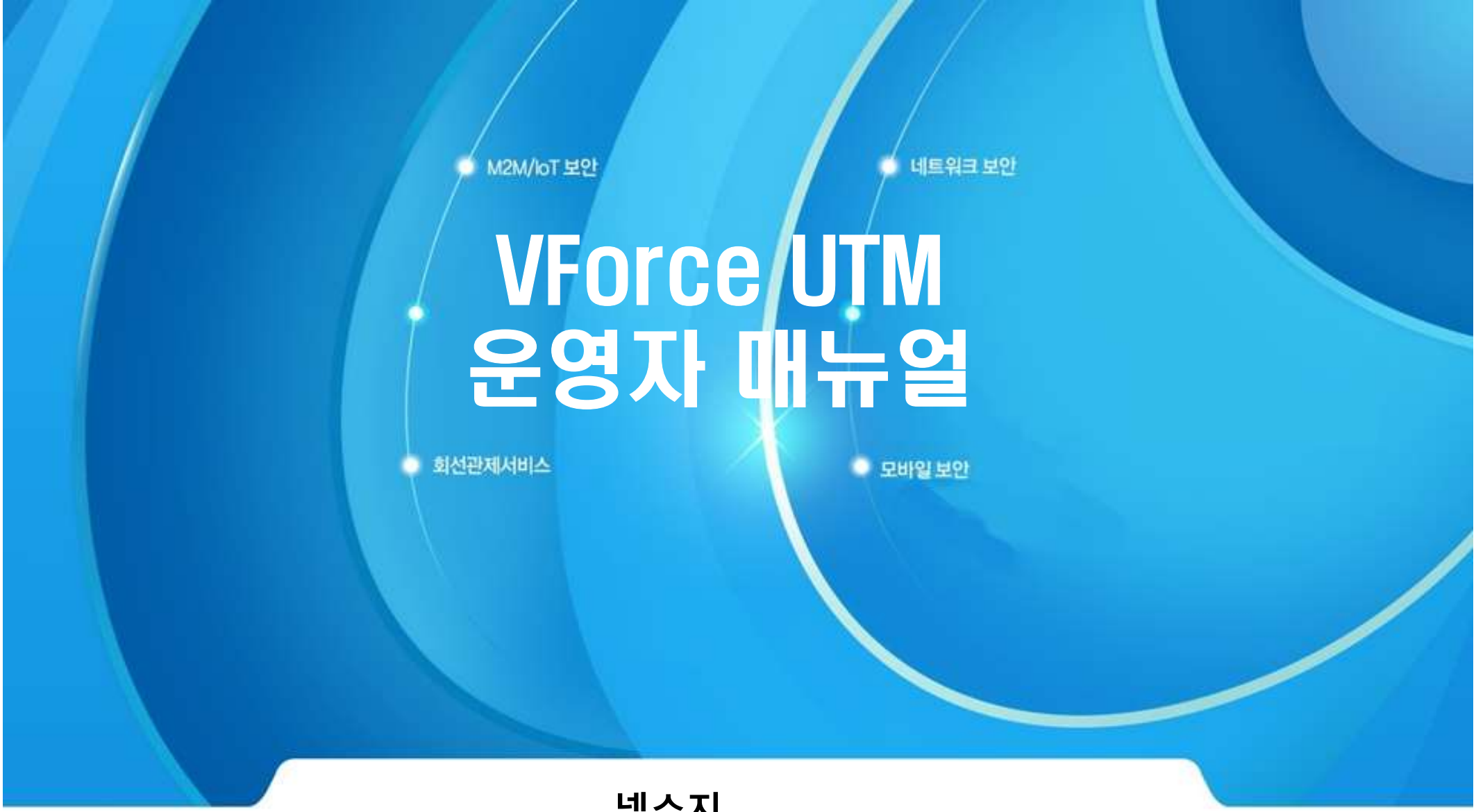


넥스지

NexG
넥스지

목 차

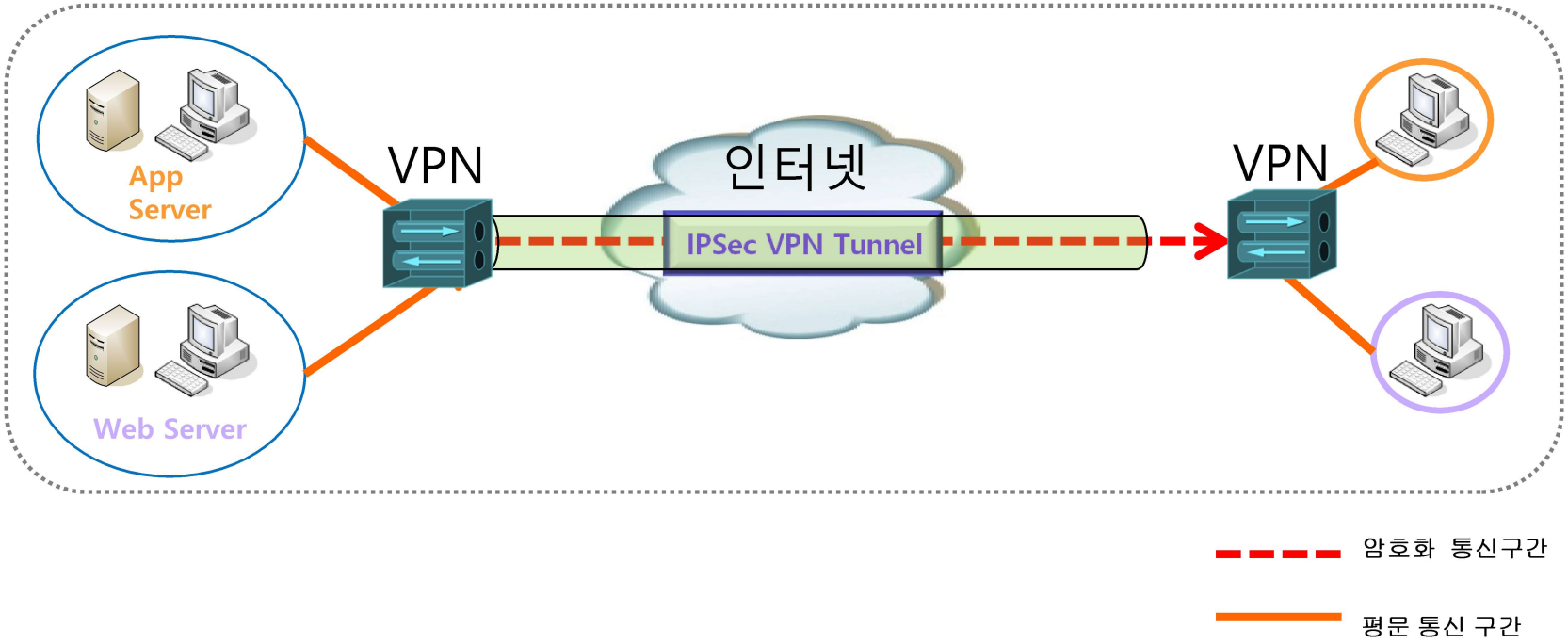
1 VPN 일반

1-1 VPN 개념
1-2 VPN 이해

1-1 VPN 개념

가상사설망 (VPN : Virtual Private Network)

공중 네트워크를 사설 네트워크로 구성하여 사용함으로써, 비용절감 및 보안성이라는 장점을 갖고 있는 기술



1-1 VPN 개념

일반적인 개념

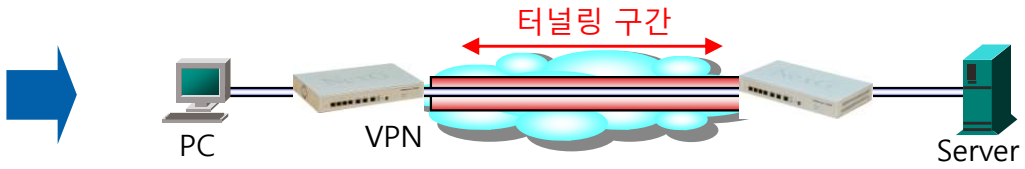
- VPN peer 사이의 가상 경로
- 인터넷 상에서 외부로부터 영향을 받지 않는 가상의 구간

기술적인 개념

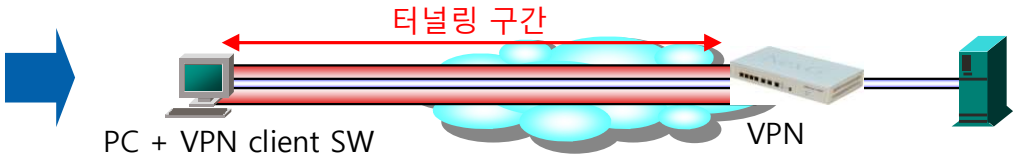
- Tunnel = Encapsulation
- 패킷에 대해 암호화, 인증, 무결성 기술이 적용되는 구간
- VPN peer 사이에 서로 약속된 프로토콜로 세션 구성 (터널링 구성)
- 송신단 : 소스 패킷을 약속된 프로토콜로 encapsulation 해서 송신 – 암호화, 인증 적용
- 수신단 : 인터넷을 통해 전달된 패킷을 decapsulation 해서 실제 목적지로 전달 – 복호화, 인증 적용

Tunnel (터널) 구성 예

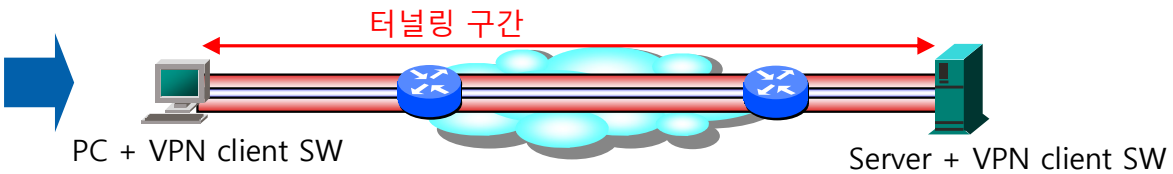
- VPN Gateway to Gateway 터널링



- VPN Gateway to Client 터널링



- VPN Client to Client 터널링



1-1 VPN 개념

Security Gateway	OSI Layer	Tunnel Protocol
Application Gateway	(L7) Application	
	(L6) Presentation	
Session Layer Proxy	(L5) Session	Socks , SSL
	(L4) Transport	
Packet Filtering	(L3) Network	IPSec, VTP
	(L2) Data Link	L2F, PPTP, L2TP
	(L1) Physical	

Data Link Layer VPN

- L2F (Layer2 Forwarding) ➔ Cisco 프로토콜
  - Domain name과 User ID를 바탕으로 인증과정 구현
  - Compulsory Tunnel 모드만 지원 (Gateway to Gateway)
- PPTP (Point to Point Tunneling Protocol) ➔ Microsoft 프로토콜
  - Voluntary (Gateway to Client), Compulsory (Gateway to Gateway) Tunnel 모드 모두 지원
  - 데이터 암호화 지원 안함
  - PPP를 이용하면서, GRE헤더로 다시 encapsulation 함
- L2TP (Layer2 Tunneling Protocol) ➔ Cisco + Microsoft 프로토콜
  - Cisco의 L2F, Microsoft의 PPTP 수용
  - Remote client에 IP를 할당하기 위해, NCP(Network Control Protocol) 사용
  - 데이터 암호화 지원 안함
  - 데이터 암호화 지원하기 위해, L2TP with IPsec 으로 발전

Network Layer VPN

- VTP (Virtual Tunneling Protocol) ➔ Nortel Networks 프로토콜
  - Frame Relay 망에서 회선 속도를 보장하기 위해서 사용
  - 타 장비와 호환 불가능
- IPsec (IP Security) ➔ IETF 표준
  - 인증 기반 : AH (Authentication Header) 프로토콜 사용
  - 암호화 기반 : ESP (Encapsulating Security Payload) 프로토콜 사용
  - 키교환 : Manual 또는 IKE (Internet Key Exchange) 프로토콜 사용
  - Layer3 기반의 가장 강력한 암호화 터널링 기술
  - 표준 IPsec 기반의 장비간에 VPN 터널 연동 가능

1-2 VPN 이해

IKE(Internet Key Exchange)

- IKE는 KEY Exchange, Security Services 협상 등을 ISAKMP를 사용
- IKE는 여러 Exchange와 각각의 Exchange에 적용될 옵션에 대해 정의
- IKE는 ISAKMP의 두 Phase를 사용한다.(Phase 1, Phase 2)
  각 phase마다 별도의 SA가 설정되며, 이 SA마다 쌍방은 상호 인증 후 공유 마스터 키를 생성

