Listas de controle de acesso de trânsito: Filtração em sua borda

Índice

Introdução

Este documento apresenta diretrizes e recomenda técnicas de implantação para a filtragem de trânsito e tráfego de borda nos pontos de entrada da rede. Listas de controle de acesso (ACLs) de trânsito são utilizadas para aumentar a segurança da rede permitindo explicitamente apenas o tráfego necessário na(s) rede(s).

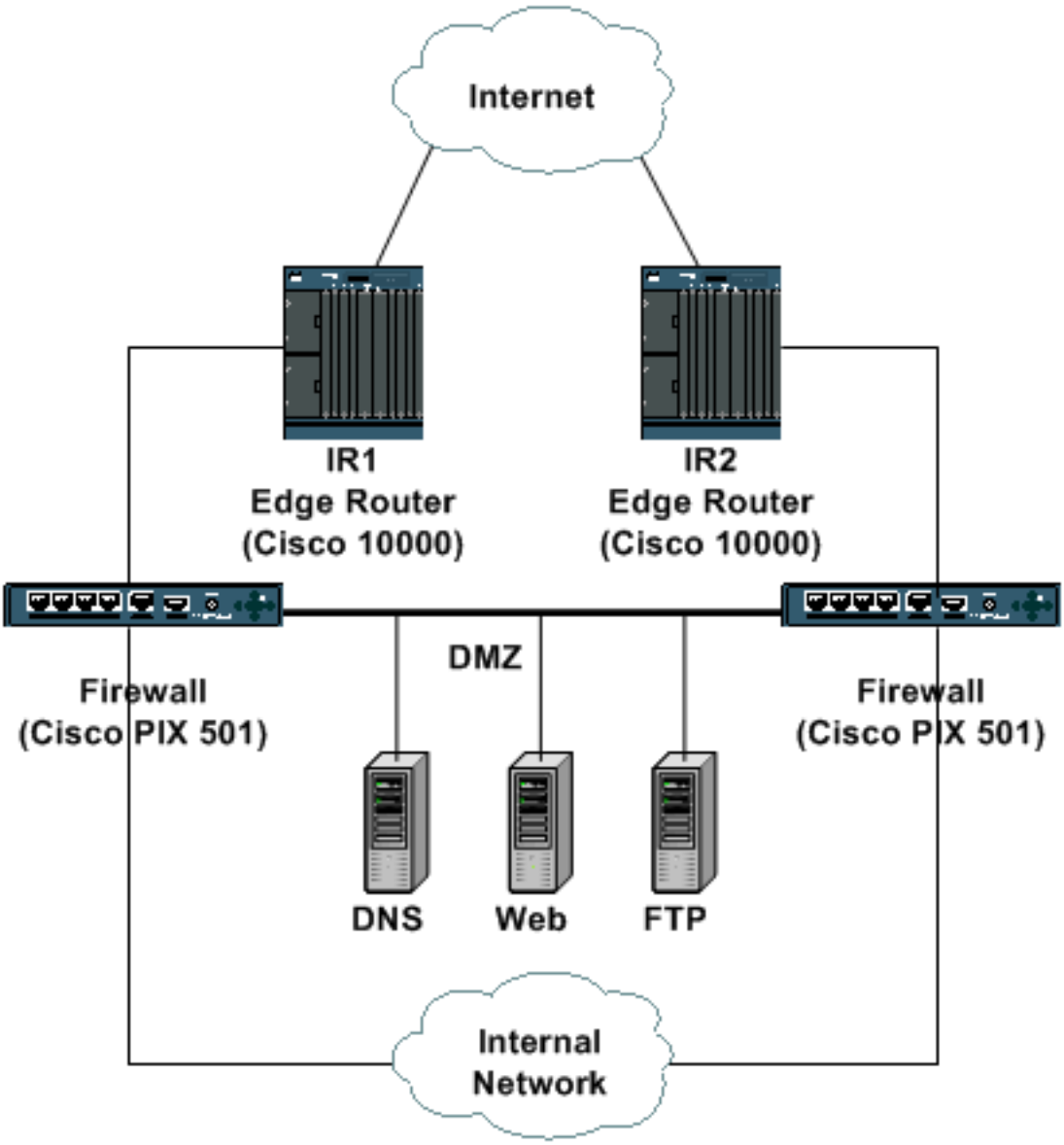
Filtros de trânsito

Configuração típica

Na maioria de ambientes de rede de ponta, tais como um Point of Presence dos internet de rede da empresa típica, o filtragem de ingresso deve ser usado para deixar cair tráfego desautorizado na borda da rede. Em determinadas disposições do provedor de serviços, este formulário da filtração da borda ou do tráfego de trânsito pode igualmente ser usado eficazmente para limitar o fluxo do tráfego de trânsito a e dos clientes aos protocolos permitidos específico somente. Este documento enfoca um modelo de implementação empresarial.

Este exemplo descreve um projeto da conectividade de Internet da empresa típica. Dois roteadores de ponta, IR1 e IR2, fornecem a conectividade direta ao Internet. Atrás deste dois

Roteadores, um par dos Firewall (PIXes de Cisco neste exemplo) fornece capacidades e acesso da inspeção stateful à rede interna e à zona desmilitarizada (DMZ). O DMZ contém serviços do público-revestimento tais como o DNS e a Web; esta é a única rede acessível diretamente dos Internet públicas. A rede interna nunca deve ser acessada diretamente pela Internet, mas o tráfego originado na rede interna deve ter capacidade para alcançar sites da Internet.



Os roteadores de extremidade devem ser configurados de forma a oferecerem primeiro nível de segurança por meio do uso de ACLs de entrada. Os ACL permitem somente especificamente o tráfego permitido ao DMZ e permitem o tráfego de retorno para os usuários internos que alcançam o Internet. Todo o tráfego nonauthorized deve ser deixado cair nas interfaces de ingresso.

Seções ACL de transição

Geralmente, um trânsito ACL é composto de quatro seções.

- Endereço de uso especial e entradas anti-falsificação que não permitem que fontes ilegítimas e pacotes com endereços de origem que pertençam à sua rede entrem na rede a partir de uma fonte externa**Nota:** O RFC 1918 define o espaço de endereço reservado que não é um endereço de origem válido na Internet. O RFC 3330 define endereços de uso especial que

possam requerer uma filtragem. O RFC 2827 fornece diretrizes anti-falsificação.
- Tráfego de retorno explicitamente permitido para conexões internas ao Internet
- Tráfego externamente originado explicitamente permitido destinado aos endereços internos protegidos
- **Instrução de negação** explícita**Nota:** Embora todos os ACL contenham uma **instrução de negação** implícita, Cisco recomenda o uso de uma **instrução de negação** explícita, por exemplo, **deny ip any any**. Na maioria das plataforma, essas instruções mantém uma contagem do número de pacotes negados que pode ser exibida usando o comando show access-list.

Como desenvolver um trânsito ACL

A primeira etapa no desenvolvimento de um trânsito ACL é determinar os protocolos exigidos dentro de suas redes. Embora cada local tenha exigências específicas, os determinados protocolos e aplicativos são amplamente utilizados e são permitidos o mais frequentemente. Por exemplo, se o segmento DMZ fornece a Conectividade para um servidor de Web publicamente acessível, o TCP do Internet ao endereço do servidor DMZ na porta 80 é exigido. Similarmente, as conexões internas ao Internet exigem que o retorno da licença ACL estabeleceu o tráfego TCP – trafique que tem o jogo do bit do reconhecimento (ACK).

Identifique protocolos exigidos

O desenvolvimento desta lista de protocolos exigidos pode ser umas tarefas de afastamento, mas há diversas técnicas que podem ser usadas, como necessário, a fim ajudar a identificar o tráfego exigido.

- **Revise sua política de segurança local/política de serviço.**A política do site local deve ajudar a fornecer uma linha de base de serviços permitidos e negados.
- **Revise e faça uma auditoria na configuração do seu firewall.**A configuração de firewall atual deve conter indicações explícitas da **licença** para serviços permitidos. Em muitos casos, você pode traduzir esta configuração ao formato ACL e usá-la para criar o volume das entradas ACL.**Nota:** Os firewalls totais geralmente não têm regras explícitas para retornar tráfego às conexões autorizadas. Como ACLs de roteador não são stateful, o tráfego de retorno deve ser explicitamente permitido.
- **Revise/realize auditorias em seus aplicativos.**Os aplicativos hospedados no DMZ e aqueles usados internamente podem ajudar a determinar exigências de filtração. Reveja os requisitos do aplicativo a fim fornecer detalhes essenciais sobre o projeto de filtração.
- **Use uma ACL de classificação.**Uma classificação ACL é composta de indicações da **licença** para os vários protocolos que poderiam ser destinados à rede interna. (Veja o apêndice A para uma lista de protocolos e de aplicativos de uso geral.) Use o **comando show access-list** indicar uma contagem de batidas da entrada de controle de acesso (ACE) para identificar protocolos exigidos. Investigue e compreenda todos os resultados suspeitos ou surpreendentes antes que você crie indicações explícitas da **licença** para protocolos inesperados.
- **Utilize o recurso de switching Netflow.**O Netflow é uns recursos de switching que, se permitidos, forneçam informação de fluxo detalhada. Se o Netflow é permitido em seus roteadores de ponta, o **comando show ip cache flow** dá uma lista de protocolos registrados pelo Netflow. O Netflow não pode identificar todos os protocolos, assim que esta técnica deve

ser usada conjuntamente com outro.

Identifique o tráfego inválido

Além do que a proteção direta, o trânsito ACL deve igualmente fornecer uma primeira linha de defesa contra determinados tipos de tráfego inválido no Internet.

- Negue o espaço do RFC 1918.
- Negue pacotes com um endereço de origem que caia sob o espaço de endereços do especial-uso, como definido no RFC 3330.
- Aplique filtros do anti-spoof, de acordo com o RFC 2827; seu espaço de endereços deve nunca ser o origem de pacotes fora de seu sistema autônomo.

Outros tipos de tráfego a considerar incluem:

- **Protocolos externos e endereços IP de Um ou Mais Servidores Cisco ICM NT que precisam de se comunicar com o roteador de ponta**ICMP dos endereços IP de Um ou Mais Servidores Cisco ICM NT do provedor de serviçosProtocolos de RoteamentoIPSec VPN, se um roteador de ponta é usado como a terminação
- **Tráfego de retorno explicitamente permitido para conexões internas ao Internet**Tipos específicos de Protocolo de Mensagem de Controle da Internet (ICMP)Respostas de partida da pergunta do Domain Name System (DNS)TCP estabelecidoTráfego de retorno do User Datagram Protocol (UDP)Conexões de dados FTPConexões de dados TFTPConexões de multimídia
- **Tráfego externamente originado explicitamente permitido destinado aos endereços internos protegidos**Tráfego de VPNInternet Security Association and Key Management Protocol (ISAKMP)Network Address Translation (NAT) TraversalEncapsulamento de proprietárioEncapsulating Security Payload (ESP)Authentication Header (AH)HTTP aos servidores de WebSecure Socket Layer (SSL) aos servidores de WebFTP aos servidores FTPConexões de dados de entrada FTPConexões de dados do FTP de entrada passivo (**pasv**)SMTP (protocolo simples de transferência de correspondência)Outros aplicativos e serverPerguntas de entrada DNSTransferências de entrada da zona DNS

Aplique o ACL

A ACL recém-construída deve ser aplicada na entrada a interfaces voltadas à Internet dos roteadores de extremidade. No exemplo ilustrado na seção de instalação típica, o ACL isapplied dentro nas relações da face Internet no IR1 e no IR2.

Veja as seções em diretrizes de distribuição e em exemplo de distribuição para mais detalhes.

Exemplo de ACL

Esta lista de acessos fornece um simples contudo o exemplo realista das entradas típicas exigidas em um trânsito ACL. É necessário personalizar esse ACL básico com detalhes de configuração específicos de site local.

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
```

```
for additional special use addresses.

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
access-list 110 deny ip host 255.255.255.255 any
!--- The deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny ip host 0.0.0.0 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 !---
Permit Border Gateway Protocol (BGP) to the edge router. access-list 110 permit tcp host
bgp_peer gt 1023 host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host
router_ip gt 1023 !--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip
your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow specific
ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary DNS
server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list 110
permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries.

access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
 !-- These are zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
secondary DNS server gt 1023 host primary DNS server eq 53 !--- Permit older DNS zone transfers.
access-list 110 permit tcp host secondary DNS server eq 53 host primary DNS server eq 53 !---
Deny all other DNS traffic. access-list 110 deny udp any any eq 53 access-list 110 deny tcp any
any eq 53 !--- Allow IPSec VPN traffic. access-list 110 permit udp any host IPSec headend device
eq 500 access-list 110 permit udp any host IPSec headend device eq 4500 access-list 110 permit
50 any host IPSec headend device access-list 110 permit 51 any host IPSec headend device access-
list 110 deny ip any host IPSec headend device !--- These are Internet-sourced connections to !-
-- publicly accessible servers. access-list 110 permit tcp any host public web server eq 80
access-list 110 permit tcp any host public web server eq 443 access-list 110 permit tcp any host
public FTP server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit
established ACE. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host public FTP server gt 1023 access-list 110 permit tcp
any host public SMTP server eq 25 !--- Explicitly deny all other traffic.

access-list 101 deny ip any any
```

Nota: Mantenha por favor estas sugestões na mente quando você aplica o trânsito ACL.

- A palavra-chave do **log** pode ser usada a fim fornecer o detalhe adicional sobre a fonte e os destinos para um protocolo dado. Embora esta palavra-chave forneça o insight valioso nos detalhes de batidas ACL, batidas excessivas a uma entrada ACL que use a utilização CPU do aumento da palavra-chave do **log**. O impacto de desempenho associado ao registro varia por plataforma.
- Os mensagens que não chega a seu destino do ICMP são gerados para os pacotes que são negados administrativamente por um ACL. Isso poderia causar impacto no roteador e no desempenho do enlace. Considere o uso do **comando no ip unreachables** a fim desabilitar inalcançáveis IP na relação onde o trânsito (borda) ACL é distribuído.

- Este ACL pode inicialmente ser distribuído com todas as indicações da **licença** a fim assegurar-se de que o tráfego legitimado do negócio não esteja negado. Após a identificação e à contabilização do tráfego de negócios legítimo, os elementos específicos de negação podem ser configurados.

ACL e pacotes fragmentados

Os ACL têm uma palavra-chave dos **fragmentos** que permita o comportamento fragmentado especializado do manuseio de pacotes. Geralmente, os fragmentos não-iniciais que combinam as indicações da camada 3 (protocolo, endereço de origem, e endereço de destino) — independentemente da informação da camada 4 em um ACL — são afetados pela indicação do **permit or deny da** entrada combinada. Note que o uso da palavra-chave dos **fragmentos** pode forçar ACL a nega ou permite fragmentos não-iniciais com mais granularidade.

Filtrar fragmentos adiciona uma camada adicional de proteção contra um ataque de recusa de serviço (DOS) que use somente fragmentos não-iniciais (como FO > 0). O uso de uma **instrução de negação** para fragmentos não-iniciais no início do ACL nega todos os fragmentos não-iniciais de alcançar o roteador. Sob circunstâncias raras, uma sessão válida pode exigir a fragmentação e, por isso, ser filtrada se uma declaração negada de fragmento existir no ACL. As circunstâncias que puderam conduzir à fragmentação incluem o uso dos Certificados digitais para a autenticação de ISAKMP e o uso do IPsec NAT Traversal.

Por exemplo, considere o ACL parcial mostrado aqui.

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

Adicionar estas entradas ao começo de um ACL nega todo o acesso não-inicial do fragmento à rede, quando os pacotes não fragmentados ou os fragmentos iniciais passarem às linhas seguintes do ACL não afetado pelas indicações do **fragmento da negação**. O snippet de ACL precedente igualmente facilita a classificação do ataque desde cada protocolo — UDP, TCP, e ICMP — incrementos separa contadores no ACL.

Desde que muitos ataques confiam na inundação com pacotes fragmentados, filtrar fragmentos entrantes à rede interna fornece uma medida adicionada da proteção e as ajudas asseguram-se de que um ataque não possa injetar fragmentos simplesmente combinando regras da camada 3 no trânsito ACL.

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

Avaliação de risco

Quando você distribui a proteção ACL do tráfego de trânsito, considere duas áreas principal do risco.

- Assegure-se de que a **licença/instruções de negação** apropriadas esteja no lugar. Para que o ACL seja eficaz, você deve permitir todos os protocolos exigidos.
- O desempenho do ACL varia da plataforma à plataforma. Antes que você distribua ACL,

reveja as características de desempenho de seu hardware.

Cisco recomenda que você testa este projeto no laboratório antes do desenvolvimento.

Apêndices

Protocolos e aplicativos de uso geral

Nomes de porta TCP

Esta lista de nomes de porta TCP pode ser usada em vez dos números de porta quando você configura o ACL no Cisco IOS ® Software. Refira o RFC do assigned number atual a fim encontrar uma referência a estes protocolos. Os números de porta que correspondem a estes protocolos podem igualmente ser encontrados por quando você configurar o ACL incorporando a**?** no lugar de um número de porta.

bgp	kshell
Chargen (geração de caracteres)	login
cmd	lpd
daytime	NNTP
discard	pim
domínio	pop2
eco	pop3
exec	smtp
finger	sunrpc
ftp	syslog
ftp-data	tacacstalk
gopher	telnet
hostname	tempo
ident	uucp
irc	WHOIS
klogin	WWW

Nomes de porta UDP

Esta lista de nomes da porta UDP pode ser usada em vez dos números de porta quando você configura o ACL no Cisco IOS Software. Refira o RFC do assigned number atual a fim encontrar uma referência a estes protocolos. Os números de porta que correspondem a estes protocolos podem igualmente ser encontrados por quando você configurar o ACL incorporando a**?** no lugar de um número de porta.

biff	ntp
bootpc	pim-auto-rp
bootps	rip
discard	snmp:
dnsix	snmptrap

domínio	sunrpc
eco	syslog
isakmp	tacacs
mobile-ip	conversa
nameserver	tftp
netbios-dgm	tempo
netbios-ns	quem
NetBIOS-SS	xdmcp

Diretrizes de distribuição

Cisco recomenda práticas conservadoras do desenvolvimento. Você deve ter um entendimento claro de protocolos exigidos a fim distribuir com sucesso o trânsito ACL. Estas diretrizes descrevem muito um método conservador para o desenvolvimento da proteção ACL que usam a aproximação iterativa.

1. **Identifique os protocolos usados na rede com uma classificação ACL.**Distribua um ACL que permita todos os protocolos conhecidos que são usados na rede. Esta descoberta, ou a classificação, ACL devem ter um endereço de origem de **alguns** e um destino de um endereço IP de Um ou Mais Servidores Cisco ICM NT ou da sub-rede inteira IP do Internet roteável. Configurar uma última entrada que permita o **IP toda a qualquer** ordem do **início de uma sessão** ajudar a identificar os protocolos adicionais que você precisa de permitir.O objetivo é determinar todos os protocolos exigidos que estão no uso na rede. Use o registro para a análise a fim determinar que poder outro se comunica 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. Use os períodos de tempo da palavra-chave do **log** para breve e somente quando necessário a fim ajudar a classificar o tráfego.Note por favor que a rede é em risco do ataque quando um ACL que consista em todas as indicações da **licença** for no lugar. Execute o processo da classificação o mais rapidamente possível de modo que os controles de acesso apropriados possam ser postos no lugar.
2. **Reveja pacotes identificados e comece a filtrar o acesso à rede interna.**Após identificar e revisar os pacotes filtrados pelo ACL no passo 1, atualize o ACL de classificação para responder pelos protocolos e endereços de IP recém-identificados. Adicionar entradas ACL para anti-falsificação. Como necessário, o específico substitute **nega** entradas para indicações da **licença na** classificação ACL. Você pode usar o **comando show access-list** monitorar o específico **nega** entradas pode ser monitorado para a contagem da batida. Isso fornece informações sobre tentativas de acesso a redes proibidas sem que seja necessário habilitar o registro em entradas de ACL. A última linha da ACL deve ser deny ip any any. Mais uma vez, a contagem da batida contra esta última entrada pode fornecer a informação sobre tentativas de acesso proibidas.
3. **O monitor e atualiza o ACL.**Monitore o ACL terminado a fim assegurar-se de que os protocolos exigidos recentemente introduzidos estejam adicionados em uma maneira controlada. Se você monitora o ACL, igualmente fornece a informação sobre as tentativas proibidas do acesso de rede que poderiam fornecer a informação sobre ataques iminentes.

Exemplo de distribuição

Este exemplo mostra um trânsito ACL que proteja um baseado na rede neste endereçamento.

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador ISP é 10.1.1.1.O endereço IP de Um ou Mais Servidores Cisco ICM NT da face Internet do roteador de ponta é 10.1.1.2.A sub-rede roteável de Internet é 192.168.201.0 255.255.255.0.O fim do cabeçalho VPN é 192.168.201.100.O servidor de Web é 192.168.201.101.O servidor FTP é 192.168.201.102.O servidor de SMTP é 192.168.201.103.O servidor de DNS principal é 192.168.201.104.O servidor de DNS secundário é 172.16.201.50.

A proteção ACL do trânsito foi desenvolvida com base nesta informação. O ACL permite o peering eBGP ao roteador ISP, fornece filtros do anti-spoof, permite o tráfego de retorno específico, permite o tráfego de entrada específico, e nega explicitamente todo tráfego restante.

```
no access-list 110
!--- Phase 1 - Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses.

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
access-list 110 deny   ip host 255.255.255.255 any
!--- This deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny   ip host 0.0.0.0 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 !---
Permit BGP to the edge router. access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq
bgp access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023 !--- Deny your space
as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0 0.0.0.255 any !--- Phase
2 - Explicitly permit return traffic. !--- Allow specific ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq domain host
192.168.201.104 gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-
list 110 permit udp any eq domain host 192.168.201.104 eq domain !--- Permit legitimate business
traffic. access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established access-list 110
permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Allow FTP data connections.
access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data
and multimedia connections. access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt
1023 !--- Phase 3 - Explicitly permit externally sourced traffic. !--- These are incoming DNS
queries.

access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain
!--- Zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--- Permit older DNS zone transfers.
access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain !--- Deny
all other DNS traffic. access-list 110 deny udp any any eq domain access-list 110 deny tcp any
any eq domain !--- Allow IPSec VPN traffic. access-list 110 permit udp any host 192.168.201.100
eq isakmp access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp access-list 110
permit esp any host 192.168.201.100 access-list 110 permit ahp any host 192.168.201.100 access-
list 110 deny ip any host 192.168.201.100 !--- These are Internet-sourced connections to !---
publicly accessible servers. access-list 110 permit tcp any host 192.168.201.101 eq www access-
list 110 permit tcp any host 192.168.201.101 eq 443 access-list 110 permit tcp any host
```

```
192.168.201.102 eq ftp !--- Data connections to the FTP server are allowed !--- by the permit
established ACE in Phase 3. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023
access-list 110 permit tcp any host 192.168.201.103 eq smtp

!--- Phase 4 - Add explicit deny statement.

access-list 110 deny   ip any any

Edge-router(config)#interface serial 2/0
Edge-router(config-if)#ip access-group 110 in
```

Informações Relacionadas

- Página de Suporte das Listas de Acesso
- Referência de comandos dos Serviços de comutação Cisco IOS, Versão 12.2 - Comandos: taxa-limite da lista de acesso através do cef IP
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems