Protegendo sua base: Listas de controle de acesso de proteção de infraestrutura

Contents

Introduction

Este documento apresenta diretrizes e técnicas de implantação recomendadas para ACLs (Listas de controle de acesso) de proteção de infra-estrutura. As ACLs de infraestrutura são usadas para minimizar o risco e a eficácia do ataque direto da infraestrutura, explicitamente permitindo somente o tráfego autorizado ao equipamento de infraestrutura ao passo que permite todos outros tráfegos de trânsito.

Proteção da infraestrutura

Background

Em um esforço para proteger os roteadores de vários riscos, acidentais e mal-intencionados, as ACLs de proteção de infraestrutura devem ser implantadas nos pontos de entrada da rede. Essas ACLs IPv4 e IPv6 negam o acesso de fontes externas a todos os endereços de infraestrutura, como interfaces de roteador. Ao mesmo tempo, as ACLs permitem que o tráfego de trânsito de rotina flua ininterruptamente e fornecem filtragem básica RFC 1918 , RFC 3330 e anti-spoof.

Os dados recebidos por um roteador podem ser divididos em duas grandes categorias:

- tráfego que passa pelo roteador através do caminho de encaminhamento
- tráfego destinado ao roteador através do caminho de recebimento para tratamento do processador de rota

Em operações normais, a grande maioria do tráfego simplesmente flui através de um roteador em rota até seu destino final.

No entanto, o RP (Route Processor) deve lidar diretamente com certos tipos de dados, principalmente protocolos de roteamento, acesso remoto ao roteador (como Secure Shell [SSH]) e tráfego de gerenciamento de rede, como o SNMP (Simple Network Management Protocol). Além disso, protocolos como o Internet Control Message Protocol (ICMP) e as opções de IP podem exigir processamento direto pelo RP. Na maioria das vezes, o acesso direto ao roteador de infraestrutura é necessário apenas de fontes internas. Algumas exceções notáveis incluem peering de Protocolo de Gateway de Borda (BGP - Border Gateway Protocol) externo, protocolos que terminam no roteador real (como encapsulamento de roteamento genérico [GRE - Generic Routing Encapsulation] ou túneis IPv6 sobre IPv4) e pacotes ICMP potencialmente limitados para testes de conectividade, como solicitação de eco ou mensagens ICMP inalcançáveis e tempo de vida expirado (TTL - Time to) para traceroute.

Observação: lembre-se de que o ICMP é frequentemente usado para ataques simples de negação de serviço (DoS) e deve ser permitido somente de fontes externas, se necessário.

Todos os RPs têm um envelope de desempenho no qual operam. O tráfego excessivo destinado ao RP pode sobrecarregar o roteador. Isso causa alto uso da CPU e, por fim, resulta em descartes de pacotes e protocolos de roteamento que causam uma negação de serviço. Ao filtrar o acesso a roteadores de infraestrutura de fontes externas, muitos dos riscos externos associados a um ataque direto de roteador são atenuados. Os ataques de origem externa não podem mais acessar equipamentos de infraestrutura. O ataque é descartado em interfaces de entrada no sistema autônomo (AS).

As técnicas de filtragem descritas neste documento foram projetadas para filtrar dados destinados ao equipamento da infra-estrutura de rede. Não confunda filtragem de infraestrutura com filtragem genérica. A finalidade singular da ACL de proteção de infraestrutura é restringir em um nível granular quais protocolos e fontes podem acessar equipamentos de infraestrutura críticos.

O equipamento de infraestrutura de rede abrange estas áreas:

- Todos os endereços de gerenciamento de roteador e switch, incluindo interfaces de loopback
- Todos os endereços de link internos: links de roteador a roteador (ponto a ponto e acesso múltiplo)
- Servidores ou serviços internos que não devem ser acessados de fontes externas

Neste documento, todo o tráfego não destinado à infraestrutura é frequentemente chamado de tráfego de trânsito.

Técnicas

A proteção da infraestrutura pode ser obtida através de uma variedade de técnicas:

- **ACLs de recepção (rACLs)**As plataformas Cisco 12000 e 7500 suportam rACLs que filtram todo o tráfego destinado ao RP e não afetam o tráfego de trânsito. O tráfego autorizado deve ser explicitamente permitido e o rACL deve ser implantado em cada roteador. Consulte GSR: Receber Listas de Controle de Acesso para obter mais informações.
- **ACLs de roteador salto por salto**Os roteadores também podem ser protegidos definindo ACLs que permitem somente tráfego autorizado para as interfaces do roteador, negando todos os outros, exceto o tráfego de trânsito, que deve ser explicitamente permitido. Essa ACL é

logicamente semelhante a uma rACL, mas afeta o tráfego de trânsito e, portanto, pode ter um impacto negativo no desempenho na taxa de encaminhamento de um roteador.

