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

Índice

Introdução

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 de infraestrutura

Background

Em um esforço para proteger o Roteadores dos vários riscos — acidental e malicioso — a proteção de infraestrutura ACL deve ser distribuída em pontos de ingresso de rede. Este IPv4 e o IPv6 ACL negam o acesso dos origens externa a todos os endereços da infraestrutura, tais como interfaces do roteador. Ao mesmo tempo, o tráfego de trânsito do ACLs permitem que o tráfego de rotina a fluir ininterrupto e fornecer o RFC 1918 básico , o RFC 3330 , e o filtragem anti-falsificação.

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

- trafique que passagens através do roteador através do trajeto de encaminhamento
- tráfego destinado para o roteador através do trajeto da recepção para a manipulação do

processador de rotas

Nas operações normal, a grande maioria do tráfego corre através simplesmente de um roteador a caminho a seu destino final.

Contudo, o route processor (RP) deve segurar determinados tipos de dados diretamente, especialmente protocolos de roteamento, acesso do roteador remoto (tal como o [SSH] do Secure Shell), e tráfego de gerenciamento de rede tal como o Simple Network Management Protocol (SNMP). Além, os protocolos tais como o Internet Control Message Protocol (ICMP) e as opções IP podem exigir o processamento direto pelo RP. O mais frequentemente, o acesso direto do roteador de infraestrutura é exigido somente dos origens interna. Algumas exceções notável incluem o Protocolo de Gateway Limite externo (eBGP) (BGP) que espreita, os protocolos que terminam no roteador real (tal como o [GRE] ou o IPv6 do encapsulamento de roteamento genérico sobre túneis do IPv4), e pacotes ICMP potencialmente limitados para testes da Conectividade tais como a requisição de eco ou os ICMP não alcançável e o Time to Live (TTL) expiraram mensagens para o traceroute.

Nota: Recorde que o ICMP é usado frequentemente para o ataque de recusa de serviço (DOS) simples e deve somente ser permitido dos origens externa caso necessário.

Todos os RP têm um envelope de desempenho em que se operam. O tráfego excessivo destinado para o RP pode oprimir o roteador. Isto causa o uso da alta utilização da CPU e conduz finalmente ao pacote e às gotas do protocolo de roteamento que causam uma recusa de serviço. Filtrando o acesso aos roteadores de infraestrutura dos origens externa, muitos dos riscos externos associados com um ataque direto do roteador são abrandados. Os ataques externamente originado enlatam já não o equipamento da infraestrutura de acesso. O ataque é deixado cair em interfaces de ingresso no sistema autônomo.

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

O equipamento da infraestrutura de rede abrange estas áreas:

- Todos os endereços do roteador e do gerenciamento de switch, incluindo interfaces de loopback
- Todos os endereços de link internos: o roteador para roteador liga (ponto a ponto e o acesso múltiplo)
- Servidores internos ou serviços que não devem ser alcançados dos origens externa

Neste documento, todo o tráfego não destinado para a infraestrutura é referido frequentemente como o tráfego de trânsito.

Técnicas

A proteção de infraestrutura pode ser conseguida com uma variedade de técnicas:

- **Receba ACL (o rACLs)**Cisco 12000 e 7500 rACLs do apoio de Plataformas que filtram todo o tráfego destinado ao RP e não afetam o tráfego de trânsito. O tráfego autorizado deve explicitamente ser permitido e o rACL deve ser distribuído em cada roteador. Consulte GSR: Receba listas de controle de acesso para mais informação.
- **ACLs de roteador do salto a salto**O Roteadores pode igualmente ser protegido definindo os

ACL que permitem somente o tráfego autorizado às relações do roteador, negando todos os outro à exceção do tráfego de trânsito, que deve explicitamente ser permitido. Este ACL é logicamente similar a um rACL mas afeta o tráfego de trânsito, e pode consequentemente ter um impacto no desempenho negativo na taxa de encaminhamento de um roteador.

