

FNS

(Fundamental Network Security)

Ch6. CBAC(Context - based Access Control)

hjlee@dongseo.ac.kr
<http://kowon.dongseo.ac.kr/~hjlee>
<http://crypto.dongseo.ac.kr>

2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

1

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6주차 : CBAC 실습

 이번 강의의 학습목표를 살펴보도록 하겠습니다.

학 습 목 표

- Standard/Extended/Named ACL을 정의할 수 있다.
- Access List를 적용하고, 확인할 수 있다.
- Logging 및 Audit Trail을 설정할 수 있다.
- 검사 규칙 ACL을 정의하고 적용할 수 있다.
- CBAC (Context-based Access Control)을 테스트하고 검증할 수 있다.

완료 인터넷

2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

2

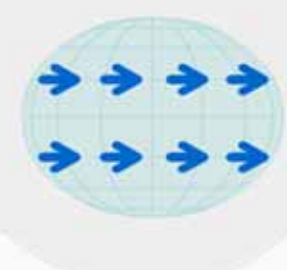
http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 : CBAC 실습

Standard, Extended, Named, Context ACL 실습

목표

- Standard Access List 정의 방법
- Extended Access List 정의 방법
- Named Access List 정의 방법
- Access List 적용 방법
- Access List 확인 방법
- Access List 에 주석 달기



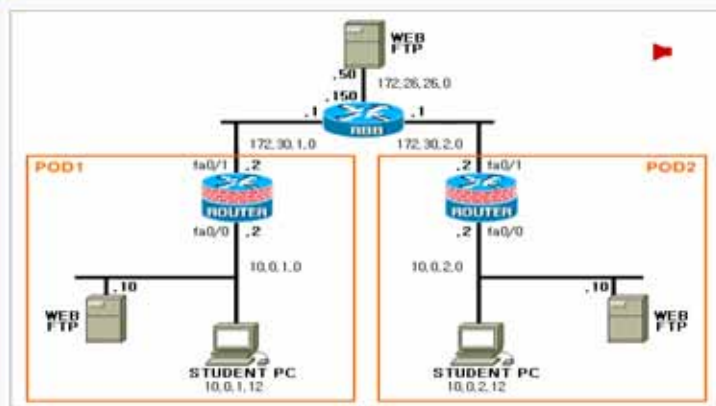
2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 3

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 : CBAC 실습

Standard, Extended, Named, Context ACL 실습

실습 토출로지



실습은 대부분 POD 1 또는 POD 2에 있는 라우터 한대와 Student PC 한대를 가지고 할 수 있다.
POD 1 라우터의 이름은 Router1과 POD 2 라우터의 이름은 Router2로 명명하며, POD 1과 POD 2의 PC는 각각 Student PC1, Student PC2로 명명한다.
본 실습 과정에서 특별한 언급을 하지 않는 한 POD 1 라우터 Router1과 Student PC1을 가정하여 실습을 진행한다.

2005-11-15 4

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6주차 - CBAC 실습

Standard, Extended, Named, Context ACL 실습

실습

제 1 단계: Standard Access Control List **Check**

Q 호스트 10.0.1.12로부터 외부로 나가는 (outbound) 트래픽을 차단하는 standard ACL (ACL number=77)을 작성해본다.
(아래 텍스트 입력란에 access list 77에 대한 syntax를 입력해 보자. <입력 후 Enter>)

A Router(config)#access-list 77 deny 10.0.1.12 0.0.0.0 또는
Router(config)#access-list 77 deny host 10.0.1.12

인터페이스에 access list를 적용하기 전에 POD 1 내부 호스트 10.0.1.12로부터 POD 2 내부 호스트 10.0.2.12로 Ping 테스트를 수행하여 네트워크 연결성을 확인해 본다.
(ping 테스트는 성공할 것인가) **Check**

Q 위의 standard access list 77을 외부 인터페이스 (outside interface)의 라우터 출력 방향 (outbound) 트래픽에 적용하는 명령어를 입력해 보자. (<입력 후 Enter>)

A Router(config)#interface fa0/1
Router(config-if)#ip access-group 77 out

이제 다시 위의 2문제와 같은 ping 테스트를 해보면 트래픽이 차단되어 ping 테스트에 실패함을 확인할 수 있다.

Standard Access List는 1~99 사이의 ACL 넘버를 사용하며, 시스템 관리자로 하여금 임의의 IP 주소 집합이나 특정 IP 주소로부터의 트래픽을 허용(permit)하거나 거절(deny) 한다.

Ping 테스트는 성공한다. 이는 현재 ACL을 정의하기만 했을 뿐 인터페이스에는 아직 적용하지 않았기 때문에 10.0.1.12 호스트로부터의 네트워크 연결성은 아무 문제가 없다.

실습하기

6/17

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 5

http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer

실습 결과

POD 1 라우터 설정하기

1. 설정모드 들어가기
2. 호스트나임 설정하기
3. fastethernet 0/0 설정하기
4. Fastethernet 0/1 설정하기
5. Route 설정하기
6. 재검하기(지금 설정한 모든 설정이 올바르게 동작을 합니다.)

