enhanced interior gateway routing (EIGRP), e o caminho mais curto aberto (OSPF) são fornecidos primeiramente quando apropriados.

Autenticação e verificação do protocolo de roteamento com

message digest 5

A falha para fixar a troca de informação de roteamento permite que um atacante introduza a informação de roteamento falsa na rede. Usando a autenticação de senha com protocolos de roteamento entre roteadores, você pode ajudar na segurança da rede. Contudo, porque esta autenticação é enviada como a minuta, pode ser simples para que um atacante subverta este controle de segurança.

Quando você adiciona recursos de hash MD5 ao processo de autenticação, as atualizações de roteamento não contêm mais senhas de texto claro e todo o conteúdo da atualização de roteamento é mais resistente à violação. Contudo, a autenticação md5 é ainda suscetível à força brutal e aos ataques do dicionário se as senhas fracas são escolhidas. Você é recomendado usar senhas aleatórias suficientemente. Desde que a autenticação md5 é muito mais segura quando comparada à autenticação de senha, estes exemplos é específica à autenticação md5. O IPSec pode igualmente ser usado a fim validar e fixar protocolos de roteamento, mas estes exemplos não detalham seu uso.

O EIGRP e o RIPv2 utilizam portas-chaves como parte da configuração. Refira a chave para obter mais informações sobre da configuração e do uso das portas-chaves.

Este é um exemplo de configuração para a autenticação do roteador EIGRP que usa MD5:

key chain <key-name>

key <key-identifier>

key-string <password>

interface <interface> ip authentication mode eigrp <as-number> md5

ip authentication key-chain eigrp <as-number> <key-name>

Esta é uma configuração da autenticação de roteador do exemplo MD5 para o RIPv2. O RIPv1 não suporta a autenticação.

key chain <key-name>

key <key-identifier>

key-string <password>

interface <interface> ip rip authentication mode md5

ip rip authentication key-chain <key-name>

Este é um exemplo de configuração para a autenticação do roteador OSPF que usa MD5. O OSPF não utiliza portas-chaves.

interface <interface> ip ospf message-digest-key <key-id> md5 <password>

router ospf <process-id>

network 10.0.0.0 0.255.255.255 area 0 area 0 authentication message-digest

Refira configurar o OSPF para mais informação.

Comandos passive-interface

Os vazamentos de informações, ou a introdução de informações falsas em um IGP, podem ser atenuados através do uso do comando passive-interface que ajuda no controle do anúncio de informações de roteamento. Você é recomendado não anunciar nenhuma informação às redes que estão fora de seu controle administrativo.

Este exemplo demonstra o uso desta característica:

router eigrp <as-number> passive-interface default

no passive-interface <interface>

Filtragem de rota

Para reduzir a possibilidade de apresentar informações falsas de roteamento na rede, você deve usar o recurso Route Filtering. Ao contrário do comando configuração router interface passiva , distribuir ocorre em relações uma vez que o filtragem de rota é permitido, mas a informação que é anunciada ou processada é limitada.

Para EIGRP e RIP, o uso do comando distribute-list com a palavra-chave out limita as informações anunciadas, enquanto o uso da palavra-chave in limita as atualizações processadas. O comando distribute-list está disponível para o OSPF, mas não impede que um roteador propague rotas filtradas. Em lugar de, o comando area filter-list pode ser usado.

Este exemplo EIGRP filtra propagandas de partida com o comando distribute-list e uma lista de prefixo:

ip prefix-list <list-name>

seq 10 permit <prefix>

router eigrp <as-number>

passive-interface default

no passive-interface <interface>

distribute-list prefix <list-name> out <interface>

Este exemplo EIGRP filtra atualizações de entrada com uma lista de prefixo:

ip prefix-list <list-name> seq 10 permit <prefix>

router eigrp <as-number>

passive-interface default

no passive-interface <interface>

distribute-list prefix <list-name> in <interface>

Consulte Filtragem de Rota EIGRP para obter mais informações sobre como controlar a publicidade e o processamento de atualizações de roteamento.

Este exemplo de OSPF usa uma lista de prefixo com o comando area filter-list específico do OSPF:

ip prefix-list <list-name> seq 10 permit <prefix>

router ospf <process-id>

area <area-id> filter-list prefix <list-name> in

Consumo do recurso do processo de roteamento

Os prefixos do protocolo de roteamento são armazenados por um roteador na memória, e o consumo do recurso aumenta com prefixos adicionais que um roteador deve sustentar. A fim de impedir o esgotamento de recurso, é importante configurar o protocolo de roteamento para limitar o consumo do recurso. Isso é possível com o OSPF, se você usar o recurso Link State Database Overload Protection.

Este exemplo demonstra a configuração dos recursos de proteção da sobrecarga do banco de dados de estado de link OSPF:

router ospf <process-id> max-lsa <maximum-number>

Refira a limitação do número da Auto-Geração LSA para um processo de OSPF para obter mais informações sobre da proteção da sobrecarga do banco de dados de estado de link OSPF.

Proteger os First Hop Redundancy Protocols

Os First Hop Redundancy Protocols (FHRPs) fornecem resiliência e redundância para dispositivos que atuam como gateways padrão. Esta situação e estes protocolos são comuns nos ambientes onde um peer de dispositivos da camada 3 fornece a funcionalidade do gateway padrão para um segmento de rede ou um conjunto de vlan que contêm server ou estações de trabalho.

O protocolo da Função de Balanceamento de Carga do Gateway (GLBP), o protocolo de roteador de Standby Recente (HSRP), e o protocolo de redundância de roteador virtual (VRRP) são todo o FHRPs. Por padrão, esses protocolos usam comunicações não autenticadas. Este tipo de comunicação pode permitir que um atacante levante como um dispositivo FHRP-falante para supor o papel do gateway padrão na rede. Esta aquisição maioritária permitiria que um atacante

executasse um ataque que envolva pessoas e interceptasse todo o tráfego de usuário que retira a rede.

Para evitar esse tipo de ataque, todos os FHRPs suportados pelo Cisco IOS XE Software incluem um recurso de autenticação com MD5 ou strings de texto. Devido à ameaça levantada por FHRPs não-autenticado, recomenda-se que os exemplos destes protocolos usam a autenticação md5. Este exemplo de configuração demonstra o uso da autenticação md5 GLBP, HSRP, e VRRP:

interface FastEthernet 1

descrição *** Autenticação GLBP ***

glbp 1 authentication md5 key-string <glbp-secret>

glbp 1 ip 10.1.1.1

interface FastEthernet 2

descrição *** Autenticação HSRP ***

standby 1 authentication md5 key-string <hsrp-secret>

standby 1 ip 10.2.2.1

interface FastEthernet 3

description *** VRRP Authentication ***

vrrp 1 authentication md5 key-string <vrrp-secret>

vrrp 1 ip 10.3.3.1

Plano dos dados

Embora o plano dos dados seja responsável para mover dados da fonte para o destino, dentro do contexto da segurança, o plano dos dados seja menos importante dos três planos. Por isso, é importante proteger os planos de gerenciamento e controle de preferência sobre o plano de dados, quando você protege um dispositivo de rede.

Contudo, dentro do plano próprio dos dados, há muitas características e opções de configuração que podem ajudar o tráfego seguro. Estas seções detalham estas características e opções tais que você pode mais facilmente segurar sua rede.

Endurecimento do plano dos dados gerais

A grande maioria de fluxos de tráfego plano dos dados através da rede como determinado pela configuração de roteamento da rede. Contudo, a funcionalidade da rede IP existe para alterar o trajeto dos pacotes através da rede. As características tais como opções IP, especificamente a opção de roteamento de origem, formam um desafio da segurança em redes de hoje.

