

수업 내용 정리 보고서

작성일: 2026년 6월 30일

챕터 구성

- IDS/IPS 동작 원리 및 패킷 처리 구조
- 네트워크 트래픽 미러링(SPAN/RSPAN/ERSPAN) 기술
- GNS3 및 QEMU 기반 가상화 환경 구축
- 실무 적용 및 설정 검증 체크리스트

IDS/IPS 동작 원리 및 패킷 처리 구조

네트워크 보안의 핵심 요소인 **침입 탐지 시스템(IDS, Intrusion Detection System)**과 **침입 방지 시스템(IPS, Intrusion Prevention System)**은 네트워크 트래픽을 실시간으로 모니터링하여 공격 시그니처(Signature, 공격 요청에 포함되는 공통적인 패턴)를 탐지하고 대응하는 역할을 수행합니다. 본 장에서는 이들 시스템의 동작 차이점과 패킷이 하드웨어에서 탐지 엔진까지 도달하는 처리 과정을 상세히 살펴봅니다.

1. IDS와 IPS의 개념 및 비교

IDS와 IPS는 모두 네트워크 트래픽 내의 악성 패턴을 찾아내는 것이 목적이지만, 탐지 이후의 '**대응 방식**'과 '**네트워크 구성**'에서 결정적인 차이를 보입니다.

- IDS (Intrusion Detection System):** 네트워크 트래픽을 모니터링하고 이상 징후가 발견되면 이를 기록하거나 관리자에게 알림을 보냅니다. 트래픽 흐름을 직접 차단하지 않으므로 서비스의 **가용성(Availability)**을 유지하는 데 유리합니다. 만약 IDS 장비에 문제가 생기더라도 실제 서비스 트래픽은 계속 흐를 수 있습니다.
- IPS (Intrusion Prevention System):** 탐지에 그치지 않고 위험한 패킷을 즉시 **드롭(Drop, 패킷 폐기)**하여 공격을 차단합니다. 따라서 네트워크 흐름을 실제로 막을 수 있는 능력을 갖추고 있습니다.

구분	IDS (침입 탐지 시스템)	IPS (침입 방지 시스템)
주요 기능	탐지 및 로그 기록 (Detection)	탐지 및 패킷 차단 (Prevention/Drop)
네트워크 위치	Out-of-band (포트 미러링/TAP 이용)	In-line (회선 중간에 설치)
서비스 영향	장비 장애 시에도 서비스 가용성 유지	장비 성능/장애가 네트워크 속도에 영향
구성 모드	관제/사후 대응 중심	실시간 방어 중심

[실무 포인트] IPS를 운영할 때는 장비의 처리 속도가 전체 네트워크 성능의 병목 지점(Bottleneck)이 될 수 있음을 유의해야 합니다. 따라서 고성능 하드웨어나 최적화된 엔진이 필수적입니다.

2. 패킷 처리 파이프라인 (Packet Processing Pipeline)

Snort와 같은 NIDS/NIPS 장비 내부에서 패킷이 수신되어 최종적으로 탐지 결과가 출력되기까지는 다음과 같은 단계별 과정을 거칩니다. 이 과정은 하드웨어의 실행속도부터 소프트웨어의 논리적 판단까지 이어지는 일련의 흐름입니다.

- NIC (Network Interface Card) 수신:** 케이블을 통해 들어온 전기적/광학적 신호를 NIC가 수신하여 하드웨어 버퍼에 임시 저장합니다.
- DAQ (Data Acquisition) 단계:** NIC 버퍼에 있는 데이터를 실제 분석 프로그램이 접근할 수 있는 메모리 영역(사용자 영역)으로 퍼 올리는 과정입니다. *libpcap*이나 *afpacket*과 같은 라이브러리가 이 역할을 수행합니다.
- Decoder (해독) 단계:** 수신된 로우 데이터(Raw Data)를 각 프로토콜(Ethernet, IP, TCP/UDP 등) 규격에 맞게 해독합니다.
- Preprocessor (전처리) 단계:** 쪼개져서 들어온 패킷들을 재조립(Reassembly)하거나, 세션 관련 처리를 수행하여 분석하기 좋은 형태로 만듭니다.
- Detection (탐지) 단계:** 해독 및 전처리가 완료된 데이터를 사전에 정의된 **시그니처(Signature)**와 대조하여 공격 여부를 판단하고 결과를 출력합니다.

