Raphael Guimarães Gonçalves
raphagg@cbpf.br
Nilton Alves Jr.
naj@cbpf.br
http://mesonpi.cat.cbpf.br/naj

Listas de Acesso (ACL).

Resumo

Neste trabalho serão apresentadas as Listas de Acesso, que são uma ferramenta que existem principalmente em roteadores cisco, sendo sua principal função servir como filtro de pacotes na rede. Normalmente estes filtros são utilizados para selecionar pacotes que entram ou saem de uma determinada interface, mas em alguns casos estes filtros podem ser redistribuídos em alguns protocolos. Será dada ênfase as *IP Standard* e *IP Extended Access Lists*, por serem os tipos mais utilizados.

No presente trabalho será mostrada a sintaxe dos comandos, algumas aplicações e no fim será feito uma conclusão sobre o estudo realizado.

1. Introdução

Mecanismos de filtragem vêm sendo utilizados em larga escala há muito tempo para melhorar a segurança, pois na maioria das vezes são implementados com baixo custo pelo fato da maioria dos roteadores suportarem naturalmente esse recurso e por causarem pouco impacto no desempenho da rede.

As listas de acesso são uma ferramenta existente em alguns dispositivos de rede, porém vamos abordar especificamente os roteadores Cisco. É utilizada de forma a se obter uma maior integridade dos dados que trafegam em uma rede, pois tem característica de funcionar como filtro. As listas de acesso funcionam como se fossem várias situações condicionais de um algoritmo (IF, THEN. ELSE). Cada pacote que chega a um dispositivo de rede será analisado de acordo com as listas de acesso aplicadas neste dispositivo. Esta análise é feita percorrendo a lista de acesso de cima para baixo.

Basicamente as listas de acesso são um conjunto de regras que são implementadas na maioria das vezes ou em uma interface ou redistribuída em um protocolo, e estas regras são utilizadas de maneira que só passe trafego autorizado na rede.

É valido ressaltar que essas tais regras podem se tornar muito complexas, exigindo um maior entendimento dos protocolos por ser comum que aconteça algum erro na hora da sua elaboração.

2. Especificação das *Access Lists*

A partir da versão 11.2 do IOS da Cisco as listas de acesso começaram a ser referenciadas por nome ou por número, diferente de antes, que só eram referenciadas por números. A seguinte tabela mostra a lista de alguns protocolos que usam listas de acesso referenciadas por números e inclui também a escala de números da lista de acesso que é valida para cada protocolo.

Protocolos com *Access Lists* referenciadas por número

Protocolo	Escala
IP Standard	1 a 99
IP Extended	100 a 199
IP Standard (expanção)	1300 a 1999
IP Extended (expanção)	2000 a 2099

A seguir uma tabela com alguns protocolos que podem usar listas de acesso referenciadas por nome.

Protocolos com *Access Lists* referenciadas por nome

Protocolo
Apollo Domain
IP Standard
IP Extended
IPX NetBIOS

De todos os tipos de listas de acesso apresentadas nas tabelas acima serão mostradas nesta nota técnica as que tratam de *IP Standard e Extended*.

3. IP Access List Standard

Este tipo de lista de acesso só analisa a origem dos pacotes e não permite a escolha de qual porta será filtrada.

3.1. IP Access List Standard Number

É válido lembrar que este tipo de lista de acesso só está especificada para números que variem de 1 até 99.

Para criar uma lista do tipo *IP access list standard number* basta seguir a sintaxe que é apresentada a seguir. Todo o comando é feito a partir do prompt **Router(config)#**.

Sintaxe	Descrição
access-list *access-list number* {deny|permit} *endereço_da_origem máscara_wildcard_da_origem* log	Define o número da access list, se ela permitirá ou proibirá o tráfego do determinado pacote, o endereço de origem, a máscara de wildcard e faz log.

A máscara de **wildcard** é essencialmente o inverso da máscara que estamos acostumados (máscara do endereço IP). A seguir serão mostrados alguns exemplos desta máscara:

Exemplos de Máscara de *Wildcard*

Endereço/Rede	Máscara Correspondente
10.1.1.1/8	0.255.255.255
146.25.258.10/16	0.0.255.255
200.20.94.254/24	0.0.0.0.255
200.20.85.1/30	0.0.0.3

Há algumas máscaras de **wildcard** que podem ser substituídas por atalhos como, por exemplo:

Atalhos para a Máscara de *Wildcard*

Máscara	Atalho
endereço 0.0.0.0	Antes do endereço escreva a palavra **host**.
0.0.0.0 255.255.255.255	Substitua o endereço e a máscara pela palavra **any**.

