

TRABAJO N.º 2 CISCO

7.2.6. CONFIGURE LOCAL AAA FOR CONSOLE AND VTY ACCESS-ILM

Esta configuración establece un usuario y una contraseña locales, activa la autenticación para la línea de consola y las líneas VTY, utiliza la autenticación local como predeterminada, y permite el acceso exclusivo a través de SSH para las líneas VTY.

Objectives

- Configure a local user and password.
- Verify local AAA configuration.

Background / Scenario

The network topology is shown in the diagram. You will create a local user account on the routers.

The routers have the following configuration:

- Enable secret passwords.
- OSPF routing.

Note: The console and VTY lines are configured for local authentication.

Note: Newer IOS images use MD5 for password storage.

Configuration for R1:

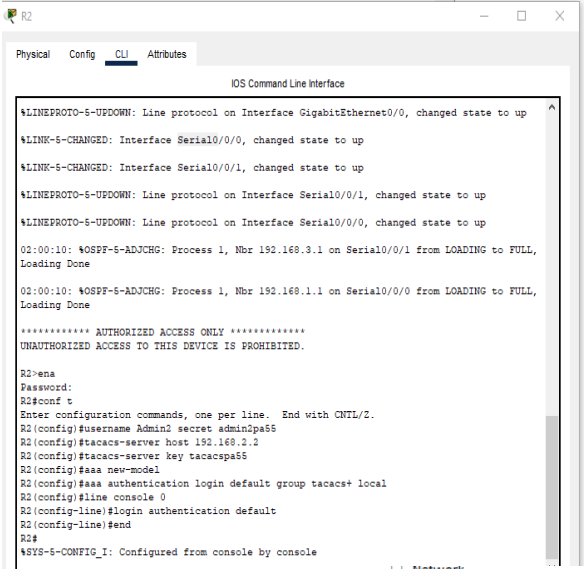
```
R1>enable
R1#config terminal
R1(config)#username Admin1 secret admin1pa55
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#ip domain-name netsec.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.netsec.com
R1(config)#aaa authentication login SSH-LOGIN local
R1(config)#line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
sSIS-S-CONFIG_I: Configured from console by console
```

Configuration Status for R1:

Category	Item	Status	Count	Type
AAA	Authentication			
	✓ Authn Command 1	Correct	1	Other
	✓ Authn Command 2	Correct	1	Other
Console Line	✓ AAA Method List Name	Correct	1	Other
	✓ IP Domain Name	Correct	1	Other
VTY Lines	VTY Line 0			
	✓ AAA Method List Name	Correct	1	Other
	✓ Transport Input	Correct	1	Physical
	VTY Line 1			
	✓ AAA Method List Name	Correct	1	Other
✓ Transport Input	Correct	1	Physical	
VTY Line 2				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 3				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 4				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	

7.4.9. CONFIGURE SERVER-BASED AUTHENTICATION WITH TACACS+ AND RADIUS – ILM

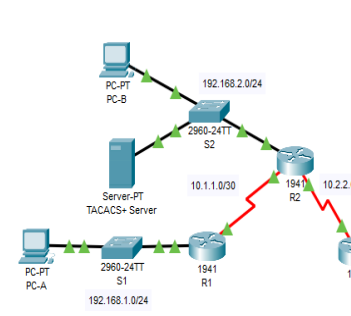
En el enrutador R2 se configura la autenticación usando TACACS+ como primera opción y luego la autenticación local, mientras que en el enrutador R3 se configura la autenticación usando RADIUS como primera opción y luego la autenticación local. Esto permite una redundancia de autenticación en caso de que los servidores remotos no estén disponibles.

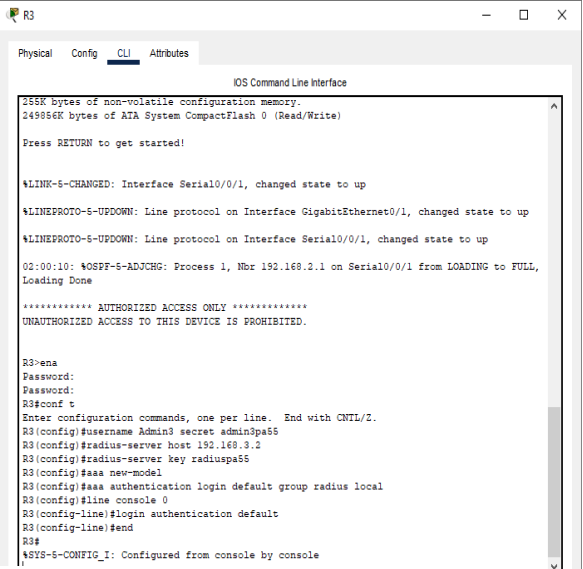


```

R2>enable
R2#configure terminal
R2(config)#username Admin2 secret admin2pa55
R2(config)#tacacs-server host 192.168.2.3
R2(config)#tacacs-server key tacacspa55
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#line console 0
R2(config-line)#login authentication default
R2(config-line)#end
R2#
$SYS-S-CONFIG_I: Configured from console by console