3. 네트워크 트래픽 가로채기: 미러링과 모드

보안 장비가 트래픽을 분석하기 위해서는 대상 트래픽을 장비로 가져오는 과정이 필요합니다. 이때 사용하는 기술이 **포트 미러링(Port Mirroring)**입니다.

3.1 Promiscuous Mode (무차별 모드)

일반적인 랜카드는 자신의 IP나 MAC 주소를 목적지(Destination)로 하는 패킷만 받아들이고 나머지는 버립니다(Non-promiscuous mode). 하지만 IDS/IPS는 네트워크 전체의 트래픽을 관찰해야 하므로, 목적지와 상관없이 인터페이스로 들어오는 모든 패킷을 읽을 수 있는 **Promiscuous mode**로 동작해야 합니다.

3.2 미러링 기술의 종류 (Cisco 기준)

트래픽을 어디서 어디로 복사하느냐에 따라 세 가지 방식으로 구분됩니다.

- SPAN (Switched Port Analyzer):** 로컬 미러링입니다. 분석 대상 포트와 보안 장비가 **동일한 스위치**에 연결되어 있을 때 사용합니다.
- RSPAN (Remote SPAN):** L2 기반의 원격 미러링입니다. 여러 대의 스위치를 거쳐 트래픽을 전달해야 할 때, 특정 **VLAN**을 **미러링 전용 통로**로 지정하여 트래픽을 보냅니다.
- ERSPAN (Encapsulated Remote SPAN):** L3 기반의 원격 미러링입니다. 트래픽을 캡슐화(Encapsulation)하여 다른 네트워크 대역으로 전송할 수 있습니다.

4. 실습 구성 및 명령어 분석

학습 자료에 제시된 Cisco 스위치 설정을 통해 SPAN과 RSPAN의 동작 차이를 확인합니다.

[사례 1] SPAN 설정 (로컬 미러링)

SW1의 gi0/1 포트로 들어오고 나가는 모든 트래픽(both)을 gi0/0 포트로 복사하여 보내는 설정입니다.

```
[SW1]
conf t
monitor session 1 source interface gi0/1 both
monitor session 1 destination interface gi0/0
end
```

[사례 2] RSPAN 설정 (원격 미러링)

SW1에서 발생한 트래픽을 VLAN 100을 통해 SW2로 전달하고, SW2에서 이를 다시 특정 포트로 뽑아내는 과정입니다. 핵심은 두 스위치 사이에 RSPAN 전용 VLAN이 설정되어 있어야 한다는 점입니다.

1단계: SW1 설정 (트래픽을 원격 VLAN으로 송출)

```
[SW1]
conf t
vlan 100
 name RSPAN-VLAN
 remote-span <-- RSPAN 전용 VLAN임을 명시
exit

interface gi1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 100
 no shutdown
exit

monitor session 1 source interface gigabitEthernet 0/1 both
monitor session 1 destination remote vlan 100
end
```

2단계: SW2 설정 (원격 VLAN에서 트래픽을 수신하여 포트로 출력)

```
[SW2]
conf t
vlan 100
 name RSPAN-VLAN
 remote-span
exit

interface gi0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
end

interface gi0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
exit

interface gi1/0
 switchport mode access
 no shutdown
exit

monitor session 1 source remote vlan 100
monitor session 1 destination interface gi0/1
end
```

[주의사항] 미러링 전용 포트는 트래픽을 보내기만 하는 용도이므로, 해당 포트로 들어오는 인바운드(Inbound) 통신은 처리되지 않습니다. 즉, 미러링 포트를 통해 다른 장비와 통신하는 것은 불가능합니다.