POD 2 설정하기

fa0/0 : 172.30.1.1/24
fa0/1 : 172.30.2.1/24

실습 요약

1. Router>en
1. Router(config)#hostname POD1
2. POD1(config)#interface fastethernet 0/0
3. POD1(config-if)#ip address 172.30.1.1 255.255.0.0
3. POD1(config-if)#no shutdown
3. POD1(config-if)#exit
4. POD1(config)#interface fastethernet 0/1

4. 실행된 Lab5 started

실험장

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 6

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차: CBAC 실습

Standard, Extended, Named, Context ACL 실습

실습

제 2 단계: Extended Access Control List

Q 아래와 같은 파라미터를 갖는 extended ACL을 작성해보자. 단, ACL 번호는 101번으로 한다.

- 호스트 10.0.1.12에서 172.26.26.50으로 가는 ftp 트래픽 차단
- 호스트 10.0.1.12에서 호스트 10.0.2.12로 가는 ICMP 트래픽 차단
- 모든 다른 TCP 트래픽 허용
- 모든 다른 IP 트래픽 허용

(※ 입력 후 Enter)

A

```
Router1(config)#access-list 101 deny tcp host 10.0.1.12 host 172.26.26.50 eq ftp
Router1(config)#access-list 101 deny icmp host 10.0.1.12 host 10.0.2.12
Router1(config)#access-list 101 permit tcp any any
Router1(config)#access-list 101 permit ip any any
```

Q 이제 앞에서 작성한 extended ACL 101을 외부 인터페이스의 라우터 출력 방향에 적용한다. 이를 위한 명령어를 입력해 보자.(※입력 후 Enter)

A

```
Router1(config)#interface fa0/1
Router1(config-if)#ip access-group 101 out
```

Q 이제 ping 테스트나 telnet 연결을 사용하지 않는다. 라우터에 적용된 상기 access list를 확인하는 명령어를 입력해 보자.(※입력 후 Enter)

A

```
Router1#show ip access-lists 101
```

Extended Access List는 시스템 관리자로 하여금 네트워크 트래픽을 훨씬 더 구체적으로 제어할 수 있게 한다. Extended access list는 송신지/수신지 주소 모두를 이용할 수 있으며, 프로토콜이나 포트 번호를 기준으로 트래픽에 대한 필터링도 할 수 있다.

2005-11-15

7

http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer

실습 절차

Extended ACL 설정하기

1. 실행모드 들어가기
2. ACL 101번 작성하기
3. 외부 인터페이스에 ACL 적용하기
4. 적용된 ACL 확인하기
5. ACL 적용 후 Ping 테스트 하기

ACL 번호: 101
조건: 10.0.1.12에서 172.26.26.50으로 가는 ftp 트래픽과 10.0.1.12로 가는 ICMP 트래픽 차단. 모든 다른 TCP/IP 트래픽 허용
외부 인터페이스: fa0/1

실습 명령어

1. Router1 enable
1. Router1(config) terminal
2. Router1(config)#access-list 101 deny tcp host 10.0.1.12 host 172.26.26.50 eq ftp
2. Router1(config)#access-list 101 deny icmp host 10.0.1.12 host 10.0.2.12
2. Router1(config)#access-list 101 permit tcp any any
2. Router1(config)#access-list 101 permit ip any any
3. Router1(config)#interface fa0/1

2005-11-15

http://kowon.dongseo.ac.kr/~hj lee

8

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 : CBAC 실습

Standard, Extended, Named, Context ACL 실습

실습

제 3 단계: Named IP Access Control List **실습**

Q NOPING이라는 이름의 extended access list를 작성해 보자. (※입력 후 Enter)

A Router1(config)#ip access-list extended NOPING

Q 아래와 같은 파라미터를 갖는 extended named ACL을 작성해 보자. (※입력 후 Enter)

- 호스트 10.0.1.12에서 호스트 10.0.2.12로의 icmp 트래픽 차단
- 모든 다른 TCP 트래픽 허용
- 모든 다른 IP 트래픽 허용

A Router1(config-ext-nacl)#deny icmp host 10.0.1.12 host 10.0.2.12
Router1(config-ext-nacl)#permit tcp any any
Router1(config-ext-nacl)#permit ip any any

라우터에의 named ACL 적용과 적용된 named ACL의 확인 방법은 이전과 동일하다.

