Packet Tracer – Konfigurowanie list kontroli dostępu ACL z protokołem IPv6

Topologia

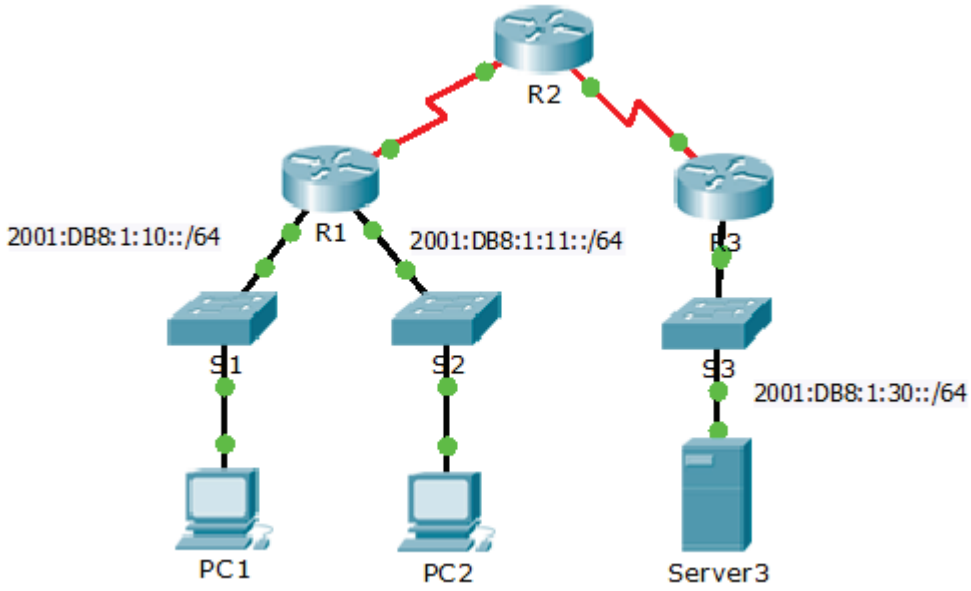

Tabela adresacji

Urządzenie	Interfejs	Adres IPv6/Prefiks	Brama domyślna
Server3	Karta sieciowa	2001:DB8:1:30::30/64	FE80::30

Cele

Część 1: Konfigurowanie, stosowanie i weryfikacja listy ACL z protokołem IPv6

Część 2: Konfigurowanie, stosowanie i weryfikacja drugiej listy ACL z protokołem IPv6

Część 1: Konfigurowanie, stosowanie i weryfikacja listy ACL z protokołem IPv6

Dzienniki logowania wskazują, że jakiś komputer pracujący w sieci 2001:DB8:1:11::0/64 ciągle odświeża stronę internetową powodujący tym samym atak Denial-of-Service (DoS) na serwer **Server3**. Dopóki ten host nie zostanie zidentyfikowany, to musisz zablokować ruch HTTP i HTTPS, wykorzystując do tego listę kontroli dostępu.

Krok 1: Skonfiguruj listę ACL blokującą dostęp do HTTP i HTTPS.

Skonfiguruj listę ACL nazwaną **BLOCK_HTTP** na **R1** za pomocą następujących instrukcji.

a. Blokuj ruch HTTP i HTTPS kierowany do **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Pozostały ruch IPv6 ma być dozwolony.

Krok 2: Zastosuj listę ACL do właściwego interfejsu.

Zastosuj listę ACL do interfejsu, który znajduje się najbliżej źródła, z którego ruch ma być blokowany.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Krok 3: Sprawdź implementację listy ACL.

Sprawdź, czy lista ACL działa prawidłowo. W tym celu przeprowadź następujące testy:

- Otwórz **przeglądarkę internetową** na komputerze **PC1** i wpisz następujący adres http://2001:DB8:1:30::30 lub https://2001:DB8:1:30::30. Powinna pojawić się strona internetowa.
- Otwórz **przeglądarkę internetową** na komputerze **PC2** i wpisz następujący adres http://2001:DB8:1:30::30 lub https://2001:DB8:1:30::30. Strona internetowa powinna być blokowana.
- Na komputerze **PC2** wpisz polecenie ping 2001:DB8:1:30::30. Badanie za pomocą ping powinno być pozytywne.

Część 2: Konfigurowanie, stosowanie i weryfikacja drugiej listy ACL z protokołem IPv6

Dzienniki logowań pokazują, że Twój serwer otrzymuje żądania ping z wielu różnych adresów IPv6, co oznacza atak tzw. rozproszonej odmowy usługi Distributed Denial of Service (DDoS). Musisz filtrować protokół ICMP zawierający żądania ping kierowane do Twojego serwera.

Krok 1: Utwórz listę blokującą dostęp dla protokołu ICMP.

Skonfiguruj listę ACL nazwaną **BLOCK_ICMP** na **R3** z następującymi instrukcjami:

a. Blokuj cały ruch ICMP z każdego hosta do każdego adresu docelowego.

b. Pozostały ruch IPv6 ma być dozwolony.

Krok 2: Zastosuj listę ACL do właściwego interfejsu.

W tym przypadku ruch ICMP może przychodzić z każdego źródła. Aby upewnić się, że ruch ICMP jest blokowany niezależnie od źródła lub od zmiany w topologii sieci, zastosuj listę ACL jak najbliżej miejsca docelowego.

Krok 3: Sprawdź czy lista dostępu ACL działa prawidłowo.

a. Na komputerze **PC2** wpisz polecenie ping 2001:DB8:1:30::30. Test powinien zakończyć się niepowodzeniem.

b. Na komputerze **PC1** wpisz polecenie ping 2001:DB8:1:30::30. Test powinien zakończyć się niepowodzeniem.

c. Otwórz **przeglądarkę internetową** na komputerze **PC1** i wpisz następujący adres http://2001:DB8:1:30::30 lub https://2001:DB8:1:30::30. Powinna pojawić się strona internetowa.