SOLUCIONARIO

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

```
Router R1
enable
config terminal
username Admin1 secret admin1pa55
aaa new-model
aaa authentication login default local
line console 0
login authentication default
ip domain-name netsec.com
crypto key generate rsa general-keys modulus 1024
aaa authentication login SSH-LOGIN local
line vty 0 4
login authentication SSH-LOGIN
transport input ssh
```

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

```
Router R2
conf t
username Admin2 secret admin2pa55
tacacs-server host 192.168.2.2
tacacs-server key tacacspa55
aaa new-model
aaa authentication login default group tacacs+ local
line console 0
 login authentication default
```

```
Router R3
conf t
username Admin3 secret admin3pa55
radius-server host 192.168.3.2
radius-server key radiuspa55
aaa new-model
aaa authentication login default group radius local
line console 0
login authentication default
```

8.1.5. ACL DEMONSTRATION – ILM

TEORIA

8.5.5. CONFIGURE NAMED STANDARD IPV4 ACLS –ILM

```
Router R1
enable
configure terminal
ip access-list standard File_Server_Restrictions
 permit host 192.168.20.4
 permit host 192.168.100.100
 deny any
interface f0/1
 ip access-group File_Server_Restrictions out
```

8.5.6. CONFIGURE NUMBERED STANDARD IPV4 ACLS –ILM

```
Router R2
enable
configure terminal
interface GigabitEthernet0/0
 ip access-group 1 out
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
end

Router R3
enable
configure terminal
interface GigabitEthernet0/0
 ip access-group 1 out
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
end
```

8.5.12. CONFIGURE EXTENDED ACLS-ESCENARIO 1 –ILM

```
Router R1
enable
configure terminal
access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
interface gigabitEthernet 0/0
 ip access-group 100 in
ip access-list extended HTTP_ONLY
 permit tcp 172.22.34.96 0.0.0.15
 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
interface gigabitEthernet 0/1
ip access-group HTTP_ONLY in
```

8.5.13. CONFIGURE EXTENDED ACLS-ESCENARIO 2 –ILM

```
Router RT1
enable
configure terminal
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
interface GigabitEthernet0/0
 ip access-group ACL in
end
```

8.6.5. CONFIGURE IP ACLS TO MITIGATE ATTACKS – ILM

```
Router R1
access-list 10 permit host 192.168.3.3
line vty 0 4
 access-class 10 in
access-list 120 permit udp any host 192.168.1.3 eq domain
access-list 120 permit tcp any host 192.168.1.3 eq smtp
access-list 120 permit tcp any host 192.168.1.3 eq ftp
access-list 120 deny tcp any host 192.168.1.3 eq 443
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
interface s0/0/0
 ip access-group 120 in
access-list 120 permit icmp any any echo-reply
access-list 120 permit icmp any any unreachable
access-list 120 deny icmp any any
access-list 120 permit ip any any

Router R2
access-list 10 permit host 192.168.3.3
line vty 0 4
 access-class 10 in

Router R3
access-list 10 permit host 192.168.3.3
line vty 0 4
 access-class 10 in
access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit ip any
interface s0/0/1
 ip access-group 100 in
access-list 110 permit ip 192.168.3.0 0.0.0.255 any
interface g0/1
 ip access-group 110 in
```

8.7.4. CONFIGURE IPV6 ACLS –ILM

```
Router R1
enable
config t
ipv6 access-list BLOCK_HTTP
 deny tcp any host 2001:db8:1:30::30 eq www
 deny tcp any host 2001:db8:1:30::30 eq 443
 permit ipv6 any any
interface GigabitEthernet0/1
 ipv6 traffic-filter BLOCK_HTTP in
end

Router R3
enable
config t
ipv6 access-list BLOCK_ICMP
```

```
 deny icmp any any
 permit ipv6 any any
interface GigabitEthernet0/0
 ipv6 traffic-filter BLOCK_ICMP out
end
```

9.2.4 IDENTIFY PACKET FLOW – ILM

TEORIA

10.3.11. CONFIGURE A ZPF – ILM

```
Router R3
enable
config terminal
zone security IN-ZONE
zone security OUT-ZONE
access-list 101 permit ip 192.168.3.0 0.0.0.255 any
class-map type inspect match-all IN-NET-CLASS-MAP
match access-group 101
policy-map type inspect IN-2-OUT-PMAP
class type inspect IN-NET-CLASS-MAP
inspect
zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
service-policy type inspect IN-2-OUT-PMAP
interface GigabitEthernet0/1
zone-member security IN-ZONE
interface Serial0/0/1
zone-member security OUT-ZONE
end
```

