Acesso Inicial

ACLs IPV6

Descrição: Abaixo serão apresentadas as configurações iniciais do ACLs IPV6.

Observação: Necessário prévia configuração de IPV6 nos roteadores.

ACLs: Uma ACL é uma lista sequencial de instruções de permissão ou de negação, conhecidas como entradas de controle.

ACLs em IPV6: Somente nomeadas**.** Tipos de comandos usados abaixo:

- **ACL** nomeada = Ex. *ipv6 access-list NO_TELNET*
    - Filtra os pacotes IP com base apenas no endereço de origem;
    - Atribui nome para identificar a ACL;

Comandos usados de exemplo:

- **deny** = especifica que o pacote será descartado;
- **permit** = especifica que o pacote será encaminhado;
- **host xxxxxxx** = Endereço do host que deseja adicionar à lista NO_TELNET;
- **access-list =** cria uma lista especifica da **ACL;**

IPV6: Habilitando IPV6 nos roteadores.

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ipv
Router(config-if)#ipv6 add
Router(config-if)#ipv6 address 2001:1643:4321:1::/64
Router(config-if)#ipv
Router(config-if)#ipv6 au
Router(config-if)#ipv6 add
Router(config-if)#ipv6 address au
Router(config-if)#ipv6 address autoconfig
Router(config-if)#no sh
Router(config-if)#no shutdown
```

Criando uma ACL para negar ou permitir acesso

Obs.: Isso é apenas uma simulação, não deve ser testado em ambiente de produção.

A partir do exemplo de configuração abaixo, a declaração de autorização só permite que o host com o IP descrito execute o protocolo *TELNET*.

```
Router(config)#ipv6 access-list NO_TELNET
Router(config-ipv6-acl)#perm
Router(config-ipv6-acl)#permit tc
Router(config-ipv6-acl)#permit tcp ho
Router(config-ipv6-acl)#permit tcp host 2001:DB8:43:12::1 an
Router(config-ipv6-acl)#permit tcp host 2001:DB8:43:12::1 any eq 23
Router(config-ipv6-acl)#permit tcp host 2001:DB8:43:12:201:63FF:FE08:61A9 an
Router(config-ipv6-acl)#permit tcp host 2001:DB8:43:12:201:63FF:FE08:61A9 any eq 23
Router(config-ipv6-acl)#
```

Bloqueando o acesso ao *HTTP* e a porta 443 (*HTTPS), de um determinado host:*

```
Router(config)#ipv6 access-list BLOCK_HTTP
Router(config-ipv6-acl)#den
Router(config-ipv6-acl)#deny t
Router(config-ipv6-acl)#deny tcp a
Router(config-ipv6-acl)#deny tcp any host
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:43:12::1
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:43:12::1 eq www
Router(config-ipv6-acl)#
```

```
Router(config)#ipv6 access-list BLOCK_HTTP
Router(config-ipv6-acl)#den
Router(config-ipv6-acl)#deny t
Router(config-ipv6-acl)#deny tcp a
Router(config-ipv6-acl)#deny tcp any host
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:43:12::1
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:43:12::1 eq www
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:43:12::1 eq 443
Router(config-ipv6-acl)#
```

Bloqueando o acesso ao FTP via *ACL*:

```
Router(config)#ipv6 access-list NO-FTP-TO-12
Router(config-ipv6-acl)#DEN
Router(config-ipv6-acl)#DENy tcp any 2001:DB8:43:12::/64 eq ftp
Router(config-ipv6-acl)#
```

Criando uma *ACL* com múltiplas regras:

```
Router(config)#ipv6 access-list RETRICTED-ACCESS
Router(config-ipv6-acl)#remark permit access only HTTP and HTTPS to
network 1
Router(config-ipv6-acl)#permit tcp any host 2001:DB8:43:12::10 eq 80
Router(config-ipv6-acl)#permit tcp any host 2001:DB8:43:12::10 eq 443
Router(config-ipv6-acl)#remark deny all other traffic to network 10
Router(config-ipv6-acl)#deny ipv6 any 2001:DB8:43:12::/64
Router(config-ipv6-acl)#remark permit PC2 telnet access to PC3
Router(config-ipv6-acl)#permit tcp 2001:DB8:43:12::12 eq 53
                                   ^
% Invalid input detected at '^' marker.

Router(config-ipv6-acl)#remark deny telnet access to PC2 for all
other device
Router(config-ipv6-acl)#deny tcp any host 2001:1643:4321:1::11 eq 23
Router(config-ipv6-acl)#remark permit access to everything else
Router(config-ipv6-acl)#permit ipv6 any any
Router(config-ipv6-acl)#exit
Router(config)#
```

Depois de criar a lista *ACL*, foi executado na interface de saída.

```
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ipv
Router(config-if)#ipv6 traf
Router(config-if)#ipv6 traffic-filter RE
Router(config-if)#ipv6 traffic-filter RETRICTED-ACCESS in
Router(config-if)#
```

Conforme imagens abaixo, as listas foram criadas de acordo com as regras.

Para executar a *ACL* no roteador, segue o ex.:

```
RO01(config)#interface gigabitEthernet 0/0/0
RO01(config-if)#ipv6 traffic-filter BLOCK_HTTP in
RO01(config-if)#
```

Lista de *ACL* no **RO01**:

```
RO01#show access-lists
IPv6 access list BLOCK_HTTP
    deny tcp any host 2001:DB8:43:12::1
    deny tcp any host 2001:DB8:43:12::1 eq www
    deny tcp any host 2001:DB8:43:12::1 eq 443

RO01#
```

Lista de *ACL* no **RO02**:

```
RO02#show access-lists
IPv6 access list NO_TELNET
    permit tcp host 2001:DB8:43:12::1 any eq telnet
    permit tcp host 2001:DB8:43:12:201:63FF:FE08:61A9 any eq telnet
IPv6 access list NO-FTP-TO-12
    deny tcp any 2001:DB8:43:12::/64 eq ftp
IPv6 access list RETRICTED-ACCESS
    permit tcp any host 2001:DB8:43:12::10 eq www
    permit tcp any host 2001:DB8:43:12::10 eq 443
    deny ipv6 any 2001:DB8:43:12::/64
    deny tcp any host 2001:1643:4321:1::11 eq telnet
    permit ipv6 any any

RO02#
```

RESUMO

- A última instrução de uma ***ACL*** é sempre um ***implicit deny*** que bloqueia todo o tráfego. Para evitar que as instruções ***implicit deny*** no fim da ***ACL*** bloqueiem todo o tráfego, é possível adicionar a instrução ***permit ip any any***.
- Quando o tráfego da rede passa por meio de uma interface configurada com uma ACL, o Roteador compara as configuradas com uma ACL. O Roteador compara as informações no pacote com cada entrada, em ordem sequencial, para determinar se o pacote corresponde a uma das instruções. Se uma correspondência for encontrada, o pacote será processado em conformidade.

FIM