

SECUI

—

BLUEMAX NGF V1.0

IPSec VPN

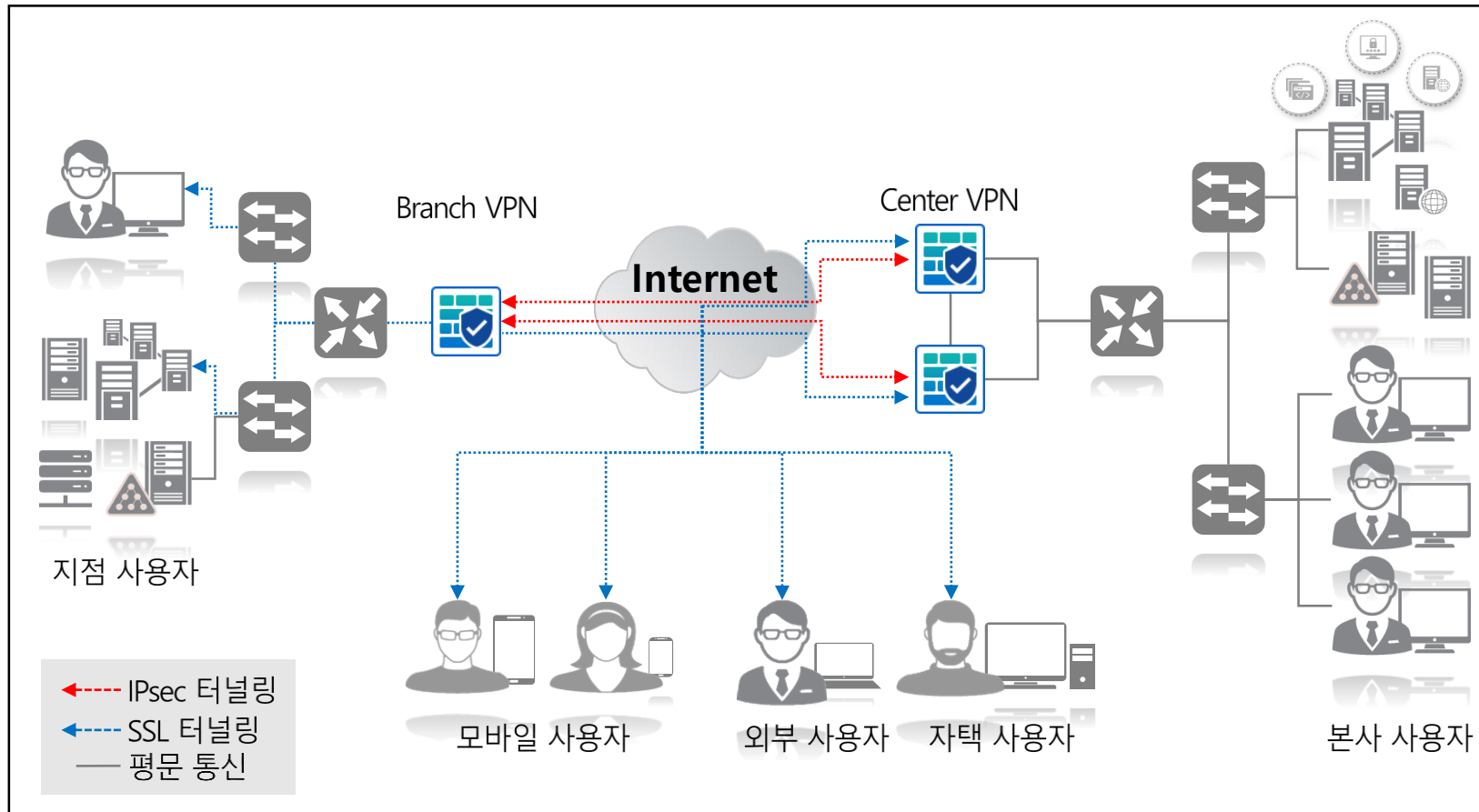
TABLE OF CONTENTS

1. VPN 개요
2. 암호화 기법
3. IPSec, IKEv2
4. BLUEMAX NGF IPSec VPN 특징
5. IPSec VPN 메뉴 설명
6. 구성 실습
7. 일반 터널링
8. CLI 명령어

[별첨] 보안 강도 별 권고 암호 알고리즘 (출처-KISA)

1.1 VPN (Virtual Private Network) 란?

- 기능 : 공중망(Internet)을 사설망(Private Network)과 같이 안전한 통신이 가능하도록 가상(Virtual)의 터널을 만들어 암호화된 데이터를 전송하는 기술



1.2 VPN의 필요성

• 내가 사용하는 인터넷 통신은 안전한가?

- IPv4 는 Payload Data에 대한 비밀성(Secrecy), 무결성(Integrity), 발신인 인증(Origin Authentication)등이 매우 취약함.
- Packet의 모든 내용이 Plain Text로 Open되어 있어 비밀성을 보장 할 수 없음.
- 중간에 있는 공격자가 packet의 내용을 훼손하거나 수정하여도 감지할 수 있는 방법이 없음.
- 발신지 주소를 변조하여 거짓 packet을 보내와도 사전에 막을 수 있는 방법이 없음.

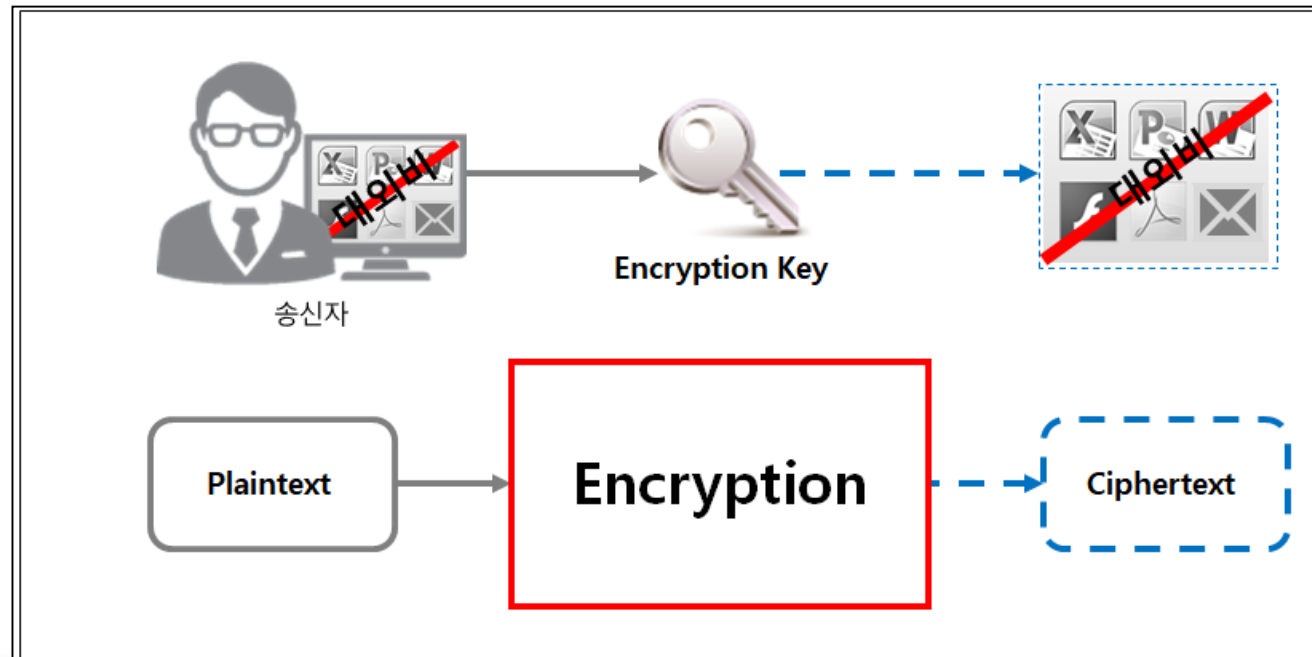
• 안전한 통신을 위해선?

- IPsec VPN은 Layer3 에서 packet 단위의 보안 제공을 위해 IETF에서 제안되어진 국제 표준으로 Application에 구매를 받지 않고 만족스러운 보안성을 확보할 수 있음. (이기종간 VPN 연결 가능)
- IPv4 SSL(Secure Socket Layer)는 Netscape 사에서 TCP를 사용하는 Application의 end-to-end간의 보안 제공을 위하여 개발되었고, 각각의 Application들에 대한 설정 및 변경이 필요함.

2.1 암호화 기법

- 데이터 암호화

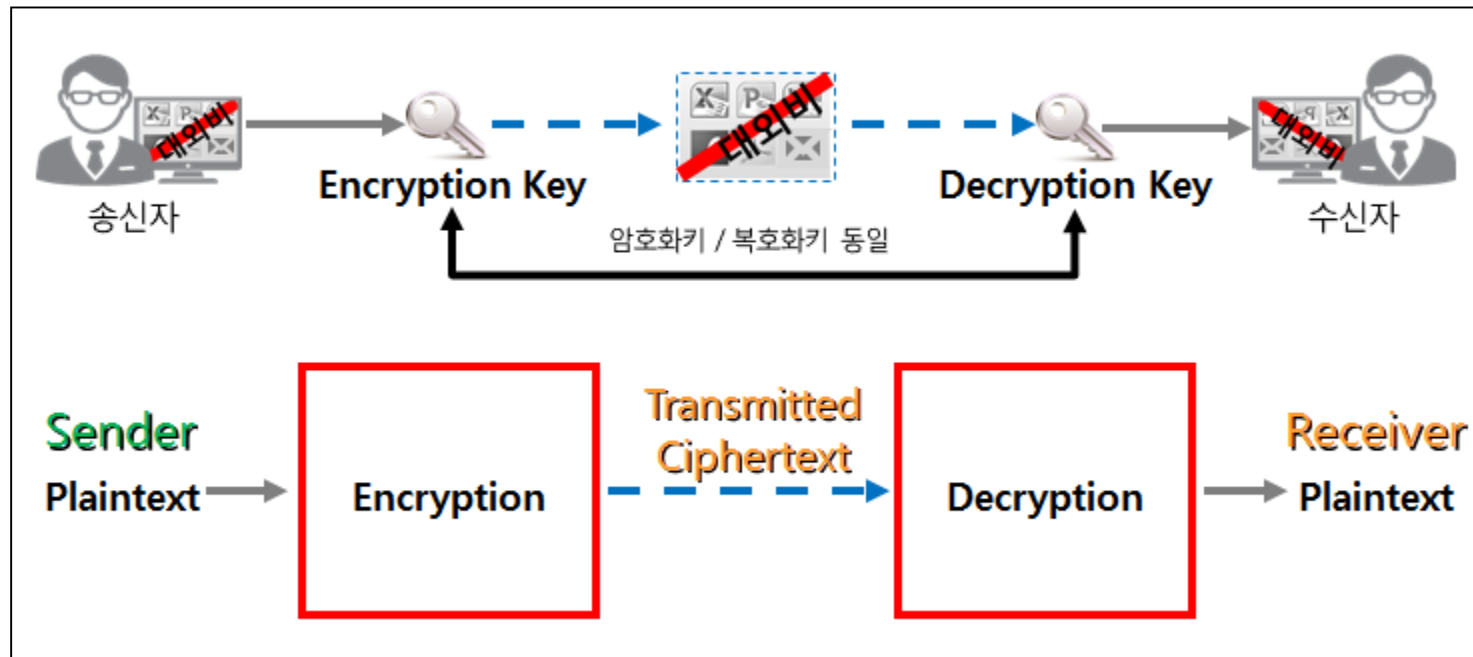
- 사용자가 네트워크를 통해 전송하는 데이터는 누구나 훔쳐볼 수 있기 때문에 안전하지 못한 통신을 하게 되는데 이런 문제점을 해결 하기 위해 만들어진 것이 암호화 이다.
- 암호화 시스템은 암호화 (Encryption) Key라는 비밀 값을 복잡한 알고리즘과 함께 사용 하여 평문 문서(Plain text)를 아무나 읽을 수 없도록 암호화한 것을 암호문(Cipher text) 이라고 한다.



2.1 암호화 기법

- 비밀키 암호화 (Secret Key Encryption) 특징

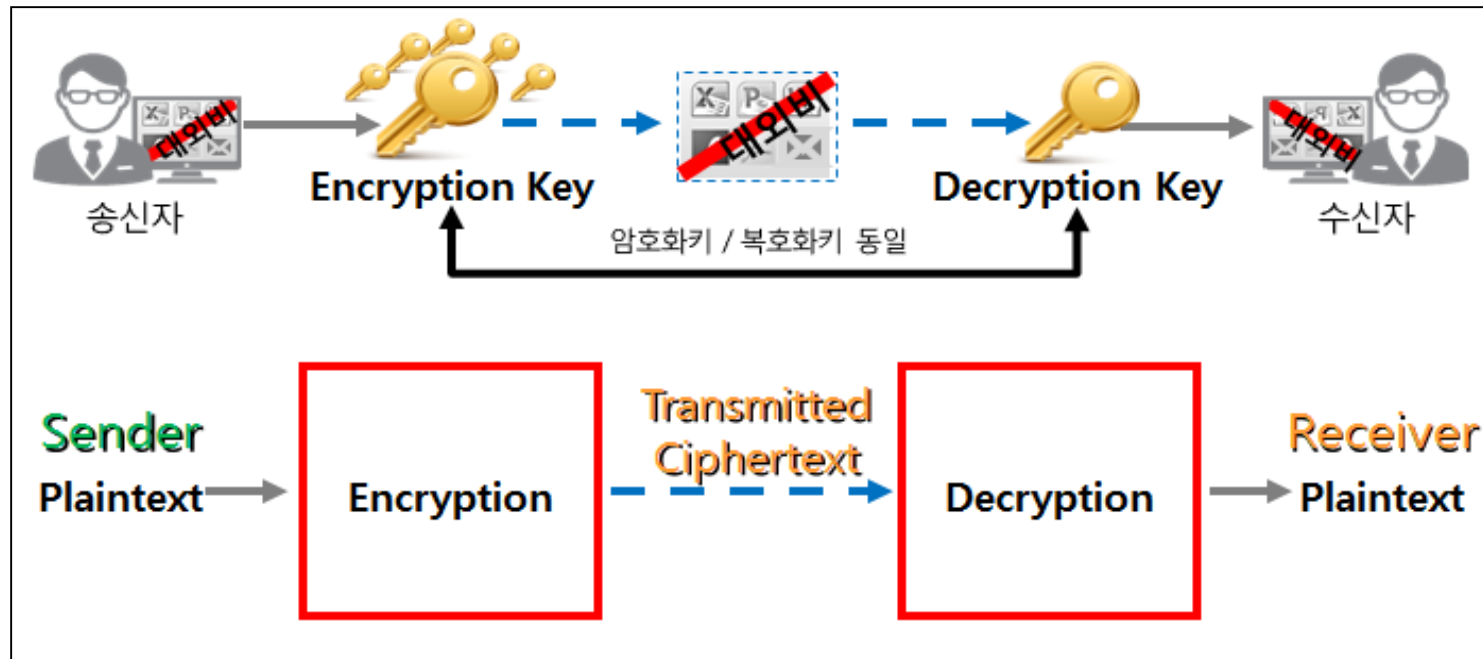
- 비밀키 암호화 방식(Secret-Key Algorithm, Symmetric Algorithm)은 암호화 키와 복호화 키가 동일하므로 두 개체가 같은 키를 공유하면서 하나의 키를 사용하여 암호화 하고 복호화 한다.
- 암호화 키에서 복호화 키를 계산하거나 복호화 키에서 암호화 키를 계산 할 수 있을 때 비밀키 암호화 방식 이라고 한다.
- 장점 : 암호화 / 복호화 속도가 빠름 , 단점 : 키의 공유 문제 발생 시 안전한 키 전달이 어려움



2.1 암호화 기법

• 공개키 암호화 (Public Key Encryption) 특징

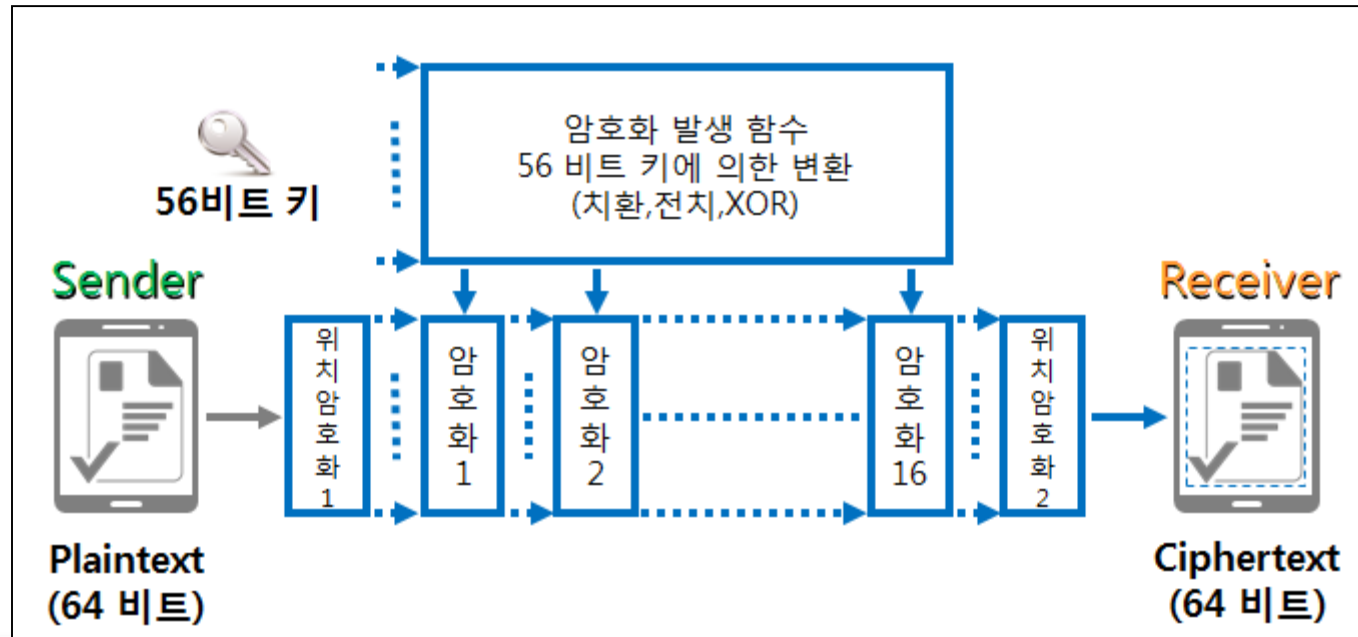
- 공개키 암호화 방식(Public-Key Algorithm, Asymmetric Algorithm)은 암호화 키와 복호화 키가 서로 다르다.
- 공개키는 누구나 원하는 내용을 암호화 할 수 있지만 개인키 Private Key를 소유 해야 암호문을 복호화 할 수 있다.
- 송신자는 여러 공개키 중 수신자의 공개키로 암호화 하여 수신자에 전송 하고 수신자는 비밀키 (개인키로) 암호문을 복호화 한다.
- 장점 : 비밀키 암호화 방식에 비해 안전함 , 단점 : 많은 양의 자료 암/복호화가 시 느리고 불편함



2.2 암호화 알고리즘

- 대표적 대칭 알고리즘 (DES)

- DES (Data Encryption Standard) 1974년 미국 NBS 요청으로 IBM에서 루시퍼 암호 알고리즘을 제안 했고 이를 수정하여 1975년 DES를 발표 1977년 미국 NIST에 의해 표준으로 채택 되었다.
- 평문(Plain Text) 64 bits를 암호문(Cipher Text) 64 bits로 변환시키는 Block 암호 방식 이다.
- Key length = 56 bits
- DES는 16 round로 구성되며 각각의 round는 secret key로 암호화를 수행함 한다.