O uso do trânsito ACL é igualmente relevante ao endurecimento do plano dos dados.

Consulte a seção Filtrar tráfego em trânsito com ACLs em trânsito deste documento para obter mais informações.

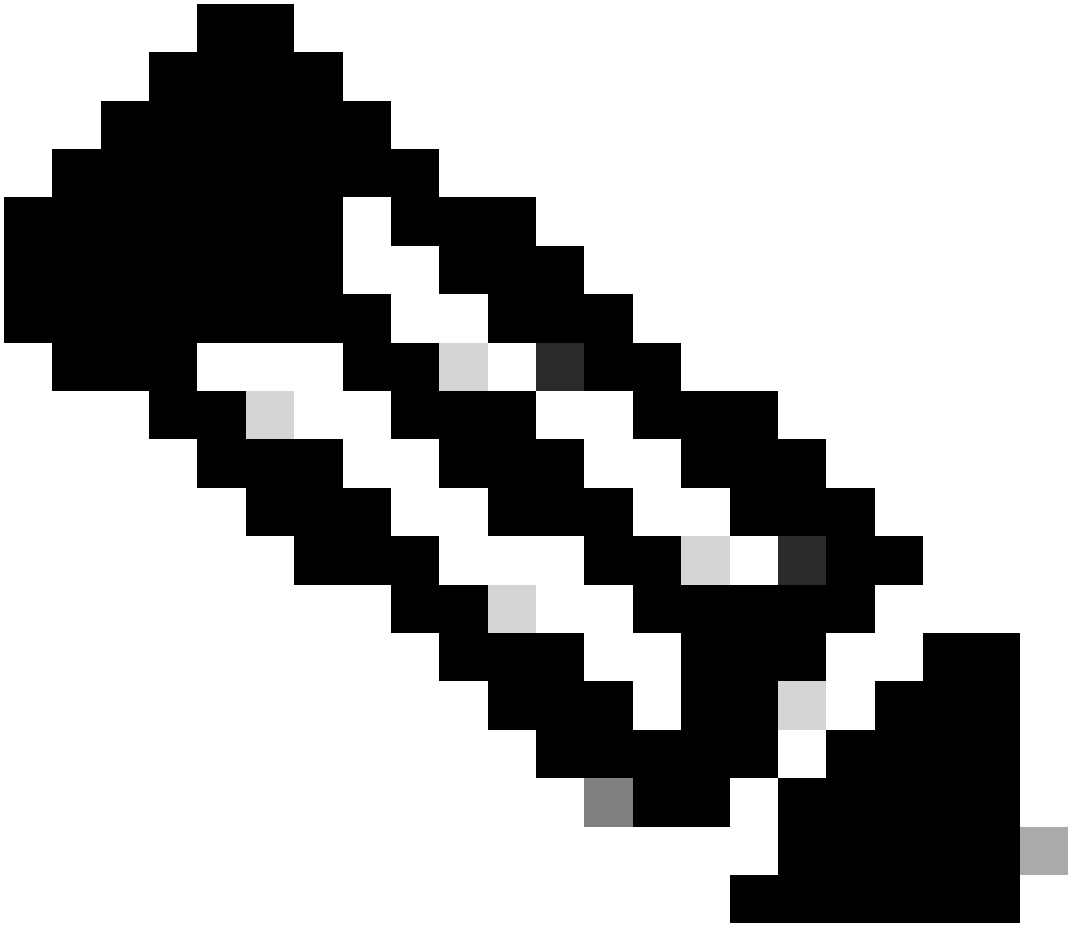
Queda seletiva das opções IP

Há dois interesses de segurança apresentados por opções IP. O tráfego que contém opções IP deve ser comutado por processo pelos dispositivos Cisco IOS XE, o que pode levar a uma carga elevada da CPU. As opções IP também incluem a funcionalidade para alterar o caminho que o tráfego percorre pela rede, o que possivelmente permite subverter os controles de segurança.

Devido a estes interesses, as opções do global configuration command ip {drop | ignore} foi adicionado ao Cisco IOS XE Software Releases 16.6.4 e posteriores. Na primeira forma desse comando, ip options drop, todos os pacotes IP que contêm opções IP recebidas pelo dispositivo Cisco IOS XE são descartados. Isto impede a carga de CPU elevado e a subversão possível dos controles de segurança que as opções IP podem permitir.

A segunda forma desse comando, ip options ignore, configura o dispositivo Cisco IOS XE para ignorar as opções IP que estão contidas nos pacotes recebidos. Quando isto abrandar as ameaças relativas às opções IP para o dispositivo local, é possível que os dispositivos de downstream poderiam ser afetados pela presença de opções IP. É por esta razão que o formulário queda deste comando é altamente recomendado. Isto é demonstrado no exemplo de configuração:

queda de opções IP



Observação: alguns protocolos, por exemplo, o RSVP, fazem uso legítimo de opções IP. A funcionalidade destes protocolos é impactada por este comando.

Uma vez que a queda seletiva das opções IP foi permitida, o comando exec do tráfego IP da mostra pode ser usado a fim de determinar o número de pacotes que são deixado cair devido à presença de opções IP. Esta informação esta presente no contador de queda forçado.

Refira a queda seletiva das opções IP ACL para obter mais informações sobre desta característica.

Desabilite o roteamento do origem de IP

O roteamento do origem de entrega de IP a rota de origem e as opções de rota de registro fracas em tandem ou a rota de origem restrita junto com a opção de rota de registro permitir a fonte do IP datagrama de especificar o caminho de rede tomadas de um pacote. Esta funcionalidade pode ser usada nas tentativas de distribuir o tráfego em torno dos controles de segurança na rede.

Se as opções IP não foram completamente desabilitadas através da característica seletiva da gota das opções IP, ele são importantes que o roteamento do origem de IP é deficiente. O roteamento de origem IP, que é ativado por padrão em todos os Cisco IOS XE Software Releases, é desativado por meio do comando de configuração global no ip source-route.

Este exemplo de configuração ilustra o uso deste comando:

no ip source-route

Desabilite o redirecionamentos de ICMP

Os redirecionamentos de ICMP são usados a fim informar um dispositivo de rede de um trajeto melhor a um destino IP. Por padrão, o Cisco IOS XE Software envia um redirecionamento se receber um pacote que deve ser roteado através da interface que foi recebido.

Em algumas situações, pode ser possível para um invasor fazer com que o dispositivo Cisco IOS XE envie muitas mensagens de redirecionamento ICMP, o que resulta em uma carga de CPU elevada. Por este motivo, recomenda-se que a transmissão dos redirecionamentos de ICMP seja deficiente. Os redirecionamentos ICMP são desativados com o comando interface configuration no ip redirects, conforme mostrado no exemplo de configuração:

interface FastEthernet 0

no ip redirects

Desabilite ou limite broadcasts direto de IP

Os broadcasts direto de IP tornam possível enviar um pacote da transmissão IP a uma sub-rede do IP remoto. Uma vez que alcança a rede remota, o dispositivo IP da transmissão envia o pacote como uma transmissão da camada 2 a todas as estações na sub-rede. Essa funcionalidade de broadcast direcionada foi aproveitada como uma amplificação e auxílio à reflexão em vários ataques que incluem o ataque smurf.

As versões atuais do Cisco IOS XE Software têm essa funcionalidade desabilitada por padrão; no entanto, ela pode ser habilitada por meio do comando de configuração de interface ip directed-broadcast. As versões do Cisco IOS XE Software anteriores à 12.0 têm essa funcionalidade habilitada por padrão.

