Cisco guia para endurecer dispositivos IOS Cisco

Índice

Limitadores da taxa do hardware
Fixe o BGP
As proteções de segurança dos TTL-estabelecimentos de bases
Autenticação do bgp peer com MD5
Configurar prefixos máximos
Filtre prefixos BGP com listas de prefixo
Filtre prefixos BGP com Listas de acesso do trajeto do sistema autônomo
Fixe protocolos Interior Gateway Protocols
Autenticação e verificação do protocolo de roteamento com message digest 5
Comandos passive-interface
Filtragem de rota
Consumo do recurso do processo de roteamento
Fixe primeiros protocolos da redundância de salto
Plano dos dados
Endurecimento do plano dos dados gerais
Queda seletiva das opções IP
Desabilite o roteamento do origem de IP
Desabilite o redirecionamentos de ICMP
Desabilite ou limite broadcasts direto de IP
Tráfego de trânsito do filtro com trânsito ACL
Filtração do pacote ICMP
Filtre fragmentos IP
Apoio ACL para opções IP de filtração
Proteções anti-falsificação
Unicast RPF
Proteção de origem de IP
Segurança da porta
Inspeção ARP dinâmica
ACL anti-falsificação
Impacto do limite CPU do tráfego plano dos dados
Características e tipos de tráfego que impactam o CPU
Filtro no valor TTL
Filtro na presença de opções IP
Controle a proteção plana
Trafique a identificação e o retorno de monitoramento
Netflow
Classificação ACL
Controle de acesso com mapas VLAN e lista de controle de acesso da porta
Controle de acesso com mapas VLAN
Controle de acesso com PACL
Controle de acesso com MAC
Uso do VLAN privado
Vlan isolado
VLAN de comunidade
Portas misturadas

Introdução

Este documento descreve a informação para ajudá-lo a fixar seus dispositivos de sistema do ® do Cisco IOS, que aumenta a segurança total de sua rede. Estruturado em torno dos três planos em que as funções de um dispositivo de rede podem ser categorizadas, este original fornece uma vista geral de cada característica incluída e referências à documentação relacionada.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

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

Informações de Apoio

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

- **Plano de gerenciamento** - O plano de gerenciamento controla o tráfego que é enviado ao dispositivo IOS Cisco e composto dos aplicativos e dos protocolos tais como o Shell Seguro (ssh) e o Simple Network Management Protocol (SNMP).

- **Plano do controle** - O plano do controle de um dispositivo de rede processa o tráfego que é primordial 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).

- **Plano dos dados** - Dos dados do plano os dados para a frente através de um dispositivo de rede. O plano dos dados não inclui o tráfego que é enviado ao dispositivo local IOS Cisco.

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 maioria destes documentos seja devotado à configuração segura de um dispositivo IOS Cisco, as configurações apenas não fixam 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 de Segurança e as respostas estão disponíveis em http://www.cisco.com/go/psirt.

A informação adicional sobre estes veículos de uma comunicação está disponível na política da vulnerabilidade do Cisco Security.

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. Refira a triagem do risco para anúncios da vulnerabilidade de segurança para o auxílio a este processo de avaliação.

Entrega de Autenticação, Autorização e Relatório

A estrutura do Authentication, Authorization, and Accounting (AAA) é vital fixar 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. Veja a seção do autenticação, autorização e relatório deste documento para obter mais informações sobre de como leverage o AAA.

Centralize a coleção e a monitoração do registro

A fim ganhar o conhecimento sobre a existência, emergindo, e os eventos históricos relacionaram-se aos incidentes de segurança, sua organização deve ter uma estratégia unificada para o logging de evento e a correlação. 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.

Veja a seção de registo dos melhores prática deste documento para obter mais informações sobre de como executar dispositivos de abertura da rede de IOS Cisco.

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.

Veja a seção interativa segura das sessões de gerenciamento deste documento para obter mais informações sobre do Gerenciamento seguro dos dispositivos IOS Cisco.

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 informação sobre esta característica está disponível na seção da identificação e do retorno de monitoramento do tráfego deste documento e em http://www.cisco.com/go/netflow (somente clientes 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 do dispositivo IOS Cisco, dois aspectos adicionais do gerenciamento de configuração são críticos: configuração de arquivo 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 IOS Cisco contém muitos detalhes sensíveis. 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 a fim arquivar configurações do dispositivo IOS Cisco precisa de ser fixado. 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. Isto inclui as sessões de gerenciamento interativas que usam o SSH, assim como estatística-recolhem-no 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 deste original detalham os recursos de segurança e as configurações disponíveis no Cisco IOS Software que ajudam 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 fixar o plano de gerenciamento e o plano do controle de um dispositivo, porque os funcionamentos do plano do controle afetam diretamente funcionamentos do plano de gerenciamento. Esta lista de protocolos é usada pelo plano de gerenciamento:

- Protocolo simples de gestão de rede
- Telnet
- Protocolo secure shell
- Protocolo de transferência de arquivo
- Protocolo trivial file transfer
- Protocolo da cópia segura
- TACACS+
- RADIUS
- Netflow
- Protocolo de tempo de rede
- 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. Isto é realizado com a definição uma senha ou um segredo que sejam usados a fim autenticar pedidos. 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. Contudo, note que uma senha localmente configurada para o acesso de privilegiado está precisada ainda no caso da falha do TACACS+ ou dos serviços de raio. 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 a fim ajustar a senha que concede o acesso administrativo privilegiado ao sistema do Cisco IOS. 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 **service password-encryption** de configuração global dirige o Cisco IOS Software para criptografar as senhas, Challenge Handshake Authentication Protocol (CHAP) segredos, e os dados similares que são salvas no 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. Contudo, o algoritmo usado pelo **comando service password-encryption** é um Vigen simples com referência à cifra. 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. Todo o arquivo de configuração IOS Cisco que contiver senhas criptografada deve ser tratado com o mesmo cuidado que é usado para uma lista de texto puro daquelas 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 a característica aumentada da segurança de senha usam o Message Digest 5 (MD5) para o hashing 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

A segurança de senha aumentada característica, introduzida no Cisco IOS Software Release 12.2(8)T, permite que um administrador configure o hashing MD5 das 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 do Vigen com referência à cifra. 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>

!
```

Refira a segurança de senha aumentada para obter mais informações sobre desta característica.

Fechamento da nova tentativa da senha de login

A característica do fechamento da nova tentativa da senha de login, adicionada no Cisco IOS Software Release 12.3(14)T, permite que você trave para fora uma conta de usuário local após um número configurado de tentativas de login mal sucedidas. 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.

Note que os usuários autorizados podem se travar fora de um dispositivo se o número de tentativas de login mal sucedidas é alcançado. 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 Software Release 12.3(14)T e Mais Recente, nenhuma característica da recuperação de senha do serviço não permite que qualquer um com acesso de console alcance incerta a configuração de dispositivo e cancele a senha. Igualmente não permite que os usuários maliciosos mudem o valor do registro de configuração e o acesso NVRAM.

```
!

no service password-recovery

!
```

O Cisco IOS Software fornece um procedimento de recuperação de senha que confie no acesso ao modo do monitor de ROM (ROMMON) que usa a tecla break durante a inicialização do sistema. No ROMMON, o software do dispositivo pode ser recarregado a fim alertar uma

configuração de sistema nova que inclua uma senha nova.

O procedimento de recuperação da senha atual permite qualquer um com acesso de console de alcançar o dispositivo e sua rede. Nenhuma característica da recuperação de senha do serviço impede a conclusão da sequência de tecla break e entrar 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 é necessário recuperar uma vez a senha de um dispositivo IOS Cisco esta característica está permitida, a configuração completa está suprimida.

Consulte para fixar o exemplo de configuração ROMMON para obter mais informações sobre desta característica.

Desabilite serviços não utilizados

Como uma melhor prática da segurança, todo o serviço desnecessário deve ser deficiente. Estes serviços unneeded, especialmente aqueles que usam o User Datagram Protocol (UDP), raramente são usados para os propósitos legítimos mas podem ser usados a fim lançar o DoS e os outros ataques que são impedidos de outra maneira pelo filtragem de pacote de informação.

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

- eco (número de porta 7)
- rejeite (número de porta 9)
- dia (número de porta 13)
- 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 deficientes por padrão nos Cisco IOS Software Release 12.0 e Mais Recentes. 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:

- Não emita o **no ip finger**comando global configuration a fim de desabilitar o serviço Finger. Cisco IOS Software Release posteriores ao 12.1(5) e 12.1(5)T desabilitam este serviço por padrão.
- Emita o comando global configuration do **no ip bootp server** a fim desabilitar o protocolo de bootstrap (BOOTP).
- No Cisco IOS Software Release 12.2(8)T e posterior, emita o **comando ignore BOOTP DHCP IP** no modo de configuração global a fim desabilitar o BOOTP. Isto deixa serviços do protocolo de configuração dinâmica host (DHCP) habilitados.

- 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.

- Não emita **nenhum comando mop enabled** no modo de configuração da interface a fim desabilitar o serviço de Protocolo de Manutenção de Operação (MOP).

- Emita o **no ip domain-lookup** comando de configuração global a fim desabilitar serviços da resolução do Domain Name System (DNS).

- 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.

- O Server do HTTP pode ser desabilitado com o **comando no ip http server no** modo de configuração global, e o server seguro HTTP (HTTPS) pode ser desabilitado com **nenhum** comando global configuration do **servidor seguro do HTTP de IP**.

- A menos que os dispositivos IOS Cisco recuperarem configurações da rede durante a partida, o comando de configuração global do **no service config** deve ser usado. Isto impede o dispositivo IOS Cisco de uma tentativa de encontrar um arquivo de configuração na rede com TFTP.

- 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.

- 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.

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. À revelia, as sessões são desligadas após dez minutos da inatividade.

```
!

line con 0
exec-timeout <minutes> [seconds]
```

```
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

Keepalives para sessões de TCP

O serviço TCP-Keepalives-em e os comandos global configuration do TCP-**Keepalives-para fora do serviço** permitem um dispositivo de enviar manutenções de atividade TCP para sessões de 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. Isto assegura-se de que o dispositivo na extremidade remota da conexão seja ainda acessível e que as conexões entreabertas ou órfãs são removidas do dispositivo IOS Cisco local.

```
!

service 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
 ip address 192.168.1.1 255.255.255.0
!
```

Notificações do ponto inicial da memória

A notificação do ponto inicial da memória da característica, adicionada no Cisco IOS Software Release 12.3(4)T, permite que você abrande condições de memória baixa em um dispositivo. Esta característica usa dois métodos a fim realizar esta: Notificação do ponto inicial da memória e reserva da 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> !
```

Refira a notificações do ponto inicial da memória para obter mais informações sobre esta característica.

Notificação do limiar CPU

Introduzido no Cisco IOS Software Release 12.3(4)T, a característica da notificação do limiar CPU permite que você detecte e seja notificado quando a carga de CPU em um dispositivo cruza um limiar configurado. Quando o ponto inicial é cruzado, o dispositivo gera e envia um mensagem de armadilha de SNMP. Dois métodos do limiar da utilização CPU são apoiados no Cisco IOS Software: Limiar de elevação e limiar 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
!

process cpu threshold type <type> rising <percentage> interval <seconds>
[falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

Refira a notificação do limiar de CPU para obter mais informações sobre esta característica.

&

Memória da reserva para o acesso de console

No Cisco IOS Software Release 12.4(15)T e Posterior, a memória da reserva para a característica do acesso de console pode ser usada a fim de reservar bastante memória para assegurar o acesso de console a um dispositivo IOS Cisco para administrativo e propósitos de Troubleshooting. Esta característica é especialmente benéfica quando a memória do dispositivo esteja baixa. Você pode emitir o comando global configuration do **console da reserva da memória** a fim de permitir esta característica. Este exemplo configura um dispositivo IOS Cisco para reservar 4096 quilobytes por este motivo.