2.2 암호화 알고리즘

• 대표적 대칭 알고리즘 (3DES)

- 3DES (Triple Data Encryption Standard)는 1998년 EFF 에서 56시간 안에 암호 해독(무차별 대입 공격 하드웨어 개발) 성공 하였다. 이 후 1999년 22시간 안에 암호 해독 성공으로 문제점을 보완하기 위해 DES를 3번 적용하는 암호화 알고리즘 개발 하였다.
- DES Key1, Key2, Key3를 사용하여 암호화 & 복호화 암호화 단계를 거쳐 동작 한다. 이로 인하여 DES에 비해 3배 이상 느리다.
- 복호화는 암호화의 역순 (K3, K2, K1 단계)
- Total Key length = 56 bits * 3 = 168 bits

• 대표적 대칭 알고리즘 (AES)

- AES (Advanced Encryption Standard) 데이터 암호화 표준(DES)의 차세대 국제 표준 암호로 대체하는 순서 공개형의 대칭 키 암호 방식이다.
- 128 bits 에서는 10라운드 , 192 bits에서는 12라운드, 256 bits에서는 14라운드를 실시하여 암호문을 만든다.
- Key length = 128 / 192 / 256 bits 가변적 키 크기를 선택 사용

• 대표적 대칭 알고리즘 (SEED)

- 한국인터넷진흥원(KISA)에서 개발, 2007년 국제 표준화 기구 IETF 에서 국제 표준으로 제정 되었다.
- SEED는 인터넷전화용 보안기술로 인터넷전화 사용자간 통화내용의 도청 등을 방지하기 위해 개발 되었으며 이후 인터넷 보안 (전자우편, 인터넷 통신기술(TLS, IPsec)에 SEED 적용 하였다.
- Key length = 128 / 256 bits 키 크기를 선택 사용, 128 bits 에서는 16라운드를 실시하여 암호문을 만든다.

2.2 암호화 알고리즘

- 대표적 비대칭 알고리즘 (RSA)

- RSA(Rivest Shamir Adelman) 1977년 MIT 대학의 론 리베스트(Ron Rivest), 아디 셔미르(Adi Shamir), 레오나드로 아델만 (Leonard Adelman) 3명의 수학자에 의해 개발 되었다.
- 국제 표준화 기구(ISO), ITU-ANSI.IEEE 등 여러 국제 기구에서 암호화 표준으로 제안 사용 중 이다.
- 장점 : 동작원리가 매우 복잡한 방식으로 슈퍼 컴퓨터로 1만년 이상의 해독 시간이 소요 필요 (매우 강력함) 하다.
- 단점 : 복잡한 방식(인수분해가 필요)으로 암호화 / 복호화 가 대칭 알고리즘에 비해 느리다.
- 이외 ECC(Elliptic Curve Cryptography) 알고리즘, DSA(Digital Signature Algorithm) 등이 있다.
- Key length = 512 / 1024 / 2048 bits

2.3 인증 알고리즘

- 인증 (Authentication)이란 무엇인가?

- 정보의 교류 속에서 전송 받은 정보의 내용이 변조되지 않았는지 송신자와 수신자가간 확인하는 방법이다.

- 인증 방식의 일반적인 개념

- Hash 알고리즘을 이용 하여 평문 메시지 m 에 대하여 임의의 알고리즘 G 를 사용해 암호화 한다.
- 암호문을 안전성이 보장되지 않는 통신로를 통해 수신자에게 전송한다.
- 수신자는 인증 알고리즘 V 를 이용해 복호화 평문 m' 을 얻고 수신자는 $m=m'$ 인지를 확인함으로써 메시지 인증을 수행한다.
- 송신자가 정확히 자신과 통신하는 사람인지를 확인하여 사용자 인증을 수행한다.

2.3 인증 알고리즘

- 대표적 대칭 Hash 알고리즘 (MD5)

- MD5(Message-Digest Algorithm 5) 1991년 로널드 라이베스트가 MD4를 대체 하기 위해 고안 하였다.
- 임의의 메시지를 입력으로 받아 128비트의 고정된 출력을 제공한다.
- 입력은 512비트 블록단위로 처리한다.

- 대표적 대칭 Hash 알고리즘 (SHA-1)

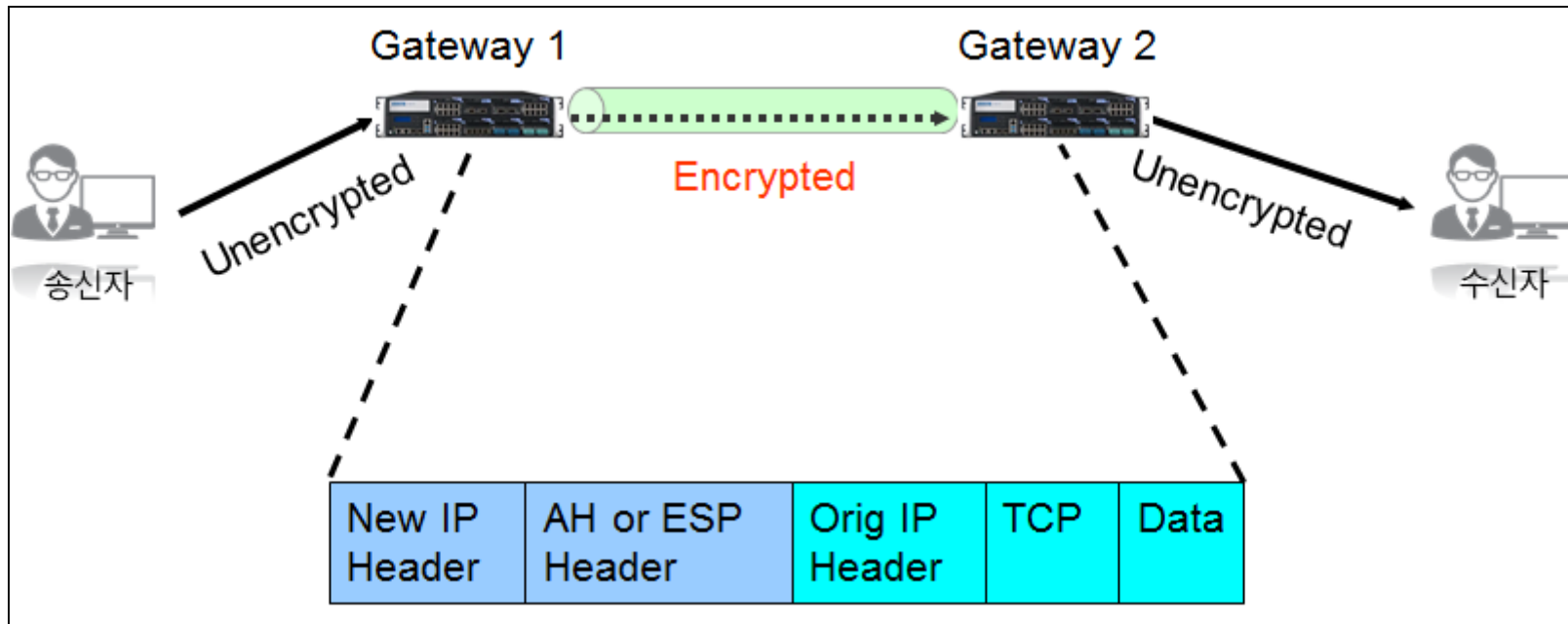
- SHA-1 (Secure Hash Algorithm) 미국 국가안보구(NSA)가 1993년 SHA로 처음 설계 후 1995년 SHA-1(SHA-1) 발표 했다.
- 이후 SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) 등을 발표 후 2002년 표준화 되었다.
- MD4 알고리즘에 기반을 둔 미국 표준 FIPS PUB 180으로 선정된 알고리즘 이다.
- TLS, SSL, PGP, SSH, Ipsec 등 많은 보안 프로토콜과 프로그램에서 사용 한다.
- 입력 메시지는 512 bits 블록으로 처리하고 출력은 160 bits를 생성 한다.

구분	MD5	SHA-1
처리 기본 단위(블록 크기)	512 비트	512 비트
해시 값	128 비트	160 비트
최대 입력 워드 크기	무한대	32
단계 수	64 단계	80 단계
사용되는 비선형 함수 개수	4	3
덧셈 상수 개수	64	4

3.1 IPSec 개요

- IPSec (Internet Protocol Security) 이란?

- Internet Protocol Security은 네트워크 계층(IP 계층)에서 양 종단 간 IP 통신 보안(보호)을 위해 표준 프로토콜로서 인증과 암호화, 키 관리 등을 제공하는 프로토콜 이다.
- 보안을 위해 AH(Authentication Header), ESP(Encapsulating Security Payload), SA (Security Association) 를 이용한다.



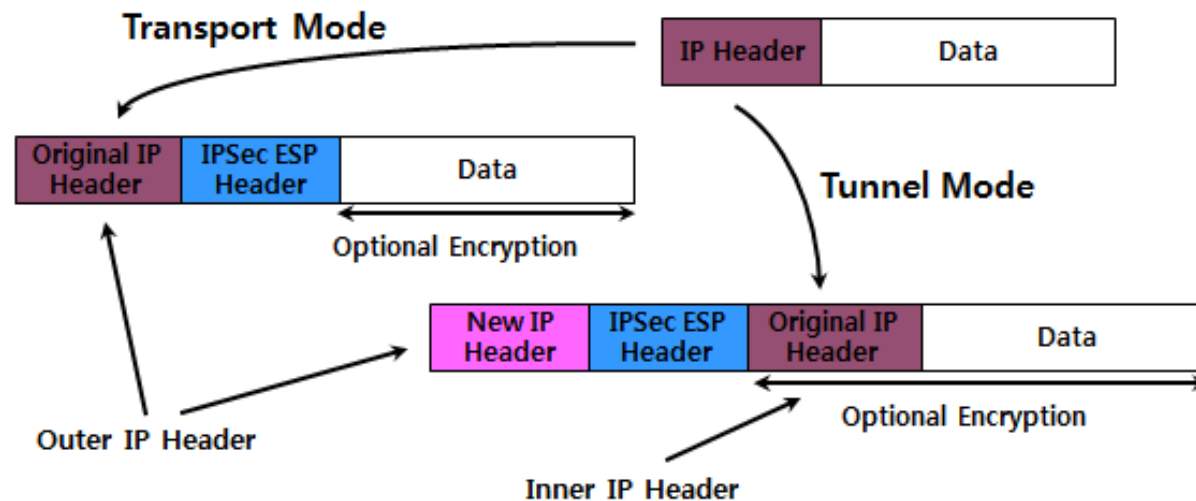
3.1 IPSec 개요

- IPSec 표준 (AH / ESP)

- AH(Authentication Header)는 IP extension Header로서 IP packet에 대한 인증 여부만 제공한다.
ESP와는 달리 AH는 전체 IP 패킷에 대한 인증여부를 결정하며 암호화는 하지 않고 인증만 한다.
- ESP(Encapsulating Security Payload) IP 데이터그램에 인증 및 암호화를 제공하고 전송 모드와 터널 모드에서 적용 가능

- IPSec 모드 (Tunnel / Transport)

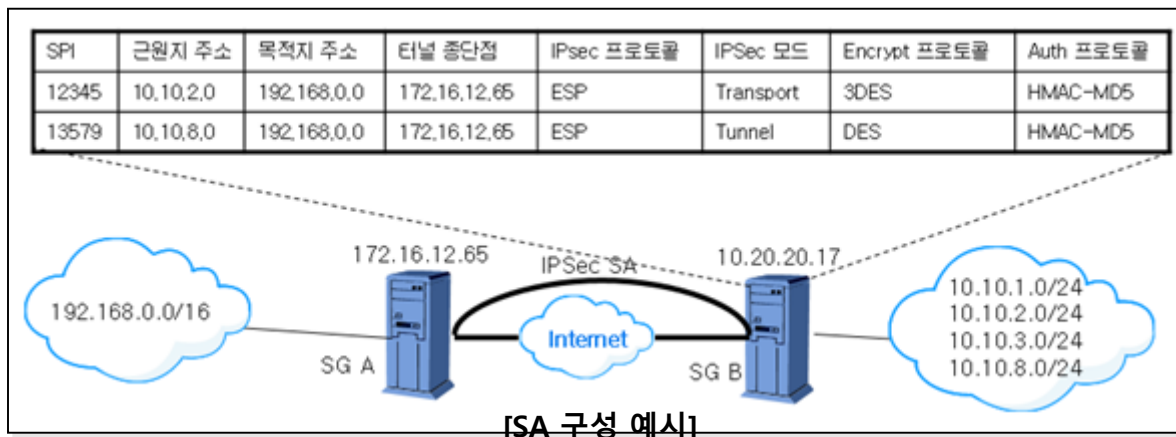
- Tunnel Mode 는 IPsec 처리가 Host/Gateway 또는 Gateway/Gateway로 이루어 짐.
- Transport Mode 는 IPsec 처리가 Host/Host로 이루어 짐.



3.1 IPSec 개요

• IPSec 표준 (SA)

- SA(Security Association) Traffic에 보안 서비스를 제공할 수 있는 단방향 Connection 정보(RFC2401)를 말한다. 양 단간의 사용자(혹은 게이트 웨이)가 secure한 통신을 하기 위해서 필수적으로 공유하고 있어야 하는 정보로서 양단은 같은 암호화 알고리즘과 키를 공유하고 있어야 한다.
- SA 특징은 다음과 같다.
 - IKE에 의해 설정 및 유지한다.
 - 프로토콜, 운용모드, 암호알고리즘, 암호 키, 키 수명 등에 대한 합의 필요하다.
 - 일방향성, 출발 트래픽과 도착 트래픽을 위해 별도의 SA 가 필요하다.
 - SA의 식별 : SPI(Security Parameter Index), Dst 주소, 프로토콜



3.1 IPSec 개요

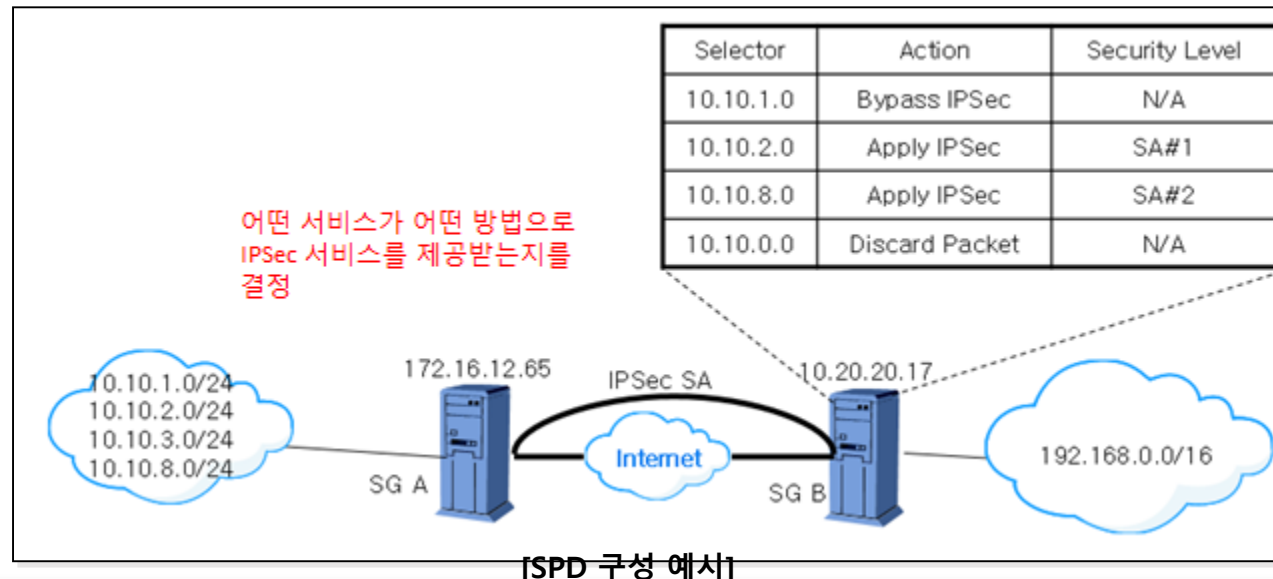
- IPSec 표준 (SAD)

- SAD(Security Association Database) 즉 SA에 대한 데이터 베이스를 뜻한다.
- SAD 특징은 다음과 같다.
 - 암호화 통신에 대한 특성 정의
 - 어떤 전송모드에서 어떤 프로토콜을 사용할 지 정의
 - IP packet 을 다루는 방법을 정의

3.1 IPSec 개요

• IPSec 표준 (SPD)

- SPD(Security Policy Database)는 호스트 또는 게이트 웨이로 부터의 모든 inbound, outbound 트래픽에 대한 정책(policy)을 담고 있는 데이터베이스를 말한다.
- SPD 특징은 다음과 같다.
 - IPsec engine은 패킷을 discard 할 것인지, bypass Ipsec 할 것인지 또는 applying IPsec 할 것인지를 결정한다.
 - 출발지 IP 주소, 목적지 IP 주소로 식별 모든 트래픽을 하나의 SA가 적용 가능하고, 설정에 따라 여러 개의 다른 SA로 적용 할 수 있다.



