ACTIVIDAD 5.4.13. CONFIGURACIÓN DE LISTAS ACL IPV4 EXTENDIDAS

Memoria Técnica

Ignacio Andrade Salazar

7 A IELC

CONTENIDO

1. ANTECEDENTES

- **1.1. Objetivos**
- **Parte 1: Configure una ACL extendida con nombre**
- **Parte 2: Aplique y verifique la ACL extendida**

1.2. Alcance

- En este escenario, se permiten dispositivos específicos en la LAN a varios servicios en servidores ubicados en Internet.

2. DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

Part 1: Configure a Named Extended ACL

PASO 1: DENEGAR A LA PC1 EL ACCESO A LOS SERVICIOS HTTP Y HTTPS EN EL SERVIDOR1 Y EL SERVIDOR2.

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

23:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done


RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443

RT1(config-ext-nacl)#
```

Copy | Paste

Top

PASO 2: DENEGAR A LA PC2 EL ACCESO A LOS SERVICIOS FTP EN EL SERVIDOR1 Y EL SERVIDOR2.

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Press RETURN to get started.

RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

RT1(config-ext-nacl)#
```

Copy | Paste

Top

PASO 3: DENEGAR A LA PC3 QUE HAGA PING A SERVIDOR1 AL SERVIDOR2.

RT1

Physical Config CLI Attributes

IOS Command Line Interface

```
RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254

RT1(config-ext-nacl)#
```

Copy Paste

Top

PASO 4: PERMITIR EL RESTO DEL TRÁFICO IP.

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254

RT1(config-ext-nacl)#permit ip zny any
                            ^
% Invalid input detected at '^' marker.

RT1(config-ext-nacl)#permit ip any any
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any

RT1(config-ext-nacl)#
```

Copy | Paste

Top

PASO 5: VERIFIQUE LA CONFIGURACIÓN DE LA LISTA DE ACCESO ANTES DE APLICARLA A UNA INTERFAZ.

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

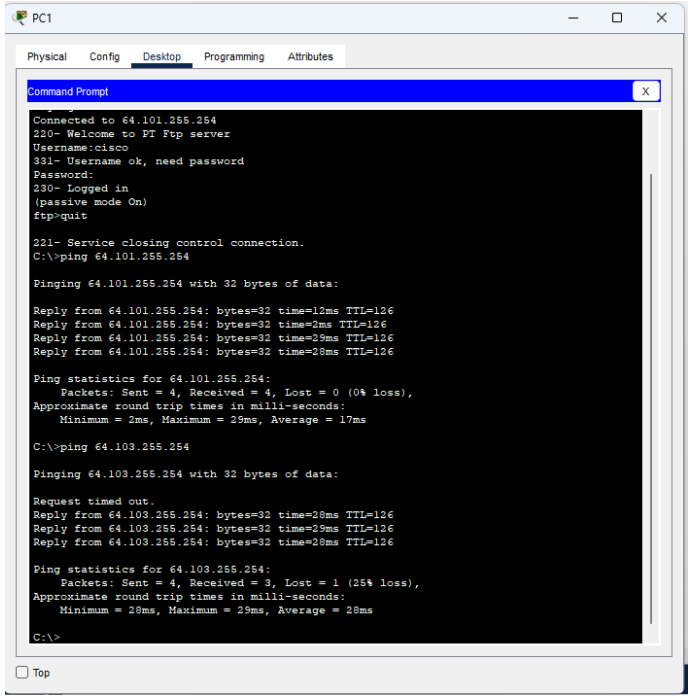
```
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any

