Firewall

NeverStop

By CCIEGilbert

ACL 개요

Unit 1. STD ACL

- 방화벽
  - 사전에 지정된 규칙에 따라 특정 패킷을 차단 또는 허용하는 것
- 라우터에서 보안 정책을 설정하는 목적
  - 라우터 자체를 보호하는 것
  - 내부로 향하는 트래픽 중 유해한 것을 라우터가 가장 먼저 탐지하고 차단하는 것
- 라우터 방화벽
  - 라우터에서 제공하는 방화벽기능
  - IOS 방화벽

Standard ACL

Unit 1. STD ACL

- Numbered STD ACL
  - 1 – 99, 1300 – 1999 사이의 번호 사용
  - 출발지 IP 주소만으로 패킷의 허용 여부 판단
- ACL은 하나씩만 사용
  - IPv4, IPv6 프로토콜별
  - 인터페이스벼
  - 입력 및 출력 방향별
- 모든 네트워크
  - 0.0.0.0 255.255.255.255 = any

STD ACL 설정

Unit 1. STD ACL

- 패킷 차단 메시지 보내지 않기
  - R(c-if)# **no ip unreachables**
- ACL 문장 추가
  - % Access rule can't configured …
  - Permit Any 문장에 의해 모든 패킷을 허용했으므로 다시 좁은 범위의 문장을 사용할 수 없다.
- 순서번호 재설정
  - R(c-if)# ip access-list **resequence** IN-ACL 10 10
  - ACL 처음 문장 번호, 번호의 증가폭

Extended ACL

Unit 2. EXT ACL

- EXT ACL
  - 100 – 199, 2000 – 2699 사이의 번호 사용
- DSCP/IP Precedence 값 이용도 가능
  - R(cfg)# ip access-list ext CHK-DSCP
  - R(c-ext-nacl)# permit ip any any **dscp** af11

Extended ACL

Unit 2. EXT ACL

- 분할된 패킷 차단
  - R(cfg)# ip access-list ext NO-FR
  - R(c-ext-nacl)# **deny ip** host 1.1.1.1 ho 2.2.2.2 **fragments**
  - R(c-ext-nacl)# permit ip any any

- Record-Route 옵션 설정된 것 차단
  - R(cfg)# ip access-list ext OP-CTL
  - R(c-ext-nacl)# **deny ip** any any **option record-route**
  - R(c-ext-nacl)# permit ip any any

ACL Log 표시

Unit 2. EXT ACL

- 특정 패킷에 대해 적용된 ACL 내용을 로그로 표시
  - R(cfg)# ip access-list ext SH-LOG
  - R(c-ext-nacl)# deny ip host 1.1.1.1 host 2.2.2.2 **log**
  - R(c-ext-nacl)# permit ip any any
  - 약 5분마다 해당 ACL 문장이 적용된 패킷 수를 표시

- 패킷이 입력된 인터페이스와 함께 로그 표시
  - R(cfg)# access-list 100 permit tcp any any **log-input**
  - R(cfg)# access-list 100 permit ip any any

ICMP Traffic 제어/TCP.UDP 패킷 제어

Unit 2. EXT ACL

- Ping 요청 패킷 및 응답 패킷 허용
  - R(cfg)# ip access-list ext ACL-IN
  - R(c-ext-nacl)# permit **icmp** host 1.1.1.1 host 2.2.2.2 **echo**
  - R(c-ext-nacl)# permit **icmp** host 1.1.1.1 host 2.2.2.2 **echo-reply**
- TCP Debugging
  - R(cfg)# access-list 100 permit tcp any any
  - R# **debug ip packet detail** 100
- Telnet 제어
  - R(cfg)# line vty 0 4
  - R(c-line)# **access-class** TELNET **in**

시간대별 패킷 제어

Unit 2. EXT ACL

- 시간대별 설정 옵션
  - R(cfg)# **time-range** W-HOUR
  - R(c-time-range)# ?
    - **Absolute**: 절대시간 지정
    - **Periodic**: 주기적 시간 지정
    - Daily, Weekdays, Weekend
- 시간대 설정
  - R(cfg)# ip access-list ext ACL-IN
  - R(c-ext-nacl)# deny tcp any host 1.1.1.1 eq telnet **time-range** W-HOUR
- Debugging
  - R# **debug ip packet detail** ACL_번호

IPv6 ACL

Unit 2. EXT ACL

- IPv6 ACL 규칙
  - **이름을 사용한 Extended ACL**만 사용
  - Wildcard Mask를 사용 않고 대신 **/n 형태의 네트워크 마스크**를 사용
  - 인터페이스에 적용할 때 **ipv6 traffic-filter** 명령을 사용
- 설정
  - R(cfg)# ipv6 access-list ACL-IN
  - R(c-ipv6-acl)# permit 89 any any
  - R(c-ipv6-acl)# permit tcp any any echo-request
  - R(c-ipv6-acl)# permit tcp any any echo-reply
  - R(cfg)# int f0/0
  - R(c-inf)# **ipv6 traffic-filter** ACL-IN in

TCP Established

Unit 3. RACL & DACL

- TCP EST 옵션
  - ACL에서 established 옵션을 사용하면 ACK나 RST 비트가 설정된 패킷을 제어할 수 있다.
  - 즉 TCP 세션을 시작할 때는 ASK나 RST 비트가 설정되어 있지 않으므로 ACK나 RST 비트가 설정되어 있지 않은 패킷을 차단하면 외부에서 내부로 세션을 만들 수 없다.
  - 일반 ACL은 인터페이스에 늘 적용되므로 ACK나 RST 비트를 설정하여 속이면 외부에서 접근이 가능하다.

- EST 옵션을 사용한 ACL
  - R(cfg)# ip access-list ext A-IN
  - R(c-ext-nacl)# permit **tcp** any any **established**

RACL

Unit 3. RACL & DACL

- Reflexive ACL
  - Packet이 내부에서 외부로 전송될 때 돌아오는 패킷을 허용하기 위한 임시 ACL을 만드는 것

- RACL 동작 원리
  - 원래 외부로 향하는 TCP 또는 UDP 패킷과 동일한 출발지 및 목적지 포트 번호를 가진다. 이 특징은 TCP와 UDP 패킷에만 적용된다. ICMP, IGMP 등과 같은 프로토콜들은 포트 번호가 없고, 다른 규정이 적용.
  - RACL은 세션 기간동안 변화하는 포트 번호를 사용하는 응용 프로그램에 대해서는 동작하지 않는다.
  - TCP가 아닌 프로토콜들은 패킷 내에 세션의 종료를 추적할 수 있는 정보가 없다.

RACL 설정

Unit 3. RACL & DACL

- RACL 설정 순서
  - 임시 ACL: Packet 검사용 ACL
  - 임시 ACL 적용용 ACL: Evaluate RACL
  - 적용: 2개 ACL 모두

RACL 설정

Unit 3. RACL & DACL

- RACL 설정
  - R(cfg)# ip access-list ext A-OUT
  - R(c-ext-nacl)# per **tcp** any any **reflect RACL**
  - R(c-ext-nacl)# per **udp** any any **reflect RACL**
  - R(c-ext-nacl)# per **icmp** any any **reflect RACL**

  - R(cfg)# ip access-list ext A-IN
  - R(c-ext-nacl)# **permit evaluate RACL**

  - R(c-inf)# ip access-group A-OUT out
  - R(c-inf)# ip access-group A-IN in

DACL

Unit 3. RACL & DACL

- Dynamic ACL = Lock & Key
  - 외부에 나가있는 직원들이 내부의 자원을 접속할 수 있도록 하는 것

- DACL 설정 순서
  - 사용자 계정 생성
  - ACL 생성: Dynamic 포함
  - ACL 적용
  - VTY 설정

DACL 설정

Unit 3. RACL & DACL

- DACL 설정
  - R(cfg)# username user1 passoword cisco1
  - R(cfg)# ip access-list ext A-IN
  - R(c-ext-nacl)# **permit tcp** any host 1.1.23.2 **eq telnet**
  - R(c-ext-nacl)# **dynamic DACL permit ip any any**
  - R(c-if)# ip access-group A-IN in
  - R(cfg)# line vty 0 4
  - R(c-line)# **autocommand access-enable host** timeout 10

CBAC 개요

Unit 4. CBAC

- CBAC(Context-Based Access Control)
  - ACL에서 사용하는 L3/L4 레벨의 트래픽을 제어할 뿐만 아니라 다양한 응용계층의 트래픽을 제어
  - NAT이나 PAT에서 내부 주소까지 변환시켜주며, FTP, H.323과 같이 복수개의 세션을 사용하는 응용프로그램에 대해서도 Stateful 방화벽 기능을 지원
  - **Stateful 방화벽 기능**
    - 외부에서 수신하는 패킷에 대해 내부에서 출발한 것인지 또는 외부에서 시작한 세션인지를 구분할 수 있는 것

CBAC 동작 방식

Unit 4. CBAC

- CBAC 동작 방식
  1. 인터페이스에 CBAC이 설정된 방향으로 패킷을 수신 또는 송신할 때 임시 ACL을 만들어 기존 ACL의 상단에 추가한다.
  2. 해당 세션의 패킷이 돌아올 때 허용한다.
  3. 해당 세션이 끝나면 임시 ACL을 제거한다.

  - TCP 세션의 종료는 FIN 패킷으로 감지하며, FIN 패킷 감지 후 5초가 지나면 상태 테이블에서 해당 세션을 제거
  - UDP 세션은 기본적으로 30초간 해당 트래픽이 없으면 종료된 것으로 간주하고 해당 CBAC 상태 테이블에서 제거
  - ICMP 세션은 10초 이내에 응답이 없으면 해당 엔트리를 제거, 응답시 해당 메시지 타입만 허용

기본적 CBAC 설정

Unit 4. CBAC

- **CBAC 설정**
  - R(cfg)# **ip inspect name** CBAC tcp
  - R(cfg)# ip inspect name CBAC udp
  - R(cfg)# ip inspect name CBAC icmp
- **ACL 설정**
  - R(cfg)# ip access-list ext A-IN
  - R(c-ext-nacl)# permit ospf host 1.1.23.3 any
- **인터페이스 적용**
  - R(cfg)# int f0/0
  - R(c-inf)# **ip inspect** CBAC **out**
  - R(c-inf)# ip access-list A-IN in

응용계층 제어 및 유해 사이트 차단

Unit 4. CBAC

- CBAC 이용한 응용계층 트래픽 제어
  - R(cfg)# ip inspect name CBAC ?
- HTTP만 허용
  - R(cfg)# ip inspect name CBAC **http audit-trail on**
  - Audit-Trail On 옵션
    - 해당되는 패킷의 로그를 표시
- CBAC이 만든 세션 정보
  - R# **show ip inspect sessions detail**

CBAC Timer

Unit 4. CBAC

- CBAC Timer 조정
  - R(cfg)# ip inspect [tcp | udp | dns-timeout] ?
- Name별 별도의 Timer 조정
  - R(cfg)# ip inspect name CBAC **tcp timeout** ?
- 자바 차단
  - CBAC을 이용하면 자바 애플릿을 차단할 수 있다.
  - 압축, 암호화되거나 FTP나 PAM(Port Address Mapping)이 설정되지 않은 비표준 HTTP 포트를 사용하는 경우에는 차단할 수 없다.
  - R(cfg)# ip inspect name CBAC **http java-list** 1
  - R(cfg)# access-list 1 permit 1.1.1.0 0.0.0.255

URL 차단

Unit 4. CBAC

- URL Filtering
  - 유해 사이트 리스트를 유지하는 서버를 이용, 특정 사이트를 차단
  - 시스코 라우터 지원 컨텐츠 필터링 서버: N2H2, WebSense

- URL 차단 동작 순서
  1. 이용자의 트래픽을 라우터가 검사
  2. 트래픽을 목적지 서버와 필터링 서버로 동시에 전송
  3. 필터링 서버가 트래픽을 허용 또는 차단을 결정하여 라우터에게 전송
  4. 차단 트래픽이면 '유해한 내용'이라는 안내문구가 있는 URL을 이용자에게 전송
  5. 허용 트래픽이면 웹 서버로부터의 트래픽을 이용자에게 전송

URL 차단

Unit 4. CBAC

- URL Filtering
  - R(cfg)# ip inspect name CBAC **http urlfilter**
  - 기본포트: N2H2(4005), WebSense(15868)
  - 서버로부터 응답 대기 타임아웃: 기본값 5초, 재전송 횟수는 2회
- URL Filter Server 지정
  - R(cfg)# **ip urlfilter server vendor** [n2h2 | websense] IP_주소
- 직접 허용/차단 도메인 지정
  - R(cfg)# **ip urlfilter exclusive-domain permit** .goodcompany.com
  - R(cfg)# ip urlfilter exclusive-domain **deny** .badcompany.com

URL 차단

Unit 4. CBAC

- URL Filter Cache 크기 조정
  - R(cfg)# **ip urlfilter cache** ?
  - URL 캐시는 12시간 동안 저장, 용량의 80% 이하를 유지
- URL Filter Cache 제거
  - R# **clear ip urlfilter cache** ?
- URL Filter allow-mode
  - R(cfg)# **ip urlfilter allow-mode** [**on** | off]
  - URL Filter가 동작하지 않을 때는 기본적으로 모든 트래픽 차단
  - 모든 트래픽을 통과하려면 On 조정

URL 차단

Unit 4. CBAC

- 동시 요청수 조정
  - R(cfg)# **ip urlfilter max-reuqest** ?
  - 기본적으로 라우터들은 동시 1000개의 URL 요청을 보낼 수 있다. 이 한계를 초과하면 새로운 접속은 Drop된다.
- URL 서버로부터의 응답을 기다리는 접속수 조정
  - R(cfg)# **ip urlfilter max-resp-pak** ?
  - 라우터는 목적지 서버에서 응답이 먼저 오면 URL 서버로부터의 응답을 기다린다. 접속수가 200이 넘어가면 Drop시킨다.

URL 차단

Unit 4. CBAC

- URL Filtering 경고 설정
  - R(cfg)# **ip urlfilter alert**
  - 기본적으로 URL 서버가 다운되거나, 타임아웃되면 URL Filting 경로를 보낸다.

- 감사 기록 설정
  - R(cfg)# **ip urlfilter audit-trail**
  - 누가 HTTP 접속을 시도하는지 등을 알려주는 감사기록이 기본적으로 비활성화되어 있다.

- URL Filtering 동작 확인 명령어
  - R# **show ip urlfilter** [cache | config | statistics]

ZFW

Unit 5. ZFW

- ZFW(Zone-based Policy Firewall)
  - 라우터의 각 인터페이스를 특정 존에 할당하고, 존 사이에 보안 정책을 적용하는 것
  - ZFW는 라우터에서 방화벽 기능을 설정하는 방식을 전용 방화벽인 ASA나 PIX와 유사하게 하였을 뿐만 아니라 기능도 거의 전용 방화벽 수준으로 향상시켰다.

- ZFW 설정방법
  - 존 생성과 할당
  - 존 페어 생성
  - 보안정책 정의
  - 보안정책 적용

Zone 생성 및 할당

Unit 5. ZFW

- Zone 생성
  - R(cfg)# **zone security IN**
  - R(cfg)# **zone security OUT**
- Zone 할당
  - R(cfg)# int f0/0
  - R(c-inf)# **zone-member security IN**
  - R(cfg)# int f0/1
  - R(c-inf)# **zone-member security OUT**
- Zone 확인
  - R# **show zone security**

Security Zone 설정시 적용 가이드라인

Unit 5. ZFW

- Guideline
  - 보안 존에 소속된 인터페이스는 CBAC을 설정할 수 없다. 즉 한 인터페이스에 ZFW와 CBAC을 동시에 설정할 수 없다.
  - **한 인터페이스는 오직 하나의 존에만 소속된다.**
  - 한 인터페이스가 보안 존에 소속되면 Policy Map에서 명시적으로 허용되지 않는 한 해당 인터페이스를 통해 입출력되는 모든 트래픽이 차단
  - 어느 보안 존에도 소속되지 않은 인터페이스는 보안 존에 소속된 인터페이스와 통신할 수 없다. Policy Map은 두 개의 존 사이에만 적용
  - 보안 존에는 ACL을 적용할수 없으나, 존 멤버 인터페이스는 ACL을 적용 가능하다.
  - **동일 보안 존에 소속된 인터페이스 간에는 자유로이 패킷이 허용된다.**
  - **서로 다른 존에 소속된 패킷들은 기본적으로 모두 차단된다.**

Zone Pair 설정

Unit 5. ZFW

- Zone Pair 설정
  - R(cfg)# **zone-pair security** IN-OUT **source** IN **destination** OUT
  - R# **show zone-pair security**
- Zone Pair 생성
  - 2개의 존간에 단방향의 방화벽 정책을 정의할 수 있다.
  - 2개의 존이 있고, 양방향의 트래픽을 허용하려면 각 방향당 하나씩의 존 페어를 만들어야 한다. 그러나 Return Traffic은 자동으로 허용되므로 항상 2개의 존 페어를 만들 필요는 없다.
- **Default Self Zone**
  - 시스템에서 정의한 존이며, 멤버가 없다.
  - 셀프 존이 포함된 존 페어는 해당 라우터가 최종 목적지이거나 해당 라우터에서 시작되는 트래픽을 제어할 때 사용한다.

