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
```

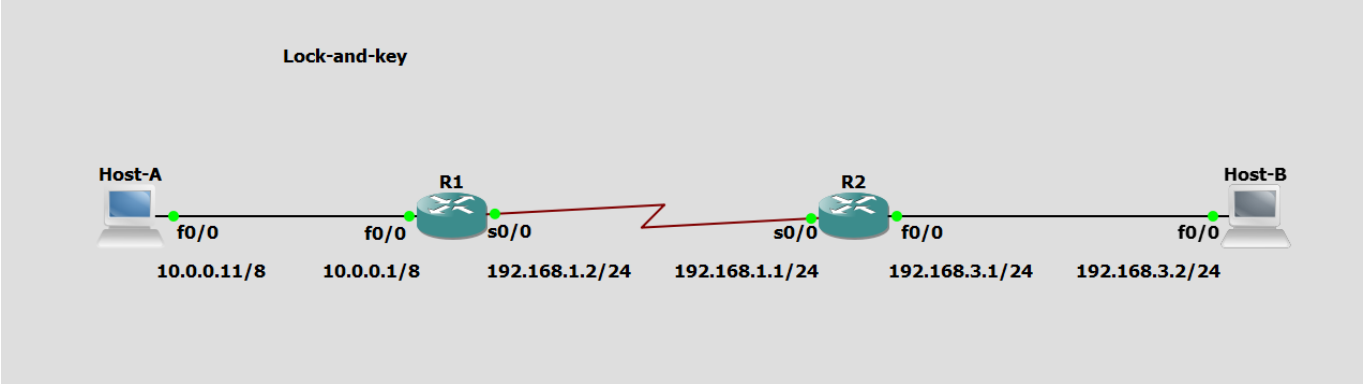
Wyświetlenie dynamicznych wpisów ACL:

```
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.

Przykład



login: ernie hasło: bert

test:

```
Host-B#ping 10.0.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.11, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Host-B#telnet 192.168.1.2
Trying 192.168.1.2 ... Open


User Access Verification

Username: ernie
Password:
[Connection to 192.168.1.2 closed by foreign host]
Host-B#ping 10.0.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/70/92 ms
Host-B#
```

konfiguracja R1:

```
R1#show running-config
Building configuration...

Current configuration : 1593 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
```

```
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username ernie password 0 bert
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
```

```
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.1.2 255.255.255.0
 ip access-group 101 in
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
!
no ip http server
no ip http secure-server
!
access-list 101 permit tcp 192.168.3.0 0.0.0.255 host 192.168.1.2 eq telnet
access-list 101 dynamic LETMEIN timeout 90 permit ip 192.168.3.0 0.0.0.255
10.0.0.0 0.255.255.255
no cdp log mismatch duplex
!
!
!
```

```
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 autocommand  access-enable host timeout 2
!
!
end
```

konfiguracja R2:

```
R2#show running-config
Building configuration...

Current configuration : 1322 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
```

```
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.0
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```