IKE Phase

- **Phase 1 (ISAKMP SA 설정과정)**

  - Phase 2에서 사용될 IKE 메시지들을 보호하기 위한 마스터 키를 설정하고 상호인증을 수행

- **Phase 2 (IPSec SA 설정과정)**

  - 실제 전송될 IPSec 패킷을 암호화 하기 위한 협상 과정

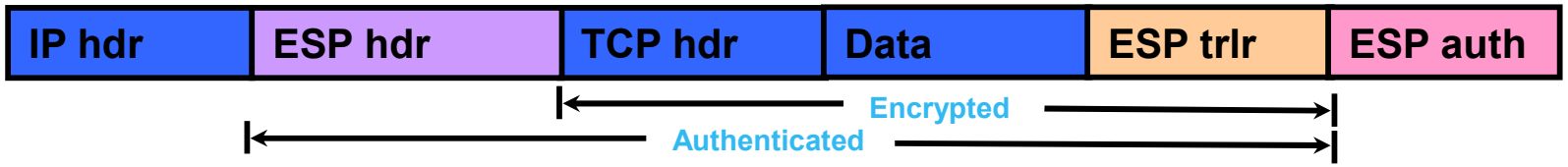
ESP(Encapsulation Security Payload)

- ESP 헤더와 트레일러 영역을 사용하여 IP의 데이터부분에 대한 암호화를 제공
- ESP AH영역을 사용하여 ESP 패킷 영역에 대한 메시지 인증 기능 제공
- IP 헤더영역에 대한 무결성은 제공하지 않음

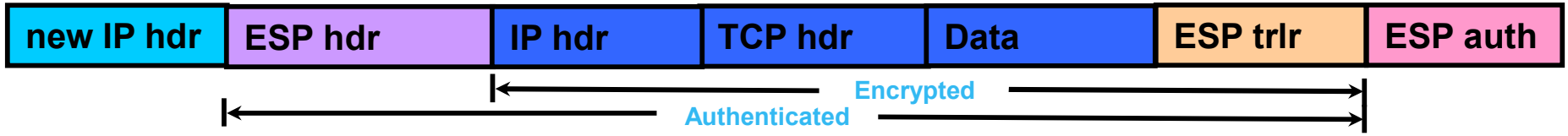
- **적용방법**
  - ESP 단독
  - ESP+AH 조합된 형태
- **보안 서비스**
  - host vs. host
  - host vs. 보안 gateway

Original IP Packet

ESP Transport Mode Protected Packet

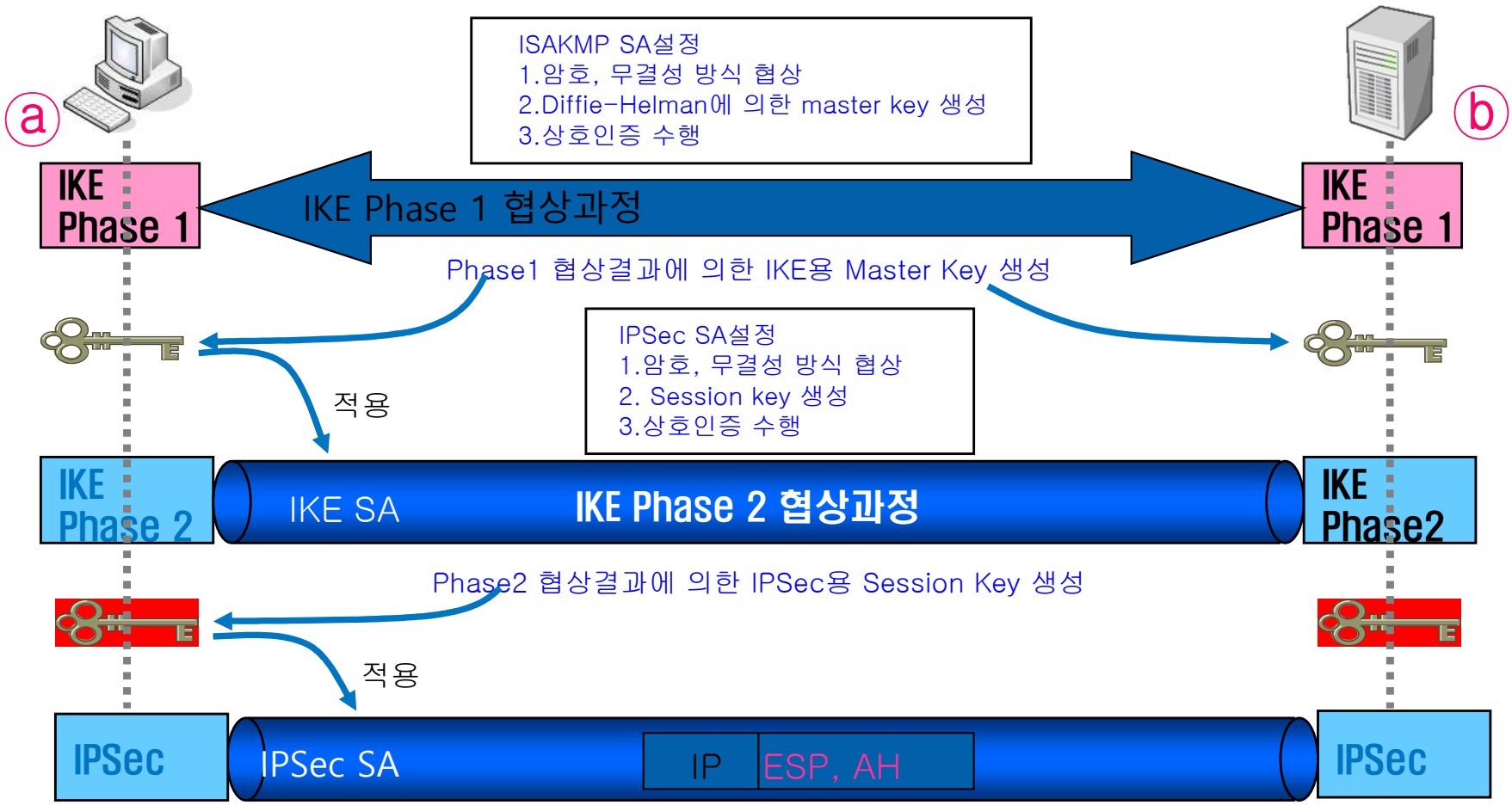


ESP Tunnel Mode Protected Packet



1-2 VPN 이해

IKE 협상 과정(표준)



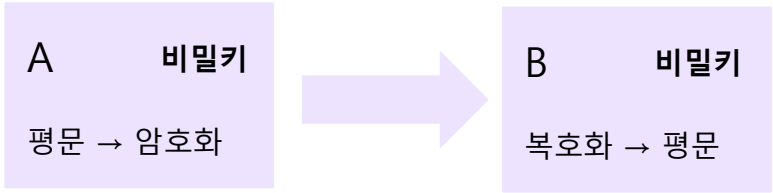
1-2 VPN 이해

Header	AH(Authentication Header)	▪ 데이터에 대한 인증과 무결성 보장 ▪ 데이터 출처에 대한 인증 서비스 제공 ▪ 단독 또는 ESP와 함께 사용
	ESP(Encapsulation Security Payload)	▪ 데이터에 대한 기밀성과 무결성을 보장 ▪ 데이터 출청에 대한 인증 서비스 제공
Key Exchange	IKE(ISKMP/Oakely) Diffie-Helman	▪ 사용할 프로토콜과 알고리즘, 키에 동의 하고 협상 ▪ 통신하는 상대방을 인증 ▪ 키 등의 보안속성을 협상하여 공유 ▪ 1단계 – 안전한 통신 채널을 설정하는 단계 (Main Mode, Aggressive Mode) ▪ 2단계 – 1단계의 SA를 기반으로 키를 재생성하는 단계 (Quick Mode)
Modes	Transport	▪ End-to-End 보안을 위해 사용(호스트에서 구현가능) ▪ IP헤더를 제외한 IP 패킷의 데이터를 보안 ▪ Traffic Analysis 가능
	Tunnel	▪ 전체 IP 패킷을 보안 ▪ Traffic Analysis 불가능 ▪ 비공인 IP 사용이 가능
Encryption		▪ DES, 3DES, RC4, IDEA

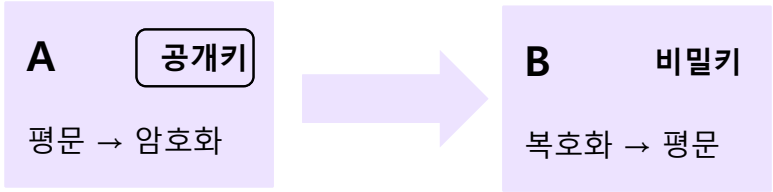
1-2 VPN 이해

암호화 형식

- **비밀키 알고리즘** - 대칭키(Symmetric) 암호화 방식
  - 동일한 키를 사용하여 암호화와 복호화를 수행
  - 속도가 빠르지만 키 분배와 관리가 어려움
  - 종류: DES, 3DES, SEED, NEAT, NES, AES 등

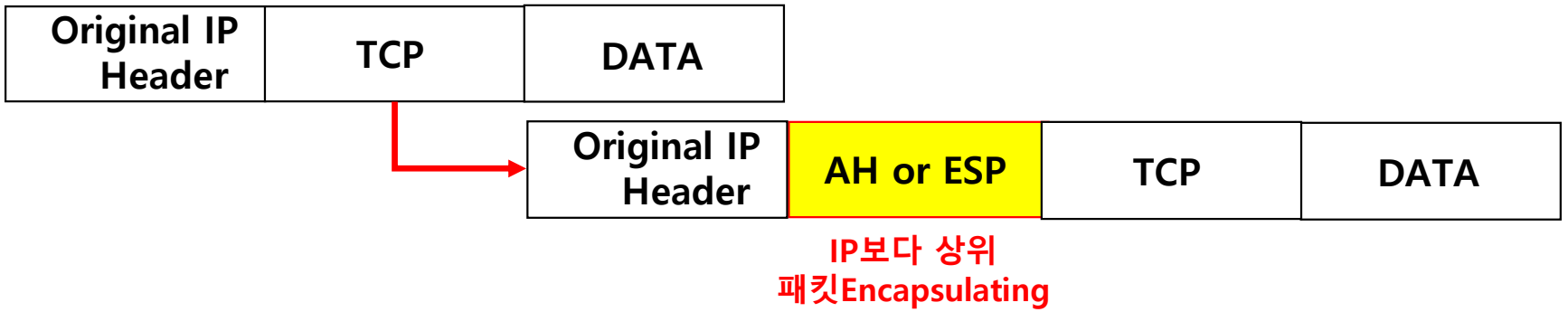


- **공개키 알고리즘** - 비대칭키(Asymmetric) 암호화 방식
  - 암호화와 복호화의 키가 서로 다름
  - 속도가 느리지만 키 분배 및 관리가 용이
  - 종류: RSA, Diffie-Helman