보안정책 정의와 적용

Unit 5. ZFW

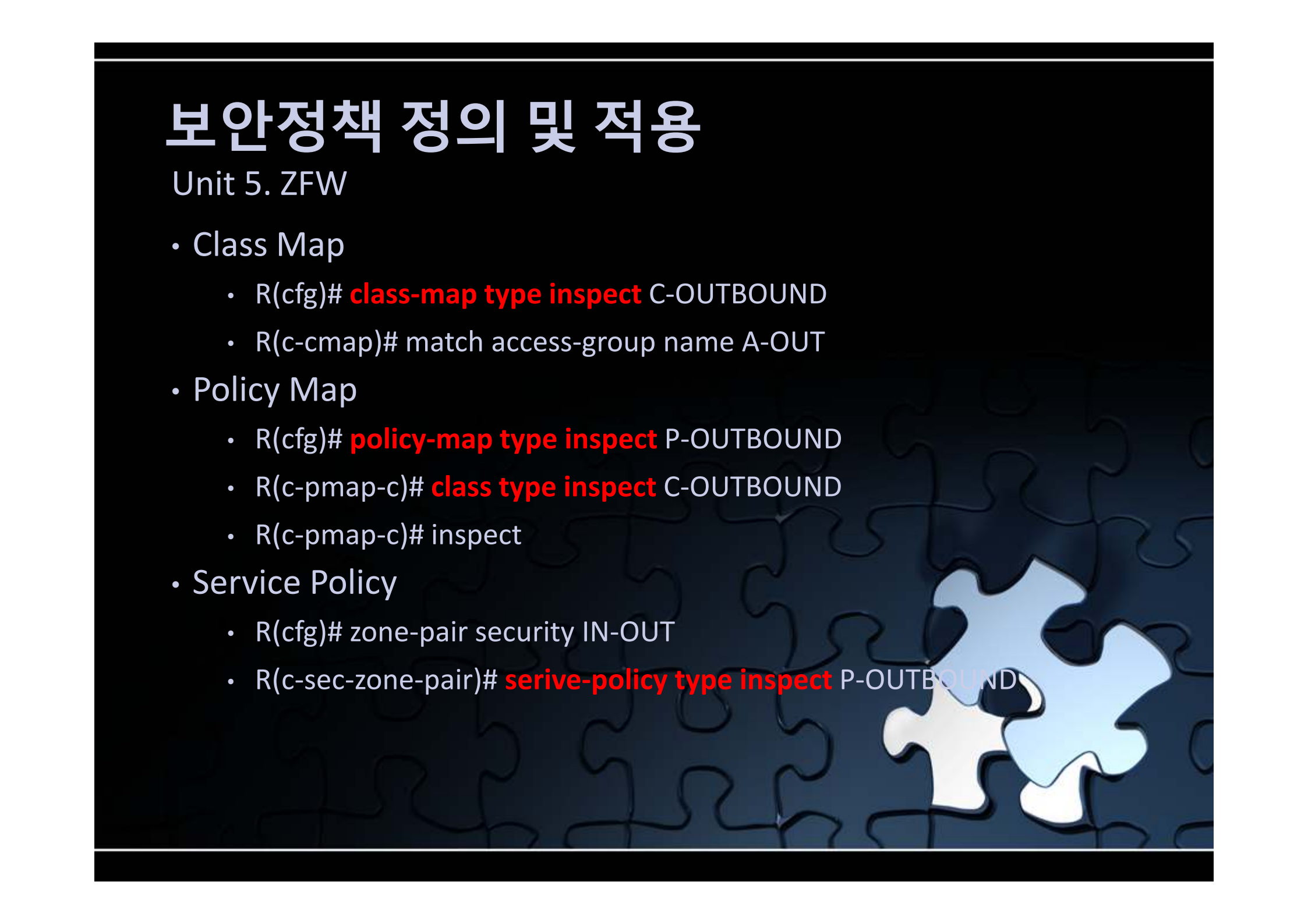
- **CPL** 이용한 보안정책 정의 및 적용
  - QoS의 MQC와 거의 같다.

- 설정 순서
  - Class-Map: 트래픽 분류
  - Policy-Map: 정책 정의(3가지 액션)
    - **Drop**: 기본 동작, ZFW은 종단장비에게 폐기 통지를 하지 않는다.
    - **Pass**: 패킷 통과, 접속이나 세션 정보를 기록하지 않는다. 돌아오는 패킷을 자동으로 허용하지 않는다.
    - **Inspect**: 패킷 통과, 접속 및 세션정보를 유지하여 돌아오는 패킷을 허용
  - Service-Policy

보안정책 정의 및 적용

Unit 5. ZFW

- Class Map
  - R(cfg)# **class-map type inspect** C-OUTBOUND
  - R(c-cmap)# match access-group name A-OUT
- Policy Map
  - R(cfg)# **policy-map type inspect** P-OUTBOUND
  - R(c-pmap-c)# **class type inspect** C-OUTBOUND
  - R(c-pmap-c)# inspect
- Service Policy
  - R(cfg)# zone-pair security IN-OUT
  - R(c-sec-zone-pair)# **serive-policy type inspect** P-OUTBOUND



ZFW와 ACL 관계

Unit 5. ZFW

- Zone에 소속된 인터페이스에 적용된 ACL과 ZFW의 동작 방식
  1. 패킷을 수신하면 ACL이 먼저 적용
  2. ACL이 통과시킨 패킷들에대해 ZFW가 적용

다수 인터페이스간 ZFW 설정

Unit 5. ZFW

- Zone 생성
  - R(cfg)# zone security IN
  - R(cfg)# zone security OUT
  - R(cfg)# zone security DMZ

출발존	목적존	허용 트래픽
IN	OUT	HTTP, HTTPS, DNS, ICMP
OUT	IN	X
IN	DMZ	SSH, FTP, POP, IMAP, SMTP, HTTP
DMZ	IN	X
DMZ	OUT	X
OUT	DMZ	HTTP, DNS, SMTP

ZFW 이용한 응용계층 제어

Unit 5. ZFW

- L7 Traffic 제어
  - L7 Class Map을 이용하여 특정 응용계층 트래픽을 분류
  - L7 Policy Map에서 특정 트래픽에 대한 동작을 정의
  - L3/L4 Class Map으로 특정 L3/L4 트래픽을 분류
  - L3/L4 Policy Map에서 L3/L4 클래스 맵을 불러, L7 폴리시 맵을 적용
  - L3/L4 Policy Map을 존 페어에 적용

- L7 Class-map으로 분류할 수 있는 프로토콜
  - R(cfg)# class-map type inspect ?

L7 Traffic Control

Unit 5. ZFW

- Parameter Map
  - R(cfg)# parameter-map type regex URI_BAD
  - R(c-profile)# pattern .*gambling
  - R(c-profile)# pattern .*game
- L7 Class Map
  - R(cfg)# class-map type inspect http C:BAD
  - R(c-cmap)# match request uri regex URI_BAD
- L7 Policy Map
  - R(cfg)# policy-map type inspect http P:BAD
  - R(c-pmap)# class type inspect http C:BAC
  - R(c-pmap-c)# log

ZFW Policing

Unit 5. ZFW

- ZFW Policing
  - ZFW에서 Policing을 시킬 수 있다.
  - ZFW Policing의 방향은 존 페어의 방향을 따른다.
  - 인터페이스에서 MQC 폴리싱이 설정되어 있는 경우에는 MQC 입력 폴리싱, ZFW 폴리싱, MQC 출력 폴리싱의 순서로 적용된다.

NAT 종류

Unit 6. NAT

구분	NAT 이름	내용
변환 IP 주소 수량	NAT	N:N 변환
	PAT	1:N 또는 M:N 변환
변환 IP 주소 지정	정적 NAT	1:1 변환 (변환 IP 주소 지정)
	동적 NAT	변환 IP 주소 지정하지 않음
변환 목적에 따른 분류	PAR (Port Address Redirection)	TCP/UDP 포트번호별 변환주소 지정
	트래픽 분산 NAT	다수의 서버 IP를 하나의 IP로 변환
	중복 NAT(Overlapping)	동일한 네트워크 주소간의 변환
NAT 이중화	NAT with HSRP	HSRP를 이용한 NAT 이중화
	SNAT	Stateful NAT 이중화

동적 NAT/PAT

Unit 6. NAT

- NAT 설정 순서
  1. 사설 IP주소 지정
     - R(cfg)# **ip access-list standard** …
  2. 공인주소 풀 지정
     - R(cfg)# **ip nat pool** 시작주소 끝주소 **netmask** 서브넷마스크
  3. 사설과 공인 주소 풀 연결
     - R(cfg)# **ip nat inside source list** 사설_ACL **pool** 공인주소풀 **overload**
  4. 인터페이스 지정
     - R(c-inf)# **ip nat [outside | inside]**
- NAT 확인
  - R# **show ip nat translations (verbose)**

Interface를 이용한 PAT

Unit 6. NAT

- Interface를 이용한 PAT
  - 별도의 공인 IP 주소 풀을 지정하지 않고, 인터페이스 명을 지정해도 된다.

- Interface 이용 설정
  - R(cfg)# ip nat inside source list PRIVATE **interface** f0/0 overload

정적 NAT

Unit 6. NAT

- 정적 NAT
  - 변환되는 두 IP주소를 미리 지정하는 것
  - 사설 IP주소를 사용하는 서버를 인터넷을 통해 접속할 수 있게 한다.

- 정적 NAT 설정
  - R(cfg)# ip nat source static 사설주소 공인주소

PAR

Unit 6. NAT

- **PAR(Port Address Redirection)**
  - TCP나 UDP의 포트 번호 별로 목적지 IP주소를 다르게 변환시키는 것
  - 사설 IP주소를 사용하는 DNS, WEB, FTP 등의 서버 주소를 변환시킬 공인 IP주소가 부족할 때 유용
  - 동일한 주소로 접속되는 트래픽이라 하더라도 HTTP 트래픽이면 10.1.1.3으로, 텔넷이면 10.1.4.4로 연결시키고자 할 때 사용

- 설정 방법
  - R(cfg)# **ip nat inside source static tcp** 10.1.3.3 80 2.2.2.201 **80**
  - R(cfg)# ip nat inside source static tcp 10.1.4.4 23 2.2.2.201 23

Extended ACL을 사용한 PAT

Unit 6. NAT

- 목적지 별 서로 다른 공인 IP주소 사용 → 변환하는 방법
  - Extended ACL 사용한 PAT
  - Route-Map 사용한 NAT 또는 PAT

- Extended ACL 사용한 PAT
  - R(cfg)# ip nat pool PUBLIC-1 시작주소 끝주소 **prefix-length** …
  - R(cfg)# ip nat pool PUBLIC-2 시작주소 끝주소 prefix-length …

  - R(cfg)# ip nat inside source list ACL-1 pool PUBLIC-1 overload
  - R(cfg)# ip nat inside source list ACL-2 pool PUBLIC-2 overload

Route-Map 이용한 Dynamic NAT

Unit 6. NAT

- Route-Map 사용한 NAT
  - ACL 작성: 외부 연결주소
  - 공인주소 풀 작성
  - Route-Map 작성
    - 사설 주소 연결
    - R(cfg)# **route-map** PRI-1
    - R(c-route-map)# **match ip address** N-Private
  - Route-Map과 공인주소 풀 연결
    - R(cfg)# **ip nat inside source route-map** PRI-1 pool PUB-1 overload

NAT 이중화

Unit 6. NAT

- NAT 이중화
  - 한 NAT 장비가 동작하지 않을 때 다른 NAT 장비를 동작시키는 것

- NAT 이중화 구분
  - HSRP만을 이용한 NAT 이중화
  - SNAT을 이용한 NAT 이중화

- **SNAT(Stateful NAT)** = Stateful NAT Failover
  - 백업으로 동작하는 NAT 장비가 원래의 NAT 장비가 가진 NAT 테이블을 그대로 물려받는 것

HSRP만 이용한 NAT 이중화

Unit 6. NAT

- HSRP에 NAT 설정
  - R(cfg)# int f0/0
  - R(c-inf)# **standby 1 name** HSRP-NAT
  - R(cfg)# ip nat inside source static ... ... **redundancy** HSRP-NAT
  - Standby Router에서도 Active Router의 NAT 변환정보를 받아 동기화 한다.
- HSRP만을 이용한 NAT 이중화는 Static NAT만 지원한다.

SNAT/HSRP를 이용한 NAT 이중화

Unit 6. NAT

- SNAT 설정
  - R(c-inf)# **standby 1 name** HSRP-NAT
  - R(cfg)# **ip nat stateful id 1**
  - R(c-ipnat-snat)# **redundayncy** HSRP-NAT
  - R(c-ipnat-snat-red)# **mapping-id 10**

  - R(cfg)# ip nat inside source list … pool … **mapping-id 10** overload
- SNAT
  - Static NAT과 Dynamic NAT 모두 지원
  - IP 헤더 이후에 존재하는 주소에 대한 변환은 지원하지 않는다.
    - FTP, TFTP, 비대칭 라우팅 등은 지원하지 않는다.

SNAT/Routing 이용한 NAT 이중화

Unit 6. NAT

- SNAT/Routing 이용한 NAT 이중화
  - R(cfg)# **ip nat stateful id 1**
  - R(c-ipnat-snat)# [**primary | backup**] 자신_주소
  - R(c-ipnat-snat-pri)# **peer** 상대방_주소
  - R(c-ipnat-snat-pri)# **mapping-id 10**

  - R(cfg)# **route-map** SNAT-MAP
  - R(c-route-map)# match ip address PRIV

  - R(cfg)# ip nat inside source route-map SNAT-MAP pool PUB **mapping-id 10** overload
  - R(cfg)# ip nat inside source static 내부주소 외부주소 **mapping-id 10**

방화벽 기본 설정

Unit 7. FW

- ASA & PIX
  - 시스코의 전용 방화벽
  - 동일 명령체계 사용
  - 비교적 새로운 장비인 ASA가 성능과 기능이 우수
    - PIX에서는 지원하지 않는 SSL VPN 기능이 제공
    - AIP-SSM(Advanced Inspection and Prevention Security Services Module) 모듈을 장착하면 IPS 기능이 지원된다.
    - CIC-SSM(Content Security and Control SSM)을 장착하면 바이러스 방지, 스파이웨어 방지, 파일 차단, 스팸 차단, 피싱 차단, URL 차단, 컨텐트 필터링 등의 기능을 제공

방화벽 기본 설정

Unit 7. FW

- ASA의 초기 프롬프트
  - ciscoasa> enable
  - 초기 패스워드는 없다.
- 현재 설정값 확인 및 설정값 저장
  - FW# show running-config
  - FW# wr
- 현재 설정값 초기화(설정 모드)
  - FW(cfg)# **clear config all**

방화벽 기본 설정

Unit 7. FW

- 저장 내용 삭제 및 재부팅
  - FW# **write erase**
  - FW# reload
- 하드웨어, 소프트웨어 정보 확인
  - FW# show version
- 장비 이름 지정
  - pixfirewall(cfg)# hostname FW

방화벽 기본 설정

Unit 7. FW

- 단축 명령어 사용
  - FW(cfg)# **command-alias** exec c conf t
  - FW(cfg)# command-alias exec r sh run
- 현재 동작 상태 확인
  - FW# **show firewall**
  - 방화벽은 L2 또는 L3로 동작시킬 수 있다.
    - L2: **Transparent Mode**, L3: **Router Mode**
  - 라우터 모드/트랜스패런트 모드로 변경
  - FW(cfg)# no firewall transparent
  - FW(cfg)# **firewall transparent**

방화벽 기본 설정

Unit 7. FW

- Context 기능 확인
  - FW# **show mode**
  - Context: 하나의 방화벽을 복수개의 방화벽으로 동작
    - 하나의 장비로 동작: Single Mode, 복수개 장비로 동작: Multiple Mode
- 관리자용 암호와 텔넷 암호 지정
  - FW(cfg)# enable password cisco
  - FW(cfg)# **passwd** cisco
- 인터페이스 상태 확인
  - FW# **show interface ip brief**

방화벽 인터페이스 설정

Unit 7. FW

- 인터페이스 설정
  - FW(cfg)# int e0
  - FW(c-if)# **nameif inside**
  - FW(c-if)# ip address 네트워크 서브넷마스크
    - ASA/PIX는 모든 인터페이스에 nameif 명령어를 사용하여 이름 부여
    - 이후 대부분 설정에서 물리적 인터페이스 대신 이름 사용
    - 인터페이스 이름을 inside로 지정하면 기본적으로 보안레벨이 100으로 설정
    - 인터페이스 이름을 inside 아닌 다른 것으로 지정하면 기본적으로 보안레벨이 0으로 설정
  - 인접 장비와방화벽 사이는 기본적으로 Ping이 된다.