```
!
memory reserve console 4096
!
```

Refira a memória da reserva para o acesso de console para obter mais informações sobre esta característica.

Detector de escape de memória

Introduzido no Cisco IOS Software Release 12.3(8)T1, a característica do detector de escape de memória permite que você detecte escapes de memória em um dispositivo. O detector de escape de memória pode encontrar escapes em todos os conjuntos de memória, buffers de pacotes, e pedaços. Os escapes de memória são estáticos ou as alocações dinâmica da memória que não servem nenhuma finalidade útil. Esta característica centra-se sobre as alocações de memória que são dinâmicas. Você pode usar o comando **show memory debug leaks** EXEC para detectar se existem vazamentos de memória.

Excesso de buffer: Detecção e correção da Redzone de corrupção

No Cisco IOS Software Release 12.3(7)T e Mais Recente, o excesso de buffer: A detecção e correção da característica da corrupção de Redzone pode ser permitida sobre por um dispositivo a fim detectar e corrigir um excesso do bloco de memória e continuar operações.

Estes comandos de configuração global podem ser usados a fim de permitir esta característica. Uma vez que configurado, o comando do **excesso da memória da mostra** pode ser usado a fim indicar as estatísticas da detecção e correção do excesso de buffer.

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

Coleção aumentada do arquivo crashinfo (informações de travamento)

A característica aumentada da coleção do arquivo crashinfo (informações de travamento) suprimem automaticamente de arquivos crashinfo (informações de travamento) velhos. Esta característica, adicionada no Cisco IOS Software Release 12.3(11)T, permite que um dispositivo recupere o espaço a fim criar arquivos crashinfo (informaçoes de travamento) novos quando o dispositivo causa um crash. Esta característica igualmente permite que a configuração do número de arquivos crashinfo (informações de travamento) sido salvar.

```
!
exception crashinfo maximum files <number-of-files>
!
```

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. A hora exata e segura for exigida para finalidades syslog, como durante investigações judiciais dos ataques potenciais, assim como para a conectividade de VPN bem sucedida quando segundo certificados para a autenticação da fase 1.

- **Zona de hora (fuso horário) NTP** - Quando você configura o NTP, a zona de hora (fuso horário) precisa de ser configurada de modo que os timestamps possam exatamente ser correlacionados. Há geralmente duas aproximações para configurar a zona de hora (fuso horário) para dispositivos em uma rede com uma 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 informação nesta característica pode ser encontrada do “no fuso horário pulso de disparo” na documentação de produtos da Cisco.

- **Autenticação de NTP** - Se você configura a autenticação de NTP, oferece a garantia que os mensagens de NTP estão trocados entre pares confiados NTP.

Configuração de exemplo usando a autenticação de NTP:

Cliente:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

Servidor:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

O desabilitação Smart instala

Os melhores prática da Segurança em torno de Cisco Smart instalam a característica (S I) dependem de como a característica é usada em um ambiente de cliente específico. Cisco diferencia estes casos do uso:

- Os clientes que não usam o Smart instalam a característica.
- Os clientes que leverage Smart instalam a característica somente para o desenvolvimento do zero-toque.
- Os clientes que leverage Smart instalam a característica para mais do que o desenvolvimento do zero-toque (configuração e Gerenciamento da imagem).

Estas seções descrevem cada encenação em detalhe:

- Os clientes que não usam Smart instalam a característica.
- Os clientes que não usam Cisco Smart instalam a característica, e executam uma liberação do Cisco IOS e o Software Cisco IOS XE onde o comando está disponível, deve desabilitar Smart instala a característica com **nenhum** comando do **vstack**.

  Nota: O comando do **vstack** foi introduzido no Cisco IOS Release 12.2(55)SE03.

Este é exemplo de saída do comando do **vstack da mostra em um** interruptor do Cisco catalyst com Smart instala os recursos de cliente desabilitados:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Os clientes que Leverage Smart instalam a característica somente para o desenvolvimento do Zero-toque

Desabilite Smart instalam a funcionalidade de cliente depois que a instalação do zero-toque está completa ou não usam **nenhum** comando do **vstack**.

A fim não propagar **nenhum** comando do **vstack na** rede, use um destes métodos:

- Não incorpore **nenhum** comando do **vstack em** todo o cliente comuta manualmente ou com um script.
- Não adicionar **nenhum** comando do **vstack** como parte da configuração do IOS da Cisco que é introduzida em cada Smart instala o cliente como parte da instalação do zero-toque.
- Nas liberações que não apoiam o comando do **vstack** (liberações do Cisco IOS Release 12.2(55)SE02 e Anterior), aplique um Access Control List (ACL) no Switches do cliente a fim obstruir o tráfego na porta TCP 4786.

A fim permitir Smart instale a funcionalidade de cliente mais tarde, incorpore o comando do **vstack em** todo o cliente comuta manualmente ou com um script.

Os clientes que Leverage Smart instalam a característica para mais do que o desenvolvimento do Zero-toque

No projeto de Smart instale a arquitetura, cuidado deve ser tomado tais que o espaço de endereços IP da infraestrutura não é acessível aos partidos não confiáveis. Nas liberações que não apoiam o comando do **vstack**, assegure-se de que somente Smart instale o diretor mande a Conectividade TCP a todo o Smart instalar clientes na porta 4786.

Os administradores podem usar estes melhores prática da Segurança para Cisco Smart instalam disposições em dispositivos afetados:

- Relação ACL
- Policiamento do plano de controle (CoPP). Esta característica não está disponível em todos os Cisco IOS Software Release.

Este exemplo mostra que uma relação ACL com Smart instala o diretor endereço IP de Um ou Mais Servidores Cisco ICM NT enquanto 10.10.10.1 e Smart instalam o endereço IP cliente como 10.10.10.200:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Este ACL deve ser distribuído em todas as interfaces IP em todos os clientes. Pode igualmente ser empurrado através do diretor quando o Switches é distribuído primeiramente.

A fim restringir mais o acesso a todos os clientes dentro da infraestrutura, os administradores podem usar estes melhores prática da Segurança em outros dispositivos na rede:

- Listas de controle de acesso da infraestrutura (iACLs)
- Listas de controle de acesso VLAN (VACL)

Acesso do limite à rede com infraestrutura ACL

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.

Um iACL é construído e aplicado a fim especificar conexões dos anfitriões ou das redes que precisam de ser permitidos aos 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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 Proteção de Sua Base: Lista de controle de acesso da proteção de infra-estrutura para obter mais informações sobre da infra-estrutura ACL.

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 Cisco IOS Software fornece a funcionalidade a fim filtrar especificamente por nome mensagens ICMP ou datilografá-los e codificá-los. 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Filtre fragmentos IP

O processo de filtro para pacotes IP fragmentados pode levantar um desafio aos 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 Cisco IOS Software usa um método específico a fim verificar fragmentos não iniciais contra lista de acesso configurado. O Cisco IOS Software avalia estes fragmentos não iniciais contra o ACL e ignora toda a 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. Este cenário é mostrada nesta configuração:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Refira listas de controle de acesso e fragmentos IP para obter mais informações sobre de como o ACL segura pacotes IP fragmentados.

Apoio ACL para opções IP de filtração

Apoio adicionado Cisco IOS Software Release 12.3(4)T para o uso dos ACL a filtrar os pacotes IP baseados nas opções IP que são 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Apoio ACL a filtrar no valor TTL

Apoio adicionado Cisco IOS Software Release 12.4(2)T ACL para filtrar os pacotes IP baseados no valor do 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 decresce o TTL a zero, e deixa cair consequentemente o pacote, é exigido a fim gerar e enviar um Time Exceeded Message ICMP à fonte do pacote.

A geração e a transmissão destas mensagens são um processo da exceção. O Roteadores pode executar esta função quando o número de pacotes IP que são devidos expirar é baixo, mas se o número de pacotes devido a expirar é alto, a geração e a transmissão destas mensagens podem consumir todos os recursos do CPU disponíveis. Isto apresenta um vetor do ataque DoS. É por esta razão que os dispositivos precisam de ser endurecidos contra os ataques DoS que utilizam uma taxa alta dos pacotes IP que são devidos expirar.

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.

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

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

> Nota: Alguns protocolos fazem o uso legítimo dos pacotes com baixos valores TTL. o eBGP é um tal protocolo. Refira a identificação e a mitigação do ataque da expiração TTL para obter mais informações sobre mitigar ataques de expiração-estabelecimentos de bases TTL.

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

Fixe sessões de gerenciamento interativas

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 imperativo fixar sessões de gerenciamento a fim impedir a divulgação e o acesso não autorizado da informação.

Proteção do plano de gerenciamento

No Cisco IOS Software Release 12.4(6)T e Mais Recente, a proteção do plano de gerenciamento da característica (PMP (produção máxima possível)) permite que um administrador restrinja em que tráfego de gerenciamento das relações 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 permitir a PMP (produção máxima possível) a fim permitir somente o SSH e o HTTPS na relação GigabitEthernet0/1:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Refira a proteção do plano de gerenciamento para obter mais informações sobre da PMP (produção máxima possível).

Controle a proteção plana

Controle construções planas da proteção (CPPr) na funcionalidade do policiamento plano do controle a fim o tráfego plano restringir e de controle de polícia que é destinado ao processador de rotas do dispositivo de IOS. CPPr, adicionado no Cisco IOS Software Release 12.4(4)T, divide o plano do controle nas categorias separadas do plano do controle que são sabidas como subinterfaces. Três subinterfaces planas do controle existem: Host, trânsito e CEF-Exceção. Além disso, CPPr inclui estes recursos de proteção adicionais do plano do controle:

- **característica defiltração** - Esta característica prevê o policiamento ou deixar cair dos pacotes que vão às portas fechados ou NON-escutando TCP e UDP.

- **recursos de política do Fila-ponto inicial** - Esta característica limita o número de pacotes para um protocolo especificado que são permitidos na fila de entrada IP do plano do controle.

CPPr permite que um administrador classifique, policie, e restrinja o tráfego que é enviado a um

dispositivo para propósitos do 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.

Nota: CPPr não apoia o IPv6 e é restringido ao trajeto da entrada do IPv4.

Refira o guia dos recursos de proteção do plano do controle - 12.4T e compreensão da proteção plana do controle para obter mais informações sobre da característica de Cisco CPPr.

Cifre sessões de gerenciamento

Porque a informação pode ser divulgada em uma sessão de gerenciamento interativa, este tráfego deve ser cifrado de modo que um usuário malicioso não possa aceder aos dados que são transmitidos. A criptografia de tráfego permite uma conexão de acesso remoto segura ao 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 cifrada e fixar a conexão de gerenciamento do Acesso remoto a um dispositivo com as características SSH ou HTTPS (protocolo secure hypertext transfer). O Cisco IOS Software apoia a versão de SSH 1,0 (SSHv1), a versão de SSH 2,0 (SSHv2), e o HTTPS que se usa fixa a camada de soquetes (SSL) e o Transport Layer Security (TLS) para a autenticação e a criptografia de dados. SSHv1 e SSHv2 não são compatíveis. SSHv1 é incerto e não estandardizado, assim que não se recomenda se SSHv2 é uma opção.

O Cisco IOS Software igualmente apoia o protocolo da cópia segura (SCP), que permite cifrada e uma conexão segura a fim copiar configurações de dispositivo ou imagens do software. O SCP confia no SSH. Este exemplo de configuração permite o SSH em um dispositivo IOS Cisco:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Este exemplo de configuração permite serviços SCP:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Este é um exemplo de configuração para serviços HTTPS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Refira o Configuring Secure Shell em routeres e em Cisco IOS running de Switches e o Secure Shell (SSH) FAQ para obter mais informações sobre a característica do Cisco IOS Software SSH.

SSHv2

A característica do apoio SSHv2 introduzida no Cisco IOS Software Release 12.3(4)T permite que um usuário configure SSHv2. (O apoio SSHv1 foi executado em uma versão anterior do Cisco IOS Software.) o SSH é executado sobre uma camada de transporte confiável e fornece forte autenticação e capacidade de 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 2 do verson do ssh IP** não é configurado explicitamente, a seguir o Cisco IOS permite a versão de SSH 1.99. A versão de SSH 1.99 permite as conexões SSHv1 e SSHv2. SSHv1 é considerado ser incerto e pode ter efeitos adversos no sistema. Se o SSH é permitido, está recomendado desabilitar SSHv1 usando o comando da **versão 2 do ssh IP**.

Este exemplo de configuração permite SSHv2 (com o SSHv1 desabilitado) em um dispositivo IOS Cisco:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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 SSHv2 suporta teclados-interativos e de métodos de autenticação baseada em senha. 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 privado/chave pública no cliente e configurar uma chave pública no servidor de SSH do Cisco IOS a fim terminar a autenticação.

Um usuário SSH que tente estabelecer as credenciais fornece uma assinatura cifrada 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. A mistura está usada a fim determinar se o server tem uma entrada que combine. Se um fósforo é encontrado, a verificação RSA-baseada da mensagem está executada com a chave pública. Daqui, o usuário é autenticado ou o acesso negado é baseado na assinatura criptografada.

Para a autenticação de servidor, o cliente SSH do Cisco IOS deve atribuir uma chave 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 a chave Host restrita que verifica a bandeira é permitida no cliente, o cliente verifica se tenha a entrada de chave Host que corresponde ao server preconfigured. Se um fósforo é encontrado, o cliente tenta validar a assinatura com a chave do host de servidor. Se o servidor é autenticado com sucesso, o estabelecimento de sessão continua; se não é terminado e indica uma **falha de mensagem da autenticação de servidor**.

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

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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

Este exemplo de configuração permite o servidor de SSH do Cisco IOS de executar a autenticação de usuário RSA-baseada. 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 a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
!

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

Refira a configurar o servidor de SSH do Cisco IOS para executar a autenticação baseados na RSA para obter mais informações sobre do uso de chaves RSA com o SSHv2.

Este exemplo de configuração permite o cliente SSH do Cisco IOS de executar a autenticação de servidor RSA-baseada.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
```

```
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Refira configurar o cliente SSH do Cisco IOS para executar a autenticação de servidor dos RSA-Estabelecimentos de bases para obter mais informações sobre do uso de chaves RSA com o SSHv2.

Console e Portas AUX

Nos dispositivos IOS Cisco, o console e as portas auxiliares (AUX) são as linhas assíncronas que podem ser usadas para o acesso local e remoto a um dispositivo. Você deve estar ciente que as portas de Console em dispositivos IOS 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 é exigida, a seguir um administrador pode remover a capacidade para executar o procedimento de recuperação de senha usando o **no service pasword-recovery** comando de configuração global; contudo, uma vez que o **comando no service password-recovery** foi habilitado, um administrador não poderá executar a recuperação de senha em um dispositivo.

Na maioria das situações, o porto auxiliar de um dispositivo deve ser desabilitado a fim impedir o acesso não autorizado. Um porto auxiliar pode ser desabilitado com estes comandos:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
```

```
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Control vty e tty Lines

As sessões de gerenciamento interativas no Cisco IOS Software usam um tty ou o 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 IOS Cisco têm um número limitado de linhas vty; o número de linha disponível pode ser determinado com o comando show line exec. Quando todas as linhas vty estão no uso, as sessões de gerenciamento novas não podem ser estabelecidas, que cria uma condição DoS para o 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 que seja conectada a um modem que seja usado para o Acesso remoto ao dispositivo, ou uma linha tty que seja conectada à porta de Console dos outros dispositivos são igualmente acessíveis através da rede. Outros formulários de controles de acesso vty e tty podem ser reforçados com os comandos configuration da **entrada de transporte** ou da acesso-**classe**, com o uso das características de CoPP e de CPPr, ou se você aplica Listas de acesso às relações no dispositivo.

A autenticação pode ser reforçada com o uso do AAA, que é o método recomendada para o acesso autenticado a um dispositivo, com o uso da base de dados de usuário local, ou pela 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** deve igualmente ser usado a fim permitir

manutenções de atividade TCP em conexões recebidas ao dispositivo. Isto assegura de que o dispositivo na extremidade remota da conexão seja ainda acessível e que as conexões entreabertas ou órfãs estão removidas do dispositivo de IOS local.

Controle o transporte para linhas vty e tty

Um vty e um tty devem ser configurados a fim aceitar cifrado somente e fixar conexões de gerenciamento do Acesso remoto ao dispositivo ou através do dispositivo se é 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 ou o acesso não autorizado da informação aos dados que são transmitidos entre o administrador e o dispositivo, o **transport input ssh** deve ser usado em vez dos protocolos da minuta, tais como o telnet e o rlogin. **A entrada de transporte nenhuns** configuração pode ser permitida em um tty, que desabilite de fato o uso da linha tty para conexões do reverso-console.

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 são necessários, então o **saída de transporte nenhum** deve ser usado. Contudo, se as conexões de saída são permitidas, a seguir o método de acesso remoto criptografado e seguro para a conexão deve ser reforçada com o uso do **ssh da saída do transporte**.

> Nota: O IPsec pode ser usado para cifrado e fixar conexões de acesso remoto a um dispositivo, se apoiado. 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 legais, pode ser impossível processar e ilegal para monitorar usuários maliciosos a menos que forem notificados que não estão permitidos para usar o sistema. Um método para fornecer esta notificação é colocar esta informação em um mensagem de banner que seja configurado com o comando banner login do Cisco IOS Software.

Os requisitos de notificação legais são complexos, variam pela jurisdição e pela situação, e devem 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:

- 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.
- Observe que toda a utilização não autorizada do sistema é ilegal e pode ser sujeita a civil e às penalidades criminal.
- 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.
- Observações específicas exigidas por leis local.

De um ponto de vista de segurança, um pouco do que legal, um banner de login não deve conter nenhuma informação específica sobre o nome de roteador, o modelo, o software, ou a posse. Esta informação pode ser abusada por usuários maliciosos.

Autenticação, autorização e contabilidade

A estrutura do Authentication, Authorization, and Accounting (AAA) é crítica a fim fixar o acesso interativo aos dispositivos de rede. A estrutura AAA fornece um ambiente altamente configurável que possa ser costurado baseie nas necessidades da rede.

Autenticação TACACS+

O TACACS+ é um protocolo de autenticação que os dispositivos IOS Cisco possam usar para a autenticação de usuários do Gerenciamento contra um servidor AAA remoto. Estes usuários da gestão podem alcançar o dispositivo de IOS através do SSH, do HTTPS, do telnet, ou do 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 está melhorada e sua responsabilidade é reforçada.

O RAIO é um protocolo similar na finalidade ao TACACS+; contudo, cifra somente a senha enviada através da rede. Ao contrário, o TACACS+ cifra o payload de TCP inteiro, que inclui ambos o nome de usuário e senha. Por este motivo, o TACACS+ deve 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 permitida em um dispositivo IOS Cisco com uma configuração similar a este exemplo:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
```

```
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

A configuração precedente pode ser usada como um ponto de início para um molde organização-específico da autenticação de AAA. Refira a autenticação, autorização, e relatórios para mais informação sobre a configuração do AAA.

Uma lista de método é uma lista sequencial que descreva os métodos de autenticação a ser perguntados a fim autenticar um usuário. As listas de método permitem-no de designar uns ou vários protocolos de segurança a ser usados para a autenticação, e asseguram-nas assim um sistema de backup para a autenticação caso que o método inicial falha. O Cisco IOS Software usa o primeiro método alistado que com sucesso aceita ou rejeita 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 configurados TACACS+ se tornam não disponíveis, a seguir um dispositivo IOS Cisco pode confiar em protocolos da autenticação secundária. 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 do segredo da possibilidade é preferido porque o segredo é picado com um algoritmo de sentido único que seja inerentemente mais seguro do que o algoritmo de criptografia que é usado com o tipo senhas 7 para a linha ou a autenticação local.

Contudo, nos Cisco IOS Software Release que suportam o uso das senhas secundárias para usuários localmente definidos, a reserva à 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 esta ação aumente a responsabilidade dos administradores de rede em indisponibilidade TACACS+, aumenta significativamente a sobrecarga administrativa porque as contas de usuário local em todos os dispositivos de rede devem ser mantidas.

Construções deste exemplo de configuração em cima do exemplo precedente da autenticação TACACS+ a fim incluir a autenticação da reserva à senha que é configurada localmente com o **comando enable secret**:

```
!
!

hostname router
!
ip domain-name cisco.c
!
```

```
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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

Uso de senhas tipo 7

Projetado originalmente a fim permitir a descriptografia rápida de senhas armazenadas, o tipo senhas 7 não é um formulário seguro do armazenamento de senha. Há muitas ferramentas disponíveis que podem facilmente decifrar estas senhas. O uso de senhas tipo 7 deve ser evitado a menos que exigido por uma característica que esteja no uso no dispositivo IOS Cisco.

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.

Veja o plano de gerenciamento geral endurecer a seção deste documento para obter mais informações sobre da remoção do tipo senhas 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 inscreve comandos EXEC, o Cisco IOS envia cada comando ao 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:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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+. A informação enviada ao server TACACS+ inclui o comando executado, a data onde foi executado, e o username do usuário que incorpora o comando. A contabilidade do comando não é apoiada com RAIO.

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.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!
```

```
crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Refira configurar esclarecendo mais informação sobre a configuração da contabilidade AAA.

Servidores AAA redundantes

Os servidores AAA que leveraged em um ambiente devem ser redundantes e distribuídos em uma maneira falha-tolerante. 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.

Quando você projeta ou executa uma solução redundante do servidor AAA, recorde estas considerações:

- Disponibilidade dos servidores AAA durante falhas da rede potencial
- Colocação geográfica dispersada dos servidores AAA
- Carregue em servidores AAA individuais em de estado estacionário e em condições de falha
- Latência da rede entre servidores do acesso de rede e servidores AAA
- Sincronização das bases de dados do servidor AAA

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

Fortifique o protocolo administración de red simple

Esta seção destaca diversos métodos que podem ser usados a fim fixar o desenvolvimento do SNMP dentro dos dispositivos de IOS. É crítico que o SNMP esteja fixado corretamente a fim proteger a confidencialidade, a integridade, e a Disponibilidade dos dados de rede e dos dispositivos de rede com que estes dados transitam por. O SNMP fornece-o uma riqueza de informação na saúde dos dispositivos de rede. Esta informação deve ser protegida dos usuários maliciosos que querem leverage estes dados a fim executar ataques contra a rede.

Strings de comunidade SNMP

Os string de comunidade são as senhas que são aplicadas a um dispositivo de IOS para restringir o acesso, de leitura apenas e o acesso de leitura/gravação, aos dados SNMP no dispositivo. Estes strings de comunidade, como com todas as senhas, devem com cuidado ser escolhidos se assegurar de que não sejam triviais. Os strings de comunidade devem ser mudados em intervalos regulares e de acordo com políticas de segurança de rede. Por exemplo, as cordas devem ser mudadas quando um administrador de rede muda papéis ou deixa a 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*:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

> Nota: Os exemplos precedentes do string de comunidade foram escolhidos a fim explicar claramente o uso destas cordas. Para ambientes de produção, os strings de comunidade devem ser escolhidos com cuidado e devem 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.