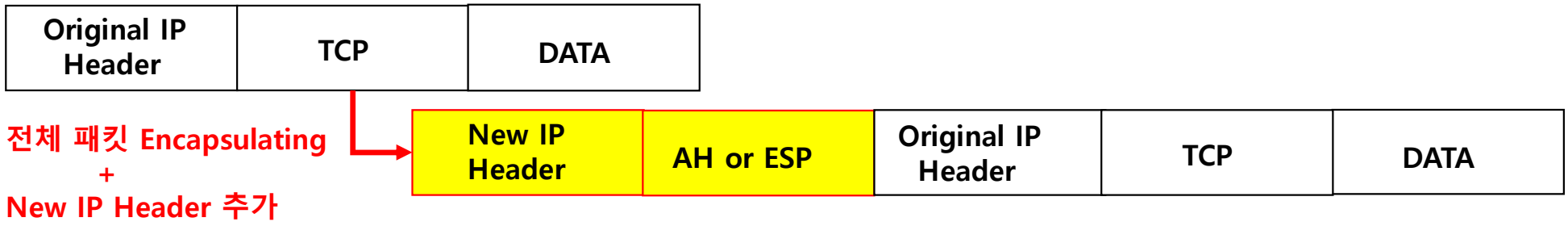


1-2 VPN 이해

✔ 트랜스포트 모드 (Transport Mode) 일 경우 ➔ IP 보다 상위 프로토콜에 대한 보호

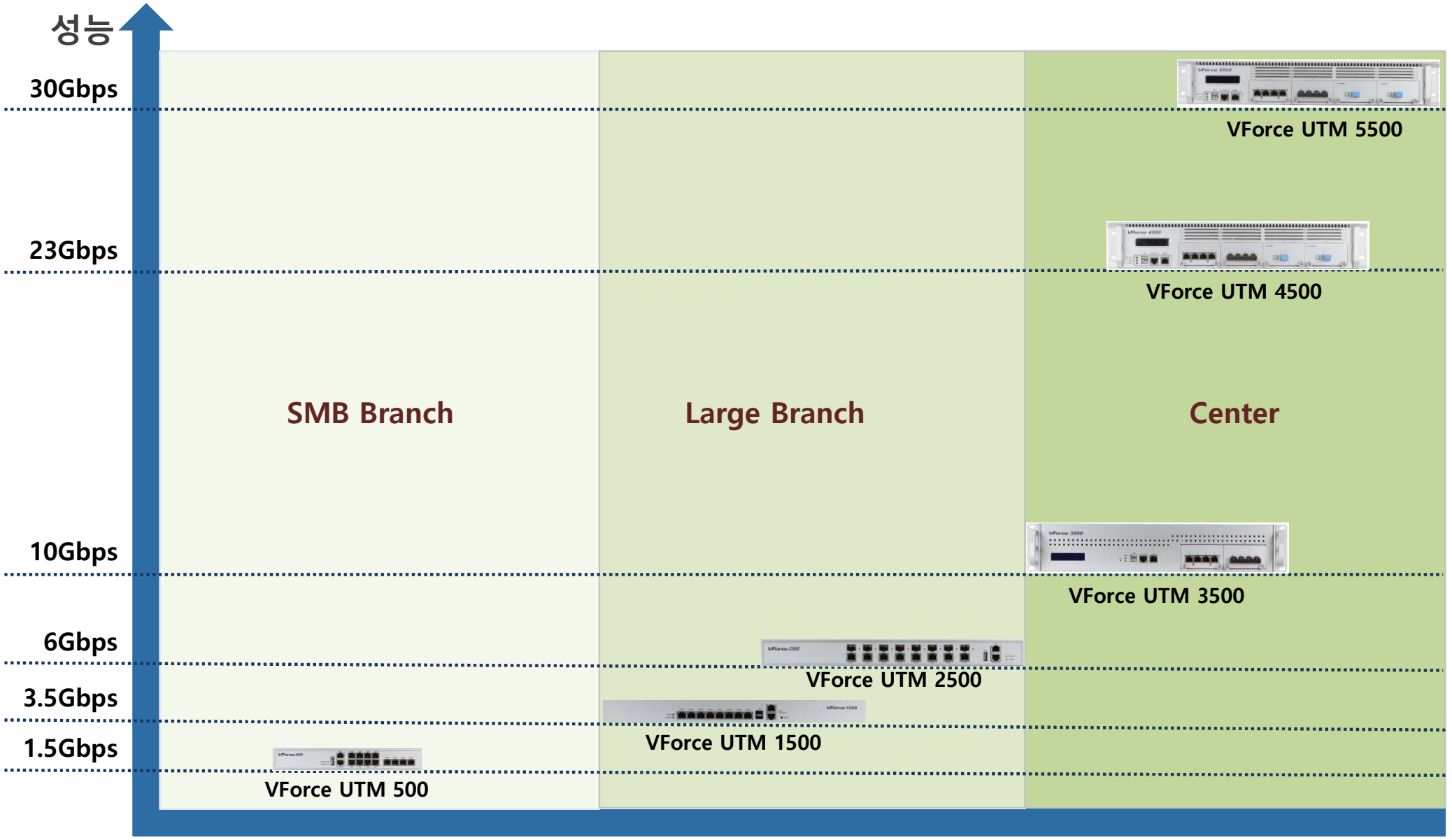


✔ 터널 모드 (Tunnel Mode) 일 경우 ➔ IP 패킷 전체 보호



2 제품소개

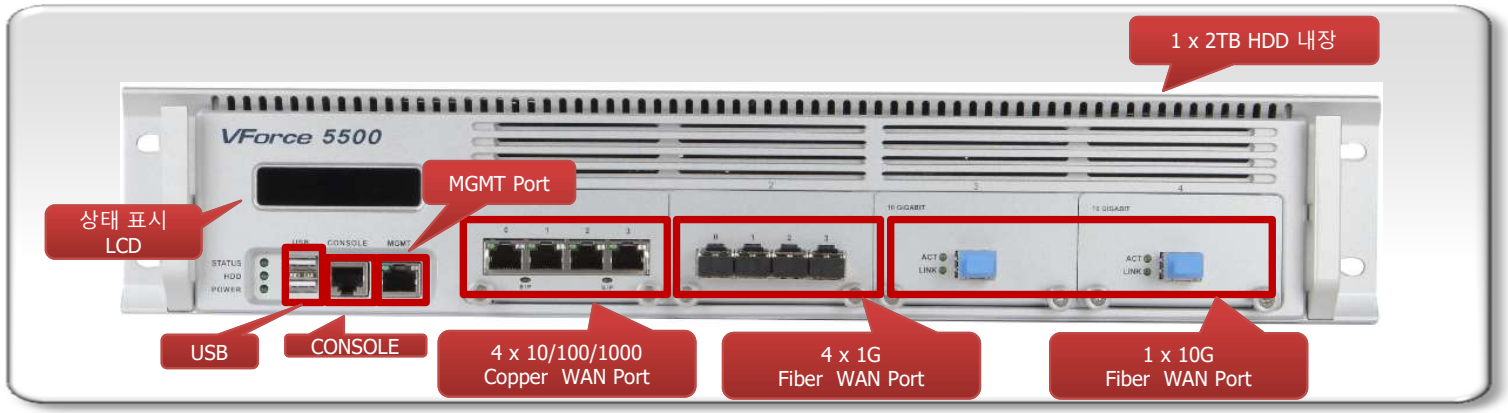
2-1 라인 업



* RFC2544 VPN(AES-256) MAX Performance 기준

2-2 H/W 소개

◈ VForce 5500

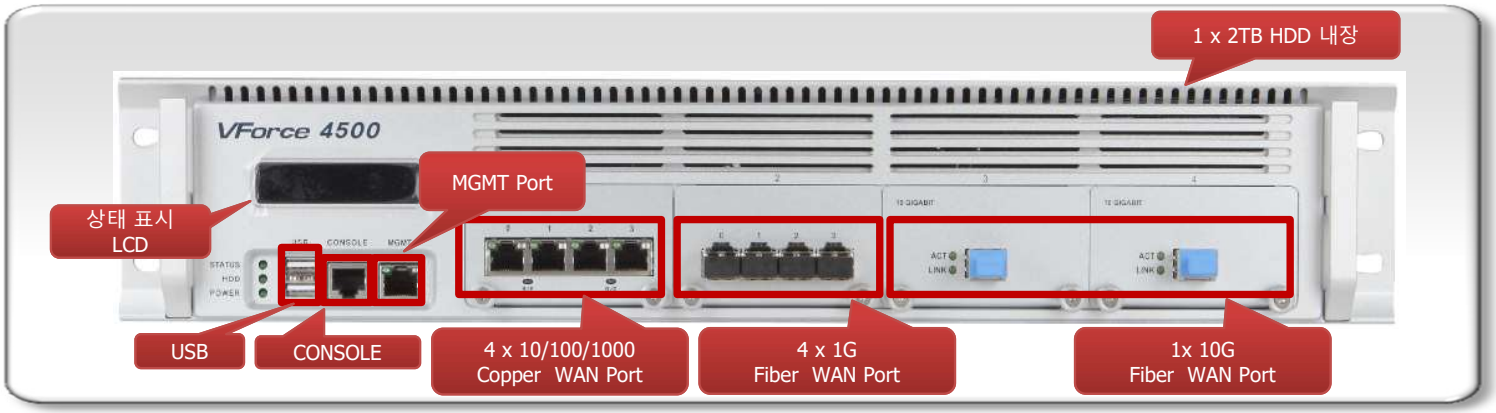


ITEM	CONTENT
CPU / Core	NPU / 32 Cores
Memory	32GB
Compact Flash	4GB
Storage Capacity	2 TB
Interface	10/100/1000 BASE-T or 1000 BASE-X * 16P(MAX)
	10G BASE-R * 4P(MAX)
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	20,000,000
Max VPN Tunnel	190,000
VPN Throughput	30 Gbps
Firewall Throughput	40 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	Center VPN

2-2 H/W 소개

◈ VForce 4500

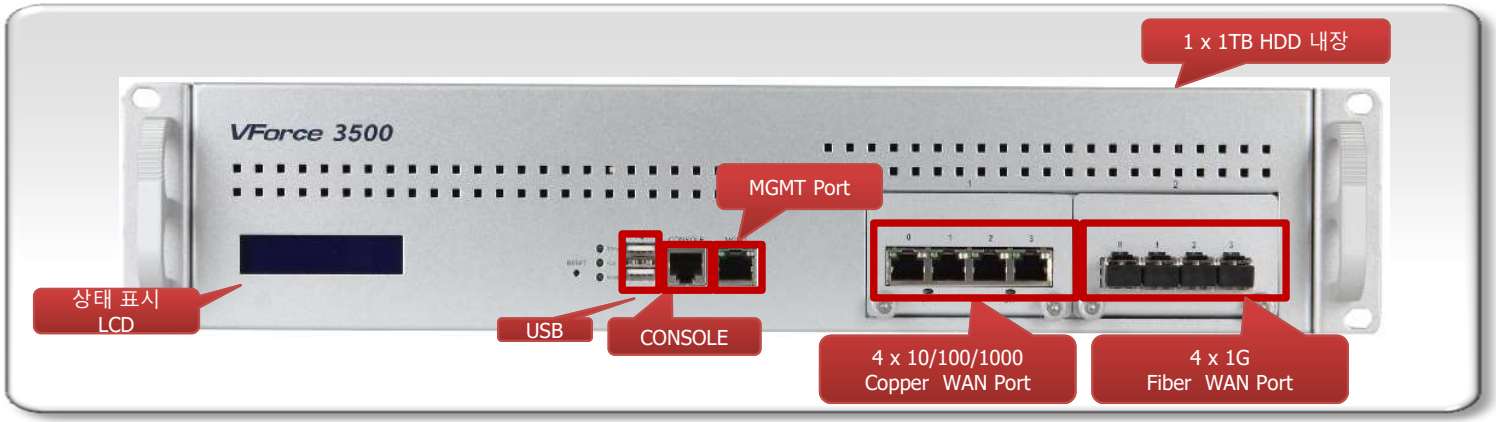


ITEM	CONTENT
CPU / Core	NPU / 24 Cores
Memory	16GB
Compact Flash	4GB
Storage Capacity	2 TB
Interface	10/100/1000 BASE-T or 1000 BASE-X * 16P(MAX)
	10G BASE-R * 4P(MAX)
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	10,000,000
Max VPN Tunnel	120,000
VPN Throughput	23 Gbps
Firewall Throughput	30 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	Center VPN

2-2 H/W 소개

◈ VForce 3500

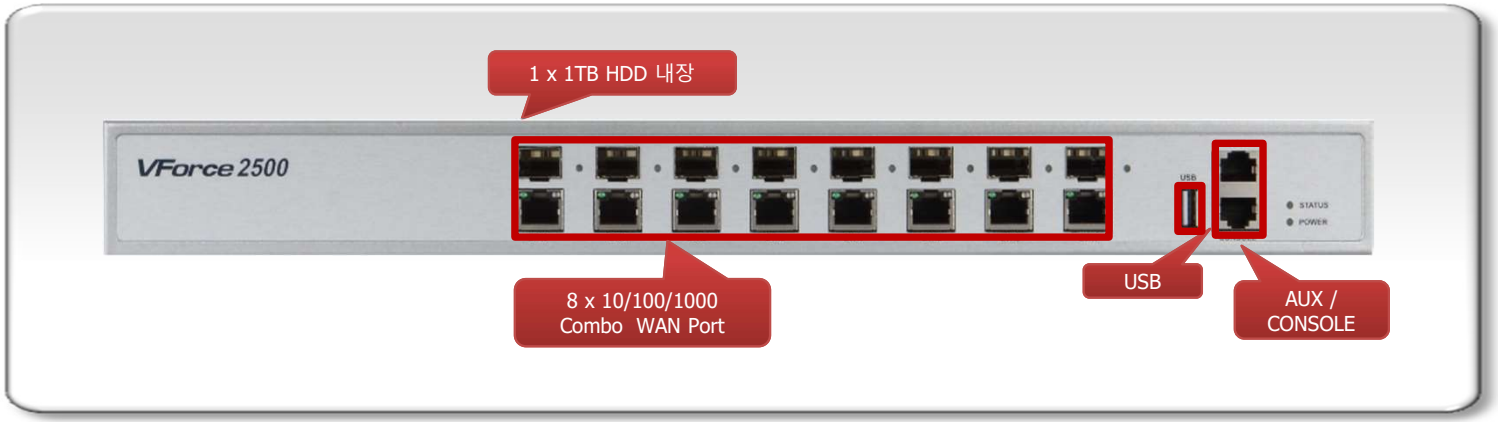


ITEM	CONTENT
CPU / Core	NPU / 10 Cores
Memory	8GB
Compact Flash	4GB
Storage Capacity	1 TB
Interface	10/100/1000 BASE-T or 1000 BASE-X * 8P(MAX)
	10G BASE-R * 2P(MAX)
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	4,000,000
Max VPN Tunnel	40,000
VPN Throughput	10 Gbps
Firewall Throughput	15 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	Center VPN

