Laboratorium - Konfiguracja i weryfikacja rozszerzonych list ACL IPv4

Topologia

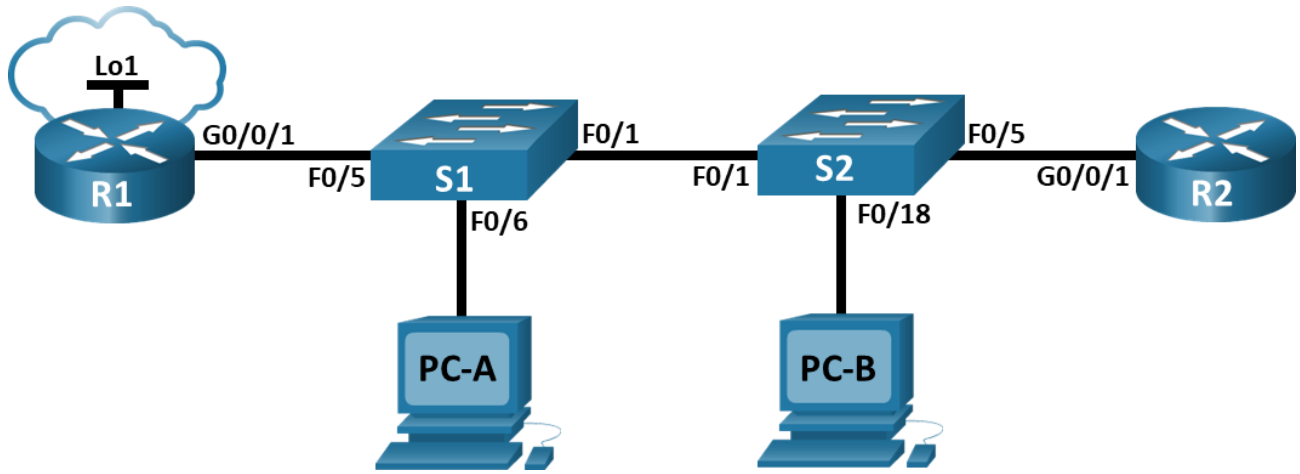

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/1	nd.	nd.	nd.
	G0/0/1.20	10.20.0.1	255.255.255.0	
	G0/0/1.30	10.30.0.1	255.255.255.0	
	G0/0/1.40	10.40.0.1	255.255.255.0	
	G0/0/1.1000	nd.	nd.	
	Loopback 1	172.16.1.1	255.255.255.0	
R2	G0/0/1	10.20.0.4	255.255.255.0	nd.
S1	VLAN 20	10.20.0.2	255.255.255.0	10.20.0.1
S2	VLAN 20	10.20.0.3	255.255.255.0	10.20.0.1
PC-A	Karta sieciowa	10.30.0.10	255.255.255.0	10.30.0.1
PC-B	Karta sieciowa	10.40.0.10	255.255.255.0	10.40.0.1

Tabela VLAN

VLAN	Nazwa	Przypisany interfejs
20	Management	S2: F0/5

VLAN	Nazwa	Przypisany interfejs
30	Operations	S1: F0/6
40	Sales	S2: F0/18
999	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2
1000	Native	nd.

Cele

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Część 2: Konfigurowanie i weryfikacja rozszerzonych list kontroli dostępu

Wprowadzenie / Scenariusz

Otrzymałeś zadanie skonfigurowania list kontroli dostępu w sieci małej firmy. ACL są jednym z najprostszych i najbardziej bezpośrednich sposobów kontrolowania ruchu w warstwie 3. R1 będzie obsługiwać połączenie internetowe (symulowane przez interfejs Loopback 1) i udostępnianie trasie domyślnej routerowi R2. Po zakończeniu konfiguracji początkowej firma ma określone wymagania bezpieczeństwa ruchu, które są odpowiedzialne za wdrożenie.

Uwaga: Routery używane w praktycznych laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.4 (obraz universalk9). Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.2 (2) (obraz lanbasek9). Można używać Innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, że konfiguracje startowe routerów i przełączników zostały wykasowane. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane zasoby

- 2 routery (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalny)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.2(2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco IOS za pośrednictwem portów konsoli
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Zbuduj sieć i skonfiguruj podstawowe ustawienia urządzeń.

Krok 1: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable tak, jak pokazano na schemacie topologii.

