Technical Guide

오픈소스 IPSec VPN 연동

VyOS, Strongswan

September 2021

SAMSUNG SDS

Contents

1. IPSec VPN 개요

이 문서에서는 IPSec(Internet Protocol Security) VPN(Virtual Private Network)의 기본 개념을 이해하고 SDS Cloud 의 IPSec VPN 과 주요 오픈소스 VPN 과의 연동에 대해서 살펴보고자 합니다.

일반적으로 IPSec VPN 은 상호호환성이 중요한 기술로, 간단한 설정값의 차이로 인해 정상적으로 연결이 되지 않거나 단방향으로 트래픽만 흐르는 등 상호 연결되는 솔루션간의 호환성에 대한 검증이 필요합니다.

Site-to-Site 로 IPSec VPN 을 연결하고자 할 때, 상대 VPN 장비가 NAT(Network Address Translation) 뒤에 위치하고 있는 네트워크 토폴로지 상황에서 주요 IPSec Parameter 를 설명하겠습니다. 그런 다음 SDS Cloud VPN 서비스 설정 그리고 오픈소스 VPN 대표라고 할 수 있는 Strongswan, VyOS 환경설정과 검증하는 방법을 설명하겠습니다.

1.1 개념

IPSec 은 연결하고자 하는 2 개 Peer 간의 암호화된 통신을 제공하기 위한 서로를 인증(Authentication)하고 데이터 패킷을 암호화는데 필요한 네트워크 프로토콜 집합입니다. Peer 는 host-to-host, host-to-network, network-to-network 등이 될수 있으며, IPSec 을 이용해 원격지 사이에 가상의 사설 네트워크인 VPN 를 구성할 수 있습니다.

IPSec 은 인증, 무결성, 기밀성을 제공하기 위해 AH(Authentication Header), ESP(Encapsulation Security Payload) 프로토콜을 사용하며, ISAKMP(Internet Security Association and Key Management Protocol) 프레임워크을 통해 인증과 키교환 등을 제공합니다.

1. AH(Authentication Header): IP Extension Header로 출발지 인증과 데이터 무결성을 보장함, 단 암호화는 제공되지 않음
2. ESP(Encapsulation Security Payload): 기존 IP Packet을 Encapsulation하는 방식으로, 출발지 인증, 데이터 무결성과 함께 기밀성도 제공함
3. SA(Security Association): 암호화된 통신을 위해, 즉 데이터 기밀성을 확보하기 위한 암호화 알고리즘, 무결성을 위한 해시 알고리즘, Lifetime, 키 교환 방법 등을 협약으로 결정함

1.2 동작 모드

IP Header 를 제외한 Payload 만을 보호하는 방식인 전송모드(Transport Mode)와 IP Packet 전체를 보호하는 터널모드(Tunneling Mode)가 가능합니다.
전송모드는 host-to-host 경우에 주로 활용되며 network-to-network, network-to-host 등과 같은 경우에는 터널모드를 활용하는 경우가 많습니다. 특히 터널모드는 NAT Traversal 를 지원하므로 일반적인 Enterprise 네트워크 환경에서 유용합니다.

	Transport Mode	Tunneling Mode
AH	Original IP Header + AH + Original IP Payload	New IP Header + AH + Original IP Packet
ESP	Original IP Header + ESP Header + Original Payload + ESP Trailer & Authentication	New IP Header + ESP Header + Original IP Packet + ESP Trailer + ESP Authentication

1.3 IKEv1과 IKEv2 비교

IKE(Internet Key Exchange)는 키교환에 사용되는 프로토콜로 IKEv1, IKEv2 가 있습니다. 특히 IKEv2 는 IKEv1 보다 다양한 인증수단을 제공하고, 이동환경을 고려하였으며, NAT-Traversal 을 규격내에서 정의하였으며 메시지 교환도 효율적으로 개선하였습니다.

각각의 특징은 아래와 같습니다.

	IKEv1	IKEv2
특징	Phase1(Main mode)에서 6 개 메시지 교환, Phase 2(Quick mode)에서 3 개 메시지 교환 필요 Policy based VPN 구성 시 TS(Traffic Selector)당 Multiple Subnet 미 지원	총 4 개 메시지 교환: IKE_SA_INIT Req/Res, IKE_AUTH Req/Res EAP 로 다양한 인증방법 지원 MOBIKE 등 Mobile device 지원 NAT-Traversal 기본 지원

1.4 Route based VPN과 Policy based VPN 비교

경로기반 VPN(Route based VPN)은 IPSec 터널 인터페이스(일반적으로 Virtual Tunnel Interface, VTI 활용)를 생성하고 Peer VPN 으로 보내야하는 트래픽은 VTI 로 보내 터널을 지나 전송되는 방식입니다.
반면, 정책기반 VPN(Policy based VPN)은 IPSec 터널을 통해 통신되어야 하는 Remote/Local Subnet 에 대한 정책을 TS(Traffic Selector)를 활용해 생성해 구현하는 방식입니다.

각각의 특징은 아래와 같습니다.

	경로 기반 VPN	정책 기반 VPN
확장성	VPN 터널 개수는 터널 인터페이스로 제한	VPN 터널 개수는 Policy 개수로 제한
동적라우팅	터널 인터페이스 너머로 동적라우팅 지원	미 지원
토폴로지	Hub & Spoke, P2P, P2MP 지원	P2P 만 지원, Hub & Spoke 미지원
SA status	터널 인터페이스가 up 이라면 SA 항상 유지	해당 트래픽이 없으면 매칭되는 SA 는 해제
Vendor Agnostic	일부 VPN 솔루션에 한해 지원	다양한 VPN 솔루션 지원
유연성	새로운 네트워크 추가 시 라우팅 설정 필요	새로운 네트워크 추가 시 새로운 정책 적용
사용 사례	VPN 통과할 때 Source or Destination NAT 가 발생함 두개 LAN 에 중복된 Subnet 존재 가능 Hub&Spoke 네트워크 토폴로지 구성 가능 Primary & Backup VPN 구성 가능 VPN 너머로 동적 라우팅이 구성 가능 원격지에 여러 개의 subnet 접근 가능	원격지에 한개 subnet 만 접근할 경우

2. IPSec VPN 연동

2.1 네트워크 Topology

다음은 SDS Cloud 에 있는 2 개의 VPC 에 존재하는 개별 Virtual Server 와 On-premises Data Center 에 존재하는 서버간 통신이 필요한 네트워크 구성입니다. On-premises Data Center 의 경우에 VPN 과 개별 서버는 NAT 안에 존재하며 사설 IP 주소를 사용하는 경우를 상정하였습니다.