- **Filtragem de borda via ACLs de infraestrutura**As ACLs podem ser aplicadas à borda da rede. No caso de um provedor de serviços (SP), essa é a borda do AS. Essa ACL filtra explicitamente o tráfego destinado ao espaço de endereço da infraestrutura. A implantação de ACLs de infraestrutura de borda exige que você defina claramente o espaço da infraestrutura e os protocolos necessários/autorizados que acessam esse espaço. A ACL é aplicada na entrada da sua rede em todas as conexões externas, como conexões de peering, conexões com o cliente e assim por diante.Este documento enfoca o desenvolvimento e a implementação de ACLs de proteção de borda.

Exemplos de ACL

Essas listas de acesso IPv4 e IPv6 fornecem exemplos simples, mas realistas, de entradas típicas necessárias em uma ACL de proteção. Essas ACLs básicas precisam ser personalizadas com detalhes de configuração específicos do local. Em ambientes duplos IPv4 e IPv6, ambas as listas de acesso são implantadas.

Exemplo de IPv4

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

Exemplo de IPv6

A Lista de acesso IPv6 deve ser aplicada como uma lista de acesso nomeada estendida.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6 any any
```

Observação: a palavra-chave **log** pode ser usada para fornecer detalhes adicionais sobre origem e destinos para um determinado protocolo. Embora essa palavra-chave forneça informações valiosas sobre os detalhes dos acertos da ACL, acertos excessivos em uma entrada da ACL que usa a palavra-chave **log** aumenta a utilização da CPU. O impacto de desempenho associado ao registro varia por plataforma. Além disso, usar a palavra-chave log desativa a comutação do Cisco Express Forwarding (CEF) para pacotes que correspondem à instrução da lista de acesso. Esses pacotes são comutados rapidamente.

Desenvolver uma ACL de proteção

Em geral, uma ACL de infraestrutura é composta de quatro seções:

- Endereço de uso especial e entradas anti-falsificação que recusam a entrada de fontes ilegítimas e pacotes com endereços de origem pertencentes a seu AS no AS de uma fonte externa.**Observação:** o RFC 3330 define endereços de uso especial do IPv4 que podem exigir filtragem. O RFC 1918 define o espaço reservado de endereço IPv4 que não é um endereço de origem válido na Internet. O RFC 3513 define a arquitetura de endereçamento IPv6. O RFC 2827 fornece diretrizes de filtragem de ingresso.
- Tráfego originado externamente explicitamente permitido destinado a endereços de infraestrutura
- **recusa as declarações de todos os outros tráfegos de origem externa para endereços de infra-estrutura**
- instruções **permit** para todo o tráfego restante para tráfego normal de backbone em rota para destinos que não sejam de infraestrutura

A linha final na ACL de infraestrutura permite explicitamente o tráfego de trânsito: **permit ip any any for IPv4 e permit ipv6 any any for IPv6.** Esta entrada garante que todos os protocolos IP sejam permitidos por meio do centro e que os clientes possam continuar a executar os aplicativos sem problemas.

A primeira etapa ao desenvolver uma ACL de proteção de infraestrutura é entender os protocolos necessários. Embora cada local tenha requisitos específicos, certos protocolos são normalmente implantados e devem ser compreendidos. Por exemplo, o BGP externo para peers externos precisa ser explicitamente permitido. Qualquer outro protocolo que exija acesso direto ao roteador de infraestrutura também precisa ser explicitamente permitido. Por exemplo, se você terminar um túnel GRE em um roteador de infraestrutura central, o protocolo 47 (GRE) também precisará ser explicitamente permitido. Da mesma forma, se você terminar um túnel IPv6 sobre IPv4 em um roteador de infraestrutura central, o protocolo 41 (IPv6 sobre IPv4) também precisará ser explicitamente permitido.

Uma ACL de classificação pode ser usada para ajudar a identificar os protocolos necessários. A ACL de classificação é composta de instruções **permit** para os vários protocolos que podem ser destinados a um roteador de infraestrutura. Consulte o apêndice sobre protocolos IP suportados no Cisco IOS® Software para obter uma lista completa. O uso do comando **show access-list** para exibir uma contagem de acertos de entrada de controle de acesso (ACE) identifica os protocolos necessários. Os resultados suspeitos ou surpreendentes devem ser investigados e compreendidos antes de você criar instruções **permit** para protocolos inesperados.

Por exemplo, essa ACL IPv4 ajuda a determinar se o GRE, o IPsec (ESP) e o tunelamento IPv6 (IP Protocol 41) precisam ser permitidos.

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any
```

```
interface <int>
 ip access-group 101 in
```

Essa ACL IPv6 pode ser usada para determinar se o GRE e o IPsec (ESP) precisam ser permitidos.