5. 학습 정리 및 점검 사항

실무/시험 핵심 포인트

- **IDS vs IPS 선택 기준:** 네트워크 성능 저하를 최소화하며 관제 위주로 운영하려면 IDS를, 실시간 차단이 필수적인 보안 구역에는 IPS를 선택합니다.
- **IPS 배치 모드:** 네트워크 대역을 분리하여 방화벽처럼 동작하게 하려면 **라우터 모드**를, 대역 분리 없이 투명하게 차단만 수행하려면 **브릿지 모드**를 사용합니다.
- **Snort 최적화:** Snort의 처리 속도를 높이기 위해 **Lua JIT**(Just-In-Time 컴파일)와 같은 기술이 활용됨을 이해해야 합니다.

자가 점검 질문

1. IPS가 네트워크 전체 속도에 영향을 미칠 수 있는 이유는 무엇인가요? (패킷 처리 파이프라인 관점에서 설명)
2. RSPAN을 설정할 때, 소스 스위치와 목적지 스위치 사이의 트렁크(Trunk) 포트에 반드시 포함되어야 하는 설정은 무엇인가요?
3. IDS가 패킷을 차단하지 못하더라도 공격을 인지할 수 있는 이유는 무엇인가요?
4. 랜카드가 Promiscuous mode가 아닐 때, 자신이 목적지가 아닌 패킷을 받으면 어떻게 처리되나요?

네트워크 트래픽 미러링(SPAN/RSPAN/ERSPAN) 기술

네트워크 보안 관제 및 침입 탐지(IDS)를 수행하기 위해서는 네트워크를 통과하는 실제 패킷 데이터를 분석 장비로 전달해야 합니다. 하지만 분석 장비가 네트워크 경로 중간에 직접 삽입되어 흐름을 방해하는 것은 서비스 가용성 측면에서 위험할 수 있습니다. 이때 사용하는 핵심 기술이 **포트 미러링(Port Mirroring)**입니다.

1. 포트 미러링의 개념과 목적

포트 미러링은 스위치(Switch)의 특정 포트(또는 VLAN)에서 발생하는 트래픽을 복사하여, 다른 특정 포트에 똑같이 전송하는 기능입니다. 이를 통해 네트워크 트래픽을 가로채거나 중단시키지 않고도 보안 장비(IDS, Snort 등)가 패킷의 복사본을 받아 실시간으로 분석할 수 있도록 합니다.

- **장점:** 네트워크의 흐름을 방해하지 않으며(Non-intrusive), 서비스 가용성을 유지하면서 관제가 가능합니다.
- **한계:** 패킷의 '복사본'을 보는 것이므로, 미러링된 패킷을 기반으로 네트워크 흐름을 직접 차단(Drop)하는 기능은 수행할 수 없습니다. (차단은 IPS나 방화벽의 영역입니다.)

2. SPAN (Switched Port Analyzer): 로컬 미러링

SPAN은 동일한 스위치 내에서 동작하는 가장 기본적인 미러링 방식입니다. 분석 대상이 되는 컴퓨터(Source)와 보안 장비(Destination)가 모두 같은 물리적 스위치에 연결되어 있을 때 사용합니다.

[실습: Cisco SPAN 설정 예시]

다음은 SW1의 gi0/1 포트에서 발생하는 모든 트래픽(인바운드 및 아웃바운드)을 gi0/0 포트로 복사하여 보내는 설정 과정입니다.

```
[SW1]
conf t
# 미러링할 대상 포트와 방향(both: 인바운드+아웃바운드)을 지정
monitor session 1 source interface gi0/1 both

# 복사본을 보낼 목적지 포트를 지정
monitor session 1 destination interface gi0/0
end
```

- **source interface:** 관찰하고자 하는 트래픽이 발생하는 포트입니다. both 옵션을 사용하면 수신(rx)과 송신(tx) 트래픽을 모두 미러링할 수 있습니다.
- **destination interface:** 미러링된 트래픽이 도달할 포트입니다. 이 포트에 IDS나 패킷 분석 장비를 연결합니다.