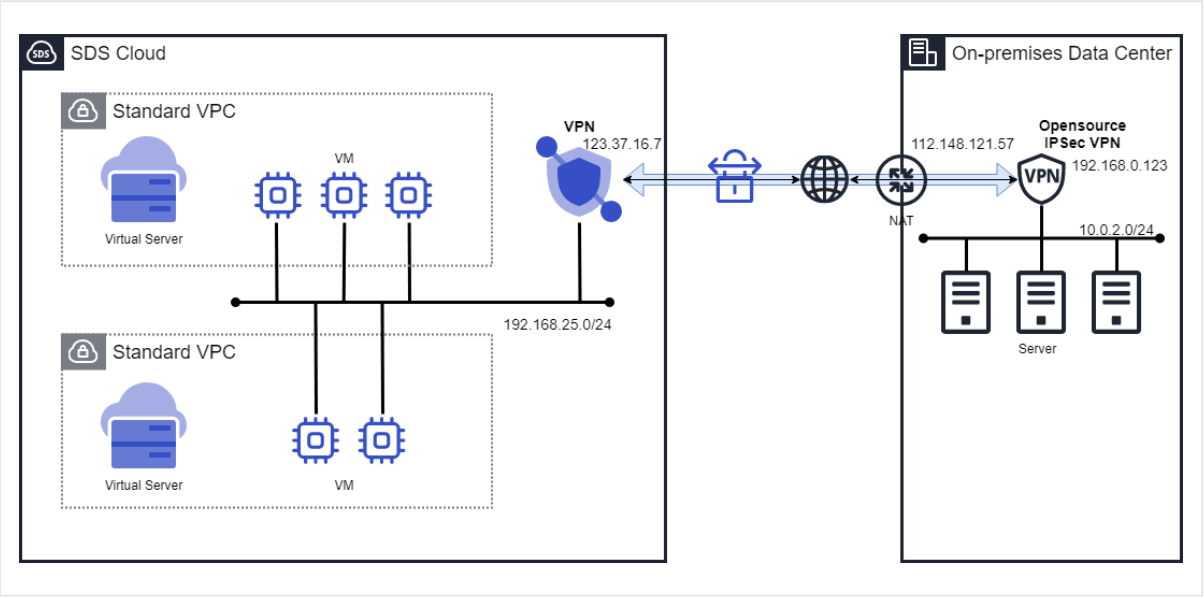


Figure 1. IPSec VPN 연동 네트워크 Topology

2.2 주요 파라미터

IPSec VPN 연결을 위해 정의해야 할 주요 파라미터로, VyOS 기준으로 설정값을 설명하겠습니다.

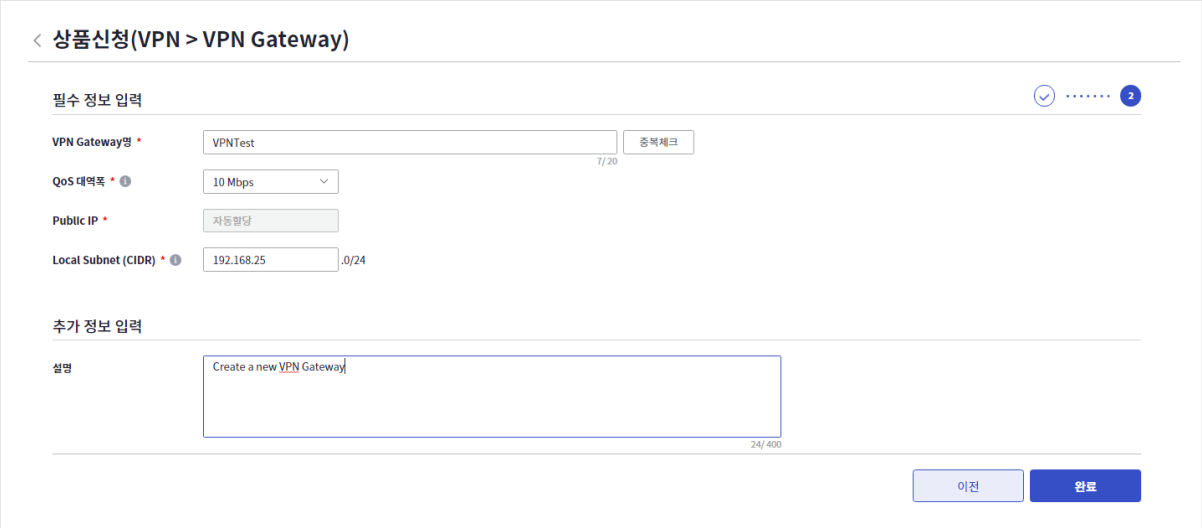
파라미터	설명
IPSec SA Mode	ESP & Tunnel mode
IPSec SA Lifetime	3600 seconds(10 Hours)
IPSec SA Proposal	Encryption AES256, Integrity(Hash) SHA256 암호화 및 해시 알고리즘
IPSec PFS	Diffie-Hellman(DH) Group 2(modp_1024) Perfect Forward Secrecy, 데이터 암호화에 동적 키 사용
IKE SA DPD	Restart, interval=15 seconds, timeout=60 seconds Dead Peer Detection, IKE Peer 의 상태 체크, 타임아웃시 연결 재협상 시도를 trigger 함
IKE SA ikev2-reauth	yes IKEv2 사용시 rekeying 프로세스에서 Peer 에 대한 재 인증

IKE SA Lifetime	86400 seconds(24 Hours)
IKE SA Proposal	DH Group 2, Encryption AES256, Integrity(Hash) SHA256 IKE SA 를 위한 제안, 암호화 및 해시 알고리즘
Site-to-Site Authentication	id=112.158.121.57, mode=pre-shared-secret Site-to-Site VPN Peer 인증에 사용할 id(일반적으로 VPN 연결에 사용한 interface 의 공인 IP 주소 활용) 및 방법(Pre Shared Key)
Site-to-Site Connection Type	Connection-type=Initiate 부팅 및 환경설정 이후 초기 연결 시도를 함
Site-to-Site ikev2-reauth	Ikev2-reauth=Inherit IKE group 의 기본동작을 승계해 사용함
Site-to-Site local-address	local-address=192.168.0.123 VPN Interface IP 주소, NAT 안에 있는 경우 사설 IP 주소
Site-to-Site vti	bind=vti1, esp-group Route based VPN 설정에 활용하는 옵션으로, Tunnel 에 사용할 Virtual Tunnel Interface(VTI). 트래픽 암호화에 사용할 ESP group 지정함
Site-to-Site tunnel #	local prefix=172.20.10.0/24 remote prefix=192.168.25.0/24 Policy based VPN 설정에 활용하는 옵션으로 IPSec 으로 암호화할 대상 Traffic Selector(Local subnet, Remote subnet)를 지정함

3. SDS Cloud VPN 서비스 환경설정

3.1 상품 신청

SDS Cloud Console 에 접속 후 프로젝트를 선택한 후, Networking 상품군의 VPN 을 선택합니다. 상품목록에서 상품신청을 클릭한 후 VPN Gateway 명, Public IP 주소(자동입력), Local Subnet(CIDR), 설명 등을 입력하고 완료합니다.