Se uma rede exigir absolutamente a funcionalidade de broadcast direcionado, seu uso poderá ser controlado. Isso é possível com o uso de uma lista de controle de acesso como opção para o comando ip directed-broadcast. Este exemplo de configuração limita as transmissões direcionadas aos pacotes UDP originados em uma rede confiável, 192.168.1.0/24:

access-list 100 permit udp 192.168.1.0 0.0.0.255 any

interface FastEthernet 0

ip directed-broadcast 100

Filtrar o tráfego em trânsito com ACLs de trânsito

É possível controlar o tráfego que transita pela rede com o uso de ACLs de trânsito (tACLs). Isto é em contraste com a infra-estrutura ACL que procura ao filtrar tráfego que é destinado à rede própria. A filtragem fornecida pelas tACLs é útil quando convém filtrar o tráfego para determinado grupo de dispositivos ou o tráfego que transita pela rede.

Este tipo de filtração é executado tradicionalmente por firewall. No entanto, há casos em que pode ser benéfico executar essa filtragem em um dispositivo Cisco IOS XE na rede, por exemplo, onde a filtragem deve ser executada, mas nenhum firewall está presente.

O trânsito ACL é igualmente um lugar apropriado em que para executar proteções estáticas anti-falsificação.

Consulte a seção Proteções antispoofing deste documento para obter mais informações.

Consulte Listas de Controle de Acesso de Trânsito: Filtragem em Sua Borda para obter mais informações sobre tACLs.

Filtração do pacote ICMP

O protocolo Protocolo de controle de mensagens de Internet (ICMP) foi projetado como um protocolo de controle para o IP. Como tal, as mensagens que ele transmite podem ter ramificações de longo alcance nos protocolos TCP e IP em geral. O ICMP é usado pelas ferramentas de solução de problemas de rede ping e traceroute, bem como pelo Path MTU Discovery; no entanto, a conectividade externa do ICMP raramente é necessária para a operação adequada de uma rede.

O software Cisco IOS XE fornece funcionalidade para filtrar especificamente mensagens ICMP por nome ou tipo e código. Este exemplo de ACL permite o ICMP de redes confiáveis, enquanto bloqueia todos os pacotes ICMP de outras fontes:

ip access-list extended ACL-TRANSIT-IN

— Permitir pacotes ICMP somente de redes confiáveis

permit icmp host <trusted-networks> any

— Negue qualquer outro tráfego IP para qualquer dispositivo de rede

deny icmp any any

Filtre fragmentos IP

Conforme detalhado anteriormente na seção Limitar o acesso à rede com ACLs para infraestrutura deste documento, a filtragem de pacotes IP fragmentados pode representar um desafio para os dispositivos de segurança.

Devido à natureza não instuitiva do fragmento que segura, os fragmentos IP frequentemente são inadvertidamente permitidos por ACL. A fragmentação é frequentemente usada nas tentativas de iludir a detecção pelo Intrusion Detection Systems. É por essas razões que os fragmentos IP são frequentemente usados em ataques e podem ser explicitamente filtrados na parte superior de qualquer tACL configurado.

A ACL inclui filtragem abrangente de fragmentos IP. A funcionalidade ilustrada neste exemplo deve ser usada conjuntamente com a funcionalidade dos exemplos anteriores:

ip access-list extended ACL-TRANSIT-IN

— Negue fragmentos IP que usam ACEs específicas de protocolo para ajudar na

— classificação do tráfego de ataque

deny tcp any any fragments

deny udp any any fragments

deny icmp any any fragmentos

deny ip any any fragments

Consulte Processamento de Lista de Acesso de Fragmentos para obter mais informações sobre o tratamento ACL de pacotes IP fragmentados.

Apoio ACL para opções IP de filtração

No Cisco IOS XE Software Release 16.6.4 e posterior, o Cisco IOS XE Software suporta o uso de ACLs para filtrar pacotes IP com base nas opções IP que estão contidas no pacote. A presença de opções IP dentro de um pacote pode indicar uma tentativa de subverter os controles de segurança na rede ou de alterar as características de trânsito de um pacote. É por esses motivos que os pacotes com opções IP podem ser filtrados na borda da rede.

Este exemplo deve ser usado com o índice dos exemplos anteriores para incluir a filtração completa dos pacotes IP que contêm opções IP:

ip access-list extended ACL-TRANSIT-IN

— Negar pacotes IP que contenham opções IP

deny ip any any option-options

Proteções anti-falsificação

Muitos ataques usam o spoofing do endereço IP de origem para serem eficazes ou para ocultar a verdadeira origem de um ataque e impedir um rastreamento preciso. O software Cisco IOS XE fornece RPF unicast e IP Source Guard (IPSG) para impedir ataques que dependem de falsificação de endereço IP de origem. Além disso, os ACL e o roteamento nulo são

frequentemente distribuídos como meios manuais da prevenção da falsificação.

O IP Source Guard minimiza o spoofing das redes que estão sob controle administrativo direto, realizando a verificação da porta do switch, do endereço MAC e do endereço de origem. O unicast RPF fornece a verificação da rede da fonte e pode reduzir ataques falsificado das redes que não são abaixo controle administrativo direto. A segurança de porta pode ser usada a fim de validar endereços MAC na camada de acesso. A Dynamic Address Resolution Protocol (ARP) Inspection (DAI) mitiga os vetores de ataque que usam envenenamento ARP nos segmentos locais.

Unicast RPF

O unicast RPF permite um dispositivo de verificar que o endereço de origem de um pacote enviado pode ser alcançado através da relação que recebeu o pacote. Você não deve confiar no unicast RPF como a única proteção contra a falsificação. Pacotes falsificados podem entrar na rede por meio de uma interface habilitada para RPF unicast se houver uma rota de retorno apropriada para o endereço IP de origem. O Unicast RPF depende de você para ativar o Cisco Express Forwarding em cada dispositivo e é configurado de acordo com a interface.

O RPF unicast pode ser configurado em um de dois modos: solto ou estrito. Nos casos onde há um roteamento assimétrico, o modo fraco é preferido porque o modo restrito é conhecido para deixar cair pacotes nestas situações. Durante a configuração do IP verifique o comando interface configuration, a palavra-chave configura o modo fraco quando a palavra-chave RX configurar o modo restrito.

Este exemplo ilustra a configuração desta característica:

ip cef

interface <interface>

ip verify unicast source reachable-via <mode>

Refira a compreendendo o Unicast Reverse Path Forwarding para obter mais informações sobre da configuração e do uso do unicast RPF.