Refira a referência do comando SNMP IO para obter mais informações sobre desta característica.

Séries de comunidade snmp com ACL

Além do que o string de comunidade, um ACL deve ser aplicado que restrinja mais o acesso SNMP a um grupo seleto de endereços IP de origem. Esta configuração restringe o acesso somente leitura SNMP aos dispositivos do host final que residem no espaço de endereços 192.168.100.0/24 e restringe o acesso de leitura/gravação SNMP somente ao dispositivo do host final em 192.168.100.1.

> Nota: Os dispositivos que são permitidos por estes ACL exigem o string de comunidade apropriado a fim alcançar a informação de SNMP pedida.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Refira a comunidade do servidor snmp na referência do comando management da rede de IOS Cisco para obter mais informações sobre desta característica.

Infra-estrutura ACL

A infraestrutura ACL (iACLs) pode ser distribuída a fim assegurar-se de que somente os host finais com endereços IP de Um ou Mais Servidores Cisco ICM NT confiados possam enviar o tráfego SNMP a um dispositivo de IOS. Um iACL deve conter uma política que negue pacotes SNMP não autorizados na porta 161 UDP.

Veja a seção Limiting Access to the Network with Infrastrucutre ACLs deste documento para mais informações no uso de iACLs.

SNMP Views

Os SNMP Views são uns recursos de segurança que possam permitir ou negar o acesso a determinado SNMP MIB. Uma vez que uma vista está criada e aplicada a um string de comunidade com os comandos global configuration da **comunidade snmp-server comunity-string view**, se você alcança dados MIB, você está restringido às permissões que são definidas pela vista. 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*:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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 o acesso seguro aos dispositivos porque autentica e cifra opcionalmente pacotes sobre a rede. Onde apoiado, o SNMPv3 pode ser usado a fim adicionar uma outra camada de Segurança quando você distribui o SNMP. O SNMPv3 consiste em três opções de configuração preliminares:

- **nenhum AUTH** - Este modo não exige nenhuma autenticação nem nenhuma criptografia dos pacotes SNMP

- **AUTH** - Este modo exige a autenticação do pacote SNMP sem criptografia

- **priv** - Este modo exige a autenticação e a criptografia (privacidade) de cada pacote SNMP

Um Engine ID competente deve existir a fim usar os mecanismos de segurança SNMPv3 - autenticação ou autenticação e criptografia - para segurar pacotes SNMP; por padrão, o Engine ID é gerado localmente. O Engine ID pode ser indicado com o **comando show snmp engineID** segundo as indicações deste exemplo:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

> Nota: Se o engineID é mudado, todas as contas de usuário SNMP devem ser reconfiguradas.

A próxima etapa é configurar um grupo SNMPv3. Este comando configura um dispositivo IOS Cisco para o SNMPv3 com um grupo de servidor SNMP AUTHGROUP e permite somente a autenticação para este grupo com a palavra-chave do **AUTH**:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Este comando configura um dispositivo IOS Cisco para o SNMPv3 com um grupo de servidor SNMP PRIVGROUP e permite a autenticação e a criptografia para este grupo com as **palavras-chave privadas**:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

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

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Note que os comandos da **configuração do usuário servidor snmp** não estão indicados nas saídas de configuração do dispositivo segundo as exigências do RFC 3414; conseqüentemente, a senha do usuário não é visualizável da configuração. A fim de ver os usuários configurados, inscreva o **comando show snmp user** segundo as indicações deste exemplo:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

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

Proteção do plano de gerenciamento

A característica da proteção do plano de gerenciamento (PMP (produção máxima possível)) no Cisco IOS Software pode ser usada a fim ajudar o SNMP seguro porque restringe as relações através de que 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.

Note que a PMP (produção máxima possível) é um subconjunto da característica de CPPr e exige uma versão de IOS que apoia 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:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

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

Melhores práticas de registo

O logging de evento fornece-lhe a visibilidade na operação de um dispositivo IOS Cisco e da rede em que é distribuída. O Cisco IOS Software fornece diversas opções de registro flexíveis que podem ajudar a conseguir os objetivos do gerenciamento de rede e da visibilidade de uma organização.

Estas seções fornecem alguns melhores prática de registo básicos que podem ajudar um administrador a leverage o registo com sucesso ao minimizar o impacto de entrar um dispositivo IOS Cisco.

Envie registros a um local central

Érecomendado enviar a informação de registro a um servidor de SYSLOG remoto. Isto torna possível correlacionar mais eficazmente e rede de auditoria e eventos de segurança através dos dispositivos de rede. Note que os mensagens do syslog estão transmitidos incerta pelo UDP e na minuta. Por este motivo, todas as proteções que uma rede tiver recursos para ao tráfego de gerenciamento (por exemplo, criptografia ou acesso out-of-band) devem ser prolongadas a fim incluir o tráfego do Syslog.

Este exemplo de configuração configura um dispositivo IOS Cisco a fim enviar a informação de registro a um servidor de SYSLOG remoto:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
```

```
Group-name: PRIVGROUP
```

Refira a identificação de incidentes usando eventos de syslog do guarda-fogo e do IOS Router para obter mais informações sobre da correlação do registro.

Integrado em 12.4(15)T e introduzido originalmente em 12.0(26)S, o registo à característica local do armazenamento permanente (disco ATA) permite mensagens do logging do sistema de ser salvar em um disco flash do acessório da tecnologia avançada (ATA). As mensagens salvas em uma movimentação ATA persistem depois que um roteador é recarregado.

Este as linhas de configuração configuram 134,217,728 bytes (128 MB) dos mensagens de registro ao diretório do Syslog do flash ATA (disco 0), especificando um tamanho do arquivo de 16,384 bytes:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Antes que os mensagens de registro estejam redigidos a um arquivo no disco ATA, o Cisco IOS Software verifica se há o espaço de 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 de arquivo é log_month: **dia: ano:: tempo**.

> Nota: Uma movimentação do flash ATA limitou o espaço de disco e assim necessidades ser mantido para evitar overwriting dados armazenados.

Este exemplo mostra como copiar mensagens de registro do disco flash do roteador ATA a 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
```

Refira o registo ao armazenamento permanente local (disco ATA) para obter mais informações sobre esta característica.

Nível de registro

Cada mensagem de registro que é gerado por um dispositivo IOS Cisco é atribuído uma de oito gravidades que variam do nível 0, emergências, através do nível 7, Debug. A menos que especificamente exigido, você é recomendado evitar registrar a nível 7. que registra a nível 7 produz uma carga de CPU elevado no dispositivo que pode conduzir ao dispositivo e à instabilidade de rede.

O nível de armadilha de registro do comando global configuration é usado a fim especificar que mensagens de registro são enviados aos servidores de 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):

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

Refira a pesquisa de defeitos, o gerenciamento de defeito, e o registo para mais informação.

Não registre para consolar ou sessões de monitor

Com Cisco IOS Software, é possível enviar mensagens de registro às sessões de monitor - as sessões de monitor são as sessões de gerenciamento interativas em que o **monitor do terminal de** comando exec foi emitido - e ao console. Contudo, isto pode elevar a carga de CPU de um dispositivo de IOS e consequentemente não é recomendado. Em lugar de, você é recomendado enviar a informação de registro ao buffer de registro local, que pode ser visto com o **comando show logging**.

Use os comandos global configuration **nenhum console de registro** e **no logging monitor** a fim desabilitar o registro ao console e às sessões de monitor. Este exemplo de configuração mostra o uso destes comandos:

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

Refira a referência do comando management da rede de IOS Cisco para obter mais informações sobre dos comandos global configuration.

Use o registo protegido

O Cisco IOS Software apoia o uso de um buffer de registro local de modo que um administrador possa ver localmente mensagens do log gerado. 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 registo protegido: o tamanho de logging buffer e as gravidades da mensagem que é armazenado no amortecedor. O tamanho do **logging buffer** é configurado com o comando global configuration que **registra o** tamanho **protegido**. A mais baixa severidade incluída no buffer é configurada com o comando protegido registrar da severidade. Um administrador pode ver os índices do logging buffer através do **comando show logging exec**.

Este exemplo de configuração inclui a configuração de um logging buffer de 16384 bytes, assim como uma severidade de 6, informativa, que indica que as mensagens a níveis 0 (emergências) com 6 (informativo) estão armazenadas:

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

Refira a referência do comando management da rede de IOS Cisco para obter mais informações sobre do registo protegido.

Configurar a interface de origem de registo

A fim fornecer um nível aumentado da consistência quando você recolhe e revê mensagens de registro, você é recomendado configurar estaticamente uma interface de origem de registro. Realizado através do comando interface de **registo da fonte-relação**, estaticamente configurar uma interface de origem de registo assegura-se de que o mesmo endereço IP apareça em todos os mensagens de registro que são enviados de um dispositivo IOS Cisco 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 global configuration de **registro da** relação da **interface de origem** a fim especificar que o endereço IP de Um ou Mais Servidores

Cisco ICM NT da relação do laço de retorno 0 esteja usado para todos os mensagens de registro:

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

Refira a referência do comando Cisco IOS para mais informação.

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. A data/hora de registro devem ser configurados para incluir a data e hora com precisão do milissegundo e para incluir a zona de hora (fuso horário) no 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):

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

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):

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

Gerenciamento de configuração do Cisco IOS Software

O Cisco IOS Software inclui diversas características que podem permitir um formulário do gerenciamento de configuração em um dispositivo IOS Cisco. 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 Software Release 12.3(7)T e Mais Recente, a configuração substitui e as características do Rollback da configuração permitem que você arquive a configuração de dispositivo IOS Cisco no dispositivo. Armazenado manualmente ou automaticamente, as configurações neste arquivo podem ser usadas a fim substituir a configuração em execução atualmente com **configurar substituem o** comando filename. 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.

Você é recomendado permitir esta característica em todos os dispositivos IOS Cisco na rede. Uma vez que permitido, um administrador pode fazer com que a configuração em execução atualmente seja adicionada ao arquivo com o comando privileged exec da **configuração do arquivo**. As configurações arquivadas podem ser vistas com o comando exec do **show archive**.

Este exemplo ilustra a configuração de arquivo da configuração automática. Este exemplo instrui o dispositivo IOS Cisco para armazenar configurações arquivadas como os arquivos nomeados *arquivar-configuração-n* no disco 0: sistema de arquivos, para manter um máximo de 14 apoios, e para arquivá-lo uma vez pelo dia (1440 minutos) e quando um administrador emitir o comando exec da **memória da escrita**.

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

Embora a funcionalidade do arquivo de configuração possa armazenar até 14 configurações de backup, você está recomendado considerar as requisições de espaço antes que você use o comando **máximo**.

Configuração Exclusiva de Alteração de Acesso

Adicionado ao Cisco IOS Software Release 12.3(14)T, os recursos de acesso exclusivos da alteração de configuração asseguram que somente um administrador faça alterações de configuração a um dispositivo IOS Cisco em um dado momento. Esta característica ajuda a eliminar o impacto indesejado das mudanças simultâneas feitas aos componentes da configuração relacionada. Esta característica é configurada com o modo **exclusivo do modo de configuração de** comando global configuration e opera-se 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 lock terminal configurar** a fim travar a configuração quando incorpora o modo de configuração.

