VPN(Virtual Private Network)

Part 1.

VPN 기본

01 VPN

VPN 개념

- 공중망(주로, 인터넷)을 통해 가상으로 구현된(확장시킨) 사설 네트워크
- 공중망을 통해 사적인 트래픽을 안전하게 통과시킴
- 공중망을 마치 확장된 전용 사설망 처럼 사용
- 회선비용을 크게 절감할 수 있는 통신 서비스

VPN 특징

- 기존의 공중망을 통한 가상망 구성 가능
- 망 구축 및 운용의 경제성
- 자유로운 주소지정 가능
-응용 및 구현 방식/방법이 대단히 많음

01 VPN

VPN 구축시 고려사항

상호운용성 : 다양한 시스템(기술/표준 등)들이 상호 동작할 수 있는 능력
확장성 : 재설계/재설치 등의 필요없이 확장이 얼마나 쉽고 가능한가에 대한 용이성
가용성 : 요구 기능을 요구 시간 동안 올바르게 수행할 수 있는 능력
보안성 : 가치있는 유무형 자산의 도난,손실,유출로부터 보호하는 것

01 VPN 구분

일반적 구분

방화벽 기반의 VPN(응용계층 기반 VPN)
라우터 기반의 VPN(네트워크 계층 기반 VPN)
전용선 기반의 VPN(물리계층 기반 VPN)

시스템 관점 구분

가입자 기반 VPN (CE-VPN, Customer Edge based VPN)
네트워크 기반 VPN (PE-VPN, Provider Edge based VPN)

서비스 관점 구분

VLL(Virtual Leased Lines) 서비스: 각 CE 라우터 간의 점대점 연결에 의한 사설망 구성 방식
VPRN(Virtual Private Routed Network) 서비스 :
공중망에서 ISP의 3계층 라우터 간에 터널링 방식으로 패킷을 전달시킴
VPDN(Virtual Private Dial Network)서비스 : 원격 사용자들이 공중망을 이용하여 원격터미널 형식을 빌어 사용
VPRS(Virtual Private LAN Segment)서비스 : ISP Edge 라우터들을 이용하여 가상 사설 LAN을 구성

Part 2.

Tunnling

02 Tunneling

터널링 기본

1. 터널링

데이터 스트림을 인터넷 상에서 가상의 파이프를 통해 전달시키는 기술
패킷 내에 터널링할 대상을 캡슐화시켜 목적지까지 전송

2. 터널링 기법

○ 두 노드 또는 두 네트워크 간에 가상의 링크(VPN 등)를 형성하는 기법
- 하나의 프로토콜이 다른 프로토콜을 감싸는 캡슐화 기능을 통해 운반

※ 일반적으로 터널링 기법은,
- 대부분 보안 채널의 역할을 하므로, 암호화 기법 적용이 일반적임
- 엄격하게 계층화된 프로토콜들을 심지어 뒤집어 감싸서 만들 수 있음
  . 오버레이 네트워크 구성도 가능하게 함

02 Tunneling

GRE

GRE (Generic Routing Encapsulation)

- ㅇ 원격 네트워크가 마치 로컬 네트워크인 것처럼 보이게하는 터널링 프로토콜
  - 임의 계층 프로토콜의 캡슐화가 가능케하여 이를 라우팅할 수 있도록 설계됨