3.1 IPSec 개요

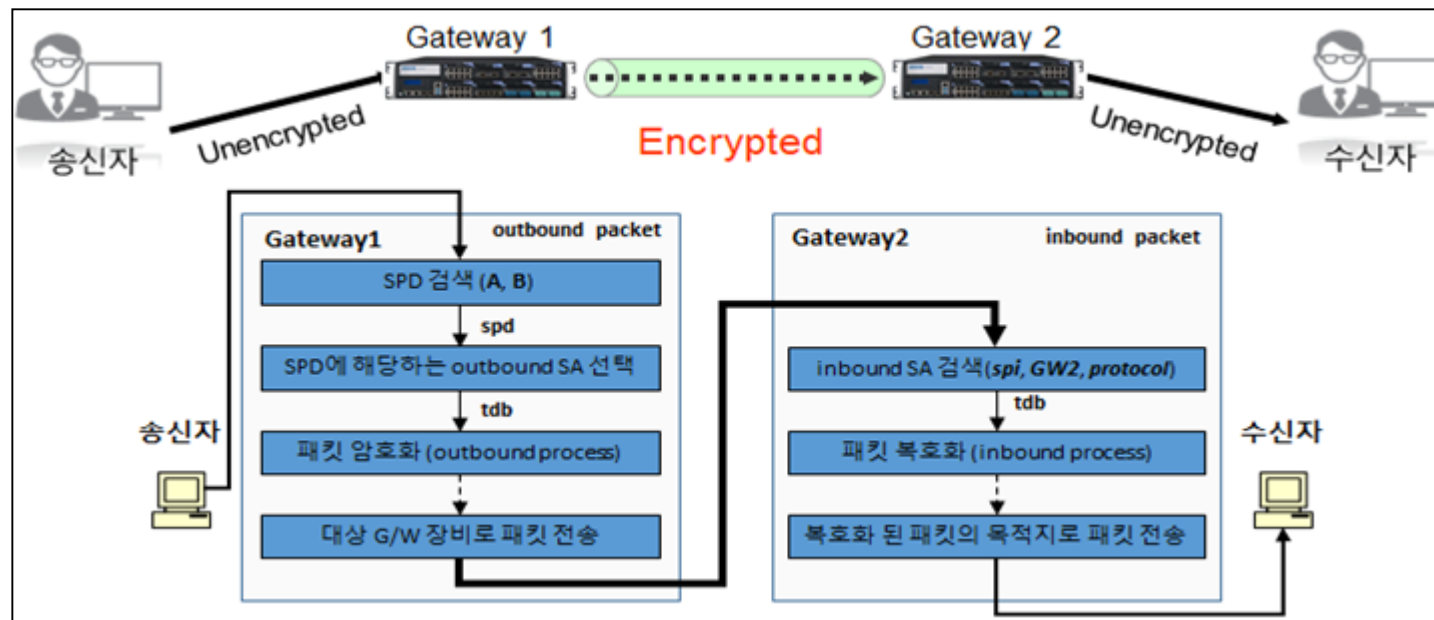
• IPSec 패킷의 흐름

■ Outbound 패킷의 흐름

- SPD로부터 패킷의 출발지/목적지에 해당하는 outbound SA를 선택
- 해당 SA를 사용해 패킷을 암호화
- 암호화 된 패킷을 peer G/W장비로 전송

■ Inbound 패킷의 흐름

- 수신된 암호 패킷의 SPI, Dst 주소,
프로토콜(ESP/AH)에 해당하는 inbound SA를 선택
- 해당 SA를 사용해 패킷을 복호화
- 복호화 된 패킷을 라우팅을 태워 목적지로 전송



3.2 IKE 개요

- IKE(Internet Key Exchange) 이란?

- IKE (Internet Key Exchange)는 IPSec VPN 에서 키 교환 및 터널에 대한 정책을 협상하기 위해 사용되는 인터넷 표준 암호 키 교환 프로토콜로서 RFC 2409에 규정 되어 있다.
- 키 교환 방식
 - Manual Keying (SA를 정의하는 데 요구되는 모든 정보를 수동으로 구성)
 - Dynamic Keying (SA를 정의하는 데 필요한 정보를 자동으로 구성, IKE 프로토콜에서 지원)
- IKE (Internet Key Exchange) 특징은 다음과 같다.
 - 상호 간 인증, 키 관리 및 배포, 터널링 등을 자동으로 관리 한다.
 - IPsec 세션 키는 새로운 IKE 협상 단계를 통해서 갱신될 수 있다.
 - Dynamic Keying 으로 협상된 세션 키와 SA를 IPsec에 전송하는 역할을 한다.
 - 버전은 IKEv1 / IKEv2 이 있다.

3.3 IKE 버전 별 차이점

- IKEv1 vs IKEv2 차이점

- IKEv1

- IKEv1는 서로 다른 프로토콜(ISAKMP, Oakley, SKEME) 들을 혼합한 프로토콜로 복잡성이 높고, 확장성 및 속도, 효율성, 안정성에 문제가 있다.
- 키 교환 및 인증을 위한 프레임워크, 메시지 포맷 및 페이지(phase) 개념은 ISAKMP에서 가져왔으며, Oakley 프로토콜로부터 2가지 키 교환 모드를 가져왔다.
- IKEv1은 키 교환을 위해 3가지 모드(Main Mode, Aggressive Mode, Quick Mode)를 사용

- IKEv2

- IKEv1 보다 심플하고 보안성 및 성능이 높도록 설계되었다.
- IKEv1 과 기본적인 개념은 비슷하지만 복잡했던 페이지 및 모드 개념 삭제함.
- IPSec SA를 생성 절차가 간소화(교환하는 메시지의 수를 줄여서)되어 빠르고 효율적으로 IPSec SA를 생성할 수 있다.
- 빠르고 효율적으로 IPSec SA를 생성하는 것이 가능하기 때문에, 부가적인 기능(EAP 인증, MOBIKE 등)들도 지원

3.4 IKE 동작 방식

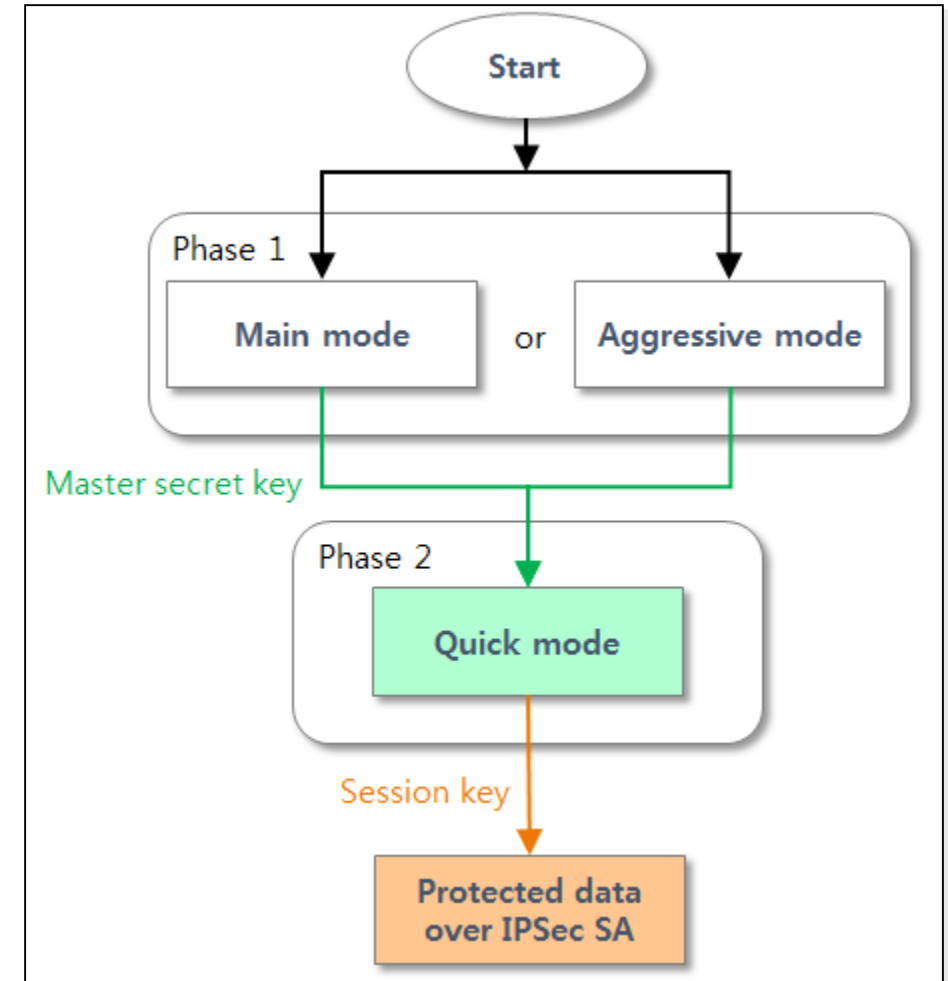
• IKEv1 동작 방식

■ Phase 1

- Phase2 협상을 보호하기 위한 SA 생성
- Main Mode 와 Aggressive Mode 중 선택

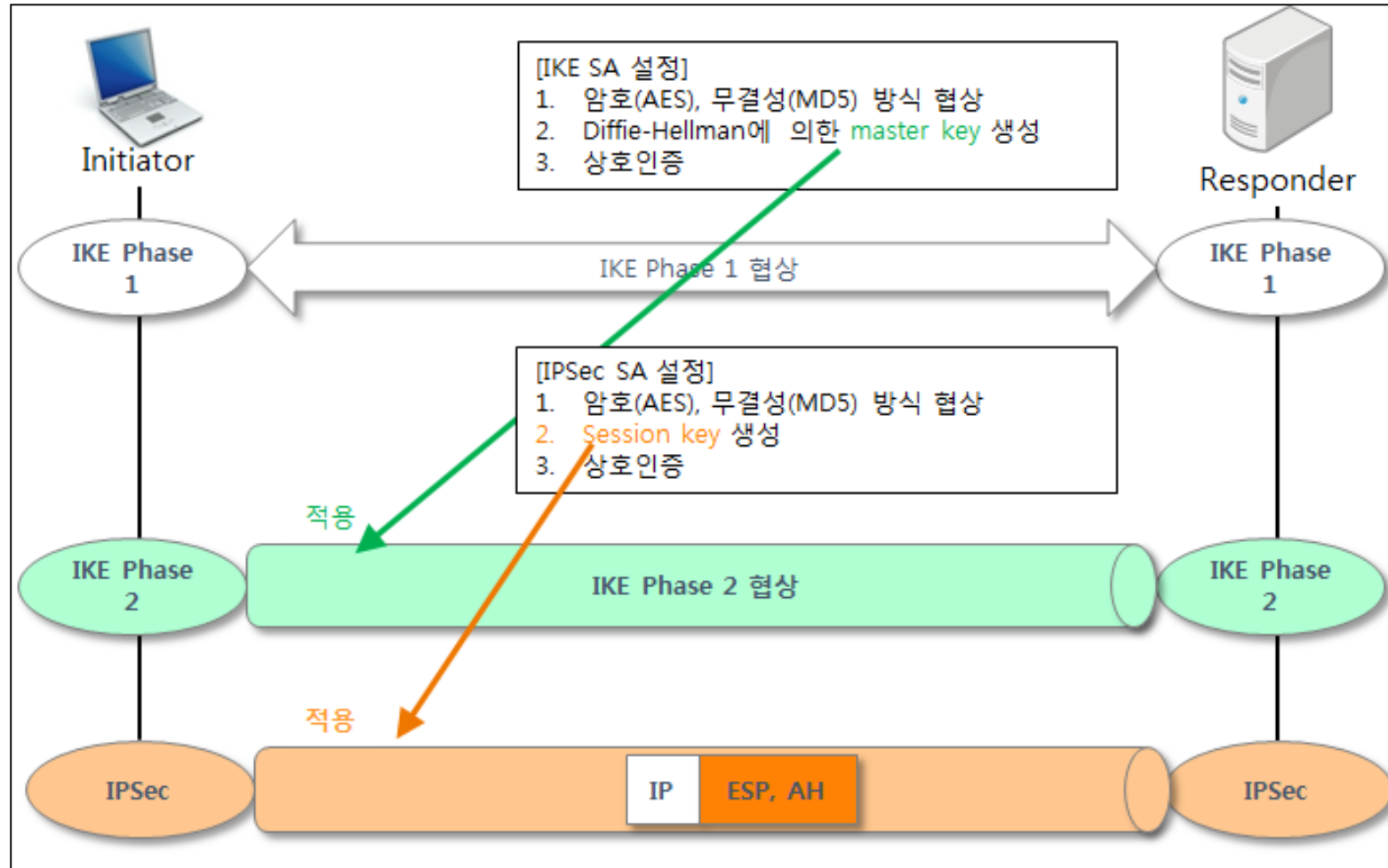
■ Phase 2

- IPSec 서비스를 위한 SA 생성
- 1 단계에서 생성된 SA를 기반으로 실제 통신에서 사용할 SA와 Key를 생성하는 과정 Quick Mode와 New Group Mode로 구분



3.4 IKE 동작 방식

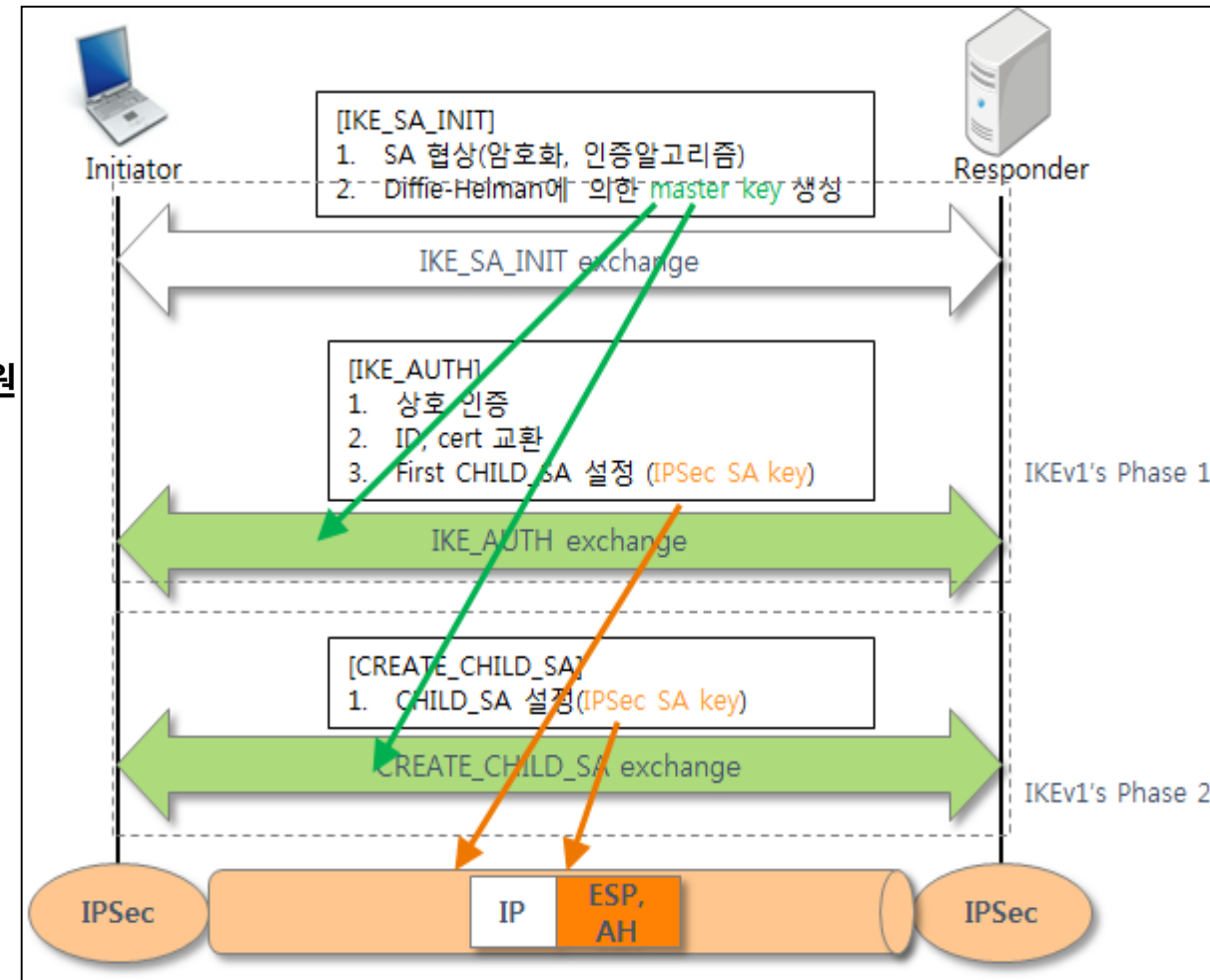
• IKEv1 동작 방식



3.4 IKE 동작 방식

• IKEv2 동작 방식

- IKEv2는 IKEv1에서 사용했던 페이지 개념 및 모드 개념을 없애고 IKE SA 및 CHILD SA (=IPSec SA)를 생성하기 위해 Initial Exchange(IKE_SA_INIT Exchange, IKE_AUTH Exchange)를 수행
- CREATE_CHILD_SA Exchange를 통해 새로운 CHILD SA를 생성하거나 rekeying을 수행
- 부가적인 정보(예> SA 삭제) 교환을 위해 INFORMATIONAL Exchange를 지원
- 모든 Exchange는 request 메시지와 response 메시지의 쌍으로 되어 있음 즉 두 개의 메시지가 교환

