

ZTiT

Zakład Teleinformatyki i Telekomunicacji



LABORATORIUM SIECI

Instrukcja do ćwiczenia: **Firewalling**

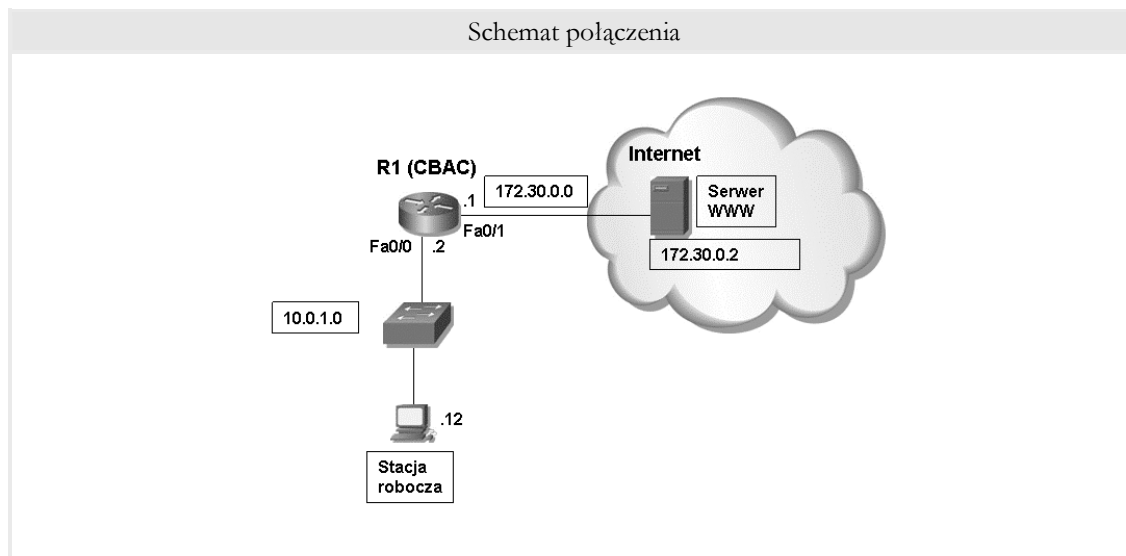
Przedmiot: **Ochrona Informacji w Sieciach OINS**

Wojciech Mazurczyk



Warszawa, kwiecień 2008

ZTiT, Zakład Teleinformatyki i Telekomunicacji
Instytut Telekomunikacji
Wydział Elektroniki i Technik Informatycznych
Politechnika Warszawska



Command	Description
<code>logging on</code>	Enable logging to the console
<code>logging 10.0.P.12</code>	Enable logging to the syslog server
<code>ip inspect audit-trail</code>	Enable the audit trail
<code>show access-lists</code>	Check ACLs
<code>show ip inspect name</code>	View the CBAC configuration and session information.
<code>show ip inspect config</code>	Displays the complete CBAC inspection configuration
<code>show ip inspect interfaces</code>	Displays interface configuration with respect to applied inspection rules and access lists.
<code>show ip inspect sessions detail</code>	Displays existing sessions that are currently being tracked and inspected by CBAC. The optional detail keyword causes additional details about these sessions to be shown.
<code>show ip inspect all</code>	Displays all CBAC configurations and existing sessions that are currently being tracked and inspected by CBAC.

1 Wprowadzenie

Przy stosowaniu firewalli wyróżniamy dwa podstawowe rodzaje sieci: **wewnętrzną** (zaufaną, którą chcemy chronić i zabezpieczać) oraz **zewnętrzną** (niezaufaną; uznaje się że większość zagrożeń pochodzi z niej). **Content-Based Access Control (CBAC)** wykorzystuje dynamiczne listy kontroli dostępu (ACL), w celu poprawy zabezpieczeń sieci wewnętrznej. CBAC zapewnia większy poziom bezpieczeństwa niż klasyczne mechanizmy dostępu na routerach Cisco (np. poprzez listy kontroli dostępu).