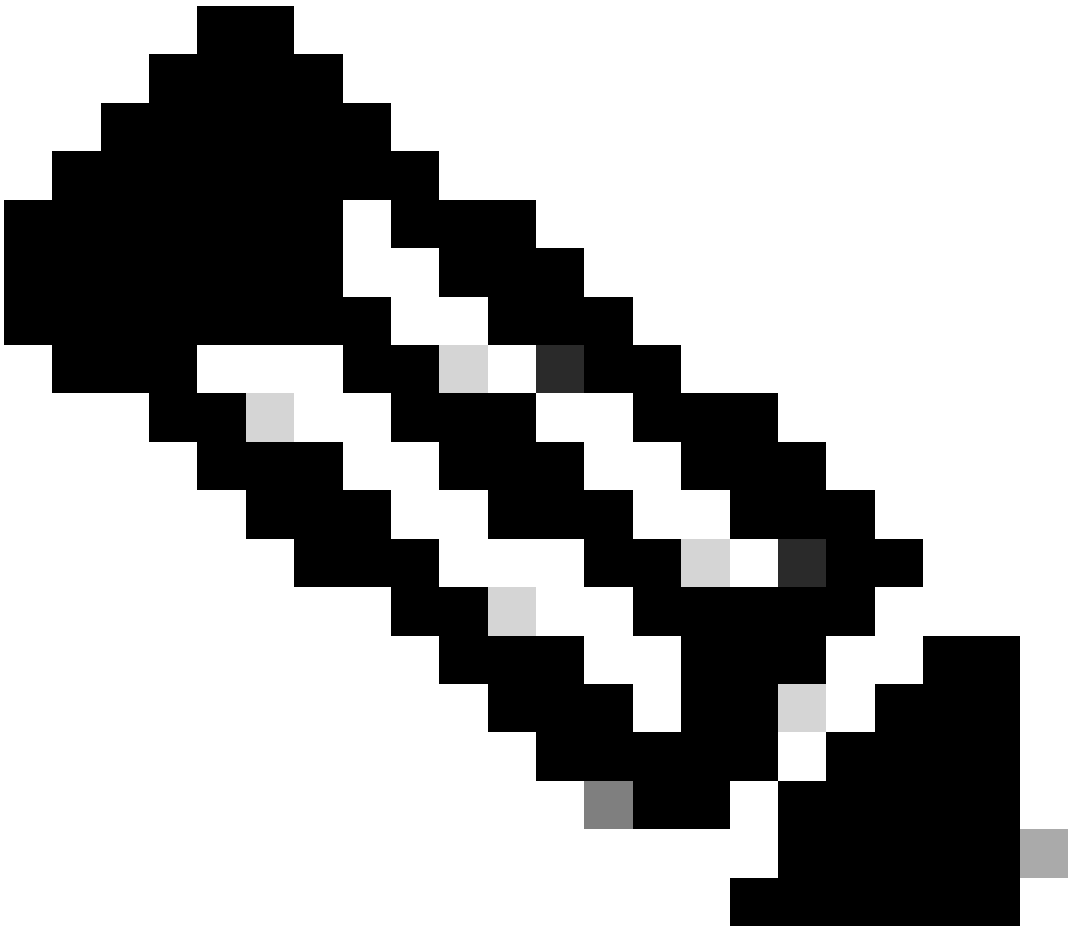
Proteção de origem de IP

A proteção de origem de IP é os significados efetivo da prevenção da falsificação que podem ser usados se você tem o controle sobre interfaces de camada 2. Informação dos usos da proteção de origem de IP da espião DHCP para configurar dinâmicamente um Access Control List da porta (PACL) na interface de camada 2, negando algum tráfego dos endereços IP que não são associados na tabela de ligação do origem de IP.

A proteção de origem de IP pode ser aplicada às interfaces de camada 2 que pertencem aos DHCP com VLANs com espião habilitado. Esta espião dos comandos enable DHCP:

ip dhcp snooping

ip dhcp snooping vlan <vlan-range>



> Observação: para suportar o IP Source Guard, o chassi/roteador precisa de um módulo de switching de camada 2.

A segurança de porta pode ser permitida com o IP verifica o comando configuration da interface de segurança da porta de origem. Isso requer o comando de configuração global ip dhcp snooping information option; além disso, o servidor DHCP deve suportar a opção 82 do DHCP.

Consulte IP Source Guard para obter mais informações sobre esse recurso.

Segurança da porta

A segurança de porta é usada a fim de abrandar a falsificação do MAC address na interface de acesso. A segurança de porta pode usar endereços (pegajosos) dinâmicamente instruídos MAC para facilitar na configuração inicial. Quando a segurança de porta determina uma violação de MAC, pode usar um dos quatro modos de violação. Estes modos protegem, restringem, parada

programada, e parada programada VLAN. Nos casos em que uma porta fornece acesso apenas para uma única estação de trabalho com o uso de protocolos padrão, um número máximo de um pode ser suficiente. Os protocolos que leverage endereços MAC virtuais tais como o HSRP não funcionam quando o número máximo é ajustado a um.

interface <interface> switchport

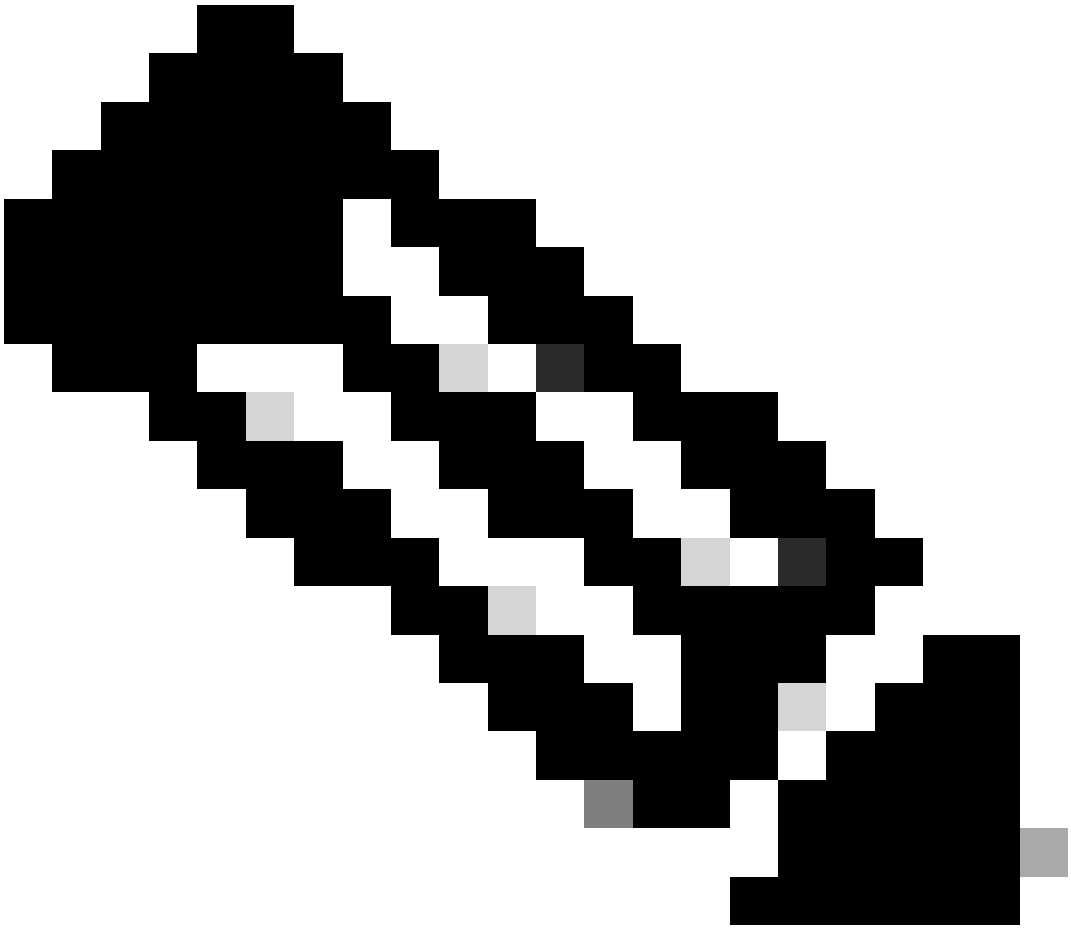
switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum <number>

switchport port-security violation <violation-mode>



Observação: para oferecer suporte à segurança de porta, o chassi/roteador precisa de um módulo de switching de camada 2.

Consulte Configuração da Segurança de Porta para obter mais informações sobre a configuração da Segurança de Porta.