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

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

Configuração resiliente do Cisco IOS Software

Adicionado no Cisco IOS Software Release 12.3(8)T, a característica de configuração resiliente torna possível armazenar firmemente uma cópia da imagem do Cisco IOS Software e da configuração de dispositivo que é usada atualmente por um dispositivo IOS Cisco. Quando esta característica é permitida, não é possível alterar ou remover estes arquivos de backup. Você é recomendado permitir esta característica a fim impedir tentativas inadvertidas e maliciosas de suprimir destes arquivos.

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

Uma vez que esta característica é permitida, é possível restaurar uma configuração ou uma imagem do Cisco IOS Software suprimida. O estado de execução atual desta característica pode ser indicado com o comando exec **seguro da bota da mostra**.

Software Cisco assinado Digital

Adicionado no Cisco IOS Software Release 15.0(1)M para Cisco 1900, 2900, e 3900 Series Router, a característica de software Cisco assinada Digital facilita o uso do Cisco IOS Software que é assinado digitalmente e confiado assim, com o uso da criptografia assimétrica segura (da chave pública).

Uma imagem digital assinada leva (com uma chave privada) uma mistura criptografada dse. Em cima da verificação, o dispositivo decifra a mistura com a chave pública correspondente das chaves que tem em sua loja chave e igualmente calcula sua própria mistura 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. O ROMMON e as imagens IOS Cisco regulares estão

assinados com uma chave do special ou da produção quando você usa a característica de software Cisco assinada Digital. A imagem de ROMMON é upgradable e deve ser assinada com a mesma chave que o special ou a imagem de produção que é carregada.

Este comando verifica a integridade da imagem c3900-universalk9-mz.SSA no flash com as chaves na loja da chave do dispositivo:

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

A característica Digital Assinada do software Cisco foi integrada igualmente na liberação 3.1.0.SG do Cisco IOS XE para a E-Série Switches do Cisco catalyst 4500.

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

No Cisco IOS Software Release 15.1(1)T e Mais Recente, a substituição chave para o software Cisco assinado Digital foi introduzida. A substituição e a revogação de chaves substituem e removem uma chave que seja usada para uma verificação assinada Digital do software Cisco do armazenamento chave de uma plataforma. Somente chaves especiais e da produção podem ser revogadas no caso de um acordo chave.

(Special ou produção) uma chave nova para a imagem a (special ou produção) vem na imagem a (produção ou revogação) que é usada a fim revogar a chave precedente do special ou da produção. A integridade da imagem da revogação é verificada com uma chave do derrubamento que venha gravado na plataforma. Uma chave rollover não muda. Quando você revoga uma chave da produção, depois que a imagem da revogação está carregada, a chave que nova leva está adicionada à loja chave e a chave velha correspondente pode ser revogada enquanto a imagem de ROMMON é promovida e a imagem de produção nova está carreg. Quando você revoga uma chave especial, uma imagem de produção está carregada. Esta imagem adiciona a chave especial nova e pode revogar a chave especial velha. Depois que você promove o ROMMON, a imagem especial nova pode ser carreg.

Este exemplo descreve a revogação de uma chave especial. Estes comandos add a chave especial nova à loja chave da imagem de produção atual, copiam uma imagem de ROMMON nova (C3900_rom-monitor.srec.SSB) à área de armazenamento (usbflash0:), promovem o arquivo ROMMON, e revogam a chave especial velha:

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

Uma imagem especial nova (c3900-universalk9-mz.SSB) pode então ser copiada ao flash a ser carregados e à assinatura da imagem é verificada com a chave especial recentemente adicionada (.SSB):

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

A revogação e a substituição chaves não são apoiadas no Switches das E-séries do Catalyst 4500 que executa o Software Cisco IOS XE, embora este Switches apoie a característica de software Cisco assinada Digital.

Refira a seção assinada Digital da revogação e da substituição da chave do software Cisco da guia Assinatura Digital do software Cisco para obter mais informações sobre esta característica.

Notificação e registo da alteração de configuração

A notificação e os recursos de registro da alteração de configuração, adicionados no Cisco IOS Software Release 12.3(4)T, tornam possível registrar as alterações de configuração feitas a um dispositivo IOS Cisco. O registro é mantido no dispositivo IOS Cisco e contem a informação sobre

o usuário do indivíduo que fez a mudança, o comando configuration inscrito, e o tempo que a mudança foi feita. Esta funcionalidade é permitida com o **registro permite o** comando configuration mode do registador da alteração de configuração. **Os hidekeys dos** comandos opcionais e as entradas de **registro do tamanho** são usados a fim melhorar a configuração padrão porque impedem o registro de dados da senha e aumentam o comprimento do log da mudança.

Você é recomendado permitir esta funcionalidade de modo que a história da alteração de configuração de um dispositivo IOS Cisco possa ser de mais fácil compreensão. Adicionalmente, você está recomendado usar o comando configuration do **Syslog da notificação** a fim permitir a geração de mensagens do syslog quando uma alteração de configuração é feita.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/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 planas do controle consistem nos protocolos e nos processos que se comunicam entre dispositivos de rede a fim mover dados da fonte para o destino. Isto inclui protocolos de roteamento tais como o Border Gateway Protocol, assim como protocolos como o ICMP e o protocolo de reserva do recurso (RSVP).

Éimportante que os eventos nos planos da gestão e dos dados não afetem adversamente o plano do controle. Se um evento do plano dos dados tal como um ataque DoS impactar o plano do controle, toda a rede pode tornar-se instável. Esta informação sobre recursos do Cisco IOS Software e configurações pode ajudar a assegurar a superação do plano do 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, você pode desabilitar a recepção e a transmissão dos determinados tipos de mensagens em uma relação a fim minimizar a quantidade de carga de CPU que é exigida para processar pacotes unneeded.

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. Ou seja os redirecionamentos de ICMP devem nunca ir além de um limite da camada 3.

Há dois tipos de mensagens do redirecionamento de ICMP: reoriente para um endereço de host e

reoriente para uma sub-rede inteira. Um usuário malicioso pode explorar a capacidade do roteador para enviar redirecionamentos de ICMP continuamente enviando pacotes ao roteador, que força o roteador a responder com mensagens do redirecionamento de ICMP, e resultados em um impacto adverso no 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 destas mensagens pode aumentar a utilização CPU no dispositivo. No Cisco IOS Software, a geração do ICMP não alcançável é limitada a um pacote a cada 500 milissegundos por padrão. A geração de mensagem que não chega a seu destino do ICMP pode ser desabilitada com o **no ip unreachables do** comando interface configuration. A limitação da taxa do ICMP não alcançável pode ser mudada do padrão com a intervalo-em-Senhora **inacessível do taxa-limite ICMP do** global configuration command ip.

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. “Falsificando” sua identidade, o roteador aceita a responsabilidade para pacotes de roteamento ao 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 diversas desvantagens à utilização do proxy ARP. Pode conduzir a um aumento na quantidade de tráfego ARP no segmento de rede e o esgotamento de recurso e os ataques que envolva pessoas. O proxy ARP apresenta um vetor do ataque do esgotamento de recurso porque cada requisição ARP proxied consome uma quantidade pequena de memória. Um atacante pode poder esgotar toda a memória disponível se envia um grande número requisições ARP.

Os ataques que envolva pessoas permitem um host na rede ao spoof o MAC address do roteador, que conduz aos anfitriões confiantes que enviam o tráfego ao atacante. O proxy ARP pode ser desabilitado com o **no ip proxy-arp do** comando interface configuration.

Refira a possibilidade do proxy ARP para obter mais informações sobre esta característica.

Limite o impacto CPU do tráfego plano do controle

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.

Compreenda o tráfego plano do controle

A fim proteger corretamente o plano do controle do dispositivo IOS Cisco, é essencial compreender os tipos de tráfego que é processo comutado pelo CPU. O tráfego comutado do processo consiste normalmente em dois tipos de tráfego diferentes. O primeiro tipo de tráfego é dirigido ao dispositivo IOS Cisco e deve ser segurado diretamente pelo dispositivo IOS Cisco CPU. Este tráfego consiste na *categoria de tráfego da adjacência da recepção*. Este tráfego

contém uma entrada no Cisco express forwarding (CEF) tabela por meio de que o salto seguinte do roteador é o dispositivo próprio, que é indicado pelo termo recebe na saída do **cef** CLI da **mostra IP**. Esta indicação é a caixa para todo o endereço IP que exigir a manipulação direta pelo dispositivo CPU Cisco IOS, que inclui endereços IP da relação, endereço de espaço multicast, e espaço do endereço de broadcast.

O segundo tipo de tráfego que é segurado pelo CPU é tráfego plano de dados - trafique com um destino além do dispositivo IOS Cisco próprio - que exige o processamento especial pelo CPU. Embora não uma lista exaustiva do tráfego plano de impacto dos dados CPU, estes tipos de tráfego seja processo comutado e pode conseqüentemente afetar o funcionamento do plano do controle:

- **Registro do Access Control List** - O tráfego do logging ACL consiste em todos os pacotes que forem gerado devido a um fósforo (permit or deny) de um ACE em que a palavra-chave do log é usada.
- **Unicast Reverse Path Forwarding (unicast RPF)** - O unicast RPF, usado conjuntamente com um ACL, pode conduzir à comutação do processo de determinados pacotes.
- **Opções IP** - Todos os pacotes IP com as opções incluídas devem ser processados pelo CPU.
- **Fragmentação** - Todo o pacote IP que exigir a fragmentação deve ser passado ao CPU para processar.
- **Expiração do tempo ao vivo (TTL)** - Os pacotes que têm um valor TTL inferior ou igual a um para exigir o tempo do protocolo Protocolo de control de mensajes de Internet (ICMP) excederam (tipo 11 ICMP, código 0) as mensagens a ser enviadas, que conduz ao processamento de CPU.
- **ICMP não alcançável** - Os pacotes que conduzem aos mensagens que não chega a seu destino do ICMP devido à distribuição, o MTU, ou a filtração são processados pelo CPU.
- **Tráfego que exige uma requisição ARP** - Os destinos para que uma entrada de ARP não existe exigem o processamento pelo CPU.
- **Tráfego não-IP** - Todo o tráfego não-IP é processado pelo CPU.

Esta lista detalha diversos métodos para determinar que tipos de tráfego estão sendo processados pelo dispositivo CPU Cisco IOS:

- O **comando show ip cef** fornece a informação do salto seguinte para cada prefixo IP que é contido na tabela de CEF. Como indicado previamente, as entradas que contêm recebem como o “salto seguinte” é considerado recebe adjacências e indicam que o tráfego deve ser enviado diretamente ao CPU.
- **O comando show interface switching** fornece a informação no número de pacotes que são processo comutado por um dispositivo.
- O **comando show ip traffic** fornece a informação no número de pacotes IP:

com um destino local (isto é, receba o tráfego da adjacência)com opçõesisso exige a fragmentaçãoisso é enviado ao espaço do endereço de broadcastisso é enviado ao espaço do endereço de multicast

- Receba o tráfego da adjacência pode ser identificado com o uso do **comando show ip cache flow**. Todos os fluxos que forem destinados ao dispositivo Cisco IOS têm uma interface de destino (DstIf) do *local*.

- **O policiamento do plano do controle** pode ser usado a fim identificar o tipo e a taxa de tráfego que alcança o plano do controle do dispositivo Cisco IOS. O policiamento do plano do controle pode ser executado com o uso da classificação granular ACL, registo, e o uso do comando do **controle plano do mapa de política da mostra**.

Infra-estrutura ACL

A infra-estrutura ACL (iACLs) limita uma comunicação externa aos dispositivos da rede. A infraestrutura ACL é coberta extensivamente no acesso do limite à rede com a seção da infraestrutura ACL deste documento.

Você é recomendado executar iACLs a fim proteger o plano do controle de todos os dispositivos de rede.