- **Filtragem de ponta através da infraestrutura ACL**Os ACL podem ser aplicados à borda da rede. No caso de um provedor de serviços (SP), esta é a borda do COMO. Este ACL filtra explicitamente o tráfego destinado para o espaço de endereços da infraestrutura. A distribuição de infraestrutura ACL exige que você define claramente seus espaço da infraestrutura e protocolos exigidos/autorizados que alcançam este espaço. O ACL é aplicado no ingresso a sua rede em todas as conexões externas, tais como conexões espreitando, conexões de cliente, e assim por diante.Este documento enfoca o desenvolvimento e a implementação de ACLs de proteção de borda.

Exemplos de ACL

As Listas de acesso TheseIPv4 e de IPv6 fornecem simples contudo exemplos realistas das entradas típicas exigidas em uma proteção ACL. Estes ACL básicos precisam de ser personalizados com detalhes de configuração locais do específico de site. Em ambientes duplos do IPv4 e do IPv6, ambas as listas de acesso são distribuídas.

Exemplo do 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 do IPv6

A lista de acesso do IPv6 deve ser aplicada como um prolongado, lista de acesso nomeada.

```
!--- 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
```

Nota: A palavra-chave log pode ser utilizada para fornecer detalhes adicionais sobre a origem e os destinos de um protocolo específico. Embora esta palavra-chave forneça o insight valioso nos detalhes de batidas ACL, as batidas excessivas a uma entrada ACL que use a palavra-chave do **log** aumentam a utilização CPU. O impacto de desempenho associado ao registro varia por plataforma. Também, usar a palavra-chave do log desabilita o switching do Cisco Express Forwarding (CEF) para os pacotes que combinam a instrução de lista de acesso. Esses pacotes são comutados rapidamente.

Desenvolva uma proteção ACL

Geralmente, uma infraestrutura ACL 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.**Nota:** O RFC 3330 define os endereços de uso especial 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 do filtragem de ingresso.
- O tráfego externamente originado explicitamente permitido destinou aos endereços da infraestrutura
- recusa as declarações de todos os outros tráfegos de origem externa para endereços de infra-estrutura
- **permita** indicações para todo tráfego restante para o tráfego de backbone normal a caminho aos destinos do noninfrastructure

A linha final na infraestrutura ACL 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 quando você desenvolve uma proteção de infraestrutura ACL é compreender os protocolos exigidos. Embora cada local tenha exigências específicas, determinados protocolos geralmente são distribuídos e devem ser compreendidos. Por exemplo, o BGP externo aos peer externos precisa de ser permitido explicitamente. Alguns outros protocolos que exigirem de acesso direto à necessidade do roteador de infraestrutura de ser permitido explicitamente também. Por exemplo, se você termina um túnel GRE em um roteador da infraestrutura de centro, a seguir necessidades do protocolo 47 (GRE) também de ser permitido explicitamente. Similarmente, se você termina um IPv6 sobre o túnel do IPv4 em um roteador da infraestrutura de centro, a seguir necessidades do protocolo 41 (IPv6 sobre o IPv4) também de ser permitido explicitamente.

Uma classificação ACL pode ser usada para ajudar a identificar os protocolos exigidos. A classificação ACL é composta de indicações da **licença** para os vários protocolos que podem ser destinados para um roteador de infraestrutura. Refira o apêndice em protocolos IP apoiados no software de Cisco IOS® para uma lista completa. O uso do comando do **comando show access-list** indicar uma contagem de batidas da entrada de controle de acesso (ACE) identifica protocolos exigidos. Os resultados suspeitos ou surpreendentes devem ser investigados e compreendido antes que você crie indicações da **licença** para protocolos inesperados.

Por exemplo, este as ajudas do IPv4 ACL determinam se GRE, IPsec (ESP) e IPv6 que escava um túnel (protocolo IP 41) a necessidade de ser permitido.

```
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
```

Este IPv6 ACL pode ser usado para determinar se o GRE e o IPsec (ESP) precisam de 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 do que protocolos exigidos, o espaço de endereços da infraestrutura precisa de ser identificado desde que este é o espaço que o ACL protege. O espaço de endereços da infraestrutura inclui todos os endereços que forem usados para a rede interna e alcançados raramente por origens externa tais como interfaces do roteador, endereçamento de link de ponto a ponto, e serviços da infraestrutura crítica. Desde que estes endereços são usados para a parte de destino da infraestrutura ACL, a sumarização é crítica. Na medida do possível, estes endereços devem ser agrupados em blocos do Classless Interdomain Routing (CIDR).