ACL anti-falsificação

As ACLs configuradas manualmente podem fornecer proteção antispoofing estática contra ataques que usam o espaço de endereço não utilizado e não confiável. Geralmente, estes ACL anti-falsificação são aplicados ao tráfego de ingresso em limites de rede como um componente de um ACL maior. As ACLs antispoofing exigem monitoramento regular, pois podem ser alteradas com frequência. O spoofing pode ser minimizado no tráfego originado na rede local, se você aplicar ACLs de saída que limitam o tráfego a endereços locais válidos.

Este exemplo demonstra como os ACL podem ser usados a fim de limitar a falsificação de IP. Este ACL é de entrada aplicado na interface desejada. Os ACE que compõe este ACL não são completos. Se você configura estes tipos de ACL, procure uma referência atualizada que seja conclusiva.

ip access-list extended ACL-ANTISPOOF-IN

deny ip 10.0.0.0 0.255.255.255 any

deny ip 192.168.0.0 0.0.255.255 any

interface <interface>

ip access-group ACL-ANTISPOOF-IN in

Consulte Configuração de ACLs IPv4 para obter mais informações sobre como configurar Listas de Controle de Acesso.

Limitar o impacto do tráfego do plano de dados na CPU

O propósito principal dos roteadores e dos interruptores é enviar avante pacotes e quadros através do dispositivo aos destinos finais. Estes pacotes, que transitam pelos dispositivos distribuíram durante todo a rede, podem impactar funcionamentos CPU de um dispositivo. O plano de dados, que consiste no tráfego que transita pelo dispositivo de rede, pode ser protegido para garantir a operação dos planos de gerenciamento e controle. Se o tráfego de trânsito pode fazer com que um dispositivo processe o tráfego do switch, o plano de controle de um dispositivo pode ser afetado, o que pode levar a uma interrupção operacional.

Características e tipos de tráfego que impactam o CPU

Embora não exaustiva, esta lista inclui os tipos de tráfego plano dos dados que exigem o processamento de CPU especial e são processo comutados pela CPU:

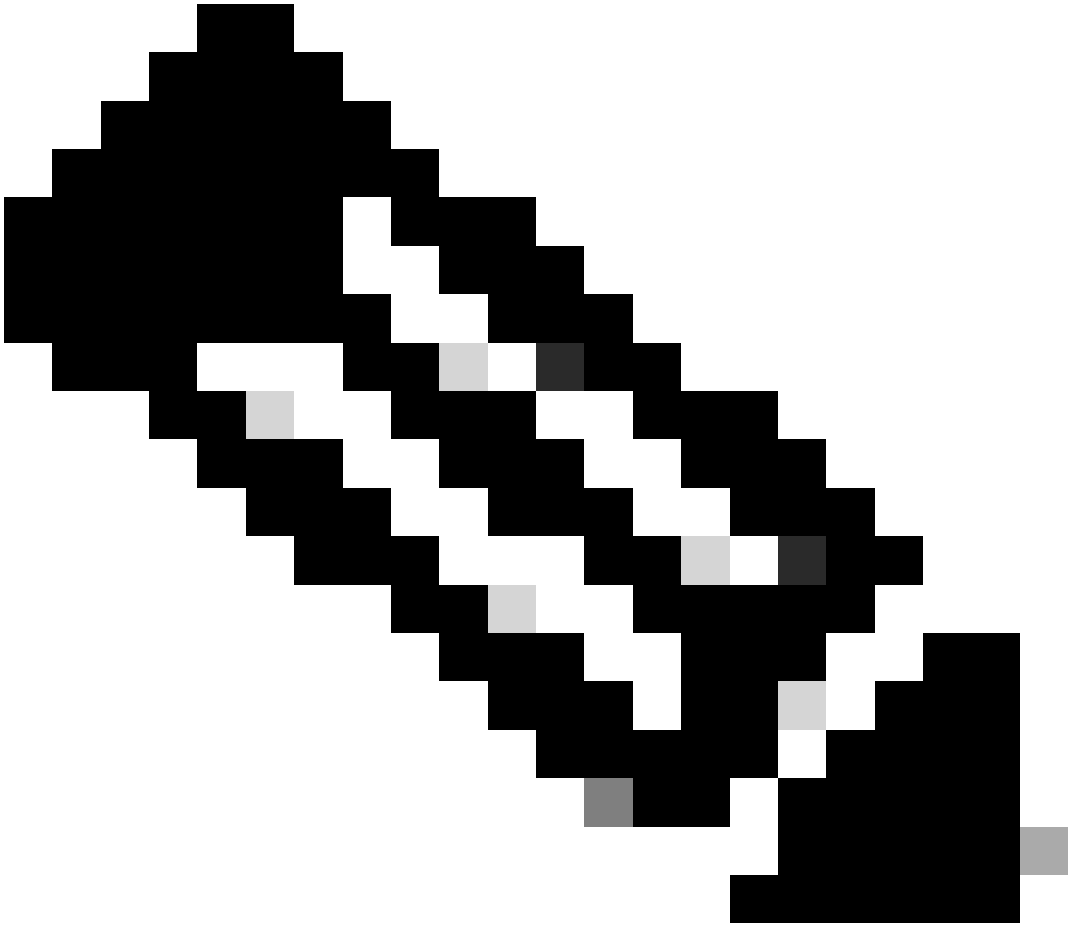
1. Registro da ACL – O tráfego de registro da ACL consiste em todos os pacotes gerados devido a uma correspondência (permissão ou negação) de uma ACE em que a palavra-chave log é usada.

2. RPF unicast - O RPF unicast usado em conjunto com uma ACL pode resultar na comutação do processo de determinados pacotes.
3. Opções de IP – Todos os pacotes IP com opções incluídas devem ser processados pela CPU.
4. Fragmentação – Qualquer pacote IP que exija fragmentação deve ser passado para a CPU para processamento.
5. Expiração Time-to-Live (TTL) – Os pacotes que têm um valor TTL menor ou igual a um exigem o envio de mensagens Internet Control Message Protocol Time Exceeded (ICMP Tipo 11, Código 0), o que resulta no processamento da CPU.
6. ICMP inacessíveis – Os pacotes que resultam em mensagens inacessíveis de ICMP devido ao roteamento, à MTU ou à filtragem são processados pela CPU.
7. Tráfego que exige uma solicitação ARP – Os destinos para os quais não existe uma entrada ARP exigem processamento pela CPU.
8. Tráfego não IP – Todo o tráfego não IP é processado pela CPU.

   Veja a seção de endurecimento plana dos dados gerais deste documento para obter mais informações sobre do endurecimento plano dos dados.

Filtrar o valor TTL

Você pode usar o recurso Suporte ACL para filtragem no valor TTL, introduzido no Cisco IOS XE Software Release 16.6.4, em uma lista de acesso IP estendida para filtrar pacotes com base no valor TTL. Esta característica pode ser usada a fim proteger um dispositivo que recebe o tráfego de trânsito onde o valor TTL é um zero ou esse. Os pacotes de filtragem baseados em valores TTL também podem ser usados para garantir que o valor TTL não seja inferior ao diâmetro da rede, protegendo assim o plano de controle dos dispositivos de infraestrutura downstream de ataques de expiração TTL.



> Observação: algumas aplicações e ferramentas, como o traceroute, usam pacotes de expiração TTL para fins de teste e diagnóstico. Alguns protocolos, tais como o IGMP, usam legìtimamente um valor TTL de um.

Este exemplo de ACL cria uma política que filtra os pacotes IP onde o valor TTL é menor do que o 6.

— Crie uma política de ACL que filtre pacotes IP com um valor TTL.