3. RSPAN (Remote SPAN): L2 원격 미러링

RSPAN은 분석 대상 스위치와 보안 장비가 서로 다른 스위치에 위치할 때 사용합니다. 여러 대의 스위치를 거쳐 트래픽을 전달해야 하므로, 미러링된 트래픽만을 실어나르는 **전용 VLAN(Remote-SPAN VLAN)**을 활용합니다.

[실습: RSPAN 설정 절차 및 분석]

트래픽이 발생하는 SW1에서 보안 장비가 연결된 SW2까지 트래픽을 전달하는 과정입니다.

단계 1: 트래픽을 전송할 SW1 설정

먼저 RSPAN 전용 VLAN을 생성하고, 대상 트래픽을 해당 VLAN으로 밀어 넣어야 합니다.

```
[SW1]
conf t
# 1. RSPAN 전용 VLAN 생성 및 속성 부여
vlan 100
  name RSPAN-VLAN
  remote-span
exit

# 2. SW2와 연결된 Trunk 포트 설정 (VLAN 100이 통과할 수 있어야 함)
interface gil/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 100
  no shutdown
exit

# 3. 미러링 세션 설정: gi0/1 트래픽을 VLAN 100으로 전송
monitor session 1 source interface gigabitEthernet 0/1 both
monitor session 1 destination remote vlan 100
end
```

단계 2: 트래픽을 수신할 SW2 설정

SW2는 VLAN 100을 통해 들어온 트래픽을 받아 실제 물리 포트로 내보내주는 역할을 합니다.

```
[SW2]
conf t
# 1. SW2에도 동일한 RSPAN 전용 VLAN 설정
vlan 100
  name RSPAN-VLAN
  remote-span
exit

# 2. SW1과 연결된 Trunk 포트 설정
interface gi0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
end

# 3. VLAN 100이 통과할 수 있도록 허용
interface gigabitEthernet 0/0
  switchport mode trunk
  switchport trunk allowed vlan 100
  no shutdown
exit

# 4. 보안 장비가 연결된 포트를 Access 모드로 설정
interface gigabitEthernet 0/1
  switchport mode access
  no shutdown
exit

# 5. 미러링 세션 설정: VLAN 100의 트래픽을 gi0/1 포트로 출력
monitor session 1 source remote vlan 100
monitor session 1 destination interface gi0/1
end
```

4. ERSPAN (Encapsulated Remote SPAN): L3 원격 미러링

ERSPAN은 RSPAN의 한계를 넘어, 서로 다른 네트워크 대역(L3 경계)을 넘나들며 트래픽을 전송할 때 사용합니다. RSPAN이 VLAN(L2)을 이용해 트래픽을 운반 한다면, ERSPAN은 **캡슐화(Encapsulation)** 기술을 사용하여 미러링된 패킷을 IP 패킷 안에 담아 보냅니다. 이를 통해 라우터를 거쳐 먼 거리의 네트워크에 있는 분석 장비로도 트래픽을 보낼 수 있습니다.

5. 미러링 기술 비교 요약

구분	SPAN (Local)	RSPAN (Remote)	ERSPAN (Encapsulated)
동작 범위	동일 스위치 내	동일 L2 네트워크(여러 스위치)	서로 다른 L3 네트워크(라우터 통과)
전송 방식	내부 스위치 버스	전용 VLAN 사용	IP/GRE 캡슐화 사용
주요 특징	설정이 매우 간단함	Trunk 라인을 통해 VLAN 전송	네트워크 경계를 넘을 수 있음