방화벽 라우팅 설정

Unit 7. FW

- FW 설정
  - FW(cfg)# route outside 0 0 1.1.30.2
  - FW(cfg)# router ospf 1
  - FW(c-router)# network 1.1.20.2 255.255.255.255 area 0
  - FW(c-router)# default-information originate
    - **방화벽에선네트워크 지정시 와일드 카드 대신 서브넷 마스크 사용**
  - 방화벽에서 지원되는 라우팅
    - Static, RIP, EIGRP, OSPF
- 정적 경로 및 동적 경로 설정 확인
  - FW(cfg)# **show run route**
  - FW(cfg)# **show run router**

방화벽 라우팅 설정

Unit 7. FW

- IOS와 ASA/PIX 명령어 차이
  - ASA/PIX는 IOS와 달리 설정모드에서도 show 명령어 사용 가능하다.
  - ASA/PIX는 IOS와 달리 대부분 명령어에서 ip가 빠져 있다.

- OSPF Neighbor 확인
  - FW(cfg)# **show ospf neighbor**

- 라우팅 테이블 확인
  - FW(cfg)# **show route**

방화벽 동작 확인

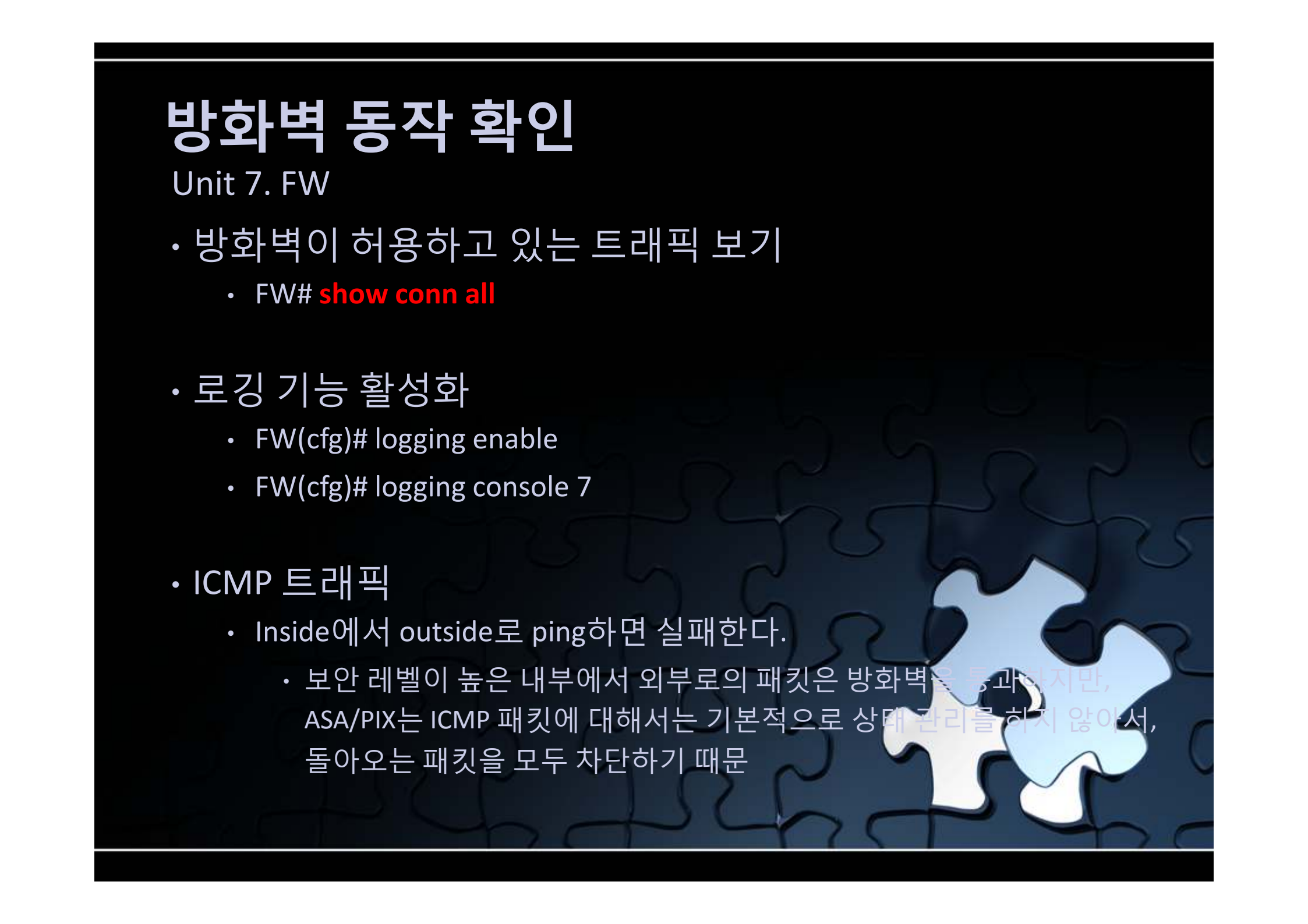
Unit 7. FW

- 기본적 방화벽의 동작 확인
  - 보안 레벨이 높은 인터페이스에서 낮은 인터페이스로의 트래픽은 모두 허용된다.
    - 반면에 보안 레벨이 낮은 인터페이스에서 높은 인터페이스로의 트래픽은 모두 차단된다.
  - TCP/Udp와 같은 Statefull한 트래픽은 보안 레벨이 높은 곳에서 낮은 곳으로 갔다가 들어오는 패킷들도 허용된다.
    - 즉, 외부에서 오는 패킷들 중에서 포트 번호 등의 정보를 이용하여 확인 후, 내부에서 시작된 것들은 허용된다.

방화벽 동작 확인

Unit 7. FW

- 방화벽이 허용하고 있는 트래픽 보기
  - FW# **show conn all**
- 로깅 기능 활성화
  - FW(cfg)# logging enable
  - FW(cfg)# logging console 7
- ICMP 트래픽
  - Inside에서 outside로 ping하면 실패한다.
    - 보안 레벨이 높은 내부에서 외부로의 패킷은 방화벽을 통과하지만, ASA/PIX는 ICMP 패킷에 대해서는 기본적으로 상태 관리를 하지 않아서, 돌아오는 패킷을 모두 차단하기 때문



텔넷을 통한 ASA/PIX 접속

Unit 8. FW 접속 제어

- FW Telnet 접속
  - PC에서 방화벽으로 텔넷을 하면 안된다.
    - 기본적으로 ASA/PIX로의 텔넷이 차단되기 때문
- FW Telnet 허용 – 내부 컴퓨터
  - FW(cfg)# telnet 1.1.10.0 255.255.255.0 inside
- FW Telnet 허용 – 외부 라우터
  - FW(cfg)# telnet 1.1.20.2 255.255.255.255 outside
  - 텔넷 실패
    - 보안레벨이 가장 낮은 인터페이스를 통한 ASA/PIX로의 텔넷은 차단되기 때문
  - FW(cfg)# int e1
  - FW(c-if)# security-level 100

SSH를 통한 ASA/PIX 접속

Unit 8. FW 접속 제어

- SSH(Secure Shell)
  - 패킷을 보호하기 위한 암호화 기능 및 패킷 변조 확인 기능이 제공
  - 버전 1과 버전 1의 취약성을 보완한 버전 2가 있다.
  - SSH를 사용하면 ASA/PIX의 보안 레벨이 가장 낮은 인터페이스를 통하여도 접속이 가능하다.

- SSH 설정
  - FW(cfg)# username admin password cisco123
  - FW(cfg)# aaa authentication ssh console LOCAL
  - FW(cfg)# crypto key generate rsa modulus 1024
  - FW(cfg)# ssh 1.1.10.1 255.255.255.255 inside
  - FW(cfg)# ssh 1.1.20.2 255.255.255.255 outside

SSH를 통한 ASA/PIX 접속

Unit 8. FW 접속 제어

- SSH 접속
  - SSH 접속을 위해서는 이용자명과 패스워드가 필요하다
  - 기본적으로는 ASA의 이용자명은 ciscoasa이고 패스워드는 password 이다.
  - PIX는 이용자명이 pix이고 패스워드는 cisco이다.

- FW 접속
  - R# ssh –l 사용자명 주소
  - 텔넷과 달리 SSH를 이용하면 보안 레벨이 가장 낮은 인터페이스를 통해서도 방화벽과 연결된다.

ASDM 설치

Unit 8. FW 접속 제어

- ASDM(Adaptive Security Device Manager)
  - GUI 방식으로 ASA/PIX를 설정하고 모니터링할 수 있게 하는 S/W
- ASDM 설치
  1. ASDM.bin 파일을 tftp 서버에 복사
  2. 적당한 tftp 서버를 동작시키고 upload/download 폴더를 조정
  3. ASDM 파일을 FW로 복사
     - FW# copy tftp flash
  4. ASA/PIX에서 ASDM 동작을위해 HTTP 서버를 활성화하고, ASDM 접속을 위해 HTTPS를 허용
     - FW(cfg)# http server enable
     - FW(cfg)# http 1.1.10.1 255.255.255.255 inside
  5. 브라우저 창에 https://1.1.20.1을 입력하여 접속(이용자명, 아무숫자)

방화벽 ACL

Unit 9. FW ACL

- FW ACL
  - 라우터의 ACL과 거의 유사
  - 기본적으로 L2/L3/L4 트래픽을 ACL을 이용하여 차단 또는 허용
  - 응용계층의 트래픽을 포함한 상세한 트래픽의 제어는 MPF를 이용
  - NAT 설정할 때도 ACL을 사용할 수 있다.
- FW ACL 종류
  - Standard ACL
  - Extended ACL
  - IPv6 ACL
  - Ethertype ACL
  - Web Type ACL

방화벽 ACL 종류

Unit 9. FW ACL

- Standard ACL
  - OSPF 경로의 목적지 IP주소만 제어, OSPF 재분배 Route-MAP에 사용
  - 인터페이스에 적용할 수 없다.
- Extended ACL
  - 방화벽에서 가장 많이 사용
- IPv6 ACL
  - IPv6 트래픽 제어
- Ether Type ACL
  - L2 모드 방화벽에서 트래픽 제어
- Web Type ACL
  - Clientless SSL VPN 트래픽 제어

ACL 설정 및 동작 확인

Unit 9. FW ACL

- Extended ACL 설정 및 적용
  - FW(cfg)# access-list 이름 [standard | extended] [permit | deny] 프로토콜 출발지 S_M 목적지 S_M 연산자 포트번호
    - EXTENDED: 이 옵션을 지정하지 않아도 자동으로 설정
    - HOST: 하나의 IP주소만 지정시
    - 여러 개의 주소를 지정할 때 와일드카드가 아닌 SUBNET MASK 사용
    - TCP나 UDP 옵션을 제어하는 경우에는 출발지/목적지 포트 번호 또는 이름을 지정
  - 포트 번호 지정시의 옵션
    - **Neq**: Port not equal to operator
    - **Range**: Port range operator

ACL 설정 및 동작 확인

Unit 9. FW ACL

- Extended ACL 추가적 옵션
  - **Inactive**
    - ACL 내부의 특정 ACE(Access Control Entry)를 비활성화
  - Log
  - Object-group
  - Time-range

  - TIP
    - **라우터와 달리 방화벽에선 자신이 목적지인 패킷은 기본적으로 허용**
    - 인접라우터에서 전송하는 OSPF 패킷은 ACL에서 별도로 허용하지 않아도 된다.

ACL 적용과 확인

Unit 9. FW ACL

- ACL 적용
  - FW(cfg)# **access-group** 이름 [**in | out**] **interface** 인터페이스이름
- 각 ACE별 적용된 내용 확인
  - FW(cfg)# **show access-list**
- ACL 내용 확인
  - FW(cfg)# **show run access-list**

ACL 수정

Unit 9. FW ACL

- 특정 위치에 새로운 ACE 추가
  - FW(cfg)# access-list 이름 line 번호 …
- 하나의 ACE 제거
  - FW(cfg)# no access-list 이름 …
- 전체 ACL 제거
  - FW(cfg)# **clear configure access-list** 이름
- ACL 적용 확인
  - FW(cfg)# **show run access-group**
    - 특정 ACL을 삭제하면 해당 ACL 적용된 것도 따라서 삭제된다.

Extended ACL 로그 생성 및 해석

Unit 9. FW ACL

- Remark 옵션
  - FW(cfg)# access-list 이름 **remark** 주석
    - ACL 만들 때 remark 옵션을 사용하여 적당한 설명을 달면 장애처리 및 ACL 해석시 편리
- Extended ACL 로그
    - 기본적으로 차단되는 패킷들은 패킷 수만큼 모두 로그를 남긴다.
    - 그러나 허용되는 패킷은 각 세션당 하나씩만 기록한다.
- Log Message 생성
  - FW(cfg)# logging enable
  - FW(cfg)# logging console 7
    - 차단 ACE에 해당되는 트래픽은 모든 패킷에 대해 로그 메시지 생성
    - 허용 ACE에 해당되는 것은 세션의 시작과 끝만 로그메시지 생성

Log 옵션

Unit 9. FW ACL

- Log 옵션 지정
  - FW(cfg)# access-list 이름 … **log** 심각도 **interval** 초
    - Log 옵션 사용
      - 해당 ACE 적용 패킷에 대해 기존 메시지 106023 대신 106100 생성
    - 로그 106100를 사용 로깅 활성화
      - 각 차단 패킷에 대해 로그 메시지를 생성하는 대신, 각 ACE별로 통계 제공
      - 생성되는 시스템 메시지의 수 제한
    - 로그 메시지의 심각도(Severity): 0 – 7 사이의 값 또는 해당값 이름 지정
      - 기본적으로 심각도 6의 메시지 생성
    - Interval: 1 – 600초 사이의 값 , 로그 메시지 생성 주기 지정
      - 기본값은 300초(5분)

Log 옵션

Unit 9. FW ACL

- Log 옵션 지정
  - ACL에 있는 ACE만 로그 메시지 생성
    - 모든 차단 패킷에 대해 로그 메시지 생성하려면 deny ip any any log와 같이 명시적으로 모든 패킷을 차단
  - 106100 메시지 로깅이 활성화되면 특정 ACE에 해당되는 패킷에 대해 Flow Control을 만들어 특정 기간동안 수신한 패킷의 수를 추적
    - Flow Control은 출발지/목적지 IP주소, 프로토콜 종류, 포트 번호로 구분
  - 모든 차단 패킷에 대해 로그 메시지를 생성하는 대신, 주기적으로 특정 Flow Entry에 대한 통계치를 보여준다.
  - 허용 패킷에 대한 히트 카운트는 증가시키지 않는다.