2 Define and Apply Inspection Rules and ACLs using IOS CLI

Complete the following steps to define and apply inspection rules and Access Control Lists (ACLs):

- a. Enter global configuration mode on the perimeter router and perform basic router configuration.

```
configure terminal

hostname R1

username admin priv 15 secret cisco
enable secret cisco

interface FastEthernet0/0
description inside
ip address 10.0.1.2 255.255.255.0
no shutdown

interface FastEthernet0/1
description outside
ip address 172.30.1.1 255.255.255.0
no shutdown
```

Configure static routing:

```
ip route 10.0.1.0 255.255.255.0 FastEthernet 0/0
ip route 172.30.1.0 255.255.255.0 FastEthernet 0/1
```

Answer: Explain what these two *ip route* commands are for? What exactly do they configure?

Configure telnet access:

```
line vty 0 4
transport input telnet
login local
```

Configure console access:

```
line console 0
login local
```

Verify configuration:

```
show running-config
show interface
```

- b. On the router, define a CBAC rule to inspect all TCP and FTP traffic.

```
R1(config)# ip inspect name FWRULE tcp timeout 300
R1(config)# ip inspect name FWRULE ftp timeout 300
R1(config)# ip inspect name FWRULE icmp
```

- c. Define the ACLs to allow outbound ICMP traffic and CBAC traffic (FTP and WWW). Block all other inside-initiated traffic.

Configure RFC 2827 filtering - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

```
R1(config)# access-list 100 deny ip 172.30.1.0 0.0.0.255 any
```

RFC 1918 filtering - Address Allocation for Private Internets

```
R1(config)# access-list 100 deny ip host 255.255.255.255 any
R1(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 100 permit ip any any
```

e. Define ACLs to allow inbound ICMP traffic and CBAC traffic (FTP and WWW) to the inside web or FTP server. Block all other outside-initiated traffic.

Configure RFC 2827 filtering - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

```
R1(config)# access-list 101 deny ip 10.0.1.0 0.0.0.255 any
```

Permit ping:

```
R1(config)# access-list 101 permit icmp any host 172.30.1.2 echo-reply
R1(config)# access-list 101 permit icmp any host 172.30.1.2 time-exceeded
R1(config)# access-list 101 permit icmp any host 172.30.1.2 unreachable
R1(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any
```

RFC 1918 filtering - Address Allocation for Private Internets

```
R1(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 101 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 101 deny ip host 255.255.255.255 any
R1(config)# access-list 101 deny ip host 0.0.0.0 any
R1(config)# access-list 101 deny ip any any log
```

f. Apply the ACL to the inside interface:

```
R1(config)# interface fa0/0
R1(config-if)# ip access-group 100 in
```

g. Apply the inspection rule and ACL to the outside interface:

```
R1(config-if)# interface fa0/1
R1(config-if)# ip inspect FWRULE out
R1(config-if)# ip access-group 101 in
R1(config-if)# exit
```

3 Configure Logging and Audit Trails

Complete the following steps to configure logging and auditing trails:

- a. Log into the perimeter router and access global configuration mode.
- b. On the router, enable logging to the console and the Syslog server.

```
R1(config)# logging on
R1(config)# logging console
R1(config)# logging 10.0.1.12
```

- c. Enable the audit trail:

```
R1(config)# ip inspect audit-trail
```

- d. Start the Kiwi Syslog software on the Student PC.

4 Test and Verify CBAC

Complete the following steps to verify and test the firewall configuration.

