GSR: Receber listas de controle de acesso

Contents

Introduction

Este documento descreve um novo recurso de segurança chamado de listas de controle de acesso de recebimento (rACLs)1 e fornece recomendações e diretrizes de implementação de rACL. Os ALCs de recepção são usados para aumentar a segurança em Cisco 12000 routers, protegendo o GRP (gigabit route processor) do roteador de tráfego desnecessário e possivelmente abominável. As ACLs de recebimento foram adicionadas como um waiver especial ao acelerador de manutenção para o Cisco IOS ® Software Release 12.0.21S2 e integradas no Cisco IOS Software Release 12.0(22)S.

Proteção GRP

Os dados recebidos por um roteador de switch gigabit (GSR) podem ser divididos em duas grandes categorias:

- Tráfego que passa pelo roteador através do caminho de encaminhamento.
- Tráfego que deve ser enviado através do caminho de recebimento para o GRP para análise adicional.

Em operações normais, a grande maioria do tráfego simplesmente flui através de um GSR em rota para outros destinos. No entanto, o GRP deve lidar com certos tipos de dados, principalmente protocolos de roteamento, acesso remoto a roteadores e tráfego de gerenciamento de rede (como SNMP). Além desse tráfego, outros pacotes da Camada 3 podem exigir a flexibilidade de processamento do GRP. Elas incluem certas opções IP e certas formas de pacotes ICMP (Internet Control Message Protocol). Consulte o apêndice sobre adjacências de recepção e pacotes pontuados para obter detalhes adicionais sobre rACLs e tráfego de caminho

de recepção no GSR.

Um GSR tem vários caminhos de dados, cada um atendendo diferentes formas de tráfego. O tráfego de trânsito é encaminhado da placa de ingresso (LC) para a tela e depois para a placa de saída referente à entrega do próximo salto. Além do caminho de dados de tráfego de trânsito, um GSR tem dois outros caminhos para o tráfego que exige processamento local: LC para LC CPU e LC para LC CPU para fabric para GRP. A tabela a seguir mostra os caminhos dos diversos recursos e protocolos normalmente utilizados.

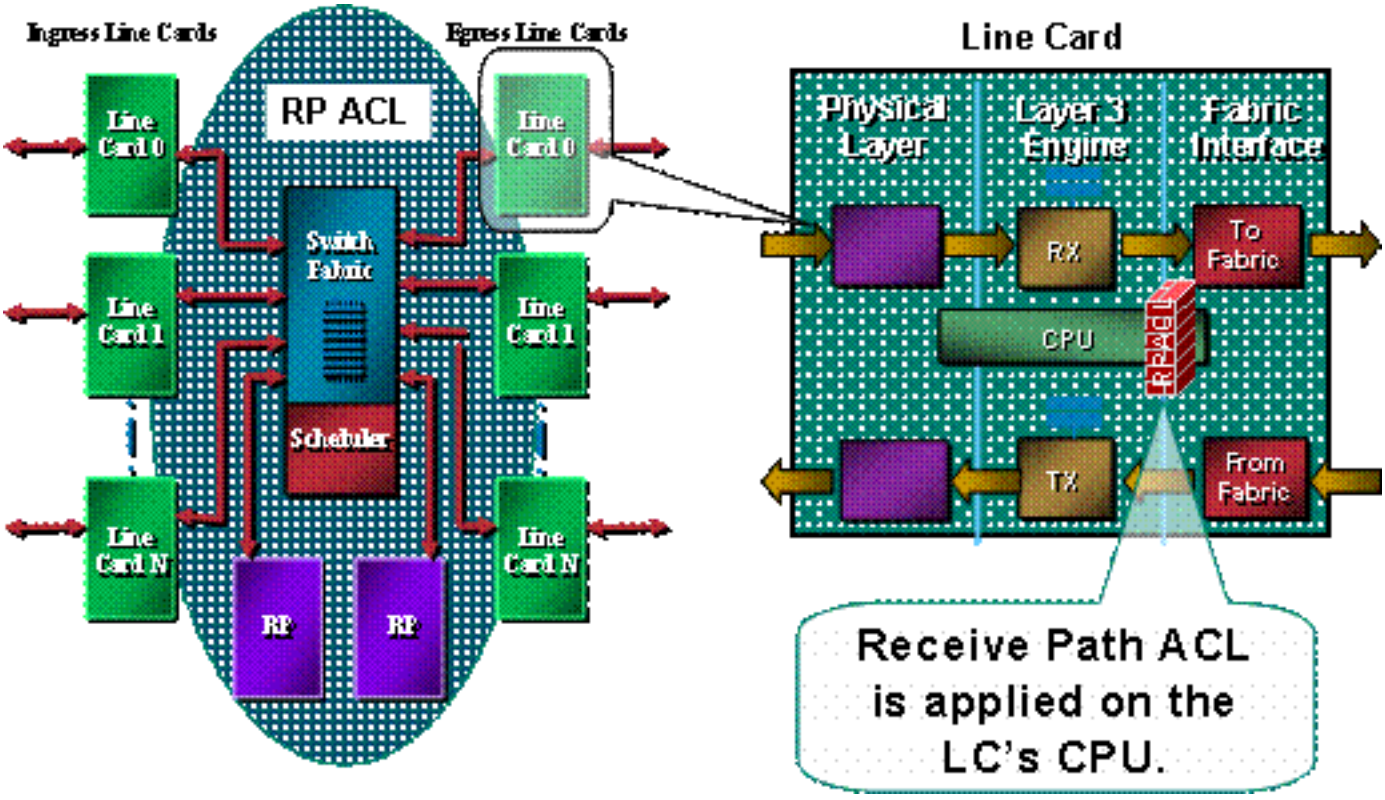
Tipo de tráfego	Caminho de dados
Tráfego normal (em trânsito)	LC para estrutura para LC
Protocolos de roteamento/SSH/SNMP	LC para LC CPU para fabric para GRP
Eco ICMP (ping)	LC para CPU LC
Registro	

O processador da rota para o GSR tem uma capacidade limitada para processar o tráfego entregue dos LCs destinados para o próprio GRP. Se um alto volume de dados exigir o encaminhamento ao GRP, esse tráfego poderá sobrecarregar o GRP. Isso resulta em um ataque de negação de serviço (DoS) eficaz. A CPU do GRP luta para acompanhar o exame do pacote e começa a descartar pacotes, inundando as filas input-hold e Selective Packet Discard (SPD). [2] Os GSRs devem ser protegidos contra três cenários, que podem resultar de ataques de DoS direcionados a um GRP do roteador.

- Perda de Routing Protocol Packet a partir de uma inundação de prioridade normal
- Perda de pacote de sessão de gerenciamento (Telnet, Secure Shell [SSH], SNMP) de uma inundação de prioridade normal
- Perda de pacote de inundação de alta prioridade falsificada

A possível perda de dados do protocolo de roteamento durante uma inundação de prioridade normal é atualmente aliviada pela classificação estática e pela limitação da taxa de tráfego destinado ao GRP a partir das LCs. Infelizmente, este enfoque tem limitações. O limite de taxa para o tráfego de prioridade normal destinado ao GRP é insuficiente para garantir a proteção aos dados do protocolo de roteamento de alta prioridade se um ataque for entregue por várias LCs. Reduzir o limite no qual os dados de prioridade normal são descartados para fornecer tal proteção apenas aumenta a perda de tráfego de gerenciamento de uma inundação de prioridade normal.

Como esta imagem mostra, o rACL é executado em cada LC antes de o pacote ser transmitido ao GRP.



Énecessário um mecanismo de proteção para o GRP. As rACLs afetam o tráfego enviado ao GRP devido às adjacências de recepção. As adjacências de recepção são adjacências do Cisco Express Forwarding para o tráfego destinado aos endereços IP do roteador, como o endereço de broadcast ou os endereços configurados nas interfaces do roteador. [3] Consulte a seção do apêndice para obter mais detalhes sobre adjacências de recepção e pacotes punted.

O tráfego que entra em uma LC é enviado primeiro à CPU local da LC, e os pacotes que exigem processamento pelo GRP são enfileirados para encaminhamento ao processador de rota. O ACL de recebimento é criado no GRP e enviado para os CPUs dos diversos LCs. Antes de o tráfego ser enviado da CPU do LC para o GRP, o tráfego é comparado ao rACL. Se permitido, o tráfego passa para o GRP, enquanto todo o tráfego restante é negado. O rACL é inspecionado antes para o LC para a função de limitação de taxa GRP. Uma vez que o rACL é usado para todas as adjacências de recepção, alguns pacotes tratados pelo LC CPU (como requisições de eco) estão sujeitos também à filtragem de rACL. Isso deve ser levado em consideração ao designar entradas rACL.

As ACLs de recepção fazem parte de um conjunto de mecanismos de vários programas para proteger os recursos em um roteador. O trabalho futuro incluirá um componente de limitação de taxa para o rACL.

Impacto de desempenho

Nenhuma memória é consumida além da necessária para manter a entrada de configuração única e a própria lista de acesso definida. O rACL é copiado para cada LC, de modo que uma pequena área de memória é tomada em cada LC. Em geral, os recursos utilizados são escassos, especialmente quando comparados com os benefícios da implantação.

Uma ACL de recepção não afeta o desempenho do tráfego encaminhado. O rACL se aplica somente ao tráfego de adjacência de recebimento. O tráfego encaminhado nunca está sujeito ao rACL. O tráfego de trânsito é filtrado usando ACLs de interface. Essas ACLs "regulares" são aplicadas às interfaces em uma direção especificada. O tráfego está sujeito ao processamento de

ACL antes do processamento de rACL, de modo que o tráfego negado pela ACL da interface não será recebido pelo rACL. [4]

O LC que executa a filtragem real (em outras palavras, o LC que recebe o tráfego filtrado pelo rACL) terá maior utilização da CPU devido ao processamento do rACL. Esse aumento na utilização da CPU, no entanto, é causado por um alto volume de tráfego destinado ao GRP; o benefício do GRP da proteção rACL supera muito o aumento da utilização da CPU em um LC. O uso de CPU em uma LC varia de acordo com o tipo de mecanismo LC. Por exemplo, dado o mesmo ataque, um Engine 3 LC terá uma utilização de CPU menor que um Engine 0 LC.

Habilitar ACLs turbo (usando o comando **access-list collection**) converte ACLs em uma série altamente eficiente de entradas da tabela de pesquisa. Quando as ACLs turbo estão ativadas, a profundidade da rACL não afeta o desempenho. Em outras palavras, a velocidade de processamento é independente do número de entradas na ACL. Se o rACL for curto, as ACLs turbo não aumentarão significativamente o desempenho, mas consumirão memória; com rACLs curtas, as ACLs compiladas provavelmente não são necessárias.

Ao proteger o GRP, o rACL ajuda a garantir a estabilidade do roteador e, por fim, da rede durante um ataque. Como descrito acima, o rACL é processado na CPU do LC, de modo que a utilização da CPU em cada LC aumentará quando um grande volume de dados for direcionado ao roteador. Em E0/E1 e alguns pacotes E2, a utilização da CPU de mais de 100% pode levar a quedas do protocolo de roteamento e da camada de enlace. Esses descartes estão localizados na placa, e os processos de roteamento de GRP são protegidos, mantendo assim a estabilidade. Placas E2 com microcódigo habilitado para limitação [5] ativam o modo de limitação quando estão sob carga pesada e encaminham apenas o tráfego de precedência 6 e 7 para o protocolo de roteamento. Outros tipos de mecanismo têm arquiteturas de várias filas; por exemplo, as placas E3 têm três filas para a CPU, com pacotes de protocolo de roteamento (precedência 6/7) em uma fila separada de alta prioridade. A CPU de LC alta, a menos que os pacotes de alta precedência a causem, não resultará em descartes do protocolo de roteamento. Os pacotes para as filas de prioridade mais baixa serão descartados posteriormente. Finalmente, as placas baseadas em E4 têm oito filas para a CPU, com uma dedicada aos pacotes do protocolo de roteamento.

Sintaxe

Uma ACL de recebimento é aplicada com o seguinte comando de configuração global para distribuir a rACL a cada LC no roteador.

```
[no] ip receive access-list
```

Nesta sintaxe, *<num>* é definido da seguinte forma.

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

Modelo básico e exemplos de ACL

Para poder usar esse comando, você precisa definir uma lista de acesso que identifique o tráfego que deve ter permissão para se comunicar com o roteador. A lista de acesso precisa incluir protocolos de roteamento e tráfego de gerenciamento (Border Gateway Protocol [BGP], Open

Shortest Path First [OSPF], SNMP, SSH, Telnet). Consulte a seção sobre diretrizes de distribuição para obter mais detalhes.

A seguinte amostra de ACL fornece um descrição simples e apresenta alguns exemplos de configuração que podem ser adaptador para usos específicos. A ACL ilustra as configurações exigidas para diversos serviços/protocolos comumente necessários. Para SSH, Telnet e SNMP, um endereço de loopback é usado como o destino. Para os protocolos de roteamento, o endereço real da interface é usado. A escolha de interfaces do encaminhador para usar no rACL é determinada por políticas e operações do site local. Por exemplo, se os loopbacks forem usados para todas as sessões de peering do BGP, somente esses loopbacks precisarão ser permitidos nas instruções **permit** para o BGP.

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

Como com todas as ACLs da Cisco, há uma instrução **deny** implícita no final da lista de acesso, portanto qualquer tráfego que não corresponda a uma entrada na ACL será negado.

Observação: a palavra-chave **log** pode ser usada para ajudar a classificar o tráfego destinado ao GRP que não é permitido. Embora a palavra-chave **log** forneça informações valiosas sobre os detalhes dos acertos de ACL, acertos excessivos em uma entrada de ACL que usa essa palavra-chave aumentarão a utilização da CPU LC. O impacto no desempenho associado ao registro varia com o tipo de mecanismo LC. Em geral, o registro deve ser usado somente quando necessário nos mecanismos 0/1/2. Para os mecanismos 3/4/4+, o registro resulta em muito menos impacto devido ao aumento do desempenho da CPU e da arquitetura de várias filas.

O nível de granularidade dessa lista de acessos é determinado pela política de segurança local (por exemplo, o nível de filtragem necessário para vizinhos OSPF).

rACLS e pacotes fragmentados

As ACLs têm uma palavra-chave **fragments** que permite um comportamento especializado de manipulação de pacotes fragmentados. Em geral, os fragmentos não iniciais que correspondem às instruções L3 (independentemente das informações L4) em uma ACL são afetados pela instrução **permit** ou **deny** da entrada correspondente. Observe que o uso da palavra-chave **fragments** pode forçar as ACLs a negar ou permitir fragmentos não iniciais com mais granularidade.

No contexto rACL, a filtragem de fragmentos adiciona uma camada adicional de proteção contra um ataque DoS que usa apenas fragmentos não iniciais (como FO > 0). O uso de uma instrução deny para fragmentos não-iniciais no começo do rACL impede que todos os fragmentos não-iniciais acessem o roteador. Em circunstâncias raras, uma sessão válida pode exigir fragmentação e, portanto, ser filtrada se uma instrução **deny fragment** existir no rACL.