차단 Flow 관리

Unit 9. FW ACL

- 차단 Flow 관리
  - ASA는 최대 32K Logging Flow를 가진다.
  - 메모리와 CPU가 로깅을 위해 무제한 할당되는 것을 방지하기 위해 동시 차단 Flow의 수를 제한
  - 최대치에 도달하면 기존 Flow가 만료될 때까지 새로 만들지 않는다.
- 차단 로그 Flow 수 조정
  - FW(cfg)# **access-list deny-flow-max** ?
    - 기본값 4096
- 메시지 간격 조정
  - FW(cfg)# **access-list alert-interval** ?
    - 기본값 300초
    - 1 – 3600초 사이의 값으로 조정

IPv6 ACL

Unit 9. FW ACL

- IPv6 ACL 설정
  - FW(cfg)# **ipv6 access-list** 이름 [permit | deny] 프로토콜 출발지 목적지 연산자 포트번호
- IPv6 ACL 적용
  - FW(cfg)# access-group 이름 [in | out] interface 이름
- IPv6 ACL 설정 확인
  - FW(cfg)# **show running-config ipv6**
  - FW(cfg)# **show ipv6 access-list**

Object Group

Unit 9. FW ACL

- Object Group
  - 특정한 IP주소나 네트워크 등을 이름으로 정의하고 이를 ACL 등 필요한 설정에서 불러 사용
  - FW(cfg)# **object-group** ?
  - 4가지 종류
    - **Icmp-Type**
    - **Nework**
    - **Protocol**
    - **Service**

Object Group

Unit 9. FW ACL

- ICMP Type 지정
  - FW(cfg)# object-group icmp-type …
  - FW(c-icmp)# icmp-object …
- Network 지정
  - FW(cfg)# object-group network …
  - FW(c-network)# network-object 네트워크 서브넷마스크
- Protocol 지정
  - FW(cfg)# object-group protocol …
  - FW(c-protocol)# protocol-object …
- Service 지정
  - FW(cfg)# object-group service … ?
    - TCP, TCP-UDP, UDP, <CR>

Object Group

Unit 9. FW ACL

- Object Group을 ACL에서 부르기
  - FW(cfg)# access-list I-I deny tcp any object-group 이름
- Object Group 확인
  - FW(cfg)# **show run object-group**
- Object Group 적용 확인
  - FW(cfg)# show access-list
    - Object Group이 아닌 실제 내용이 표시
- Nesting 기능
  - Object Group에서 또 다른 Object Group을 호출할 수 있다.
  - FW(cfg)# object-group network …
  - FW(c-network)# **group-object** …

Time Range

Unit 9. FW ACL

- 시간대별 트래픽 제어
  - 라우터와 마찬가지로 방화벽에서도 시간대별로 트래픽을 제어
  - FW(cfg)# **time-range** 이름
  - FW(c-time-range)# ?
    - **Absolute**: 절대적 시간 지정
    - **Periodic**: 주기적 시간 지정
- 주중 시간대 지정
  - FW(cfg)# time-range WorkHour
  - FW(c-time-range)# peiodic weekdays 09:00 to 18:00
- 시간대를 ACL에서 호출
  - FW(cfg)# access-list 이름 … **time-range** WorkHour

FW NAT

Unit 10. FW NAT/PAT

- 동작방식에 다른 분류
  - 동적 NAT/PAT
  - 정적 NAT/PAT
  - Policy NAT/PAT
  - Bypass NAT

- **NAT 명령어 적용순서**
  1. NAT 면제
  2. 정적 NAT/PAT
  3. Policy Dynamic NAT
  4. 일반 동적 NAT

동적 NAT

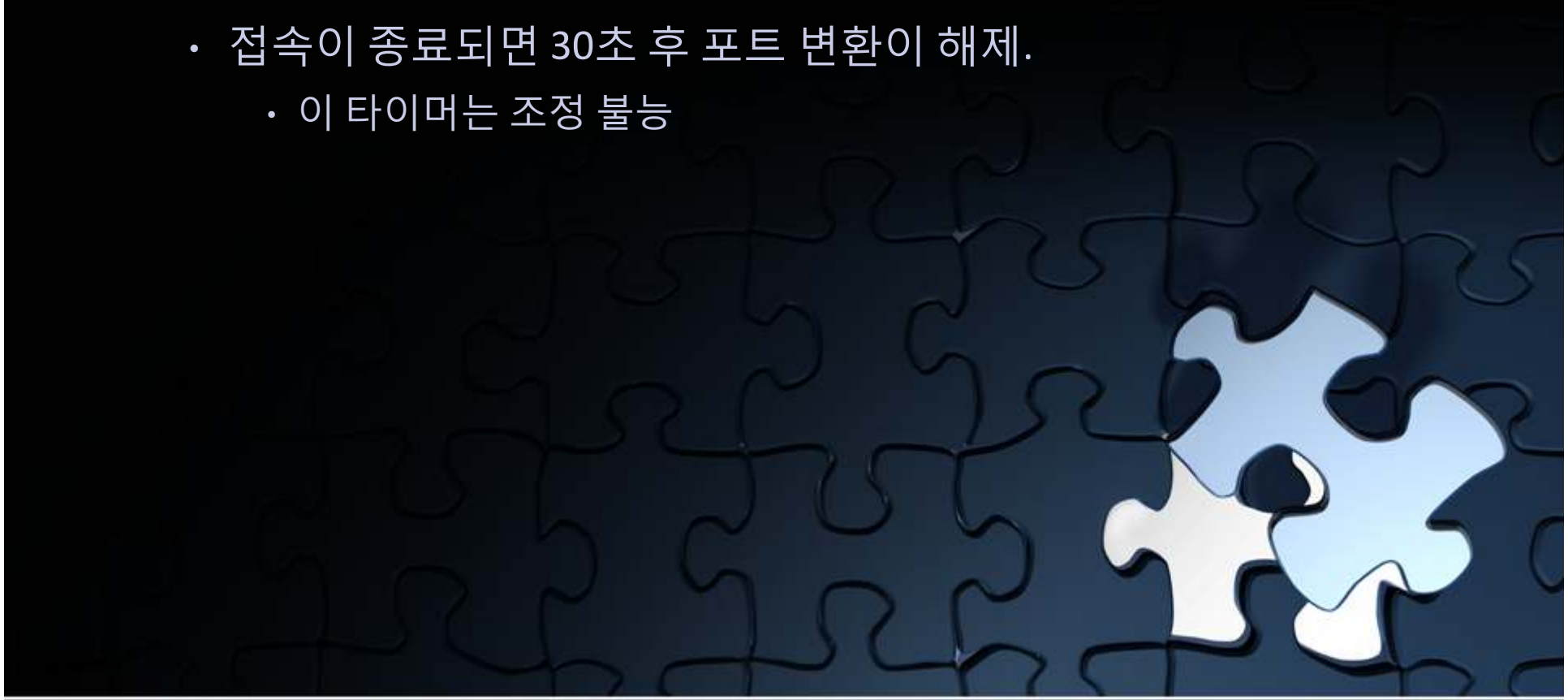
Unit 10. FW NAT/PAT

- 동적 NAT
  - 실제 IP(사설 IP)주소 그룹을 목적지까지 라우팅가능한 IP(공인 IP)주소 풀로 변환
  - 통신이 끝나면 기본적으로 3분후 변환이 해제
  - 동적 NAT 변환 타이머 조정
    - FW(cfg)# **timeout xlate** …
  - 동적 NAT 사용시 현재변환이 이루어져도 외부에서 내부의 변환된 주소로 직접 연결되는 것은 차단
    - 동적 NAT에서 PIX는 내부에서 시작된 패킷이 돌아오는 것만 허용

동적 PAT

Unit 10. FW NAT/PAT

- 동적 PAT
  - 복수 개의 사설 IP주소를 하나의 공인 IP주소로 변환(1024 포트 이후 번호)
  - 접속이 종료되면 30초 후 포트 변환이 해제.
    - 이 타이머는 조정 불능



정적 NAT/PAT

Unit 10. FW NAT/PAT

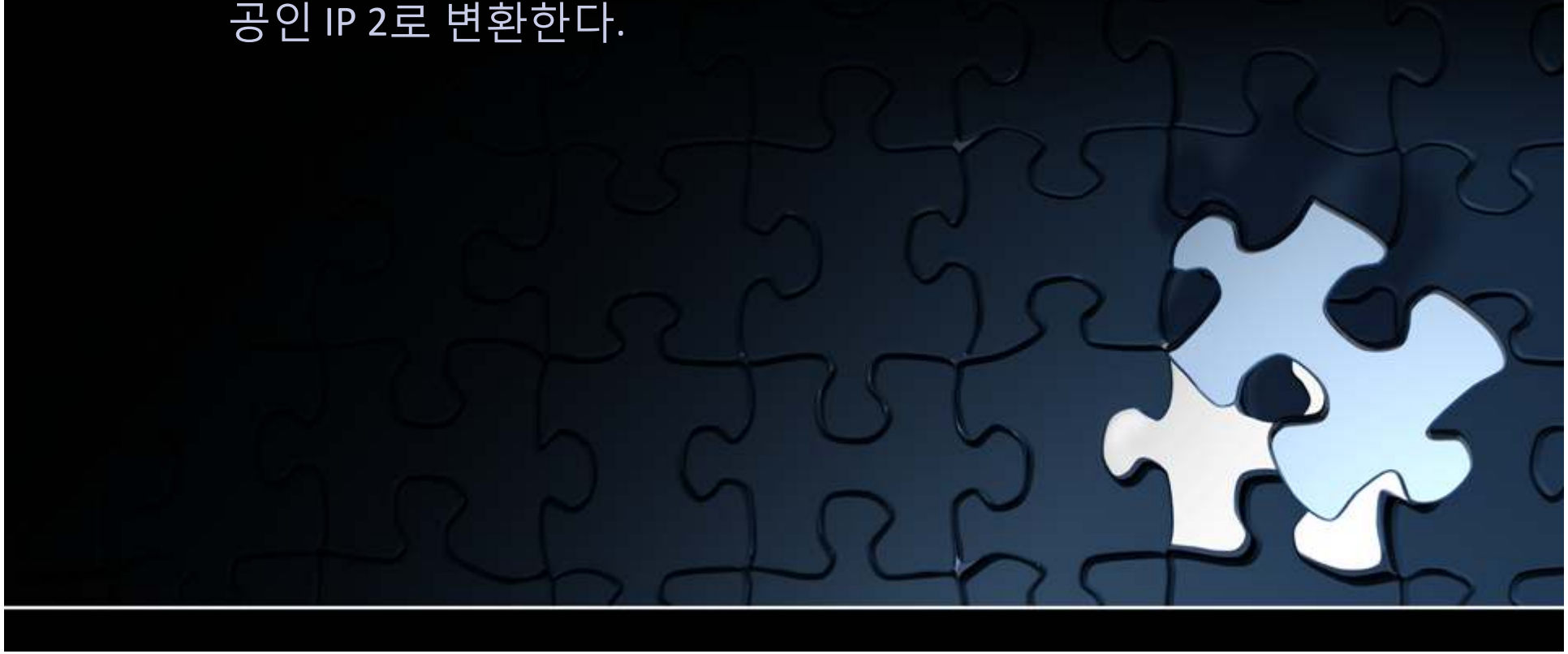
- 정적 NAT
  - 사설 주소와 공인 주소를 1:1로 변환
  - 외부망에서 변환된 내부망의 IP주소로 직접 연결

- 정적 PAT
  - 사설 IP주소와 공인 IP주소의 TCP/UDP 포트 번호를 직접 지정해주는 것 외에는 정적 NAT와 동일
  - 서로 다른 사설 IP주소를 가진 웹 서버, FTP 서버, 메일 서버 등을 하나의 공인 IP주소를 이용하여 접속할 수 있게 할 수 있다.
  - **표준 포트 번호와 비표준 포트 번호를 매핑할 수 있다.**
    - 예) 공인 HTTP 포트 번호 80번의 웹서버 → 비공인포트번호의 8000번 매핑이 가능하다.

Policy NAT/PAT

Unit 10. FW NAT/PAT

- Policy NAT/PAT
  - **ACL을 이용**
  - 출발지(사설 IP)와 목적지에 따라 변환이 일어나게 한다.
  - 서버 1에 접속할 때는 공인 IP 1로 변환시키고, 서버 2에 접속할 때는 공인 IP 2로 변환한다.



Bypass NAT

Unit 10. FW NAT/PAT

- Bypass NAT
  - **NAT Control을 사용하면 높은 보안 레벨에서낮은 보안 레벨로 라우팅시 NAT에 해당되지 않는 패킷들은 폐기한다.**
  - NAT 제어 기능을 사용하면 내부에서 외부로 라우팅되는 패킷들은 반드시 NAT가 적용되어야 한다.
  - **특정 호스트들에 대해 NAT 기능을 사용하지 않으려면 Bypass NAT을 사용한다.**

동적 NAT/PAT 설정

Unit 10. FW NAT/PAT

- 동적 PAT 설정
  - FW(cfg)# **nat (inside) 1 사설네트워크 서브넷마스크**
  - FW(cfg)# **global (outside) 1 interface**
- 동적 NAT 설정
  - FW(cfg)# **global (outside) 1 공인주소시작-끝**
  - 동적 NAT/PAT는 외부에서 변환된 내부로의 주소로는 통신이 되지 않는다.
- FW NAT Table
  - FW(cfg)# **show xlate**
- NAT에 의해 변환된 패킷수
  - FW# **show nat**

정적 NAT/PAT

Unit 10. FW NAT/PAT

- 정적 NAT 설정
  - FW(cfg)# **static (dmz,outside) 공인주소 실제주소**
  - 정적 NAT를 사용하면 외부에서 내부로의 접속이 가능하다.
- 정적 PAT 설정
  - FW(cfg)# static (dmz,outside) tcp 공인주소 www 실제주소 www
- 텔넷, WWW 세션 허용 ACL
  - FW(cfg)# access-list O-I permit tcp any host 공인주소 eq 23
  - FW(cfg)# access-list O-I permit tcp any host 공인주소 eq www
  - FW(cfg)# access-group O-I in interface outside
- 통신 확인
  - FW(cfg)# **show conn**

Policy NAT

Unit 10. FW NAT/PAT

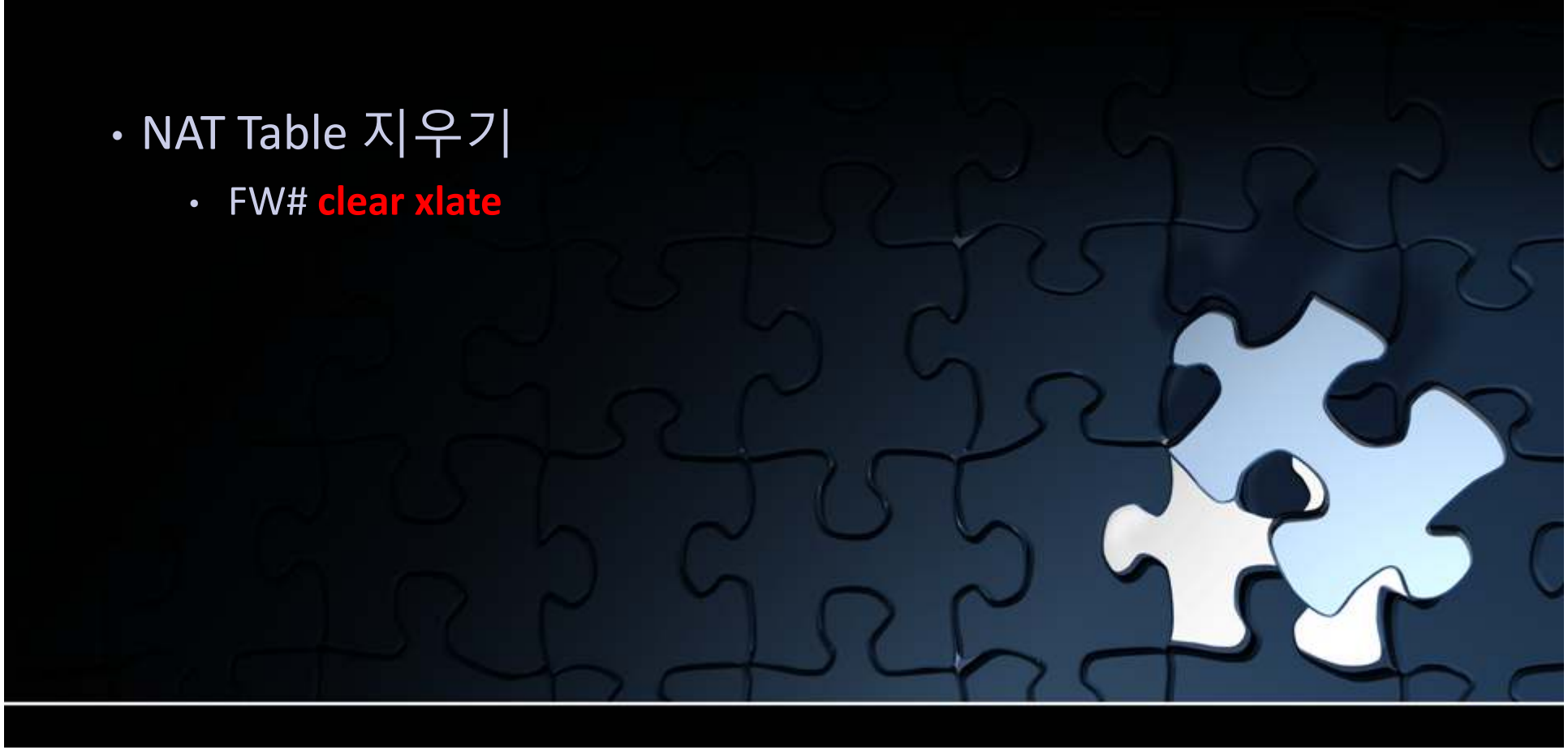
- Policy NAT
  - ACL을 사용하여 출발지와 목적지 IP주소에 따라 서로 다른 공인 IP주소를 사용할 수 있게 하는 것
- 돌아오는 트래픽 허용
  - FW(cfg)# access-list O-I permit tcp host 외부주소 eq 23 host 공인주소
- Policy NAT 설정
  - FW(cfg)# access-list 이름 permit ip 내부주소 S-M 외부주소 S-M
  - FW(cfg)# **nat (inside) 1 access-list 이름**
  - FW(cfg)# **global (outside) 1 공인주소**
  - Policy NAT은 목적지 포트번호로 따라 서로 다른 출발지 공인 IP주소를 사용할 수 있다.