⚠ 실무 및 시험 핵심 주의사항

- **미러링 전용 포트의 특성:** 미러링의 목적지(Destination)로 지정된 포트는 일반적인 통신 포트처럼 동작하지 않습니다. 즉, 이 포트로 들어오는 인바운드 트래픽은 네트워크 내부로 전달되지 않으며, 미러링 용도로만 사용됩니다.
- **RSPAN 구성 시 필수 체크리스트:**
 1. 모든 경유 스위치에 `remote-span` 설정이 된 동일한 VLAN이 생성되어 있는가?
 2. 스위치 간 연결된 Trunk 포트에 해당 VLAN이 허용(Allowed)되어 있는가?
- **성능 영향:** 미러링할 트래픽 양이 목적지 포트의 대역폭을 초과할 경우, 패킷 드랍이 발생하여 정확한 분석이 어려울 수 있습니다.

학습 확인 질문

1. 보안 장비가 다른 스위치에 있지만 동일한 VLAN 대역에 있을 때, 가장 효율적인 미러링 방식은 무엇인가요?
2. RSPAN 설정 시, 트래픽이 전달되는 경로 역할을 하는 스위치 간 연결 포트의 모드는 무엇이어야 하나요?
3. 미러링을 통해 패킷을 복사받는 것이 공격을 실시간으로 차단하는 것과 어떤 차이가 있나요?

GNS3 및 QEMU 기반 가상화 환경 구축

모의해킹 및 네트워크 보안 실습을 위해서는 실제 물리적인 라우터, 스위치, 그리고 IDS/IPS 장비를 구성하는 것이 가장 이상적이지만, 비용과 공간의 제약이 따릅니다. 따라서 **GNS3**와 **QEMU**를 활용하여 가상화된 네트워크 환경을 구축함으로써, 실제 장비와 유사한 동작을 수행하는 시뮬레이션 환경을 만드는 것이 필수적입니다.

1. 가상화 기술 및 이미지 포맷

효율적인 네트워크 시뮬레이션을 위해서는 하드웨어의 자원을 논리적으로 나누어 사용하는 가상화 기술에 대한 이해가 선행되어야 합니다.

- **GNS3 (Graphical Network Simulator-3):** 네트워크 토폴로지를 설계하고 시뮬레이션하는 도구입니다. 실습의 효율성을 높이기 위해 장비의 연산 부하가 큰 라우터나 스위치 이미지는 PC 내부가 아닌 **GNS3 외부 서버**(GNS3 VM 등)를 구축하여 해당 서버의 자원을 끌어다 쓰는 방식을 권장합니다.
- **QEMU (Quick Emulator):** 가상화 기술 중 하나로, 다양한 아키텍처의 프로세서를 에뮬레이션할 수 있습니다. 최근에는 시스코(Cisco) 장비 자체가 VM(Virtual Machine) 형태로 배포되는 경우가 많아, 이를 구동하기 위한 핵심 엔진으로 사용됩니다.
- **qcow2 (QEMU Copy On Write):** QEMU/KVM 가상화 기술에서 사용하는 가상 디스크 이미지 파일 포맷입니다. 'Copy On Write' 방식의 특성을 가져, 데이터가 변경될 때만 새로운 영역에 기록하므로 저장 공간을 매우 효율적으로 사용할 수 있습니다.
- **IOU (IOS on Linux):** 시스코의 운영체제인 IOS를 리눅스 환경에서 가볍게 구동할 수 있도록 컨버팅한 것입니다. 물리 장비의 기능을 매우 유사하게 재현하면 서도 리소스를 적게 차지하여 가상화 환경에서 널리 사용됩니다.
- **gns3a (GNS3 Appliance):** 특정 장비의 설정 파일과 이미지를 자동으로 받아와서 복잡한 설정 없이 바로 사용할 수 있게 도와주는 애플리케이션(Appliance) 관리 도구입니다.

2. 네트워크 트래픽 미러링 (Port Mirroring)

IDS(침입 탐지 시스템)나 IPS(침입 방지 시스템) 같은 보안 장비가 네트워크의 공격을 탐지하기 위해서는, 실제 통신이 일어나는 패킷의 복사본을 전달받아야 합니다. 이를 위해 스위치에서 제공하는 **Port Mirroring** 기능을 사용합니다.