2-2 H/W 소개

◈ VForce 2500



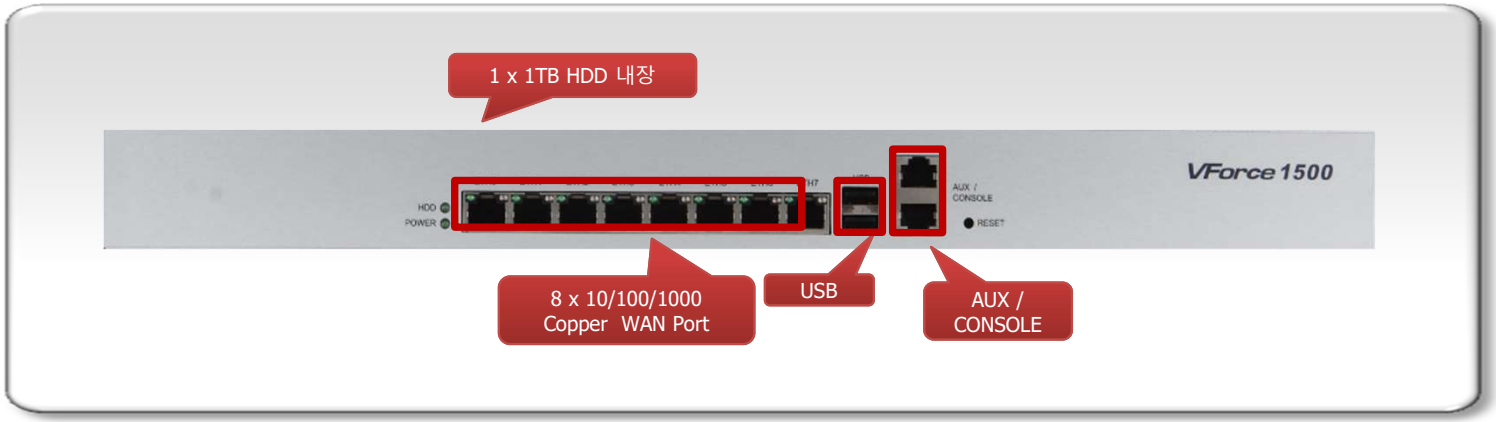
ITEM	CONTENT
CPU / Core	NPU / 6 Cores
Memory	4GB
Compact Flash	4GB
Storage Capacity	1 TB
Interface	10/100/1000 COMBO * 8P
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	2,000,000
Max VPN Tunnel	20,000
VPN Throughput	6 Gbps
Firewall Throughput	8 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	Large Branch

Power Redundant (Option)

2-2 H/W 소개

◈ VForce 1500

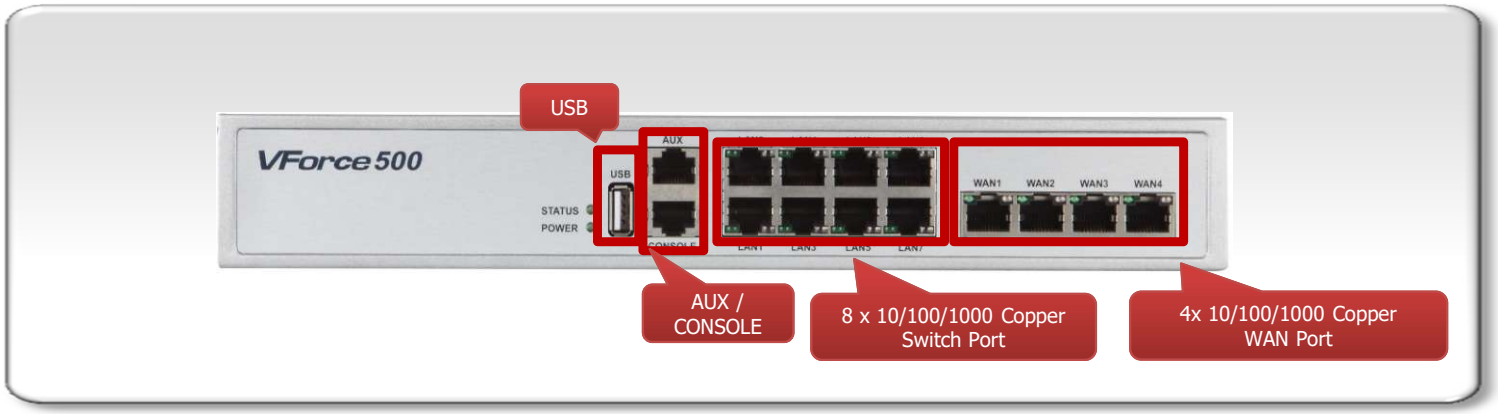


ITEM	CONTENT
CPU / Core	NPU / 4 Cores
Memory	4GB
Compact Flash	4GB
Storage Capacity	500 GB
Interface	10/100/1000 BASE-T * 8P
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	2,000,000
Max VPN Tunnel	20,000
VPN Throughput	3.5 Gbps
Firewall Throughput	4 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	Large Branch

2-2 H/W 소개

◈ VForce 1500



ITEM	CONTENT
CPU / Core	NPU / 2 Core
Memory	4GB
Compact Flash	4GB
Storage Capacity	N/A
Interface	10/100/1000 BASE-T * 4P(WAN) 10/100/1000 BASE-T * 8P(LAN)
지원기능	VPN, 방화벽, IPS, Content Filter, QoS 등

ITEM	CONTENT
OS	자체 OS
Max Concurrent sessions	1,000,000
Max VPN Tunnel	10,000
VPN Throughput	1.5 Gbps
Firewall Throughput	2 Gbps
IPv6	Support
Certification	CC(EAL4), KC
장비등급	SMB Branch

2-2 H/W 소개

VForce NMS는 VForce UTM 시리즈를 모니터링 및 관리하는 솔루션 입니다.

Items	VForce NMS 1000N	VForce NMS 2000N	VForce NMS 3000N
Image			
구성	전용하드웨어/소프트웨어	전용하드웨어/소프트웨어	전용하드웨어/소프트웨어
장비등급	Low	Medium	High
권장 관리 디바이스	1,000대 >	2,000대	3,000대 <
OS	Ubuntu	Ubuntu	Ubuntu
CPU	Intel® Xeon 2.5GHz * 1	Intel® Xeon 2.6GHz * 2	Intel® Xeon 2.8GHz * 2
RAM	4GB DDR3	8GB DDR3	16GB DDR3
HDD	2TB SATA	2TB(RAID 1) SATA	2TB(RAID 1) SATA
RAID	N/A	HW RAID 0,1,5,6,10,50,60	HW RAID 0,1,5,6,10,50,60
Interface	2 X 10/100/1000 BASE-T	2 X 10/100/1000 BASE-T	2 X 10/100/1000 BASE-T
Redundant Power	X	O	O
SIZE	1U	2U	2U

2-3 Specifications

Hardware Specifications

		VForce UTM 500	VForce UTM 1500	VForce UTM 2500	VForce UTM 3500	VForce UTM 4500	VForce UTM 5500
Chassis							
CPU		2 Cores	4 Cores	6 Cores	10 Cores	24 Cores	32 Cores
Memory		4 GB	4 GB	4 GB	8 GB	16 GB	32 GB
Storage	HDD	-	500 GB	1TB	1TB	2TB	2TB
	Flash	4 GB					
Network Interface	10/100/1000 Base-TX	4	8	-	MAX 8	MAX 16	MAX 16
	10/100/1000 Combo	-	-	8	-	-	-
	10/100/1000 LAN Switch	8	-	-	-	-	-
	1000 Base-X	-	-	-	MAX 8	MAX 16	MAX 16
	10G Base-R	-	-	-	MAX 2	MAX 4	MAX 4
	Module Slot	-	-	-	2	4	4
	BYPASS	0/0	1(opt)/0	1(opt)/0	Option	Option	Option
	MGMT Ports	0	0	0	1	1	1
	Console	1 (RJ-45)					
Throughput (RFC2544)	VPN(Gbps, AES-256)	1.5	3.5	6	10	23	30
	Firewall(Gbps)	2	4	8	15	30	40
VPN Tunnel		10,000	20,000	20,000	40,000	120,000	190,000
Concurrent Session		1,000,000	2,000,000	2,000,000	4,000,000	10,000,000	20,000,000
Power		Single			Redundant		
Dimensions(WxHxD mm)		300 x 44 x 180	440 x 44 x 315	440 x 44 x 405	430 x 88 x 455	430 x 510 x 88	430 x 510 x 88
Weight(Kg)		1.9	4	6	9	11	12
Rack mountable		1U Mini	1U	1U	2U	2U	2U
Temperature		0 ~ 40 ℃					
Humidity		5~90%(non-condensing)					

Expansion NIC Modules	1G Copper	4 Port 1G Copper Module(bypass)	VForce UTM 3500 ~ VForce UTM 5500
	1G Fiber	4 Port 1G Fiber Module(no bypass)	
	10G Fiber	1 Port 10G Fiber Module(no bypass)	

2-3 Specifications

Software Specifications

Firewall

Firewall

- Stateful Inspection
- 5 Tuples (IP/Port/Protocol)
- Zone 기반 정책 지원
- 사용자 기반 정책 지원
- MAC Address 기반 정책 지원
- Object 및 Schedule 기반 정책 지원
- 정책 및 세션 수에 독립적
- 정책 통계 및 검색 지원
- Static, Dynamic NAT
- Excluded, Twice NAT

VPN

Gateway To Gateway

- Crypto H/W 가속기 내장
- Multi-tunnel
- Bonding Tunnel
- Split Tunneling
- IKE Version 1 / 2
- Transport / Tunnel Mode
- Crypto Algorithm
  (3DES, AES128/192/256, SEED, ARIA)
- Integrity Algorithm
  (MD5, SHA1, SHA2)
- DPD (Dead Peer Detection)
- NAT Traversal
- L2 Bridge VPN

Remote Access

- NexG SecureClient
  (PC 및 모바일 환경 지원)
  - Windows Application
    (Windows 7, 8, 8.1, 10 32/64bit 지원)
  - Android App
    (Android version 4.0 이상)
  - iOS : IPsec, PPTP, L2TP over IPsec
- User Authentication
- (ID, Password, 인증서)
- 인증 서버(Radius, LDAP) 연동 지원
- User Grouping / Control

IPS

IPS

- Deep Packet Inspection
- 패턴 매챙 H/W 가속 내장
- 3000+ 시그니처 유지
- Snort Rule Format 지원
- Profile 기반 정책 설정
- PCRE 지원
- Black-list / White-list
- Anti-Evasion
- Anti-Virus(Stream 기반)
  탐지 및 차단

Anti-DDoS

- TCP/UDP/ICMP/DNS/HTTP
- Flooding 방어
- Scan, Sweep 방어
- 시그니처 기반 방어
- 위/변조 행위 기반 방어
- Traffic Limit 기반 방어

Applica-tion Control

- Application 별 행위 제어
- Game, P2P, HTS 제어
- Web Mail, Web Hard 제어
- Instants Messenger 제어
- Streaming, File-type 제어

Contents Filter

Web Filter

- URL 및 URI 확장 검사
- 사용자 정의 DB 필터
- 96개 Web Category DB
  필터 통한 웹 서핑 제어
- KISCOM, Malware,
  Phishing 등 외부 DB 필터

HA

HA

- Active-Active / Active-Standby
- VRRP, IPAT
- LLCF
- L2 Bypass
- Synchronization
  (Policy, Session)

Network

Network

- Route / Bridge Mode
- 802.1Q VLAN Trunk
- 802.3ad LACP
- ECMP Routing
- Policy-based Routing
- RIP, OSPF
- PIM-SM/DM, IGMP
- VoIP(H.323, SIP) 지원
- QoS (보장, 제한, DSCP)
- DHCP Server , Relay, HA
- 3G/LTE 지원
- DDNS 지원
- Secure DNS 지원
- LLDP 지원

IPv6

- IPv6 Routing
- IPv6 Firewall
- IPv6 IPsec
- IPv6 DHCP Server
- 6 to 4, ISATAP

NAC

NAC

- Genian NAC Sensor
- 사용자 기반 접근 통제
- Compliance 강제화
- Genian Policy Center 연동

Management

Manag-ement

- CLI ,Web UI
- Dashboard
- SNMP Version 1 / 2 / 3 지원
- Syslog 전송 지원
- 정책 Export / Import 지원
- 미사용 정책 및 객체 조회
- 통계 및 Report 지원
- 시스템 설정 / Firmware 백업 및
  복구 지원
- VForce NMS 연동

2-4 인증서

KC(Korea Certification)인증서-1

9E12-D5E4-90CA-C0DA

방송통신기자재등의 적합등록 필증

Registration of Broadcasting and Communication Equipments

상호 또는 성명 *Trade Name or Registrant*	한솔넥스지 주식회사
기자재 명칭 *Equipment Name*	UTM
기본모델명 *Basic Model Number*	VForce2500
파생모델명 *Series Model Number*	
등록번호 *Registration No.*	MSIP-REM-NEG-VForce2500
제조자/제조(조립)국가 *Manufacturer/Country of Origin*	한솔넥스지 주식회사 / 중국
등록연월일 *Date of Registration*	2013-07-19
기타 *Others*	

위 기자재는 「전파법」 제58조의2 제3항에 따라 등록되었음을 증명합니다.
It is verified that foregoing equipment has been registered under the Clause 3, Article 58-2 of Radio Waves Act.