Por exemplo, considere a ACL parcial mostrada abaixo.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

Adicionar essas entradas ao início de um rACL nega qualquer acesso de fragmento não inicial ao GRP, enquanto pacotes não fragmentados ou fragmentos iniciais passam para as próximas linhas do rACL não afetadas pelas instruções **deny fragment**. O trecho rACL acima também facilita a classificação do ataque, pois cada protocolo - Universal Datagram Protocol (UDP), TCP e ICMP - incrementa contadores separados na ACL.

Consulte Listas de Controle de Acesso e Fragmentos IP para obter uma discussão detalhada das opções.

Avaliação de risco

Certifique-se de que a rACL não filtre o tráfego crítico, como protocolos de roteamento ou acesso interativo aos roteadores. Filtrar o tráfego necessário pode resultar na incapacidade de acessar remotamente o roteador, exigindo, assim, uma conexão de console. Por esse motivo, as configurações do laboratório devem imitar a implantação real o mais próximo possível.

Como sempre, a Cisco recomenda que você teste esse recurso no laboratório antes da implantação.

Apêndices e notas

Receber adjacências e pacotes punted

Conforme descrito anteriormente neste documento, alguns pacotes requerem processamento GRP. Os pacotes são direcionados do plano de encaminhamento de dados para o GRP. Esta é uma lista das formas comuns de dados da Camada 3 que exigem acesso GRP.

- Protocolos de Roteamento
- Tráfego de controle multicast (OSPF, Hot Standby Router Protocol [HSRP], TDP (Tag Distribution Protocol [protocolo de distribuição de etiquetas]), PIM (Protocol Independent Multicast [protocolo independente], entre outros))
- Pacotes Multiprotocol Label Switching (MPLS) que precisam de fragmentação
- Pacotes com certas opções de IP, como alerta de roteador
- Primeiro pacote de fluxos multicast
- Pacotes ICMP fragmentados que exigem remontagem
- Todo o tráfego destinado ao próprio roteador (exceto o tráfego tratado no LC)

Como rACLs se aplicam para receber adjacências, o rACL filtra algum tráfego que não é direcionado ao GRP, mas é uma adjacência de recebimento. O exemplo mais comum é uma requisição de eco ICMP (ping). As solicitações de eco ICMP direcionadas ao roteador são tratadas pela CPU do LC; como as solicitações recebem adjacências, elas também são filtradas pelo rACL. Portanto, para permitir ping nas interfaces (ou loopbacks) do roteador, rACLS deve permitir explicitamente as solicitações de eco.

Épossível ver a recepção de adjacências usando o comando show ip cef.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

Diretrizes de implantação

A Cisco recomenda práticas conservadoras de implantação. Para implantar rACLs com êxito, os requisitos de acesso do plano de controle e gerenciamento existentes devem ser bem compreendidos. Em algumas redes, pode ser difícil determinar o perfil de tráfego exato necessário para criar as listas de filtragem. As seguintes diretrizes descrevem um método bastante conservador para implantar rACLs usando configurações rACL iterativas para ajudar a identificar e eventualmente filtrar o tráfego.

1. **Identificar os protocolos usados na rede com uma ACL de classificação.**Implante um rACL que permita todos os protocolos conhecidos que acessam o GRP. Esse rACL de "descoberta" deve ter os endereços de origem e de destino definidos como **qualquer**. O registro pode ser usado para desenvolver uma lista de endereços de origem que correspondem às instruções **permit** do protocolo. Além da instrução **permit** do protocolo, uma **permit any any log** line no final do rACL pode ser usada para identificar outros protocolos que seriam filtrados pelo rACL e que poderiam exigir acesso ao GRP.O objetivo é determinar quais protocolos a rede específica utiliza. O registro deve ser usado para análise para determinar "o que mais" pode estar se comunicando com o roteador.**Observação:** embora a palavra-chave **log** forneça informações valiosas sobre os detalhes de acertos de ACL, acertos excessivos em uma entrada de ACL que usa essa palavra-chave podem resultar em um número esmagador de entradas de log e possivelmente alto uso de CPU do roteador. Use a palavra-chave log para pequenos períodos de tempo e somente quando necessário para ajudar a classificar o tráfego.
2. **Revise os pacotes identificados e comece a filtrar o acesso ao GRP.**Assim que os pacotes filtrados pelo rACL na etapa 1 tenham sido identificados e revistos, implemente um rACL com uma instrução permit any any para os protocolos permitidos. Assim como na etapa 1, a palavra-chave **log** pode fornecer mais informações sobre os pacotes que correspondem às entradas **permit**. O uso de deny any any log no final pode ajudar a identificar pacotes inesperados destinados ao GRP. Este rACL fornecerá proteção básica e permitirá que os engenheiros da rede assegurem que todo o tráfego necessário seja permitido.O objetivo é testar o intervalo de protocolos que precisam se comunicar com o roteador sem ter o intervalo explícito de endereços IP origem e destino.
3. **Restringir um intervalo de macro de endereços de origem.**Permita que apenas o intervalo total de seu Classless Interdomain Routing (CIDR) Block seja permitido como o endereço de