Krok 2: Skonfiguruj podstawowe ustawienia dla każdego routera.

a. Przypisz routerowi nazwę.

```
router(config)# hostname R1
```

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

```
R1(config)# no ip domain lookup
```

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

```
R1(config)# enable secret class
```

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
```

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

f. Zaszyfruj hasła zapisane jawnym tekstem.

```
R1(config)# service password-encryption
```

g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

```
R1(config)# banner motd $ Authorized Users Only! $
```

h. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

```
R1# copy running-config startup-config
```

Krok 3: Wykonaj podstawową konfigurację przełączników.

a. Przypisz nazwę urządzenia do przełącznika.

```
switch(config)# hostname S1
```

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

```
S1(config)# no ip domain-lookup
```

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

```
S1(config)# enable secret class
```

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
```

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
```

f. Zaszyfruj hasła zapisane jawnym tekstem.

```
S1(config)# service password-encryption
```

g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

```
S1(config)# banner motd $ Authorized Users Only! $
```

h. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

```
S1(config)# exit
S1# copy running-config startup-config
```

Część 2: Konfiguracja sieci VLAN na przełącznikach.

Krok 1: Utwórz sieci VLAN na przełączniku.

a. Utwórz i nazwij wymagane sieci VLAN na każdym przełączniku z powyższej tabeli.

```
S1(config)# vlan 20
S1(config-vlan)# name Management
S1(config-vlan)# vlan 30
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 40
S1(config-vlan)# name Sales
S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# exit

S2(config)# vlan 20
S2(config-vlan)# name Management
S2(config-vlan)# vlan 30
S2(config-vlan)# name Operations
S2(config-vlan)# vlan 40
S2(config-vlan)# name Sales
S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot
S2(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S2(config-vlan)# exit
```

b. Skonfiguruj interfejs zarządzania i bramę domyślną na każdym przełączniku, korzystając z informacji o adresie IP z tabeli adresowania.

```
S1(config)# interface vlan 20
S1(config-if)# ip address 10.20.0.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 10.20.0.1
S1(config)# end

S2(config)# interface vlan 20
```

```
S2(config-if)# ip address 10.20.0.3 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 10.20.0.1
S2(config)# end
```

c. Przypisz wszystkie nieużywane porty przełącznika do sieci VLAN ParkingLot, skonfiguruj je w trybie dostępu statycznego i dezaktywuj je administracyjnie.

Uwaga: Polecenie interface range jest pomocne, aby wykonać to zadanie z minimalną koniecznych poleceń.

```
S1(config)# interface range f0/2 - 4, f0/7 - 24, g0/1 - 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S1(config-if-range)# end

S2(config)# interface range f0/2 - 17, f0/19 - 24, g0/1 - 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
S2(config-if-range)# end
```

Krok 2: Przypisz sieci VLAN do odpowiednich interfejsów przełącznika.

a. Przypisz używane porty do odpowiedniej sieci VLAN (określonej w powyższej tabeli VLAN) i skonfiguruj je w trybie dostępu statycznego.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 30

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 40
```

b. Wydaj polecenie **show vlan brief** i sprawdź, czy sieci VLAN są przypisane do odpowiednich interfejsów.

```
S1# show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/5
10 Management active
20 Sales active Fa0/6
30 Operations active
999 ParkingLot active Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
```

```
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
S2# show vlab brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1
10 Management active
30 Operations active
40 Sales active Fa0/18
999 ParkingLot active Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
```

Część 3: Konfiguracja połączeń trunk

Krok 1: Ręcznie skonfiguruj interfejs trunk F0/1.

a. Zmień tryb przełączania na interfejsie F0/1, aby wymusić trunking. Pamiętaj, aby to zrobić na obu przełącznikach.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk

S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

b. W ramach konfiguracji łącza trunk ustaw natywną sieć jako VLAN 1000 na obu przełącznikach. Komunikaty o błędach mogą być tymczasowo wyświetlane, gdy oba interfejsy są skonfigurowane z różnymi natywnymi sieciami VLAN.

```
S1(config-if)# switchport trunk native vlan 1000

S2(config-if)# switchport trunk native vlan 1000
```

c. W ramach innej części konfiguracji łącza trunk określ, że tylko sieci VLAN 10, 20, 30 i 1000 mogą korzystać z łącza.

```
S1(config-if)# switchport trunk allowed vlan 20,30,40,1000

S2(config-if)# switchport trunk allowed vlan 20,30,40,1000
```

d. Wydaj polecenie **show interfaces trunk**, aby zweryfikować porty trunk, natywną sieć VLAN i dozwolone sieci VLAN na łączu trunk.

```
S1# show interfaces trunk

Port Mode Encapsulation Status Native vlan
```

```
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain
Fa0/1 20,30,40,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 20,30,40,1000

S2# show interface trunk

Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain
Fa0/1 30,40,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 30,40
```