```





```

R3>enable
R3#configure terminal
R3(config)#username Admin3 secret admin3pa55
R3(config)#radius-server host 192.168.3.3
R3(config)#radius-server key radiuspa55
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#end
R3#
$SYS-S-CONFIG_I: Configured from console by console

```

Ctrl+F6 to exit CLI focus

Network	Configuration Item	Status	Count	Other
R2	AAA		0	Other
	Authentication		0	Other
	Authen Command 1	Correct	1	Other
	New-model	Correct	1	Other
	Console Line		0	Other
R3	AAA		0	Other
	Authentication		0	Other
	Authen Command 1	Correct	1	Other

8.5.5. CONFIGURE NAMED STANDARD IPV4 ACLS –ILM

esta configuración establece una lista de control de acceso que permite el tráfico hacia dos hosts específicos y bloquea todo el otro tráfico saliente a través de la interfaz FastEthernet 0/1 en el enrutador R1.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

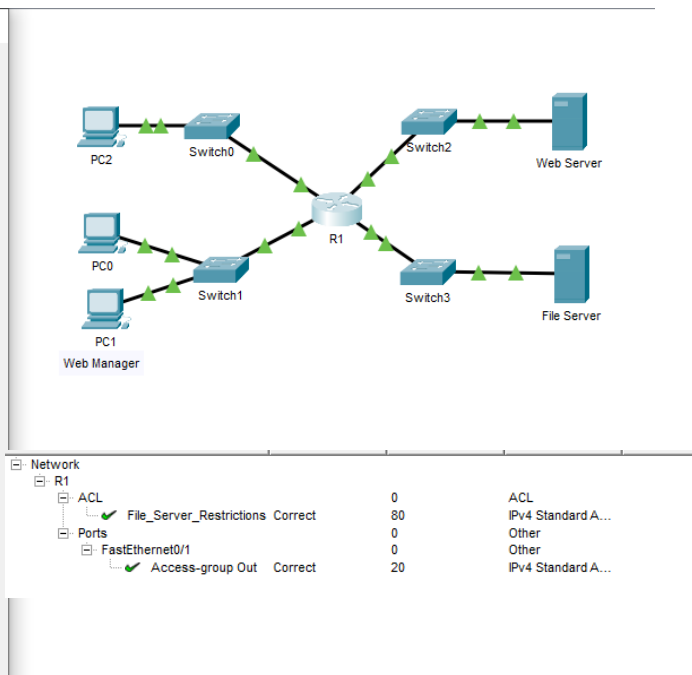
2 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
32768K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 16-May-06 14:54 by pt_team

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0, changed state to up

R1>ena
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
R1(config-std-nacl)#interface f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#end
R1#
*SYS-5-CONFIG_I: Configured from console by console

```



8.5.6. CONFIGURE NUMBERED STANDARD IPV4 ACLS –ILM

ambos enrutadores se están aplicando una ACL numerada en la interfaz de salida GigabitEthernet0/0. Estas ACLs bloquean todo el tráfico saliente de una subred específica (192.168.11.0/24 en R2 y 192.168.10.0/24 en R3), permitiendo cualquier otro tráfico saliente que no pertenezca a esas subredes.

```

R2
CLI
IOS Command Line Interface

2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249956K 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
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-S-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency
%DUAL-S-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R2>ena
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#end
R2#
*SYS-5-CONFIG_I: Configured from console by console

```

```

R3
CLI
IOS Command Line Interface

2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249956K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-S-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.1 (Serial0/0/1) is up: new adjacency
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-S-NBRCHANGE: IP-EIGRP 100: Neighbor 10.3.3.1 (Serial0/0/0) is up: new adjacency