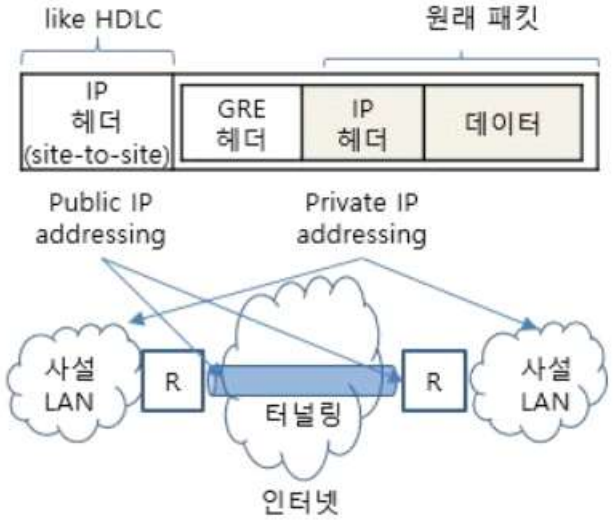
GRE 특징

- ㅇ Site to Site IP 터널링 프로토콜
  - 원래 시스코社에서 개발된 프로토콜
- ㅇ 데이터 암호화 기능은 제공하지 않음
  - 보안성 확보를 위해서는, IPsec 기능을 추가적으로 적용해야 함
- ㅇ 터널링 내 운반 가능 프로토콜
  - 3계층(IPv4, IPv6, IPX, IPSec), 2계층용 프레임 등 다양함
- ㅇ GRE 터널을 만들기 위해서는 미리,
  - 2 이상의 종단 라우터 간에 가상의 시리얼 링크 인터페이스를 설정하여야 함

02 Tunneling

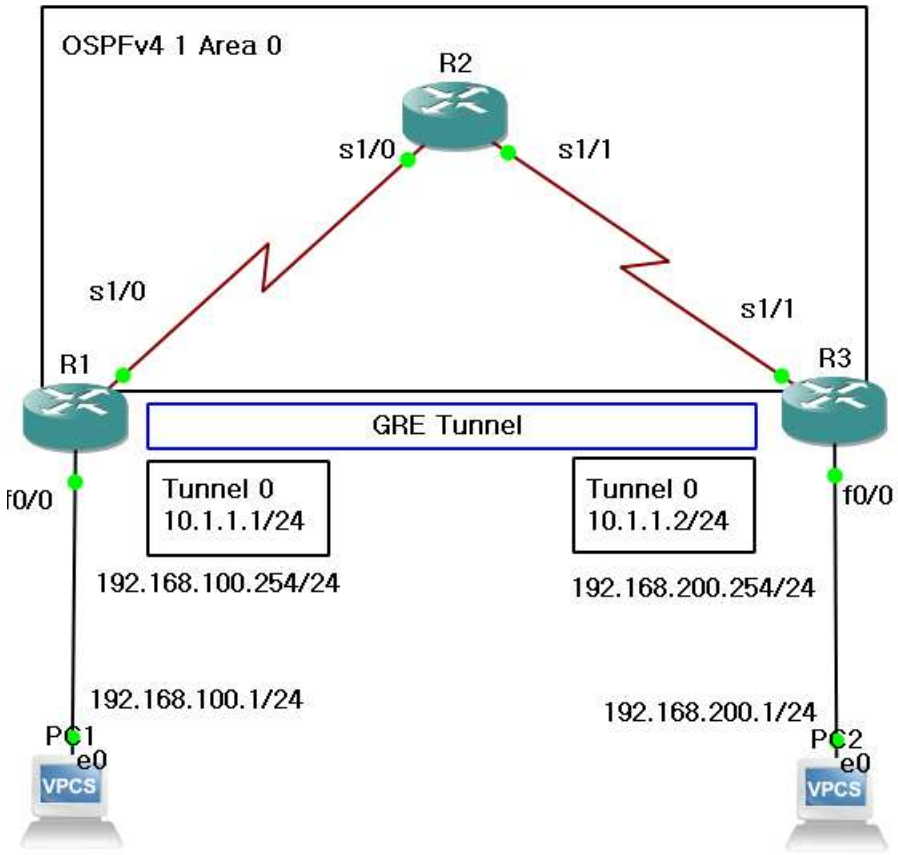
GRE Header

- 원래 패킷에 GRE 헤더를 붙이고,
  - 이 패킷을 2 이상의 라우터 간에, 미리 설정된 가상의 링크 상으로 전달하며,
  - 라우터 간에는, 단대단 HDLC 캡슐화시킨 것 처럼 취급함



