Laboratorium - Konfigurowanie dostępu do urządzeń sieciowych za pomocą SSH

Topologia sieci

Tabela adresowania

Urządzenie	interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/1	192.168.1.1	255.255.255.0	nd.
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1

Cele

Część 1: Konfiguracja podstawowych ustawień urządzenia

Część 2: Konfiguracja dostępu do routera poprzez SSH

Część 3: Konfiguracja dostępu do przełącznika poprzez SSH

Część 4: Użycie sesji SSH na przełączniku za pomocą wiersza poleceń

Wprowadzenie

Telnet w przeszłości był powszechnym i szeroko stosowanym protokołem używanym do zdalnego konfigurowania urządzeń sieciowych. Telnet nie szyfruje informacji między klientem a serwerem. Pozwala to snifferom sieciowym na przechwytywanie haseł oraz konfiguracji.

Secure Shell (SSH) jest protokołem sieciowym który pozwala zestawić bezpieczne połączenie terminalowe do routera lub innych urządzeń sieciowych. SSH szyfruje wszystkie informacje które przechodzą przez sieć i wprowadza mechanizm bezpiecznego uwierzytelniania zdalnego komputera. Profesjonaliści sieciowi szybko zastąpili, używany do zdalnego logowania Telnet protokołem SSH.SSH jest najczęściej używany do logowania się do zdalnego urządzenia i wykonywania poleceń. Może jednak również przesyłać pliki przy użyciu powiązanych protokołów Secure FTP (SFTP) lub Secure Copy (SCP).

Komunikujące się urządzenia sieciowe muszą być skonfigurowane do obsługi SSH, aby SSH działało. W tym laboratorium skonfigurujesz serwer SSH na routerze a potem połączysz się z nim używając komputera PC posiadającego zainstalowanego klienta SSH.W sieci lokalnej połączenia zwykle są zestawiane poprzez Ethernet i IP.

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 użyć również innych routerów i przełączników Cisco z różnymi wersjami Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, czy konfiguracje routerów oraz przełączników zostały wymazane i nie posiadają konfiguracji początkowej. Jeśli nie jesteś pewien, to poproś o pomoc instruktora.

Wymagane zasoby

- 1 router (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalnym)
- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.2 (2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Konfigurowanie podstawowych ustawień urządzenia

W części 1 będziesz tworzyć topologię sieci i konfigurować podstawowe ustawienia takie jak adresy IP dla interfejsu, dostęp do urządzenia oraz hasła w routerze.

Krok 1: Zbuduj sieć zgodnie z topologią.

Krok 2: Zainicjuj i zrestartuj router i przełącznik.

Krok 3: Konfiguracja routera.

a. Połącz się konsolą do routera i przejdź do uprzywilejowanego trybu EXEC.

b. Wejdź do trybu konfiguracji globalnej.

c. Wyłącz DNS lookup, aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych komend, jako nazw hostów.

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

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

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

g. Zaszyfruj hasła zapisane jawnym tekstem.

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

i. Skonfiguruj i włącz interfejs G0/0/1 w routerze przy użyciu informacji zawartych w tabeli adresowania.

j. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).

Krok 4: Skonfiguruj PC-A.

a. Skonfiguruj adres IP i maskę podsieci dla komputera PC-A.

b. Skonfiguruj bramę domyślną dla komputera PC-A.

Krok 5: Sprawdzanie połączenia sieci.

Wykonaj ping od PC-A z R1. Jeżeli ping nie powiedzie się, to poszukaj rozwiązania problemu.

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Część 2: Konfigurowanie routera dla zdalnego dostępu poprzez SSH

Użycie Telnet do połączenia z urządzeniem sieciowym stanowi zagrożenie bezpieczeństwa, ponieważ wszystkie informacje są przesyłane w postaci czystego tekstu. Zalecane jest używanie protokołu SSH dla połączeń zdalnych, ponieważ SSH szyfruje dane sesji oraz zapewnia mechanizm uwierzytelniania urządzenia. W części 2 będziesz konfigurować linie VTY routera w celu akceptacji połączenia SSH.

Krok 1: Skonfiguruj uwierzytelnianie urządzenia.

Do generowania klucza szyfrującego RSA używane są nazwa urządzenia i nazwa domeny. Dlatego nazwy te muszą być wprowadzone przed wydaniem polecenia **crypto key**.

a. Skonfiguruj nazwę urządzenia.

b. Skonfiguruj domenę dla tego urządzenia.

Krok 2: Skonfiguruj klucz szyfrowania.

Krok 3: Skonfiguruj nazwę użytkownika w lokalnej bazie danych.

Skonfiguruj nazwę użytkownika **admin**, jako nazwę użytkownika i **Adm1nP@55** jako hasło.

Krok 4: Włącz SSH na liniach VTY.

a. Włącz Telnet oraz SSH na liniach wejściowych VTY za pomocą polecenia **transport input** .

b. Zmień metodę logowania do lokalnej bazy danych w celu weryfikacji użytkownika.

Krok 5: Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).

Krok 6: Ustanów połączenie SSH do routera.

a. Uruchom Tera Term na PC-A.

b. Ustanowienie sesji SSH do R1.Użyj nazwy użytkownika **admin** i hasła **Adm1nP@55** .Powinieneś być w stanie ustanowić sesję SSH z R1.

Część 3: Konfiguracja dostępu do przełącznika poprzez SSH

W części 3 będziesz konfigurować przełącznik aby ustanowić połączenie SSH. Po skonfigurowaniu przełącznika nawiąż sesję SSH przy użyciu Tera Term.

Krok 1: Skonfiguruj podstawowe ustawienia przełącznika.

a. Połącz się do konsoli przełącznika i przejdź do trybu uprzywilejowanego.

b. Wejdź do trybu konfiguracji globalnej.

c. Wyłącz DNS lookup, aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych komend, jako nazw hostów.

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

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

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

g. Zakoduj wszystkie hasła występujące w konfiguracji w jawnej postaci.

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

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

i. Skonfiguruj i aktywuj interfejs VLAN 1 na przełączniku zgodnie z tabelą adresowania.

j. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).

Krok 2: Skonfiguruj przełącznik dla połączeń poprzez SSH.

Aby skonfigurować SSH dla przełącznika, zastosuj te same polecenia, których używałeś do konfigurowania SSH na routerze w części 2.

a. Skonfiguruj nazwę urządzenia zgodnie z listą w tabeli adresowania.

b. Skonfiguruj domenę dla tego urządzenia.

c. Skonfiguruj klucz szyfrowania.

d. Skonfiguruj nazwę użytkownika w lokalnej bazie danych.

e. Włącz telnet i SSH na liniach VTY.

f. Zmień metodę logowania do lokalnej bazy danych w celu weryfikacji użytkownika.

Krok 3: Ustanów połączenie SSH do przełącznika.

Uruchom Tera Term z komputera PC-A, a następnie za pomocą SSH połącz się z interfejsem SVI w S1.

Czy jesteś w stanie ustanowić sesję SSH do przełącznika?

Część 4: Uruchamianie SSH z linii poleceń CLI w przełączniku

Klient SSH jest wbudowany w systemie Cisco IOS i można go uruchomić z CLI.W części 4 będziesz używać SSH za pomocą wiersza poleceń CLI w przełączniku, do łączenia się z routerem.

Krok 1: Wyświetl parametry dostępne dla klienta Cisco IOS SSH.

Aby wyświetlić opcje parametrów dostępne za pomocą polecenia **ssh** użyj znaku zapytania **?**.

```
S1# ssh ?
-c Select encryption algorithm
-l Log in using this user name
-m Select HMAC algorithm
-o Specify options
-p Connect to this port
-v Specify SSH Protocol Version
-vrf Specify vrf name
WORD IP address or hostname of a remote system
```

Krok 2: Połącz się korzystając z SSH na S1 do R1.

a. Jeżeli chcesz połączyć się do R1 poprzez SSH, to musisz użyć opcji **–l admin**. To pozwoli ci zalogować się jako **admin**. Jeżeli zostaniesz zapytany o hasło, to wpisz **Adm1nP@55** .

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

b. Możesz wrócić do S1 bez zamykania sesji SSH ustanowionej do R1 za pomocą kombinacji klawiszy **Ctrl**+**Shift**+**6**.Zastosuj kombinację **Ctrl**+**Shift**+**6** i wpisz **x**. Powinieneś zobaczyć znak zachęty przełącznika w trybie uprzywilejowanym.

```
R1>
S1#
```

c. Aby powrócić do sesji SSH ustanowionej w R1, naciśnij klawisz Enter w pustej linii CLI. Może będziesz musiał nacisnąć klawisz Enter po raz drugi, aby zobaczyć wiersz poleceń routera (CLI).

```
S1#
[Resuming connection 1 to 192.168.1.1 ...].

R1>
```

d. Aby zakończyć sesję SSH na R1, w wierszu poleceń routera wpisz **exit**.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Jakie wersje SSH są obsługiwane w wierszu poleceń CLI?

Pytania do przemyślenia

Jak można skonfigurować dostęp dla wielu użytkowników (każdy ma swoją nazwę) do urządzenia sieciowego?

Tabela zbiorcza interfejsów routerów

Model routera	Interfejs Ethernet nr 1	Interfejs Ethernet nr 2	Interfejs szeregowy nr 1	Interfejs szeregowy nr 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 0/0/1 (S0/0/1)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy, aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma jednego sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdego modelu routera. Tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, pomimo iż dany router może być w nie wyposażony. Przykładem takiego interfejsu może być ISDN BRI. Informacje umieszczone w nawiasach są dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.

©2013 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

www.netacad.com