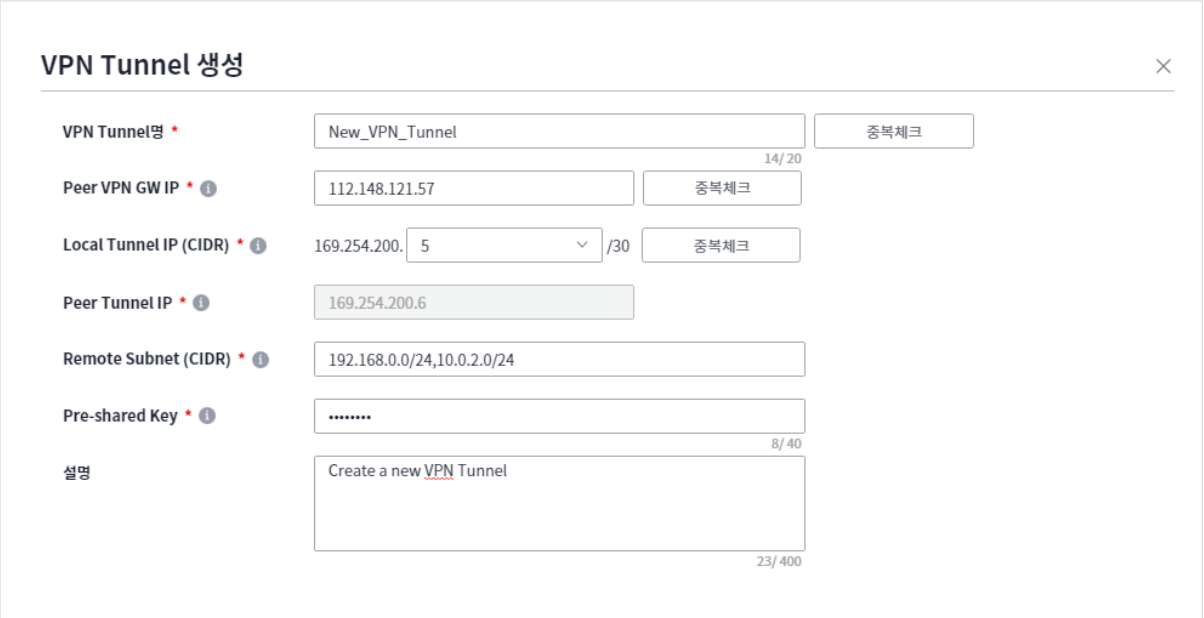


3.2 VPN tunnel 생성

VPN Gateway 상세정보에서 상태(active)를 확인하고, VPN Tunnel 탭 메뉴에서 VPN tunnel 생성을 선택합니다.

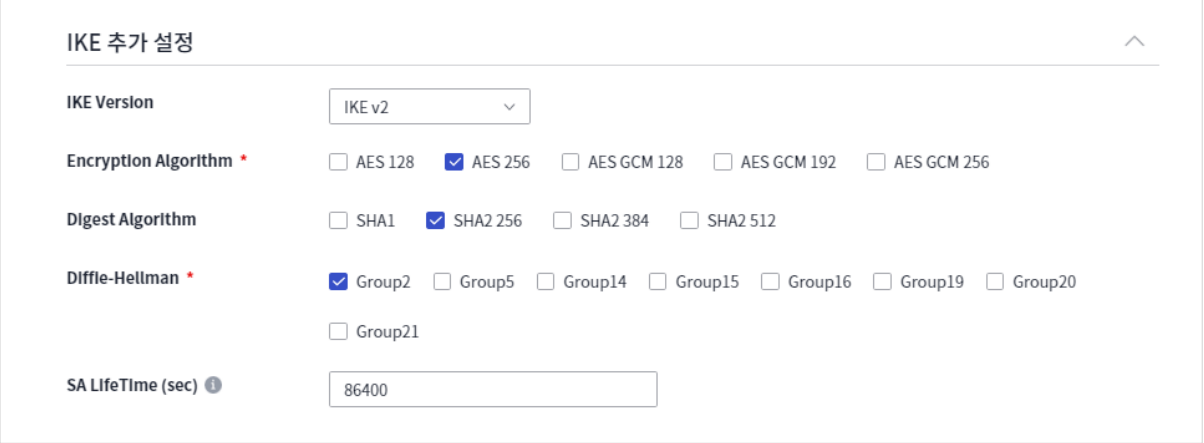
- 기본 설정

Tunnel 명, Peer VPN Gateway IP 주소(NAT 안에 있는 VPN 의 경우라면 Peer VPN Gateway 인터페이스가 가진 사설 IP 주소가 NAT 를 거치고 난 후 공인 IP 주소), Local Tunnel IP(Virtual Tunnel Interface, VTI 설정을 위한 IP 주소 선택 169.254.200.x/30), Peer Tunnel IP(Local Tunnel IP 가 선택되면 자동으로 결정됨), Remote Subnet(Peer VPN Gateway 을 통해 연결할 서브넷 대역), Pre-shared-Key(인증에 사용할 암호) 를 저장합니다.



- IKE 추가 설정

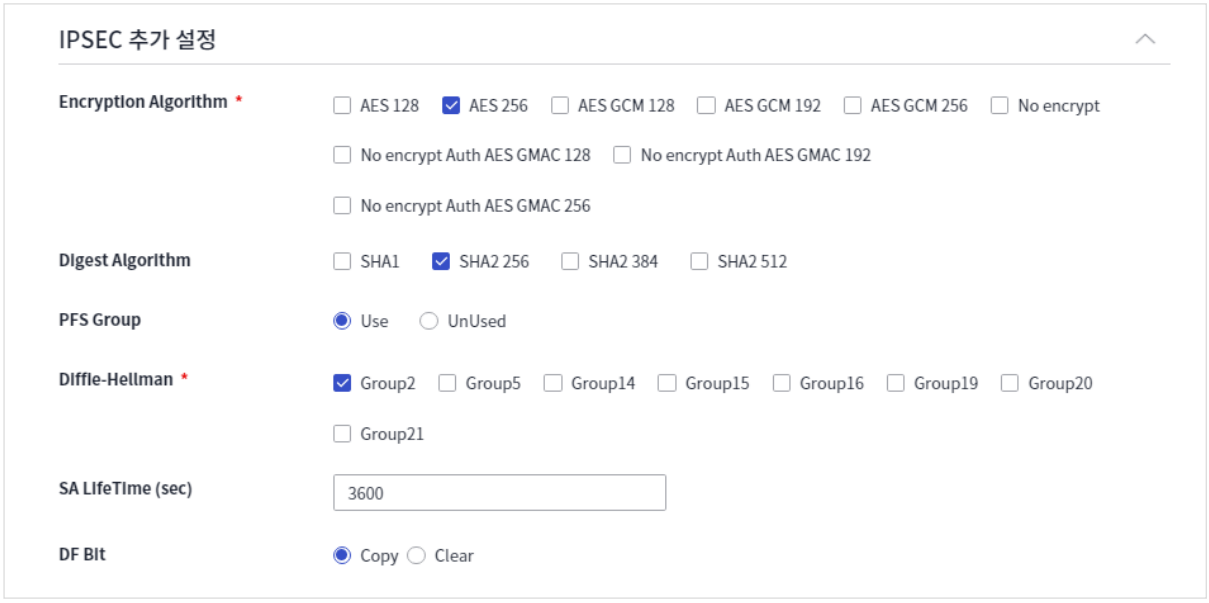
IKE SA(Security Association) 에 사용될 옵션(Proposal)을 설정합니다. 상대 VPN 이 제공하는 다양한 알고리즘을 모두 선택할 수 있습니다.
Key Exchange Protocol(IKEv1, IKEv2, IKE Flex= Peer VPN 요청에 따라 IKEv1,v2 로 동적으로 결정됨), IKE SA 에 활용할 Proposal 옵션 Encryption Algorithm(AES256), Digest Algorithm(SHA2 256), Diffie-Hellman Group(2, modp_1024)을 선택하고, SA Lifetime 값을 입력합니다.