Policy NAT

Unit 10. FW NAT/PAT

- NAT Table 상세 보기
  - FW# **show xlate detail**

- NAT Table 지우기
  - FW# **clear xlate**



NAT Control & NAT Bypass

Unit 10. FW NAT

- NAT Control
  - NAT에 의해 변환되지 않은 IP주소를 사용하는 패킷을 모두 차단
- NAT Control 설정
  - FW(cfg)# **nat-control**
  - NAT Control을 설정하면 변환되지 않은 주소를 사용하는 패킷을 모두 차단한다.
- NAT Bypass
  - 변환되지 않은 주소를 허용하는 것
  - 3가지 방법
    - **Identity NAT**
    - **정적 Identity NAT**
    - **NAT 면제(Exemption)**

Identity NAT & 정적 Identity NAT

Unit 10. FW NAT

- Identity NAT 설정
  - FW(cfg)# **nat (dmz) 0 공인주소 255.255.255.255**
  - Identity NAT을 사용하면 외부에서 내부로 접속할 수 없다.
  - 이를 해결하려면 정적 Identity NAT을 사용한다.

- 정적 Identity NAT 설정
  - FW(cfg)# **static (dmz,outside) 공인주소 공인주소 netmask 255.255.255.255**
  - 가상 IP주소와 실제 IP가 동일한 정적 NAT을 사용하는 것

NAT 면제

Unit 10. FW NAT/PAT

- NAT Exemption 설정
  - FW(cfg)# access-list EXEMPT permit ip host … any
  - FW(cfg)# **nat (dmz) 0 access-list EXEMPT**
  - NAT 면제는 ACL을 사용하여 NAT를 바이패스할 주소를 설정하고, 이를 NAT ID 0을 사용하여 지정하는 것

- NAT 없이 inside에서 dmz로 통신이 가능하게 하는 설정
  - FW(cfg)# **access-list NONAT permit ip 내부주소 S-M DMZ주소 S-M**
  - FW(cfg)# **nat (inside) 0 access-list NONAT**

NAT & DNS

Unit 10. FW NAT/PAT

- 정적 NAT을 설정하면서 DNS 옵션 사용
  - FW(cfg)# **static (inside,outside)** DNS-서버 웹-서버 netmask 255.255.255.255 **dns**
  - 웹 서버는 내부에 있고, DNS 서버는 외부에 있는 경우

MPF 개요

Unit 11. MPF

- **MPF(Modular Policy Framework)**
  - **모듈화된 보안 정책 설정**
  - **응용 계층 트래픽 제어와 같은 복잡한 작업**

- MPF 의 기능
  - 응용 계층 제어
  - QoS Policing, Shaping, Queuing
  - TCP 정규화, TCP/UDP 접속수 제한, 타임아웃 제어, TCP 순서번호 무작위화
  - ASA AIP 모듈과 CSC 모듈 제어
  - 네트워크 계층 제어

기본적 MPF 구성

Unit 11. MPF

- 기본적 MPF 구성
  - **Inspect_default** 라는 클래스 맵을 사용하여 트래픽 분류
    - **Default-Inspection-Traffic**
      - DNS(UDP 53), FTP(TCP 21), H323-H225(TCP 1720), H323-RAS(UDP 1718-1719), NetBIOS(UDP 137-138), RSH(TCP 514), RSTP(TCP 554), SIP (TCP 5060), SKINNY (TCP 2000), SMTP(TCP 25), SQLNET(TCP 1521), TFTP(UDP 69), XDMCP(UDP 177)
  - **Global_policy**라는 폴리시 맵이 **inspect** 명령으로 트래픽 검사
  - **Service-policy global_policy global** 명령어를 이용하여 활성화
    - **Global** 옵션: 전체 인터페이스 적용
    - **Interface** 옵션: 특정 인터페이스에만 적용

기본적 MPF 동작

Unit 11. MPF

- 기본적 MPF 동작
  - 많은 프로토콜들이 별개의 두번째 TCP 또는 UDP 포트 번호를 사용
  - **결과적으로 MPF가 기본적으로 검사하는 프로토콜들은 자동적으로 동적인 포트번호 사용아니 내부 IP 주소의 변환 등이 이뤄진다.**
  - 예를 들어 MPF가 ICMP 패킷을 검사한다는 의미는 내부에서 출발한 ICMP 트래픽은 돌아올 때 ASA/PIX를 통과할 수 있다.

MPF 설정 및 동작확인

Unit 11. MPF

- 절차
  - Class-map
    - 트래픽 분류
  - Policy-map
    - 보안 정책 설정
  - Service-policy
    - 정책 활성화
  - Show service-policy
    - 정책의 동작 확인

트래픽 분류

Unit 11. MPF

- 클래스 맵 확인
  - FW# **show run all class-map/show run class-map**
  - 미리 설정된 클래스 맵
    - **Class-default**
    - **Inspection_default**
  - 일반 클래스 맵은 ¾ 계층의 트래픽을 분류하기 위해 사용
    - 단일 모드에서는 최대 255개의 클래스 맵을 사용할 수 있다.
    - Context 모드에서는 Context 당 255개를 사용할 수 있다.
- 클래스 맵 설정
  - FW(cfg)# class-map …
  - FW(c-cmap)# match …

정책 설정

Unit 11. MPF

- 폴리시 맵 확인
  - FW# **show run all policy-map/show run policy-map**
- 폴리시 맵 설정
  - FW(cfg)# policy-map …
  - FW(c-pmap)# class 클래스이름
  - FW(c-pmap-c)# **inspect** …
    - INSPECT: 검사할 트래픽을 지정할 때 사용
    - **SET CONNECTION**: TCP 관련 각종 정책을 지정
- Match default-inspection-traffic 명령어
  - **하나의 클래스에서는 하나의 클래스만 검사할 수 있다.**
  - **Match default-inspection-traffic** 사용한 클래스: 다수개의 검사 가능

정책 활성화

Unit 11. MPF

- 정책 활성화
  - **MPF를 global 인터페이스에 적용시키면 모든 인터페이스에서 패킷을 수신할 때에만 검사**
  - **MPF를 inside, outside 등 개별 인터페이스에 적용시키면 해당 인터페이스를 통해 수신 또는 송신하는 패킷을 모두 검사한다.**
  - 동일한 검사를 global과 개별 인터페이스에 동시에 적용했을 때는 개별 인터페이스에 설정된 것이 우선한다.
- MPF 카운트 초기화
  - FW# **clear service-policy**
- 정책 적용 결과 확인
  - FW# **show service-policy**

MPF 패킷 검사 순서

Unit 11. MPF

- **동일한 패킷에 대해 특성이 다른 검사를 수행하는 것은 모두 적용된다.**
- MPF 패킷 검사 순서
  1. QoS 입력 폴리싱
  2. TCP 정규화
  3. CSC
  4. 응용계층 검사
  5. H323
  6. HTTP
  7. ICMP
  8. ICMP error
  9. ILS
  10. MGCP …

MPF 이용한 TCP Sync Flooding 완화

Unit 11. MPF

- **TCP Sync Flooding 공격**
  - **공격자가 TCP Sync 패킷을 다수 전송하고 ACK를 해주지 않는 것**
  - 웹 서버로 가는 HTTP 트래픽을 검사하고, TCP Sync Flooding 공격을 완화시키기 위해 TCP ACK를 수신하지 못한 세션수를 제한하는 방법
- TCP Sync Flooding 공격 완화
  - FW(cfg)# class-map C-HTTP
  - FW(c-cmap)# match access-list WEB-SERVER
  - FW(cfg)# policy-map P-OUTSIDE
  - FW(c-pmap)# class C-HTTP
  - FW(c-pmap-c)# **inspect http**
  - FW(c-pmap-c)# **set connection embryonic-conn-max 500**
  - FW(cfg)# service-policy P-OUTSIDE interface outside

Inspection Policy Map 개요

Unit 12. Inspection Policy Map

- Inspection Policy Map
  - ASA/PIX에서 응용계층의 특정한 프로토콜을 정밀하게 검사할 때 사용한다.
  - 특정 프로토콜을 정밀하게 검사하는 Inspection Policy Map을 만든 다음, 다시 일반적인 Policy Map에서 호출해서 사용한다.
  - 설정 명령어
  - FW(cfg)# **policy-map type inspect** …

기본적 Inspection Policy Map

Unit 12. Inspection Policy Map

- 기본적 Inspection Policy Map
  - ASA/PIX에는 기본적인 Inspection Policy Map이 미리 만들어져 적용되고 있다.
  - 확인
  - FW# **show run all policy-map**

- Inspection Policy Map의 적용 위치
  - 기본 Policy Map인 global_policy에서 inspect dns preset_dns_map처럼 inspect 명령어 다음에 특정 프로토콜 이름과 함께 적용되어 있다.

Inspection Policy Map 설정 프로토콜

Unit 12. Inspection Policy Map

- Inspection Policy Map이 가능한 프로토콜
  - FW(cfg)# **policy-map type inspect** ?
- Inspection Policy Map에서 사용할 수 있는 명령어
  - **Class**
    - 미리 만든 Inspection Class Map을 호출하거나, Inspection Policy Map 내에서 직접 Inspection Class Map을 만들 수 있다.
  - **Match**: Inspection Policy Map에서도 사용 가능
  - **Parameter**
    - 각 프로토콜에서 좀더 세밀한 조건을 지정할 때 사용되며, 내용은 프로토콜별로 다른다.
- Inspection Class Map
  - FW(cfg)# **class-map type inspect** ?

Regex

Unit 12. Inspection Policy Map

- Regex: Regular Expression
  - Inspection Policy Map의 class, match, parameters 명령어에서 정규식을 만들어 특정한 문자열을 검사할 수 있다.
- Regex 기호

기호	의미	설명
.	마침표	한글자
(exp)	부표현	주위의 다른 문자로부터 분리되어 다른 문자 사용
[abc]	문자클래스	a, b, 또는 c를 의미
“”	따옴표	글자의 앞 또는 뒤에 스페이스를 넣을 때 사용
?	물음표	직전 문자의 수가 0 또는 1임을 의미
*	별표	직전 문자가 0개 이상을 의미
^	삿갓	줄의 시작
\	이스케이프문자	특수 문자를 일반 문자로 사용

Regex 이용 특정 사이트 접속 차단

Unit 12. Inspection Policy Map

- Regex 이용한 특정 사이트 접속 차단
- 1단계: Regex
  - FW(cfg)# **regex** NO-GG ".*\google\.com"
- 2단계: Inspection Class Map
  - FW(cfg)# **class-map type inspect http match-all** BL-ST
  - FW(c-cmap)# match request header host regex NO-GG
- 3단계: Inspection Policy Map
  - FW(cfg)# **policy-map type inspect http** P-HTTP
  - FW(c-pmap)# **parameters**
  - FW(c-pmap-p)# class BL-ST
  - FW(c-pmap-c)# **drop-connection** log

Regex 이용 특정 사이트 접속 차단

Unit 12. Inspection Policy Map

- 4단계: Class Map
  - FW(cfg)# class-map C-HTTP
  - FW(c-cmap)# **match port tcp eq www**
- 5단계: Policy Map
  - FW(cfg)# policy-map P-INSIDE
  - FW(c-pmap)# class C-HTTP
  - FW(c-pmap-c)# **inspect http** P-HTTP
- 6단계: Service Policy
  - FW(cfg)# service-policy P-INSIDE interface inside

Regex Class Map

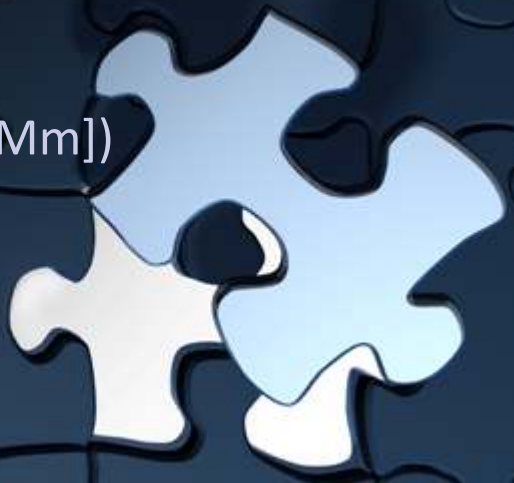
Unit 12. Inspection Policy Map

- 여러 개 Regex를 하나의 Inspection Policy Map에 사용할 경우
  - FW(cfg)# regex NO-GG ".*\.google\.com"
  - FW(cfg)# regex NO-CC ".*\.cisco\.com"
  - FW(cfg)# regex NO-HP ".*\.hp\.com"
  - FW(cfg)# **class-map type regex match-any** BL-ST
  - FW(c-cmap)# **match regex** NO-GG
  - FW(c-cmap)# match regex NO-CC
  - FW(c-cmap)# match regex NO-HP
  - FW(cfg)# class-map type inspect http match-all C-BL
  - FW(c-cmap)# match request header host **regex class** BL-ST

Regex 만들기 및 테스트

Unit 12. Inspection Policy Map

- Regex 만들기
  - 확장자가 .exe나 .com인 파일들을 지정하는 Regex 생성시
  - FW(cfg)# **regex urllist1** .*\.([Ee][Xx][Ex]|[Cc][Oo][Mm])
- Regex 표현 테스트
  - FW(cfg)# **test regex asa.exe** .*\.([Ee][Xx][Ex]|[Cc][Oo][Mm])
- 필요한 부분 수정
  - FW(cfg)# regex urllist1 .*\.([Ee][Xx][Ee]|[Cc][Oo][Mm])



HTTP 동작 개요

Unit 13. HTTP Traffic Control

- WWW 3대 요소
  - HTML(Hypertext Markup Language)
    - 웹 문서를 만들 때 사용하는 언어
  - HTTP(Hypertext Transfer Protocol)
    - 웹에서 사용되는 HTML 문서, 멀티미디어 파일 등의 데이터를 전송할 때 사용되는 통신 프로토콜
  - URI(Uniform Resource Identifier)
    - 웹 상에 존재하는 HTML 문서, 멀티미디어 파일 등의 위치를 지정할 때 사용하는 표현

HTTP Message Format

Unit 13. HTTP Traffic Control

- HTML Message 구성
  - Start-line, Header, Empty line, Body(필요시)

- 2가지 종류의 메시지
  - HTTP 요청 메시지
    - 요청 메시지의 시작줄 처음에 사용되는 명령어: Method
    - HTTP 1.1에는 총 8개의 Method가 정의되어 있다.
  - HTTP 응답 메시지
    - 응답 메시지의 시작줄에는 상태 코드와 이유 구문이 표시된다.