구분	명칭	동작 원리 및 특징
L2 로컬	SPAN (Switched Port Analyzer)	분석 대상 포트와 보안 장비가 동일한 스위치 에 연결된 경우, 특정 포트의 트래픽을 지정된 포트로 복사하여 보냅니다.
L2 원격	RSPAN (Remote SPAN)	여러 대의 스위치를 거쳐 트래픽을 전달해야 할 때, 특정 VLAN 을 미러링 전용 통로로 지정하여 원격지의 스위치로 트래픽을 보냅니다.
L3 원격	ERSPAN (Encapsulated Remote SPAN)	트래픽을 Encapsulation(캡슐화) 하여 다른 네트워크 대역으로 전송합니다. L3 계층을 통해 원격지 전송이 가능합니다.

주의사항: 미러링 전용 포트는 기본적으로 '없는 포트'처럼 취급됩니다. 즉, 미러링 목적지(Destination)로 설정된 포트는 다른 장비로부터 들어오는 인바운드(Inbound) 통신을 처리할 수 없으므로, 설정 시 네트워크 구성에 주의해야 합니다.

3. 실습: Cisco 장비를 이용한 미러링 설정

가상 환경에서 구축된 스위치를 대상으로 SPAN과 RSPAN을 설정하는 절차는 다음과 같습니다.

[Case 1] SPAN 설정 (로컬 미러링)

gi0/1 포트에서 발생하는 모든 트래픽(인바운드/아웃바운드)을 gi0/0 포트로 복사하여 보안 장비(Snort 등)가 감시할 수 있도록 설정합니다.

```
[SW1]
conf t
# gi0/1의 인바운드(rx)와 아웃바운드(tx) 트래픽 모두를 소스로 지정
monitor session 1 source interface gi0/1 both
# 복사된 트래픽을 gi0/0 포트로 출력
monitor session 1 destination interface gi0/0
end
```

[Case 2] RSPAN 설정 (원격 미러링)

SW1의 트래픽을 VLAN 100을 통해 SW2로 전달하는 과정입니다. 먼저 두 스위치 모두에 미러링 전용 VLAN을 생성해야 합니다.

Step 1: SW1 설정 (트래픽 송신측)

```
[SW1]
conf t
# RSPAN 전용 VLAN 생성 및 설정
vlan 100
 name RSPAN-VLAN
 remote-span
exit

# 트래픽이 전달될 Trunk 인터페이스 설정
interface gi1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 100
 no shutdown
exit

# 소스 포트 지정 및 목적지를 원격 VLAN으로 설정
monitor session 1 source interface gigabitEthernet 0/1 both
monitor session 1 destination remote vlan 100
end
```

Step 2: SW2 설정 (트래픽 수신측)

```
[SW2]
conf t
# SW1과 동일한 RSPAN 전용 VLAN 생성
vlan 100
 name RSPAN-VLAN
 remote-span
exit

# SW1으로부터 트래픽을 받아올 Trunk 인터페이스 설정
interface gi0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
end

# Trunk 포트 허용 설정 및 활성화
interface gi0/0
 switchport trunk allowed vlan 100
 no shutdown
exit

# 수신 포트(Access 모드) 설정
interface gi0/1
 switchport mode access
 no shutdown
exit

# 원격 VLAN에서 들어온 트래픽을 실제 물리 포트(gi0/1)로 출력
monitor session 1 source remote vlan 100
monitor session 1 destination interface gi0/1
end
```

4. 실무 및 점검 포인트

가상화 환경 구축 후, 보안 장비(예: Snort)가 정상적으로 패킷을 수신하는지 확인하기 위해 다음 사항을 점검해야 합니다.

