Ch.10 Security

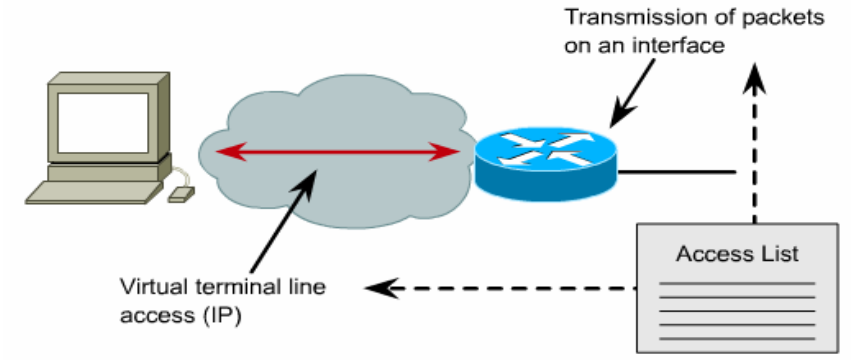
Lee, HoonJae
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

Dongseo University

Ch10. Security

Cryptography and Network Security Lab.

IP Access List



Access lists can be used to limit transmission of packets through an interface and limit vitual terminal line access.

Cisco IOS Access List Numbers

Access List Number	Description
1 to 99	IP standard access list
100 to 199	IP extended access list
200 to 299	Protocol type-code access list
300 to 399	DECnet access list
400 to 499	XNS standard access list
500 to 599	XNS extended access list
600 to 699	AppleTalk access list
700 to 799	48-bit MAC address access list
800 to 899	IPX standard access list
900 to 999	IPX extended access list
1000 to 1099	IPX SAP access list
1100 to 1199	Extended 48-bit MAC address access list
1200 to 1299	IPX summary address access list
1300 to 1999	IP standard access list (expanded range)
2000 to 2699	IP extended access list (expanded range)

Access List Syntax

Standard Access List Syntax

```
Router(config)#access-list access-list-number {deny |
permit} source [source-wildcard] [log]
```

Extended Access List Syntax

```
Router(config)# access-list access-list-number {deny |
permit}  protocol source source-wildcard destination
destination-wildcard   [precedence precedence] [tos tos]
[established] [log]  [time-range time-range-name
```


Configuring an Extended Named Access List

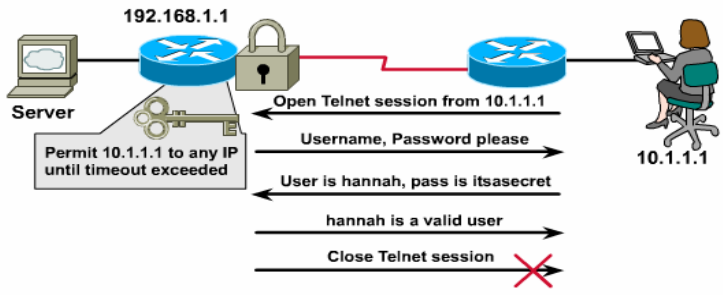
```
RTA(config)#ip access-list extended WEBONLY
RTA(config-ext-nacl)#permit tcp any 10.0.0.0 0.255.255.255 eq 80
RTA(config-ext-nacl)#deny ip any 10.0.0.0 0.255.255.255
RTA(config-ext-nacl)#permit ip any any
RTA(config-ext-nacl)#^Z

RTA#show access-lists
Extended IP access list WEBONLY
   permit tcp any 10.0.0.0 0.255.255.255 eq www
   deny ip any 10.0.0.0 0.255.255.255
      permit ip any any
```

Configuring Time-Based Access Lists with time-range

```
RTA(config)#time-range NO-HTTP
RTA(config-time-range)#periodic weekdays 8:00 to 18:00
RTA(config-time-range)#exit
RTA(config)#time-range UDP-YES
RTA(config-time-range)#periodic weekend 12:00 to 20:00
RTA(config-time-range)#exit
RTA(config)#ip access-list extended STRICT
RTA(config-ext-nacl)#deny tcp any any eq http time-range NO-HTTP
RTA(config-ext-nacl)#permit udp any any time-range UDP-YES
RTA(config-ext-nacl)#deny udp any any range netbios-ns netbios-ss
RTA(config-ext-nacl)#permit ip any any
```


10.3 Dynamic Access Lists

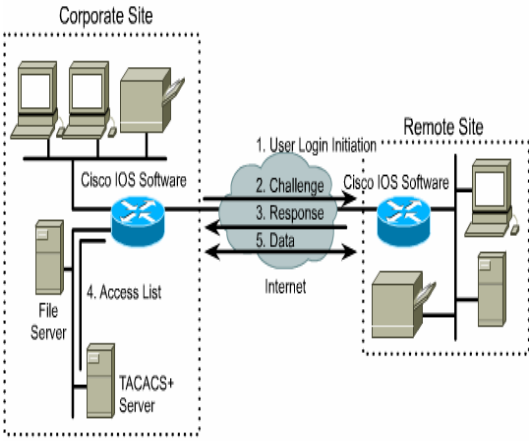
Lock-and-Key



Lock-and-key is a Cisco IOS feature that enables users to temporarily open a hole in a firewall without compromising other configured security restrictions.

