Cisco: Lock-and-Key (Dynamic Access Control)

Wprowadzenie

Lock-and-Key (Dynamic Access Lists) to mechanizm bezpieczeństwa Cisco, który umożliwia **dynamiczne otwieranie dostępu przez ACL-e**, po **udanym logowaniu użytkownika przez Telnet lub SSH**.

Zasada działania:

1. Początkowo lista ACL blokuje dostęp.
2. Użytkownik łączy się na router przez Telnet/SSH i podaje login.
3. Po uwierzytelnieniu router tymczasowo otwiera ACL (dynamicznie) dla danego IP.
4. Po zakończeniu sesji ACL wraca do stanu początkowego (zamknięta).

Krok 1: Konfiguracja użytkownika

```
Router(config)# username user1 password cisco123
```

Krok 2: Włączenie serwera Telnet/SSH i logowania lokalnego

```
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# autocommand access-enable
Router(config-line)# exit
```

Polecenie `autocommand access-enable` uruchamia dynamiczny dostęp po uwierzytelnieniu.

Krok 3: Skonfiguruj dynamiczną ACL

Załóżmy, że chcemy zezwolić na dostęp **z zewnątrz** do hosta `192.168.1.10` na porcie `80` (HTTP), ale **dopiero po autoryzacji**.

```
Router(config)# ip access-list extended LOCK_AND_KEY
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# dynamic AUTH_ACCESS permit tcp any host
192.168.1.10 eq 80
Router(config-ext-nacl)# exit
```

Tutaj:

- `LOCK_AND_KEY` – nazwa listy ACL przypisanej do interfejsu.
- `AUTH_ACCESS` – nazwa dynamicznej sesji.
- Domyślnie ruch jest blokowany (`deny ip any any`), chyba że sesja zostanie dynamicznie otwarta.

Krok 4: Przypisanie ACL-a do interfejsu

Załóżmy, że interfejs zewnętrzny to `GigabitEthernet0/0`:

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip access-group LOCK_AND_KEY in
Router(config-if)# exit
```

Krok 5: Uwierzytelnienie użytkownika

Z hosta zdalnego (np. `192.0.2.50`) łączymy się do routera przez Telnet:

```
telnet 203.0.113.1
```

Po zalogowaniu router wyświetli komunikat:

```
Router> access-enable host timeout 10
```

To polecenie aktywuje dynamiczną regułę ACL dla tego adresu IP na 10 minut.

Sprawdzanie działania mechanizmu

Wyświetlenie aktywnych sesji:

```
Router# show access-lists
```

Zakończenie dynamicznego dostępu:

```
Router> access-disable
```

Wyświetlenie dynamicznych wpisów ACL:

```
Router# show ip access-lists
```

Uwagi końcowe

- Lock-and-Key działa tylko z Telnet/SSH – nie obsługuje np. HTTP ani konsoli.
- Mechanizm przydatny przy ochronie czułych zasobów przed dostępem publicznym.
- Dynamiczne wpisy są tymczasowe – po wygaśnięciu sesji zostają automatycznie usunięte.
- Można ograniczyć dostęp tylko dla wybranych użytkowników przez `username ... privilege` i ACL-e.