- **Promiscuous Mode 확인:** 보안 장비의 NIC(랜카드)는 자신의 IP/MAC이 목적지가 아닌 패킷도 모두 읽어들이 수 있는 **Promiscuous Mode**로 동작해야 합니다. 그렇지 않으면(Non-promiscuous) 미러링된 패킷을 대부분 드랍(Drop)하게 됩니다.

- **Snort 실행 및 검증:** 설정된 인터페이스(예: ens160)를 통해 패킷을 캡처하고 탐지 규칙이 동작하는지 확인합니다.

```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort/snort.lua -i ens160 -A alert_fast
```

- **트러블슈팅 체크리스트:**

1. 미러링 대상 포트가 `both`, `rx`, `tx` 중 적절하게 설정되었는가?
2. RSPAN 사용 시, 경로상에 있는 모든 스위치에 해당 VLAN이 `remote-span`으로 설정되어 있는가?
3. Trunk 포트에서 미러링용 VLAN이 `allowed vlan`에 포함되어 있는가?
4. 보안 장비의 인터페이스가 Promiscuous Mode로 활성화되어 있는가?

실무 적용 및 설정 검증 체크리스트

본 챕터에서는 네트워크 침입 탐지 및 차단 시스템(IDS/IPS)을 실무 환경에 구축할 때, 설계 단계에서 고려해야 할 기술적 차이점과 네트워크 미러링(Mirroring) 설정의 정확성을 검증하기 위한 핵심 항목을 다룹니다. 특히 Snort와 같은 탐지 엔진이 정상적으로 트래픽을 수집하고 분석할 수 있도록 하는 인프라 설정 검증에 집중합니다.

1. IDS 및 IPS 도입 설계 검증

보안 장비를 네트워크에 배치할 때는 **가용성(Availability)**과 **보안성(Security)** 중 어디에 우선순위를 둘 것인지에 따라 설치 방식이 달라집니다. 설계 단계에서 다음 사항을 반드시 검증해야 합니다.

- **IDS(Intrusion Detection System) 모드 검증:**
 - 장비 장애 시 서비스 연속성이 보장되는가? (IDS는 복사본을 받아 분석하므로 장비가 중단되어도 트래픽 흐름에 영향을 주지 않음)
 - 사후 대응을 위한 로그 기록 및 관제 기능이 정의되었는가?
 - 네트워크 구성이 포트 미러링(Port Mirroring) 또는 TAP을 통해 트래픽을 전달받는 구조인가?
- **IPS(Intrusion Prevention System) 모드 검증:**
 - 실제 위협 패킷을 차단(Packet Drop)하기 위해 **Inline(회선 중간)** 방식으로 배치되었는가?
 - 장비의 처리 속도가 전체 네트워크의 처리량(Throughput)을 저해하지 않는가? (IPS의 속도가 네트워크 전체 속도에 직접적인 영향을 미침)
 - **브릿지 모드(Bridge Mode)**로 설정되어 네트워크 대역 분리 없이 패킷 흐름을 제어하는가?

2. 네트워크 트래픽 수집(Mirroring) 설정 검증

보안 장비가 분석할 트래픽을 전달받기 위해서는 스위치에서의 미러링 설정이 정확해야 합니다. 구성 환경(로컬, 원격, L2 기반)에 따른 설정 명령어를 통해 검증합니다.

[검증 A] SPAN (Switched Port Analyzer) - 로컬 미러링

분석 대상 장비와 보안 장비가 동일한 스위치에 연결된 경우입니다. 지정한 포트의 트래픽을 다른 포트로 복제합니다.

```
[SW1 설정 예시]
conf t
monitor session 1 source interface gi0/1 both ; gi0/1의 인바운드(rx)와 아웃바운드(tx) 모두 지정
monitor session 1 destination interface gi0/0 ; 미러링된 트래픽을 gi0/0로 전송
```

⚠ **주의사항:** 미러링 전용 포트는 트래픽을 내보내는 용도이므로, 해당 포트로 들어오는 인바운드 통신은 허용되지 않습니다.