11.4.6. IMPLEMENT A LOCAL SPAN – ILM

```
Switch S1
enable
config terminal
monitor session 1 source interface f0/5
monitor session 1 destination interface f0/6
end
```

14.3.11. IMPLMENT PORT SECURITY –ILM

```
Switch S1
enable
config t
interface range f0/1 - 2
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation restrict
interface range f0/3 - 24, g0/1 - 2
 shutdown
end
```

14.8.10. INVESTIGATE STP LOOP PREVENTION – ILM

TEORIA

14.9.10. IMPLEMENT STP SECURITY – ILM

```
Central
spanning-tree vlan 1 root primary
SW-1
spanning-tree vlan 1 root secondary
interface range f0/23 - 24
 spanning-tree guard root
SW-2
interface range f0/23 - 24
 spanning-tree guard root
SW-A
interface range f0/1 - 4
 spanning-tree portfast
 spanning-tree bpduguard enable
SW-B
interface range f0/1 - 4
 spanning-tree portfast
 spanning-tree bpduguard enable
end of document
```

14.9.11. LAYER 2 VLAN SECURITY – ILM

```
SW-1
conf t
interface f0/23
 switchport mode trunk
 switchport trunk native vlan 15
 switchport nonegotiate
 no shutdown
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.3 255.255.255.0
SW-2
conf t
interface f0/23
 switchport mode trunk
 switchport trunk native vlan 15
 switchport nonegotiate
 no shutdown
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.4 255.255.255.0
SW-A
conf t
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
interface f0/1
 switchport access vlan 20
 no shutdown
SW-B
conf t
vlan 20
```

```
 exit
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
Central
conf t
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.5 255.255.255.0
R1
conf t
interface GigabitEthernet0/0.1
 ip access-group 101 in
interface GigabitEthernet0/0.2
 ip access-group 101 in
interface g0/0.3
 encapsulation dot1q 20
 ip address 192.168.20.100 255.255.255.0
access-list 101 deny ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
access-list 102 permit ip host 192.168.20.50 any
line vty 0 4
 access-class 102 in
end of document
```

19.5.5. CONFIGURE AND VERIFY A SITE-TO-SITE IRSEC VPN –ILM

```
Router R1
config t
license boot module c1900 technology-package securityk9
yes
end
copy running-config startup-config
reload
config t
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
 exit
crypto isakmp key vpnpa55 address 10.2.2.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to R3
 set peer 10.2.2.2
 set transform-set VPN-SET
 match address 110
 exit
interface S0/0/0
 crypto map VPN-MAP
Router R3
config t
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
 exit
crypto isakmp key vpnpa55 address 10.1.1.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to R1
 set peer 10.1.1.2
 set transform-set VPN-SET
 match address 110
 exit
interface S0/0/1
 crypto map VPN-MAP
```

21.7.5. CONFIGURE ASA BASIC SETTINGS AND FIREWALL USING THE CLI –ILM

```
ASA 5506-X
enable
!<Enter> for password
conf t
hostname NETSEC-ASA
domain-name netsec.com
enable password ciscoenpa55
clock set 21:31:57 November 27 2023
interface g1/2
 nameif INSIDE
 ip address 192.168.1.1 255.255.255.0
 security-level 100
 no shutdown
interface g1/1
 nameif OUTSIDE
 ip address 209.165.200.226 255.255.255.248
 security-level 0
 no shutdown
route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
dhcpd address 192.168.1.5-192.168.1.36 INSIDE
dhcpd dns 209.165.201.2 interface INSIDE
dhcpd enable INSIDE
username admin password adminpa55
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 1024
no
ssh 192.168.1.0 255.255.255.0 INSIDE
ssh 172.16.3.3 255.255.255.255 OUTSIDE
ssh timeout 10
interface g1/3
 ip address 192.168.2.1 255.255.255.0
 nameif DMZ
 security-level 70
 no shutdown
object network DMZ-SERVER
 host 192.168.2.3
 nat (DMZ,OUTSIDE) static 209.165.200.227
```

```
access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
access-group OUTSIDE-DMZ in interface OUTSIDE
```

PC-B

-Change from static to DHCP addressing