— inferior a 6

ip access-list extended ACL-TRANSIT-IN

deny ip any any ttl lt 6

permit ip any any

— Aplique a lista de acesso à interface na direção de entrada.

interface GigabitEthernet 0/0

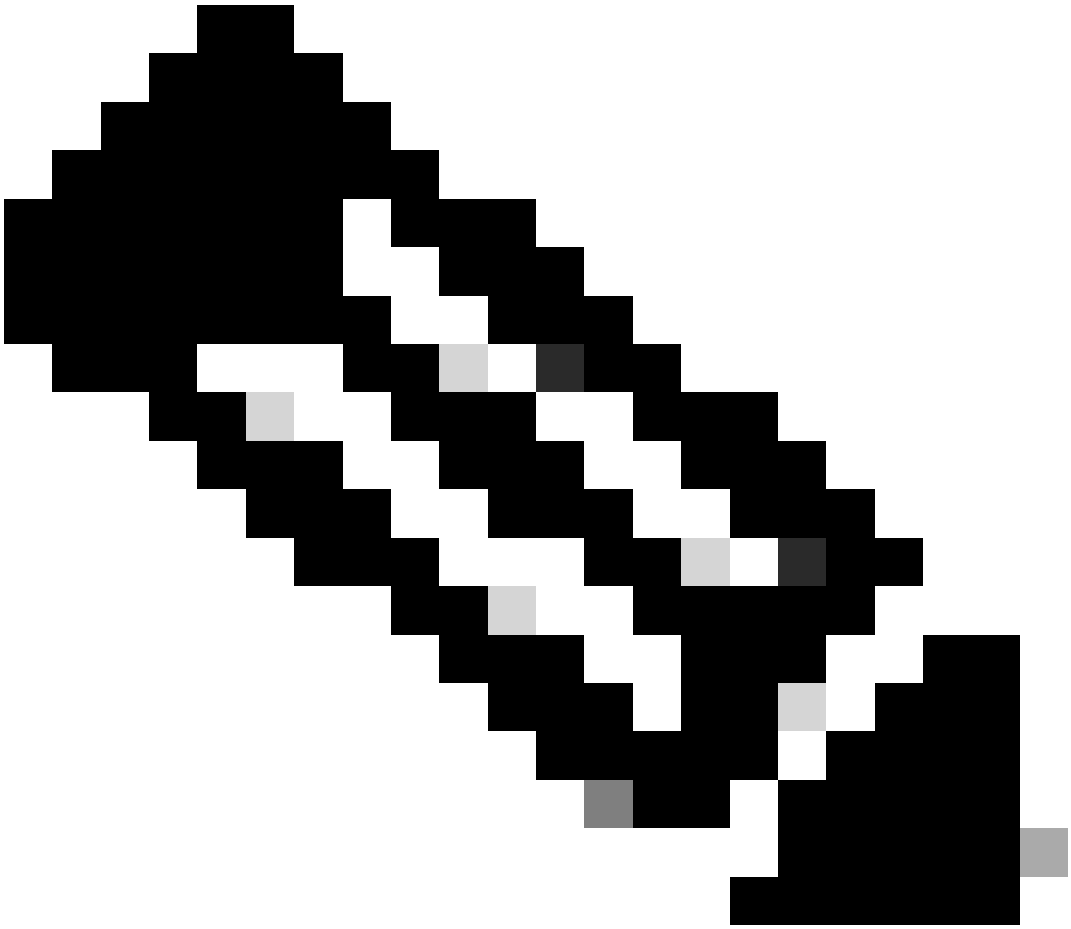
ip access-group ACL-TRANSIT-IN in

Refira a identificação e a mitigação do ataque da expiração TTL para obter mais informações sobre dos pacotes de filtragem baseados no valor TTL.

Refira ao apoio ACL filtrando no valor TTL para obter mais informações sobre desta característica.

Filtrar a presença das opções de IP

No Cisco IOS XE Software Release 16.6.4 e posterior, você pode usar o suporte ACL para o recurso Filtragem de Opções IP em uma lista de acesso IP nomeada e estendida para filtrar pacotes IP com opções IP presentes. Os pacotes IP de filtragem que se baseiam na presença de opções IP também podem ser usados para evitar que o plano de controle dos dispositivos de infraestrutura tenha que processar esses pacotes no nível da CPU.



Observação: o recurso Suporte ACL para opções IP de filtragem pode ser usado somente com ACLs nomeadas e estendidas.

Também é possível observar que o RSVP, a Engenharia de Tráfego Multiprotocol Label Switching, as Versões 2 e 3 do IGMP e outros protocolos que usam pacotes de opções IP não podem funcionar corretamente se os pacotes desses protocolos forem descartados. Se esses protocolos estiverem em uso na rede, o suporte ACL para opções IP de filtragem poderá ser usado; no entanto, o recurso Derivação seletiva das opções IP ACL poderia descartar esse tráfego e esses protocolos não poderiam funcionar corretamente. Se não houver protocolos em uso que exijam opções IP, o recurso ACL IP Options Selective Drop é o método preferencial para descartar esses pacotes.

Este exemplo de ACL cria uma política essa os pacotes IP dos filtros que contêm todas as opções IP:

ip access-list extended ACL-TRANSIT-IN

deny ip any any option-options

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN in

Este exemplo ACL demonstra uma política essa pacotes IP dos filtros com cinco opções IP específicas. Os pacotes que contêm estas opções são negadas:

1. 0 extremidades da lista de opções (eool)
2. 7 Rota do registro (registro-rota)
3. 68 Selo de tempo (timestamp)
4. 131 - Rota de origem fraca (lsr)
5. 137 - Rota de origem restrita (ssr)

ip access-list extended ACL-TRANSIT-IN

deny ip any any option eool

deny ip any any option record-route

deny ip any any option timestamp

deny ip any any option lsr

deny ip any any option ssr

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN in

Veja a seção de endurecimento plana dos dados gerais deste original para obter mais informações sobre da gota seletiva das opções IP ACL.

Outro recurso no software Cisco IOS XE que pode ser usado para filtrar pacotes com opções IP é o CoPP. No Cisco IOS XE Software Release 16.6.4 e posterior, o CoPP permite que um administrador filtre o fluxo de tráfego de pacotes de plano de controle. Um dispositivo que suporta CoPP e suporte ACL para opções IP de filtragem, introduzido no Cisco IOS XE Software Release 16.6.4, pode usar uma política de lista de acesso para filtrar pacotes que contenham opções IP.

Esta política de CoPP deixa cair os pacotes de trânsito que estão recebidos por um dispositivo quando todas as opções IP estão presentes:

ip access-list extended ACL-IP-OPTIONS-ANY

permit ip any any option

class-map ACL-IP-OPTIONS-CLASS

match access-group name ACL-IP-OPTIONS-ANY

policy-map COPP-POLICY

class ACL-IP-OPTIONS-CLASS

police 80000 conformar transmitir exceder queda

plano de controle

service-policy input COPP-POLICY !

Esta política de CoPP deixa cair os pacotes de trânsito recebidos por um dispositivo quando estas opções IP estão presentes:

1. 0 extremidades da lista de opções (eool)
2. 7 Rota do registro (registro-rota)
3. 68 Selo de tempo (timestamp)
4. 131 Rota de origem fraca (lsr)
5. 137 Rota de origem restrita (ssr)

```
ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
police 80000 conformar transmitir exceder queda

plano de controle
service-policy input COPP-POLICY
```

Nas políticas anteriores de CoPP, as entradas da lista de controle de acesso (ACEs) que correspondem a pacotes com a ação de permissão resultam no descarte desses pacotes pela função de queda do mapa de política, enquanto os pacotes que correspondem à ação de negação (não mostrada) não são afetados pela função de queda do mapa de política.

