Ćwiczenie – Konfiguracja i weryfikacja ograniczeń dostępu na liniach VTY

.

Topologia

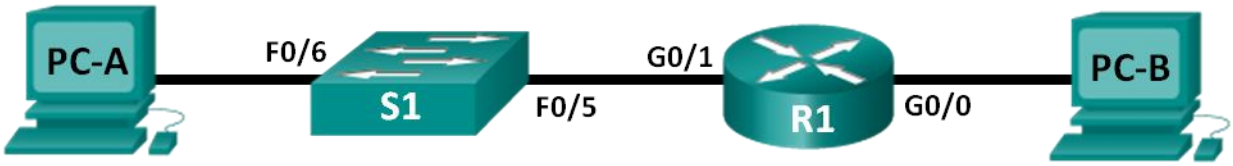

Tabela adresów

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Cele nauczania

Część 1: Podstawowa konfiguracja urządzeń

Część 2: Konfiguracja list kontroli dostępu na routerze R1

Część 3: Weryfikacja list kontroli dostępu przy użyciu protokołu Telnet

Część 4: Wyzwanie – Konfiguracja list kontroli dostępu na przełączniku S1

Wprowadzenie

Dobrą praktyką jest ograniczanie dostępu do interfejsów, przez które możliwe jest zarządzanie routerem np. Port konsolowy czy linie vty. Listy kontroli dostępu mogą być użyte do zezwolenia na ruch z konkretnych adresów IP, zapewniając, że tylko administrator ma dostęp do routera poprzez Telnet lub SSH.

Uwaga: W urządzeniach Cisco nazwy list ACL są skrócone do list dostępu.

Na tym laboratorium utworzysz i zastosujesz nazywane listy ACL w celu ograniczenia zdalnego dostępu do routera poprzez linie vty.

Po utworzeniu list ACL przetestujesz je i zweryfikujesz poprzez dostęp do routera przy użyciu protokołu Telnet z różnych adresów IP.

W tym laboratorium poznasz komendy niezbędne do utworzenia i zastosowania list ACL.

Uwaga: Preferowane routery to model Cisco 1941 Integrated Services Router (ISR) z systemem Cisco IOS Release 15.2(4)M3 (universalk9 image), natomiast przełączniki to model Cisco Catalyst 2960s z systemem Cisco IOS Release 15.0(2) (lanbasek9 image). Inne urządzenia i systemy mogą być również używane. W zależności od modelu i wersji IOS dostępne komendy mogą się różnić od prezentowanych w instrukcji

Uwaga: Upewnij się, że routery i przełączniku zostały wyczyszczone i nie posiadają konfiguracji startowej. Jeśli nie jesteś pewny/a wezwij instruktora**.**

Uwaga dla instruktorów: Procedury inicjalizacji i ponownego uruchomienia urządzeń znajdują się w instrukcji dla instruktorów.

Wymagane zasoby

- 1 router (Cisco 1941 z systemem Cisco IOS Release 15.2(4)M3 universal image lub kompatybilnym)
- 1 przełącznik (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image lub kompatybilnym)
- 2 komputery (Windows 7, Vista, lub XP z programem Putty lub innym programem terminalowym)
- Kabel konsolowy do konfiguracji urządzeń Cisco przez port konsolowy
- Kable sieciowe i serialowe pokazane na rysunku topologii

Uwaga: Na interfejsach gigabitowych routerów Cisco 1941 włączone jest autowykrywanie, dlatego też kabel prosty może być użyty do połączenia komputera z routerem. W przypadku innego routera może być konieczne użycie kabla z przeplotem.

Część 1: Podstawowa konfiguracja urządzeń

W części 1 zbudujesz sieć zgodnie z topologią i skonfigurujesz adresy IP na interfejsach, zdalny dostęp a także hasła.

Krok 1: Budowa sieci zgodnie z topologią.

Krok 2: Konfiguracja interfejsów sieciowych komputerów PC-A i PC-B zgodnie z tabelą adresów.