10.3 Dynamic Access Lists

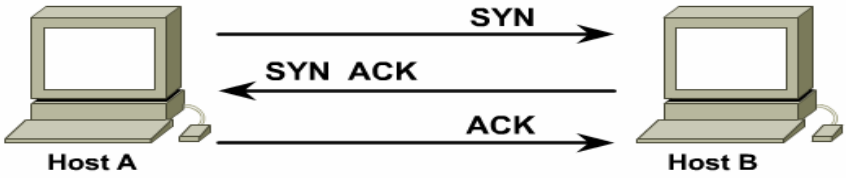
Lock-and-Key Operation



1. A user opens a Telnet session to a firewall router configured for lock-and-key. The user connects via one of the VTYs on the router.
2. The Cisco IOS receives the Telnet packet, opens a Telnet session, prompts the user for a username and password, and performs the authentication process. The authentication can be done by the router or by a security server (such as a TACACS+ or RADIUS box).
3. When a user passes authentication, he or she is logged out of the Telnet session, and the software creates a temporary entry in the dynamic access list. Depending on the configuration, this temporary entry can limit the range of networks to which the user is given temporary access.
4. The user exchanges data through the "hole" in the firewall.
The IOS deletes the temporary access list entry when a configured timeout is reached, or when the system administrator manually clears it. The configured timeout can be either an idle timeout or an absolute timeout.
5. The temporary access-list entry is not automatically deleted when the user terminates a session. It remains until the timeout is reached or until it is cleared by the system administrator.

10.4 Session Filtering

Using Extended Access Lists with the `established` Argument



IP hosts use the SYN and ACK code bits to perform the TCP three-way handshake.

Define the Reflexive Access List

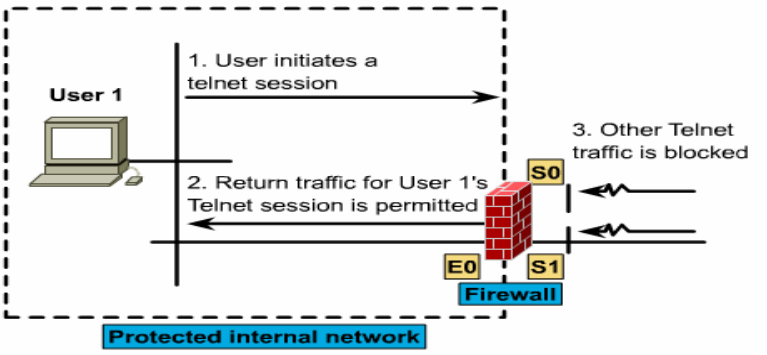
Task	Command
External interface: Specify the outbound access list. or Internal interface: Specify the inbound access list. (Performing this task also causes you to enter the access-list configuration mode).	**ip access-list extended** *name*
Define the relfexive access list using the reflexive **permit** entry. Repeat the step for each IP upper-layer protocol; for example, you can define reflexive filtering for TCP sessions and also for UDP sessions. You can use the same name for multiple protocols.	**permit** *protocol* **any any** **reflect** *name* **[timeout** *seconds***]**

Reflexive Access List Configuration Example

A reflexive access list can be placed on RTA's external interface (S0) so that incoming traffic can be evaluated before it enters the router.

10.5 Context-Based Access Control

How CBAC Works



CBAC dynamically opens holes in the firewall so that invited traffic can pass through.