Consulte Implantação da fiscalização do plano de controle para obter mais informações sobre o recurso CoPP.

Controle a proteção plana

No Cisco IOS XE Software Release 16.6.4 e posterior, a Proteção do Plano de Controle (CPPr - Control Plane Protection) pode ser usada para restringir ou policiar o tráfego do plano de controle pela CPU de um dispositivo Cisco IOS XE. Embora semelhante ao CoPP, o CPPr tem a capacidade de restringir ou policiar o tráfego que usa granularidade mais fina que o CoPP. CPPr divide o plano de controle agregado em três categorias de plano de controle separadas conhecidas como subinterfaces: Host, Trânsito e CEF. Existem subinterfaces de exceção.

Esta política de CPPr deixa cair os pacotes de trânsito recebidos por um dispositivo onde o valor TTL seja menos do que 6 e pacotes do trânsito ou de não-trânsito recebidos por um dispositivo onde o valor TTL seja zero ou um. A política de CPPr igualmente deixa cair pacotes com as

opções IP selecionadas recebidas pelo dispositivo.

```
ip access-list extended ACL-IP-TTL-0/1
permit ip any any tl eq 0 1
class-map ACL-IP-TTL-0/1-CLASS
match access-group name ACL-IP-TTL-0/1
ip access-list extended ACL-IP-TTL-LOW
permit ip any any ttl lt 6
class-map ACL-IP-TTL-LOW-CLASS
match access-group name ACL-IP-TTL-LOW
ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
policy-map CPPR-CEF-EXCEPTION-POLICY
class ACL-IP-TTL-0/1-CLASS
queda de conformação de 80000 de polícia
class ACL-IP-OPTIONS-CLASS
police 8000 queda de ação de conformidade
policy-map CPPR-TRANSIT-POLICY
class ACL-IP-TTL-LOW-CLASS
police 8000 queda de ação de conformidade
trânsito de plano de controle
service-policy input CPPR-TRANSIT-POLICY
```

Na política CPPr anterior, as entradas da lista de controle de acesso correspondentes aos pacotes com a ação de permissão resultam no descarte desses pacotes pela função policy-map drop, enquanto os pacotes correspondentes à ação de negação (não mostrada) não são afetados pela função policy-map drop.

Consulte Política de Plano de Controle para obter mais informações sobre o recurso CPPr.

Trafique a identificação e o retorno de monitoramento

Às vezes, você precisa identificar e rastrear rapidamente o tráfego de rede, especialmente durante a resposta a incidentes ou o desempenho ruim da rede. As ACLs de NetFlow e Classificação são os dois métodos principais para realizar isso com o software Cisco IOS XE. O NetFlow pode fornecer a visibilidade em todo o tráfego na rede. Além disso, o NetFlow pode ser implementado com coletores que podem fornecer tendências de longo prazo e análise automatizada. A classificação ACL é um componente dos ACL e exige o PRE-planeamento identificar o tráfego e a intervenção manual específicos durante a análise. Estas seções fornecem uma breve visão geral de cada característica.

Netflow

O NetFlow identifica a atividade de rede anômala e relacionado à segurança por fluxos de rede de seguimento. Os dados NetFlow podem ser visualizados e analisados usando a CLI ou exportados para um coletor NetFlow comercial ou gratuito para agregação e análise. Os coletores de Netflow, com da tensão a longo prazo, podem fornecer a análise do comportamento de rede e do uso. O NetFlow funciona executando a análise em atributos específicos dentro dos pacotes IP e criar fluxo. A versão 5 é a versão de uso mais comum do NetFlow, contudo, a versão 9 é mais elástica. Os fluxos NetFlow podem ser criados com os dados de tráfego amostrados em ambientes de volume elevado.

O CEF, ou CEF distribuído, é um pré-requisito para ativar o NetFlow. O NetFlow pode ser configurado em roteadores e em interruptores.

Este exemplo ilustra a configuração básica desta característica. Em versões anteriores do Cisco IOS XE Software, o comando para ativar o NetFlow em uma interface é ip route-cache flow em vez de ip flow {ingress | egresso}.

ip flow-export destination <ip-address> <udp-port>

ip flow-export version <version>

interface <interface>

ip flow <ingess|egress>

Este é um exemplo do NetFlow output do CLI. O atributo de SrcIf pode ajudar no retorno de monitoramento.

router#show ip cache flow IP packet size distribution (distribuição do tamanho do pacote IP)

(26662860 total de pacotes):

1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480

.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000 .000

Cache de switching de fluxo de IP, 4456704 bytes

55 ativos, 65481 inativos, 1014683 adicionados

41000680 pesquisas ager, 0 falhas de alocação de fluxo

Tempo limite de fluxos ativos em 2 minutos

Tempo limite de fluxos inativos em 60 segundos

Cache de subfluxo de IP, 336520 bytes

110 ativos, 16274 inativos, 2029366 adicionados 1014683 adicionados ao fluxo

0 falhas de alocação, 0 livre de força 1 bloco, 15 blocos adicionados última limpeza de estatísticas nunca

Total de Fluxos de Protocolo Pacotes Bytes Pacotes Ativos (Sec) Ociosos (Sec)

-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow

TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8

TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1

TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1

TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5

TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4

TCP-X 351 0.0 2 40 0.0 0.0 60.8

TCP-BGP 114 0.0 1 40 0.0 0.0 62.4

TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4

TCP-outros 556070 0.6 8 318 6.0 8.2 38.3

UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1

UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6

UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2

UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8

UDP-outros 86247 0.1 226 29 24.0 31.4 54.3

ICMP 19989 0.0 37 33 0.9 26.0 53.9

IP-other 193 0.0 1 22 0.0 3.0 78.2

Total: 1014637 1,2 26 99 32,8 13,8 43,9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts

Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3

Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9

Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1

Consulte Flexible NetFlow para obter mais informações sobre os recursos do NetFlow.

Classificação ACL

A classificação ACL fornece a visibilidade no tráfego que atravessa uma relação. A classificação ACL não altera a política de segurança de uma rede e é construída tipicamente para classificar protocolos, endereços de origem, ou destinos individuais. Por exemplo, um ACE que permitisse todo o tráfego poderia ser separado em protocolos específicos ou em portas. Esta classificação mais granular do tráfego em ACE específicos pode ajudar a fornecer uma compreensão do tráfego de rede porque cada categoria de tráfego tem seu próprio contador de acertos. Um administrador também pode separar a negação implícita no final de uma ACL em ACEs granulares para ajudar a identificar os tipos de tráfego negado.

Um administrador pode agilizar uma resposta a incidentes usando ACLs de classificação com os comandos EXEC show access-list e clear ip access-list counters.

Este exemplo ilustra a configuração de uma classificação ACL para identificar o tráfego SMB antes de uma negação padrão:

ip access-list extended ACL-SMB-CLASSIFY

remark Conteúdo existente da ACL

remark Classificação do tráfego TCP específico de SMB

deny tcp any any eq 139

deny tcp any any eq 445

deny ip any any

Para identificar o tráfego que usa uma ACL de classificação, use show access-list acl-name

Comando EXEC. Os contadores ACL podem ser limpos com o comando EXEC clear ip access-list counters aclname.

router#show access-list ACL-SMB-CLASSIFY Lista de acesso IP estendida ACL-SMB-CLASSIFY

10 deny tcp any any eq 139 (10 correspondências)

20 deny tcp any any eq 445 (9 correspondências)

30 deny ip any any (184 correspondências)

Refira a compreendendo a Lista de Controle de Acesso Registrando para obter mais informações sobre como permitir potencialidades de registro dentro dos ACL.