Krok 3: Inicjalizacja i ponowne uruchomienie routera i przełącznika.

a. Wyłącz niepożądane zapytania DNS (DNS lookup).

b. Skonfiguruj nazwy urządzeń zgodnie z topologią.

c. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC.

d. Ustaw **cisco** jako hasło do połączeń konsolowych i wymuś logowanie.

e. Ustaw **cisco** jako hasło do połączeń wirtualnych w celu uruchomienia dostępu przez Telnet i wymuś logowanie.

f. Włącz szyfrowanie haseł.

g. Ustaw baner MODT ostrzegający przed nieautoryzowanym dostępem.

h. Skonfiguruj adresy IP na interfejsach zgodnie z tabelą adresacji.

i. Ustaw bramę domyślną na przełączniku.

j. Zapisz bieżącą konfigurację urządzeń jako startową.

Część 2: Konfiguracja list kontroli dostępu na routerze R1

W części 2 skonfigurujesz standardową nazywaną listę ACL I zastosujesz ją do linii vty routera w celu ograniczenia zdalnego dostępu do routera.

Krok 1: Konfiguracja standardowej nazywanej listy ACL.

a. Zestaw połączenie konsolowe do routera R1 i wejdź do trybu uprzywilejowanego.

b. W trybie globalnej konfiguracji wyświetl opcje komendy **ip access-list** wpisując znak zapytania po spacji

```
R1(config)# ip access-list ?
  extended    Extended Access List
  helper      Access List acts on helper-address
```

```
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List
```

c. Wyświetl opcje komendy **ip access-list standard** wpisując znak zapytania po spacji.

```
R1(config)# ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
```

d. Dodaj **ADMIN-MGT** na końcu komendy **ip access-list standard** i naciśnij Enter. Jesteś teraz w trybie konfiguracji stnadardowej nazywanej listy dostepu (config-std-nacl).

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```

Wejdź do trybu zezwoleń lub zakazów listy kontroli dostępu ACE (access control entry) zwanym również oświadczeniem listy ACL. Pamiętaj, że na końcu listy znajduje się wpis **denny any,** który efektywnie blokuje cały ruch. Wpisz znak zapytania w celu wyświetlenia opcji komendy.

```
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

Utwórz wpis zezwalający na ruch od administratora PC-A (192.168.1.3) i dodatkowy wpis zezwalający na dostęp z adresów od 192.168.1.4 do 192.168.1.7. Zauważ, że pierwszy wpis dotyczy pojedynczego adresu poprzez użycie wpisu **host**. Zamiast tego można użyć komendy **permit 192.168.1.3 0.0.0.0.** Drugi wpis zezwala na ruch z adresów 192.168.1.4 do 192.168.1.7 poprzez użycie maski blankietowej 0.0.0.3, która jest odwróceniem maski sieciowej 255.255.255.252.

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

Nie ma potrzeby konfigurowania indywidulanych blokad, ponieważ na końcu listy znajduje się wpis **deny any**.

e. Przypisz utworzoną listę ACL do linii vty.

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

Część 3: Weryfikacja list kontroli dostępu przy użyciu protokołu Telnet

W części 3 użyjesz protokołu Telnet w celu zdalnego dostępu i weryfikacji, że utworzona lista działa poprawnie.

a. **Uwaga**: SSH jest bezpieczniejszy od Telnetu; jednakże SSH wymaga aby urządzenia sieciowe były odpowiednio skonfigurowane. Na tym laboratorium Telnet używany jest dla wygody.

b. Otwórz wiersz poleceń na komputerze PC-A i sprawdź czy mozliwa jest komunikacja z routerem przy użyciu polecenia **ping**.

```
C:\Users\user1> ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

c. Z komputera PC-A połącz się do routera R1 przy użyciu protokołu Telnet. Wejdź do trybu uprzywilejowanego po wpisaniu hasła. Po poprawnym zalogowaniu zobaczysz baner powitalny i znak zachęty routera.

```
C:\Users\user1> telnet 192.168.1.1

Unauthorized access is prohibited!

User Access Verification

Password:
R1>enable
Password:
R1#
```

Czy udało się połączyć z routerem? _____
Połączenie telnet powinno się udać, I słuchacze powinni zostać poproszeni o wpisanie hasła na

d. Wpisz **exit** i naciśnij Enter w celu zamknięcia połączenia Telnet.

e. Zmień adres IP komputera na 192.168.1.100 w celu sprawdzenia czy lista ACL blokuje ruch z nieuprawnionych adresów IP.

f. Połącz się do routera przez Telnet jeszcze raz. Czy połączenie zakończyło się sukcesem?