제 4 단계: Access List에 주석 달기

- ACL에 주석을 달기 위해서는 remark 명령어를 사용한다.
(예) Router1(config-ext-nacl)#remark NOPING is a named ACL.
- running configuration를 보면 ACL에 대한 주석을 볼 수 있다.
(예) Router1#show running-config

완료 **실습하기**

Standard Access List와 Extended Access List에는 이름을 붙일 수 있다. Access List를 명명하는 명령어는 아래와 같다.
단, global configuration mode에서 입력해야 한다.
ip access-list {standard|extended} name

2005-11-15

9

http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer

실습 절차

NAMED Extended ACL 실습

- 실습모드 들어가기
- NOPING이라는 이름의 extended access list를 작성하기
- 일부 인터페이스에 ACL 적용하기
- 적용된 ACL 확인하기
- ACL 적용 후 Ping 테스트 하기

ACL 이름 : NOPING
조건 : 10.0.1.12에서 10.0.2.12로 가는 ICMP 트래픽을 막고 그밖의 icmp와 ip 트래픽은 모두 허용한다.
적용 인터페이스 : Fa0/0

실습 명령어

- Router1>enable
- Router1(config)#terminal
- Router1(config)#ip access-list extended NOPING
- Router1(config-ext-nacl)#deny icmp host 10.0.1.12 host 10.0.2.12
- Router1(config-ext-nacl)#permit tcp any any
- Router1(config-ext-nacl)#permit ip any any
- Router1(config-ext-nacl)#exit

무엇을 Lab0 started

2005-11-15

http://kowon.dongseo.ac.kr/~hjlee

10

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 - CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

목표

- Logging과 Audit Trails 설정
- ACL (Access Control List)에 대한 검사 규칙 정의 및 적용
- CBAC (Context-based Access Control) 테스트 및 확인

2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

11

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 - CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

실습 토론토지

실습은 대부분 POD 1 또는 POD 2에 있는 라우터 한대와 Student PC 한대를 가지고 할 수 있다.
POD 1 라우터의 이름은 Router1로 POD 2 라우터의 이름은 Router2로 명명하며, POD 1과 POD 2의 PC는 각각 Student PC1, Student PC2로 명명한다.
본 실습 과정에서 특별한 언급을 하지 않는 한 POD 1 라우터 Router1과 Student PC1을 가정하여 실습을 진행한다.

2005-11-15

12

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 : CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

실습

제 1 단계: Logging과 Audit Trails 설정

Q Console과 Syslog server로의 logging을 enable 한다.
(단, syslog server는 호스트 10.0.1.12에 설정되어 있다고 한다.) (<입력 후 Enter)

A Router(config)#logging on
Router(config)#logging 10.0.1.12

Q 다음으로 audit trail을 enable 한다.(<입력 후 Enter)

A Router(config)#ip inspect audit-trail

구체적인 logging 정보를 보기 위해서는 show logging 명령어를 사용할 수 있으며,
logging buffer 내의 항목들을 지우기 위해서는 clear logging 명령어를 사용한다.
(예) Router#show logging
(예) Router#clear logging

완료 인터넷

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 13

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 : CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

실습

제 2 단계: ACL에 대한 검사 규칙 정의 및 적용

Q 모든 TCP 및 FTP 트래픽을 검사하기 위한 CBAC 규칙을 정의한다.
단, 검사 규칙명은 CBAC으로 하고 timeout은 5분으로 한다.(<입력 후 Enter)

A Router(config)#ip inspect name CBACRULE tcp timeout 300
Router(config)#ip inspect name CBACRULE ftp timeout 300

Q Outbound ICMP 트래픽과 CBAC 트래픽을 허용하는 ACL을 정의하고, 그 외의 내부에서 발생하는 모든 다른 트래픽은 차단한다. ACL 번호는 101번을 사용한다.(<입력 후 Enter)

A Router(config)#access-list 101 permit icmp any any
Router(config)#access-list 101 permit ip 10.0.1.0.0.0.255 any
Router(config)#access-list 101 deny ip any any

Q Inbound ICMP 트래픽을 허용하는 ACL을 정의하고, 그 외의 외부에서 발생한 다른 모든 트래픽은 차단한다. ACL 번호는 102번을 사용한다.(<입력 후 Enter)

A Router(config)#access-list 102 permit icmp any any

완료 인터넷

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 14

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 - CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

실습

제 2 단계: ACL에 대한 검사 규칙 정의 및 적용

Q 검사 규칙과 ACL 101을 내부 인터페이스 (fa0/0)에 적용한다. (<입력 후 Enter)

A

```
Router(config)#interface fa0/0
Router(config-if)#ip inspect CBACRULE in
Router(config-if)#ip access-group 101 in
```

Q ACL 102를 외부 인터페이스 (fa0/1)에 적용한다.(<입력 후 Enter)

A

```
Router(config)#interface fa0/1
Router(config-if)#ip access-group 102 in
```

완료

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 15

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

6회차 - CBAC 실습

Cisco Router를 이용한 IOS Firewall CBAC 실습

실습

제 3 단계: CBAC 테스트 및 확인

Q CBAC 설정을 확인하는 명령어를 입력해 본다 (총 3개 명령어). (<입력 후 Enter)

A

```
Router(config)#interface fa0/0
Router(config-if)#ip inspect CBACRULE in
Router(config-if)#ip access-group 101 in
```

Q CBAC 설정을 확인하는 명령어를 입력해 본다 (총 3개 명령어). (<입력 후 Enter)

A

```
Router#show ip inspect sessions
Router#show ip inspect sessions detail
Router#show ip inspect all
```

실행하기

완료

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 16

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 17

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 18

End of Lecture



2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

19