Krok 2: Ręcznie skonfiguruj interfejs trunk F0/5 na S1.

a. Skonfiguruj F0/5 na S1 z tymi samymi parametrami trunk co F0/1. To jest trunk do routera.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 1000
S1(config-if)# switchport trunk allowed vlan 20,30,40,1000
```

b. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

```
S1# copy running-config startup-config
```

c. Użyj polecenia **show interfaces trunk**, aby sprawdzić ustawienia trunk.

Część 4: Konfiguracja routingu

Krok 1: Skonfiguruj routing między sieciami VLAN na R1.

a. Aktywuj interfejs G0/0/1 na routerze.

```
R1(config)# interface g0/0/1
R1(config-if)# no shutdown
```

b. Skonfiguruj podinterfejsy dla każdej sieci VLAN zgodnie z tabelą adresowania IP. Wszystkie podinterfejsy używać będą enkapsulacji 802.1Q. Upewnij się, że podinterfejs dla natywnej sieci VLAN nie ma przypisanego adresu IP. Dołącz opis dla każdego podinterfejsu.

```
R1(config)# interface g0/0/1.20
R1(config-subif)# description Management Network
```

```
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 10.20.0.1 255.255.255.0
R1(config-subif)# interface g0/0/1.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# description Operations Network
R1(config-subif)# ip address 10.30.0.1 255.255.255.0
R1(config-subif)# interface g0/0/1.40
R1(config-subif)# encapsulation dot1q 40
R1(config-subif)# description Sales Network
R1(config-subif)# ip address 10.40.0.1 255.255.255.0
R1(config-subif)# interface g0/0/1.1000
R1(config-subif)# encapsulation dot1q 1000 native
R1(config-subif)# description Native VLAN
```

c. Skonfiguruj interfejs Loopback 1 na R1 z adresowaniem z powyższej tabeli.

```
R1(config)# interface Loopback 1
R1(config-if)# ip address 172.16.1.1 255.255.255.0
```

d. Użyj polecenia **show ip interface brief**, aby sprawdzić, czy podinterfejsy działają.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES unset administratively down down
GigabitEthernet0/0/1 unassigned YES unset up up
Gi0/0/1.20 10.20.0.1 YES manual up up
Gi0/0/1.30 10.30.0.1 YES manual up up
Gi0/0/1.40 10.40.0.1 YES manual up up
Gi0/0/1.1000 unassigned YES unset up up
Serial0/1/0 unassigned NO unset down down
Serial0/1/1 unassigned NO unset down down
GigabitEthernet0 unassigned YES unset administratively down down
Loopback1 172.16.1.1 YES manual up up
```

Krok 2: Skonfiguruj interfejs g0/0/1 R2 przy użyciu adresu z tabeli i domyślnej trasy z następnym przeskokiem 10.20.0.1

```
R2(config)# interface g0/0/1
R2(config-if)# ip address 10.20.0.4 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 10.20.0.1
```

Część 5: Konfiguracja zdalnego dostępu

Krok 1: Skonfiguruj wszystkie urządzenia sieciowe do podstawowej obsługi SSH.

a. Utwórz lokalnego użytkownika z nazwą użytkownika SSHadmin i zaszyfrowanym hasłem $cisco123!

```
R1(config)# username SSHadmin secret $cisco123!
```

b. Użyj **ccna-lab.com** jako nazwy domeny.

```
R1(config)# ip domain name ccna-lab.com
```

c. Wygeneruj zestaw kluczy kryptograficznych o module 1024-bitowym.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

d. Skonfiguruj pierwsze pięć wierszy VTY na każdym urządzeniu, aby obsługiwały tylko połączenia SSH i uwierzytelniały się w lokalnej bazie danych użytkowników.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
```

Krok 2: Włącz bezpieczne, uwierzytelnione usługi internetowe na R1.

a. Włącz serwer HTTPS na R1.

```
R1(config)# ip http secure-server
```

b. Skonfiguruj R1, aby uwierzytelniać użytkowników próbujących połączyć się z serwerem WWW.