- IPSec 추가 설정

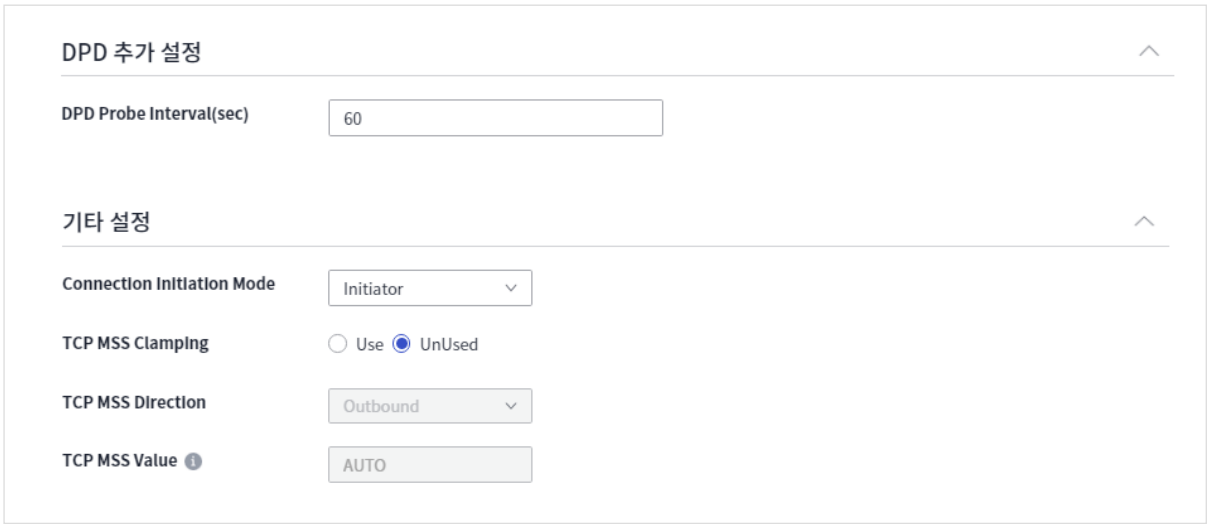
IPSec SA(Security Association) 에 사용될 옵션을 설정합니다. 상대 VPN 이 제공하는 다양한 알고리즘을 모두 선택할 수 있습니다.
IPSec SA 에 활용할 Proposal 옵션 Encryption Algorithm(AES256), Digest Algorithm(SHA2 256), PFS(Perfect Forward Secrecy) 사용유무, Diffie-Hellman

Group(2, modp_1024)을 선택하고, SA Lifetime(3600 초), DF(Don't Fragment) Bit 복사 여부(Copy)을 선택합니다.



- 기타 설정

DPD(Dead Peer Detection) Probe Interval, Connection Mode(Initiator)를 입력하고 선택합니다. TCP MSS(Maximum Segment Size) Clamping 기능은 IPSec 트래픽 암호화로 덧붙은 Header(IP, UDP, ESP 등)로 IP Packet 이 조각나는 상황을 예방하고자 MSS 값을 조정하는 것입니다.



4. 오픈소스 IPSec VPN 환경설정

4.1 VyOS

VyOS 는 오픈소스 Vyatta 에서 Forking 된 프로젝트로 Debian Linux 배포판을 기반한 오픈소스 NOS(Network Operating System)입니다. 라우터, 방화벽, IPSec VPN 등으로 자주 활용되곤 합니다.

아래 언급된 환경설정과 예시는 VyOS version 1.4(Sagitta)를 기준으로 검증하였습니다.

- 인터페이스 설정

VPN Gateway 는 적어도 내부 interface 와 외부 interface 를 적어도 하나씩은 보유하고 있어야 하며, SDS Cloud VPN 에 연결되는 외부 interface 는 NAT 안에 구성될 수 있습니다. VTI interface 는 Routed based VPN 설정에서 터널에 사용되는 논리적인 interface 입니다.

각 Interface 에 대한 확인은 아래 명령어로 확인할 수 있습니다.

```
vyos@vyos:~$ show configuration
interfaces {
    ethernet eth0 {
        address 192.168.0.123/24
        hw-id 08:00:27:e9:29:03
        description OUTSIDE
        duplex auto
        speed auto
    }
    ethernet eth1 {
        address 10.0.2.1/24
        hw-id 08:00:27:08:97:23
        description INSIDE
    }
    loopback lo {
    }
    vti vti1 {
        address 169.254.200.6/30
    }
}
```

- 환경 설정

VyOS 는 SSH 서비스 설정으로 접근이 가능하며, 연결되면 'configure' 명령어로 편집모드에 진입할 수 있습니다.

```
vyos@vyos:~$ configure
[edit]

SSH 서비스 설정
set service ssh

IPSec ESP 설정
set vpn ipsec esp-group SDS-Cloud-VPN lifetime 386000
set vpn ipsec esp-group SDS-Cloud-VPN mode tunnel
set vpn ipsec esp-group SDS-Cloud-VPN pfs dh-group2
set vpn ipsec esp-group SDS-Cloud-VPN proposal 1 encryption aes256
set vpn ipsec esp-group SDS-Cloud-VPN proposal 1 hash sha256

IPSec IKE 설정
set vpn ipsec ike-group SDS-Cloud-VPN ikev2-reauth yes
set vpn ipsec ike-group SDS-Cloud-VPN key-exchange ikev2
set vpn ipsec ike-group SDS-Cloud-VPN lifetime 36000
set vpn ipsec ike-group SDS-Cloud-VPN proposal 1 encryption aes256
set vpn ipsec ike-group SDS-Cloud-VPN proposal 1 hash sha256
set vpn ipsec ike-group SDS-Cloud-VPN proposal dh-group 2

IPSec Site-to-Site Tunnel 설정
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec site-to-site peer 123.37.16.7 authentication id 112.148.121.57
set vpn ipsec site-to-site peer 123.37.16.7 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 123.37.16.7 authentication pre-shared-secret 'password'
set vpn ipsec site-to-site peer 123.37.16.7 connection-type initiate
set vpn ipsec site-to-site peer 123.37.16.7 ike-group SDS-Cloud-VPN
set vpn ipsec site-to-site peer 123.37.16.7 ikev2-reauth inherit
set vpn ipsec site-to-site peer 123.37.16.7 local-address 192.168.0.123
# CASE 1. Route based VPN 설정
set vpn ipsec site-to-site peer 123.37.16.7 vti bind vti1
set vpn ipsec site-to-site peer 123.37.16.7 vti esp-group SDS-Cloud-VPN
set protocols static route 192.168.25.0/24 next-hop 169.254.200.5
# CASE 2. Policy based VPN 설정
set vpn ipsec site-to-site peer 123.37.16.7 tunnel 0 esp-group SDS-Cloud-VPN
set vpn ipsec site-to-site peer 123.37.16.7 tunnel 0 local prefix 192.168.0.0/24, 10.0.2.0/24
set vpn ipsec site-to-site peer 123.37.16.7 tunnel 0 remote prefix 192.168.25.0/24

기타 설정: TCP MSS 및 MTU 조정
set firewall options interface vti0 adjust-mss 1394
set interfaces vti vti0 mtu 1436
```