2014년(Year) 04월(Month) 15일(Date)

국립전파연구원장 국립전파연구원장인

Director General of National Radio Research Agency

※ 적합등록 방송통신기자재는 반드시 "적합성평가표시"를 부착하여 유통하여야 합니다.
위반시 과태료 처분 및 등록이 취소될 수 있습니다.

67D2-1842-C989-A1C2

방송통신기자재등의 적합등록 필증

Registration of Broadcasting and Communication Equipments

상호 또는 성명 *Trade Name or Registrant*	한솔넥스지 주식회사
기자재 명칭 *Equipment Name*	UTM
기본모델명 *Basic Model Number*	VForce3500
파생모델명 *Series Model Number*	
등록번호 *Registration No.*	MSIP-REM-NEG-VForce3500
제조자/제조(조립)국가 *Manufacturer/Country of Origin*	한솔넥스지 주식회사 / 한국
등록연월일 *Date of Registration*	2013-07-24
기타 *Others*	

위 기자재는 「전파법」 제58조의2 제3항에 따라 등록되었음을 증명합니다.
It is verified that foregoing equipment has been registered under the Clause 3, Article 58-2 of Radio Waves Act.

2014년(Year) 04월(Month) 15일(Date)

국립전파연구원장 국립전파연구원장인

Director General of National Radio Research Agency

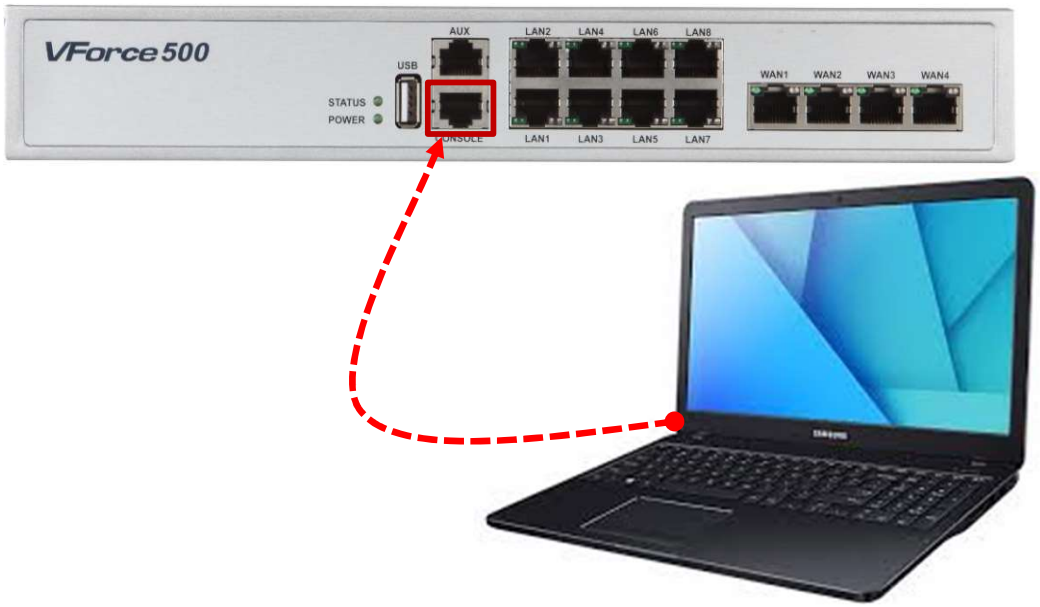
※ 적합등록 방송통신기자재는 반드시 "적합성평가표시"를 부착하여 유통하여야 합니다.
위반시 과태료 처분 및 등록이 취소될 수 있습니다.

3 시스템 접속

3-1 콘솔(Console) 연결
3-2 CLI(telnet, ssh) 연결
3-3 웹(http, https) 연결

3-1 콘솔 (Console) 접속

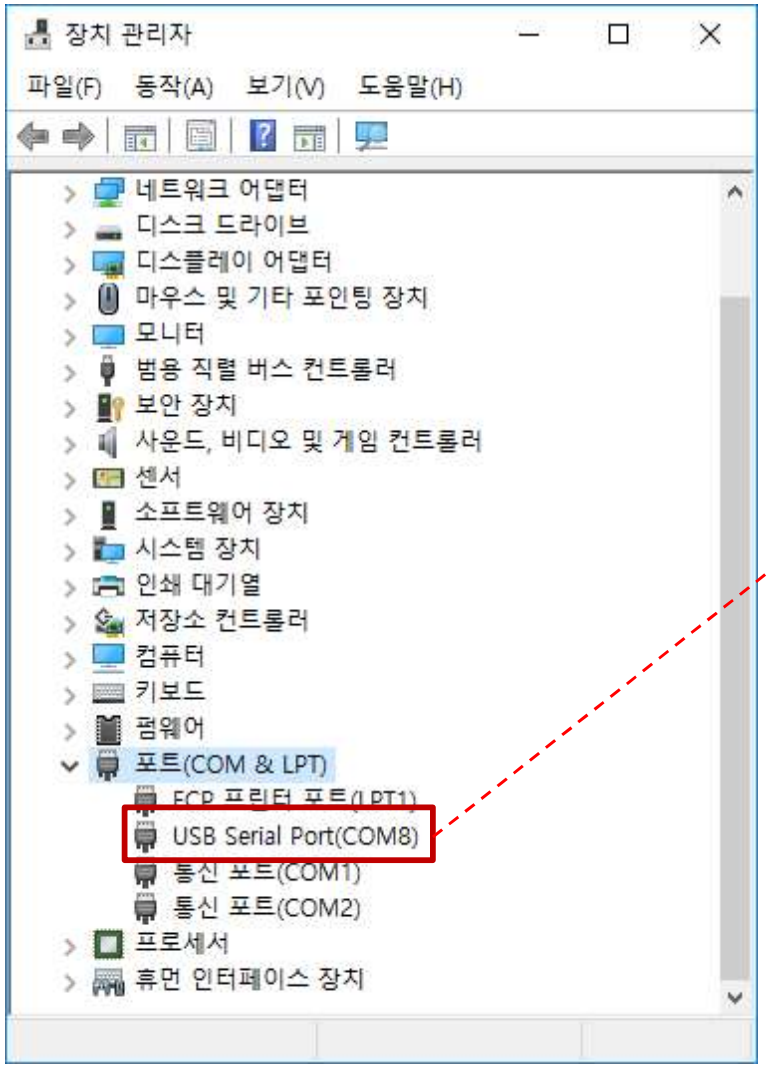
RS-232 케이블

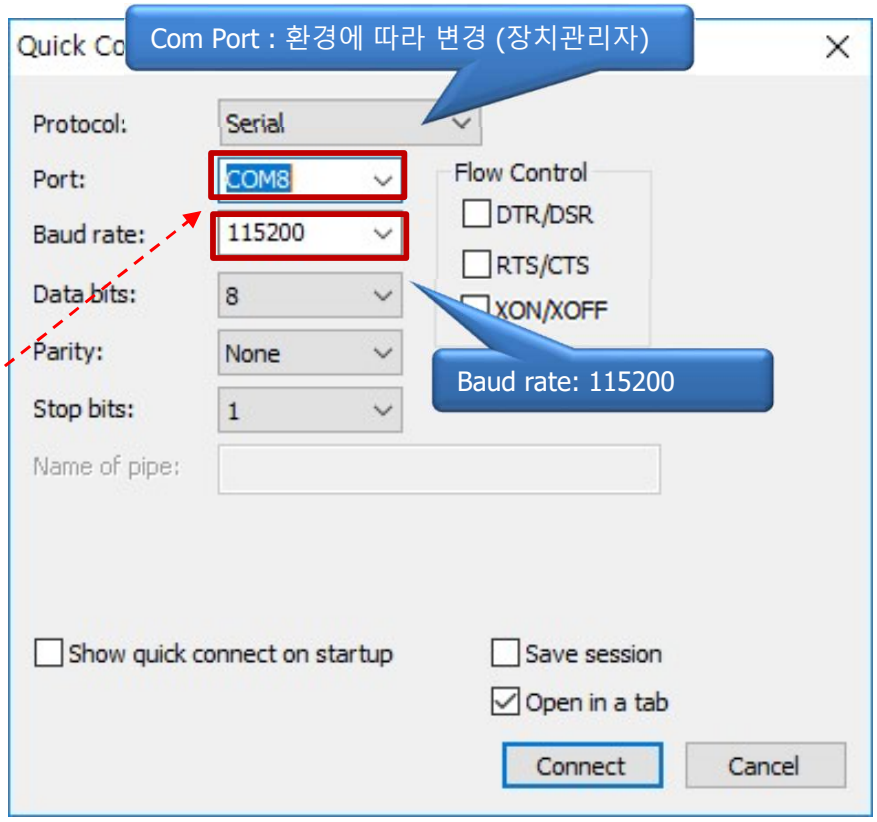


RJ45 Console 케이블 (cisco pin)

- ✓ 콘솔 연결을 위해 RS-232 케이블과 RJ45 Console 케이블을 준비
- ✓ 두 케이블을 결합하여 RJ45 를 장비 콘솔포트에 연결
- ✓ 노트북에 USB 시리얼 드라이버를 설치

3-1 콘솔 (Console) 접속





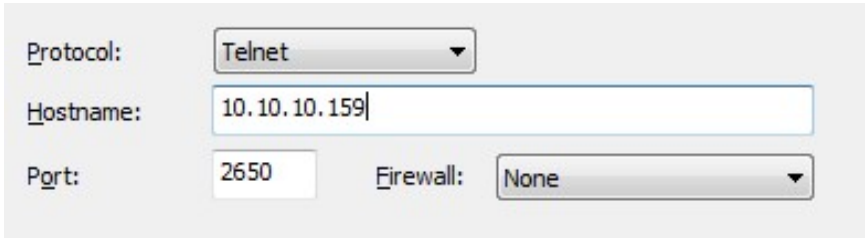
※ Putty, SecureCRT 와 같은 터미널 프로그램을 사용을 권장

3-2 CLI (Telnet, SSH) 접속

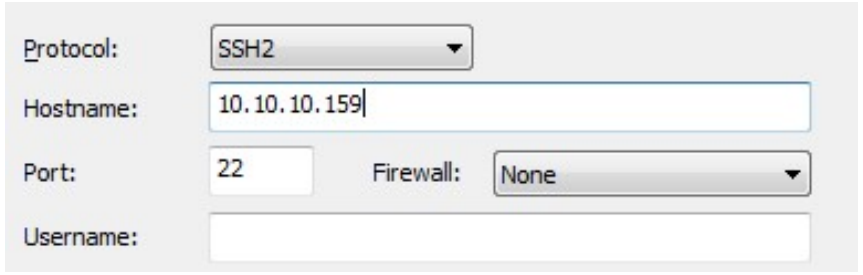
- ✓ CLI(telnet) 접속에 사용되는 포트는 2650 이며 설정을 통해 변경 가능함
- ✓ CLI(ssh) 접속에 사용되는 포트는 22 이며 설정을 통해 변경 가능함

ex) telnet x.x.x.x 2650

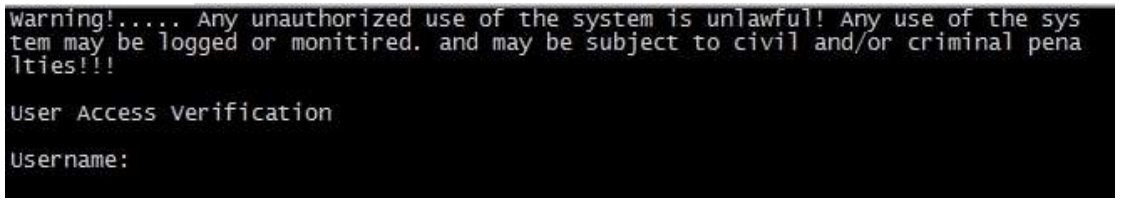
ssh x.x.x.x 22



TELNET



SSH



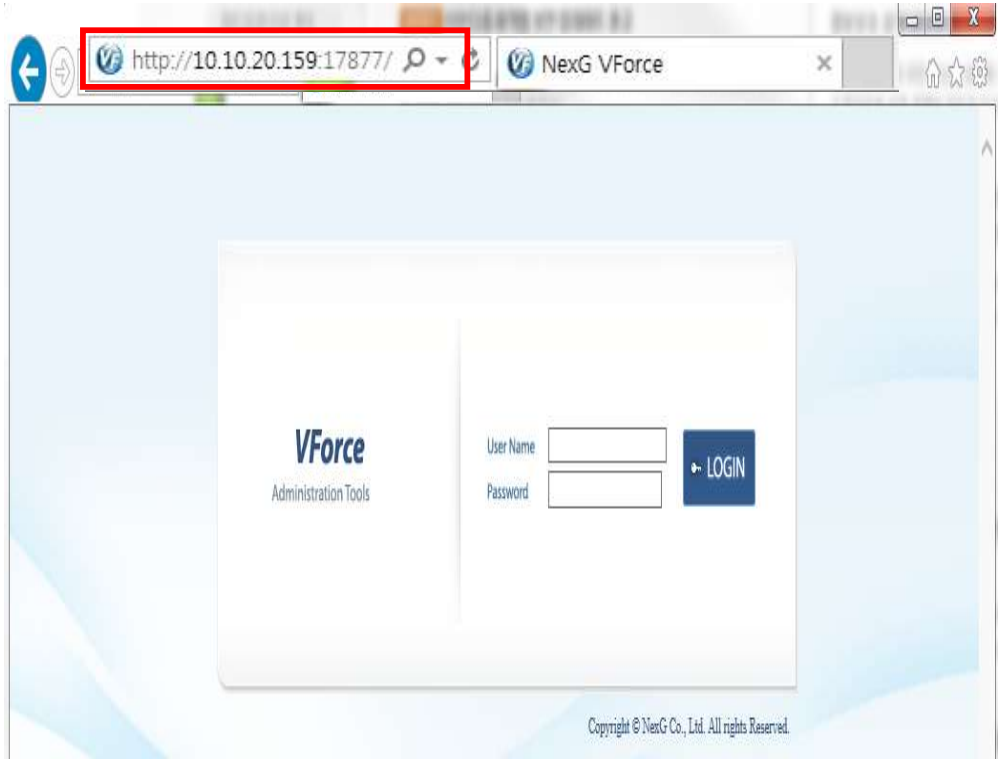
CLI 접속 화면

3-2 WEB (Http, Https) 접속

- ✓ 웹(http) 접속에 사용되는 포트는 17877 이며 설정을 통해 변경 가능함
- ✓ 웹(https) 접속에 사용되는 포트는 17878 이며 설정을 통해 변경 가능함

ex) http:x.x.x.x:17877
https:x.x.x.x:17878

※ Mozila Firefox 를 권장



4 시스템 설정

4-1 CLI 시스템 명령어
4-2 WebUI 시스템 설정

4-1 CLI 시스템 명령어

com1 (115200) – Global Mode

Please press Enter to activate this console.