[검증 B] RSPAN (Remote SPAN) - L2 원격 미러링

여러 대의 스위치를 거쳐 원격지에 있는 보안 장비로 트래픽을 보낼 때 사용합니다. 특정 VLAN을 미러링 전용 통로로 활용합니다.

RSPAN 검증 절차:

1. **Source 스위치:** 미러링할 VLAN을 생성하고 `remote-span` 옵션을 부여했는가?
2. **Trunk 구성:** 스위치 간 연결 포트가 Trunk 모드이며, RSPAN 전용 VLAN이 허용(Allowed)되어 있는가?
3. **Destination 스위치:** 수신 포트가 RSPAN VLAN으로부터 트래픽을 받아 보안 장비로 전달하도록 설정되었는가?

```
[RSPAN 설정 핵심 명령어]
; Source 스위치 (SW1)
vlan 100
  remote-span
exit
monitor session 1 source interface gi0/1 both
monitor session 1 destination remote vlan 100

; Destination 스위치 (SW2)
vlan 100
  remote-span
exit
monitor session 1 source remote vlan 100
monitor session 1 destination interface gi0/1
```

3. Snort 엔진 및 인터페이스 동작 검증

수집된 패킷이 Snort 엔진에 도달하여 올바르게 처리되는지 확인하기 위해 다음의 데이터 흐름과 실행 옵션을 점검합니다.

데이터 처리 단계 점검

패킷이 다음의 5단계를 거쳐 정상적으로 처리되는지 확인합니다.

- 1. **NIC:** 케이블 신호를 수신하여 하드웨어 버퍼에 저장하는가?
- 2. **DAQ (Data Acquisition):** 커널 영역의 패킷을 사용자 영역(프로그램 메모리)으로 성공적으로 퍼 올리는가? (예: libpcap, afpacket 활용)
- 3. **Decoder:** 프로토콜 규격에 맞게 패킷을 해독하는가?
- 4. **Preprocessor:** 세션 재조립 및 데이터 전처리가 수행되는가?
- 5. **Detection:** 설정된 규칙(Rule)에 따라 공격 시그니처를 탐지하는가?

Snort 실행 명령어 분석 및 검증

실제 환경에서 Snort를 구동할 때 사용되는 명령어의 각 옵션이 의도대로 설정되었는지 확인합니다.

```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort/snort.lua -i ens160 -A alert_fast
```

- **-c [경로]:** Snort 설정 파일(snort.lua)의 경로가 정확한가?
- **-i [인터페이스]:** 트래픽을 수신할 NIC(예: ens160)가 올바르게 지정되었는가?
- **-A alert_fast:** 경보(Alert) 출력 방식이 실무 요구사항(빠른 경보 출력)에 부합하는가?

실무 핵심 포인트: Promiscuous Mode 확인
Snort가 자신의 IP/MAC 주소가 아닌 다른 목적지의 패킷까지 모두 분석하려면 랜카드가 **Promiscuous Mode(무차별 모드)**로 동작해야 합니다. 기본 모드 (Non-promiscuous)에서는 자신에게 오는 패킷만 수신하므로, 미러링된 트래픽을 놓칠 수 있습니다.

4. 최종 실무 적용 체크리스트

구분	점검 항목	확인 방법 및 기준
장비 모드	IDS vs IPS 선택 적절성	가용성 우선 시 IDS(Mirroring), 차단 우선 시 IPS(Inline)
네트워크	미러링 방식(SPAN/RSPAN)	동일 스위치 내는 SPAN, 원격지는 RSPAN/ERSPAN 설정 확인
스위치 설정	RSPAN VLAN 설정	VLAN에 remote-span 명령어가 적용되었는가?
스위치 설정	Trunk 허용 범위	미러링용 VLAN이 Trunk 포트에서 allowed 되어 있는가?
Snort 설정	인터페이스 모드	NIC가 Promiscuous Mode로 동작 중인가?
Snort 설정	규칙(Rule) 적용	Snort Community Rules 및 사용자 정의 룰이 정상 로드되었는가?