R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#end
R3#
*SYS-5-CONFIG_I: Configured from console by console

```

Network					
R2	ACL	1	Correct	0	ACL
	Ports			25	IPv4 Standard A...
	GigabitEthernet0/0			0	Other
		Access-group Out	Correct	0	Other
				25	IPv4 Standard A...
R3	ACL	1	Correct	0	ACL
	Ports			25	IPv4 Standard A...
	GigabitEthernet0/0			0	Other
		Access-group Out	Correct	0	Other
				25	IPv4 Standard A...

8.5.12. CONFIGURE EXTENDED ACLS-ESCENARIO 1 –ILM

estas ACLs permiten diferentes tipos de tráfico (FTP, ICMP, HTTP) desde diferentes rangos de direcciones IP hacia destinos específicos en las interfaces designadas del enrutador R1.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Cisco IOS XE 3.17.1 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
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
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

R1>ena
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#interface gigabitEthernet 0/1
R1(config-if)#ip access-group HTTP_ONLY in
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Network	Status	Count	Component(s)
ACL			
100	Correct	40	IPv4 Extended A...
HTTP_ONLY	Correct	40	IPv4 Extended A...
Ports			
GigabitEthernet0/0		0	Other
Access-group In	Correct	10	IPv4 Extended A...
GigabitEthernet0/1		0	Other
Access-group In	Correct	10	IPv4 Extended A...

8.5.13. CONFIGURE EXTENDED ACLS-ESCENARIO 2 –ILM

esta ACL permite un amplio tráfico IP pero deniega específicamente ciertos tipos de tráfico desde determinados hosts hacia destinos específicos en los puertos FTP, HTTP, HTTPS, y también el tráfico ICMP entre ciertos pares de hosts y destinos en la interfaz GigabitEthernet0/0 del enrutador RT1.

Physical Config **CLI** Attributes

IOS Command Line Interface

```

BRAN 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

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

RT1>ena
RT1#configure terminal
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 www
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 www
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
RT1(config-ext-nacl)#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)#permit ip any any
RT1(config-ext-nacl)#interface GigabitEthernet0/0
RT1(config-if)#ip access-group ACL in
RT1(config-if)#end
RT1#
%SYS-5-CONFIG_I: Configured from console by console

```

Ctrl+F6 to exit CLI focus

Copy Paste

Network

- RT1
 - ACL
 - ACL: Correct, 80, IPv4 Extended A...
 - Ports
 - GigabitEthernet0/0
 - Access-group In: Correct, 20, IPv4 Extended A...

8.6.5. CONFIGURE IP ACLS TO MITIGATE ATTACKS – ILM

estas configuraciones están diseñadas para permitir o denegar tipos específicos de tráfico en las interfaces correspondientes para mitigar ciertos ataques, controlar el acceso a través de las líneas virtuales y restringir el tráfico desde redes específicas en los diferentes routers.

```

% Invalid input detected at '^' marker.

R1>access-list 120 permit ip any any
% Invalid input detected at '^' marker.

R1>ena
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit host 192.168.3.3
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

Ctrl+F6 to exit CLI focus

Copy Paste

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
2 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!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

User Access Verification

Password:

R2>ena
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit host 192.168.3.3
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

R3

Physical

Config

CLI

Attributes

IOS Command Line Interface

LINK-3-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification

Password:

R3>ena

Password:

R3#config t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#access-list 10 permit host 192.168.3.3

R3(config)#line vty 0 4

R3(config-line)#access-class 10 in

R3(config-line)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3

R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any

R3(config)#access-list 100 permit ip any

% Incomplete command.

R3(config)#interface s0/0/1

R3(config-if)#ip access-group 100 in

R3(config-if)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any

R3(config)#interface g0/1

R3(config-if)#ip access-group 110 in

R3(config-if)#end

R3#

%SYS-5-CONFIG_I: Configured from console by console

Ctrl+F6 to exit CLI focus

Copy

Paste

Network					
R1	ACL	10	Correct	1	ACL
		120	Correct	1	ACL
	Ports	Serial0/0/0		0	Other
		Access-group In	Correct	1	ACL
	VTY Lines	VTY Line 0		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 1		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 2		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 3		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 4		0	Other
		Access Control In	Correct	1	ACL
R2	ACL	10	Correct	0	ACL
				1	ACL
	VTY Lines	VTY Line 0		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 1		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 2		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 3		0	Other
		Access Control In	Correct	1	ACL
R3	ACL	10	Correct	1	ACL
		100	Incorrect	1	ACL
		110	Correct	1	ACL
	Ports	GigabitEthernet0/1		0	Other
		Access-group In	Correct	1	ACL
	Serial0/0/1			0	Other
		Access-group In	Correct	1	ACL
	VTY Lines	VTY Line 0		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 1		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 2		0	Other
		Access Control In	Correct	1	ACL
		VTY Line 3		0	Other
		Access Control In	Correct	1	ACL