```
R1(config)# ip http authentication local
```

Część 6: Weryfikacja łączności

Krok 1: Skonfiguruj hosty PC.

Skonfiguruj adresy IP na komputerach zgodnie z tabelą adresacji.

Krok 2: Wykonaj następujące testy. Wszystkie powinny się powieść.

Uwaga: Aby ping zakończył się pomyślnie, może być konieczne wyłączenie zapory ogniowej komputera.

Od	Protokół	Cel
PC-A	Ping	10.40.0.10
PC-A	Ping	10.20.0.1
PC-B	Ping	10.30.0.10
PC-B	Ping	10.20.0.1
PC-B	Ping	172.16.1.1
PC-B	HTTPS	10.20.0.1
PC-B	HTTPS	172.16.1.1
PC-B	SSH	10.20.0.1
PC-B	SSH	172.16.1.1

Część 7: Konfigurowanie i weryfikacja rozszerzonych list kontroli dostępu.

Po zweryfikowaniu podstawowej łączności firma wymaga wdrożenia następujących zasad zabezpieczeń:

Zasada 1: Sieć Sales nie może łączyć się przez SSH z siecią Management (ale inne protokoły SSH są dozwolone).

Zasada 2: Sieć Sales nie może uzyskać dostępu do adresów IP w sieci Management przy użyciu żadnego protokołu internetowego (HTTP/HTTPS). Sieć Sales nie ma również dostępu do interfejsów R1 za pomocą

dowolnego protokołu www. Dozwolony jest cały inny ruch www (uwaga — Sales może uzyskać dostęp do interfejsu Loopback 1 na R1).

Zasada 3: Sieć Sales nie może wysyłać żądań echo ICMP do sieci Operations lub Management. Dozwolone są żądania echa ICMP do innych miejsc docelowych.

Zasada 4: Sieć Operations nie może wysyłać żądań echo ICMP do sieci Sales. Dozwolone są żądania echo ICMP do innych miejsc docelowych.

Krok 1: Przeanalizuj sieć i wymagania polityki bezpieczeństwa, aby zaplanować implementację listy ACL.

Odpowiedzi mogą się różnić. Wymienione powyżej wymagania wymagają wdrożenia dwóch rozszerzonych list dostępu. Zgodnie z wskazówkami umieszczania rozszerzonych list dostępu jak najbliżej źródła ruchu, który ma być filtrowany, te listy ACL będą działać na interfejsach G0/0/0.30 i G0/0/0.40.

Krok 2: Opracuj i zastosuj rozszerzone listy dostępu, które będą zgodne z oświadczeniami dotyczącymi zasad bezpieczeństwa.

Odpowiedzi mogą się różnić. listy ACL powinny być podobne do następujących:

```
R1(config)# access-list 101 remark ACL 101 fulfills policies 1, 2, and 3
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 22
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 80
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq 80
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq 80
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 443
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq 443
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq 443
R1(config)# access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 echo
R1(config)# access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255 echo
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/0/1.40
R1(config-subif)# ip access-group 101 in

R1(config)# access-list 102 remark ACL 102 fulfills policy 4
R1(config)# access-list 102 deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 echo
R1(config)# access-list 102 permit ip any any
R1(config)# interface g0/0/1.30
R1(config-subif)# ip access-group 102 in
```

Krok 3: Sprawdź, czy zasady zabezpieczeń są wymuszane przez wdrożone listy dostępu.

Wykonaj następujące testy. Oczekiwane wyniki są przedstawione w tabeli:

Od	Protokół	Cel	Wynik
PC-A	Ping	10.40.0.10	Nie przeszedł
PC-A	Ping	10.20.0.1	Ukończono pomyślnie
PC-B	Ping	10.30.0.10	Nie przeszedł
PC-B	Ping	10.20.0.1	Nie przeszedł

PC-B	Ping	172.16.1.1	Ukończono pomyślnie
PC-B	HTTPS	10.20.0.1	Nie przeszedł
PC-B	HTTPS	172.16.1.1	Ukończono pomyślnie
PC-B	SSH	10.20.0.4	Nie przeszedł
PC-B	SSH	172.16.1.1	Ukończono pomyślnie

Konfiguracja urządzeń

Router R1

```
R1# show run
Building configuration...