Hansol NexG VForce Software, Version 4.6-150102
vforce# ?
Exec commands:

boot	Select boot process
bwt	bandwidth test
cat	Concatenate files
cd	Change directory
clear	Reset functions
clock	clock setting
configure	Enter configuration mode
convert-ip-info	refleash convert info
copy	Copy one file from another
crypto	Cryptographic module
debug	Debugging functions (see also 'undebug')
delete	Delete a file or a directory
df	Report file system disk space usage
disable	Turn off privileged mode command
du	Estimate file system usage
enable	Turn on privileged mode command
exit	End current mode and down to previous mode
export-config	export-config
generate	Generate
halt	Halt the system
help	Description of the interactive help system
import-config	import config
ip	Internet Protocol (IP)
ip-static-route	ip-static-route

com1 (115200) – Configuration Mode

Please press Enter to activate this console.

Hansol NexG VForce Software, Version 4.6-150102

vforce# conf t
vforce(config)# ?
Configure commands:

access-list	Add an access list entry
appgw	Application level gateway
archive	Enter configuration archive mode
arp	Address Resolution Protocol (ARP)
banner	Define a login banner
bridge	Bridge group commands
bypass	Bypass Function
checksum	OS Files checksum
clear	Reset functions
clock	Time-of-day clock
crypto	Cryptographic module
cvlan	Configure C-VLAN parameters
debug	Debugging functions (see also 'undebug')
enable	Modify enable password parameters
exit	End current mode and down to previous mode
fib	FIB information
healthcheck	daemon healthcheck
help	Description of the interactive help system
hostname	Set system's network name
interface	Interface information

4-1 CLI 시스템 명령어

com1 (115200) – show 명령어

```
vforce# show ?
  access-list       List IP access lists
  appgw             Application level gateway
  archive           Archive config
  arp               Address Resolution Protocol (ARP)
  bond-group        bonding group
  boot              Boot image
  bridge            Display forwarding information
  bypass            Bypass Function
  cdp               cdp
  check-slot        Check slot type
  checksum          OS Files checksum
  clear             clear memory free
  cli               Show CLI tree of current mode
  clock             show current time
  crypto            Cryptographic module
  debugging         Debugging functions (see also 'undebug')
  delete            Configure logging system
  dhcp              dhcp
  disk0:            disk0 file system
  disk1:            disk1 file system
  eix               EtherIP eXtended
  filesystem        Filesystem information
```

com1 (115200) – show 명령어

```
vforce# show int ?
  IFNAME       Interface name
  switchport   Display the modes of the Layer2 interfaces
  |            Output modifiers
  <cr>

vforce# show interface eth0 ?
  |  Output modifiers
  <cr>

vforce# show ip interface brief
Interface     IP-Address       Status          Protocol     Link-detect
lo            unassigned       up              up           none
eth0          192.168.100.2    up              up           none
eth1          unassigned       up              down         none
eth2          unassigned       up              down         none
eix0          unassigned       up              up           none
vlan0.1       unassigned       up              down         none

vforce# show link
lan1 : Down, 10Base-T/HD, Auto
lan2 : Down, 10Base-T/HD, Auto
lan3 : Down, 10Base-T/HD, Auto
lan4 : Down, 10Base-T/HD, Auto
eth1 : Down, 10Base-T/HD
eth2 : Down, 10Base-T/HD
```

4-1 CLI 시스템 명령어

com1 (115200) – 파이프 출력 기능

vforce# show ? |
  begin   Begin with the line that matches
  exclude Exclude lines that match
  include Include lines that match
  match   Include mode that match

vforce# sh run | **begin** interface eth2
interface eth2
!
interface eth3
!

입력 문자와 매칭 되는 줄부터 화면에 출력함

vforce# sh run | **exclude** !
hostname UTM-1
ip domain-lookup
spanning-tree mode rstp-vlan-bridge
interface eth0

입력 문자가 포함한 줄을 제외한 나머지 줄을 출력함

vforce# sh run | **include** hostname
hostname UTM-1

입력한 문자가 매칭되는 줄을 화면에 출력함

vforce# sh run | **match** vty
line vty
 login

정규 표현식 또는 IP Prefix 으로 설정 블록의 내용을 화면에 출력함

com1 (115200) – 명령어 자동 완성 기능

vforce# configure ?
  replace   Replace configure from archive
  terminal Configure from the terminal

vforce# configure te[TAB]
vforce# configure terminal ?
  <cr>

com1 (115200) – CLI 단축 기능

vforce# configure terminal
vforce(config)# end [CTRL + z]
vforce# conf t
vforce(config)# exit [CTRL + d]
vforce#
vforce# show ip route 1.1.1.33 [CTRL + u]
Vforce#

- [CTRL + a] 현재줄의 제일 첫번째 글자로 이동
- [CTRL + e] 현재줄의 제일 마지막 글자로 이동
- [CTRL + p] 이전 실행 명령어 찾기
- [CTRL + w] 앞에 단어 지우기

4-1 CLI 시스템 명령어

com1 (115200) – Hostname 설정

vforce# conf t
vforce(config)# hostname [호스트네임]
vforce(config)# end
vforce(config)# wr
Building configuration...
[OK]
vforce(config)#

com1 (115200) – 수동 시간 설정

vforce# configure terminal
vforce(config)# clock timezone KST 9
vforce(config)# end
vforce# clock set 10:49:30 28 10 2015
vforce# sh clock
Wed Oct 28 10:49:33 KST 2015

형식 : clock set [시간] [일] [월] [년도]

com1 (115200) – 설정 초기화

vforce# configure reset
Are you sure to reset configuration? [yes/no] y
System Configuration has been reseted

vforce# reload
Proceed with reload? [yes/no] y

init: The system is going down NOW !!

com1 (115200) – NTP 서버 시간 가져오기

vforce# clock ntpdate 203.248.240.140
vforce# sh clock
Tue Apr 28 10:24:36 KST 2015

4-1 CLI 시스템 명령어

com1 (115200) – SSH 서버 설정

vforce# generate crypto key rsa label shinhan ------> *RSA Key 생성*
This command might take a while to process...
vforce# show crypto key mypubkey rsa
This command might take a while to process...
Private key test
    Usage: General purpose
    Algorithm: 2048-bit RSA
    Generated at: 2015-04-29 09:32:05

vforce# configure terminal
vforce(config)# ip ssh rsa keypair-name shinhan
vforce(config)# ip ssh port 22 ----------> *SSH Port 설정*
vforce(config)# ip ssh server ----------> *SSH Server 구동*
vforce(config)# end
vforce# sh ip ssh server status----------> *SSH Server 상태 보기*
SSH server status: Enabled
SSH server port: 22
SSH server keypair: /media/disk0/.ssh/test.prv

com1 (115200) – https(SSL) 서버 설정

vforce# configure terminal
vforce(config)# ip http secure-port 17877
vforce(config)# ip http secure-server

com1 (115200) – 사용자 추가

vforce# configure terminal
vforce(config)# username root secret admin1234
vforce# sh run hosts
!
username root secret 5 1Lqun8/Lq$jKPdIQZ/1jfliQxWV2UMS/

4-1 CLI 시스템 명령어

com1 (115200) – VOS 업그레이드(1)

vforce# copy ? ----------→ *복사 명령어*

```
  disk0:    Copy from disk0: file system
  disk1:    Copy from disk1: file system
  flash:    Copy from flash: file system
  ftp:      Copy from ftp: file system
  http:     Copy from http: file system
  tftp:     Copy from tftp: file system
  usbdisk:  Copy from usbdisk: file system
```

vforce# copy ftp://ID:Password@1.1.1.1/vos-4.6-octeon-150105.bin
disk0:/ /f ----------→ *FTP에 있는 파일을 disk0: 으로 복사*

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
* 생 략 *
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
62641274 bytes transferred
```

vforce# show disk0:/ ----------→ *다운로드 받은 파일 확인*

```
-#- --type--  nlen ---length--- -------date/time-------- name
1   File      25   62641274     Wed Apr 29 09:46:20 2015 vos-4.6-
    octeon-150105.bin
```

com1 (115200) – VOS 업그레이드(2)

vforce# boo system vos-4.6-octeon-150105.bin
Set boot system... Wait a moment ----------→ *Boot 이미지 변경 설정*

```
checking checksum... ok
vos-4.6-octeon-150105.bin selected
```

vforce# show boot system ----------→ *Boot 이미지 선택 확인*

```
Selected boot image : vos-4.6-octeon-150105.bin
```

vforce# reload ----------→ *장비 재부팅*

```
Proceed with reload? [yes/no]  yes
```

vforce# sh ver detail ----------→ *부팅 완료 후 버전 확인*

```
Hansol NexG VForce Software, Version 4.6-150105
Support: http://www.hansolnexg.com
Copyright (c) 2007-2015 All Rights Reserved
ATM-1 uptime is 6 days 18:19:58
System image file is "vos-4.6-octeon-150105.bin"
Hansol NexG VForce406 (CN5020p1.1-500-SCP) Processor with 512M
DRAM at 265MHz
Processor board serial number NZT04001530561
Cavium Octeon+ CPU (2 cores) at 500MHz
```

4-1 CLI 시스템 명령어

com1 (115200) – 설정 백업

vforce# sh run ----------▶ ***Show run 명령어를 통한 백업 / 메모장 copy 보관***