Estes atalhos mostrados valem para qualquer tipo de lista de acesso que será abordada neste trabalho.

3.2. IP Access List Standard Name

Para criar uma *IP access list standard name* basta seguir a sintaxe apresentada a seguir. Todo o comando é feito dentro **Router(config)#**.

Sintaxe	Descrição
ip access-list standard *name*	Define o nome da *access list*
{deny|permit} *endereço_da_origem máscara_de_wildcard* log	Define se ela permitirá ou proibirá o tráfego do determinado pacote, o endereço de origem, a máscara de wildcard e faz log.

4. IP Access List *Extended*

Este tipo de lista de acesso checa tanto o endereço de origem quanto o endereço de destino, porém há como checar outros tipos de parâmetros como número de portas específicas.

4.1. IP Access List Extended Number

É válido lembrar que este tipo de lista de acesso está especificada para números entre 100 e 199.

Para criar uma *IP access list extended number* basta seguir a sintaxe que é apresentada a seguir. Todo o comando é feito dentro do prompt **Router(config)#**.

Sintaxe	Descrição
access-list *access-list number* {deny|permit} *endereço_da_origem máscara_wildcard_ da_ origem endereço_de_destino máscara_ de_ wildcard_de_destino* {eq|lt|gt|neq} *número_da_porta*	Define se ela permitirá ou proibirá o trafégo de determinado pacote, o endereço de origem, o endereço de destino, e por qual porta(s) o pacote virá para ser feita a checagem.

4.2. IP Access List Extended Name

Para criar uma *IP access list extended name* basta seguir a sintaxe apresentada na tabela a seguir. Todo o comando é feito dentro do prompt **Router(config)#**.

Sintaxe	Descrição
ip access-list extended *name*	Define o nome da *access list*
{deny|permit} *endereço_da_origem máscara_de_wildcard_da_origem endereço_de_destino máscara_de_wildcard_de_destino* {eq|lt|gt|neq} *número_da_porta*	Define se ela permitirá ou proibirá o tráfego do determinado pacote, o endereço de origem, o endereço de destino, e por qual porta(s) o pacote virá para ser feita a checagem.

É válido ressaltar que os operadores *eq*, *lt*, *gt*, *neq*, significam respectivamente *equal*, *less than*, *greater than*, *not equal*, e são utilizados para especificar qual ou quais portas serão checadas.

5. Comentando *Access List*

Na versão 12.0(2)T do IOS, já é possível incluir comentários nas listas de acesso, comentários estes que tem como maior finalidade facilitar o entendimento dos filtros por parte do administrador da rede. Este tipo de comentário é limitado à 100 caracteres.

Para comentar listas de acesso definidas por número é utilizado o seguinte comando:

```
access-list núemro_da_lista_de_acesso remark comentário
```

Para comentar listas de acesso definidas por nome é utilizado o seguinte comando:

```
remark comentário
```

Este comando é feito dentro do prompt que aparece quando é criada uma lista de acesso definida por nome.

6. Aplicações das *Access Lists*

Anteriormente foi falado que as listas de acesso são utilizadas para uma variedade de propósitos. Neste item serão mostrados alguns exemplos destas utilizações.

6.1. Filtro de pacotes na interface de um roteador utilizando uma lista de acesso *Standard Number*

Neste primeiro exemplo, vamos imaginar que há uma rede classe B cujo o endereço IP é 137.77.0.0 diretamente conectada à interface Ethernet 0 de um roteador. Nosso interesse é filtrar qualquer pacote da subrede 137.77.13.0 com exceção do host 137.77.13.7, e que também qualquer outro pacote da rede 137.77.13.0 seja permitido. Para este cenário descrito a lista de acesso melhor a ser criada será:

```
access-list 7 permit host 137.77.13.7
access-list 7 deny 137.77.13.0 0.0.0.255
access-list 7 permit 137.77.0.0 0.0.255.255
```

Depois de criada a lista de acesso é muito importante saber como aplicá-la. Para isto existe o comando **ip access-group** que é utilizado para dizer onde a lista de acesso vai ser aplicada, comando este que será mencionado mais à frente com maior profundidade. Para conseguirmos aplicar a lista de acesso criada na interface Ethernet 0 do roteador conforme o proposto pelo exemplo é necessário seguir os seguintes passos:

```
interface ethernet 0
ip access-group 7 in
```

Utilizando o comando **ip access-group** desta maneira, a lista de acesso criada esta aplicada a todos os pacotes que entram (**in**) na interface Ethernet 0.