ACLs de Recebimento

Para plataformas distribuídas, receba ACL (rACL) pode ser uma opção para Cisco IOS Software Release 12.0(21)S2 para os 12000 (GSR), 12.0(24)S para os 7500, e 12.0(31)S para os 10720. 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. Em conseqüência, o endereço IP de destino que é usado nas entradas ACL do exemplo abaixo refere somente os endereços IP físicos ou virtuais do roteador. Receba ACL igualmente são considerados uma melhor prática da segurança de rede e deve ser considerada como uma adição a 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:

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

Consulte GSR: Receba lista de controle de acesso a fim ajudar a identificar e permitir o tráfego legitimado a um dispositivo e a negar todos os pacotes indesejados.

CoPP

A característica de CoPP pode igualmente ser usada a fim restringir os pacotes IP que são destinados ao dispositivo de infraestrutura. Neste exemplo, somente o tráfego SSH dos host confiável é permitido para alcançar o dispositivo IOS Cisco CPU.

> Nota: O tráfego deixando cair dos endereços IP de Um ou Mais Servidores Cisco ICM NT desconhecidos ou não confiáveis pode impedir que os anfitriões com endereços IP de Um ou Mais Servidores Cisco ICM NT dinâmico-atribuídos conectem ao dispositivo IOS Cisco.

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

No exemplo precedente de CoPP, as entradas ACL que combinam os pacotes não autorizados com a ação da licença conduzem a um descarte destes pacotes pela função da gota do mapa de política, quando os pacotes que combinam a ação da negação não forem afetados pela função da gota do mapa de política.

CoPP está disponível nos trens de Cisco IOS Software Release 12.0S, 12.2SX, 12.2S, 12.3T, 12,4, e 12.4T.

Refira ao plano de distribuição do controle que policia para obter mais informações sobre da configuração e do uso da característica de CoPP.

Controle a proteção plana

Controle a proteção plana (CPPr), introduzida no Cisco IOS Software Release 12.4(4)T, possa ser usado a fim o tráfego plano restringir ou de controle de polícia que é destinado ao CPU do dispositivo Cisco IOS. 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:

- **característica defiltração** - Esta característica prevê policiando e deixando cair dos pacotes que são enviados às portas fechados ou NON-escutando TCP ou UDP.

- **característica do Fila-limiar** - Esta característica limita o número de pacotes para um protocolo especificado que são permitidos na fila de entrada IP do controle plano.

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. HWRLs pode proteger o dispositivo IOS Cisco de uma variedade de ataques que exigem pacotes se processados pelo CPU.

Há diversos HWRLs habilitados por padrão. Refira a configurações padrão com base em hardware do limitador da taxa PFC3 para mais informação.

Refira a limitadores com base em hardware da taxa no PFC3 para obter mais informações sobre de HWRLs.

Fixe o BGP

O Border Gateway Protocol (BGP) é a fundação do roteamento da Internet. Como tal, toda a organização com requisitos de conectividade mais do que modestos usa frequentemente o BGP. O BGP frequentemente é visado por atacantes devido a sua ubiquidade e ao *grupo e esquece a*

natureza das configurações de BGP em organizações menores. 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.

Sabido como ambos o corte TTL-baseado generalizado do mecanismo de segurança (GTSM) e da Segurança BGP TTL (BTSH), uma proteção de segurança TTL-baseada leverages o valor TTL dos pacotes IP a fim assegurar-se de que os pacotes BGP que são recebidos sejam de um par diretamente conectado. Esta característica exige frequentemente a coordenação dos roteadores peering; contudo, uma vez permitida, pode derrotar completamente muitos ataques com base em TCP contra o BGP.

GTSM para o BGP é permitido com a opção da TTL-**Segurança** para o comando configuration **vizinho do** BGP Router. Este exemplo ilustra a configuração desta característica:

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

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 peer com MD5 cria um resumo MD5 de cada pacote enviado como parte de uma sessão de 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 auto-falante de BGP de recepção usa o mesmos algoritmo e chave secreta a fim regenerar o message digest. Se os resumos recebidos e computados não são idênticos, o pacote está rejeitado.

A autenticação de peer com MD5 é configurada com a **opção de senha ao** comando configuration **vizinho do** BGP Router. O uso deste comando é ilustrado como segue:

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

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

Configurar prefixos máximos

Os prefixos BGP são armazenados por um roteador na memória. Mais prefixos um roteador deve guardar, mais memória o BGP deve consumir. Em algumas configurações, um subconjunto de todos os prefixos do Internet pode ser armazenado, como nas configurações que entregam

somente uma rota padrão ou rotas para as redes cliente de um fornecedor.

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 esta característica com o comando configuration **vizinho do** BGP Router do máximo-**prefixo**, um argumento está exigido: 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.

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

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

Filtre prefixos BGP com listas de prefixo

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 devem ser usadas sempre que seja possível a fim assegurar-se de que o tráfego de rede esteja enviado sobre os trajetos pretendidos. As listas de prefixo devem ser aplicadas a cada peer do eBGP no de entrada e em direções externas.

As listas de prefixo configuradas limitam os prefixos que são enviados ou recebidos àqueles permitidos especificamente pela política de roteamento de uma rede. Se este não é praticável devido ao grande número de prefixos recebidos, uma lista de prefixos deve ser configurada para obstruir especificamente prefixos ruins 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 prefixo de partida devem ser configuradas para permitir especificamente somente 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.

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

Refira a conexão a um provedor de serviços que usa o BGP externo para a cobertura completa da filtração do prefixo BGP.

Filtre prefixos BGP com Listas de acesso do trajeto do 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. Isto pode ser usado conjuntamente com listas de prefixo a fim estabelecer um grupo robusto de filtros.

Os usos deste exemplo de configuração COMO Listas de acesso do trajeto a fim restringir prefixos de entrada àqueles originaram pelo telecontrole COMO e os prefixos de partida àqueles originaram pelo sistema autônomo local. Os prefixos que são originados de todos os sistemas autônomos restantes são filtrados e não instalados na tabela de roteamento.

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

Fixe protocolos 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. Você pode frequentemente executar um Interior Gateway Protocol (IGP) em ordem fornece esta vista. 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 à segurança da rede. Contudo, porque esta autenticação é enviada como a minuta, pode ser simples para que um atacante subverta este controle de segurança.

Adicionando capacidades da mistura MD5 ao processo de autenticação, as atualizações de roteamento já não contêm senhas de texto claro, e os índices inteiros da atualização de roteamento são mais resistentes à alteração. 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 EIGRP Router usando o MD5:

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

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

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

Este é um exemplo de configuração para a autenticação do OSPF Router usando o MD5. O OSPF não utiliza portas-chaves.

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

Refira configurar o OSPF para mais informação.

Comandos passive-interface

Os escapes da informação, ou a introdução de informação falsa em um IGP, podem ser

abrandados com o uso do **comando passive-interface** que ajuda em controlar a propaganda da informação 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:

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

Filtragem de rota

A fim reduzir a possibilidade que você introduz a informação de roteamento falsa na rede, você deve usar o filtragem de rota. 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 o EIGRP e o RASGO, uso do **comando distribute-list** com os limites da palavra-chave da **saída** que informação está anunciada, quando o uso do na palavra-chave limitar que atualizações estão 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:

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

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

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

Refira configurar características independentes do protocolo de IP Routing para obter mais informações sobre de como controlar a propaganda e o processamento das atualizações de roteamento.

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

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

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. Isto é possível com OSPF se você usa os recursos de proteção da sobrecarga do base de dados do estado do link.

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

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

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.

Fixe primeiros protocolos da redundância de salto

Os primeiros protocolos da redundância de salto (FHRPs) fornecem a elasticidade e a Redundância para os 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. À revelia, estes protocolos comunicam-se com as comunicações não-autenticados. 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.

A fim impedir este tipo de ataque, todo o FHRPs que é apoiado pelo Cisco IOS Software inclui uma capacidade da autenticação com o MD5 ou as sequências de caracteres 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:

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

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. É por esta razão que é importante proteger os planos do Gerenciamento e do controle na preferência sobre o plano dos dados quando você fixa 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.

Veja o tráfego de trânsito do filtro com seção do trânsito ACL deste documento para mais informação.

Queda seletiva das opções IP

Há dois interesses de segurança apresentados por opções IP. Trafique que contem opções IP deve ser comutado por processamento pelos dispositivos IOS Cisco, que podem conduzir à carga de CPU elevado. As opções IP igualmente incluem a funcionalidade para alterar o trajeto que o tráfego toma através da rede, que permite potencialmente que subverta controles de segurança.

Devido a estes interesses, as **opções do** global configuration command ip {drop **| ignore}** foi adicionado aos Cisco IOS Software Release 12.3(4)T, 12.0(22)S, e 12.2(25)S. No primeiro

formulário deste comando, as **opções IP deixam cair**, todos os pacotes IP que contêm as opções IP que são recebidas pelo dispositivo IOS Cisco são deixadas cair. Isto impede a carga de CPU elevado e a subversão possível dos controles de segurança que as opções IP podem permitir.

O segundo formulário deste comando, **opções IP ignorar**, configura o dispositivo IOS Cisco para ignorar as opções IP que são contidas em uns 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:

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

Note que alguns protocolos, por exemplo o RSVP, fazem o uso legítimo das 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 do origem de IP, que é permitido à revelia em todos os Cisco IOS Software Release, é deficiente através do comando global configuration do **no ip source-route**. Este exemplo de configuração ilustra o uso deste comando:

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

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 Software envia uma reorientação se recebe um pacote que deva ser roteado através da relação que foi recebido.

Em algumas situações, pôde ser possível para um atacante fazer com que o dispositivo IOS Cisco envie muitas mensagens do redirecionamento de ICMP, que conduz a uma carga de CPU elevado. Por este motivo, recomenda-se que a transmissão dos redirecionamentos de ICMP seja deficiente. Os redirecionamentos de ICMP são desabilitados com o **comando no ip redirects da** configuração da interface, segundo as indicações do exemplo de configuração:

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

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. Esta funcionalidade da transmissão direcionada de entregue como um auxílio da amplificação e da reflexão em diversos ataques, incluindo o ataque de smurf.

As versões atuais do Cisco IOS Software têm esta funcionalidade desabilitada por padrão; contudo, pode ser permitida através do comando interface configuration da **transmissão direta de IP**. As versões do Cisco IOS Software antes de 12.0 têm esta funcionalidade permitida por padrão.

Se uma rede absolutamente requer a funcionalidade da transmissão direcionada, seu uso deve ser controlado. Isto é possível com o uso de um Access Control List como uma opção ao **comando ip directed-broadcast**. Este exemplo de configuração limita transmissões direcionada 2 aqueles pacotes de UDP que originam em uma rede confiável, 192.168.1.0/24:

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

Tráfego de trânsito do filtro com trânsito ACL

Épossível controlar que tráfego transita pela rede com o uso do trânsito ACL (tACLs). Isto é em contraste com a infra-estrutura ACL que procura ao filtrar tráfego que é destinado à rede própria. A filtração fornecida por tACLs é benéfica quando é desejável ao filtrar tráfego a um grupo particular de dispositivos ou de tráfego que transite pela rede.

Este tipo de filtração é executado tradicionalmente por firewall. Contudo, há os exemplos onde pode ser benéfico executar isto que filtra em um dispositivo IOS Cisco na rede, por exemplo, onde filtrar deve ser executada mas nenhum firewall esta presente.

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

Veja a seção anti-falsificação das proteções deste documento para mais informação.