02 Tunneling

환경구축



[R1]

```
config terminel
interface  Tunnel 0
ip address 10.1.1.1 255.255.255.0
tunnel source 1.1.1.1
tunnel destination 2.1.1.3

router eigrp 100
network 10.1.1.1 0.0.0.0
network 192.168.100.254 0.0.0.0
```

[R3]

```
config terminel
interface  Tunnel 0
ip address 10.1.1.2 255.255.255.0
tunnel source 2.1.1.3
tunnel destination 1.1.1.1

router eigrp 100
network 10.1.1.2 0.0.0.0
network 192.168.200.254 0.0.0.0
```

Part 3.

IPSec VPN

03 IPSec VPN

IPSec

네트워크계층(IP 계층) 상에서 IP 패킷 단위로 `인증`,`암호화`,`키관리`를 하는 프로토콜

IPSec 특징

인터넷 경유 구간에 일종의 보안 통로인 터널링을 형성해 줌
- Layer 3에서 캡슐화에 의해 보안 통로 제공

응용 소프트웨어 필요 없이, 대부분 운영체제에서 직접 제공
- 수송계층(TCP,UDP등) 하위에서 구현되기 때문에, 응용에 투명함
- 대부분, 운영체제 쪽에서 IPSec 구현 기능을 직접 제공하는 편임

가상사설망(VPN)에서 특히 많이 사용
- 사이트 투 사이트, 클라이언트 투 서버, 클라이언트 투 게이트웨이 등 다양한 적용 가능

03 IPSec VPN

IPSec 주요 보안 서비스

- 통신 상대방 인증 (Peer Authentication)
- 데이터 원천(근원지) 인증 (Data Origin Authentication)
- 비연결형 무결성 (Connectionless Integrity)
- 기밀성 (Confidentiality)
- 접근제어 (Access Control)
- 재생공격 방지 (Replay Attack Protection) 등

03 IPSec VPN

IPSec 프로토콜 구조

※ IP 계층에서 안전하게 데이터를 보호하기 위하여 다음과 같이 복수의 요소들로 구성

ㅇ 보안성을 제공하기 위한 2가지 종류의 프로토콜 `헤더`
- AH (인증 헤더, Authentication Header)
  . 발신지 인증,데이터 무결성 만을 보장
- ESP (캡슐화된 보안 페이로드, Encapsulating Security Payload)
  . 발신지 인증,데이터 무결성,기밀성 모두를 보장

ㅇ `키 관리` 프로토콜
- IKE (Internet Key Exchange)
  . IPSec을 위한 SA(보안연관)을 생성하며, 그에따른 키 관리를 수행하는 복합 프로토콜
    .. 공개 키 방식 구현이 가능하도록, 공개키,개인키 교환을 하는 프로토콜
- ISAKMP (Internet Security Association and Key Management Protocol)
  . IKE 교환을 위한 메세지 형식 및 기반구조로써 설계됨

- 여기서, SA(Security Association,보안연관) 이라 함은,
  . 보안 속성들을 함께 결합시켜, 세분화 및 추상화된 개념을 말하며,
  . 일련의 보안연관을 생성하는 과정이, 바로 IKE에 의함

03 IPSec VPN

IPSec 운용모드

○ Tunnel 모드 (터널 모드)
- IP 패킷 전체를 보호하고, 그 위에 새로운 IP 헤더를 추가하는 방식
- `두 라우터 간에`, `호스트와 라우터 간에`, `두 게이트웨이 간에` 주로 사용
  . 즉, IPSec VPN 구현

○ Transport 모드 (수송 모드)
- IP 헤더 이외 나머지 데이터 부분 만 보호하는 방식
  . 주로, 상위 계층 프로토콜 만을 보호하기 위해 사용
- `호스트-호스트 간에` 주로 사용
  . 즉, 종단대종단 구현

