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

Introduction

Lock-and-Key (Dynamic Access Lists) is a Cisco security mechanism that makes it possible to **dynamic access opening via ACLs**after **successful user login via Telnet or SSH.**.

Operating principle:

1. Initially, the ACL list blocks access.
2. The user connects to the router via Telnet/SSH and provides a login.
3. After authentication, the router temporarily opens the ACL (dynamically) for the IP in question.
4. When the session ends, the ACL returns to its initial state (closed).

Step 1: User configuration

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

Step 2: Enable Telnet/SSH server and local login

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

The `autocommand access-enable` command starts dynamic access after authentication.

Step 3: Configure a dynamic ACL

Suppose we want to allow access **from outside** to the host `192.168.1.10` on port `80` (HTTP), but **only after authorization**.

```
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
```

Here:

- `LOCK_AND_KEY` - the name of the ACL assigned to the interface.
- `AUTH_ACCESS` - the name of the dynamic session.
- By default, traffic is blocked (`deny ip any`) unless the session is dynamically opened.

Step 4: Assign an ACL to an interface.

Assume that the external interface is `GigabitEthernet0/0`:

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

Step 5: User authentication

From the remote host (e.g. `192.0.2.50`), we connect to the router via Telnet:

```
telnet 203.0.113.1
```

After logging in, the router will display the message:

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

This command activates a dynamic ACL rule for this IP address for 10 minutes.

Checking the operation of the mechanism

Display the active sessions:

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

Termination of dynamic access:

```
Router> access-disable
```

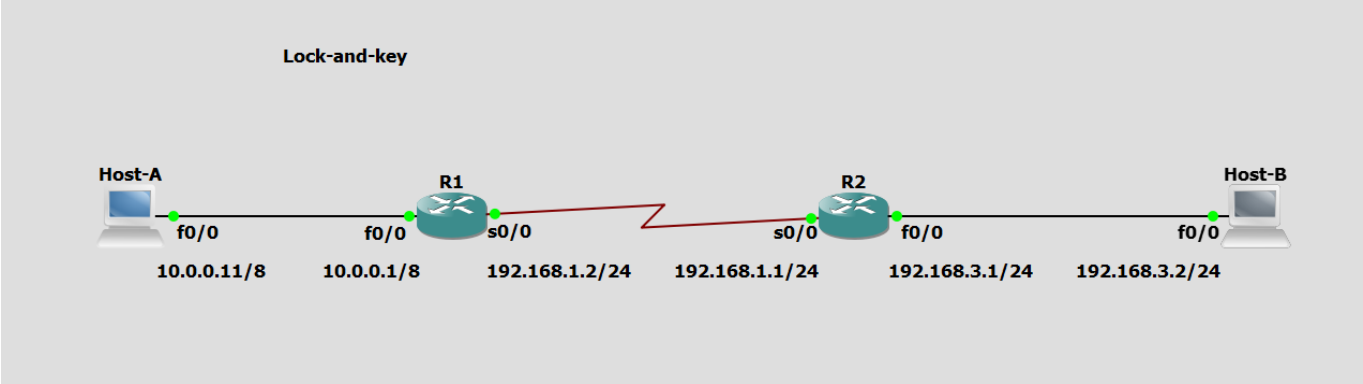
Display of dynamic ACL entries:

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

Concluding remarks

- Lock-and-Key only works with Telnet/SSH - it does not support HTTP or console, for example.
- Mechanism useful for protecting sensitive resources from public access.
- Dynamic entries are temporary - they are automatically deleted when the session expires.
- You can restrict access to only selected users via `username ... privilege' and ACLs.

Example



login: ernie password: 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#
```

R1 configuration:

```
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
```

R2 configuration:

```
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
```