- 환경 저장

아래와 같은 명령어로 설정된 환경을 저장하고 startup configuration 에 반영합니다.

```
vyos@vyos:~# commit
[edit]

vyos@vyos:~# save
Saving configuration to '/config/config.boot'...
Done
```

4.2 Strongswan

Strongswan 은 오픈소스 IPSec VPN 으로 Linux, Android, macOS, Windows 등 다양한 플랫폼에서 동작합니다. 아래 환경설정과 예시는 strongswan 5.9.1(Charon)를 기준으로 검증하였습니다.

- 패킷 포워딩 활성화 설정

```
# 환경 설정
[root@vpn ~]# vi /etc/sysctl.conf

net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0

# 새 설정값 적용
[root@vpn ~]# sysctl -p
```

- VPN 환경 설정

/etc/strongswan/ipsec.conf, /etc/strongswan/ipsec.secrets 에 환경을 설정할 수 있습니다.

```
[root@vpn ~]# cat /etc/strongswan/ipsec.conf

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        strictcrlpolicy=yes
        uniqueids = no
       charondebug="cfg 2, ike 2, knl 2"

# Add connections here.
conn SDS-Cloud-VPN
        left=192.168.0.123
        leftid="112.148.121.57"
        right=123.37.16.7
        rightsubnet=192.168.25.0/24
        leftsubnet=10.0.2.0/24
        ike=aes256-sha256-modp1024!
        keyexchange=ikev2
        reauth=yes
        ikelifetime=86400s
        dpddelay=15s
        dpdtimeout=60s
        dpdaction=restart
        closeaction=none
        esp=aes256-sha256-modp1024!
        keylife=3600s
        rekeymargin=540s
        type=tunnel
        compress=no
        authby=secret
        auto=start
        keyingtries=%forever
```

```
[root@vpn ~]# cat /etc/ipsec.secrets

# ipsec.secrets - strongSwan IPsec secrets file
192.168.0.123 123.37.16.7 112.148.121.57 : PSK "password"
```

5. 오픈소스 IPSec VPN 연결 테스트 및 검증

5.1 VyOS

- IKE SA, IPSec SA 정상 연결 여부 확인

```
vyos@vyos:~$ show vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
123.37.16.7 123.37.16.7                 192.168.0.123 112.158.121.57

 State  IKEVer  Encrypt      Hash            D-H Group       NAT-T  A-Time  L-Time
 -----  ------  -------      ----            ---------       -----  ------  ------
 up     IKEv2   AES_CBC_256  HMAC_SHA2_256_128 MODP_1024       yes    266     0

vyos@vyos:~$ show vpn ipsec sa
Connection              State    Uptime     Bytes In/Out    Packets In/Out    Remote
address     Remote ID     Proposal
--------------------  -------  --------  --------------  ----------------  ----------------  ---------
--  ---------------------------------------
peer_123-37-16-7_vti  up       4m34s      1K/2K           14/36
123.37.16.7         N/A           AES_CBC_256/HMAC_SHA2_256_128/MODP_1024
```

- IPSec 연결 상태 상세 확인

```
vyos@vyos:~$ show vpn ipsec state
src 192.168.0.123 dst 123.37.16.7
        proto esp spi 0xad716f3e reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha256)
0x5ba80c61dee59a161a22d4311d41b63479b223d9dded2f06f4709a59e2de4c26 128
        enc cbc(aes)
0x32ba1855204aa95c2ef297dada14cec4ca59387e3c48422481b4813a66683dc2
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x24, bitmap 0x00000000
        if_id 0x1
src 123.37.16.7 dst 192.168.0.123
        proto esp spi 0xcc38892a reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha256)
0x55bc3fee9add1aa0c3c1afc106455325227848a6449bbddbbdcb583252105a05 128
        enc cbc(aes)
0x635912634140900a7a73dcbe07896a469b5cd224c2ad5b69b425eebae3d01304
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0xe, oseq 0x0, bitmap 0x00003fff
        if_id 0x1
```

- IPSec VPN 디버깅

```
vyos@vyos:~$ show vpn debug
Status of IKE charon daemon (strongSwan 5.9.1, Linux 5.10.57-amd64-vyos, x86_64):
  uptime: 5 minutes, since Aug 12 10:44:37 2021
  malloc: sbrk 2011136, mmap 0, used 1058224, free 952912
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon test-vectors ldap pkcs11 tpm aesni aes rc2 sha2 sha1 md5 mgf1
rdrand random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp
dnskey sshkey pem openssl gcrypt af-alg fips-prf gmp curve25519 agent chapoly xcbc cmac
hmac ctr ccm gcm drbg curl attr kernel-netlink resolve socket-default connmark stroke vici
updown eap-identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-radius eap-tls eap-ttls
eap-tnc xauth-generic xauth-eap xauth-pam tnc-tnccs dhcp lookip error-notify certexpire
led addrblock counters
Listening IP addresses:
  172.20.10.5
Connections:
peer_123-37-16-7:   192.168.0.123...123.37.16.7   IKEv2, dpddelay=15s
peer_123-37-16-7:    local:   [112.158.121.57] uses pre-shared key authentication
peer_123-37-16-7:    remote: uses pre-shared key authentication
peer_123-37-16-7_vti:    child:   0.0.0.0/0 ::/0 === 0.0.0.0/0 ::/0 TUNNEL,
dpdaction=restart
Security Associations (1 up, 0 connecting):
peer_123-37-16-7[1]: ESTABLISHED 5 minutes ago,
192.168.0.123[112.158.121.57]...123.37.16.7[123.37.16.7]
peer_123-37-16-7[1]: IKEv2 SPIs: 81ff24e12c24e9ef_i* aa77470fcbc244cc_r, rekeying in 3
hours
peer_123-37-16-7[1]: IKE proposal:
AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
peer_123-37-16-7_vti{1}:   INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: ce5885e7_i
6fc7c1f6_o
peer_123-37-16-7_vti{1}:   AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i (0 pkts, 144s
ago), 0 bytes_o (0 pkts, 145s ago), rekeying in 49 minutes
peer_123-37-16-7_vti{1}:    0.0.0.0/0 === 0.0.0.0/0
peer_123-37-16-7_vti{2}:   INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cc38892a_i
ad716f3e_o
peer_123-37-16-7_vti{2}:   AES_CBC_256/HMAC_SHA2_256_128/MODP_1024, 1176
bytes_i (14 pkts, 144s ago), 3024 bytes_o (36 pkts, 145s ago), rekeying in 50 minutes
peer_123-37-16-7_vti{2}:    0.0.0.0/0 === 0.0.0.0/0
```