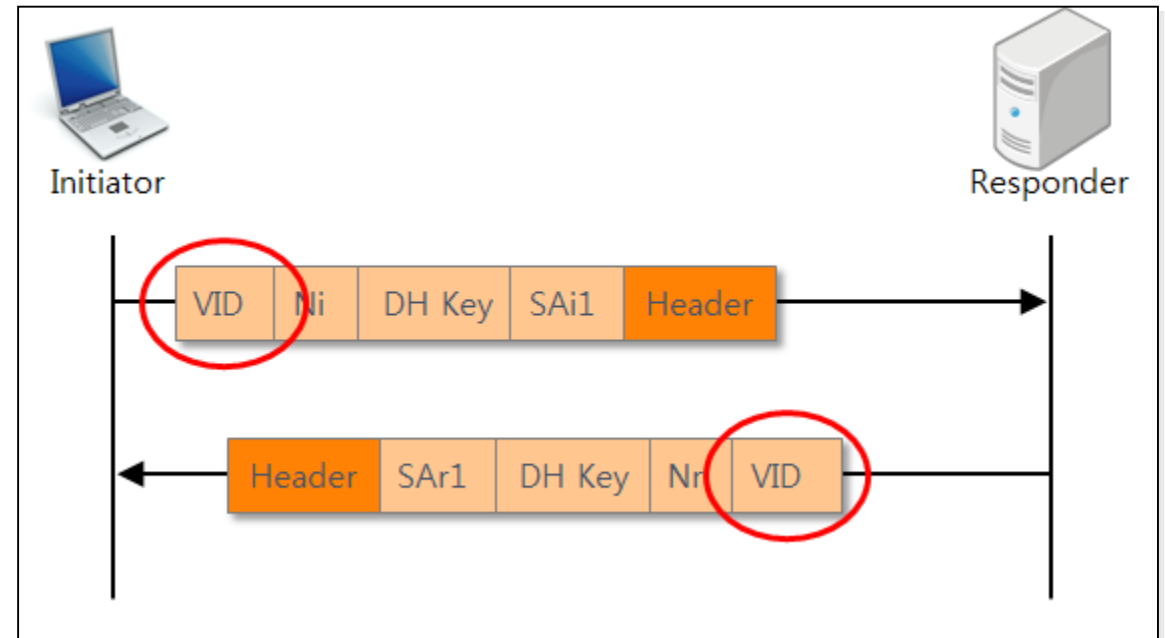


3.4 IKE 동작 방식

- SECUI 확장 (vendor ID 교환)

- SECUI 확장 (vendor ID 교환)

- 키 교환 과정을 시작할 때 대상 장비가 **SECUI 제품인지 확인**하기 위해 다음과 같이 Vendor ID를 교환
- IKEv1의 경우 Phase1 키 교환 단계에서 수행
- IKEv2의 경우 IKE_SA_INIT exchange 단계에서 수행



3.4 IKE 동작 방식

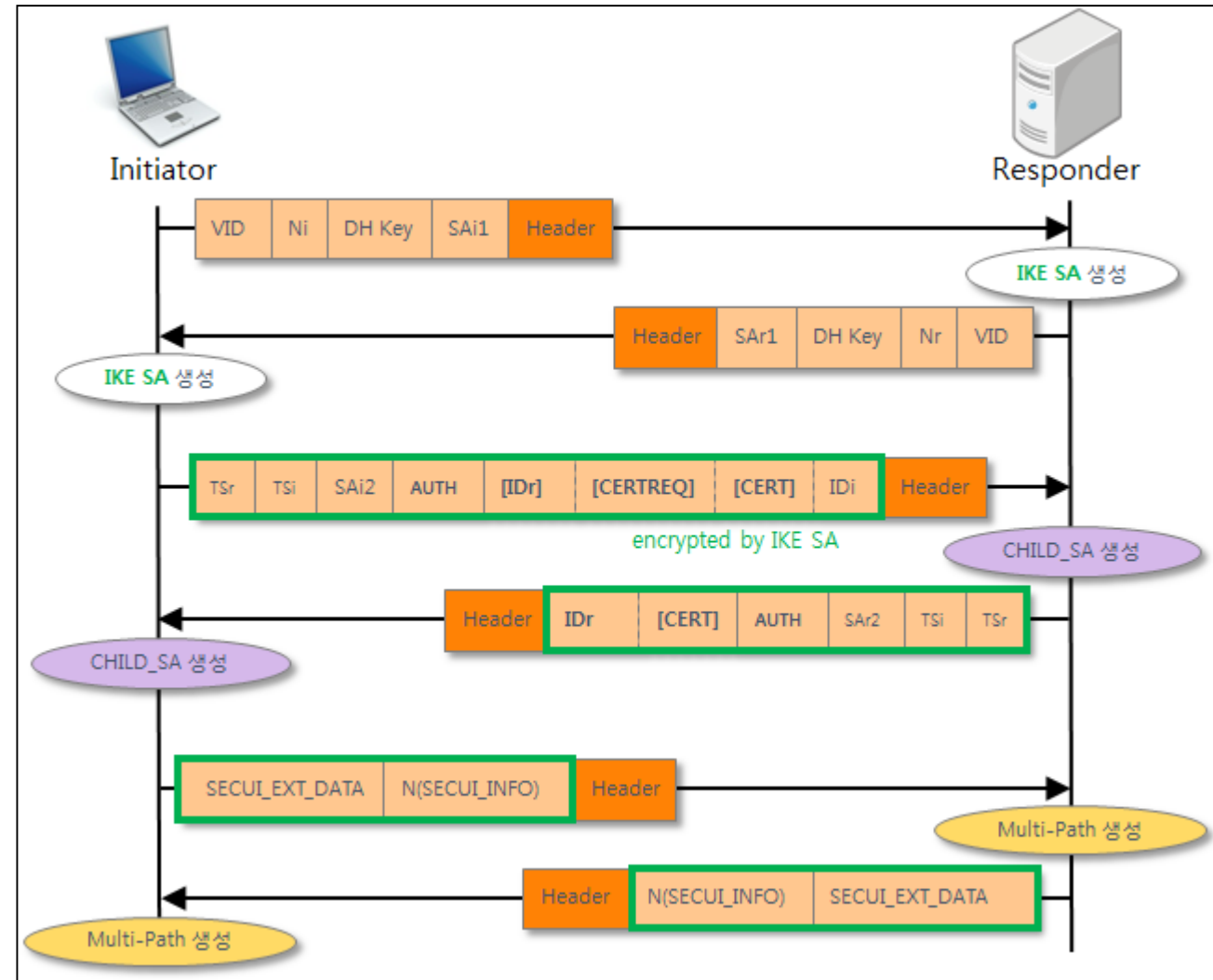
• SECUI 확장 (INFO exchange)

▪ SECUI 확장 (INFO exchange)

- INFORMATIONAL exchange 과정을 확장해 SECUI 벤더 속성을 교환
- SECUI_INFO notify 타입을 추가

▪ SECUI 벤더 속성에는 다음 내용이 포함되어 있다.

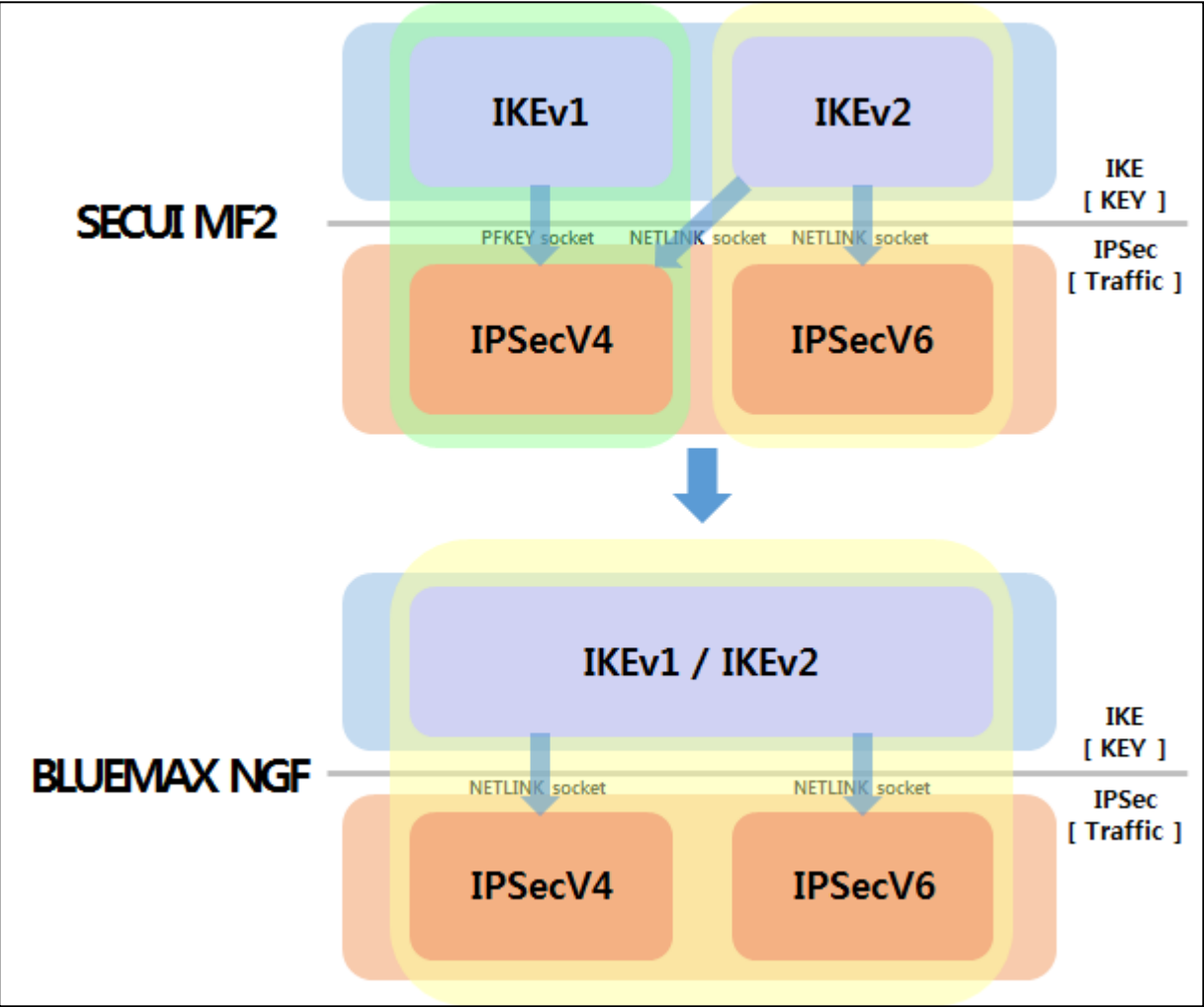
- 센터 장비의 회선 정보 (회선 이름, 회선의 IP 주소)
- 지점의 선택된 회선 정보 (회선 이름, Active/Standby)
- 회선 경로간 분배 방식 (Session/Round-robin)
- 장비 역할 (센터/지점)
- 터널 우선순위 (Active/Standby, 우선 순위 값)
- IKEv1 의 경우 설정된 네트워크 정책 목록



4.1 BLUEMAX NGF IPSec VPN 특징

- IKEv1 & IKEv2 데몬 통합
 - 통합 내용은 다음과 같다.
 - IKEv1/IKEv2 데몬을 기반
 - 터널링 성능 및 타사 VPN 호환성 향상
 - IKEv1 IPv6 지원 추가 되었다.
 - IKEv1+IKEv2 데몬 통합으로 인한 NXG/SNXG 호환 이슈

대상 제품	연동성
NXG / SNXG	VPN 연동 불가
MF2	IKEv2 사용 시 VPN 연동 가능



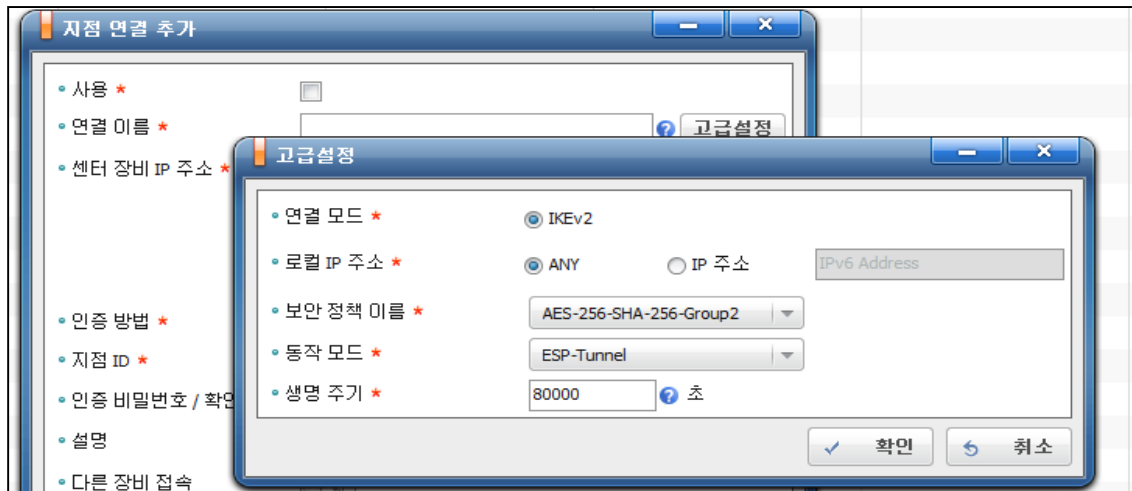
4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

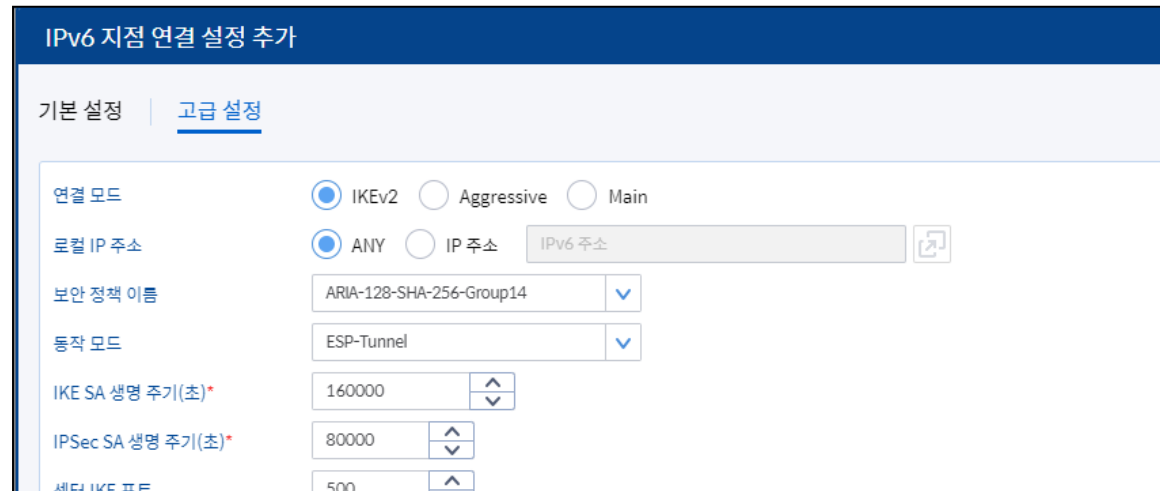
- IKEv1 사용 시 IPv6 지원 가능

- BLUEMAX NGF IKEv1 사용 시 IPv6 지원한다.

- MF2에서는 IPv6 사용 시 **IKEv2 연결만 지원**
- IPv6 지점 연결 설정 > 고급 설정에 IKEv1 연결 옵션 지원 추가 (IKEv2 / Aggressive Mode / Main Mode 선택 사용 가능)



[MF2 IPv6 지점연결 설정 화면]



[NGF IPv6 지점연결 설정 화면]

4.1 BLUEMAX NGF IPSec VPN 특징

- UDP Encapsulation 강제 적용 옵션 제공

- 중국 방화벽 우회 가능 한 UDP Encapsulation 강제 적용 옵션 제공

- 암호화 된 ESP 패킷을 UDP 헤더로 래핑
- 중국 방화벽 정책 변경에 유연하게 대응할 수 있도록 UDP 포트를 변경 할 수 있는 기능 제공

※ (참고) 황금 방패 (만리 방화벽, Great Firewall 등) - wiki

지점 연결 설정 편집

기본 설정 | 고급 설정

연결 모드: ☒ IKEv2 ☐ Aggressive ☐ Main

로컬 IP 주소: ☒ ANY ☐ IP 주소 [] . [] . [] . []

보안 정책 이름: ARIA-128-SHA-256-Group14

동작 모드: ESP-Tunnel

IKE SA 생명 주기(초)*: 160000

IPSec SA 생명 주기(초)*: 300

센터 IKE 포트: 500

UDP Encapsulation 강제 적용*: ☒ ON ☐ OFF

표준 IPSec: ☐ ON ☒ OFF

UDP encapsulation 강제 적용

[NGF 지점연결 설정 > 고급설정 화면]

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

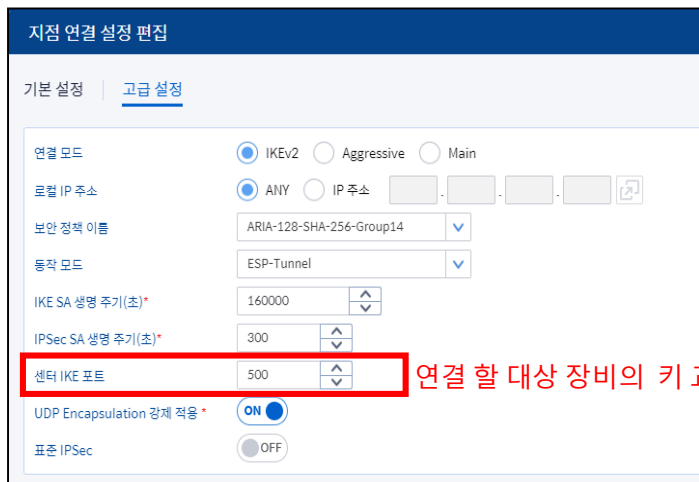
• IKE 포트 변경 기능 개선

■ 키 교환 포트 및 NAT-T (NAT Traversal) 포트 변경 기능 개선

- 기존 MF2 제품에서는 센터/지점 장비가 동일한 키 교환 포트를 사용해야 했음
- 일반 설정에서 키 교환 포트, NAT-T 포트를 지정 할 수 있도록 개선

■ 센터/지점 장비가 서로 다른 키 교환 포트를 지정해서 사용 할 수 있도록 기능 개선

- 일반 설정에서 자신이 LISTEN 할 키 교환 포트, NAT-T를 지정 가능
- 지점연결설정에서 자신이 연결 할 대상 장비의 키 교환 포트를 지정



지점 연결 설정 편집

기본 설정 | 고급 설정

연결 모드: ☒ IKEv2 ☐ Aggressive ☐ Main

로컬 IP 주소: ☒ ANY ☐ IP 주소

보안 정책 이름: ARIA-128-SHA-256-Group14

동작 모드: ESP-Tunnel

IKE SA 생명 주기(초): 160000

IPSec SA 생명 주기(초): 300

센터 IKE 포트: 500

UDP Encapsulation 강제 적용: ☒ ON ☐ OFF

표준 IPSec: ☐ ON ☒ OFF

[NGF 지점연결 설정 > 고급설정 화면]