Com o uso dos protocolos e dos endereços identificados, a infraestrutura ACL pode ser construída para permitir os protocolos e para proteger os endereços. Além do que a proteção direta, o ACL igualmente fornece uma primeira linha de defesa contra determinados tipos de tráfego inválido no Internet.

- O espaço do RFC 1918 deve ser negado.
- Os pacotes com um endereço de origem que caem sob o espaço de endereços do especial-uso, como definido no RFC 3330, devem ser negados.
- os filtros do Anti-spoof devem ser aplicados. (Seu espaço de endereços deve nunca ser o origem de pacotes da parte externa sua COMO.)

Este ACL recentemente construído deve ser de entrada aplicado em todas as interfaces de ingresso. Veja as seções em diretrizes de distribuição e em exemplos de distribuição para mais detalhes.

ACL e pacotes fragmentados

Os ACL têm uma palavra-chave dos **fragmentos** que permita o comportamento fragmentado especializado do manuseio de pacotes. Sem esta palavra-chave dos **fragmentos**, os fragmentos não-iniciais que combinam as indicações da camada 3 (independentemente da informação da camada 4) em um ACL são afetados pela indicação do permit or deny da entrada combinada. Contudo, adicionando os **fragmentos** palavra-chave, você pode forçar ACL a nega ou permite fragmentos não-iniciais com mais granularidade. Este comportamento é o mesmo para listas de acesso do IPv4 e do IPv6, com exceção, quando o IPv4 ACL permitir o uso da palavra-chave dos fragmentos dentro das indicações da camada 3 e da camada 4, o IPv6 ACL permite somente o uso da palavra-chave dos fragmentos dentro das indicações da camada 3.

Filtrar fragmentos adiciona uma camada adicional de proteção contra um ataque de recusa de serviço (DOS) que use 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. Sob circunstâncias raras, uma sessão válida pôde exigir a fragmentação, e consequentemente seja filtrada se uma indicação do **fragmento da negação** existe no ACL.