- 패킷 덤프 확인

```
vyos@vyos:~$ sudo su
root@vyos:/home/vyos# tcpdump -i vti1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on vti1, link-type RAW (Raw IP), snapshot length 262144 bytes
10:50:43.716524 IP 192.168.25.3 > 10.0.2.1: ICMP echo request, id 9970, seq 11, length 64
10:50:43.716543 IP 10.0.2.1 > 192.168.25.3: ICMP echo reply, id 9970, seq 11, length 64
10:50:44.720615 IP 192.168.25.3 > 10.0.2.1: ICMP echo request, id 9970, seq 12, length 64
10:50:44.720633 IP 10.0.2.1 > 192.168.25.3: ICMP echo reply, id 9970, seq 12, length 64
```

5.2 strongswan

- IPSec 연결 및 디버깅

```
[root@vpn ~]# strongswan start

[root@vpn ~]# strongswan statusall
Status of IKE charon daemon (strongSwan 5.9.1, Linux 4.18.0-147.8.1.el8_1.x86_64,
x86_64):
  uptime: 2 minutes, since Aug 26 02:23:57 2021
  malloc: sbrk 1998848, mmap 0, used 1015712, free 983136
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon test-vectors ldap pkcs11 tpm aesni aes rc2 sha2 sha1 md5 mgf1
rdrand random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp
dnskey sshkey pem openssl gcrypt af-alg fips-prf gmp curve25519 agent chapoly xcbc cmac
hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default connmark stroke vici
updown eap-identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-radius eap-tls eap-ttls
eap-tnc xauth-generic xauth-eap xauth-pam tnc-tnccs dhcp lookip error-notify certexpire
led addrblock counters
Listening IP addresses:
  192.168.0.123
Connections:
SDS-Cloud-VPN:  192.168.0.123...123.37.16.7  IKEv2, dpddelay=15s
SDS-Cloud-VPN:   local:  [112.158.121.57] uses pre-shared key authentication
SDS-Cloud-VPN:   remote: [123.37.16.10] uses pre-shared key authentication
SDS-Cloud-VPN:   child:  10.0.2.0/24 === 192.168.25.0/24 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
SDS-Cloud-VPN[1]: ESTABLISHED 2 minutes ago,
192.168.0.123[112.158.121.57]...123.37.16.7[123.37.16.7]
SDS-Cloud-VPN[1]: IKEv2 SPIs: 771dfb03de6d3ac4_i* 853390be58e29d9d_r, pre-shared
key reauthentication in 23 hours
SDS-Cloud-VPN[1]: IKE proposal:
AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
SDS-Cloud-VPN{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c9ce42eb_i 7a716a14_o
SDS-Cloud-VPN{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i (0 pkts, 5s ago), 0
bytes_o (0 pkts, 5s ago), rekeying in 39 minutes
SDS-Cloud-VPN{1}:   10.0.2.0/24 === 192.168.25.0/24
```

- IPSec 연결 상태 확인

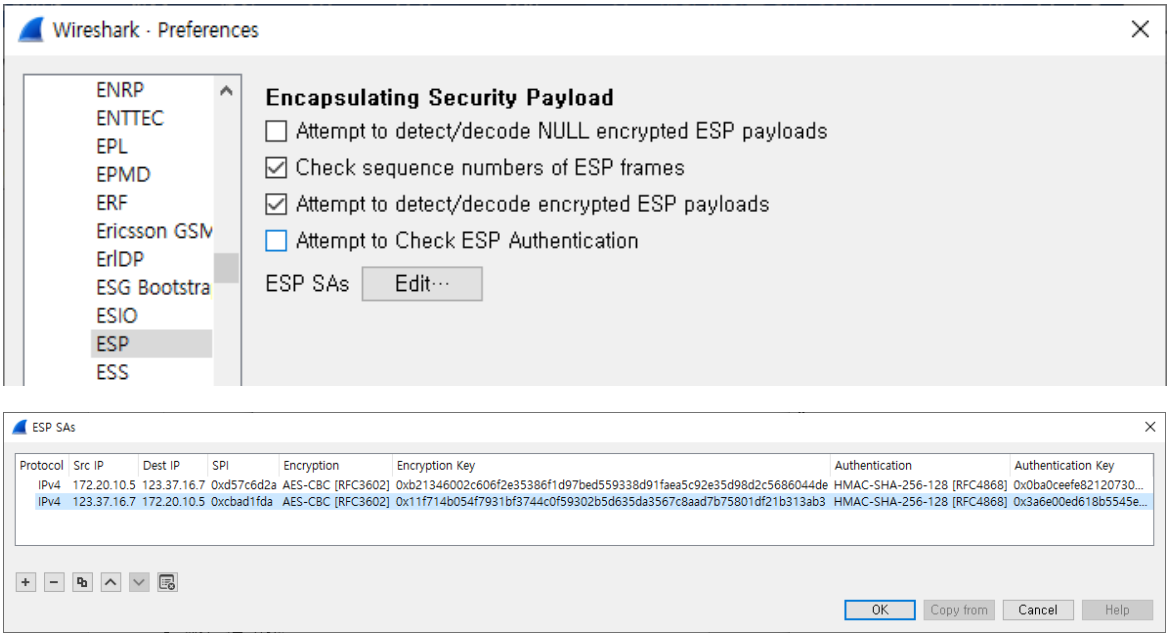
```
[root@vpn ~]# ip -s xfrm state
src 192.168.0.123 dst 123.37.16.7
        proto esp spi 0x7a716a14(2054253076) reqid 1(0x00000001) mode tunnel
        replay-window 0 seq 0x00000000 flag af-unspec (0x00100000)
        auth-trunc hmac(sha256)
0x8fce17d5f1f35fba72c26bb4b333bdb3954aa889e8c8050b0f2c6701a4e9c8b7 (256 bits)
128
        enc cbc(aes)
0x95db5c60b4d21f1fb43e4d006e6104d51cd3962083ea0d96565ed0de7e533c84 (256
bits)
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
          expire add: soft 2633(sec), hard 3600(sec)
          expire use: soft 0(sec), hard 0(sec)
        lifetime current:
          0(bytes), 0(packets)
          add 2021-08-26 02:24:01 use -
        stats:
          replay-window 0 replay 0 failed 0
src 123.37.16.7 dst 192.168.0.123
        proto esp spi 0xc9ce42eb(3385737963) reqid 1(0x00000001) mode tunnel
        replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
        auth-trunc hmac(sha256)
0x8e28679a4348bbda7787eaad61d7246704f33233f986a860cda6fdc488bafaf7 (256 bits)
128
        enc cbc(aes)
0x12b9d972b3d06cc25993f7640d97e1dee18b9723e336963806e340e5c5b21d34 (256
bits)
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
          expire add: soft 2536(sec), hard 3600(sec)
          expire use: soft 0(sec), hard 0(sec)
        lifetime current:
          0(bytes), 0(packets)
          add 2021-08-26 02:24:01 use -
        stats:
          replay-window 0 replay 0 failed 0
```

5.3 트래픽 복호화

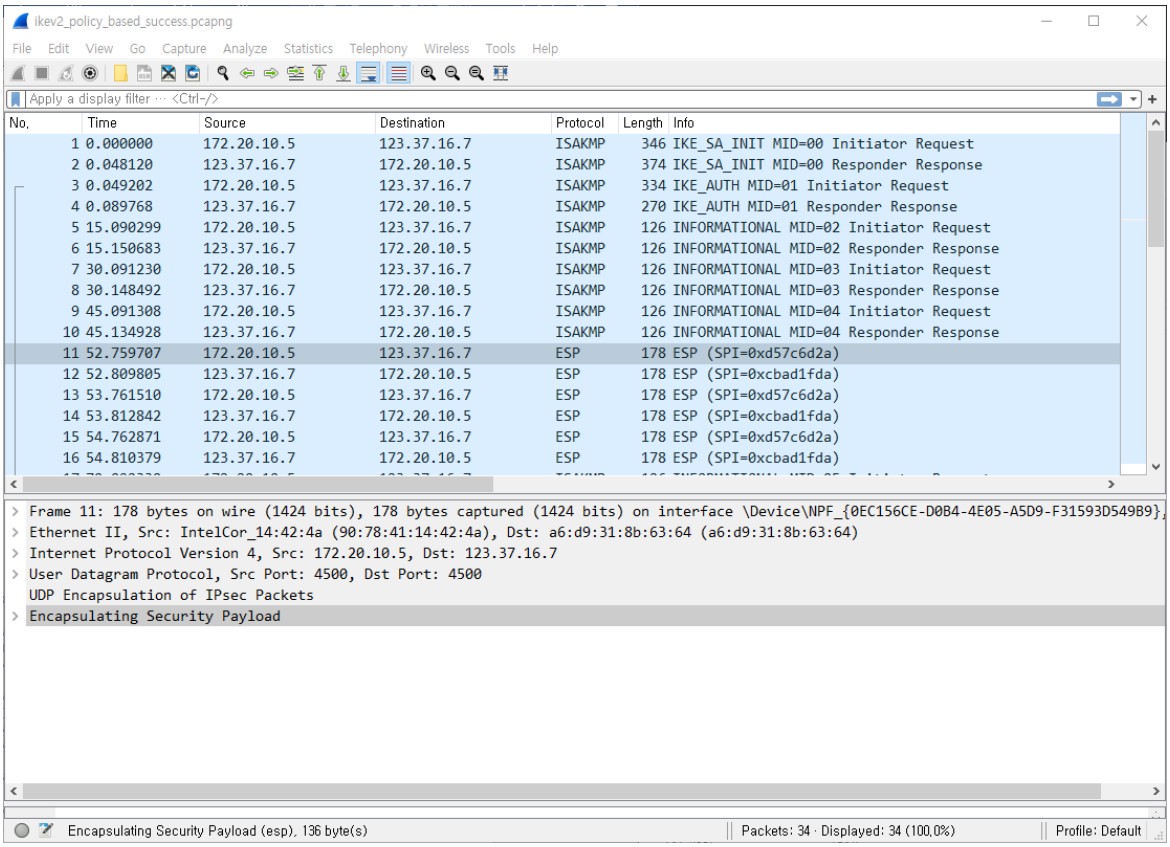
- Wireshark을 이용한 ESP 패킷 복호화

Wireshark 메뉴에서 Edit > Preferences > Protocols > ESP 를 선택하고 복호화 옵션(Attepts to detect/decode encrypted ESP payloads)을 체크한 후, 'Edit SAs'를 편집합니다. IPSec ESP SA State 관련 정보(Source IP, Destination IP, SPI, Encryption Algorithm, Encryption Key, Hash Algorithm, Hash Key)를 입력하고 저장하면 복호화된 ESP 패킷을 확인할 수 있습니다.

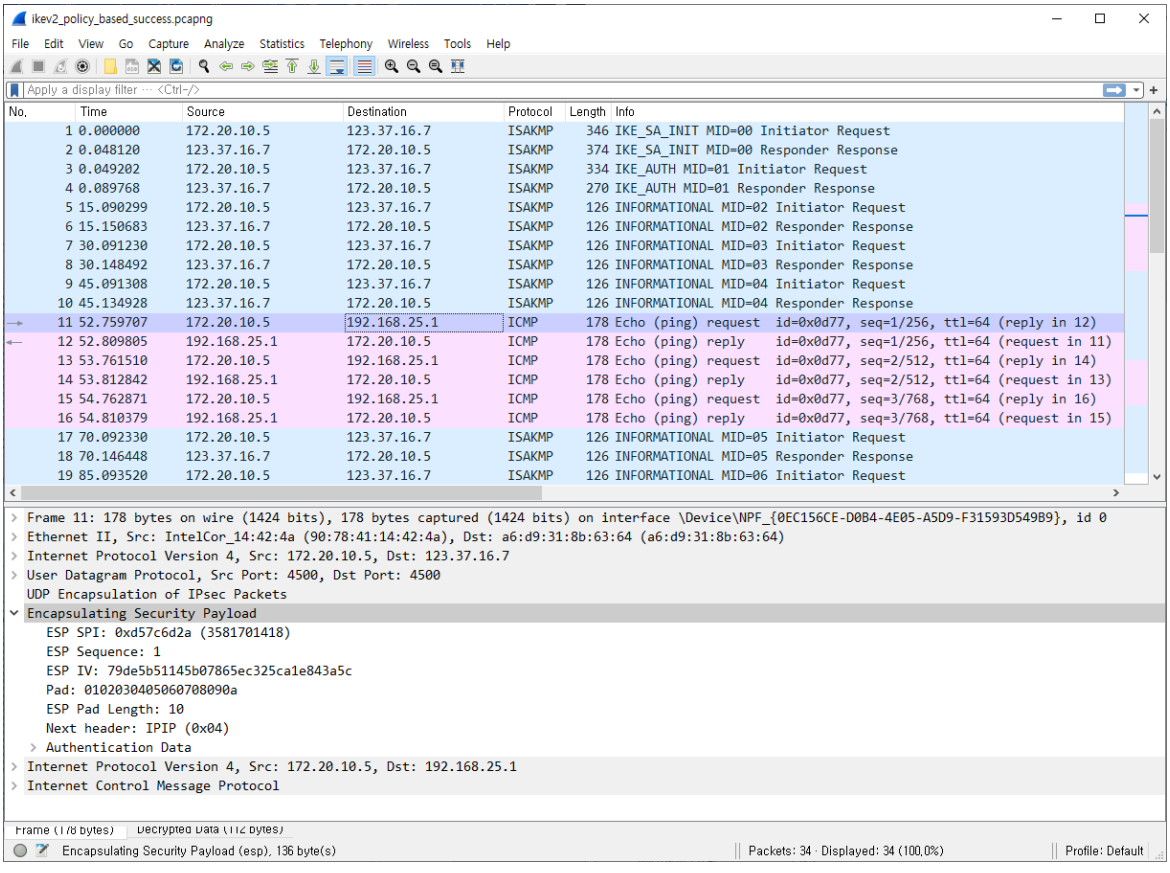
```
vyos@vyos:~$ show vpn ipsec state
src 172.20.10.5 dst 123.37.16.7
        proto esp spi 0xd57c6d2a reqid 2 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha256)
0x0ba0ceefe82120730d89cab2e43d6bfc198ad9f37782789184af9669190c408b 128
        enc cbc(aes)
0xb21346002c606f2e35386f1d97bed559338d91faea5c92e35d98d2c5686044de
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
src 123.37.16.7 dst 172.20.10.5
        proto esp spi 0xcbad1fda reqid 2 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha256)
0x3a6e00ed618b5545e117236d71c8ed5fec19e5452b4e8978f6fbd3c2457322d1 128
        enc cbc(aes)
0x11f714b054f7931bf3744c0f59302b5d635da3567c8aad7b75801df21b313ab3
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
```



복호화 전


ikev2_policy_based_success.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 172.20.10.5 123.37.16.7 ISAKMP 346 IKE_SA_INIT MID=00 Initiator Request
2 0.048120 123.37.16.7 172.20.10.5 ISAKMP 374 IKE_SA_INIT MID=00 Responder Response
3 0.049202 172.20.10.5 123.37.16.7 ISAKMP 334 IKE_AUTH MID=01 Initiator Request
4 0.089768 123.37.16.7 172.20.10.5 ISAKMP 270 IKE_AUTH MID=01 Responder Response
5 15.090299 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=02 Initiator Request
6 15.150683 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=02 Responder Response
7 30.091230 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=03 Initiator Request
8 30.148492 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=03 Responder Response
9 45.091308 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=04 Initiator Request
10 45.134928 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=04 Responder Response
11 52.759707 172.20.10.5 123.37.16.7 ESP 178 ESP (SPI=0xd57c6d2a)
12 52.809805 123.37.16.7 172.20.10.5 ESP 178 ESP (SPI=0xcbad1fda)
13 53.761510 172.20.10.5 123.37.16.7 ESP 178 ESP (SPI=0xd57c6d2a)
14 53.812842 123.37.16.7 172.20.10.5 ESP 178 ESP (SPI=0xcbad1fda)
15 54.762871 172.20.10.5 123.37.16.7 ESP 178 ESP (SPI=0xd57c6d2a)
16 54.810379 123.37.16.7 172.20.10.5 ESP 178 ESP (SPI=0xcbad1fda)
Frame 11: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface \Device\NPF_{0EC156CE-D0B4-4E05-A5D9-F31593D549B9},
Ethernet II, Src: IntelCor_14:42:4a (90:78:41:14:42:4a), Dst: a6:d9:31:8b:63:64 (a6:d9:31:8b:63:64)
Internet Protocol Version 4, Src: 172.20.10.5, Dst: 123.37.16.7
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
Encapsulating Security Payload (esp), 136 byte(s)
Packets: 34 · Displayed: 34 (100,0%)
Profile: Default

복호화 후


ikev2_policy_based_success.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 172.20.10.5 123.37.16.7 ISAKMP 346 IKE_SA_INIT MID=00 Initiator Request
2 0.048120 123.37.16.7 172.20.10.5 ISAKMP 374 IKE_SA_INIT MID=00 Responder Response
3 0.049202 172.20.10.5 123.37.16.7 ISAKMP 334 IKE_AUTH MID=01 Initiator Request
4 0.089768 123.37.16.7 172.20.10.5 ISAKMP 270 IKE_AUTH MID=01 Responder Response
5 15.090299 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=02 Initiator Request
6 15.150683 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=02 Responder Response
7 30.091230 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=03 Initiator Request
8 30.148492 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=03 Responder Response
9 45.091308 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=04 Initiator Request
10 45.134928 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=04 Responder Response
11 52.759707 172.20.10.5 192.168.25.1 ICMP 178 Echo (ping) request id=0x0d77, seq=1/256, ttl=64 (reply in 12)
12 52.809805 192.168.25.1 172.20.10.5 ICMP 178 Echo (ping) reply id=0x0d77, seq=1/256, ttl=64 (request in 11)
13 53.761510 172.20.10.5 192.168.25.1 ICMP 178 Echo (ping) request id=0x0d77, seq=2/512, ttl=64 (reply in 14)
14 53.812842 192.168.25.1 172.20.10.5 ICMP 178 Echo (ping) reply id=0x0d77, seq=2/512, ttl=64 (request in 13)
15 54.762871 172.20.10.5 192.168.25.1 ICMP 178 Echo (ping) request id=0x0d77, seq=3/768, ttl=64 (reply in 16)
16 54.810379 192.168.25.1 172.20.10.5 ICMP 178 Echo (ping) reply id=0x0d77, seq=3/768, ttl=64 (request in 15)
17 70.092330 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=05 Initiator Request
18 70.146448 123.37.16.7 172.20.10.5 ISAKMP 126 INFORMATIONAL MID=05 Responder Response
19 85.093520 172.20.10.5 123.37.16.7 ISAKMP 126 INFORMATIONAL MID=06 Initiator Request
Frame 11: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface \Device\NPF_{0EC156CE-D0B4-4E05-A5D9-F31593D549B9}, id 0
Ethernet II, Src: IntelCor_14:42:4a (90:78:41:14:42:4a), Dst: a6:d9:31:8b:63:64 (a6:d9:31:8b:63:64)
Internet Protocol Version 4, Src: 172.20.10.5, Dst: 123.37.16.7
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
ESP SPI: 0xd57c6d2a (3581701418)
ESP Sequence: 1
ESP IV: 79de5b51145b07865ec325ca1e843a5c
Pad: 0102030405060708090a
ESP Pad Length: 10
Next header: IPIP (0x04)
Authentication Data
Internet Protocol Version 4, Src: 172.20.10.5, Dst: 192.168.25.1
Internet Control Message Protocol
Encapsulating Security Payload (esp), 136 byte(s)
Packets: 34 · Displayed: 34 (100,0%)
Profile: Default

6. 호환성 및 고려 사항

- VyOS version 1.4 이전 버전 호환성

IKEv2 설정에서 Route based VPN(VTI 연결) 호환성 이슈가 있어 정상적으로 연결이 되지 않습니다. IKEv1 을 사용해야 하거나, IKEv2 를 선택해야만 하는 상황이라면 Policy based VPN 으로 연동해야 합니다.

- Policy based VPN에서 IKEv1 Multi-Subnet 미 지원

IKEv1 설정에서 Policy based VPN 방법으로 연동할 경우 local subnet, remote subnet 은 한 개의 subnet 으로만 구성할 수 있으며 다수 subnet 연결하고자 정책설정하기를 희망하는 경우 키교환 프로토콜을 IKEv2 로 변경해야 합니다.