Current configuration : 5264 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 $1$.Dkb$dhzFCwC9TtcbWur3lMEe10
!
no aaa new-model
!
no ip domain lookup
ip domain name ccna-lab.com
!
!
login on-success log
!
subscriber templating
!
```

```
multilink bundle-name authenticated
!
<output omitted>
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
username SSHadmin secret 5 $1$829R$mk6kzq/CCkw0irnUoa.tM1
!
redundancy
 mode none
!
!
interface Loopback1
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1.20
 description Management Network
 encapsulation dot1q 20
 ip address 10.20.0.1 255.255.255.0
!
interface GigabitEthernet0/0/1.30
 description Operations Network
 encapsulation dot1Q 30
 ip address 10.30.0.1 255.255.255.0
 ip access-group 102 in
!
interface GigabitEthernet0/0/1.40
 description Sales Network
 encapsulation dot1Q 40
 ip address 10.40.0.1 255.255.255.0
 ip access-group 101 in
!
interface GigabitEthernet0/0/1.1000
 description Native VLAN
 encapsulation dot1Q 1000 native
!
interface Serial0/1/0
 no ip address
```

```
!
interface Serial0/1/1
 no ip address
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
ip forward-protocol nd
no ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
!
!
ip access-list extended 101
 remark ACL 101 fulfills policies 1, 2, and 3
 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 22
 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq www
 deny tcp 10.40.0.0 0.0.0.255 host 10.30.0.1 eq www
 deny tcp 10.40.0.0 0.0.0.255 host 10.40.0.1 eq www
 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 443
 deny tcp 10.40.0.0 0.0.0.255 host 10.30.0.1 eq 443
 deny tcp 10.40.0.0 0.0.0.255 host 10.40.0.1 eq 443
 deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 echo
 deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255 echo
 permit ip any any
ip access-list extended 102
 remark ACL 102 fulfills policy 4
 deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 echo
 permit ip any any
!
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
 password 7 094F471A1A0A
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 14141B180F0B
 login local
 transport input ssh
!
```

```
end
```

Router R2

```
R2# show run
Building configuration...


Current configuration : 1660 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 $1$DKlp$gTX20dmMb.E9aCzmg74EY1
!
no aaa new-model
!
no ip domain lookup
ip domain name ccna-lab.com
!
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
username SSHadmin secret 5 $1$eGZ8$ltf/V6F6X90aLyQmlnyyk/
!
redundancy
```

```
 mode none
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 10.20.0.4 255.255.255.0
 negotiation auto
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
ip forward-protocol nd
no ip http server
ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 10.20.0.1
!
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
 password 7 02050D480809
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 070C285F4D06
 login local
 transport input ssh
!
end
```

Switch S1

```
S1# show run
```

```
Building configuration...

Current configuration : 3361 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$bRO6$r7VHZdiC7uKcY7PkQDRpT.
!
username SSHadmin secret 5 $1$fvd5$93v97uMBqbiGyyVm25yRO.
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
switchport trunk allowed vlan 20,30,40,1000
 switchport trunk native vlan 1000
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
```

```
 shutdown
!
interface FastEthernet0/5
 switchport trunk allowed vlan 20,30,40,1000
 switchport trunk native vlan 1000
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 999
 switchport mode access
 shutdown
```

```
!
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/19
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
```

```
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan20
 ip address 10.20.0.2 255.255.255.0
!
ip default-gateway 10.20.0.1
ip http server
ip http secure-server
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
 password 7 094F471A1A0A
 login
line vty 0 4
 password 7 094F471A1A0A
 login local
 transport input ssh
line vty 5 15
 password 7 094F471A1A0A
 login
!
end
```

Switch S2

```
S2# show run
Building configuration...

Current configuration : 3247 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S2
```

```
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$gA7R$4QXuHJCsrZgVzesdOvPUW.
!
username SSHadmin secret 5 $1$x0mr$SlSPhEU7XXlV8Hw1.bLd3.
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
switchport trunk allowed vlan 20,30,40,1000
 switchport trunk native vlan 1000
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
switchport access vlan 999
 switchport mode access
 shutdown
!
```

```
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 999
 switchport mode access
 shutdown
!
```

```
interface FastEthernet0/17
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface Vlan1
```

```
 no ip address
!
interface Vlan20
 ip address 10.20.0.3 255.255.255.0
!
ip default-gateway 10.20.0.1
ip http server
ip http secure-server
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
 password 7 030752180500
 login
line vty 0 4
 password 7 030752180500
 login local
 transport input ssh
line vty 5 15
 password 7 030752180500
 login
!
end
```