HTTP Method

Unit 13. HTTP Traffic Control

- HTTP 요청 메시지의 첫줄
  - Method, 요청 URI, HTTP 버전으로 구성
- Method
  - 클라이언트가 서버에게 특정한 작업을 요청할 때 사용하는 명령어
  - GET 명시된 정보를 찾아 클라이언트에게 전송
  - HEAD 서버가 전송할 HTTP 메시지 중 헤더만 보내라는 명령
  - POST 클라이언트가 서버에게 데이터를 전송할 때 사용
  - OPTIONS 요청 URI 관련 통신시 사용할 수 있는 옵션의 내용을 질의
  - PUT 첨부된 바디를 요청 URL 아래에 저장할 것을 요청
  - DELETE 요청 URI가 지정하는 자원을 삭제
  - TRACE 응용계층의 루프백 테스트를 수행
  - CONNECT 추후에 사용하기 위하여 예약해 둔 것

HTTP 상태 코드

Unit 13. HTTP Traffic Control

- HTTP 응답 메시지의 첫줄
  - 상태코드와 이유구문으로 시작

- HTTP 상태코드
  - 1XX 정보제공
  - 2XX 성공
  - 3XX 리다이렉션
  - 4XX 클라이언트 에러
  - 5XX 서버 에러

HTTP 상태코드의 예

Unit 13. HTTP Traffic Control

- 상태코드
  - 100: Continue
  - 200: OK
  - 300: Multiple Choice
  - 400: Bad Request
  - 403: Forbidden
  - 404: Not Found
  - 500: Internal Server Error
  - 503: Service Unavailable

HTTP 일반 헤더

Unit 13. HTTP Traffic Control

- HTTP Header Field 구분
  - General-Header
  - Request-Header
  - Response-Header
  - Entity-Header
- 일반 헤더(General Header)의 필드 종류
  - Cache-control/Connection
  - Date/Pragma
  - Trailer/Transfer-Encoding
  - Upgrade/Via
  - Warning

HTTP 요청 헤더

Unit 13. HTTP Traffic Control

- HTTP Request Header의 필드 종류
  - Accept/Accept-Charset
  - Accept-Encoding/Accept-Language
  - Authorization/Expert
  - From/Host
  - If-Match/If-Modified-Since
  - If-None-Match/If-Range
  - If-Unmodified-Since/Max-Forwards
  - Proxy-Authorization/Range
  - Referer/TE
  - User-Agent

HTTP 응답 헤더

Unit 13. HTTP Traffic Control

- HTTP Response Header의 필드 종류
  - Accept-Ranges
  - Age
  - Etag
  - Location
  - Proxy-Authenticate
  - Proxy-After
  - Server
  - Var
  - WWW-Authenticate

HTTP 실체 헤더

Unit 13. HTTP Traffic Control

- HTTP Entity Header의 필드 종류
  - Allow
  - Content-Encoding
  - Content-Language
  - Content-Length
  - Content-Location
  - Content-MD5
  - Content-Range
  - Content-Type
  - Expires
  - Last-Modifed

HTTP Inspection Class Map

Unit 13. HTTP Traffic Control

- Match 옵션
  - FW(cfg)# class-map type inspect http …
  - FW(c-cmap)# match …
    - not/req-resp/request/response

- Method 종류별 패킷 종류
  - FW(cfg)# class-map type inspect http …
  - FW(c-cmap)# match request method ?
    - connect/delete/edit/get …

HTTP Inspection Class Map

Unit 13. HTTP Traffic Control

- URI 이용한 분류
  - FW(cfg)# class-map type inspect http …
  - FW(c-cmap)# match request uri ?
    - length/regex

- Body 내용 분류
  - FW(cfg)# class-map type inspect http …
  - FW(c-cmap)# match response body?
    - active-x/java-applet/length/regex

HTTP Inspection Policy Map

Unit 13. HTTP Traffic Control

- HTTP Inspection Policy Map 주요 명령어
  - FW(cfg)# policy-map type inspect http …
  - FW(c-pmap)# ?
  - class
    - 앞서 설정한 클래스 맵을 호출할 때 사용
  - match
    - Inspection Policy Map 내부에서 트래픽 분류
  - parameters
    - 서브 명령어 사용

HTTP Inspection Policy Map

Unit 13. HTTP Traffic Control

- CLASS 명령어 내부에서 사용할 수 있는 명령어
  - FW(cfg)# poicy-map type inspect http …
  - FW(c-pmap)# class …
  - FW(c-pmap-c)# ?
  - drop-connection
    - 해당 패킷을 폐기하고, 접속을 종료
  - log
    - 로그 메시지 생성
  - reset
    - 해당 패킷을 폐기하고, 접속을 종료하며, TCP 리셋 메시지를 전송

DNS 개요

Unit 14. DNS Traffic Control

- DNS(Domain Name System)
  - 도메인 이름에 대한 IP주소를 알아내기 위해 사용하는 프로토콜
  - DNS 질의와 응답 메시지는 UDP 포트번호 53을 사용
  - 메시지 길이가 512 바이트를 초과하는 경우나, DNS 서버 간에 Zone 파일을 전송할 때는 TCP 포트 53을 사용
  - DNS Server = Name Server
- Domain Name
  - 알파벳, 숫자 및 하이픈을 사용하며, 대소문자를 구분하지 않는다.
- IDN(internationalized Domain Name)
  - 한글을 비롯한 전세계 대부분의 문자를 이용한 도메인 이름을 사용할 수 있으며, 이때 각 문자들은 DNS 시스템 내에서 알파벳, 숫자 등 ASCII 호환문자로 변환된다.

TLD

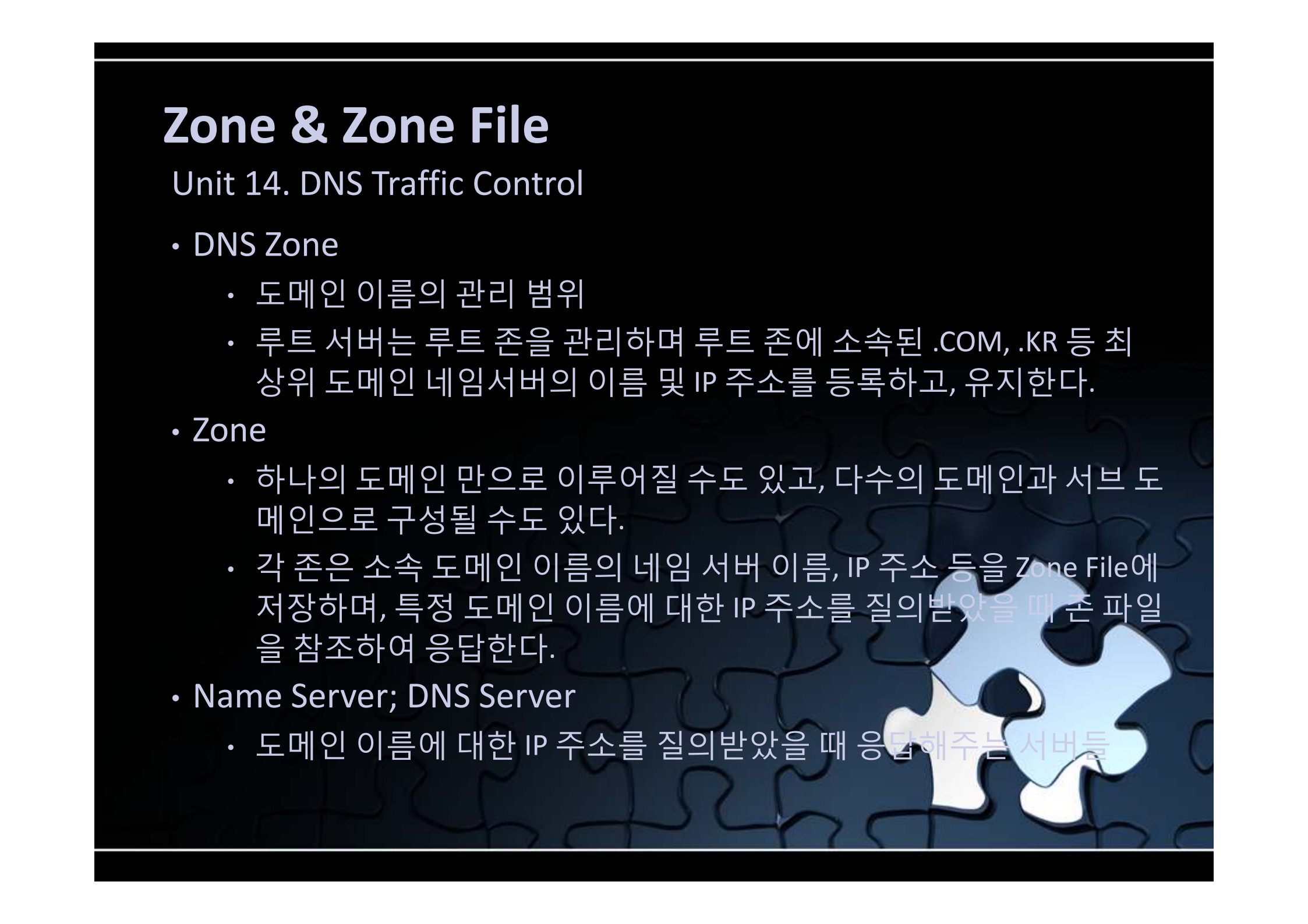
Unit 14. DNS Traffic Control

- TLD & SLD
  - Top Level Domain, Second-Level Domain
- gTLD(generic TLD) & ccTLD(country code TLD)
  - gTLD
    - .biz, .com, .info, .name, .net, .org, .pro는 누구나 비용을 지불하고 사용
    - .aero, .asia, .edu, .gov, .int, .mil, .museum 등은 해당 업종, 조직이나 지역에서만 사용
  - ccTLD
    - 두자리 수의 국가코드 사용, 약 250여개
    - 한국은 한국인터넷진흥원(KISA)이 담당
- ICANN(Internet Corporation for Assigned Names and Numbers)
  - 전세계 도메인 이름 관련 정책을 총괄

Zone & Zone File

Unit 14. DNS Traffic Control

- DNS Zone
  - 도메인 이름의 관리 범위
  - 루트 서버는 루트 존을 관리하며 루트 존에 소속된 .COM, .KR 등 최상위 도메인 네임서버의 이름 및 IP 주소를 등록하고, 유지한다.
- Zone
  - 하나의 도메인 만으로 이루어질 수도 있고, 다수의 도메인과 서브 도메인으로 구성될 수도 있다.
  - 각 존은 소속 도메인 이름의 네임 서버 이름, IP 주소 등을 Zone File에 저장하며, 특정 도메인 이름에 대한 IP 주소를 질의받았을 때 존 파일을 참조하여 응답한다.
- Name Server; DNS Server
  - 도메인 이름에 대한 IP 주소를 질의받았을 때 응답해주는 서버들



Name Server 종류

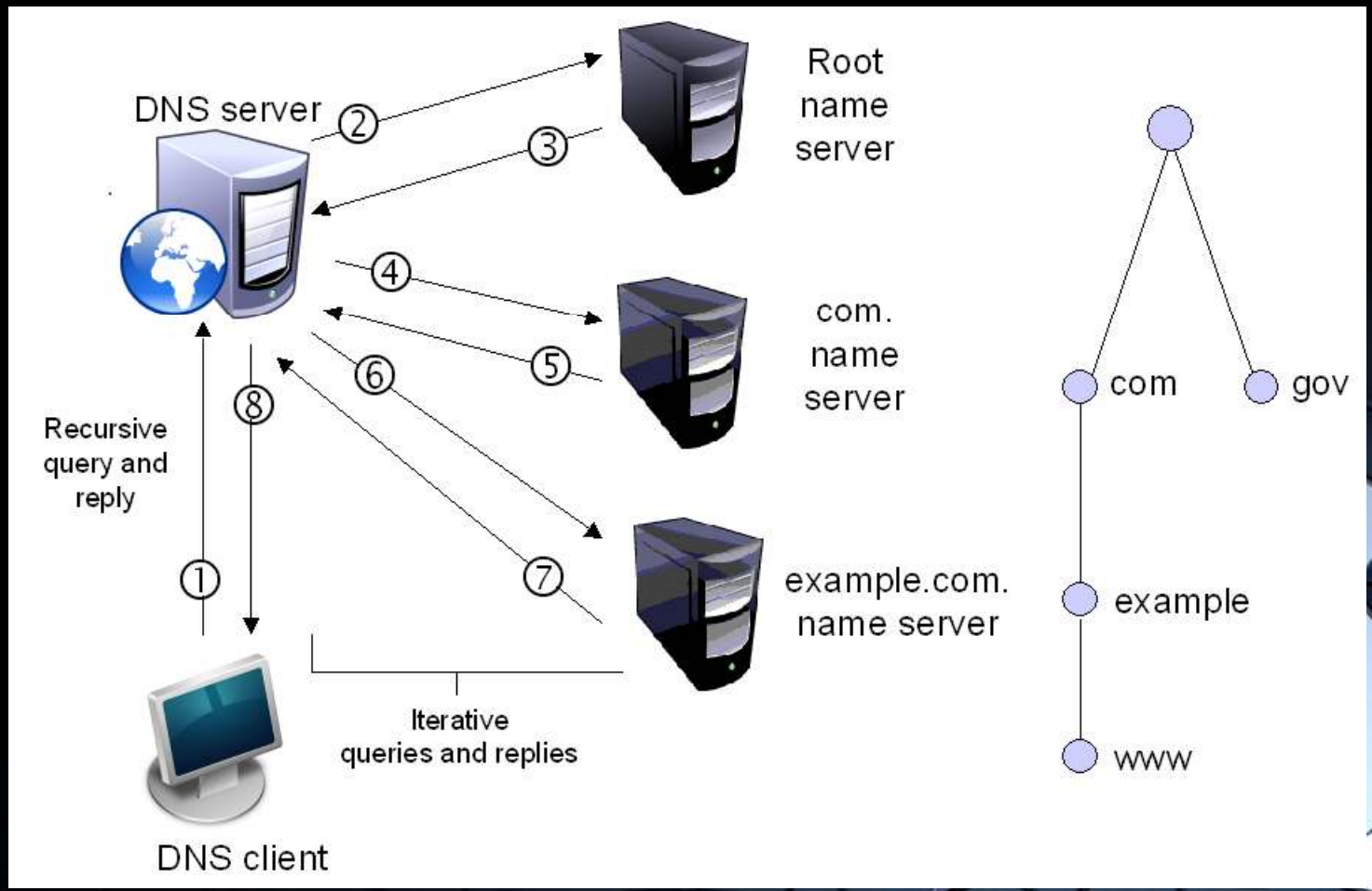
Unit 14. DNS Traffic Control

- 등록되어 있는 도메인의 계층에 따라
  - Root Server
  - TLD Name Server
  - Subdomain Name Server
- 특정 도메인의 Zone File 보유 여부에 따라
  - Authoritative Name Server
  - Caching Name Server
- 특정 도메인의 Zone File 편집 가능 여부에 따라
  - Primary Master Name Server
  - Slave Name Server

DNS 질의 및 응답 과정

Unit 14. DNS Traffic Control

- DNS 질의 및 응답 과정



PC의 DNS 정보 및 BIND

Unit 17. DNS Traffic Control

- PC의 캐시에 저장된 DNS 정보
  - C:>\ ipconfig /displaydns
- PC의 DNS 캐시 정보 삭제
  - C:>\ ipconfig /flushdns
- BIND
  - ISC에서 개발한 DNS 서버 프로그램
  - ISC 웹사이트(www.isc.org)에서 무료로 다운받아 사용할 수 있다.
  - Unix, Linux, 윈도우 등 다양한 운영체제에서 동작

DNS 동작 확인 도구

Unit 14. DNS Traffic Control

- NSLOOKUP
  - 윈도우에서 제공되는 명령어로 특정 도메인의 IP 주소 확인
  - Set type=all 명령어를 입력한 다음, 특정 도메인이름을 입력하면 그에 대한 상세 정보를 확인할 수 있다.