6.2. Filtro de pacotes na interface de um roteador utilizando uma lista de acesso *Extended Name*

Vamos supor agora que um roteador tem conectado à ele uma rede interna e também tem um enlace para a Internet via sua interface Serial 0. Esta rede interna é uma classe B cujo o endereço IP é 131.108.0.0, nós queremos que mensagens *Internet Control Message Protocol* (ICMP) oriundas de fora de sua rede sejam permitidas. Outra proposição é que pacotes *Simple Mail Transfer Protocol* (SMTP) com destino para o host 131.108.15.1 sejam aceitos. Por fim a última proposição é que pacotes vindos por portas maiores que 1023 sejam aceitos por toda a rede interna.

Para conseguirmos montar uma lista de acesso que atenda tudo o que foi proposto é necessário que sigamos os seguintes passos:

```
ip access-list extended filter-in
permit tcp 0.0.0.0 255.255.255.255 131.108.0.0 0.0.255.255 gt 1023
permit tcp 0.0.0.0 255.255.255.255 131.108.15.1 0.0.0.0 eq 25
permit icmp 0.0.0.0 255.255.255.255 131.108.0.0 0.0.255.255
```

Outra maneira de se escrever esta lista de acesso seria da seguinte forma:

```
ip access-list extended filter-in
permit tcp any 131.108.0.0 0.0.255.255 gt 1023
permit tcp any host 131.108.15.1 eq 25
permit icmp 0.0.0.0 255.255.255.255 131.108.0.0 0.0.255.255
```

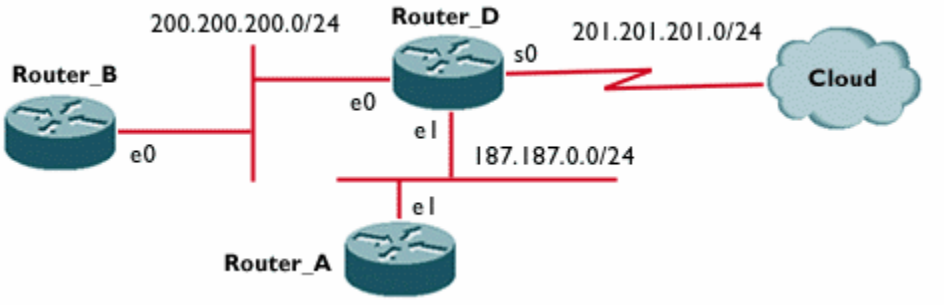
Para que esta lista de acesso seja aplicada corretamente é necessário utilizar os seguintes comandos:

```
interface s 0
ip access-group filter-in in
```

Note que a lista de acesso foi aplicada na interface Serial 0, de maneira que todos pacotes que entram (**in**) nesta interface serão analisados à partir da lista de acesso criada.

7. *Inbound* versus *Outbound Access Lists*

Para ter um melhor entendimento do commando ***ip access-group*** é necessário saber a diferença entre uma lista de acesso aplicada **in** ou **out**. A seguinte figura será utilizada para descrever a diferença entre uma e outra.



Topologia da rede

Vamos supor que nossa intenção é de proteger os roteadores D, B e A de dispositivos que se encontrem na nuvem, nós poderemos conseguir isto negando pacotes Telnet que venham da nuvem. A lista de acesso criada ficaria desta forma:

```
access-list 177 deny tcp any any eq telnet
```

Nós poderíamos aplicar esta lista de acesso de duas maneiras diferentes, a primeira maneira seria aplicá-la na interface Serial 0 do roteador D para pacotes que entram nesta interface, e a outra maneira seria aplicar a lista de acesso criada, para pacotes que saem das interfaces Ethernet do mesmo roteador.

A diferença de aplicar a lista de acesso de uma maneira ou de outra vai ser explicada fazendo-se uso de alguns exemplos.