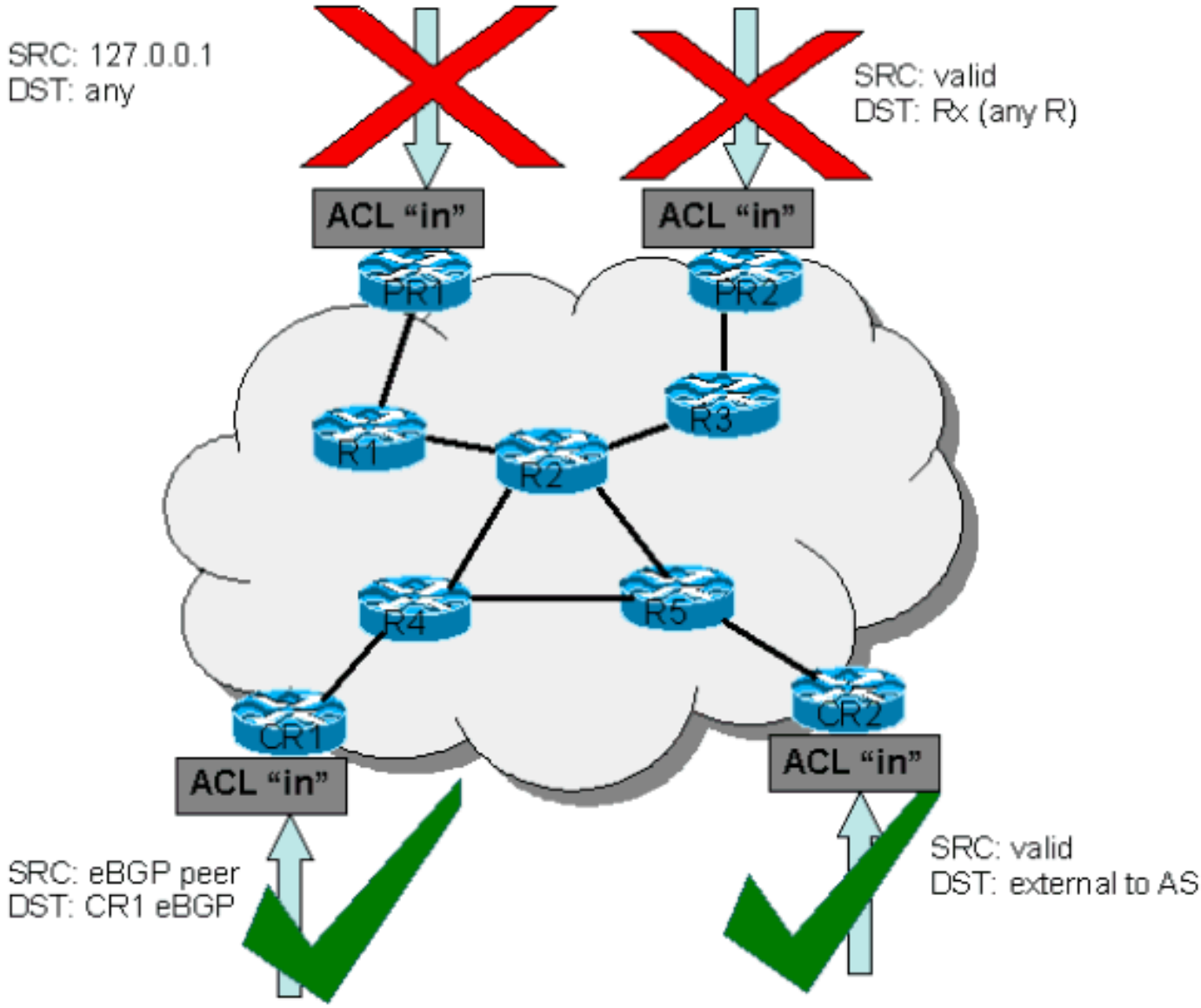
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

Além dos protocolos necessários, o espaço de endereço da infraestrutura precisa ser identificado, pois esse é o espaço que a ACL protege. O espaço de endereço de infraestrutura inclui todos os endereços usados para a rede interna e raramente acessados por fontes externas, como interfaces de roteador, endereçamento de link ponto-a-ponto e serviços de infraestrutura crítica. Como esses endereços são usados para a parte de destino da ACL de infraestrutura, a sumarização é essencial. Sempre que possível, esses endereços devem ser agrupados em blocos de roteamento entre domínios sem classe (CIDR).