_____

Gdyby adres IP na PC-A się zmienił, to połączenie telnet by się nie powiodło

Jaki komunikat się pojawił?

_____

Connecting To 192.168.1.1…Could not open connection to the host, on port 23: Connect failed

g. Zmień adres IP komputera PC-A na jeden z zakresu od 192.168.1.4 do 192.168.1.7 w celu sprawdzenia czy lista ACL zezwala na ruch z ustawionego zakresu IP. Po zmianie adresu połącz się ponownie do routera przy użyciu protokołu Telnet.

Czy połączenie zakończyło się sukcesem?

_____

_____

Gdyby adres IP na PC-A się zmienił na adres od 192.168.1.4 do 192.168.1.7,to połączenie telnet by się powiodło

h. W trybie uprzywilejowanym routera R1 użyj komendy **show ip access-lists** i naciśnij Enter. Zauważ jak system IOS pokazuje liczbę poprawnych powiązań do danego wpisu ACE (w nawiasie).

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
```

```
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

Ze względu na dwa połączenia Telnet do routera, każde z adresu IP pasującego do jednego wpisu ACE, istnieją połączenia pasujące do obydwu wpisów ACE.

Dlaczego do każdego wpisu ACE są dwa powiązania skoro wykonane zostało tylko po jednym połączeniu z każdego adresu IP?

_____

_____

_____

_____

_____

_____

Odpowiedzi mogą się różnić. Słuchacze mogą zauważyć, że dwa powiązania do wpisu ACE korespondują do tego jak protokół telnet działa w celu uzyskania stabilnego połączenia.. Fakt, że mamy dwa wpisy do jednego połączenia oznacza jak wiele razy informacje kontrolne są przesyłane do routera, generując wpisy typu pozwól ACE .

W jaki sposób można określić, w którym momencie protokół Telnet powoduje dwa powiązania podczas jednego połączenia Telnet?

_____

_____

_____

_____

Odpowiedzi mogą być różne, ale słuchacze powinni zauważyć, że analizator protokołów Wireshark, pozwala przechwycić I przeanalizować im ruch telnet, aby określić kiedy są generowane dwa wpisy ACE dla jednego połączenia Telnet

i. Na routerze R1 wejdź do trybu globalnej konfiguracji.

j. Wejdź do trybu konfiguracji list dostępu ADMIN-MGT i dodaj wpis **deny any** na końcu listy.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

Uwaga: Ze względu na niejawny wpis **deny any** na końcu każdej listy nie ma potrzeby dodawania wyraźnego wpisu **deny any**. Jednakże wpis ten może być przydatny administratorowi w celu sprawdzenia ile razy wykonano połączenia, które zostały zablokowane.

k. Połącz się z komputera PC-B do R1 przy użyciu protokołu Telnet. Spowoduje to powstanie powiązania do wpisu **deny any** na liści kontroli dostępu.

l. W trybie uprzywilejowanym użyj komendy **show ip access-lists i** naciśnij Enter. Powinny być teraz widoczne powiązania do wpisu **deny any**.

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

Połączenia Telnet zakończone niepowodzeniem, powodują więcej powiązań do wpisu deny any, niż połączenia zakończone sukcesem. Dlaczego?

_____

Odpowiedzi mogą być różne ale słuchacze powinni rozpoznać , że Telenet musi mieć trzy kroki do stworzenia sesji.

Część 4: Wyzwanie – Konfiguracja list kontroli dostępu na przełączniku S1

Krok 1: Konfiguracja standardowej nazywanej listy ACL dla linii vty przełącznika S1.

a. Bez odnoszenia się do konfiguracji routera R1 spróbuj skonfigurować listę ACL na przełączniku, zezwalającą na dostęp tylko z komputera PC-A.

b. Przypisz listę ACL do linii vty przełącznika S1. Pamiętaj, że na przełączniku jest więcej linii vty niż na routerze.

Krok 2: Weryfikacja list ACL na liniach vty przełącznika S1.

Połącz się do przełącznika przy użyciu protokołu Telnet z każdego z komputerów w celu sprawdzenia czy listy ACL działają poprawnie. Powinieneś połączyć się tylko z komputera PC-A, z komputera PC-B nie.

Do przemyślenia

1. Jak wynika z tego ćwiczenia listy ACL są bardzo potężnymi filtrami ruchu, które mogą być stosowane nie tylko na wejściowych i wyjściowych interfejsach. Gdzie jeszcze można użyć list ACL?

   _____

   _____

   Odpowiedzi mogą się różnić. Słuchacze niech zauważą , że ACLki mogą być dołączone do sieciowych aplikacji jak na przykład serwer aplikacji

2. Czy listy ACL zastosowane na liniach vty zwiększają bezpieczeństwo protokołu Telnet? Czy czyni to protokół Telnet lepszym narzędziem do zdalnego dostępu?

   _____

   _____

   _____

   Odpowiedzi mogą być różne , ale słuchacze powinni zauważyć , że nawet gdy ACLki pomagają bronić zdalnego dostępu do zarządzania urządzeniami sieciowymi, nie potrafią jednak szyfrować danych przepływających aktualnie przez sieć. Jeśli jakaś informacja zostanie podsłuchana lub przechwycona, przez firmę trzecią lub nieoprawniony host – taka sieć wtedy nie jest bezpieczna.

3. Dlaczego ustawia się listy ACL na liniach vty zamiast na konkretnych interfejsach?

   _____

   _____

   _____

   Odpowiedzi mogą być różne ale studenci powinni zauważyć, że dołączając ACL do linii logicznych vty, nie robi to żadnej różnicyskąd przychodzi zaptyanie telnet lub ssh.. Filtry na vty są niezależne od interfejsu . W dodatku filtr na vty może być dołączony w jednym miejscu w przeciwieństwie do dołącznia go do kilku interfejsów.

Tabela interfejsów routera

Interfejsy routera				
Model routera	**Interfejs Ethernet #1**	**Interfejs Ethernet #2**	**Interfejs Serial #1**	**Interfejs Serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Aby dowiedzieć się jak router jest skonfigurowany należy spojrzeć na jego interfejsy i zidentyfikować typ urządzenia oraz liczbę jego interfejsów. Nie ma możliwości wypisania wszystkich kombinacji i konfiguracji dla wszystkich routerów. Powyższa tabela zawiera identyfikatory dla możliwych kombinacji interfejsów szeregowych i ethernetowych w urządzeniu. Tabela nie uwzględnia żadnych innych rodzajów interfejsów, pomimo że podane urządzenia mogą takie posiadać np. interfejs ISDN BRI. Opis w nawiasie (przy nazwie interfejsu) to dopuszczalny w systemie IOS akronim, który można użyć przy wpisywaniu komend.

Konfiguracja urządzeń

Router R1

```
Building configuration...

Current configuration : 1467 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
```

```
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard ADMIN-MGT
 permit 192.168.1.3
 permit 192.168.1.4 0.0.0.3
 deny   any
!
!
!
!
control-plane
!
!
banner motd ^CNo unauthorized access allowed!^C
!
line con 0
 password 7 070C285F4D06
 logging synchronous
 login
line aux 0
line 2
 no activation-character
```

```
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class ADMIN-MGT in
 password 7 13061E010803
 logging synchronous
 login
 transport input all
line vty 5 15
 access-class ADMIN-MGT in
 password 7 13061E010803
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
Building configuration...

Current configuration : 1782 bytes
!
!
version 15.0
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 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
```

```
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
ip access-list standard ADMIN-MGT
 permit 192.168.1.3
!
banner motd ^CNo unauthorized access allowed!^C
!
line con 0
 password 7 01100F175804
 logging synchronous
 login
line vty 0 4
 access-class ADMIN-MGT in
 password 7 01100F175804
 logging synchronous
 login
line vty 5 14
 access-class ADMIN-MGT in
 password 7 01100F175804
 logging synchronous
 login
line vty 15
 password 7 0822455D0A16
 login
!
end
```