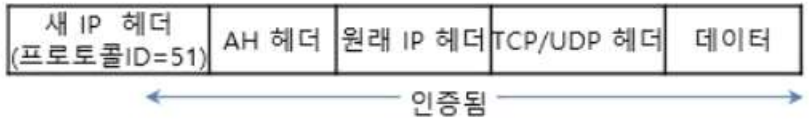
03 IPSec VPN

IPSec 운용 방식

○ AH 수송 모드 (AH Transport mode)

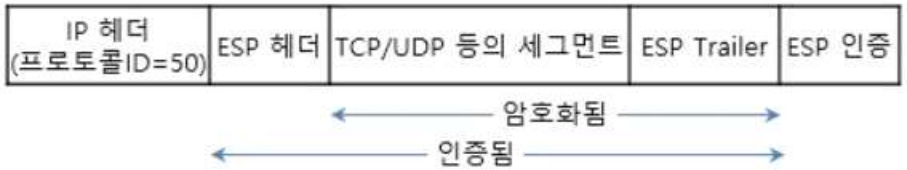
- IP 패킷 내 페이로드 및 IP 헤더 중 선택된 일부를 인증

○ AH 터널 모드 (AH Tunnel mode)

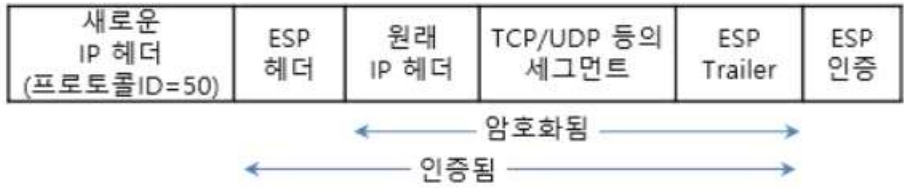


- 내부 IP 패킷 전체 및 외부 IP 헤더 중 선택된 일부를 인증

○ ESP 수송 모드 (ESP Transport mode)

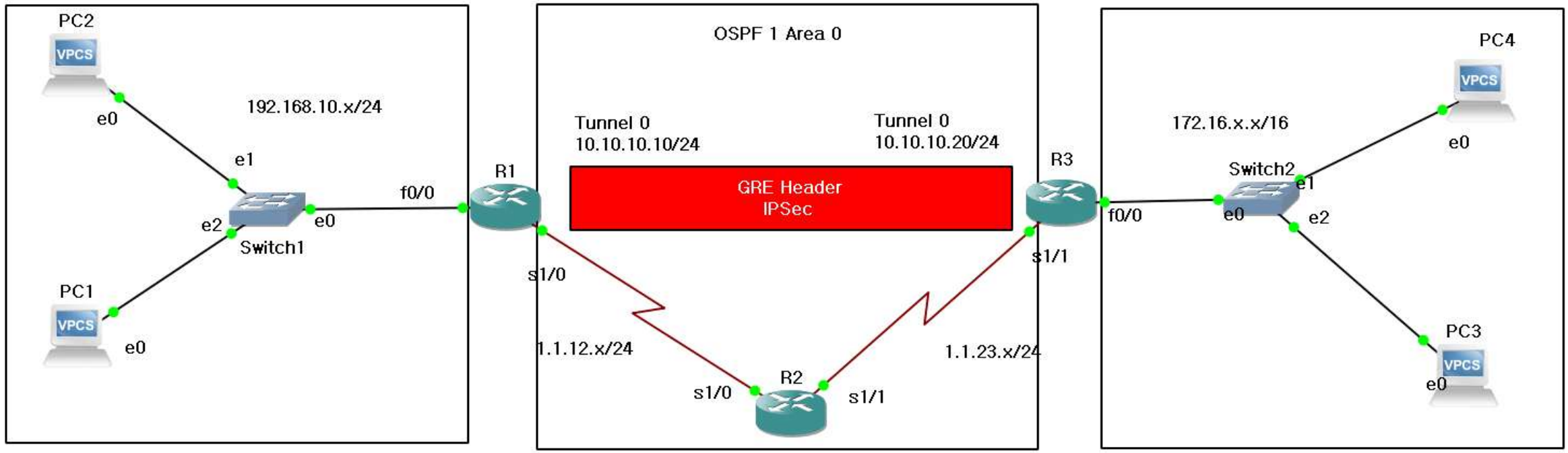


○ ESP 터널 모드 (ESP Tunnel mode)