- DIG(Domain Information Groper)
  - BIND DNS 배포 페키지에 기본적으로 포함된 DNS 진단용 도구
  - 윈도우에는 BIND 설치해야 dig도 따라서 설치
    - -h 옵션
    - aaaa 옵션
    - ns 옵션
    - + trace 옵션

DNS Message

Unit 14. DNS Traffic Control

- DNS Message의 5가지 섹션
  - Header/Question/Answer/Authority/Additional

- DNS Message Header 섹션
  - RCODE: 응답시 사용
    - 0: 에러가 발생하지 않았다.
    - 1: 포맷 에러
    - 2: 서버 에러
    - 3: 네임 에러
    - 4: 미구현
    - 5: 거부

DNS Resource Record

Unit 14. DNS Traffic Control

- A Record
  - 레코드 타입값 1 – 특정 도메인의 IPv4 주소
- AAAA Record
  - 레코드 타입값 28 – 도메인의 IPv6 주소
- CNAME Record
  - 레코드 타입값 5 – 특정 도메인의 Canonical Name
- MX(Mail Exchange) Record
  - 레코드 타입값 15 – 메일 서버 호스트 도메인 이름
- NS(name Server) Record
  - 레코드 타입값 2 – 질의한 도메인의 네임 서버 도메인 이름
- SOA(Start of Authority) Record/PTR(Pointer) Record ...

DNS Inspection Class Map

Unit 14. DNS Traffic Control

- Match 조건
  - FW(cfg)# class-map type inspect dns …
  - FW(c-cmap)# match …
- DNS Class Type에 따른 분류
  - FW(c-cmap)# match dns-class eq ?
- DNS Type에 따른 분류
  - FW(c-cmap)# match dns-type eq ?

DNS Inspection Class Map

Unit 14. DNS Traffic Control

- Domain Name에 따른 패킷 분류
  - FW(c-cmap)# match domain-name regex ?
- DNS Header Flag 값에 따른 분류
  - FW(c-cmap)# match header-flag ?
- 특정 질의나 RR 타입을 이용한 패킷 분류
  - FW(c-cmap)# match question ?
- DNS Resource Record가 소속된 섹션을 기준으로 패킷 분류
  - FW(c-cmap)# match resource-record

DNS Inspection Policy Map

Unit 14. DNS Traffic Control

- 주요 명령어
  - FW(cfg)# policy-map type inspection http …
  - FW(c-pmap)# [class | match | parameters]
- CLASS 내부 명령어
  - FW(c-pmap)# class …
  - FW(c-pmap-c)# ?
    - DROP: 해당 패킷 폐기
    - DROP-CONNETION: 해당 패킷 폐기 및 접속 종료
    - ENFORCE-TSIG: TSIP 리소스 레코드가 없을 때의 동작 지정
      - TSIG(Transaction Signature): DNS 업데이트 인증시 사용
    - LOG: 로그 메시지 생성

DNS Inspection Policy Map

Unit 14. DNS Traffic Control

- Match 명령어 옵션
  - FW(c-pmap)# match ?
    - Inspection Policy Map 내부에서 트래픽을 분류한 후, 필요동작 설정
- Match 명령어 동작
  - FW(c-pmap)# match header-flag aa
  - FW(c-pmap-c)# ?
    - MASK: 해당 헤더 플래그를 읽지 못하게 지운다.
    - …
- Parameters 서브 명령어
  - FW(c-pmap)# parameters
  - FW(c-pmap-p)# ?

Security Context

Unit 15. Security Context

- Security Context
  - 하나의 ASA/PIX를 가상적으로 다수개의 ASA/PIX처럼 사용하는 것
- Security Context 용도
  - 하나의 방화벽을 다수의 서로 다른 고객 또는 조직들이 사용할 때
  - Active/Active 이중화와 같은 Security Context에서만 동작하는 기능을 이용하고자 할 때
- Security Context 특징
  - 각 컨텍스트는 독립적 장비처럼 동작
    - 독립적 보안 정책, 인터페이스, 라우팅 테이블, 관리자 등을 가진다.
    - 그러나 동적인 라우팅, 멀티캐스팅, VPN 등은 지원되지 않는다.
  - 복수개의 컨텍스트가 하나의 인터페이스를 공유할 때는 각 컨텍스트별로 개별적인 MAC 주소를 부여해야 한다. – 수동/자동으로 부여

Security Context 설정 및 동작 확인

Unit 15. Security Context

- Context Mode 확인
  - FW(cfg)# **show version**
  - FW(cfg)# **show mode**
- Context Mode 변경
  - FW(cfg)# **mode multiple**
- Admin Context 확인
  - FW(cfg)# **show run context**
- Admin Context 생성 및 저장 위치 설정
  - FW(cfg)# **admin-context admin**
  - FW(cfg)# **context admin**
  - FW(c-ctx)# **config-url flash:/admin.cfg**

Context 생성 및 이동

Unit 15. Security Context

- Context 만들기
  - FW(cfg)# **context …**
  - FW(c-ctx)# **allocate-interface** …
  - FW(c-ctx)# **config-url ...cfg**
- Context 확인
  - FW(cfg)# show context
  - 기본적 Context: admin, system context
    - **System Context**: 시스템을 재부팅하거나, 추가적 컨텍스트를 만드는 등 시스템 전체를 관장하는 컨텍스트
- Context간 이동
  - FW(cfg)# **changeto context** …

Context 설정 및 저장

Unit 15. Security Context

- System Context로 이동
  - FW(cfg)# **changeto context system**
  - FW(cfg)# **change sys**
- 인터페이스
  - 하나의 컨텍스트 내부에서 인터페이스를 활성화/비활성화시키면 해당 컨텍스트 내부에만 영향을 미친다.
- 설정한 내용의 저장
  - System Context: **write memory all**
  - 각 Context: wr
- 인터페이스 공유시
  - 인터페이스에서 mac-address 명령어 이용하여 직접 주소 부여
  - System Context에서 **mac-address auto** 명령어 사용

Context 라우팅 설정 및 NAT 설정

Unit 15. Security Context

- Context에서 라우팅 설정
  - 컨텍스트에서 동적 라우팅은 지원되지 않는다.
  - FW/c1(cfg)# route outside …
  - FW/c1(cfg)# route inside …
  - FW/c2(cfg)# route outside …
  - FW/c2(cfg)# route dmz …
- Context에서의 NAT 설정
  - FW/c1(cfg)# nat (inside) 1 …
  - FW/c1(cfg)# global (outside) 1 …

Context 보안 정책 설정

Unit 15. Security Context

- Ping 허용
  - FW/c1(cfg)# policy-map global_policy
  - FW/c1(c-pmap)# class inspection_default
  - FW/c1(c-pmap-c)# inspect icmp

- Telnet 허용 ACL 설정
  - FW/c2(cfg)# access-list O-I permit tcp any host … eq 23
  - FW/c2(cfg)# access-group O-I in interface outside

Admin Context

Unit 15. Security Context

- SSH 접속 설정
  - FW/c1(cfg)# username admin password cisco123
  - FW/c1(cfg)# aaa authentication ssh console LOCAL
  - FW/c1(cfg)# **crypto key generate rsa modulus 1024**
  - FW/c1(cfg)# **ssh … … inside**

- SSH 접속
  - R# **ssh –l admin** …
  - 접속수 다른 컨텍스트로 들어갈 수 없다.
  - 시스템 전체나 다른 컨텍스트를 제어하려면 admin 컨텍스트로 접속해야 한다.

Transparent Mode

Unit 16. Transparent Mode

- Transparent Mode
  - ASA/PIX를 Layer 2 장비로 동작시키는 것
  - 기존 장비의 IP 주소를 변경시킬 필요가 없어 편리
  - 외부에서 보았을 때 IP 주소의 홉수가 달라지지 않으므로 방화벽의 존재를 파악하기 힘들어 보안성이 증대
- Transparent Mode 동작 방식
  - 관리용 IP가 필요하며, 컨텍스트를 사용하는 경우 각 컨텍스트마다 모두 필요하다.
  - Transparent Mode는 Inside와 Outside 인터페이스 하나씩만 사용한다.
  - 컨텍스트를 사용하는 경우, 각 컨텍스트는 별개의 네트워크 주소를 사용한다. 동일한 서브넷을 사용할 수도 있으나, 라우터와 NAT 설정에서 이를 가능하도록 해야 한다.

Transparent Mode 동작 및 설정

Unit 16. Transparent Mode

- Transparent Mode 동작
  - 수신한 패킷의 목적지 주소가 방화벽의 Mac 주소 테이블에 있으면 해당 패킷을 전송
  - 목적지 주소가 Mac 주소 테이블에 존재하지 않으면 라우터와 같이 방화벽이 해당 목적지 Mac 주소에 대해 ARP를 수행
- Transparent Mode 설정
  - Mode 확인
    - FW# **show firewall**
  - Transparent Mode 설정
    - FW(cfg)# **firewall transparent**
  - 관리용 주소 설정
    - FW(cfg)# ip address …

Transparent Mode 보안정책 및 NAT

Unit 16. Transparent Mode

- OSPF 헬로 메시지 차단
  - 이유: 라우터 모드의 방화벽과 달리 Transparent Mode에서는 OSPF 헬로 패킷이 방화벽을 통과하여 상대 라우터까지 전송되어야 하기 때문. 즉 OSPF 헬로 패킷의 최종 목적지가 방화벽이 아니라 방화벽을 지나가기 때문에 차단

- Transparent Mode에서의 보안정책 설정
  - 라우터 모드와 크게 다르지 않다.

- Transparent Mode의 NAT 설정
  - 인접 라우터에서 내부 공인 IP 주소로 가는 라우팅의 설정이 필요

Ethertype ACL

Unit 16. Transparent Mode

- **Ethertype ACL**
  - 16비트의 이더타입을 제어할 때 사용
  - Transparent Mode에서만 지원
  - 이더넷 V2 프레임만 제어하며 802.3 프레임은 타입 필드 대신 길이 필드를 사용하므로 지원하지 않는다.
    - BPDU는 예외이며, 기본적으로 허용하고 제어할 수 있다.
  - 명시적으로 any 키워드를 사용하여 모든 트래픽을 차단하면 물리계층 동작을 위한 auto-negotiation 기능 등을 제외한 모든 트래픽이 차단된다.
  - 이더타입 ACL에서 묵시적 차단은 IP나 ARP 트래피게는 영향을 미치지 않는다. 그러나 명시적으로 모든 트래픽을 차단하면 IP나 ARP도 차단된다.

Ethertype ACL 설정

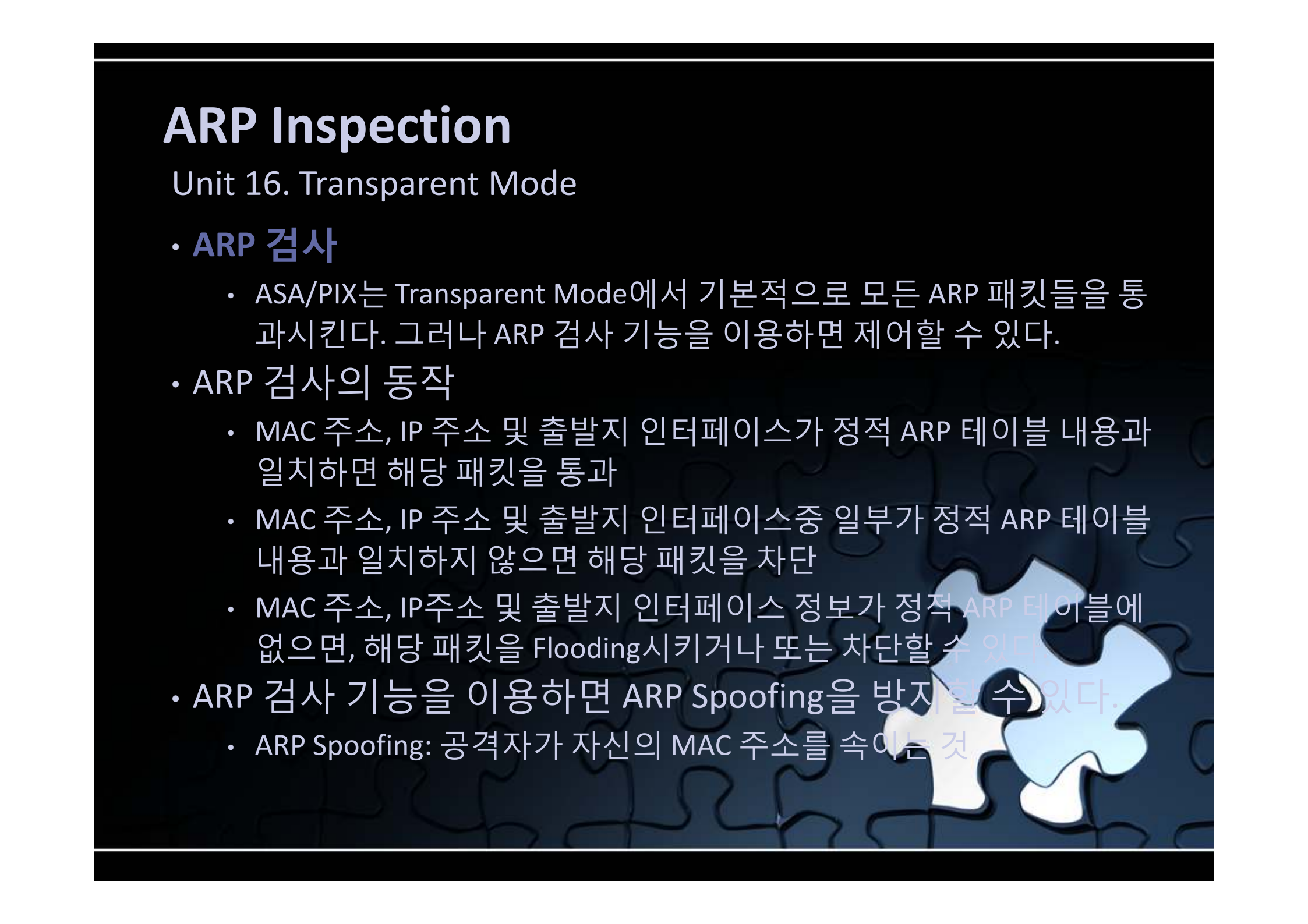
Unit 16. Transparent Mode

- IPX는 차단, 0x1234와 MPLS 유니캐스트 허용하는 ACL
  - FW(cfg)# **access-list** E-ACL **ethertype** deny ipx
  - FW(cfg)# access-list E-ACL ethertype permit 0x1234
  - FW(cfg)# access-list E-ACL ethertype permit mpls-unicast
  - FW(cfg)# access-group E-ACL in interface inside
  - FW(cfg)# access-group E-ACL in interface outside
- Ethertype 0x1234만 차단하는 ACL
  - FW(cfg)# access-list E-ACL ethertype deny 1234
  - FW(cfg)# access-list E-ACL ethertype permit any
  - FW(cfg)# access-list E-ACL in interface inside
  - FW(cfg)# access-list E-ACL in interface outside

ARP Inspection

Unit 16. Transparent Mode

- **ARP 검사**
  - ASA/PIX는 Transparent Mode에서 기본적으로 모든 ARP 패킷들을 통과시킨다. 그러나 ARP 검사 기능을 이용하면 제어할 수 있다.
- ARP 검사의 동작
  - MAC 주소, IP 주소 및 출발지 인터페이스가 정적 ARP 테이블 내용과 일치하면 해당 패킷을 통과
  - MAC 주소, IP 주소 및 출발지 인터페이스중 일부가 정적 ARP 테이블 내용과 일치하지 않으면 해당 패킷을 차단
  - MAC 주소, IP주소 및 출발지 인터페이스 정보가 정적 ARP 테이블에 없으면, 해당 패킷을 Flooding시키거나 또는 차단할 수 있다.
- ARP 검사 기능을 이용하면 ARP Spoofing을 방지할 수 있다.
  - ARP Spoofing: 공격자가 자신의 MAC 주소를 속이는 것



ARP Inspection 기능 활성화

Unit 16. Transparent Mode

- MAC 주소 확인
  - FW# **show arp**
- 정적 ARP 테이블 만들기
  - FW(cfg)# **arp inside IP_주소 MAC_주소 alias**
    - Alias 옵션: 타임아웃이 되지 않는다.
- ARP 검사 기능 활성화
  - FW(cfg)# **arp-inspection inside enable no-flood**
  - FW(cfg)# **arp-inspection outside enable no-flood**
    - **No-flood** 옵션: 해당 인터페이스로 ARP 패킷을 플러딩시키지 않는다.
- ARP 검사 상태 확인
  - FW(cfg)# **show arp-inspection**

방화벽 이중화

Unit 17. 방화벽 이중화

- 방화벽 이중화
  - 2개의 동일한 장비를 이중화 링크로 연결해야 한다.
  - 모니터링 대상 인터페이스들의 상태를 체크하다가 장애가 발생하면 Failover(역할 교대)가 동작한다.
- 이중화 동작 두 장비
  - 반드시 하드웨어 사양이 동일해야 한다.
  - 모델, 인터페이스 수량 및 종류, DRAM 크기 등이 같아야 한다.
  - Flash Memory의 사이즈는 달라도 된다.
  - 동작 모드도 동일해야 한다.
    - Router/Transparent Mode, Single/Multiple Mode 등이 같아야 한다.
  - 소프트웨어 버전도 같아야 한다.