Como primeiro exemplo vamos supor que a lista de acesso foi aplicada na saída das interfaces Ethernet do roteador D. Vamos imaginar agora, que o roteador D receba um pacote telnet destinado a interface Ethernet 1 (187.187.1.1) do roteador A, o roteador D recebe o pacote e faz o roteamento decidindo que este pacote terá que ir para a sua interface Ethernet 1, e como nesta interface está aplicada uma lista de acesso para pacotes que saem da mesma, este pacote será descartado e uma mensagem ICMP será mandada de volta à origem do pacote. Ou seja, quando uma lista de acesso é *outbound* ela só é verificada depois que o roteador já fez sua decisão para aonde o pacote será roteado.

Neste cenário, se o roteador D receber um pacote telnet destinado à sua interface Serial 0 ele será aceito, pois a lista de acesso só seria verificada se para chegar ao seu destino o pacote tivesse que passar pelas interfaces Ethernet do roteador D. Por este motivo e por outros, que é sempre aconselhável que aplique-se as listas de acesso para pacotes que entram nas interfaces, descartando assim, a possibilidade das listas de acesso não serem verificadas.

8. Redistribuindo as Listas de Acesso em protocolos

As listas de acesso podem ser utilizadas dentro de outros protocolos. Para melhor exemplificar esta aplicação, será mostrado um exemplo utilizando o protocolo RIP.

Neste exemplo, supomos que existam dois roteadores ligados entre si pelas suas interfaces Serial 0, o roteador A e B. Estes dois roteadores mandam rotas um para o outro por RIP, a rede que estão diretamente conectados é uma classe B cujo endereço IP é 131.108.0.0, o roteador A está aprendendo sobre uma rede privada 10.0.0.0 através de sua interface Ethernet 0. Atráves de uma lista de acesso podemos conseguir que o roteador B não aprenda sobre esta rede privada. É necessário utilizar o comando **distribute-list**. Este comando pode ser utilizado de duas maneiras para este tipo de cenário, estas duas maneiras serão exemplificadas abaixo.

Na primeira maneira, o comando **distribute-list** pode ser aplicado na saída da interface Serial 0 do roteador A, os comandos utilizados virão a seguir:

```
access-list 7 deny 10.0.0.0 0.255.255.255
access-list 7 permit any

router rip
network 10.0.0.0
network 131.108.10.0
distribute list 7 out serial 0
```

Se a lista de acesso fosse aplicada no roteador B, os comandos utilizados seriam estes:

```
access-list 7 deny 10.0.0.0 0.255.255.255
access-list 7 permit any

router rip
network 131.108.0.0
distribute-list 7 in serial 0
```

9. Conclusão

Ao final deste trabalho, podemos concluir que as listas de acesso têm papel fundamental no que se diz respeito à segurança da rede, pois elas podem servir como peça fundamental na política de segurança da rede.

É muito importante ressaltar que as listas de acesso só terão seu melhor funcionamento se forem devidamente configuradas. E para isso é necessário que o administrador da rede ou a pessoa encarregada da segurança tenha um bom domínio sobre as mesmas. Isto se faz necessário, pois qualquer erro na configuração ou aplicação das listas de acesso pode acarretar que o objetivo traçado para ela não seja alcançado. Vale lembrar, que antes de configurar as listas de acesso deve-se fazer um estudo detalhado da rede, pois qualquer inversão de linha na hora da sua criação, poderá acarretar que trafego indesejado chegue até a rede.

Por fim, vale notar que a simples implementação de listas de acesso em roteadores não é o suficiente para garantir a segurança da rede, trata-se de mais um recurso que deve ser utilizado de acordo com a política de segurança e com os demais elementos que componhem o perímetro de segurança da rede.

10. Referências

- "Configuring IP Access Lists", http://www.cisco.com/warp/public/707/confaccesslists.html

- "RNP News Generation Vol. 2/ No.3 – Usando Filtros de Pacotes para Aumentar a Segurança", http://www.rnp.br/newsgen/9803/filtros.shtml

- "Segurança em Roteadores", http://www.absoluta.org/seguranca/seg_router.htm

- "Melhorando a Segurança com Filtros de Pacote", http://www.absoluta.org/seguranca/seg_cisco.htm

- "Segurança de Host", http://www.absoluta.org/seguranca/seg_firewall.htm