가상 사설망 일반 설정

최대 재전송 횟수: 4

SA 점검 간격 시간(초): 60

재전송 시간 간격 증가값(초): 10

초기 재전송 타임아웃(초): 7

키교환 포트: 500

NAT-T 포트: 4500

IKEv2 DoS 공격 방어: ☐ ON ☒ OFF

[NGF IPSec VPN 일반 설정 화면]

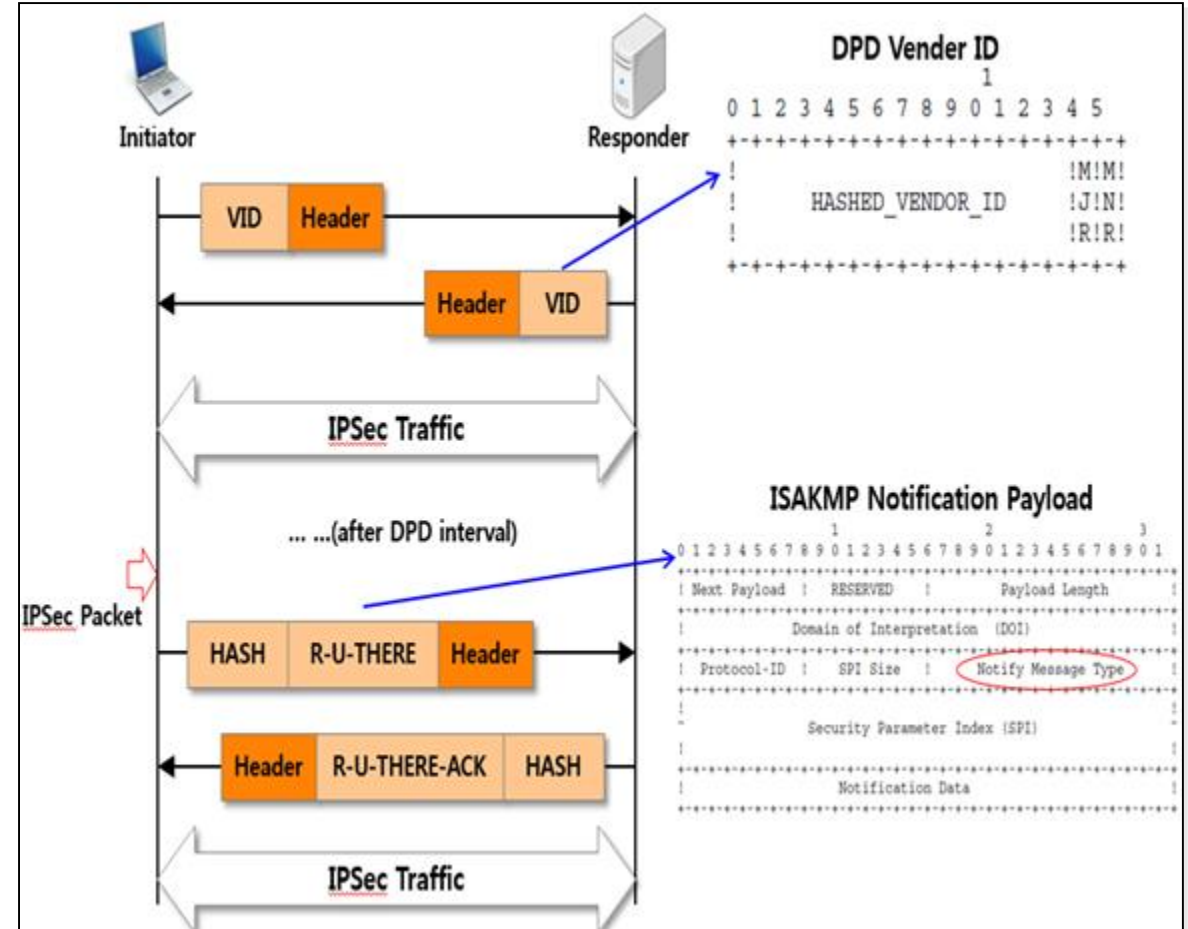
자신이 LISTEN 할 키 교환 포트를 지정

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

• 회선 장애 감지 동작 방식 개선 (DPD 지원 개선)

- 타사 제품 연동 시 DPD (Dead Peer Detection) 지원 개선
 - 기존에는 자체 회선 장애 감지 기능인 DLD (Dead Link Detection) 사용으로 인해 표준 방식인 DPD는 부분적으로만 지원 (MF2 : R-U-THERE 요청에 대한 응답만 제공)
 - 타사 벤더 제품과 연동 시 DPD를 기본으로 사용 하도록 지원



4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

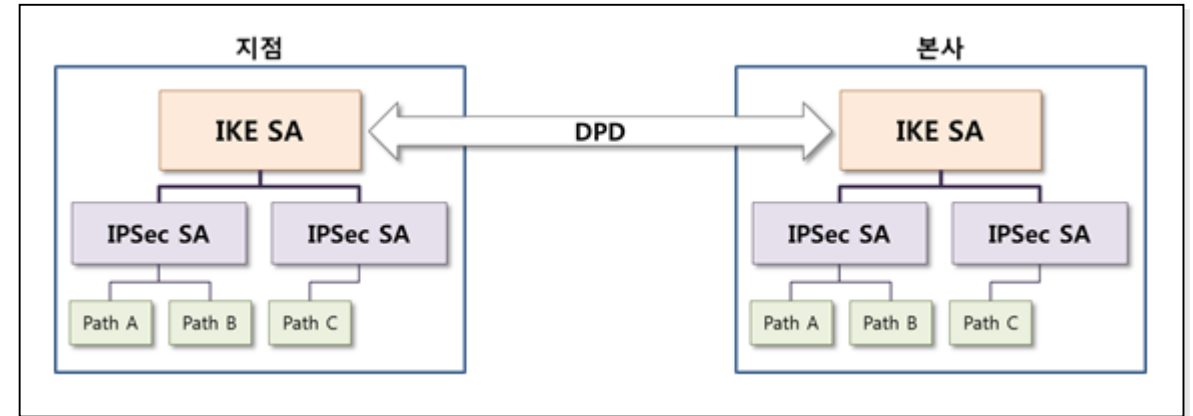
• DPD 와 DLD 차이점

■ DPD (Dead Peer Detection)

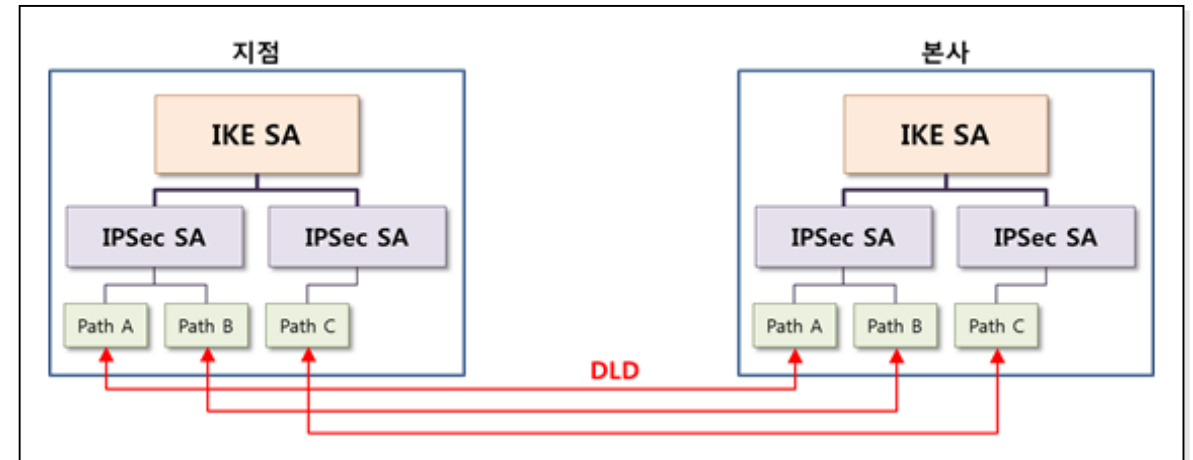
- 표준적인 터널 장애 검사 방식
- IKE 간에 R-U-THERE / R-U-THERE-ACK 메시지를 교환 하여 장애 상황을 검출
- IKE SA에 대한 연결성만 검사 (다중 회선 환경에 적합하지 않음)

■ DLD (Dead Link Detection)

- SECUI 제품 간 터널 장애 검사 방식
- IPSec에서 DLD request/reply 메시지를 생성
- 각 회선 경로 별로 DLD 검사를 수행 (다중 회선 환경에 적합)



[DPD를 이용한 터널 상태 검사]



[DLD를 이용한 터널 상태 검사]

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

• 보안정책 고급설정 분리

- Phase1, Phase2 보안정책 설정 방식 개선
 - MF2 에서는 설정을 단순화 하기 위해 Phase1, Phase2 설정을 동일하게 설정하였다.
(MF2에서는 Phase1, Phase2 보안정책이 분리되어 있었지만 CLI를 통해서 Phase1, Phase2 보안정책을 다르게 설정해야 했다.)
- BLUEMAX NGF 에서는 고객 요구사항을 만족하기 위해 Phase1, Phase2 설정을 각각 다르게 설정 할 수 있도록 고급설정 화면을 추가 하였다.

Phase1, Phase2 정책을 다르게 설정하기 위해서는 OFF로 선택

※ ON으로 선택한 경우 MF2와 동일하게 동작

Phase1
보안정책 설정

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

- SA 생명 주기 설정 개선

- IKE SA, IPSec SA 생명 주기 설정을 분리

- MF2에서는 설정을 단순화 하기 위해 IKE SA 생명주기 설정을 숨기고 IPSec SA 생명주기 값의 2배로 자동 설정 되었다.

- BLUEMAX NGF에서는 타사 VPN 장비와 연동성을 높이기 위해 지점등록설정, 지점연결설정에서 IKE SA, IPSec SA 생명주기 값을 각각 설정 할 수 있도록 개선 하였다.

지점 등록 추가

기본 설정 | 고급 설정

연결 모드 * ☒ IKEv2/Aggressive ☐ Main

지점 IP 주소 . . .

IKE SA 생명 주기(초)*

IPSec SA 생명 주기(초)*

보안 연결 동작 방식 * ☐ 우선순위

지점 연결 설정 추가

기본 설정 | 고급 설정

연결 모드 ☒ IKEv2 ☐ Aggressive ☐ Main

로컬 IP 주소 ☒ ANY ☐ IP 주소 . . .

보안 정책 이름

동작 모드

IKE SA 생명 주기(초)*

IPSec SA 생명 주기(초)*

센터 IKE 포트

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

• Main Mode 설정 방식 개선

■ Main Mode 센터 장비 설정 방식 개선

- MF2에서는 Main Mode 사용 시 센터 장비의 경우 IKEv2, Aggressive 연결 모드를 사용할 때와는 달리 지점 연결 설정에서 설정을 편집해야 했음
- 통일성이 없는 단점 개선
- BLUEMAX NGF에서는 Main Mode 센터 장비 설정 시 다른 연결 모드와 마찬가지로 지점 등록 설정에서 설정 편집 할 수 있도록 개선.
- 또한, Main Mode 선택 시 Peer 장비를 장비의 IP 주소로 식별 하기 때문에 **지점 IP 주소 항목을 필수 입력**하도록 개선

지점 등록 편집

기본 설정 | 고급 설정

고급 설정에 '지점 IP 주소' 항목 추가
Main 모드 선택 시 peer 장비를 장비의 IP 주소로 식별하기 때문에
'지점 IP 주소' 항목이 필수항목으로 바뀜

연결 모드 * ☐ IKEv2/Aggressive ☒ Main

지점 IP 주소 * 110 . 1 . 1 . 2

IKE SA 생명 주기(초)* 160000

IPSec SA 생명 주기(초)* 80000

보안 연결 동작 방식 * Active ☐ 우선순위 50

회선 선택 Active

회선 LB 방식 * ☒ 세션 ☐ 라운드로빈

4.1 BLUEMAX NGF IPSec VPN 특징

• 내장 VPN 연결 설정 방법 개선

- iPhone, Android 내장 VPN 연결 설정 방법을 개선
 - MF2에서는 iPhone 과 Android 내장 VPN 사용 시 Main Mode 연결 설정 + 원격 사용자 등록을 같이 해야함.
 - BLUEMAX NGF에서는 원격 사용자 등록 설정에서 사용자를 등록하는 것만으로 연결 설정을 완료 할 수 있도록 설정 방법을 개선.
 - 원격 사용자 등록 화면에서 로컬인증(사전 공유키), 원격 인증(XAUTH-PSK)를 선택하고 해당 사용자를 추가하는 것으로 설정 완료 되도록 개선.

원격 사용자 편집

기본 설정 | 고급 설정

사용 * ☒ ON

사용자 ID * ios_user

인증 방법 * 로컬 인증 사전 공유키 원격 인증 XAUTH-PSK

인증 비밀번호 *****

인증 비밀번호 확인 *****

원격 사용자 IP 할당 * ☐ IP Pool ☒ 고정 IP 할당

2 . 2 . 2 . 1

접근 정책 ☒ 내부망 ☐ ANY

호스트 | 네트워크 | 그룹

⊕ 추가 Search 상세 검색

객체 목록

추가할 객체

1.1.1.0_24_IN

직접 입력

취소 확인

[NGF IPSec VPN 원격 사용자 편집 화면]

4. BLUEMAX NGF IPSec VPN 특징

4.1 BLUEMAX NGF IPSec VPN 특징

- IPSec VPN 예외 정책 개선 (설정 방법 및 성능 개선)

SECUI MF2 - IPSec 우회 목록 설정 (IP / 객체)	BLUEMAX NGF – IPSec 우회 목록 (객체화)
IPSec 우회 목록이 IP 주소 기반, 객체 기반 설정 화면이 분리되어 있었음	IPSec 우회 목록을 객체 기반으로 설정하도록 개선
<div></div> <p>[MF2 IPSec VPN 우회 목록 설정 화면]</p>	<div></div> <p>[NGF IPSec VPN 우회 목록 설정 화면]</p>

5.1 BLUEMAX NGF IPSec GUI 메뉴

• IPSec VPN 메뉴 항목 및 화면 비교

▪ MF2 IPSec VPN vs BLUEMAX NGF IPSec VPN 메뉴 항목 및 메뉴 화면 비교

SECUI MF2 - IPSec VPN	BLUEMAX - NGF IPSec VPN
일반 설정	일반 설정
보안 정책 설정	보안 정책 설정
센터 연결 설정	센터 연결 설정
IPv4 정책 > 지점 연결 설정	지점 연결 설정
IPv4 정책 > 지점 등록	지점 등록
IPv4 정책 > 원격 사용자 등록	원격 사용자 등록
IPv4 정책 > 예외 정책 설정 > IPSec 우회 목록	예외 정책 설정 > IPSec 우회 목록
IPv4 정책 > 예외 정책 설정 > 비정상 터널 우회 목록	예외 정책 설정 > 비정상 터널 우회 목록
IPv4 정책 > 예외 정책 설정 > 멀티 캐스트전송 목록	예외 정책 설정 > 멀티 캐스트전송 목록
IPv6 정책 > IPv6 지점 연결 설정	IPv6 지점 연결 설정
IPv6 정책 > IPv6 지점 등록	IPv6 지점 등록
IPv6 정책 > IPv6 원격 사용자 등록	IPv6 원격 사용자 등록
IPv6 정책 > IPv6 예외 정책 설정 > IPv6 IPSec 우회 목록	IPv6 예외 정책 설정 > IPv6 IPSec 우회 목록
IPv6 정책 > IPv6 예외 정책 설정 > IPv6 비정상 터널 우회 목록	IPv6 예외 정책 설정 > IPv6 비정상 터널 우회 목록
IPv6 정책 > IPv6 예외 정책 설정 > IPv6 멀티 캐스트전송 목록	IPv6 예외 정책 설정 > IPv6 멀티 캐스트전송 목록

SECUI MF2 – GUI 메뉴	BLUEMAX NGF – GUI 메뉴

5.2 BLUEMAX NGF IPSec 메뉴 설명

- 지점 연결 설정 (IPv4 / IPv6 동일 단, IPv6 UDP Encapsulation 기능 미 지원)

지점 연결 설정

1. 지점 연결 설정 :

- 지점 장비가 센터에 IPSec 터널 생성을 요청하기 위한 설정이다.
- 지점 장비는 지점 연결 설정만하고 센터 장비에서 지점의 정책을 내려 받아 적용 한다.
- UDP Encapsulation 강제 적용 기능은 IPSec 터널 생성 시 ESP 패킷으로 암호화

※ IPv6 환경에서는 UDP Encapsulation 기능은 지원하지 않음. (Only IPv4 환경)

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 지점 등록 (IPv4 / IPv6 동일)

지점 등록

1. 지점 등록 설정

- 센터 장비에서 터널 연결을 요청하는 지점 장비의 **인증 ID/PW**를 사전에 등록하고, 인증 이후에 배포할 접근 정책을 등록.
- 확장모드는 목적지 기준으로 정책 생성 시 사용.
- 우선 순위(Priority) 설정으로 세밀한 우선 순위 제어가 가능.
- **지점에서 사용하는 회선**의 Active/Standby 선택 후 설정 필요.
- **지점에서 사용할 인터페이스를 설정**하기 위한 기능이며, 설정하지 않는 경우 회선 상태 검사 설정이 된 인터페이스를 active와 세션LB로 설정.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 원격 사용자 등록 (IPv4 / IPv6 동일)

원격 사용자 등록

원격 사용자 추가

기본 설정 | 고급 설정

사용: ☐ OFF

사용자 ID:

인증 방법: 로컬 인증 사전 공유키

원격 인증: 사전 공유키

인증 비밀번호:

원격 사용자 IP 할당: ☐ IP Pool ☐ 고정 IP 할당

원격 사용자 IP:

접근 정책: ☒ 내부망

호스트 | 네트워크 | 그룹

· 객체 목록

· 추가할 객체

원격 사용자 추가

기본 설정 | 고급 설정

IKE SA 생명 주기(초):

IPSec SA 생명 주기(초):

원격 GW IP:

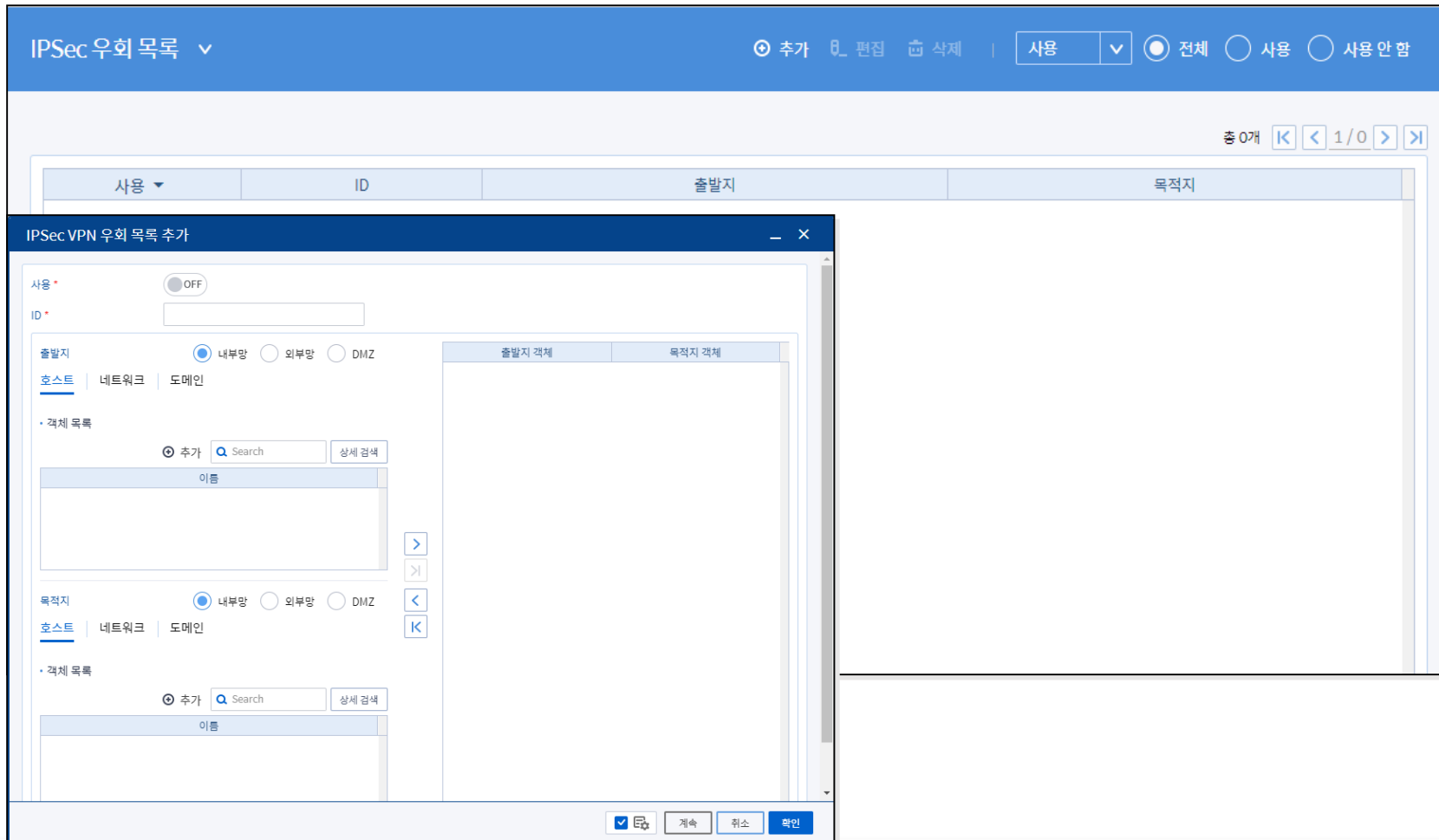
원격 사용자 등록

1. 원격 사용자 등록 설정

- 센터 장비에서 터널 연결을 요청하는 클라이언트(원격 사용자) ID를 등록하고, 클라이언트(원격 사용자)에 할당할 IP 주소와 접근 정책을 설정.
- 원격 사용자에 사설 IP를 할당하는 방식을 설정.
- IP pool 방식과 고정 IP를 할당하는 방식 중 하나 선택하여 등록 가능.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 예외 정책 설정 (IPv4 / IPv6 동일)



IPSec 우회 목록

1. IPSec 우회 목록 설정 :

- 예외 정책은 IPSec 정책의 적용을 받지 않을 정책을 의미함.
즉, IPSec의 보안 설정 기능을 적용 받지 않고 우회할 목록을 객체를 사용해서 설정함.
- 우회 목록으로 설정할 수 있도록 호스트 객체, 네트워크 객체를 지원.
- 즉, IPSec 우회 목록은 VPN 터널을 이용하지 않고 트래픽 처리.
- VPN 터널을 이용하지 않고 트래픽 처리.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 예외 정책 설정 (IPv4 / IPv6 동일)

비정상 터널 우회 목록

⊕ 추가 편집 삭제 | 사용 | ● 전체 ○ 사용 ○ 사용 안 함

총 0개 < 1 / 0 >

사용	출발지 네트워크/서브넷 마스크	목적지 네트워크/서브넷 마스크
----	------------------	------------------

비정상 터널 우회 목록 추가

사용 * ☐ OFF

출발지 네트워크 * . . . /

목적지 네트워크 * . . . /

☒ ☐ 계속 취소 확인

비정상 터널 우회 목록

1. 비정상 터널 우회 목록 설정

- 비정상 터널에 대한 VPN 정책 적용이 되지 않도록 우회 목록을 호스트/네트워크 단위로 추가 가능.

즉, 설정된 터널에 문제가 발생 시 라우팅으로 우선 처리가 필요한 경우 설정함.

- Switch-Bypass 기능과 동일.

5.2 BLUEMAX NGF IPSec 메뉴 설명

- 예외 정책 설정 (IPv4/IPv6 동일 단, IPv6 멀티캐스트 전송 기능 미 지원)

멀티캐스트 전송 목록 ▾

⊕ 추가 편집 삭제 | 🔍 Search 상세 검색

총 0개 <K < 1/0 > >I

사용 ▾	멀티패스 전송 ▾	멀티캐스트 IP 주소	SA 출발지 네트워크/서브넷 마스크	SA 목적지 네트워크/서브넷 마스크
<div><div>멀티캐스트 전송 목록 추가</div><div><div>사용 *</div><div>OFF</div></div><div><div>멀티패스 전송 *</div><div>OFF</div></div><div><div>멀티캐스트 IP 주소 *</div><div><div></div><div></div><div></div><div></div><div></div></div></div><div><div>출발지 네트워크 *</div><div><div></div><div></div><div></div><div></div><div></div><div>/</div><div></div></div></div><div><div>목적지 네트워크 *</div><div><div></div><div></div><div></div><div></div><div></div><div>/</div><div></div></div></div><div><div>✓ ⚙</div><div>계속</div><div>취소</div><div>확인</div></div></div>				

멀티캐스트 전송 목록

1. 멀티캐스트 전송 목록 설정

- 터널을 통해 멀티캐스트 IP 를 전송 할 때 사용함.
- 멀티캐스트 대역을 추가하면 해당 대역은 설정된 암호화 대역에 따라 암호화되어 전송 가능함.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 보안 정책 설정

보안 정책 설정

⊕ 추가 8 편집 삭제 | Search 상세 검색

총 1개 < 1/1 >

기본 정책	보안 정책 이름	암호 알고리즘	인증 알고리즘	DH 그룹	설명
●	ARIA-128-SHA-256-Group14	ARIA-128	SHA-256	Group14:MODP-2048	

보안 정책 추가

기본 설정 | 고급 설정

보안 정책 이름 * AES-128-MD5-Group1

암호 알고리즘 * AES-128 ▼

인증 알고리즘 * MD5 ▼

DH 그룹 * Group1:MODP-768 ▼

설명

✓ ⚙ 계속 취소 확인

보안 정책 설정

1. 보안 정책 기본 설정

- 보안 정책 설정 메뉴를 통해서 VPN에 적용할 암호 알고리즘, 인증 알고리즘, DH 그룹, 동작모드, 생명주기 등을 설정함.
- 기본 정책으로 등록된 보안 정책은 VPN 터널 생성 시 기본값으로 적용되고, 만약 보안 정책을 변경할 경우 기본 정책을 변경하거나 지점 등록에서 VPN 터널 별로 변경 가능함.
- 보안 정책 설정에서 등록한 값이 자동으로 등록되며, 유일하게 HA 멤버끼리 동기화.

5.2 BLUEMAX NGF IPSec 메뉴 설명

- **보안 정책 설정**

보안 정책 설정					
<div> <div>추가</div> <div>편집</div> <div>삭제</div> <div>Search</div> <div>상세 검색</div> </div>					
총 1개 < 1 / 1 >					
기본 정책	보안 정책 이름	암호 알고리즘	인증 알고리즘	DH 그룹	설명
	ARIA-128-SHA-256-Group14	ARIA-128	SHA-256	Group14:MODP-2048	

암호화 알고리즘	인증 알고리즘	DH 그룹
<ul style="list-style-type: none"> AES-128 AES-192 AES-256 ARIA-128 ARIA-192 ARIA-256 DES 3DES SEED Blowfish CAST-128 CAST-256 LEA-128 LEA-256 	<ul style="list-style-type: none"> MD5 SHA-1 SHA-256 SHA-384 SHA-512 HAS-160 	<ul style="list-style-type: none"> Group1:MODP-768 Group2:MODP-1024 Group5:MODP-1536 Group14:MODP-2048 Group15:MODP-3072 Group16:MODP-4096 Group17:MODP-6144 Group18:MODP-8192

보안 정책 설정

1. 보안 정책 기본 설정

- 보안 정책 설정 메뉴를 통해서 VPN 터널에 적용될 암호 알고리즘, 인증 알고리즘, DH 그룹, 동작모드, 생명주기 등을 설정.
- 기본 정책으로 등록된 보안 정책은 VPN 터널 생성 시 기본값으로 적용되고, 만약 보안 정책을 변경할 경우 기본 정책을 변경하거나 지점 등록에서 VPN 터널 별로 변경 가능.
- 보안 정책 설정에서 등록한 값이 자동으로 등록되며, 유일하게 HA 멤버끼리 동기화함.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 보안 정책 설정

기본 정책	보안 정책 이름	암호 알고리즘	인증 알고리즘	DH 그룹	설명
●	ARIA-128-SHA-256-Group14	ARIA-128	SHA-256	Group14:MODP-2048	

보안 정책 추가

기본 설정 | 고급 설정

기본 설정을 따름 * ☐ OFF

IKE SA 암호 알고리즘 * AES-128

IKE SA 인증 알고리즘 * MD5

IKE SA DH 그룹 * Group1:MODP-768

☒ ☐

보안 정책 설정

1. 보안 정책 고급 설정

- BLUEMAX NGF에서는 다양한 보안 정책 설정 가능.

즉, IKE SA 암호 알고리즘, 인증 알고리즘, DH 그룹을 기본 설정의 알고리즘과 동일한 알고리즘을 사용할 것인지 다른 알고리즘을 사용할 것인지 선택 할 수 있음.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 센터 연결 설정

센터 연결 설정 ▾

RSA 인증서 인증 ☐

인증 ID

회선 선택 ☒ IPv4 ☐ IPv6

eth0 192.168.10.11/24

eth3 210.118.20.211/24

보안 정책 이름

외부 인증 프로파일

인증 프로파일 추가

이름*

관리자 인증 전용 ☐

인증 서버 목록* |

서버 이름	서버 종류
-------	-------

인증 시도 횟수*

잠금 시간(분)*

설명

센터 연결 설정

1. 센터 연결 설정

- 지점이나 사용자가 VPN터널 생성을 요청할 때 이에 대한 정책 협상을 하기 위한 기본 사항을 설정함.
- 회선 선택 시 VPN 연결할 인터페이스를 선택.(optional, 회선이 여러개 일 경우 설정 안해도 무방함)
- 보안 정책에서 설정된 정책이 모두 표시됨.
- 외부 인증 프로파일 System > 인증 > 인증 프로파일 메뉴를 통해 등록 또는 추가 버튼을 클릭해서 추가 가능.
- VPN 터널 생성을 위한 인증 방식이 RSA 인증서를 이용한 방식인지 여부를 설정.
- 기본으로 사전 공유키 방식만 허용하나 RSA 인증서 인증까지 허용 가능.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 일반 설정

일반 설정 ▾	최대 재전송 횟수	보안 게이트웨이가 Initiator로 설정되어 IKE 연결을 시도할 때 몇 번까지 재시도를 할 것인지 결정
가상 사설망 일반 설정	SA 점검 간격 시간	보안터널이 설정되어 있는 경우 설정된 간격으로 연결 상태가 정상인지 체크. 만약 연결 상태가 잘못되어 있으면 다시 키 교환
<div> <div>최대 재전송 횟수</div> <div>4</div> </div> <div> <div>SA 점검 간격 시간(초)</div> <div>60</div> </div> <div> <div>재전송 시간 간격 증가값(초)</div> <div>2</div> </div> <div> <div>초기 재전송 타임아웃(초)</div> <div>7</div> </div> <div> <div>키교환 포트</div> <div>500</div> </div> <div> <div>NAT-T 포트</div> <div>4500</div> </div> <div> <div>IKEv2 DoS 공격 방어</div> <div>OFF</div> </div>	재전송 시간간격 증가 값	재전송할 경우 시간 간격을 조정하는 값 다음 공식으로 재전송 시간 간격이 조정 [재전송 시간 간격 = 초기 재전송 타임아웃 + (재전송 타임아웃 증가 값 * 재전송 횟수)]
SA Path 점검(DLD: Dead Link Detection)	초기 재전송 타임아웃	재전송 시간 간격의 초기값을 설정 이후 재전송 타임아웃 증가 값에 의해 시간간격이 증가
<div> <div>DLD 타임아웃(초)</div> <div>10</div> </div> <div> <div>DLD 검사 간격(초)</div> <div>5</div> </div> <div> <div>최대 DLD 시도 횟수</div> <div>3</div> </div>	키 교환 포트	VPN 설정 시 키 교환에 사용할 포트 번호를 입력
	NAT-T 포트	NAT-T에 사용할 포트 번호를 입력
	IKEv2 Dos 공격 방어	IKEv2 DoS 공격 방어 유무를 선택
	DLD 타임아웃	DLD 요청에 대한 응답을 기다리는 시간 간격
	DLD 검사 간격	DLD를 하는 시간 간격
	최대 DLD 시도 횟수	최대 DLD 시도 횟수만큼 연속적인 DLD 실패가 발생할 경우 SA를 삭제

일반 설정

1. 일반 설정

- IPSec VPN 동작을 위한 기본 사항을 설정.

5.2 BLUEMAX NGF IPSec 메뉴 설명

• 일반 설정

IPv4 정책			
가상 사설망 프로토콜 전용 라우팅	<input checked="" type="checkbox"/>	기본 게이트웨이	210 . 118 . 20 . 1
IPSec MTU, Block Fragmentation	<input checked="" type="checkbox"/>	IPSec MTU(bytes)	1380
IPv6 정책			
가상 사설망 프로토콜 전용 라우팅	<input type="checkbox"/>	기본 게이트웨이	IPv6 주소
IPSec MTU, Block Fragmentation	<input checked="" type="checkbox"/>	IPSec MTU(bytes)	1380

가상 사설망 프로토콜 전용 라우팅

- 라우팅 테이블에 설정되어 있는 디폴트 라우팅과 별개로 VPN 터널 통신을 위한 디폴트 라우팅 설정을 의미함.
- IKE, ESP, AH와 같이 VPN 터널과 관련된 통신은 기본 게이트웨이 IP 주소에서 설정하는 디폴트 라우터를 경유해서 통신함.
- 디폴트 라우팅이 VPN 터널의 방향과 다른 경우 사용.

IPsec MTU Block Fragmentation

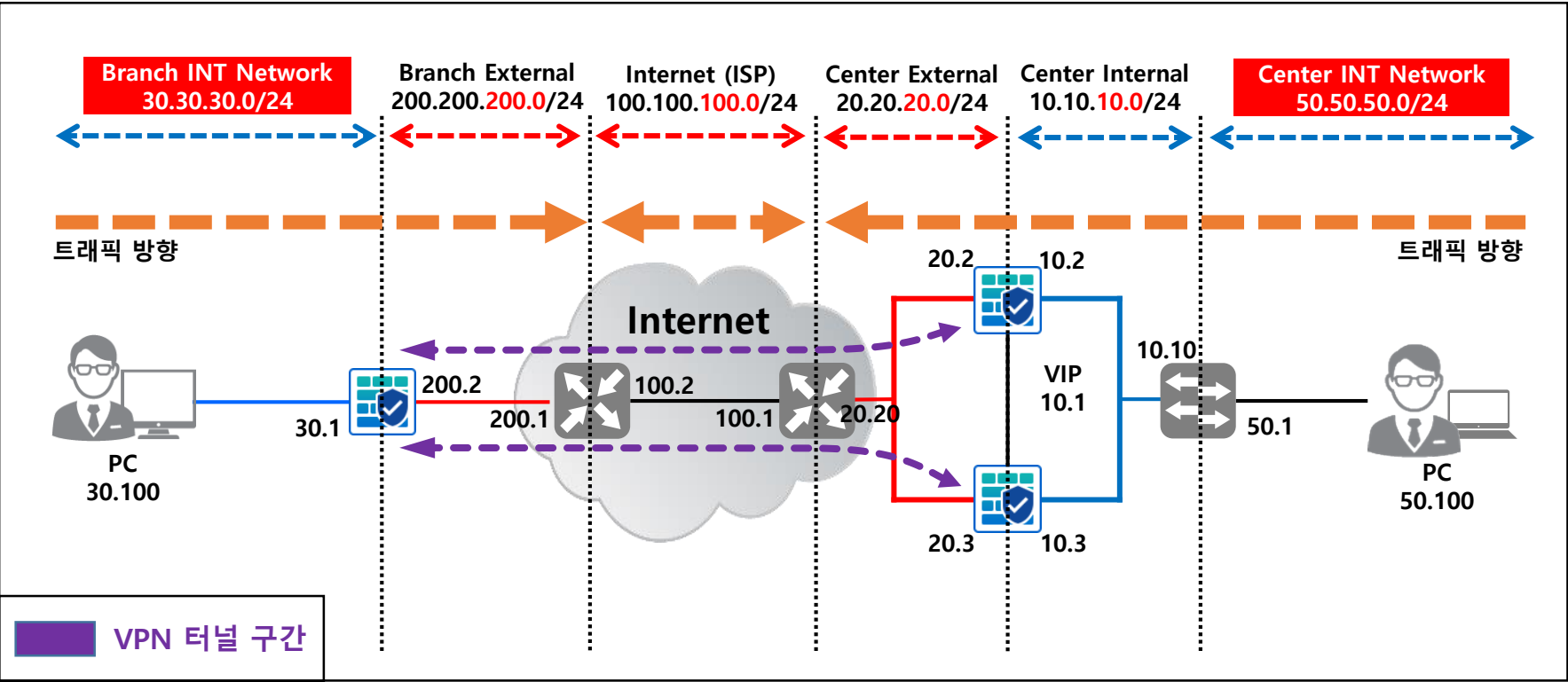
- IPsec의 MTU 크기를 설정.
- IPsec 암호화 하게 되면 **원본 패킷 크기 보다 약 28 Byte정도 증가하므로** 1,500 Byte에 가까운 패킷들은 항상 Fragmentation(단편화) 발생함.
- Fragmentation(단편화)이 발생하면 성능이 저하될 수 있기 때문에 패킷이 Fragmentation(단편화) 되는 것을 방지하기 위해 세션이 생성될 때 강제적으로 MTU를 조정하도록 IPsec MTU 설정.

일반 설정

1. 일반 설정

- IPSec VPN 동작을 위한 기본 사항을 설정

구성도



구성 설명

- 1. Center 이중화 구성
 - Route Active-Active
 - Single VIP
 - 2. Branch 단일 구성
 - 3. VPN Tunnel (Active Active)
 - VPN #1 : Branch → Center M
 - VPN #2 : Branch → Center B
- ※ Center/Branch - NAT 설정 X

센터 (Center) 설정

• 인터페이스 설정 – 회선 상태 검사

인터페이스 설정

물리적 인터페이스 | 브리지 구성 | 트렁크 구성 | ARP 관리 | LLCF 관리

인터페이스 이름	모드	IP 주소	MTU	속도	Duplex	Auto-Negotiation	Up/Down	링크 연결	Zone	설정
eth0	L3	192.168.10.10/24	1500	100M	Full Duplex	on	UP	yes	DMZ	[설정] [회선 상태 검사] [회선 속도 검사]
eth1	L3	10.10.10.2/24	1500	100M	Full Duplex	on	UP	yes	내부망	[설정] [회선 상태 검사] [회선 속도 검사]
eth2	L3	20.20.20.2/24	1500	100M	Full Duplex	on	UP	yes	외부망	[설정] [회선 상태 검사] [회선 속도 검사]
eth3	L3		1500			on	UP	no		[설정] [회선 상태 검사] [회선 속도 검사]
eth4	L3		1500			on	UP	no		[설정] [회선 상태 검사] [회선 속도 검사]
eth5	L3		1500			on	UP	no		[설정] [회선 상태 검사] [회선 속도 검사]
eth6	L3		1500			on	UP	no		[설정] [회선 상태 검사] [회선 속도 검사]
eth7	L3		1500			on	UP	no		[설정] [회선 상태 검사] [회선 속도 검사]
eth8	L3	1.1.1.1/30	1500	1G	Full Duplex	on	UP	yes	HA	[설정] [회선 상태 검사] [회선 속도 검사]

인터페이스 고급 설정

eth1

VLAN 구성 | 라우터 백업 | VRRP | 회선 상태 검사 | 회선 속도 검사 | 기타 선택 사항

사용 ☒

검사 대상 IP 주소 * IPv4 IPv6 10 . 10 . 10 . 10 [주 회선]

게이트웨이 IP 주소 10 . 10 . 10 . 10 [주 회선]

게이트웨이 IP 주소(IPv6) IPv6 주소 [주 회선]

최대 응답 대기 시간(ms) * 500

검사 주기(초) * 2

실패 허용 횟수(회) * 3

eth2

VLAN 구성 | 라우터 백업 | VRRP | 회선 상태 검사 | 회선 속도 검사 | 기타 선택 사항

사용 ☒

검사 대상 IP 주소 * IPv4 IPv6 20 . 20 . 20 . 20 [주 회선]

게이트웨이 IP 주소 20 . 20 . 20 . 20 [주 회선]

게이트웨이 IP 주소(IPv6) IPv6 주소 [주 회선]

최대 응답 대기 시간(ms) * 500

검사 주기(초) * 2

실패 허용 횟수(회) * 3

VPN Center 설정

1. 인터페이스 회선 상태 검사 설정

- 회선 상태 검사
 - 검사 대상 IP로 설정한 곳을 목적지(GW)로 Ping 체크하여 Alive/Dead 상태 확인.
- HA 구성인 경우, 내/외부 인터페이스 모두 설정하는 것이 원칙.
 - ※ 내/외부 인터페이스에 회선 상태 검사를 설정하지 않을 경우, 정상적으로 Fail-Over 되지 않을 수 있음.
- 내부 인터페이스가 여러 개인 경우, **복호화 된 트래픽이 통과할 인터페이스**에 회선 상태 검사 설정.
- 게이트 웨이 주소는 일반적으로 인접 장비의 IP를 설정함.
 - ※ 동적 인터페이스의 경우, 검사 대상 IP/게이트웨이 IP는 자동으로 설정됨.

master / backup 장비 동일하게 설정.

• 보안 정책 설정

보안 정책 설정

추가 편집 삭제 Search 상세 검색

총 1개

기본 정책	보안 정책 이름	암호 알고리즘	인증 알고리즘	DH 그룹	구분	설명
<input checked="" type="radio"/>	3DES-SHA-256-Group14	3DES	SHA-256	Group14:MODP-2048	관리자	

보안 정책 추가

기본 설정 고급 설정

보안 정책 이름: 3DES-MD5-Group1

암호 알고리즘: 3DES

인증 알고리즘: SHA-256

DH 그룹: Group2:MODP-1024

설명:

1

2

3

VPN 보안정책 설정

1. 보안 정책 설정

- **Center / Branch 장비 모두 설정**
- VPN 터널 연결 시 적용되는 보안 정책을 설정
 - 암호 알고리즘
 - 인증 알고리즘
 - DH 그룹

• 센터 연결 설정

인터페이스 설정

물리적 인터페이스 | 브리지 구성 | 트렁크 구성 | ARP 관리 | LLCF 관리

새로고침

인터페이스 이름	모드	IP 주소	MTU	속도	Duplex	Auto-Negotiation	Up/Down	링크 연결	Zone	설정
eth0	L3	192.168.10.10/24	1500	100M	Full Duplex	on	UP	yes	DMZ	[설정] [재설정] [삭제]
eth1	L3	10.10.10.2/24	1500	100M	Full Duplex	on	UP	yes	내부망	[설정] [재설정] [삭제]
eth2	L3	20.20.20.2/24	1500	100M	Full Duplex	on	UP	yes	외부망	[설정] [재설정] [삭제]
eth3	L3		1500			on	UP	no		[설정] [재설정] [삭제]
eth4	L3		1500			on	UP	no		[설정] [재설정] [삭제]

센터 연결 설정

RSA 인증서 인증 ☐ OFF

인증 ID

회선 선택

IPv4 ☒ IPv6 ☐

eth0 192.168.10.10/24

Filter

eth0 192.168.10.10/24

eth8 1.1.1.1/30

eth1 10.10.10.2/24

eth2 20.20.20.2/24

보안 정책 이름

외부 인증 프로파일

사용 안함

VPN Center 연결 설정

- Center 장비의 외부 회선을 선택
 - 외부 Real IP를 사용하는 인터페이스를 선택해서 설정

• 지점 등록

The screenshots illustrate the steps to add a new site in the SECUI system. The main interface shows the '지점 등록' (Site Registration) menu with a '추가' (Add) button. The '지점 등록 편집' (Edit Site Registration) window is shown with the '기본 설정' (Basic Settings) tab selected. The '고급 설정' (Advanced Settings) tab is also shown, detailing connection parameters like mode, IP address, and SA lifetimes. The interface also displays lists for 'Center 내부 객체' (Center Internal Objects) and 'Branch 내부 객체' (Branch Internal Objects).

지점 등록

1. 지점 등록 (기본 설정 / 고급 설정)
2. 센터 장비가 이중화 인 경우 master / backup 각각 설정 (동기화 대상 X)
3. 지점이 이중화 인 경우, 지점의 master / backup 각각 터널 연결이 필요하기 때문에 센터 master 에 지점 master / backup 정보 설정을 해야함.
 - 센터 M ↔ 지점 M (branch1)
 - 센터 M ↔ 지점 B (branch2)
 - 센터 B ↔ 지점 M (branch3)
 - 센터 B ↔ 지점 B (branch4)
4. 지점 장비에서 사용할 회선을 선택
 - 지정하지 않으면, 디폴트로 지점 장비에서 회선 상태 검사 설정을 적용한 인터페이스 모두 포함됨

지점 (Branch) 설정

- 인터페이스 설정 - 회선 상태 검사

VPN 지점 설정

1. 인터페이스 회선 상태 검사 설정
 - 회선 상태 검사
 - 검사 대상 IP로 설정한 곳을 목적지(GW)로 Ping 체크하여 Alive/Dead 상태 확인.
 - HA 구성인 경우, 내/외부 인터페이스 모두 설정하는 것이 원칙.
 - ※ 내/외부 인터페이스에 회선 상태 검사를 설정하지 않을 경우, 정상적으로 Fail-Over 되지 않을 수 있음.
 - 내부 인터페이스가 여러 개인 경우, **복호화 된 트래픽이 통과할 인터페이스**에 회선 상태 검사 설정.
 - 게이트 웨이 주소는 일반적으로 인접 장비의 IP를 설정함.
 - ※ 동적 인터페이스의 경우, 검사 대상 IP/게이트웨이 IP는 자동으로 설정됨.

인터페이스 설정

물리적 인터페이스
브리지 구성
트렁크 구성
ARP 관리
LLCF 관리

새로고침

인터페이스 이름	모드	IP 주소	MTU	속도	Duplex	Auto-Negotiation	Up/Down	링크 연결	Zone	설정
eth0	L3	192.168.10.13/24	1500	100M	Full Duplex	on	UP	yes	DMZ	
eth1	L3	200.200.200.2/24	1500	1G	Full Duplex	on	UP	yes	외부망	

인터페이스 고급 설정

인터페이스 이름
eth1

VLAN 구성
라우터 백업
VRRP
회선 상태 검사
회선 속도 검사
기타 선택 사항

사용

ON

검사 대상 IP 주소 *

IPv4

200

200

200

1

[복사]

☐ 주 회선

게이트웨이 IP 주소

200

200

200

1

[복사]

게이트웨이 IP 주소(IPv6)

IPv6 주소

[복사]

최대 응답 대기 시간(ms) *

500

[증가]

[감소]

검사 주기(초) *

2

[증가]

[감소]

실패 허용 횟수(회) *

3

[증가]

[감소]

6. 구성 실습

• 지점 연결 설정

The screenshot displays the '지점 연결 설정' (Branch Connection Settings) interface. At the top, there is a '+ 추가' (Add) button highlighted with a red dashed arrow. Below it is a table with columns: 사용 (Use), 이름 (Name), 지점 ID (Branch ID), 센터 장비 IP 주소 (Center Device IP Address), 연결 모드 (Connection Mode), 동작 모드 (Operation Mode), 수명 주기(초) (Lifetime (sec)), 구분 (Category), and 설명 (Description). The table shows 0 items. Below the table, there are two panels for editing settings. The left panel is titled '지점 연결 설정 편집' and has two tabs: '기본 설정' (Basic Settings) and '고급 설정' (Advanced Settings). The '기본 설정' tab is active, showing fields for '사용' (checked), '연결 이름' (center-m), '센터 장비 IP 주소' (20.20.20.2), '인증 방법' (사전 공유키 방식), '지점 ID' (branch1), and '인증 비밀번호 / 확인'. The right panel is titled '지점 연결 설정 편집' and has two tabs: '기본 설정' and '고급 설정'. The '고급 설정' tab is active, showing fields for '연결 모드' (IKEv2), '로컬 IP 주소' (ANY), '보안 정책 이름' (3DES-SHA-256-Group14), '동작 모드' (ESP-Tunnel), 'IKE SA 생명 주기(초)' (160000), 'IPSec SA 생명 주기(초)' (80000), '센터 IKE 포트' (500), 'UDP Encapsulation 강제 적용' (OFF), and '표준 IPSec' (OFF). Red arrows indicate the flow from the 'Add' button to the 'Basic Settings' tab and then to the 'Advanced Settings' tab.

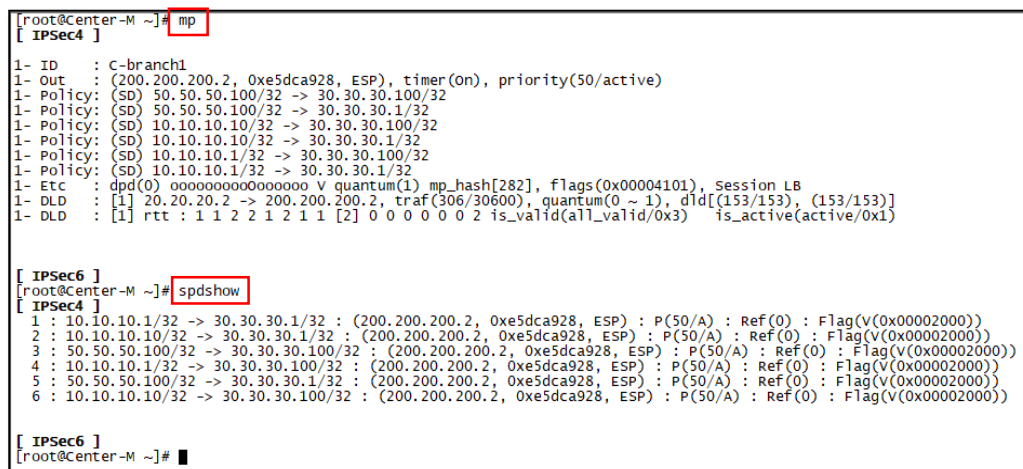
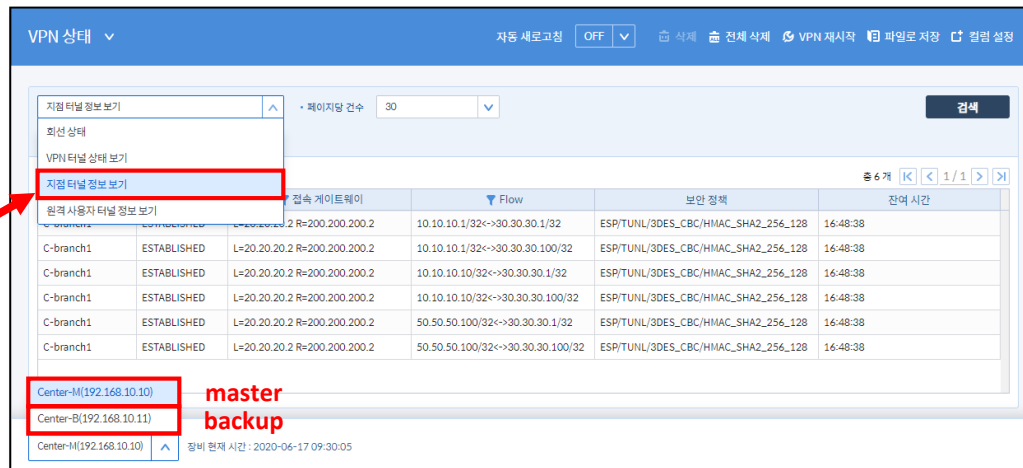
VPN 지점 설정

1. 센터 IP 주소 입력
※ 센터 장비의 회선(외부)이 여러 개인 경우 전부 등록
2. 지점에서 VPN 터널 연결을 시도할 때 인증하는 방법 및 인증ID/PW 입력
3. 연결 모드
4. IKE 생명 주기 / IPSec SA 생명 주기는 센터에서 설정한 내용과 동일하게 설정하는 것을 권고함.

VPN 터널 연결 확인

6. 구성 실습

터널 상태 확인 – Center / Branch 공통



VPN 터널 상태 확인

1. Log/Report → VPN 상태 → **회선 상태 검사**
 - CLI 명령어 : mltot
2. Log/Report → VPN 상태 → VPN 터널 상태 보기
3. Log/Report → VPN 상태 → **지점 터널 정보 보기**
 - CLI 명령어
 - mp
 - mpsa
 - spdshow

터널 상태 확인 – Center / Branch 공통

```
[root@Center-M ~]# vpnctl ike status
Security Associations (1 up, 0 connecting):
  C-branch1[7]: ESTABLISHED 17 minutes ago, 20.20.20.2[__CENTER_b59c23d_]...200.200.200.2[branch1]
  C-branch1[9]: INSTALLED, TUNNEL, reqid 6, ESP SPIs: f30a01a6_i e5dca928_o
  C-branch1[9]: 10.10.10.1/32 10.10.10.10/32 50.50.50.100/32 == 30.30.30.1/32 30.30.30.100/32
[root@Center-M ~]#
[root@Center-M ~]#
[root@Center-M ~]#
[root@Center-M ~]# vpnctl ike statusall
Status of IKE charon daemon (strongswan 5.6.2, Linux 4.14.90-1.41581, x86_64):
  uptime: 47 hours, since Jun 15 10:33:19 2020
  malloc: sbrk 2703360, mmap 0, used 1104608, free 1598752
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 10
  loaded plugins: charon cast6 lea rc2 md4 has160 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem openssl fips-prf gmp curve25519 xcbc cmac hmac sqlite attr kernel-netlink resolve socket-default stroke vici updown eap-iden
tity eap-md5 eap-mschapv2 eap-radius xauth-generic unity counters
Listening IP addresses:
  192.168.10.10
  10.10.10.2
  10.10.10.1
  20.20.20.2
  20.20.20.1
  1.1.1.1
  11.11.0.2
IKE daemon state:
  IPv4: RUNNING
  IPv6: RUNNING
Log configuration:
  ipsec_event_log: Enabled
Connections:
  C-branch1: %any...200.200.200.2 IKEv1/2, dpddelay=30s
  C-branch1: local: [__CENTER_b59c23d_] uses pre-shared key authentication
  C-branch1: remote: [branch1] uses pre-shared key authentication
  C-branch1: child: 50.50.50.100/32 10.10.10.1/32 10.10.10.10/32 == 30.30.30.100/32 30.30.30.1/32 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
  C-branch1[7]: ESTABLISHED 17 minutes ago, 20.20.20.2[__CENTER_b59c23d_]...200.200.200.2[branch1]
  C-branch1[7]: IKEv2 SPIs: 3a5cfb78daac90ac_i d2b6877aa727a054_r*, rekeying in 41 hours
  C-branch1[7]: IKE proposal: 3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  C-branch1[9]: INSTALLED, TUNNEL, reqid 6, ESP SPIs: f30a01a6_i e5dca928_o
  C-branch1[9]: 3DES_CBC/HMAC_SHA2_256_128, 27264 bytes_i (426 pkts, 1s ago), rekeying in 18 hours
  C-branch1[9]: 10.10.10.1/32 10.10.10.10/32 50.50.50.100/32 == 30.30.30.1/32 30.30.30.100/32
[root@Center-M ~]#
```

VPN 터널 상태 확인

1. IKE 상태 확인 (CLI)

- **vpnctl** 명령어 이용
 - vpnctl ike status
 - vpnctl ike statusall

GRE (Generic Routing Encapsulation) / IPIP 터널링 설정

GRE/IPIP 터널링 추가

기본 설정

고급 설정

사용 *

터널 종류 *

터널 로컬 게이트웨이 IP *

터널 리모트 게이트웨이 IP *

설명

OFF

IPIP

연결 이름 *

터널 인터페이스 이름 *

tun12

접근 정책

외부망

호스트

네트워크

그룹

객체 목록

추가

Search

상세 검색

이름

추가할 객체

직접 입력

이름

✓

⚙

계속

취소

확인

GRE / IPIP

- GRE/IPIP 터널링은 단순히 터널링을 기반으로 하는 기능으로 라우팅 기반으로 제어
- GRE
 - IP 트래픽을 위해 GRE 터널 지원
 - 멀티캐스트 패킷을 지원
- IPIP (IP over IP)는 IP 패킷을 캡슐화하여 두 라우터 간에 터널을 생성함.