Active/Active, Active/Standby 이중화

Unit 17. 방화벽 이중화

- 이중화 종류
  - **Active/Active 이중화**
    - 2장비가 모두 트래픽 처리
    - 부하분산이 가능
    - Security Context에서만 지원
    - IPSec VPN이나 SSL VPN이 지원되지 않으며, 동적인 라우팅도 지원 안함
  - **Active/Standby 이중화**
    - 한 장비만 트래픽 처리
    - Security Context를 사용하지 않거나 또는 다수의 Context Mode에서 모두 지원

Stateful/Stateless 이중화

Unit 17. 방화벽 이중화

- **Stateful 이중화**
  - 주장비가 현재의 세션 정보를 계속 Standby 장비에게 알려주어, 장애 발생시에도 현재의 접속을 유지하는 것
  - A/A, A/S 이중화 모두 지원
- 전송 정보
  - NAT 변환 테이블
  - TCP 접속 상태
  - ARP 테이블
  - MAC 주소 테이블
  - HTTP 접속 상태(HTTP 복사 기능 활성시)
  - ISKMP와 IPSec SA 테이블
  - GTP PDP 접속 데이터베이스

이중화 링크

Unit 17. 방화벽 이중화

- **이중화 링크(Failover Link)**
  - 이중화 설정 장비들은 이중화 링크를 통해 방화벽 상태 정보를 교환
- 동작 상태 확인 내용
  - 장비의 상태(Active 또는 Standby)/전원 상태
  - Hello Message/네트워크 연결 상태
  - MAC 주소 교환/설정값 복사 및 동기화
- **이중화 케이블**
  - PIX는 전용 이중화 케이블이나 Ethernet을 사용
  - ASA는 일반 Ethernet Port 중 하나를 사용.
  - 이중화 링크는 일반 트래픽을 전송할 수 없고, 오직 이중화 정보 전송만을 위해 사용

Stateful 이중화 링크

Unit 17. 방화벽 이중화

- Security Context 사용 경우
  - **이중화 링크는 시스템 컨텍스트 내에 존재해야 한다.**
  - 시스템 컨텍스트 내에 사용할 수 있는 인터페이스는 이중화 링크와 Stateful 이중화 링크 뿐.
  - Failover가 일어날 때 IP 주소와 MAC 주소는 변경되지 않는다.
- Stateful 이중화 링크
  - **Stateful 이중화 기능을 사용하려면 Stateful 이중화 링크를 사용해야**
  - 설정 옵션 3가지
    - 하나의 이더넷 인터페이스를 Stateful 이중화 링크 전용으로 사용
    - 이중화 링크를 Stateful 이중화 링크 겸용으로 사용
    - 일반 데이터 인터페이스를 Stateful 이중화 링크 겸용으로 사용
  - 전용 이더넷 인터페이스 사용하는 경우, 스위치나 크로스 케이블 사용

이중화 동작 상태 감시

Unit 17. 방화벽 이중화

- Hello Message
  - 이중화 링크를 통해 연속 3회 헬로 메시지를 수신하지 못하면 이중화 인터페이스를 포함한 모든 인터페이스로 ARP 요청 패킷을 전송
- 다른 인터페이스로 ARP 응답 수신
  - 이중화 인터페이스로는 응답을 받지 못하고, 다른 인터페이스로는 주장비로부터 수신하면 Failover는 일어나지 않는다. 다만 이중화 링크에 장애가 발생한 것으로 간주
- Failover
  - 어느 인터페이스를 통해서도 ARP 응답을 수신못하면 이중화 동작

이중화 기능

Unit 17. 방화벽 이중화

- 이중화 기능
  - 총 250개의 인터페이스 동작 상태를 감시

- 홀드 시간의 ½ 이내에 헬로 메시지를 수신하지 못하면
  - Link Up/Down 테스트
  - 네트워크 동작 테스트
  - ARP 테스트
  - 브로드캐스트 Ping 테스트

Active/Standby 이중화

Unit 17. 방화벽 이중화

- Active/Standby 이중화
  - 평상시에는 주장비가 트래픽 처리
  - 주장비나 주장비와 접속된 인터페이스에 장애가 발생하면 Standby 장비가 주장비 역할을 이어받아 트래픽을 처리

- Active/Standby 이중화 동작 방식
  - 주장비 역할을 이어받은 장비는 장애가 발생한 주장비의 IP 주소, MAC 주소를 이어받아 트래픽을 전송
  - Active 장비가 살아나도 현재의 장비가 Active 장비 역할을 계속 수행
  - Standby 장비는 주장비에서 복사된 설정을 저장하지 않는다.
    - 단일 컨텍스트 모드: write memory 명령어
    - 복수 컨텍스트 모드: write memory all 명령어

Active/Standby 이중화 동작 방식

Unit 17. 방화벽 이중화

- Write Standby 명령어 사용
  - 스탠바이 장비의 동작중인 설정이 모두 지워지고, 액티브 장비의 것으로 대체

- Failover 동작
  - 장비의 하드웨어 또는 전원 장애 발생
  - 소프트웨어 장애
  - 감시 인터페이스에 과도한 장애 발생시
  - Active 장비에서 no failover active 명령어를 사용하거나 Standby 장비에서 failover active 명령어를 사용했을 때

Active/Standby 이중화 설정

Unit 17. 방화벽 이중화

- 인터페이스 설정
  - FW(cfg)# int e0
  - FW(c-inf)# nameif outside
  - FW(c-inf)# **ip address** … **standby** …
  - FW(cfg)# int e1
  - FW(c-inf)# nameif inside
  - FW(c-inf)# ip address … standby …
  - 인터페이스에 IP 주소를 부여하면서 Standby 장비에서 사용할 주소까지 동시에 설정해야 한다.

Active/Standby 이중화 설정

Unit 17. 방화벽 이중화

- Active/Standby Failover 설정
  - FW1(cfg)# **failover lan unit primary**
  - FW1(cfg)# **failover lan interface FO e2**
  - FW1(cfg)# **failover lan enable**
    - Failover 링크가 인터페이스임을 알림 (PIX에만 해당)
  - FW1(cfg)# **failover link FO** (Stateful Failover 정보 전송용 인터페이스)
    - If Not, Stateless Failover, Active 장비에서만 설정
  - FW1(cfg)# **failover key cisco**
  - FW1(cfg)# **failover interface ip FO … standby …**
  - FW1(cfg)# **failover**
  - FW2(cfg)# failover lan unit **secondary**

Active/Standby Failover 동작 확인

Unit 17. 방화벽 이중화

- Failover 관련 전체적 내용 확인
  - FW1(cfg)# **show failover**
- Standby 장비를 Active로 변경
  - FW1# **failover active**
- 모니터링 인터페이스 화인
  - FW1# **show monitor-interface**
- 다시 FW1이 Active되게 하기
  - FW1# **no failover active**

Active/Standby 이중화 동작 확인

Unit 17. 방화벽 이중화

- Routing Protocol 사용시
  - Active/Standby 환경에서 동적인 라우팅 프로토콜을 사용할 때는 최소한의 시간 안에 라우팅 테이블이 만들어질 수 있도록 해야 한다.
  - 예를 들어, OSPF를 사용하는 경우에는 네트워크 타입을 환경에 따라 P2P나 P2MP로 설정한다. 스위치에서도 Routed Port를 사용하거나 RSTP 등을 사용하여 Convergence Time을 최소화한다.
- 텔넷 세션 정보 확인
  - FW# **show conn**
  - 마지막에 표시된 Flag
    - **U**: 접속이 살아 있다. Connection is Up
    - **I**: 데이터 수신하고 있다. Data In
    - **O**: 데이터 송신하고 있다. Data Out

추가적 Active/Standby 이중화 설정

Unit 17. 방화벽 이중화

- Stateful 이중화에서 HTTP 정보 복제
  - FW1(cfg)# **failover replication http**
  - HTTP는 세션이 짧기 때문에 Stateful Failover에서 기본적으로 세션 정보가 Standby 장비로 복제되지 않는다.

- 인터페이스 모니터링 활성 또는 비활성화
  - FW1(cfg)# **monitor-interface** …
  - **기본적으로 감시 대상 물리적인 인터페이스는 활성화되고, 서브 인터페이스는 비활성화된다.**
  - 특정 인터페이스를 추가로 감시하려는 경우에 설정

Active/Active 이중화

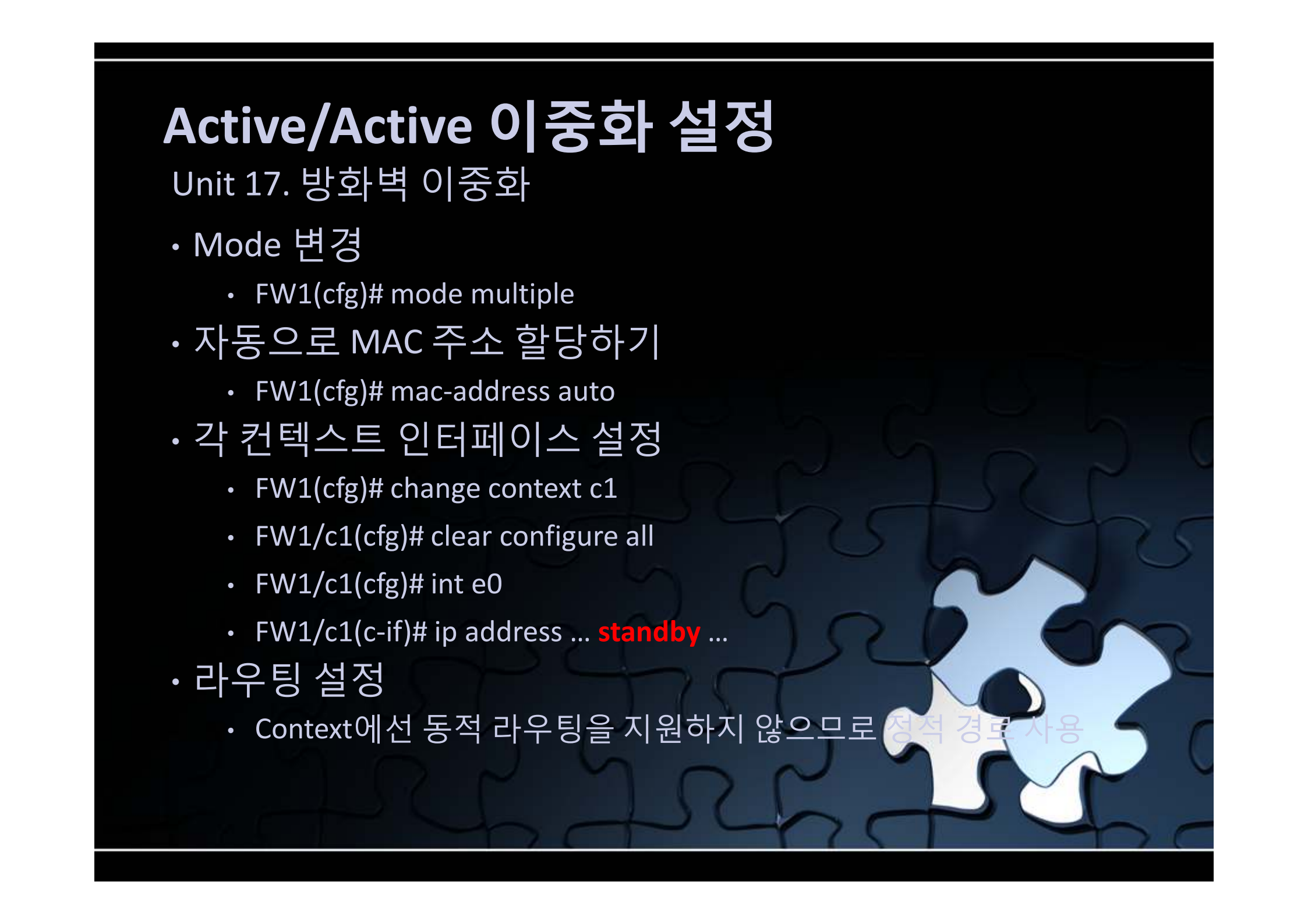
Unit 17. 방화벽 이중화

- Active/Active 이중화
  - 2대의 방화벽이 모두 트래픽을 처리
  - 2개 이상의 Security Context를 설정하고, 한 그룹의 Context는 FW1에서 Active로, 나머지 한 그룹의 Context는 FW2에서 Active로 동작
  - 한 장비에서 장애가 발생하면 두 그룹의 Context 모두 정상적인 장비에서 Active로 동작
- Active/Active 이중화 동작 방식
  - **Active/Active 이중화 는 Context 모드에서만 동작**
  - Active/Active 이중화를 위해 Context들을 Failover 그룹으로 나눈다.
  - Failover 그룹은 하나 이상의 단순한 논리적 그룹
  - Admin 컨텍스트는 항상 Failover 그룹 1의 멤버이다.
    - 특별히 할당하지 않은 컨텍스트들도 기본적으로 그룹 1의 멤버

Active/Active 이중화 설정

Unit 17. 방화벽 이중화

- Mode 변경
  - FW1(cfg)# mode multiple
- 자동으로 MAC 주소 할당하기
  - FW1(cfg)# mac-address auto
- 각 컨텍스트 인터페이스 설정
  - FW1(cfg)# change context c1
  - FW1/c1(cfg)# clear configure all
  - FW1/c1(cfg)# int e0
  - FW1/c1(c-if)# ip address … **standby** …
- 라우팅 설정
  - Context에선 동적 라우팅을 지원하지 않으므로 정적 경로 사용



Active/Active Failover 설정

Unit 17. 방화벽 이중화

- Failover 설정
  - FW1(cfg)# failover lan unit primary
  - FW1(cfg)# failover lan interface FO e2
  - FW1(cfg)# failover lan enable
  - FW1(cfg)# failover link FO
  - FW1(cfg)# failover key cisco
  - FW1(cfg)# failover interface ip FO … standby …
  - Active/Standby Failover 설정과 동일하다. 즉 Active/Active Failover를 설정하기 위해서는 먼저 Active/Standby Failover 설정을 한다.

Failover 그룹 설정

Unit 17. 방화벽 이중화

- Failover 그룹 설정
  - FW1(cfg)# **failover group 1**
  - FW1(c-fover-group)# **primary**
  - FW1(c-fover-group)# **preempt**
  - FW1(cfg)# failover group 2
  - FW1(c-fover-group)# **secondary**
  - FW1(c-fover-group)# preempt

Active/Active Failover 설정

Unit 17. 방화벽 이중화

- 각 Context를 서로 다른 Failover Group에 할당하기
  - FW1(cfg)# context c1
  - FW1(c-ctx)# **join-failover-group 1**
  - FW1(cfg)# context c2
  - FW1(c-ctx)# **join-failover-group 2**

- 서브 인터페이스 모니터링
  - FW1(cfg)# change context c1
  - FW1/c1(cfg)# monitor-interface inside

Active/Active 이중화 설정

Unit 17. 방화벽 이중화

- Failover 동작
  - FW1/c2# **change system**
  - FW1/c2(cfg)# **failover**
- 저장
  - FW1(cfg)# write memory all
- FW2 설정
  - FW2(cfg)# failover lan interface FO e2
  - FW2(cfg)# failover lan enable
  - FW2(cfg)# failover key cisco
  - FW2(cfg)# failover interface FO … standby …
  - FW2(cfg)# failover

Active/Active Failover 동작 확인

Unit 17. 방화벽 이중화

- Active/Active Failover 동작 확인
  - FW1(cfg)# show failover
- Failover 역할 교대

  FW1# failover active
- Failover Group 상태 확인
  - FW1# **show failover state**
- 연결 확인
  - FW1# show conn
- 특정 그룹에 대한 Failover 역할 교대
  - FW1# **no faiover active group 1**