Por exemplo, considere este IPv4ACL parcial:

```
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 destas entradas ao começo de um ACL nega todo o acesso não-inicial do fragmento aos

roteadores centrais, quando os pacotes não fragmentados ou os fragmentos iniciais passarem às linhas seguintes do ACL não afetado pelas indicações do **fragmento da negação**. O comando acl precedente igualmente facilita a classificação do ataque desde cada protocolo — o protocolo de datagrama universal (UDP), o TCP, e o ICMP — incrementos separa contadores no ACL.

Este é um exemplo comparável para o IPv6:

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

A adição desta entrada ao começo de um IPv6 ACL nega todo o acesso não-inicial do fragmento aos roteadores centrais. Como notável previamente, as listas de acesso do IPv6 permitem somente o uso da palavra-chave dos fragmentos dentro das indicações 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.

Refira listas de controle de acesso e fragmentos IP para uma discussão detalhada das opções.

Avaliação de risco

Considere estas duas áreas do risco chave quando você distribui a proteção de infraestrutura ACL:

- Assegure-se de que a **licença/instruções de negação** apropriadas esteja no lugar. Para que o ACL seja eficaz, todos os protocolos exigidos devem ser permitidos e o espaço de endereço correto deve ser protegido pelas **instruções de negação**.
- O desempenho do ACL varia da plataforma à plataforma. Reveja as características de desempenho de seu hardware antes que você distribua ACL.

Como sempre, recomenda-se que você testa este projeto no laboratório antes do desenvolvimento.

Apêndices

Protocolos IP suportados pelo Cisco IOS Software

Estes protocolos IP são apoiados pelo Cisco IOS Software:

- 1 – ICMP
- 2 – IGMP
- 3 – GGP
- 4 – Encapsulamento do IP in IP
- 6 – TCP
- 8 – EGP
- 9 – IGRP
- 17 – UDP
- 20 – HMP
- 27 – RDP

- 41 – IPv6 na escavação de um túnel do IPv4
- 46 – RSVP
- 47 – GRE
- 50 pés – ESP
- 51 – AH
- 53 – FURTO
- 54 – NARP
- 55 – Mobilidade IP
- 63 – alguma rede local
- 77 – Sun ND
- 80 – IP ISO
- 88 – EIGRP
- 89 – OSPF
- 90 – Sprite RPC
- 91 – LARP
- 94 – IP compatível KA9Q/NOS sobre o IP
- 103 – PIM
- 108 – Compressão IP
- 112 – VRRP
- 113 – PGM
- 115 – L2TP
- 120 – UTI
- 132 – SCTP

Diretrizes de distribuição

Cisco recomenda práticas conservadoras do desenvolvimento. A fim distribuir com sucesso a infraestrutura ACL, os protocolos exigidos devem bem ser compreendidos, e o espaço de endereços deve claramente ser identificado e definido. Estas diretrizes descrevem muito um método conservador para distribuir a proteção ACL usando uma aproximação iterativa.

1. **Identifique os protocolos usados na rede com uma classificação ACL.**Distribua um ACL que permita todos os protocolos conhecidos dispositivos dessa infraestrutura de acesso. Esta descoberta ACL tem um endereço de origem de **alguns** e de um destino que abranja o espaço IP da infraestrutura. Registrar pode ser usado para desenvolver uma lista de endereços de origem que combinam as instruções de permissão de protocolo. Uma última linha permitindo o **IP algum** (IPv4) ou o **IPv6 algum** (IPv6) é exigida para permitir o fluxo de tráfego.O objetivo é determinar quais protocolos a rede específica utiliza. Registrar é usado para que a análise determine que outro pôde se comunicar com o roteador.**Nota:** Embora a palavra-chave do **log** fornecesse o insight valioso nos detalhes de batidas ACL, as batidas excessivas a uma entrada ACL que usasse esta palavra-chave puderam conduzir a um número opressivamente de entradas de registro e possivelmente de uso alto do CPU de roteador. Também, usar a palavra-chave do **log** desabilita o switching do Cisco Express Forwarding (CEF) para os pacotes que combinam a instrução de 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. Apenas como em etapa 1, a palavra-chave do **log** pode fornecer mais informação sobre os pacotes que combinam as entradas da **licença**. A opção de recusar todos no final pode auxiliar na identificação de pacotes não esperados destinados aos roteadores. A última linha deste ACL deve ser uma **licença IP todo o algum** (IPv4) ou **permitir o IPv6 toda a qualquer** indicação (do IPv6) permitir o fluxo do tráfego de trânsito. Este ACL fornece a proteção básica e permite que os engenheiros de rede assegurem-se de que todo o tráfego exigido esteja permitido.

3. **Restrinja 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 explicitamente permitir vizinhos do BGP externo ou endereços de peer específicos 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 no ACL. (*opcional*)**Alguns provedores de serviço do Internet (ISP) puderam escolher permitir somente que os protocolos específicos usem endereços de destino específicos no roteador. Esta fase final é significada limitar a escala dos endereços de destino que podem aceitar o tráfego para um protocolo.

Exemplos de distribuição

Exemplo do IPv4

Este exemplo do IPv4 mostra uma infraestrutura ACL que protege um roteador baseado neste endereçamento:

- O bloco de endereço ISP é 169.223.0.0/16.
- O bloco da infraestrutura 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 proteção de infraestrutura ACL indicada é desenvolvida com base na informação precedente. O ACL permite o BGP externo que espreita ao peer externo, fornece filtros do 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 do IPv6

Este exemplo do IPv6 mostra uma infraestrutura ACL que protege um roteador baseado neste endereçamento:

- O bloco total do prefixo atribuído ao ISP é 2001:0DB8::/32.
- O bloco do prefixo do IPv6 usado pelo ISP para endereços da infraestrutura de rede é 2001:0DB8:C18::/48.
- Há um roteador peering BGP com um endereço do IPv6 da fonte de 2001:0DB8:C18:2:1::1 que espreita ao endereço do IPv6 do destino de 2001:0DB8:C19:2:1::F.

A proteção de infraestrutura ACL indicada é desenvolvida com base na informação precedente. O ACL permite o Multiprotocol BGP externo que espreita ao peer externo, fornece filtros do 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