Com o uso dos protocolos e endereços identificados, a ACL de infraestrutura pode ser criada para permitir os protocolos e proteger os endereços. Além da proteção direta, a ACL também fornece uma primeira linha de defesa contra certos tipos de tráfego inválido na Internet.

- O espaço RFC 1918 deve ser negado.
- Os pacotes com um endereço de origem que se enquadram no espaço de endereço de uso especial, como definido na RFC 3330, devem ser negados.
- Os filtros anti-falsificação devem ser aplicados. (O espaço de endereço nunca deve ser a origem dos pacotes de fora do AS.)

Essa ACL recém-construída deve ser aplicada na entrada em todas as interfaces de entrada. Consulte as seções sobre diretrizes de implantação e exemplos de implantação para obter mais detalhes.



ACLs e pacotes fragmentados

As ACLs têm uma palavra-chave **fragments** que permite um comportamento especializado de manipulação de pacotes fragmentados. Sem essa palavra-chave **fragments**, os fragmentos não iniciais que correspondem às instruções da Camada 3 (independentemente das informações da Camada 4) em uma ACL são afetados pela instrução permit ou deny da entrada correspondente. No entanto, adicionando a palavra-chave **fragments**, você pode forçar as ACLs a negar ou permitir fragmentos não iniciais com mais granularidade. Esse comportamento é o mesmo para as listas de acesso IPv4 e IPv6, com a exceção de que, enquanto as ACLs IPv4 permitem o uso da palavra-chave fragments nas instruções das Camadas 3 e 4, as ACLs IPv6 permitem somente o uso da palavra-chave fragments nas instruções da Camada 3.

A filtragem de fragmentos adiciona uma camada adicional de proteção contra um ataque de negação de serviço (DoS) que usa fragmentos não iniciais (isto é, FO > 0). O uso de uma instrução deny para fragmentos não-iniciais no começo do ACL 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 na ACL.

Por exemplo, considere esta ACL IPv4parcial:

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

A adição dessas entradas ao início de uma ACL nega qualquer acesso de fragmento não inicial aos roteadores centrais, enquanto pacotes não fragmentados ou fragmentos iniciais passam para as próximas linhas da ACL não afetadas pelas instruções **deny fragment**. O comando anterior da ACL também facilita a classificação do ataque, pois cada protocolo—Universal Datagram Protocol (UDP), TCP e ICMP—incrementa contadores separados na ACL.

Este é um exemplo comparável para IPv6:

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

A adição dessa entrada ao início de uma ACL IPv6 nega qualquer acesso de fragmento não inicial aos roteadores centrais. Como observado anteriormente, as listas de acesso IPv6 permitem somente o uso da palavra-chave fragments nas instruções da Camada 3.

Como muitos ataques dependem da inundação de roteadores centrais com pacotes fragmentados, a filtragem de fragmentos recebidos pela infra-estrutura central fornece uma medida adicional de proteção e ajuda a assegurar que um ataque não possa injetar fragmentos simplesmente com a correspondência de regras da camada 3 no ACL de infra-estrutura.

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

Avaliação de risco

Considere estas duas áreas de risco chave ao implantar ACLs de proteção de infraestrutura:

- Certifique-se de que as instruções **permit**/**deny** apropriadas estejam em vigor. Para que a ACL seja eficaz, todos os protocolos necessários devem ser permitidos e o espaço de endereço correto deve ser protegido pelas instruções **deny**.
- O desempenho da ACL varia de plataforma para plataforma. Revise as características de desempenho do seu hardware antes de implantar ACLs.

Como sempre, recomenda-se que você teste este projeto no laboratório antes da implantação.