Controle de acesso com PACL

Os PACL podem somente ser aplicados à direção de entrada em interfaces física da camada 2 de um interruptor. Similar aos mapas VLAN, os PACL fornecem o controle de acesso em não-roteado ou tráfego na Camada 2. A sintaxe para a criação de PACLs, que tem precedência sobre os mapas de VLAN e as ACLs do roteador, é a mesma das ACLs do roteador. Se um ACL é aplicado a uma interface de camada 2, a seguir está referido como um PACL.

A configuração envolve a criação de uma ACL de IPv4, IPv6 ou MAC e sua aplicação à interface de camada 2.

Este exemplo usa uma lista de acesso nomeada estendida para ilustrar a configuração desse recurso:

ip access-list extended <acl-name> permit <protocol> <source-address> <source-port> <destination-address> <destination-port> !

interface <type> <slot/port> switchport mode access switchport access vlan <vlan_number> ip access-group <acl-name> in !

Consulte a seção Port ACL de Configuring Network Security with Port ACLs para obter mais informações sobre a configuração de PACLs.

Vlan isolado

A configuração de um VLAN secundário como um vlan isolada impede completamente uma comunicação entre dispositivos no VLAN secundário. Pode haver apenas uma VLAN isolada por VLAN principal e somente portas misturadas podem se comunicar com portas em uma VLAN isolada. As VLANs isoladas podem ser usadas em redes não confiáveis, como redes que

suportam convidados.

Este exemplo de configuração configura o VLAN 11 como um VLAN isolado e associa-o ao VLAN principal, VLAN 20. Este exemplo também configura a interface FastEthernet 1/1 como uma porta isolada na VLAN 11:

vlan 11 private-vlan isolada

vlan 20 private-vlan primary private-vlan association 11

interface FastEthernet 1/1 descrição *** Porta em VLAN Isolada modo switchport *** switchport private-vlan host switchport private-vlan host-association 20 11

VLAN de comunidade

Um VLAN secundário que seja configurado enquanto um VLAN de comunidade permite uma comunicação entre membros do VLAN assim como com todas as portas misturadas no VLAN principal. Contudo, nenhuma comunicação é possível entre todos os dois VLAN de comunidade ou de um VLAN de comunidade a um VLAN isolado. Os VLAN de comunidade devem ser usados a fim agrupar os servidores que precisam ter conectividade um com o outro, mas onde a conectividade a todos os outros dispositivos no VLAN não é exigida. Este cenário é comum em uma redes publicamente acessível ou em qualquer lugar aquela server fornece o índice aos clientes não confiáveis.

Este exemplo configura um único VLAN de comunidade e configura os FastEthernet 1/2 da porta de switch como um membro desse VLAN. O VLAN de comunidade, VLAN 12, é um VLAN secundário ao VLAN principal 20.

vlan 12 private-vlan community

vlan 20 private-vlan primary private-vlan association 12

interface FastEthernet 1/2 descrição *** Porta na comunidade VLAN *** switchport mode private-vlan host switchport private-vlan host-association 20 12

Conclusão

Este documento fornece uma visão geral ampla dos métodos que podem ser usados para proteger um dispositivo de sistema Cisco IOS XE. Se você fixa os dispositivos, aumenta a segurança total das redes que você controla. Nesta visão geral, a proteção da gestão, o controle, e os planos dos dados são discutidos, e as recomendações de configuração são fornecidos. Sempre que possível, detalhes suficientes são fornecidos para a configuração de cada característica associada. Contudo, as referências detalhadas são fornecidas em todos os casos para fornecê-lo com a informação necessária para uma avaliação adicional.

Reconhecimentos

Algumas descrições de recurso neste original foram escritas por equipes de desenvolvimento da informação da Cisco.

Apêndice: Lista de verificação de proteção de dispositivo do Cisco IOS XE

Esta lista de verificação é uma coleção de todas as etapas de endurecimento que são apresentadas neste guia.

Os administradores podem usá-lo como um lembrete de todos os recursos de proteção usados e considerados para um dispositivo Cisco IOS XE, mesmo que um recurso não tenha sido implementado porque ele não se aplicou. É recomendável que os administradores avaliem cada opção em relação ao possível risco antes de implementá-la.

Plano de gerenciamento

1. Senhas
   Habilite o hashing MD5 (opção secreta) para senhas de ativação e de usuário localConfigure o bloqueio de nova tentativa de senhaDesabilite a recuperação de senha (considere o risco)
2. Desabilite serviços não utilizados
3. Configurar manutenções de atividade TCP para sessões de gerenciamento
4. Ajuste a memória e as notificações de threshold de CPU
5. Configurar
   Memória e notificações de limite de CPU Reservar memória para acesso ao console Detector de vazamento de memória Detecção de estouro de buffer Coleta aprimorada de informações de travamento
6. Use iACLs para restringir o acesso de gerenciamento
7. Filtre (considere o risco)
   Pacotes ICMPrgmentos IPpções IPvalor TTL em pacotes
8. Controle a proteção plana
   Configurar a filtragem de portasConfigurar limites de fila
9. Acesso de gerenciamento
   Use a Proteção do plano de gerenciamento para restringir as interfaces de gerenciamentoDefina o tempo limite de execUse um protocolo de transporte criptografado (como SSH) para o acesso via CLItransporte de controle para as linhas vty e tty (opção de classe de acesso)Avisar sobre o uso de banners
10. AAA
    Use AAA para autenticação e fallbackUse AAA (TACACS+) para autorização de comandosUse AAA para contabilizaçãoUse servidores AAA redundantes
11. SNMP
    Configurar comunidades SNMPv2 e aplicar ACLsConfigurar SNMPv3
12. Registro
    Configurar o registro centralizadoDefinir níveis de registro para todos os componentes relevantesDefinir a interface de origem do registroConfigurar a granularidade do registro de

data e hora
13. Gerenciamento de configuração
    Substituir e reverterAcesso exclusivo à alteração de configuraçãoConfiguração de resiliência do softwareNotificações de alteração de configuração.

Controle o plano

1. Desabilitar (considere o risco)
   ICMP redirecionaICMP inalcançávelProxy ARP
2. Configurar a autenticação do NTP se o NTP for usado
3. Configurar o policiamento do plano do controle/proteção (filtração da porta, os pontos iniciais da fila)
4. Fixe protocolos de roteamento
   BGP (TTL, MD5, prefixos máximos, listas de prefixos, ACLs de caminho de sistema)IGP (MD5, interface passiva, filtragem de rota, consumo de recursos)
5. Configurar limitadores da taxa do hardware
6. Fixe os primeiros protocolos da redundância de salto (GLBP, HSRP, o VRRP)

Plano dos dados

1. Configurar a queda seletiva das opções IP
2. Desabilitar (considere o risco)
   Roteamento de origem de IPbroadcasts Direcionados por IPredirecionamentos de ICMP
3. Broadcasts direto de IP do limite
4. Configurar tACLs (considere o risco)
   Filtrar ICMPiltrar fragmentos IPiltrar opções IPiltrar valores TTL
5. Configure proteções anti-falsificação exigidas
   ACLsIP Source GuardInspeção ARP dinâmicaRPFP unicastSegurança de porta
6. Controle a proteção plana (a CEF-exceção do controle plano)
7. Configurar o NetFlow e a classificação ACL para a identificação do tráfego
8. Configure exigiu o controle de acesso ACL (mapas VLAN, PACL, o MAC)
9. Configurar VLAN privados

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.