Laboratorium 1 – Zabezpieczenie dostępu do urządzeń sieciowych z wykorzystaniem serwera RADIUS i TACACS+(AAA)

Cele ćwiczenia

Celem ćwiczenia jest skonfigurowanie bezpiecznego uwierzytelnionego dostępu do urządzeń Cisco z wykorzystaniem serwerów RADIUS i TACACS+. Cele szczegółowe są następujące:

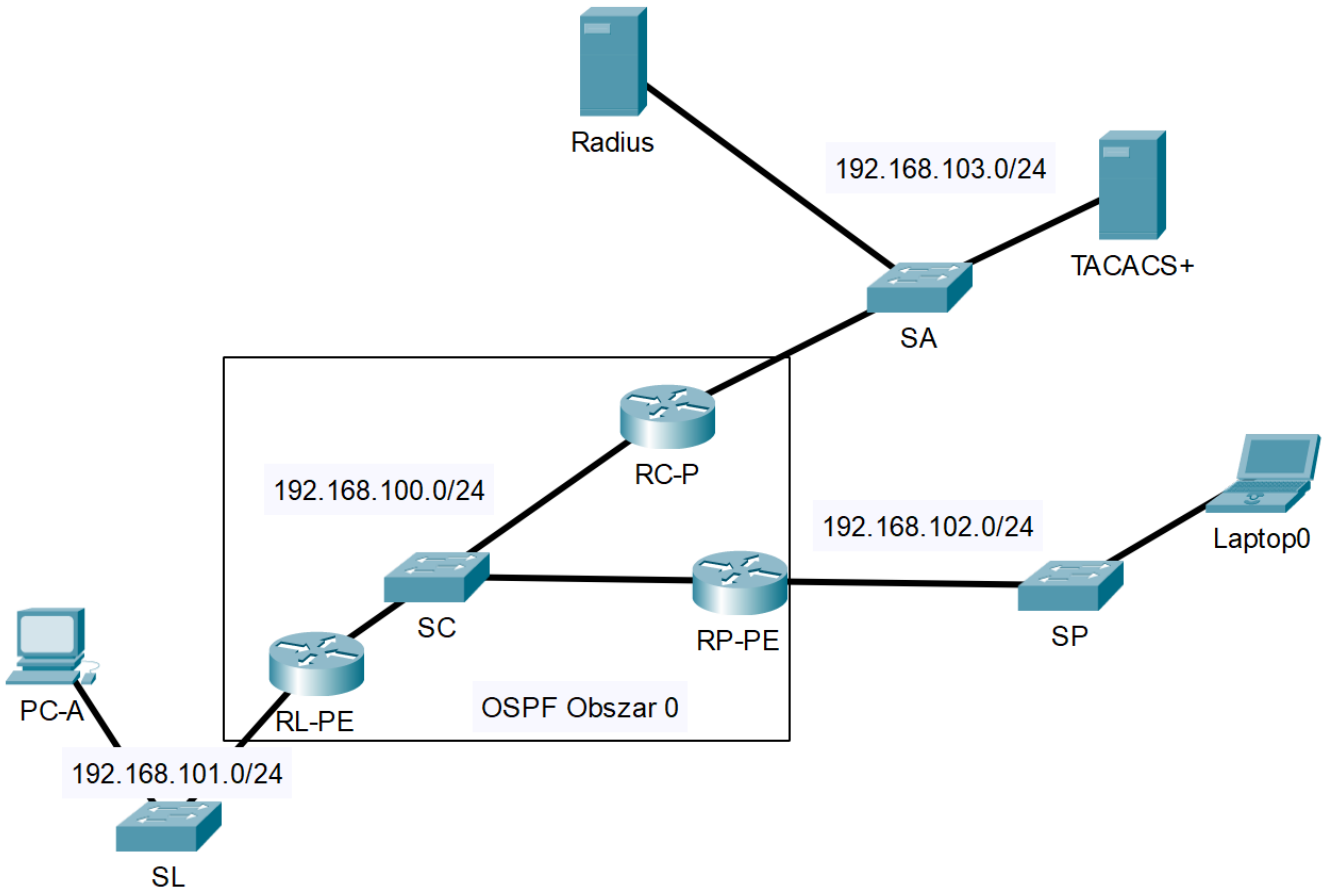
1. Konfiguracja rutingu OSPF
2. Konfiguracja serwera uwierzytelniania RADIUS
3. Konfiguracja serwera uwierzytelniania TACACS+
4. Konfiguracja dostępu konsolowego do ruterów z wykorzystaniem serwerów AAA
5. Konfiguracja zdalnego dostępu do ruterów konsolowego z wykorzystaniem serwerów AAA

Opis topologii logicznej i fizycznej sieci

1. Komputer PC-A o adresie IP 192.168.101.**2**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SL
2. Port GigabitEthernet 0/1 przełącznika SL połączy z portem GigabitEthernet 0/0/1 rutera RL-PE o adresie 192.168.101.**1**/24
3. Port GigabitEthernet 0/0/0 rutera RL-PE o adresie 192.168.100.**1**/24 połączony z portem FastEthernet 0/1 przełącznika SC
4. Port GigabitEthernet 0/0/0 rutera RP-PE o adresie 192.168.100.**2**/24 połączony z portem FastEthernet 0/2 przełącznika SC
5. Port GigabitEthernet 0/0/0 rutera RC-P o adresie 192.168.100.**3**/24 połączony z portem GigabitEthernet 0/1 przełącznika SC

6. Port GigabitEthernet 0/0/1 rutera RP-PE o adresie 192.168.102.**1**/24 połączony z portem GigabitEthernet 0/1 przełącznika SP
7. Port GigabitEthernet 0/0/1 rutera RC-P o adresie 192.168.103.**1**/24 połączony z portem GigabitEthernet 0/1 przełącznika SA
8. Komputer Laptop0 o adresie IP 192.168.102.2/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SP
9. Serwer Radius o adresie IP 192.168.103.2/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SA
10. Serwer TACACS+ o adresie IP 192.168.102.3/24 połączony łączem FastEthernet z portem FastEthernet 0/2 przełącznika SA

Graficzną reprezentację opisanej topologii przedstawiono na poniższym rysunku



Przebieg ćwiczenia

Połącz urządzenia zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadaj adresy IP urządzeniom końcowym

1. Komputer PC-A
    a. Adres 192.168.101.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.101.1 z maską 24 bitową
2. Komputer Laptop0
    a. Adres 192.168.102.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.102.1 z maską 24 bitową
3. Serwer Radius
    a. Adres 192.168.103.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.103.1 z maską 24 bitową
4. Serwer TACACS+
    a. Adres 192.168.103.3 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.103.1 z maską 24 bitową

Skonfiguruj interfejsy sieciowe ruterów

1. Ruter RL-PE

```
RL-PE#configure terminal

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

RL-PE(config)#interface GigabitEthernet 0/0/0

RL-PE(config-if)#ip address 192.168.100.1 255.255.255.0

RL-PE(config-if)#no shutdown

RL-PE(config)#interface GigabitEthernet 0/0/1

RL-PE(config-if)#ip address 192.168.101.1 255.255.255.0

RL-PE(config-if)#no shutdown
```

```
RL-PE(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state
to up
```

2. Ruter RP-PE

```
RP-PE#configure terminal

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

RP-PE(config)#interface GigabitEthernet 0/0/0

RP-PE(config-if)#ip address 192.168.100.2 255.255.255.0

RP-PE(config-if)#no shutdown

RP-PE(config)#interface GigabitEthernet 0/0/1

RP-PE(config-if)#ip address 192.168.102.1 255.255.255.0

RP-PE(config-if)#no shutdown
```

3. Ruter RC-P

```
RC-P#configure terminal

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

RC-P(config)#interface GigabitEthernet 0/0/0

RC-P(config-if)#ip address 192.168.100.3 255.255.255.0

RC-P(config-if)#no shutdown

RC-P(config)#interface GigabitEthernet 0/0/1

RC-P(config-if)#ip address 192.168.103.1 255.255.255.0

RC-P(config-if)#no shutdown
```

Wyświetl konfigurację interfejsów ruterów

1. Ruter RL-PE

```
RL-PE#show ip interface brief
```

2. Ruter RP-PE

```
RP-PE#show ip interface brief
```

3. Ruter RC-P

```
RC-P#show ip interface brief
```

Skonfiguruj protokół rutingu OSPF w pojedynczym obszarze

1. Ruter RL-PE

```
RL-PE(config)#router ospf 1
RL-PE(config-router)#network 192.168.100.0 0.0.0.255 area 0
RL-PE(config-router)#network 192.168.101.0 0.0.0.255 area 0
```

2. Ruter RP-PE

```
RP-PE(config)#router ospf 1
RP-PE(config-router)#network 192.168.100.0 0.0.0.255 area 0
RP-PE(config-router)#network 192.168.102.0 0.0.0.255 area 0
```

3. Ruter RC-P

```
RC-P(config)#router ospf 1
RC-P(config-router)#network 192.168.100.0 0.0.0.255 area 0
RC-P(config-router)#network 192.168.103.0 0.0.0.255 area 0
```

Sprawdź poprawność konfiguracji OSPF (przykład dla jednego rutera)

RP-PE#show ip ospf neighbor

```
Neighbor ID Pri State Dead Time Address Interface

192.168.101.1 1 FULL/DROTHER 00:00:39 192.168.100.1
GigabitEthernet0/0/0

192.168.103.1 1 FULL/DR 00:00:39 192.168.100.3 GigabitEthernet0/0/0
```

RP-PE>show ip route

```
Codes: […]

Gateway of last resort is not set

192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.100.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.100.2/32 is directly connected, GigabitEthernet0/0/0

O 192.168.101.0/24 [110/2] via 192.168.100.1, 02:06:17,
GigabitEthernet0/0/0

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.102.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.102.1/32 is directly connected, GigabitEthernet0/0/1

O 192.168.103.0/24 [110/2] via 192.168.100.3, 02:06:17,
GigabitEthernet0/0/0
```

Konfiguracja serwera RADIUS

1. Przejdź do konfiguracji AAA na serwerze Radius
2. Dodaj dane klienta. Klientem serwera Radius będzie ruter RL-PE. Należy zatem podać nazwę klienta, tj. „**RL-PE**”; adres IP klienta, tj. 192.168.100.1, oraz klucz o wartości „**radiusAiTech**”
3. Dodaj dane użytkownika klienta, które będą wykorzystywane do jego uwierzytelniana przy próbie uzyskania dostępu do klienta. Należy zatem podać nazwę użytkownika, tj. „**AdminRLPE**” oraz hasło „**RLPEAiTech**”

Konfiguracja serwera TACACS+

1. Przejdź do konfiguracji AAA na serwerze TACACS+
2. Dodaj dane klienta. Klientem serwera Tacacs+ będzie ruter RP-PE. Należy zatem podać nazwę klienta, tj. „**RP-PE**”; adres IP klienta, tj. 192.168.100.2, oraz klucz o wartości „**tacacsAiTech**”
3. Dodaj dane użytkownika klienta, które będą wykorzystywane do jego uwierzytelniana przy próbie uzyskania dostępu do klienta. Należy zatem podać nazwę użytkownika, tj. „**AdminRPPE**” oraz hasło „**RPPEAiTech**”

Konfiguracja rutera RL-PE w celu uwierzytelniania użytkowników konsolowych z wykorzystaniem RADIUS

1. Skonfiguruj zapasową lokalną bazę użytkowników

```
RL-PE#configure terminal

RL-PE(config)#username AdminRLPE secret RLPEAiTech
```

1. Skonfiguruj parametry serwera Radius

```
RL-PE(config)# radius-server host 192.168.103.2

RL-PE(config)#radius-server key radiusAiTech
```

2. Skonfiguruj metodę uwierzytelniania użytkowników RL-PE. W przypadku każdej próby zalogowania użytkownika na RL-PE najpierw zostanie podjęta próba uwierzytelnienia na zdalnym serwerze Radius, a dopiero później, w razie jego niedostępności, wykorzystana zostanie lokalna baza użytkowników.

```
RL-PE(config)# aaa new-model

RL-PE(config)# aaa authentication login default group radius
local
```

3. Konfiguracja uwierzytelniania dostępu konsolowego z wykorzystaniem serwera Radius

```
RL-PE(config)#line console 0

RL-PE(config-line)# login authentication default
```

4. Sprawdzenie poprawności uwierzytelniania na ruterze RL-PE z wykorzystaniem serwera Radius
   a. Opuść tryb uprzywilejowany

```
RL-PE# exit

User Access Verification

Username: AdminRLPE

Password:

RL-PE>
```

Konfiguracja rutera RP-PE w celu uwierzytelniania użytkowników konsolowych z wykorzystaniem TACACS+

1. Skonfiguruj zapasową lokalną bazę użytkowników

```
RP-PE#configure terminal

RP-PE(config)#username AdminRPPE secret RPPEAiTech
```

1. Skonfiguruj parametry serwera TACACS+

```
RP-PE(config)# tacacs-server host 192.168.103.3

RP-PE(config)#tacacs-server key tacacsAiTech
```

2. Skonfiguruj metodę uwierzytelniania użytkowników RP-PE. W przypadku każdej próby zalogowania użytkownika na RP-PE najpierw zostanie podjęta próba uwierzytelnienia na zdalnym

serwerze TACACS+, a dopiero później, w razie jego niedostępności, wykorzystana zostanie lokalna baza użytkowników.

```
RP-PE(config)# aaa new-model

RP-PE(config)# aaa authentication login default group tacacs+
local
```

2. Konfiguracja uwierzytelniania dostępu konsolowego z wykorzystaniem serwera TACACS+

```
RP-PE(config)#line console 0

RP-PE(config-line)# login authentication default
```

3. Sprawdzenie poprawności uwierzytelniania na ruterze RP-PE z wykorzystaniem serwera TACACS+
   a. Opuść tryb uprzywilejowany

```
RP-PE# exit

User Access Verification

Username: AdminRPPE

Password:

RP-PE>
```

Konfiguracja rutera RL-PE w celu uwierzytelniania użytkowników zdalnych z wykorzystaniem RADIUS

1. Nie konfiguruj lokalnej bazy użytkowników. Oznacza to brak usługi dostępu zdalnego przy braku połączenia z serwerem RADIUS
2. Skonfiguruj metodę uwierzytelniania dla użytkowników zdalnych VTY i nazwij ją jako „LINIEVTY”

```
RL-PE#configure terminal

RL-PE(config)# aaa authentication login LINIEVTY group radius
```

4. Skonfiguruj linie vty z uwierzytelnianiem zapisanym jako „LINIEVTY”

```
RL-PE#line vty 0 4
```

```
RL-PE (config-line)# login authentication LINIEVTY
```

5. Nawiąż połączenie z komputera PC-A do RL-PE