origem. Por exemplo, se você recebeu 171.68.0.0/16 para sua rede, permita endereços de origem de apenas 171.68.0.0/16.Esta etapa reduz o risco sem interromper qualquer serviço. Ele também fornece pontos de dados de dispositivos/pessoas de fora do bloco CIDR que podem estar acessando seu equipamento. Todo o endereço externo será descartado.Os peers BGP externos exigirão uma exceção, já que os endereços de origem permitidos para a sessão estarão fora do bloco CIDR.Essa fase pode ser ignorada por alguns dias para coletar dados para a fase seguinte de refinamento da rACL.

4. **Restrinja as instruções permit da rACL para permitir somente endereços de origem autorizados conhecidos.**Limitar cada vez mais o endereço de origem a apenas as fontes de permissão que se comunicam com o GRP.
5. **Limite os endereços de destino no rACL. (opcional)**Alguns provedores de serviço da Internet (ISP) podem escolher permitir apenas protocolos específicos para usar endereços de destino específicos no roteador. Essa fase final tem a finalidade de limitar o intervalo dos endereços de destino que aceitarão tráfego para um protocolo. [6]

Exemplo de implantação

O exemplo a seguir mostra uma ACL de recebimento que protege um roteador com base no seguinte endereçamento.

- O bloco de endereço do ISP é 169.223.0.0/16.
- O bloco de infraestrutura do ISP é 169.223.252.0/22.
- O circuito de retorno do roteador é 169.223.253.1/32.
- O roteador é um roteador de backbone central, portanto somente sessões de BGP estão ativas.

Considerando essas informações, a ACL de recebimento inicial pode ser algo como o exemplo abaixo. Como conhecemos o bloco de endereço de infra-estrutura, permitiremos primeiro o bloco inteiro. Posteriormente, entradas de controle de acesso (ACEs) mais detalhadas serão adicionadas, pois os endereços específicos são obtidos para todos os dispositivos que precisam de acesso ao roteador.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
!--- Note: This template must be tuned to the network’s !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
```

```
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 – Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example – Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

Notas

1. Consulte Understanding Selective Packet Discard (SPD) [&Entendendo o SPD (Descarte seletivo de pacotes)] e mantenha as diretrizes da fila para aumentar a resistência do DoS.
2. Para obter mais informações sobre o Cisco Express Forwarding e adjacências, consulte Visão geral do Cisco Express Forwarding.
3. Para uma discussão detalhada sobre as diretrizes de implantação da ACL e comandos relacionados, consulte Implementando ACLs em Cisco 12000 Series Internet Routers.
4. Isto se refere aos conjuntos Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) e Frame Relay Traffic Policing (FRTP).
5. A fase II da proteção do caminho de recepção permitirá a criação de uma interface de gerenciamento, limitando automaticamente qual endereço IP ouvirá os pacotes de entrada.

Informações Relacionadas

- Página de Suporte das Listas de Acesso
- Suporte Técnico - Cisco Systems