RT1(config-ext-nacl)#do show running-config | begin access-list
ip access-list extended ACL
 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
 deny icmp host 172.31.1.103 host 64.101.255.254
 deny icmp host 172.31.1.103 host 64.103.255.254
 permit ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
```

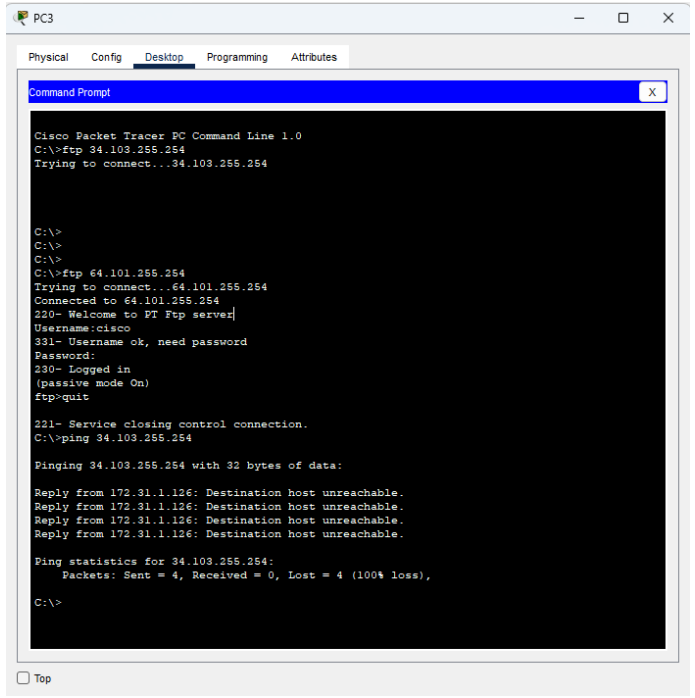
Copy | Paste

Top

2. DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

Parte 2: Aplicar y verificar la ACL Extendida





PASO 1: APLICAR LA ACL A LA INTERFAZ APROPIADA EN EL SENTIDO CORRECTO.

PASO 2: PRUEBA EL ACCESO PARA CADA PC.

RT1

Physical | Config | CLI | Attributes

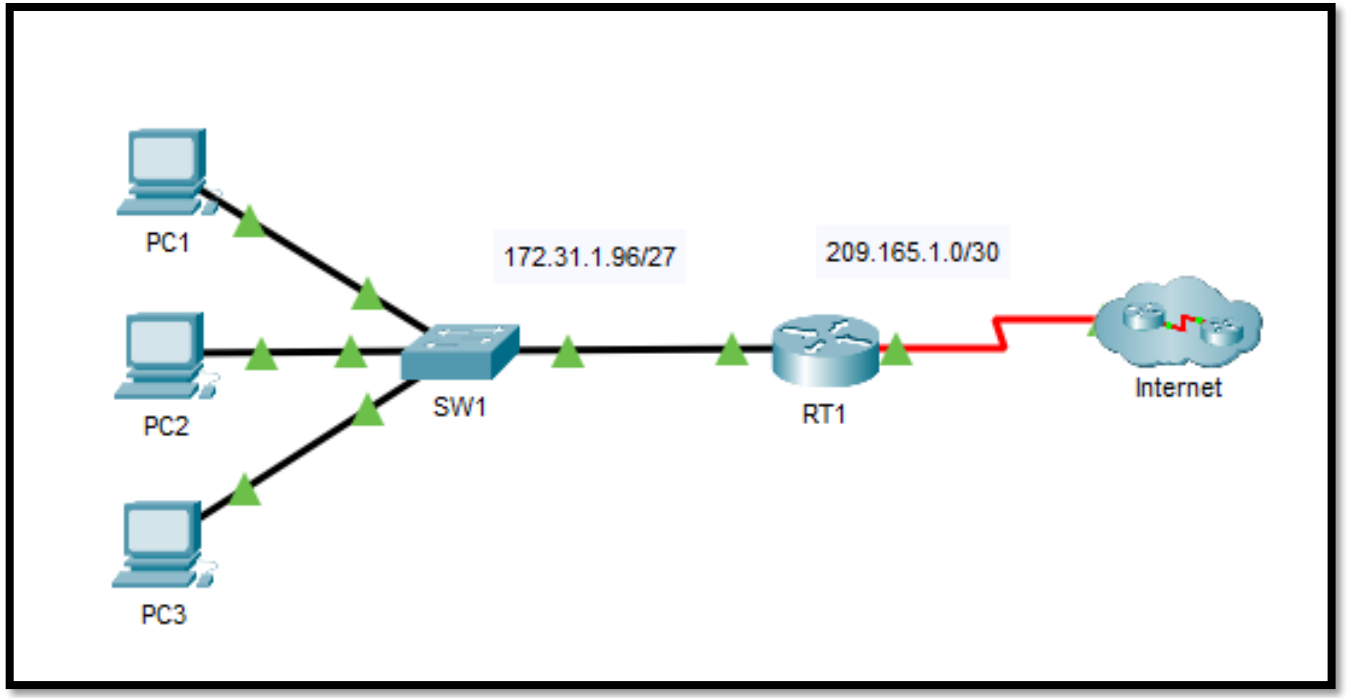
IOS Command Line Interface

```
end


RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
RT1(config-ext-nacl)#exit
RT1(config)#int g0/0
RT1(config-if)#ip access-group CL
% Incomplete command.
RT1(config-if)#ip access-group ACL
% Incomplete command.
RT1(config-if)#ip access-group ACL in
RT1(config-if)#do show access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (28 match(es))
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any

RT1(config-if)#do show access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (28 match(es))
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any (66 match(es))

RT1(config-if)#
```

Copy | Paste

Top

3.ESQUEMA GENERAL



4.SCRIPT CTC

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
RT1	G0/0	172.31.1.126	255.255.255.224	N/D
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Servidor1	NIC	64.101.255.254		
Servidor2	NIC	64.103.255.254		

5. PRUEBAS

RT1

Physical Config CLI Attributes

IOS Command Line Interface

```
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 172.31.1.126 255.255.255.224
 ip access-group ACL in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 209.165.1.2 255.255.255.252
 clock rate 4000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.31.1.96 0.0.0.31 area 0
 network 209.165.1.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended ACL
 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
 deny icmp host 172.31.1.103 host 64.101.255.254
 deny icmp host 172.31.1.103 host 64.103.255.254
 permit ip any any
!
!
```

Copy Paste

Top