Consulte Listas de Controle de Acesso de Trânsito: Filtração em sua borda para obter mais informações sobre dos 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 transporta podem ter ramificação de grande envergadura no TCP e nos protocolos IP em geral. O ICMP é usado pelas ferramentas de Troubleshooting da rede **executa o ping** e **traceroute**, assim como pelo Path MTU Discovery; contudo, a conectividade externa ICMP é raramente necessária para a operação apropriada de uma rede.

O Cisco IOS Software fornece a funcionalidade para filtrar especificamente por nome da mensagens ICMP ou para datilografá-los e codificá-los. Este exemplo ACL permite o ICMP das redes confiável quando obstruir todos os pacotes ICMP de outras fontes:

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

Filtre fragmentos IP

Como detalhado previamente no acesso do limite à rede com seção da infraestrutura ACL deste documento, a filtração de pacotes IP fragmentados pode levantar um desafio aos 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 estas razões que os fragmentos IP são frequentemente usados nos ataques e devem explicitamente ser filtrados na parte superior de todos os tACLs configurados. O ACL abaixo inclui a filtração detalhada de fragmentos IP. A funcionalidade ilustrada neste exemplo deve ser usada conjuntamente com a funcionalidade dos exemplos anteriores:

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

Refira listas de controle de acesso e fragmentos IP para obter mais informações sobre da manipulação ACL de pacotes IP fragmentados.

Apoio ACL para opções IP de filtração

No Cisco IOS Software Release 12.3(4)T e Mais Recente, o Cisco IOS Software apoia o uso dos ACL filtrar os pacotes IP baseados nas opções IP que são contidas no pacote. A presença de opções IP dentro de um pacote pôde 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 filtradas 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:

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

Proteções anti-falsificação

Muita falsificação do endereço IP de origem do uso dos ataques a ser eficaz ou para esconder o origem verdadeira de um ataque e para impedir o retorno de monitoramento exato. O Cisco IOS Software fornece o unicast RPF e a proteção de origem de IP (IPSG) a fim intimidar os ataques que confiam na falsificação do endereço IP de origem. Além disso, os ACL e o roteamento nulo são frequentemente distribuídos como meios manuais da prevenção da falsificação.

A proteção de origem de IP trabalha para minimizar a falsificação para as redes que estão sob o controle administrativo direto pela porta de switch de execução, pelo MAC address, e pela verificação 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 inspeção dinâmica do Address Resolution Protocol (ARP) (DAI) abranda os vetores do ataque que usam o envenenamento ARP em 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. Os pacotes falsificado poderiam incorporar a rede através de uma relação das RPF-possibilidades do unicast se uma rota do retorno apropriada ao endereço IP de origem existe. O unicast RPF confia em você para permitir

o Cisco Express Forwarding em cada dispositivo e é configurado em uma base da interface per.

O unicast RPF pode ser configurado em um de dois modos: fraco ou restrito. 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:

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

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:

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

Depois que a espião DHCP é permitida, estes comandos enable IPSG:

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

A segurança de porta pode ser permitida com o **IP verifica o** comando configuration da **interface de segurança da porta de origem**. Isto exige a **opção de informação da espião DHCP do** global configuration command ip; adicionalmente, o servidor DHCP deve apoiar a opção de DHCP 82.

Refira configurar características e proteção de origem de IP DHCP para obter mais informações sobre esta característica.

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. Uma vez que a Segurança de portas determinou uma violação MAC, pode usar um de quatro modos da violação. Estes modos protegem, restringem, parada programada, e parada programada VLAN. Nos exemplos quando uma porta fornece somente o acesso para uma estação de trabalho única o uso dos 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.

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

Refira configurar a Segurança de portas para obter mais informações sobre do confuration da Segurança de portas.

Inspeção ARP dinâmica

A inspeção ARP dinâmica (DAI) pode ser usada a fim abrandar ataques do envenenamento ARP em segmentos locais. Um ataque do envenenamento ARP é um método em que um atacante envia a informação falsificada ARP a um segmento local. Esta informação é projetada a fim corromper o cache ARP dos outros dispositivos. Frequentemente um atacante usa o envenenamento ARP a fim de executar um ataque que envolva pessoas.

DAI intercepta e valida o relacionamento de endereço do IP-à-MAC de todos os pacotes ARP em portas não-confiáveis. Em ambientes DHCP, DAI usa os dados que são gerados pela característica da espião DHCP. Os pacotes ARP que são recebidos em relações confiadas não são validados e os pacotes inválidos em interfaces não confiável são descartados. Em ambientes do não-DHCP, o uso de ARP ACL é exigido.

Esta espião dos comandos enable DHCP:

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

Uma vez que a espião DHCP foi permitida, estes comandos habilitam DAI:

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

Em ambientes não-DHCP, o ARP ACL é exigido para habilitar DAI. Este exemplo demonstra a configuração básica de DAI com ARP ACL:

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

Refira a configurar a inspeção ARP dinâmica para obter mais informações sobre de como configurar DAI.

ACL anti-falsificação

Os ACL manualmente configurados podem fornecer a proteção anti-falsificação estática contra os ataques que usam o espaço de endereços não utilizado e não confiável conhecido. Geralmente, estes ACL anti-falsificação são aplicados ao tráfego de ingresso em limites de rede como um componente de um ACL maior. Os ACL anti-falsificação exigem a monitoração regular porque podem frequentemente mudar. A falsificação pode ser minimizada no tráfego que origina da rede local se você aplica os ACL de partida que limitam o tráfego aos endereços de local válido.

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.

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

Refira a configurar IP de uso geral ACL para obter mais informações sobre de como configurar lista de controle de acesso.

A lista oficial de endereços do Internet não alocada é mantida pela equipe Cymru. A informação adicional sobre endereços não utilizados de filtração está disponível na página da referência de Bogon .

Impacto do limite CPU do tráfego plano dos dados

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 dos dados, que consiste no tráfego que transita pelo dispositivo de rede, deve ser fixado para assegurar o funcionamento dos planos do Gerenciamento e do controle. Se o tráfego de trânsito pode fazer com que um dispositivo processe o tráfego do interruptor, o plano do controle de um dispositivo pode ser afetado que possa conduzir a um rompimento 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:

- **Logging ACL** - O tráfego do logging ACL consiste em todos os pacotes que forem gerado devido a um fósforo (permit or deny) de um ACE em que a palavra-chave do **log** é usada.
- **Unicast RPF** - O unicast RPF usado conjuntamente com um ACL pôde conduzir à comutação do processo de determinados pacotes.
- **Opções IP** - Todos os pacotes IP com as opções incluídas devem ser processados pelo CPU.
- **Fragmentação** - Todo o pacote IP que exigir a fragmentação deve ser passado ao CPU para processar.
- **Expiração do tempo ao vivo (TTL)** - Os pacotes que têm um valor TTL inferior ou igual a 1 para exigir o tempo do protocolo Protocolo de control de mensajes de Internet (ICMP) excederam (tipo 11 ICMP, código 0) as mensagens a ser enviadas, que conduz ao processamento de CPU.
- **ICMP não alcançável** - Os pacotes que conduzem aos mensagens que não chega a seu destino do ICMP devido à distribuição, ao MTU ou à filtração são processados pelo CPU.
- **Tráfego que exige uma requisição ARP** - Os destinos para que uma entrada de ARP não existe exigem o processamento pelo CPU.
- **Tráfego não-IP** - Todo o tráfego não-IP é processado pelo CPU.

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

Filtre no valor TTL

Você pode usar o apoio ACL para filtrar na característica do valor TTL, introduzido no Cisco IOS Software Release 12.4(2)T, em uma lista de acesso IP estendido para filtrar os pacotes baseados 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 podem igualmente ser usados a fim assegurar que o valor TTL não é mais baixo do que o diâmetro da rede, assim a proteção do plano do controle de dispositivos de infra-estrutura a jusante dos ataques da expiração TTL.

Note que algumas aplicações e ferramentas tais como o **traceroute** usam pacotes da expiração TTL para o teste e os propósitos de 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.

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

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.

No Cisco IOS Software Release 12.4(4)T e Mais Recente, o pacote flexível que combina (FPM) permite que um administrador combine em bit arbitrários de um pacote. Esta política FPM deixa cair pacotes com um valor TTL menos de seis.

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

Refira a harmonização flexível do pacote, situada no pacote flexível do Cisco IOS que combina o homepage, para obter mais informações sobre a característica.

Filtre na presença de opções IP

No Cisco IOS Software Release 12.3(4)T e Mais Recente, você pode usar o apoio ACL para a característica de filtração das opções IP em um Nomeado, lista de acesso IP estendido a fim filtrar pacotes IP com as opções IP atuais. Os pacotes IP de filtração que são baseados na presença de opções IP podem igualmente ser usados a fim impedir que o plano do controle dos dispositivos de infra-estrutura tenha que processar estes pacotes a nível CPU.

Note que o apoio ACL para opções IP que de filtração a característica pode ser usada somente com nomeado, ACL estendido. Deve-se igualmente notar que o RSVP, a Engenharia de tráfego Multiprotocol Label Switching, os Versão 2 do IGMP e 3, e outros protocolos que usam pacotes das opções IP não puderam poder funcionar corretamente se os pacotes para estes protocolos são deixados cair. Se estes protocolos estão no uso na rede, a seguir o apoio ACL para opções IP de filtração pode ser usado; contudo, a característica seletiva da gota das opções IP ACL poderia deixar cair este tráfego e estes protocolos não puderam funcionar corretamente. Se não há nenhum protocolo no uso que exige opções IP, a gota seletiva das opções IP ACL é o método preferido para deixar cair estes pacotes.

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

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

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

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

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```
Veja a seção de endurecimento plana dos dados gerais deste original para obter mais informações sobre da gota seletiva das opções IP ACL.

Consulte Listas de Controle de Acesso de Trânsito: Filtração em sua borda para obter mais informações sobre do tráfego de filtração do trânsito e da borda.

Uma outra característica no Cisco IOS Software que pode ser usado a fim filtrar pacotes com opções IP é CoPP. No Cisco IOS Software Release 12.3(4)T e Mais Recente, CoPP permite que um administrador filtre o fluxo de tráfego de pacotes do plano do controle. Um dispositivo que apoie CoPP e apoio ACL para opções IP de filtração, introduzidos no Cisco IOS Software Release 12.3(4)T, pode usar uma política da lista de acessos para filtrar os pacotes que contêm 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:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```
Esta política de CoPP deixa cair os pacotes de trânsito recebidos por um dispositivo quando estas opções IP estão presentes:

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

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```
Nas políticas precedentes de CoPP, as entradas do Access Control List (ACE) pacotes dessa combinação com o resultado da ação da *licença n*estes pacotes que estão sendo rejeitados pela função da *queda do* mapa de política, quando os pacotes que combinam a ação da *negação* (não mostrada) não forem afetados pela função da *queda do* mapa de política.

Refira o Policiamento do plano de controle de distribuição para obter mais informações sobre da característica de CoPP.

Controle a proteção plana

No Cisco IOS Software Release 12.4(4)T e Mais Recente, controle a proteção plana (CPPr) pode ser usado a fim tráfego plano restringir ou de controle de polícia pelo CPU de um dispositivo IOS Cisco. Quando similar a CoPP, CPPr tem a capacidade para restringir ou policiar o tráfego usando a granularidade mais fina do que CoPP. CPPr divide o plano agregado do controle em três categorias separadas do plano do controle conhecidas como subinterfaces: As subinterfaces do host, do trânsito, e da CEF-Exceção existem.

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.

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

Na política precedente de CPPr, as entradas do Access Control List que combinam pacotes com a ação da licença conduzem a estes pacotes que estão sendo rejeitados pela função da gota do mapa de política, quando os pacotes que combinam a ação da negação (não mostrada) não forem afetados pela função da gota do mapa de política.