Apêndices

Protocolos IP suportados pelo Cisco IOS Software

Esses protocolos IP são suportados pelo software Cisco IOS:

- 1 - ICMP
- 2 - IGMP
- 3 - GGP

- 4 - IP no encapsulamento IP
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv6 em tunelamento IPv4
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 - SWIPE
- 54 - NARP
- 55 - Mobilidade IP
- 63 - qualquer rede local
- 77 - Dom
- 80 - IP ISO
- 88 - EIGRP
- 89 - OSPF
- 90 - RPC Sprite
- 91 - LARP
- 94 - KA9Q/NOS compatível IP sobre IP
- 103 - PIM
- 108 - compactação IP
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - ITU
- 132 - SCTP

Diretrizes de implantação

A Cisco recomenda práticas conservadoras de implantação. Para implantar com êxito ACLs de infraestrutura, os protocolos necessários devem ser bem compreendidos e o espaço de endereço deve ser claramente identificado e definido. Essas diretrizes descrevem um método muito conservador para implantar ACLs de proteção usando uma abordagem iterativa.

1. **Identificar os protocolos usados na rede com uma ACL de classificação.**Implante uma ACL que permita todos os protocolos conhecidos que acessam dispositivos de infraestrutura. Essa ACL de descoberta tem um endereço de origem de **qualquer** destino que abrange o espaço IP da infraestrutura. O registro pode ser usado para desenvolver uma lista de endereços de origem que correspondem às instruções **permit** do protocolo. Uma última linha permitindo **ip any any** (IPv4) ou **ipv6 any any any** (IPv6) é necessária para permitir o fluxo de tráfego.O objetivo é determinar quais protocolos a rede específica utiliza. O registro é 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. Além disso, usar a palavra-chave **log** desativa a comutação do Cisco Express Forwarding (CEF) para pacotes que correspondem à instrução da lista de acesso. Esses pacotes são comutados rapidamente. Use a palavra-chave log para pequenos períodos de tempo e somente quando necessário para ajudar a classificar o tráfego.

2. **Reveja os pacotes identificados e comece a filtrar o acesso ao RP do processador de rotas.**Quando os pacotes filtrados pelo ACL no passo 1 forem identificados e analisados, distribua um ACL com uma permissão de qualquer origem para endereços de infra-estrutura 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**. A opção de recusar todos no final pode auxiliar na identificação de pacotes não esperados destinados aos roteadores. A última linha desta ACL deve ser uma **instrução permit ip any any** (IPv4) ou **permit ipv6 any any any** (IPv6) para permitir o fluxo de tráfego de trânsito. Essa ACL fornece proteção básica e permite que os engenheiros de rede assegurem que todo o tráfego necessário seja permitido.
3. **Restrinja os endereços de origem.**Depois de entender claramente os protocolos que devem ser permitidos, será possível realizar uma filtragem adicional para permitir apenas as fontes autorizadas para esses protocolos. Por exemplo, você pode permitir explicitamente vizinhos BGP externos ou endereços específicos de peer GRE.Essa etapa reduz o risco sem interromper serviços e permite aplicar o controle granular a fontes que acessam o equipamento de infra-estrutura.
4. **Limite os endereços de destino na ACL. (opcional)**Alguns provedores de serviços de Internet (ISP) podem optar por permitir apenas protocolos específicos para usar endereços de destino específicos no roteador. Essa fase final tem como objetivo limitar o intervalo de endereços de destino que podem aceitar tráfego para um protocolo.

Exemplos de implantação

Exemplo de IPv4

Este exemplo de IPv4 mostra uma ACL de infraestrutura protegendo um roteador com base neste endereçamento:

- O bloco de endereços 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 peer e faz o peer com 169.254.254.1 (para o endereço 169.223.252.1).

A ACL de proteção de infraestrutura exibida é desenvolvida com base nas informações anteriores. A ACL permite o peering de BGP externo para o peer externo, fornece filtros anti-spoof e protege a infraestrutura de todo o acesso externo.

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).
```

```
!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

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

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

Exemplo de IPv6

Este exemplo de IPv6 mostra uma ACL de infraestrutura protegendo um roteador com base neste endereçamento:

- O bloco de prefixo geral alocado ao ISP é 2001:0DB8::/32.
- O bloco de prefixo IPv6 usado pelo ISP para endereços de infraestrutura de rede é 2001:0DB8:C18::/48.
- Há um roteador de peering BGP com um endereço IPv6 origem 2001:0DB8:C18:2:1::1 que corresponde ao endereço IPv6 destino 2001:0DB8:C19:2:1::F.

A ACL de proteção de infraestrutura exibida é desenvolvida com base nas informações anteriores. A ACL permite o peering de BGP multiprotocolo externo para o peer externo, fornece filtros anti-spoof e protege a infraestrutura de todo o acesso externo.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 -
```

```
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 - Explicit Permit for
Transit Traffic permit ipv6 any any
```

Informações Relacionadas

- Página de Suporte das Listas de Acesso
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems