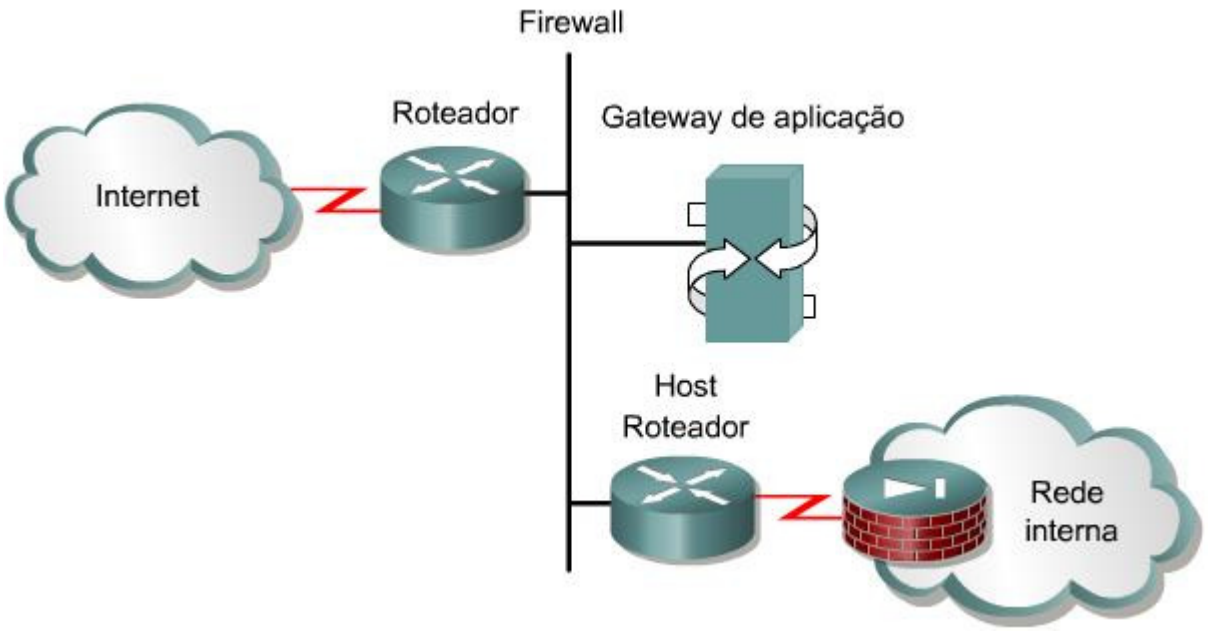
Universidade do Sul de Santa Catarina

ACL's - Access Control Lists
Listas de Controle de Acesso

Prof.ª Ana Lúcia Rodrigues Wiggers
Ana.wiggers@unisul.br

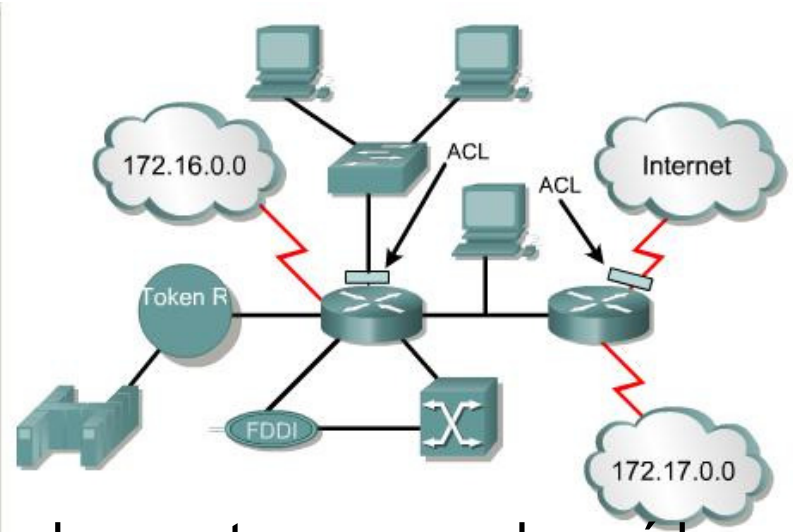
Firewall


Firewall
Roteador
Gateway de aplicação
Internet
Host
Roteador
Rede
interna

Listas de Controle de Acesso

- ACL é uma lista seqüencial de instruções de permissão ou de recusa que se aplica a endereços ou a protocolos das camadas superiores.
- As ACL's filtram o tráfego da rede, controlando se os pacotes roteados são encaminhados ou bloqueados nas interfaces dos roteadores.
- As ACL's podem ser criadas para todos os protocolos de rede roteados, como o IP e o IPX.
- Alguns pontos de decisão das ACL's são: endereços de origem e destino, protocolos e números de portas de camadas superiores.

Funções e operações das ACL's



Para controlar o fluxo de tráfego em uma interface, deve-se definir uma ACL para cada protocolo ativado na interface.

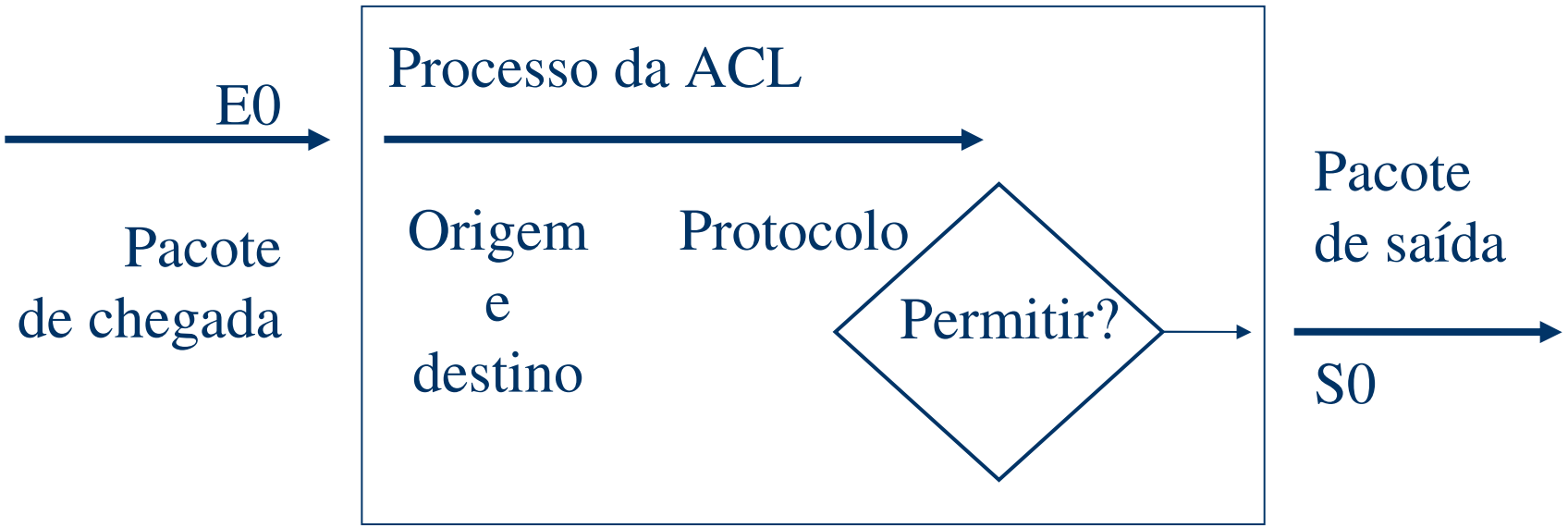
Como também é necessário criar uma ACL separada para cada direção, uma para o tráfego de entrada e outra para o de saída.

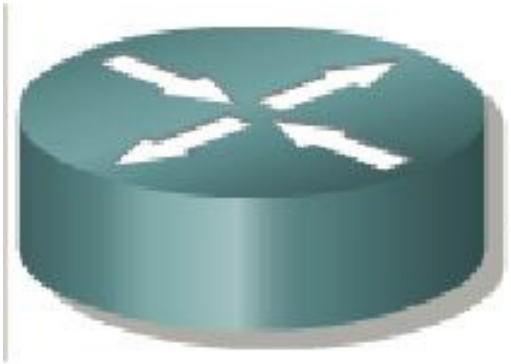
Por fim, é possível definir vários protocolos e várias direções para cada interface.

Por exemplo: se o roteador tiver duas interfaces configuradas para IP, AppleTalk e IPX, serão necessárias 12 ACL's.

Uma ACL para cada protocolo, vezes dois (direções de entrada e saída), vezes dois (quantidade de portas).

Funções e operações das ACL's





Funções e operações das ACL’s

- As ACL's podem ser aplicadas da seguinte forma:
  - **Listas de acesso de chegada**: os pacotes são processados antes de serem roteados para uma interface de saída. Uma ***ACL de entrada é mais eficiente do que uma de saída porque economiza o custo das consultas em tabelas de roteamento*** se o pacote for descartado pelos testes de filtragem. Se passar pelos teste será processado para roteamento.
  - **Listas de acesso de saída**: os pacotes recebidos são roteados para a interface de saída e então processados através da ACL de saída antes da transmissão.

Funções e operações das ACL's

- Os principais tipos de listas de controle de acesso:
  - **Listas de acesso padrão:** verificam o ***endereço de origem*** dos pacotes que podem ser roteados. A ACL padrão não especifica endereço de destino; portanto, deve ser posicionada o mais perto possível do destino. Por exemplo, uma ACL padrão deve ser posicionada em Fa0/0 do roteador D para impedir o tráfego do roteador A.
  - **Listas de acesso estendida:** verificam os ***endereços de pacotes de origem e de destino***. Também podem verificar protocolos específicos, números de portas e outros parâmetros. A regra geral é colocar a ACL estendida o mais perto possível da origem do tráfego negado.

Funções e operações das ACL's

- As ***instruções da ACL operam em ordem seqüencial e lógica***. Se a correspondência com uma condição é verdadeira, o pacote é permitido ou negado e as instruções restantes da ACL não são verificadas.
- Caso não haja correspondência em nenhuma das instruções da ACL, uma instrução ***`deny any` implícita*** é colocada no final da lista por padrão. Mesmo que o **`deny any`** não seja visível na última linha de uma ACL, ele está lá e ***não permite que nenhum pacote sem correspondência na ACL seja aceito***.
- Na criação de uma ACL é ***recomendável adicionar o `deny` implícito no final das ACL's***, para reforçar a presença dinâmica do **`deny`** implícito.

Regras básicas de criação das ACL's

Estas regras básicas devem ser seguidas ao se criar e aplicar listas de acesso:

1. Uma lista de acesso pode ser implementada por protocolo e por direção.
2. As listas de acesso padrão devem ser aplicadas o mais perto possível do destino.
3. As listas de acesso estendidas devem ser aplicadas o mais perto possível da origem.
4. Use a referência de interface de entrada ou de saída como se estivesse olhando a porta de dentro do roteador.
5. As instruções são processadas seqüencialmente do topo da lista para baixo, até que uma correspondência é encontrada; se não é encontrada nenhuma correspondência, o pacote é negado.
6. **Existe um deny any implícito no final de todas as listas de acesso**. Isso não aparece na listagem da configuração.
7. As entradas das listas de acesso devem filtrar na ordem do específico para o geral. Hosts específicos devem ser recusados primeiro e grupos ou filtros gerais devem vir por último.

Regras básicas de criação das ACL’s

8. A condição de correspondência é examinada primeiro. A permissão ou recusa é examinada SOMENTE se a correspondência é verdadeira.
9. Nunca trabalhe com uma lista de acesso que seja aplicada ativamente.
10. Use um editor de texto para criar comentários delineando a lógica; em seguida, preencha as instruções que realizam essa lógica.
11. As novas linhas sempre são adicionadas na parte inferior da lista de acesso. Um comando **no access-list *x* remove a lista inteira.** Não é possível adicionar ou remover linhas específicas de ACL's numeradas.
12. **Uma lista de acesso IP envia uma mensagem "host ICMP não pode ser alcançado" para o remetente do pacote rejeitado e descarta o pacote**.
13. Deve-se tomar cuidado ao remover uma lista de acesso. Se a lista de acesso está aplicada a uma interface de produção e é removida, dependendo da versão do IOS, pode haver um "deny any" padrão aplicado à interface e todo o tráfego será bloqueado.
14. Os filtros de saída não afetam o tráfego originário do roteador local.

Modo de configuração das ACL's

- Router(config)#
- Existem tipos diferentes de ACL's: padrão, estendido, IPX, AppleTalk e outros.
- Ao ser configurada em um roteador, cada ACL deve ser definida de maneira exclusiva, recebendo um número que identificará o tipo de lista de acesso criado e deve estar dentro do intervalo específico de números válidos para esse tipo de lista.

Protocolo	Intervalo
IP	1-99, 1300-1999
IP Estendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX Estendido	900-999
Protocolo de Anúncio de Serviço IPX	1000-1099

Modo de configuração das ACL's

- **Definição de uma ACL:**

Etapa 1	Defina a ACL, usando o seguinte comando: `Router(config)#access-list access-list-number {permit | deny} {test-conditions}` Uma instrução global identifica a ACL. Especificamente, a faixa entre 1 e 99 está reservada para o IP padrão. Esse número refere-se ao tipo de ACL. No Cisco IOS Versão 11.2 ou mais recente, as ACLs também podem usar um nome ACL, como education_group, ao invés de um número. O termo permit ou deny na instrução ACL global indica como os pacotes que satisfazem as condições de testes são tratados pelo software Cisco IOS. Permit geralmente significa que o pacote terá a autorização para usar uma ou mais interfaces que serão especificadas mais tarde. O termo ou termos finais especifica as condições de teste usadas pela instrução da ACL.

Modo de configuração das AC’Ls

- **Aplicação de uma ACL:**

Etapa 2	Em seguida, é necessário aplicar as ACLs a uma interface, usando o comando access-group, conforme este exemplo: `Router(config-if)#(protocol) access-group access-list-number` Todas as instruções da ACL identificadas pelo número de lista de acesso são associadas a uma ou mais interfaces. Quaisquer pacotes que passam nas condições de teste ACL podem ter a permissão de usar quaisquer interfaces no grupo de acesso das interfaces.

Modo de configuração das ACL's
Máscara Curinga

- A máscara curinga é composta de 32 bits divididos em quatro octetos.
- Máscaras curinga (wildcard) usam uns e zeros binários para filtrar endereços IP individuais ou grupos de endereços IP, permitindo ou negando o acesso aos recursos com base nesses endereços.
- access-list 1 permit 172.16.0.0 **0.0.255.255**
- Máscara curinga (source-wildcard)
  00000000.00000000.11111111.11111111 =
  00000000.00000000.XXXXXXXX.XXXXXXXX onde um zero significa "**deixe o valor passar para ser verificado**", enquanto que um X (1) significa "**bloqueie o valor e não deixe que ele seja comparado**".

Obs.: capítulo 11.1.4

Modo de configuração das ACL's
Máscara Curinga

- Há duas palavras-chave especiais que são usadas nas ACL's, as opções **any** e **host**.
- A opção **any substitui o endereço IP e a máscara curinga por 255.255.255.255**. Essa opção coincide com qualquer endereço que é comparado com ela.
- A opção **host substitui a máscara 0.0.0.0**. Essa máscara requer que todos os bits do endereço da ACL e do endereço do pacote coincidam. Essa opção faz coincidir apenas um endereço.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

Pode ser escrito como:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Pode ser escrito como:
Router(config)#access-list 1 permit host 172.30.16.29
```

Modo de configuração das ACL's
Máscara Curinga

- A máscara curinga de uma máscara de sub-rede completa pode ser encontrada subtraindo-se a máscara de sub-rede de 255.255.255.255.

  Por exemplo, se a máscara de sub-rede for do tipo 255.255.240.0 ou /20, a seguinte equação seria utilizada:

  255.255.255.255 *(máscara pasdrão/default)*

  \- 255.255.240.0 *(máscara de sub-rede)*

  0. 0. 15. 255 *esta é a máscara curinga.*

Verificando as ACL’s

- O comando **`show ip interface`** exibe as informações da interface IP e indica se há alguma ACL definida.
- O comando **`show access-lists`** exibe o conteúdo de todas as ACL's do roteador. Para ver uma lista específica, adicione o nome ou número da ACL como opção para esse comando.
- O comando **`show running-config`** também revela as listas de acesso de um roteador e as informações de atribuição de interface.

Tipo ACL Padrão

- A versão padrão do comando de configuração global **`access-list`** é usada para definir uma ACL padrão com um número no intervalo de **1** e **99**. Na **versão 12.0.1 do Cisco IOS**, ACL's padrão passaram a usar uma faixa adicional de números (**1300 a 1999**), podendo prover até 798 possíveis ACL's padrão. Esses números adicionais são referenciados como ACL's IP expandidas.

Configuração ACL Padrão

- **A sintaxe completa do comando da ACL padrão é:**

```
Router(config)#   access-list   access-list-number
{deny | permit | remark} source [source-wildcard ]
```

- **A palavra-chave `remark` torna a lista de acesso fácil de entender. Cada comentário pode ter até 100 caracteres.**

```
Access-list 1 remark Permite que passe somente o
tráfego da estação do Fulano access-list 1 permit
host 171.69.2.88
```

- **O comando `ip access-group` associa uma ACL padrão existente a uma interface:**

```
Router(config-if)# ip access-group {access-list-
number | access-list-name} {in | out }
```

Tipo ACL Estendida

- As ACL's estendidas são usadas com mais freqüência do que as ACL's padrão porque proporcionam um intervalo maior de controle.
- As ACL's estendidas usam um número de lista de acesso no intervalo entre **100 e 199** (também entre **2000 e 2699 nos IOS mais recentes**).
- Os pacotes podem ter acesso permitido ou negado com base no seu local de origem ou de destino, bem como no tipo de protocolo e nos endereços das portas.
- É possível especificar operações lógicas, que serão realizadas pela ACL estendida em determinados protocolos, tais como:
  - **igual (eq), diferente (neq), maior do que (gt) e menor do que (lt).**

Configuração ACL Estendida

Exemplo: ***ACL 101 permite o tráfego TCP do IP 172.16.0.1 0.0.0.0 para o destino 192.168.0.0 0.0.255.255 (verificar 2 últimos octetos) para FTP***

```
router1(config)#access-list 101 permit tcp
172.16.0.1 0.0.0.0 192.168.0.0 0.0.255.255 eq ftp
```

Exemplo: ***ACL 101 permite o tráfego TCP do IP 172.16.0.1 0.0.0.0 para qualquer IP destino (verificar 2 últimos octetos) para FTP***

```
router1(config)#access-list 101 permit tcp host
172.16.0.1 any eq ftp
```

Aplicar a ACL em uma interface

```
router1(config-if)#ip access-group access-list-
number {in | out}
```

Tipo ACL com nome

- A configuração de uma ACL com nome é muito semelhante à configuração de uma ACL padrão ou estendida.

  A primeira diferença é que, em vez de iniciar o comando com **access-list**, a ACL com nome utiliza **ip access-list**:

- `router1(config)# ip access-list {extended-standard} name`

Restrigindo o acesso via terminal virtual (vty)

- O processo de criação da lista de acesso vty é o mesmo descrito para uma interface. Entretanto, a aplicação da ACL a uma linha de terminal requer o comando **`access-class`** em vez do comando **`access-group`**
- Deve-se considerar o seguinte ao se configurar listas de acesso em linhas vty:
  - Quando se estiver controlando o acesso a uma interface, pode-se usar um nome ou um número.
  - **Somente listas de acesso com número podem ser aplicadas a linhas virtuais (telnet)**.
  - Defina restrições idênticas em todas as linhas de terminais virtuais, porque um usuário pode tentar conectar-se a qualquer uma delas.

Configuração ACL para terminais virtuais

- **Comandos necessários para configurar o acesso via terminal virtual:**

  Rt1(config)# **access-list 2 permit 172.16.1.0 0.0.0.255**

  Rt1(config)# **access-list 2 permit 172.16.2.0 0.0.0.255**

  Rt1(config)# **access-list 2 deny any**

- **Comandos necessários para aplicar a lista de acesso:**

  Rt1(config)# **line vty 0 4**

  Rt1(config-line)# **login**

  Rt1(config-line)# **password** *secret*

  Rt1(config-line)# **access-class 2 in**