- a. On the router, use the following commands to verify the CBAC configuration:

```
R1# show ip inspect name FWRULE
R1# show ip inspect config
R1# show ip inspect interfaces
R1# show ip inspect all
```

- b. View the current inspection sessions.

```
R1#show ip inspect sessions
```

(There should not be any active sessions)

- c. Ping 172.30.1.2 from the Student PC command prompt:

```
C:\> ping 172.30.1.2
```

```
Pinging 172.30.1.2 with 32 bytes of data:
Reply from 172.30.1.2: bytes=32 time=34ms TTL=125
Reply from 172.30.1.2: bytes=32 time=34ms TTL=125
Reply from 172.30.1.2: bytes=32 time=34ms TTL=125
Reply from 172.30.1.2: bytes=32 time=36ms TTL=125
```

- d. On the router, use the following command to view the new dynamic ACL.

```
R1# show ip inspect sessions
```

```
Established Sessions
Session 8447EF40 (10.0.1.12:0)=>(172.30.1.2:0) icmp SIS_OPEN
```

e. Use the following commands to view the session detail. This command must be used within 10 seconds of the ping to achieve the results shown below. Repeat the ping if needed.

```
R1# show ip inspect sessions detail
```

```
Established Sessions
Session 84521F20 (10.0.1.12:0)=>(0.0.0.0:0) icmp SIS_OPEN
Created 00:00:04, Last heard 00:00:01
Destinations: 1
Dest addr [172.30.1.2]
Bytes sent (initiator:responder) [128:128]
In SID 172.30.1.2[0:0]=>10.0.1.12[0:0] on ACL 101 (4 matches)
In SID 0.0.0.0[0:0]=>10.0.1.12[14:14] on ACL 101
In SID 0.0.0.0[0:0]=>10.0.1.12[3:3] on ACL 101
In SID 0.0.0.0[0:0]=>10.0.1.12[11:11] on ACL 101
```

f. Wait 10 seconds and reissue the command.

```
R1# show ip inspect sessions
```

Answer: There should not be any active sessions. Why?

g. From the Student PC, telnet to 172.30.1.2.

```
C:\> telnet 172.30.1.2
```

h. Use the following command to view the new dynamic ACL.

```
R1# show ip inspect sessions
```

```
Session 84521F20 (10.0.1.12:4525)=>(172.30.1.2:23) tcp SIS_OPEN
```

Answer: How can this session be identified as a telnet session?

i. Use the following commands to view the session detail.

```
R1# show ip inspect sessions detail
```

```
Established Sessions
Session 84521F20 (10.0.1.12:4597)=>(172.30.1.2:23) tcp SIS_OPEN
Created 00:00:07, Last heard 00:00:05
Bytes sent (initiator:responder) [37:66]
In SID 172.30.1.2[23:23]=>10.0.1.12[4597:4597] on ACL 101 (9 matches)
```

j. Close the telnet session.

k. From the Student PC, use the web browser to connect to 172.30.1.2.

Enter **http://172.30.1.2** in the URL field. Do not enter the password.

l. Use the following command to view the new dynamic ACL.

```
R1# show ip inspect sessions
```

Session 844B5980 (10.0.1.12:4695)=>(172.30.1.2:80) tcp SIS_OPEN

Answer: How can this session be identified as a web session?

m. Use the following commands to view the session detail.

```
R1# show ip inspect sessions detail
```

```
Established Sessions
Session 844B5980 (10.0.1.12:4695)=>(172.30.1.2:80) tcp SIS_OPEN
Created 00:01:51, Last heard 00:01:51
Bytes sent (initiator:responder) [358:338]
In SID 172.30.1.2[80:80]=>10.0.1.12[4675:4695] on ACL 101 (3 matches)
```

n. Return to web browser to enter the password to 172.30.1.2

o. Observe the console or Kiwi Sylog window as the dynamic ACLs entries are removed.

```
00:40:06: %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator
(10.0.1.12:4695) sent 440 bytes -- responder (172.30.1.2:80) sent 823
bytes
```

Answer: How long does a typical TCP session remain open to a device?

Odpowiedz:

Proszę opisać sposób działania CBAC oraz scharakteryzować różnice między CBAC a klasycznymi listami kontroli dostępu (ACL) na podstawie doświadczeń przeprowadzonych w trakcie laboratorium.