PPTP (Point to Point Tunneling Protocol) / L2TP (Layer 2 Tunneling Protocol)

PPTP/L2TP 설정 ▾

터널링 설정 | 사용자 등록

PPTP 터널링 설정 ☒ 사용 ☐ 사용 안 함

DNS 주소

WINS 주소

로컬 IP 주소*

IP 할당 범위*

L2TP 터널링 설정 ☒ 사용 ☐ 사용 안 함

DNS 주소

WINS 주소

로컬 IP 주소*

IP 할당 범위*

DNS 주소	DNS 주소를 입력
WINS 주소	WINS 주소를 입력
로컬 IP	PPTP / L2TP 터널링 통신 시 장비에서 사용되는 IP를 입력
IP 할당 범위	PPTP / L2TP 클라이언트에 할당할 IP 범위를 입력

PPTP/L2TP 사용자 추가

사용* ☐ OFF

사용자 ID*

터널 종류* ☐ PPTP ☐ L2TP

인증 비밀번호*

인증 비밀번호 확인*

설명

☒ ☐

PPTP / L2TP

1. PPTP는 컴퓨터와 컴퓨터가 1대1 방식으로 데이터를 전송
- 다른 시스템이나 인터넷으로 보안을 유지하면서 VPN을 지원해주는 프로토콜
2. L2TP는 PPTP와 L2F를 통합한 프로토콜
- 인터넷을 포함한 공중 통신망에서 VPN 사용할 때 설정

- ✓ 사용자 등록
- 사용자 ID
 - 터널 종류 : PPTP / L2TP
 - 인증 비밀번호

회선 상태 확인 - mltot

```
[root@BLUEMAX ~]# mltot
```

Multiline Status					
Multiline status	:	Enable			
Multiline check interval	:	2 sec			
HA Packet Forwarding	:	Enable			
IKE Status	:	[Enable]		[Enable]	
DLD Status	:	[On]		[On]	
Int line status	:	IPv4 [Alive]		IPv6 [Alive]	
DMZ line status	:	IPv4 [Alive]		IPv6 [Alive]	
Ext line status	:	IPv4 [Alive]		IPv6 [None]	
Ext alive lines	:	[1/1 lines]		[0/0 lines]	

<<<< Multiline Configuration >>>>					
M/L if:eth12(Static,Int)	IPv4: 40.40.40.10	CHK: 40.40.40.1	G/W: 40.40.40.1	-Alive	
	Pv6: ::	CHK: ::	G/W: ::		
M/L if:eth16(Static,Ext)	IPv4: 30.30.30.10	CHK: 30.30.30.1	G/W: 30.30.30.1	-Alive	
	Pv6: ::	CHK: ::	G/W: ::		

회선 상태 확인

- mltot 명령어를 이용해서 회선 상태 확인
 - Alive : 검사 대상 IP / 게이트 웨이 IP 로 ping
체크가 정상
 - Dead : 검사 대상 IP / 게이트 웨이 IP로 ping

체크 불가 및 통신 불가

※ 회선 상태가 Dead 일 경우, 인접 장비와 통신에 문제가 발생한 것으로 인지하고 정상 유무 확인 필요.

VPN 관련 프로세스(데몬) 상태 확인 - **vl**

```
[root@BLUEMAX ~]# vl
[ Feature Code Check ]
VPN Feature           : ON
[ Module & Process Status ]
IPSec  Crypto module type : SW module
IPSec6 Crypto module type : SW module
module secui_crypto       : Running
module ipsec              : Running
module ipsec6             : Running
process multiline        : Running
process starter           : Running
process secui_rip         : Running
process secui_rip6        : Running
process secui_ml_rip      : Running
process secui_ml_rip6     : Running
process sa_routing        : Running
process rtt_to_center     : Running
process autospeedchk      : Running
process vpnlog            : Running
process log_supportd      : Running
startup mtu_adj           : -----
startup replay_status     : -----
startup secui_protocol_rt : -----
startup ipsec_dld_app     : -----
startup vpnctl ipsec4 app.: -----
startup vpnctl ipsec4 app.: -----
startup vpnctl ipsec4 app.: -----
startup ipsec_pre_spd     : -----
startup mtu_adj -6        : -----
startup secui_protocol_rt.: -----
startup vpnctl ipsec6 app.: -----
startup vpnctl ipsec6 app.: -----
startup vpnctl ipsec6 app.: -----
```

vpn 프로세스 상태 확인

- VPN 터널 접속 장애 시 process(데몬)가 활성화 되어 있는지 확인.
- Running 되지 않을 경우 지점장비와 센터장비와의 터널 접속시도가 없으면 vl 명령어를 이용하여 VPN 서비스 재기동 필요.
- 프로세스 정지 : vl -k -u
- 프로세스 재실행 : init_vpn
- vl -k -u ; init_vpn

※ [주의]

센터 장비에서 적용할 경우, 연결되어 있는 VPN 터널이 끊어지며 새로이 터널이 생성되기 때문에 세션 단절 발생함

터널 상태 확인 – **spdshow** / **mp**

```
[root@BLUEMAX ~]# spdshow
[ IPsec4 ]
 1 : 10.10.10.1/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 2 : 10.10.10.1/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 3 : 10.10.10.2/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 4 : 10.10.10.1/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 5 : 10.10.10.2/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 6 : 10.10.10.3/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 7 : 10.10.10.2/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 8 : 10.10.10.3/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 9 : 10.10.10.3/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
10 : 200.200.200.154/32 -> 20.20.20.1/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
11 : 200.200.200.154/32 -> 20.20.20.2/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
12 : 200.200.200.154/32 -> 20.20.20.3/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))

[ IPsec6 ]
[root@BLUEMAX ~]# mp
[ IPsec4 ]

1- ID      : C-secui00
1- Out     : (30.30.30.11, 0x075283e6, ESP), timer(0n), priority(50/active)
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.3/32
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.2/32
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.1/32
1- Etc     : dpd(0) 0000000000000000 V quantum(1) mp_hash[980], flags(0x00004101), Session LB
1- DLD     : [1] 30.30.30.10 -> 30.30.30.11, traf(486/52488), quantum(0 ~ 1), dld[(243/243), (243/243)]
1- DLD     : [1] rtt : 0 0 [1] 1 0 2 1 1 0 1 0 0 0 1 0 0 is_valid(all_valid/0x3) is_active(active/0x1)
```

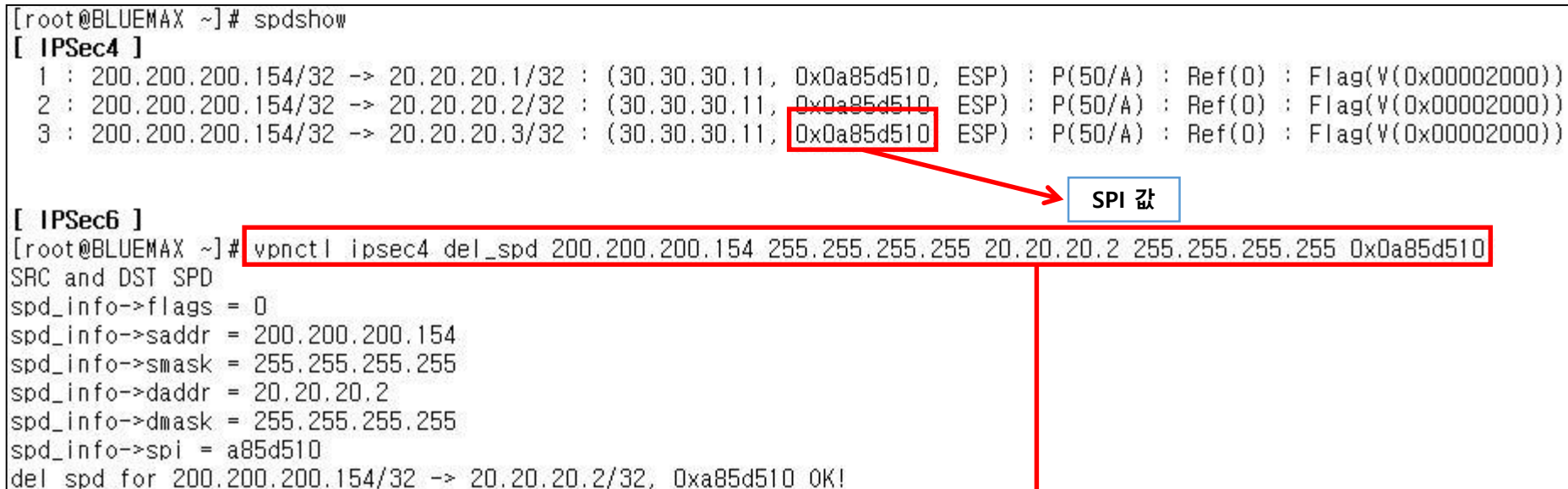
V : 연결정상, IV : 연결 끊김

rtt 값 체크 진행중이며 멈춤이나
~ 표시 또는 값이 커지면 회선에
이상여부 확인 필요함

SPD 삭제 – `vpnctl ipsec4 del_spd`

```
[root@BLUEMAX ~]# spdshow
[ IPsec4 ]
 1 : 200.200.200.154/32 -> 20.20.20.1/32 : (30.30.30.11, 0x0a85d510, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
 2 : 200.200.200.154/32 -> 20.20.20.2/32 : (30.30.30.11, 0x0a85d510, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
 3 : 200.200.200.154/32 -> 20.20.20.3/32 : (30.30.30.11, 0x0a85d510, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))

[ IPsec6 ]
[root@BLUEMAX ~]# vpnctl ipsec4 del_spd 200.200.200.154 255.255.255.255 20.20.20.2 255.255.255.255 0x0a85d510
SRC and DST SPD
spd_info->flags = 0
spd_info->saddr = 200.200.200.154
spd_info->smask = 255.255.255.255
spd_info->daddr = 20.20.20.2
spd_info->dmask = 255.255.255.255
spd_info->spi = a85d510
del spd for 200.200.200.154/32 -> 20.20.20.2/32, 0xa85d510 OK!
```



`vpnctl ipsec4 del_spd [src_addr] [src_mask] [dst_addr] [dst_mask] [spi]`

KEY 교환 상태 확인 – **vpnctl ike_statusall (ike_status)**

Center 확인

```
[root@NGF2000_B ~]# vpnctl ike statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.14.90-1.34217, x86_64):
  uptime: 89 minutes, since Jan 31 14:46:37 2019
  malloc: sbrk 2703360, mmap 0, used 986848, free 1716512
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 75
  loaded plugins: charon aria cast6 lea rc2 md4 has160 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem openssl fips-prf gmp curve25519 xcbc cmac hmac sqlite attr kernel-netlink resolve socket-default stroke vici updown eap-identity
eap-md5 eap-mschapv2 eap-radius xauth-generic unity counters
Listening IP addresses:
  192.168.10.10
  100.100.100.100
  40.40.40.11
  30.30.30.11
  11.11.0.2
IKE daemon state:
  IPv4: RUNNING
  IPv6: RUNNING
Log configuration:
  ipsec_event_log: Enabled
Connections:
  B-secui00: %any...30.30.30.10 IKEv2, dpddelay=30s
  B-secui00: local: [secui00] uses pre-shared key authentication
  B-secui00: remote: uses pre-shared key authentication
  B-secui00: child: 0.0.0.0/0 === 0.0.0.0/0 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
  B-secui00[22]: ESTABLISHED 33 minutes ago, 30.30.30.11[secui00]...30.30.30.10[___CENTER___]
  B-secui00[22]: IKEv2 SPIs: c96e68098b41c8b1_i* 21d7e9e80ac86966_r, rekeying in 40 hours
  B-secui00[22]: IKE proposal: ARIA_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  B-secui00[29]: INSTALLED, TUNNEL, reqid 21, ESP SPIs: 075283e6_i 56fbb63c_o
  B-secui00[29]: ARIA_CBC_128/HMAC_SHA2_256_128, 50048 bytes_i (782 pkts, 3s ago), 50048 bytes_o (782 pkts, 3s ago), rekeying in 18 hours
  B-secui00[29]: 20.20.20.1/32 20.20.20.2/32 20.20.20.3/32 === 200.200.200.154/32
```

Branch 확인

```
[root@BLUEMAX ~]# spdshow
[ IPsec4 ]
  1 : 10.10.10.1/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  2 : 10.10.10.1/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  3 : 10.10.10.2/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  4 : 10.10.10.1/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  5 : 10.10.10.2/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  6 : 10.10.10.3/32 -> 20.20.20.1/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  7 : 10.10.10.2/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  8 : 10.10.10.3/32 -> 20.20.20.2/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
  9 : 10.10.10.3/32 -> 20.20.20.3/32 : (30.30.30.11, 0xffffffff, ESP) : P(50/A) : Ref(0) : Flag(IV(0x00002400))
 10 : 200.200.200.154/32 -> 20.20.20.1/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
 11 : 200.200.200.154/32 -> 20.20.20.2/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))
 12 : 200.200.200.154/32 -> 20.20.20.3/32 : (30.30.30.11, 0x075283e6, ESP) : P(50/A) : Ref(0) : Flag(V(0x00002000))

[ IPsec6 ]
[root@BLUEMAX ~]# mp
[ IPsec4 ]

1- ID : C-secui00
1- Out : (30.30.30.11, 0x075283e6, ESP), timer(0n), priority(50/active)
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.3/32
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.2/32
1- Policy: (SD) 200.200.200.154/32 -> 20.20.20.1/32
1- Etc : dpd(0) oooooooooooooooooo V quantum(1) mp_hash[980], flags(0x00004101), Session LB
1- DLD : [1] 30.30.30.10 -> 30.30.30.11, traf(716/77328), quantum(0 ~ 1), dld[(358/358), (358/358)]
1- DLD : [1] rtt : 1 1 1 0 [1] 0 1 1 2 0 0 2 1 1 is_valid(all_valid/0x3) is_active(active/0x1)

[ IPsec6 ]
[root@BLUEMAX ~]# vpnctl ike status
Security Associations (1 up, 0 connecting):
  C-secui00[21]: ESTABLISHED 30 minutes ago, 30.30.30.10[___CENTER___]...30.30.30.11[secui00]
  C-secui00[29]: INSTALLED, TUNNEL, reqid 21, ESP SPIs: 56fbb63c_i 075283e6_o
  C-secui00[29]: 200.200.200.154/32 === 20.20.20.1/32 20.20.20.2/32 20.20.20.3/32
```

[별첨] 보안 강도 별 권고 암호 알고리즘 (출처 – KISA)

미국, 일본, 유럽 및 국내에서는 아래와 같은 암호 알고리즘 이용을 권고함

- 출처: KISA
- 자료: 암호 알고리즘 및 키 길이 안내서_2013)

분류		NIST(미국) (2012)	CRYPTREC(일본) (2011)	ECRYPT(유럽) (2011)	국내 ¹ (2012)
대칭키 암호 알고리즘		AES 2TDEA ² 3TDEA ²	AES 3TDEA Camellia Cipherunicorn-A Cipherunicorn-E Hierocrypt-3 Hierocrypt-L1 MISTY1 SC2000	AES 2TDEA 3TDEA KASUMI Blowfish1) ¹	SEED ARIA HIGHT
해쉬함수		SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256 SHA-384/512 RIPEMD-160	SHA-1 SHA-224/256 SHA-384/512 RIPEMD-128/160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
공개키 암호 알고 리즘	키 공유용	DH ECDH MQV ECMQV	DH ECDH PSEC-KEM	ACE-KEM PSEC-KEM RSA-KEM	DH ECDH
	암 · 복호화용	RSA	RSAES-OAEP RSAES-PKCS1(v1.5)	RSAES-OAEP	RSAES-OAEP ³
	전자 서명용	RSA DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSASSA-PKCS1(v1.5) ³ RSASSA-PSS ³ KCDSA ECDSA EC-KCDSA

해시 함수

- 출처: KISA
- 자료: 암호 알고리즘 및 키 길이 안내서_2013)

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	SHA-1 SHA-224/256/ 384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
112 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
128 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
192 비트 이상	SHA-256/ 384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-256/384/512
256 비트 이상	SHA-256/ 384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512

대칭키 암호 알고리즘

- 출처: KISA
- 자료: 암호 알고리즘 및 키 길이 안내서_2013)

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	AES-128/192/256 2TDEA 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 2TDEA 3TDEA KASUMI Blowfish1) ¹	SEED HIGHT ARIA-128/192/256
112 비트 이상	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 Blowfish KASUMI 3TDEA	SEED HIGHT ARIA-128/192/256
128 비트 이상	AES-128/192/256	AES-128/192/256 Camellia-128/192/256 MISTY1	AES-128/192/256 KASUMI Blowfish	SEED HIGHT ARIA-128/192/256
192 비트 이상	AES-192/256	AES-192/256 Camellia-192/256	AES-192/256 Blowfish	ARIA-192/256
256 비트 이상	AES-256	AES-256 Camellia-256	AES-256 Blowfish	ARIA-256