- 전체 IP 패킷을 암호화하는데 사용
- 내부 IP 패킷의 인증은 선택사항 임

환경 설정



[환경 설정]

-R1-
```
enable
config ter
inter f0/0
ip add 192.168.10.254 255.255.255.0
no sh
inter s1/0
ip add 1.1.12.1 255.255.255.0
no sh
router os 1
router-id 1.1.1.1
net 1.1.12.0 0.0.0.255 area 0
```

-R2-
```
enable
config ter
inter s1/0
ip add 1.1.12.2 255.255.255.0
no sh
inter s1/1
ip add 1.1.23.2 255.255.255.0
no sh
router os 1
router-id 2.2.2.2
net 1.1.12.0 0.0.0.255 area 0
net 1.1.23.0 0.0.0.255 area 0
```

-R3-
```
enable
config ter
inter s1/1
ip add 1.1.23.3 255.255.255.0
no sh
inter f0/0
ip add 172.16.255.254 255.255.0.0
no sh
router os 1
router-id 3.3.3.3
net 1.1.23.0 0.0.0.255 area 0
```

03 IPSec VPN

IPSec(R1)

step1 - IKE Phase 1(ISAKMP) 정책 설정

```
- SA -
crypto  isakmp  policy  10
encryption  3des                    - 암호화 알고리즘지정
hash  md5                           - 해시화 알고리즘지정
authentication  pre-share           - 인증키 설정
group  2                            - 키교환 방식지정(디피헬먼 그룹)

-KEY-
crypto isakmp key 1234 address 2.1.1.3
```

step2 - IKE Phase 2(IPSec) 정책 설정

```
iaccess-list 100 permit gre host 1.1.12.1 host 1.1.23.3
access-list 100 permit gre 192.168.10.0 0.0.0.255 host 1.1.23.3

crypto ipsec transform-set IKE13 esp-3des esp-md5-hmac
정책 식별 이름 / IPSec암호화 알고리즘 / 인증 알고리즘
```

step3 - Phase1 + Phase2 정책 조합

```
crypto map vpn-map 10 ipsec-isakmp
match address 100
set peer 1.1.23.3
set transform-set IKE13
```

step4 - IPSec VPN 적용

```
interface s0/0
crypto map vpn-map
```

IPSec(R3)

step1 - IKE Phase 1(ISAKMP) 정책 설정

```
- SA -
crypto  isakmp  policy  10
encryption  3des                    - 암호화 알고리즘지정
hash  md5                           - 해시화 알고리즘지정
authentication  pre-share           - 인증키 설정
group  2                            - 키교환 방식지정(디피헬먼 그룹)

-KEY-

crypto isakmp key 1234 address 1.1.12.1
```

step2 - IKE Phase 2(IPSec) 정책 설정

```
access-list 100 permit gre host 1.1.23.3 host 1.1.12.1
access-list 100 permit gre 172.16.0.0 0.0.255.255 host 1.1.12.1

crypto ipsec transform-set IKE31 esp-3des esp-md5-hmac
```

step3 - Phase1 + Phase2 정책 조합

```
crypto map VPN31 10 ipsec-isakmp
match address R31
set peer 1.1.12.1
set transform-set IKE31
```

step4 - IPSec VPN 적용

```
interface s1/1
crypto map VPN31
```

END

고생하셨습니다