Refira a compreendendo a proteção plana do controle e controle a proteção plana para obter mais informações sobre da característica de CPPr.

Trafique a identificação e o retorno de monitoramento

Às vezes, você pode precisar de identificar rapidamente e tráfego de rede do retorno de monitoramento, especialmente durante a resposta do incidente ou o desempenho da rede deficiente. O Netflow e a classificação ACL são os dois métodos principais para realizar isto com Cisco IOS Software. O NetFlow pode fornecer a visibilidade em todo o tráfego na rede. Adicionalmente, o NetFlow pode ser executado com coletores que podem fornecer a tensão do prazo e a 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 de Netflow podem ser vistos e analisado através do CLI, ou os dados podem ser exportados para um coletor de Netflow do anúncio publicitário ou do freeware para a agregação e a 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 do Netflow podem ser criados com os dados de tráfego provados em ambientes do volume alto.

O CEF, ou o CEF distribuído, são uma condição prévia a permitir 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 Software, o comando habilitar o NetFlow em uma relação é o **fluxo do cache de rota IP** em vez do **fluxo IP {entrada | saída}**.

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

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 (26662860 total packets):
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

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
```

```
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(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-other 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-other 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
```

Refira ao NetFlow do Cisco IOS para obter mais informações sobre das capacidades do NetFlow.

Refira a introdução ao NetFlow do Cisco IOS - uma visão geral técnica para uma visão geral técnica 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 pôde igualmente separar o implícito nega no fim de um ACL em ACE granulados para ajudar a identificar os tipos de tráfego negado.

Um administrador pode expedir uma resposta do incidente usando a classificação ACL com a **lista de acesso da mostra** e os comandos exec **claros dos contadores da lista de acesso IP**.

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

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
```

```
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

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(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-other 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-other 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
```

A fim de identificar o tráfego que usa uma classificação ACL, use o comando EXEC **show access-list acl-name**. Os contadores ACL podem ser cancelados com pelo comando exec **claro do ACL-nome dos contadores da lista de acesso IP**.

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

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 mapas VLAN e lista de controle de acesso da porta

As lista de controle de acesso VLAN (VACL), ou os mapas VLAN e a porta ACL (PACL), fornecem a capacidade para reforçar o controle de acesso no tráfego não-roteado que é mais perto dos dispositivos de ponto final do que as lista de controle de acesso que são aplicadas às interfaces roteada.

Estas seções fornecem uma vista geral das características, dos benefícios, e das encenações do uso potencial dos VACL e dos PACL.

Controle de acesso com mapas VLAN

Os VACL, ou o mapas VLAN aplicam a todos os pacotes que incorporam o VLAN, fornecem a capacidade para reforçar o controle de acesso no tráfego do intra-VLAN. Isto não é possível com os ACL em interfaces roteada. Por exemplo, um mapa VLAN pôde ser usado a fim impedir os anfitriões que são contidos dentro do mesmo VLAN de uma comunicação um com o otro, que reduza oportunidades para que atacantes ou os worms locais explorem um host no mesmo segmento de rede. A fim negar pacotes de usar um mapa VLAN, você pode criar um Access Control List (ACL) essa combinação de tráfego e, no mapa VLAN, se ajusta à ação para deixar cair. Uma vez que um mapa VLAN é configurado, todos os pacotes que incorporam o LAN estão avaliados sequencialmente contra o mapa do VLAN configurado. Os mapas do acesso de vlan apoiam o IPv4 e as listas de acessos MAC; contudo, não suportam o registo ou o IPv6 ACL.

Este exemplo usa uma lista de acesso nomeada prolongada que ilustre a configuração desta característica:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Este exemplo demonstra o uso de um mapa VLAN a fim negar portas TCP 139 e 445 assim como o protocolo VINES-IP:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Refira a configurar a segurança de rede com os ACL para obter mais informações sobre da configuração de mapas VLAN.

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 PACL, que toma a precedência sobre mapas e ACLs de roteador VLAN, é a mesma que ACLs de 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 um IPv4, do IPv6, ou do MAC ACL e aplicativo dela à interface de camada 2.

Este exemplo usa uma lista de acesso nomeada prolongada a fim ilustrar a configuração desta característica:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Refira a seção ACL da porta de configurar a segurança de rede com os ACL para obter mais informações sobre da configuração dos PACL.

Controle de acesso com MAC

As lista de controle de acesso MAC ou as lista prolongadas podem ser aplicadas na rede IP com o uso deste comando no modo de configuração da interface:

```
Cat6K-IOS(config-if)#mac packet-classify
```

> Nota: É classificar pacotes da camada 3 como pacotes da camada 2. O comando é apoiado no Cisco IOS Software Release 12.2(18)SXD (para Sup720) e nos Cisco IOS Software Release 12.2(33)SRA ou Posterior.

Este comando de interface tem que ser aplicado na interface de entrada e instrui o Forwarding Engine para não inspecionar o cabeçalho IP. O resultado é que você pode usar uma lista de acessos MAC no ambiente IP.

Uso do VLAN privado

Os VLAN privados (PVLAN) são uns recursos de segurança da camada 2 que limitem a conectividade entre estações de trabalho ou server dentro de um VLAN. Sem PVLAN, todos os dispositivos em uma camada 2 VLAN podem comunicar-se livremente. As situações da comunicação de rede existem onde a segurança pode ser ajudada limitando uma comunicação entre dispositivos em um único VLAN. Por exemplo, os PVLAN são frequentemente usados a fim de proibir uma comunicação entre um servidor em uma sub-rede publicamente acessível. Se um servidor único torna-se comprometida, a falta da Conectividade a outros server devido ao aplicativo dos PVLAN pôde ajudar a limitar o acordo ao um server.

Há três tipos de VLAN privados: VLAN isolada, VLAN de comunidade, e VLAN principal. A configuração dos PVLAN utiliza preliminar e VLAN secundários. O VLAN principal contem todas as portas misturadas, que são descritas mais tarde, e inclui uns ou vários VLAN secundários, que podem ser isolados ou VLAN de comunidade.

Vlan isolado

A configuração de um VLAN secundário como um vlan isolada impede completamente uma comunicação entre dispositivos no VLAN secundário. Pôde somente haver um vlan isolada pelo VLAN principal, e somente as portas misturadas podem comunicar-se com as portas em um vlan isolada. Os vlan isolados devem ser usados em redes não confiáveis como as redes que apoiam convidados.

Este exemplo de configuração configura o VLAN 11 como um VLAN isolado e associa-o ao VLAN principal, VLAN 20. O exemplo abaixo igualmente configura os FastEthernet 1/1 da relação como uma porta isolada no VLAN 11:

```
Cat6K-IOS(config-if)#mac packet-classify
```

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.

```
Cat6K-IOS(config-if)#mac packet-classify
```

Portas misturadas

As portas de switch que são colocadas no VLAN principal são conhecidas como portas misturadas. As portas misturadas podem comunicar-se com todas portas restantes no preliminar e nos VLAN secundários. Roteadores ou as interfaces de firewall são os dispositivos mais comuns encontrados nestes VLAN.

Este exemplo de configuração combina os exemplos precedentes isolado e do VLAN de comunidade e adiciona a configuração dos FastEthernet 1/12 da relação como uma porta misturada:

```
Cat6K-IOS(config-if)#mac packet-classify
```

Quando você executa PVLAN, é importante assegurar-se de que a configuração da camada 3 no lugar apoie as limitações que são impostas por PVLAN e não as permita a configuração de PVLAN ser subvertidas. A camada 3 que filtra com um roteador ACL ou o Firewall pode impedir a subversão da configuração de PVLAN.

Refira os VLAN privados (os PVLAN) - Promíscuo, isolado, a comunidade, encontrado no homepage da Segurança para LAN, para obter mais informações sobre do uso e da configuração dos VLAN privados.

Conclusão

Este original dá-lhe uma visão geral ampla dos métodos que podem ser usados a fim fixar um dispositivo de sistema do Cisco IOS. 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.

Anexo: Dispositivo IOS Cisco que endurece a lista de verificação

Esta lista de verificação é uma coleção de todas as etapas de endurecimento que são apresentadas neste guia. Os administradores podem usá-la enquanto um lembrete de todo o

endurecimento caracteriza usado e considerado para um dispositivo IOS Cisco, mesmo se uma característica não foi executada porque não se aplicou. Os administradores estão recomendados avaliar cada opção para seu risco potencial antes que executem a opção.

Plano de gerenciamento

- Senhas

  Permita o hashing MD5 (opção secreta) para senhas habilitadas e de usuários locais.Configurar o fechamento da nova tentativa da senhaDesabilite a recuperação de senha (considere o risco)

- Desabilite serviços não utilizados

- Configurar manutenções de atividade TCP para sessões de gerenciamento

- Ajuste a memória e as notificações de threshold de CPU

- Configurar

  Notificações da memória e de threshold de CPUMemória da reserva para o acesso de consoleDetector de escape de memóriaDetecção do excesso de bufferColeção aumentada do crashinfo

- Use iACLs para restringir o acesso de gerenciamento

- Filtre (considere o risco)

  Pacotes ICMPFragmentos IPOpções IPValor TTL nos pacotes

- Controle a proteção plana

  Configurar a filtração da portaConfigurar pontos iniciais da fila

- Acesso de gerenciamento

  Use a proteção do plano de gerenciamento para restringir interfaces de gerenciamentoAjuste o intervalo do executivoUse um protocolo de transporte cifrado (tal como o SSH) para o acesso CLIControle o transporte para as linhas vty e o tty (opção da classe do acesso)Advirta usando bandeiras

- AAA

  Use o AAA para a autenticação e a reservaUse AAA (TACACS+) para o comando authorizationUse o AAA explicandoUse servidores AAA redundantes

- SNMP:

Configurar as comunidades SNMPv2 e aplique ACLConfigurar o SNMPv3

- Registro

  Configure o registro centralizadoAjuste níveis de registro para todos os componentes relevantesAjuste a fonte-interface de registoConfigurar a granularidade do data/hora de registro

- Gerenciamento de configuração

  Substitua e rollbackConfiguração Exclusiva de Alteração de AcessoConfiguração de resiliência do softwareNotificações da alteração de configuração

Controle o plano

- Desabilitar (considere o risco)

  Redirecionamentos de ICMPICMP não alcançávelProxy ARP

- Configurar a autenticação de NTP se o NTP está sendo usado
- Configurar o policiamento do plano do controle/proteção (filtração da porta, os pontos iniciais da fila)
- Fixe protocolos de roteamento

  BGP (TTL, MD5, prefixos máximos, listas de prefixo, trajeto ACL do sistema)IGP (MD5, interface passiva, filtragem de rota, consumo do recurso)

- Configurar limitadores da taxa do hardware
- Fixe os primeiros protocolos da redundância de salto (GLBP, HSRP, o VRRP)

Plano dos dados

- Configurar a queda seletiva das opções IP
- Desabilitar (considere o risco)

  Roteamento do origem de IPBroadcasts direto de IPRedirecionamentos de ICMP

- Broadcasts direto de IP do limite
- Configurar tACLs (considere o risco)

  Filtre o ICMPFiltre fragmentos IPFiltre opções IPFiltre valores TTL

- Configure proteções anti-falsificação exigidas

  ACLProteção de origem de IPInspeção ARP dinâmicaUnicast RPFSegurança da porta

- Controle a proteção plana (a CEF-exceção do controle plano)
- Configurar o NetFlow e a classificação ACL para a identificação do tráfego
- Configure exigiu o controle de acesso ACL (mapas VLAN, PACL, o MAC)
- Configurar VLAN privados