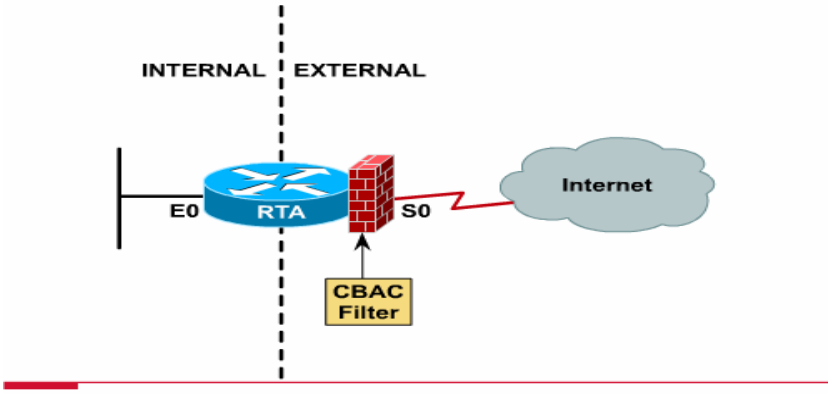
10.5 Context-Based Access Control

CBAC-Supported Application Protocols

- CU-SeeMe (only the White Pine version)
- FTP
- H.323 (such as NetMeeting, ProShare)
- HTTP (Java blocking)
- Java
- Microsoft NetShow
- UNIX r-commands (such as rlogin, rexec, and rsh)
- RealAudio
- RPC (Sun RPC, not DCE RPC)
- Microsoft RPC
- Simple Mail Transfer Protocol (SMTP)
- SQL*Net
- StreamWorks
- Trivial File Transfer Protocol (TFTP)
- VDOLive

10.5 Context-Based Access Control

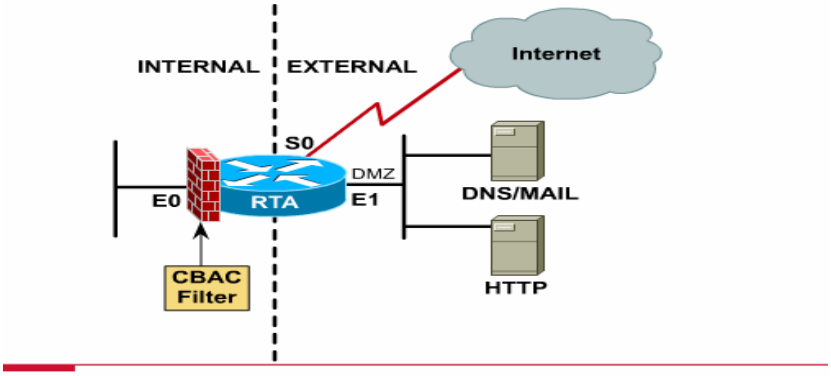
Simple Topology



In a simple topology, CBAC is typically configured on an external interface.

10.5 Context-Based Access Control

External Interface with DMZ



The CBAC traffic filter can be applied to an internal interface so that outside traffic can pass through the router to a public segment (DMZ).

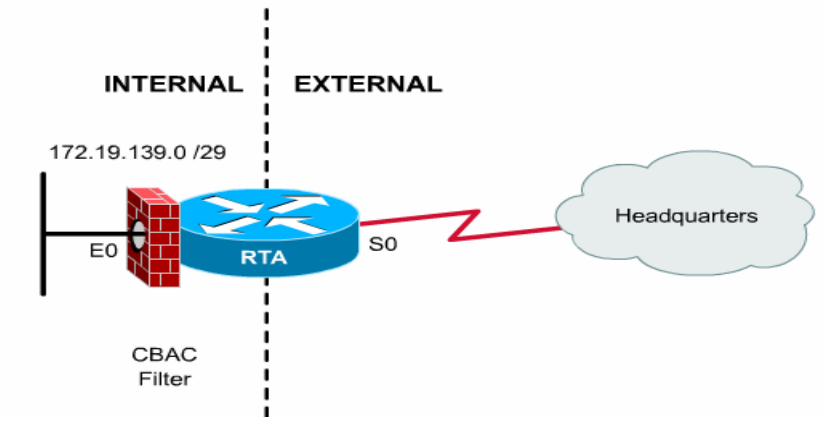
10.5 Context-Based Access Control

Configuring Application-layer Protocols

Command	Purpose
Router(config)# ip inspect name **inspection-name protocol** [alert (on|off)] [audit-trail {on|off}][timeout **seconds**]	Configure CBAC inspection for an application-layer protocol (expect for RPC and JAVA). Use one of the protocol keywords defined in Table 2. Repeat this command for each desired protocol. Use the same inspection-name to create a single inspection rule.
Router(config)# ip inspect name **inspection-name protocol** rpc program-number **number**[wait-time] **minutes**][alert {on|off}] [audit-trail {on|off}] [timeout **seconds**]	Enable CBAC inspection for the RPC application-layer protocol. You can specify multiple RPC program numbers by repeating this command for each program number. Use the same inspection-name to create a single inspection rule.

10.5 Context-Based Access Control

CBAC Configuration Example



10.6 Using an Alternative to Access Lists

Configuring Null Interface