```
!
clock timezone KST 9
!
hostname Jukjeon-Center1
!
username root except-expired secret 5
$1$Cqb3K/Cq$.9nzPAHwDnYQE.Fl5idxa/
!
!
logging remote 192.168.2.101 ips l7filter session appgw-http appgw-
mail appgw-im appgw-ftp ipsec system audit vpdn user-identity
logging source interface eth0
!
!
ip bwt port 2960
ip bwt server
!
ip domain-lookup
!
spanning-tree mode rstp-vlan-bridge
!
!
!
interface lo
 ipv6 address ::1/128
!
interface eth0
 description ### INTERNAL ###
```

com1 (115200) – 설정 복원

CLI(telnet 및 ssh, console)로 접속하여 백업 파일 복사 후 붙여 넣기를 통하여 복구

4-1 CLI 시스템 명령어

com1 (115200) – 로그 설정

vforce# configure terminal

vforce(config)# **logging local all** ----------▶ *로컬 모든 로그 저장*

vforce(config)# **logging local path disk1:/log alert 30 purge 20**

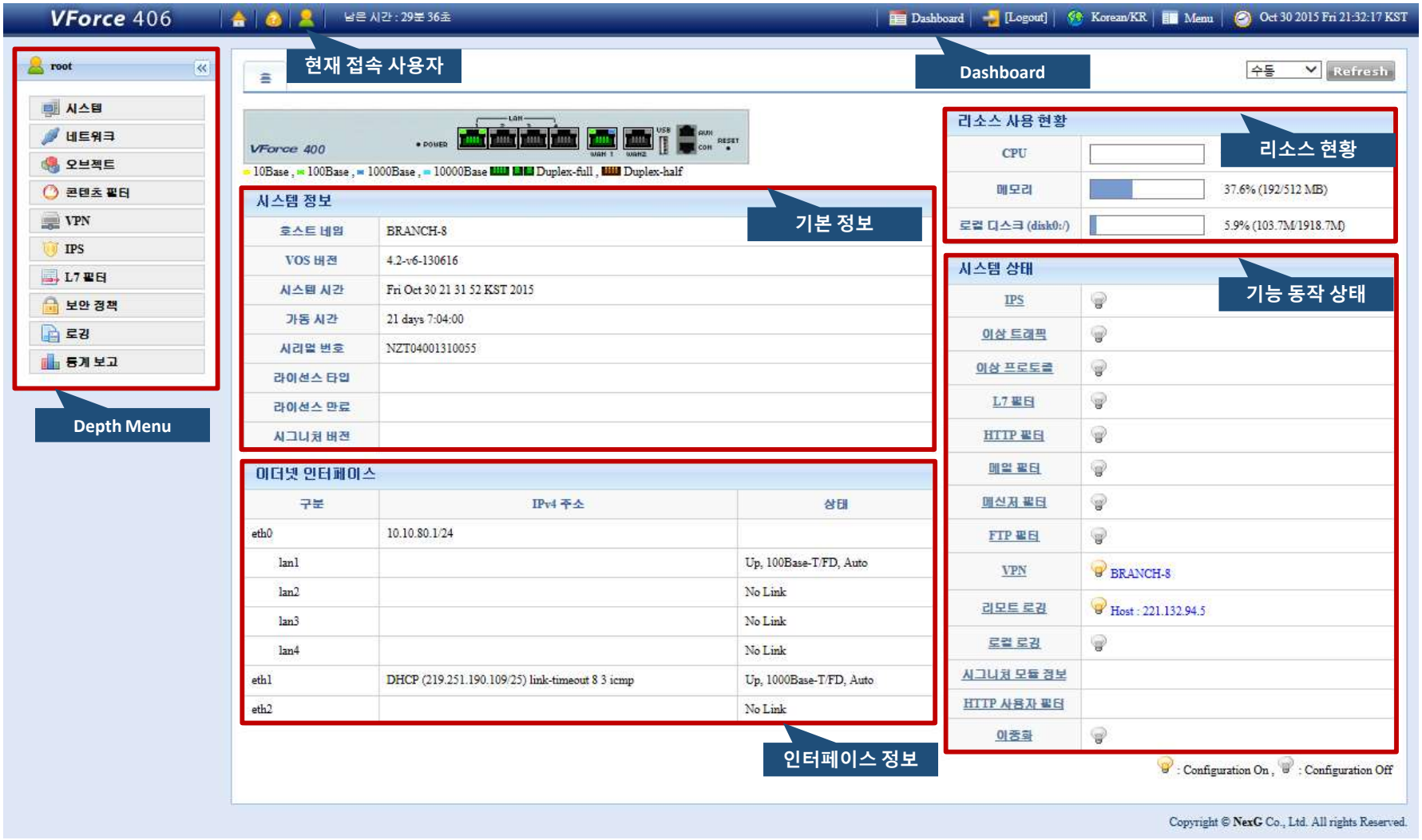
└----------▶ *로컬 로그 저장 위치, 로그파일 공간할당*

vforce(config)# **logging remote 10.10.10.10 all**

└----------▶ *로그 서버로 전송*

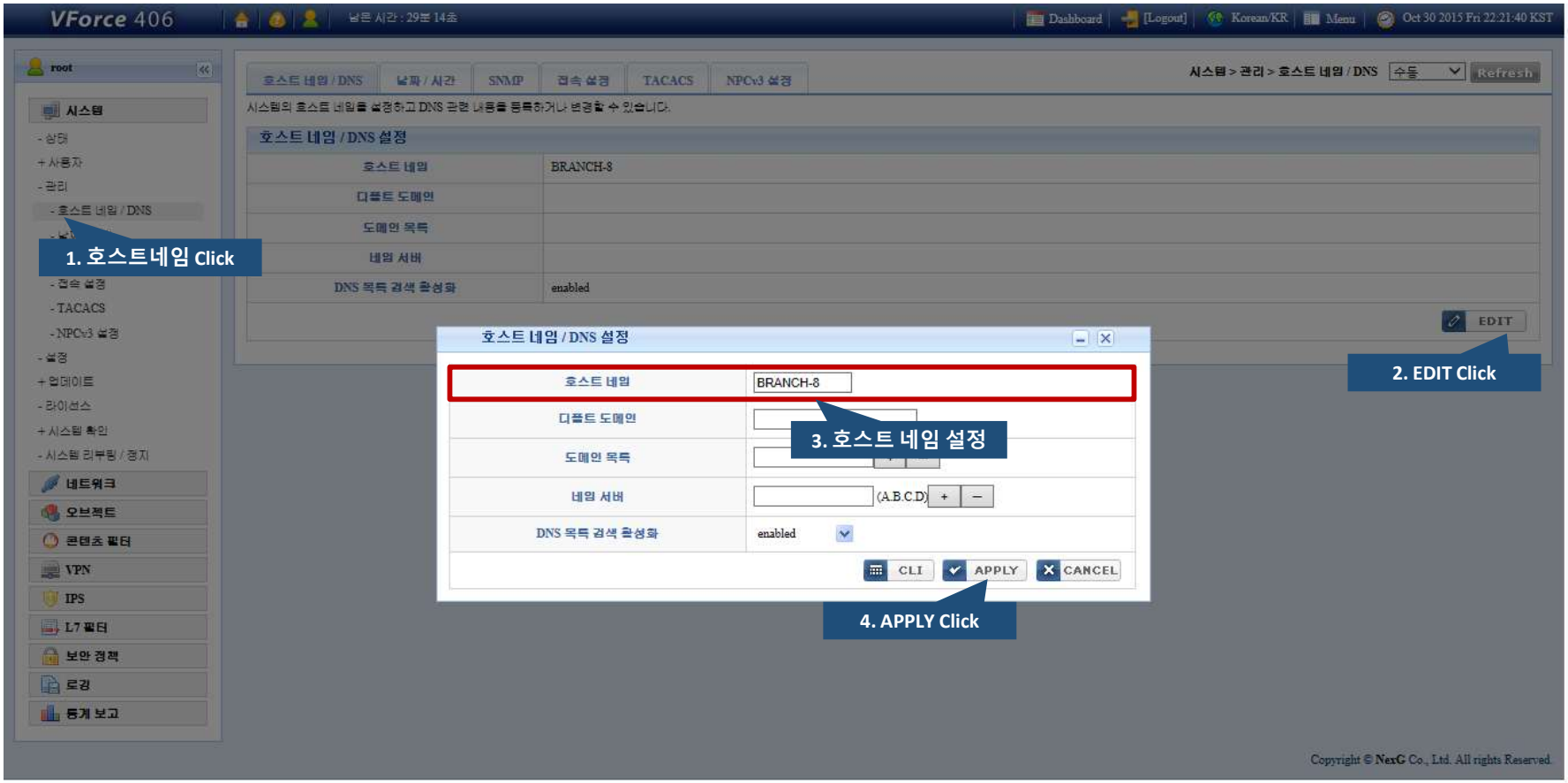
4-2 WebUI 시스템 설정

http / https – WebUI 기본 화면



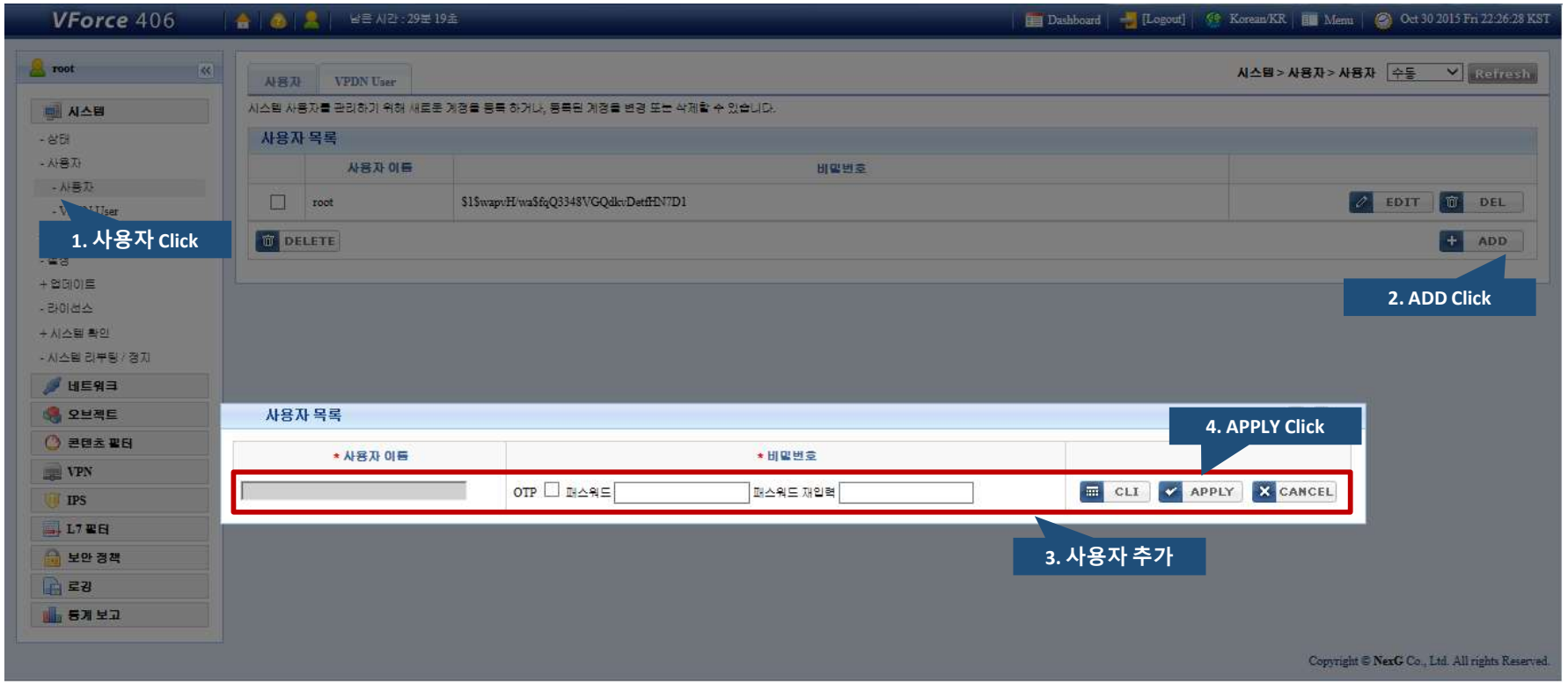
4-2 WebUI 시스템 설정

http / https – Hostname 설정



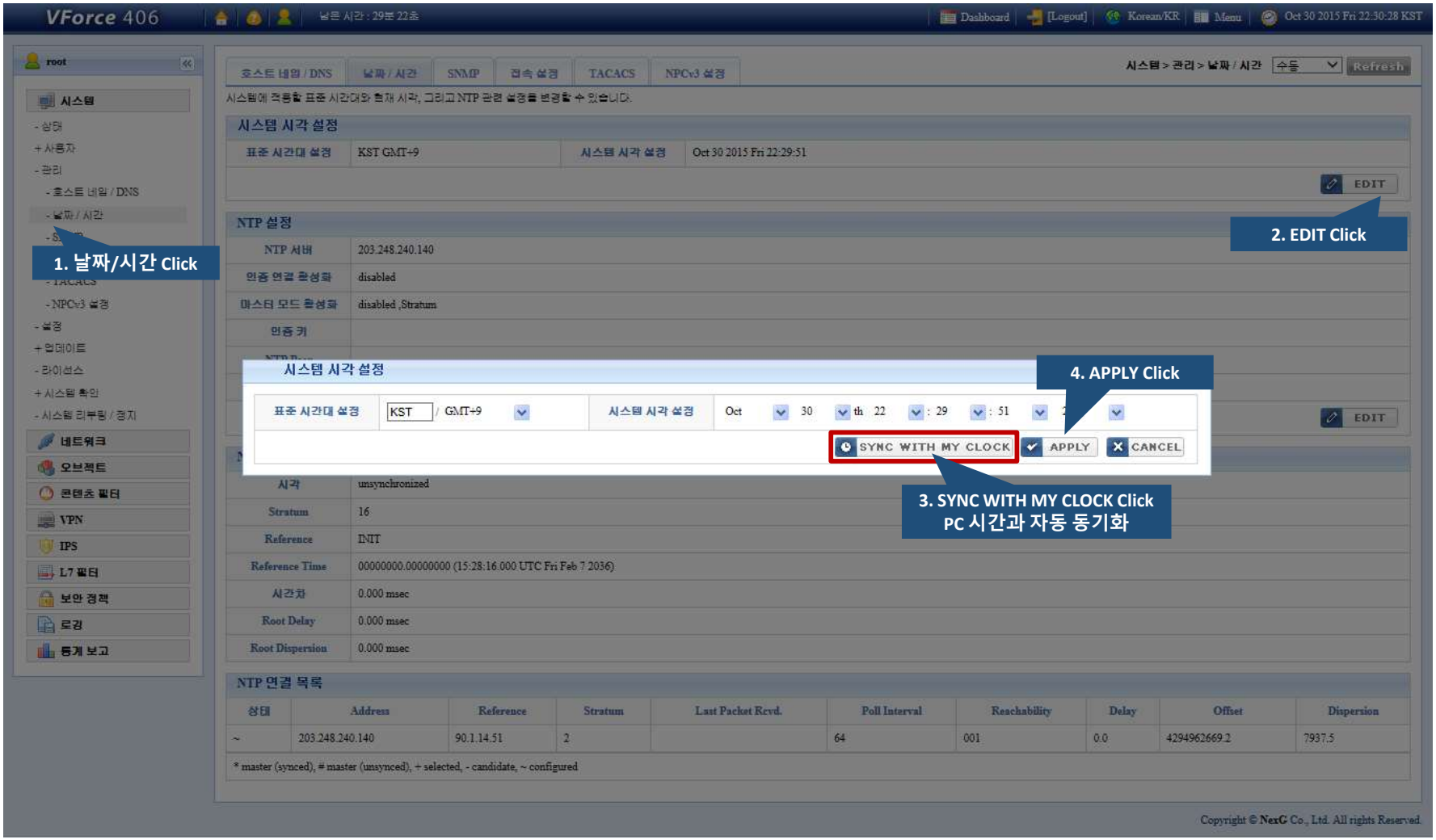
4-2 WebUI 시스템 설정

http / https – 사용자(관리자) 추가



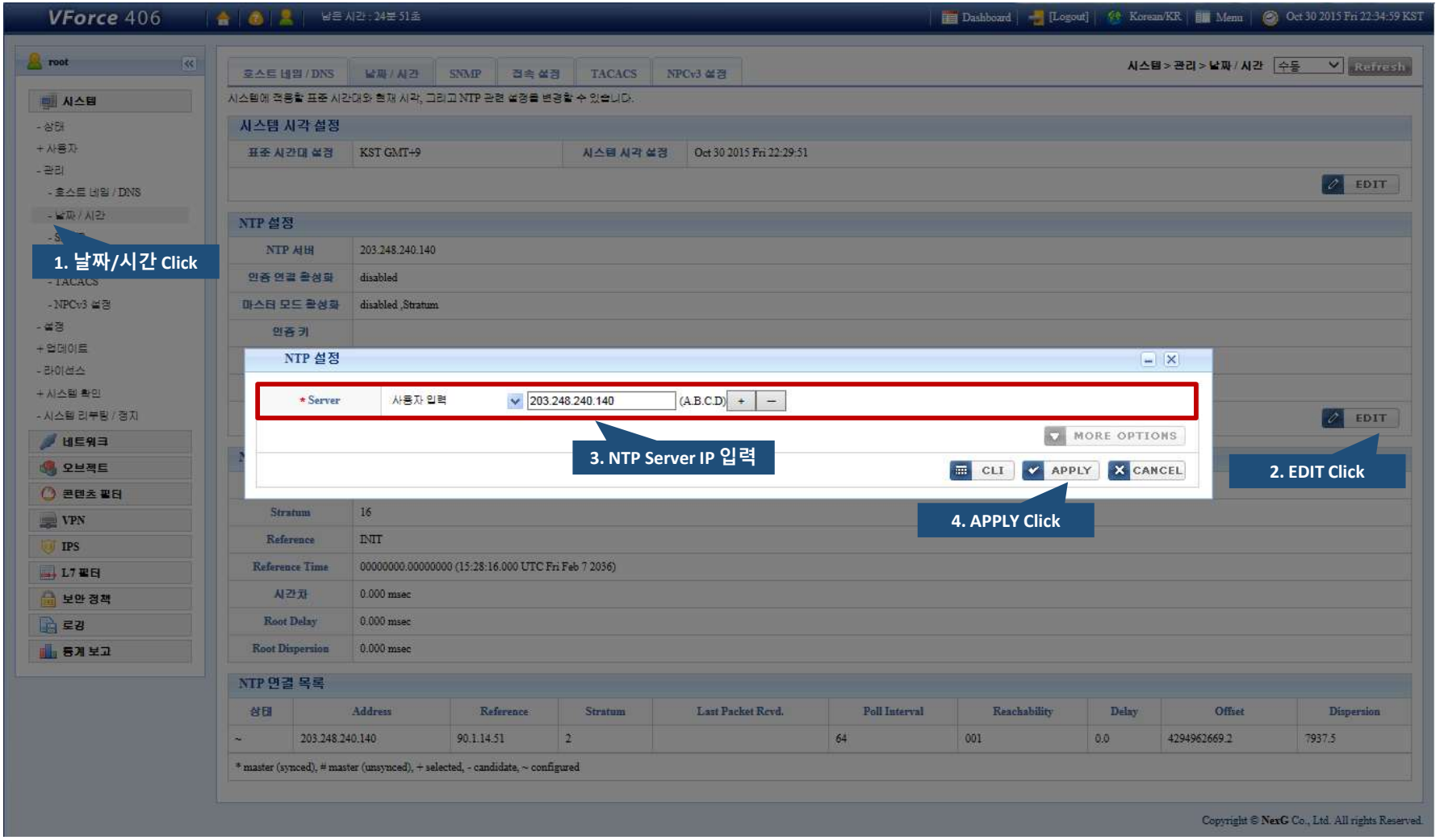
4-2 WebUI 시스템 설정

http / https – 시스템 시간 설정



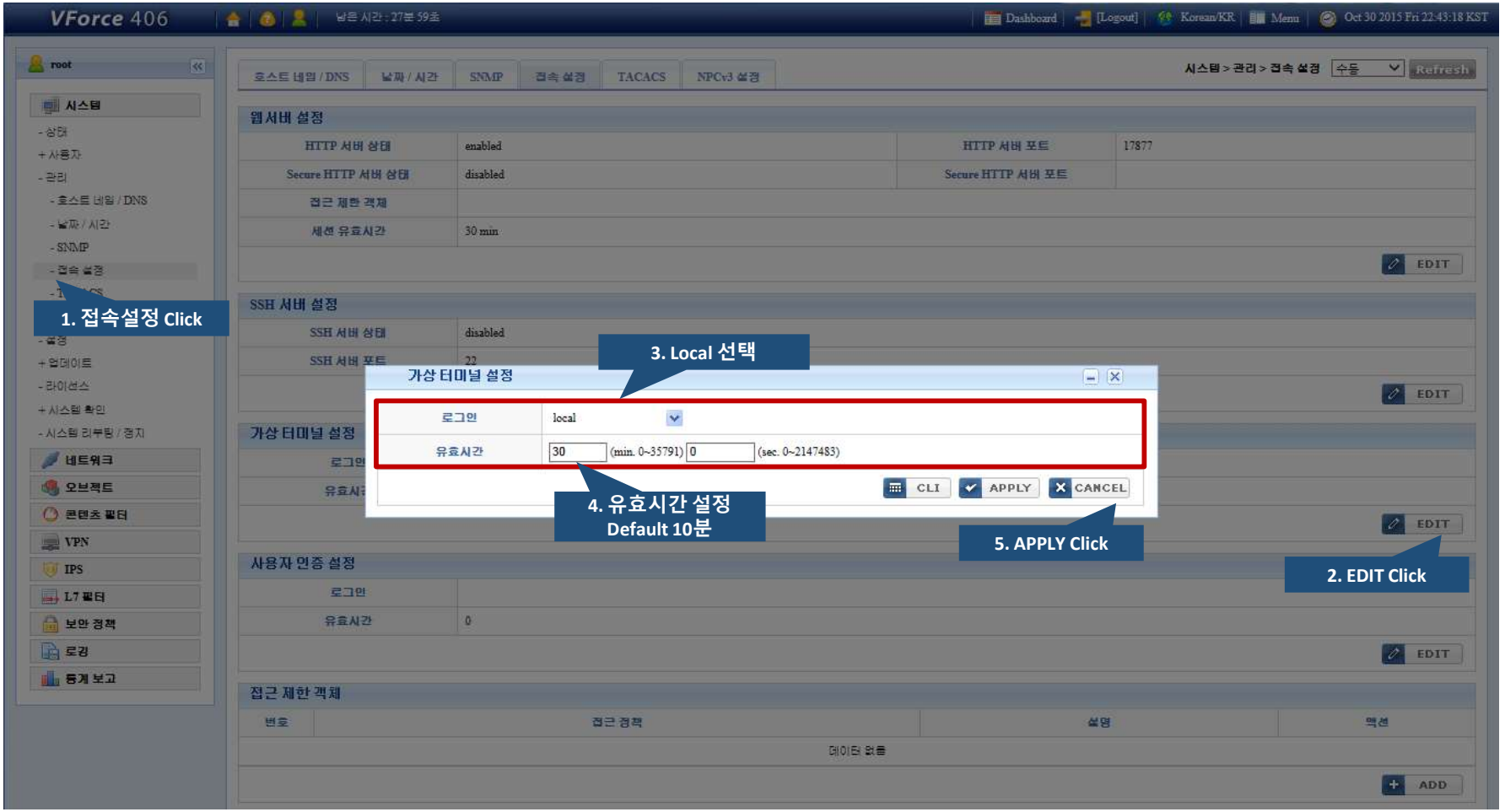
4-2 WebUI 시스템 설정

http / https – NTP Server 설정



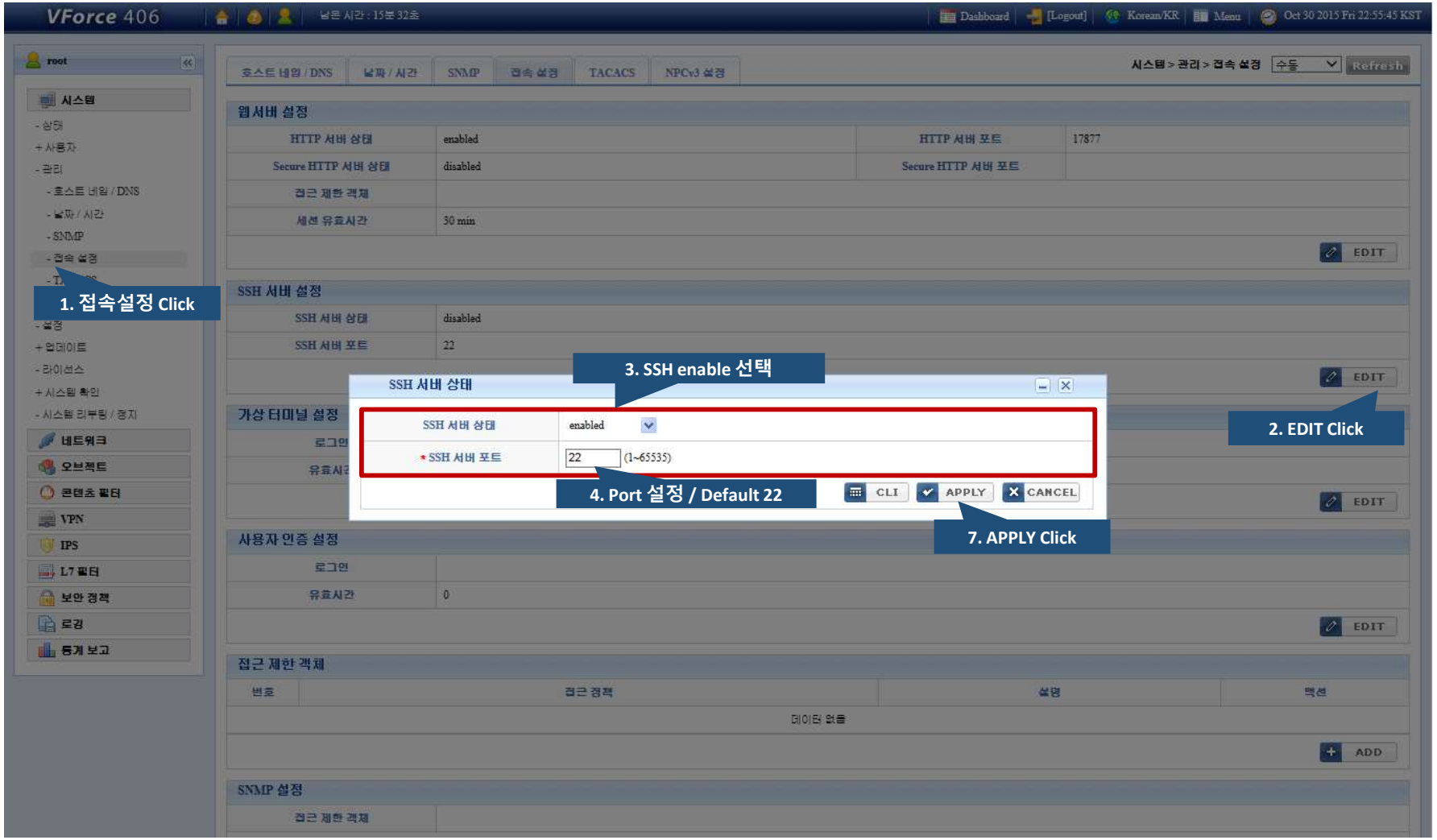
4-2 WebUI 시스템 설정

http / https – Telnet 접속 설정



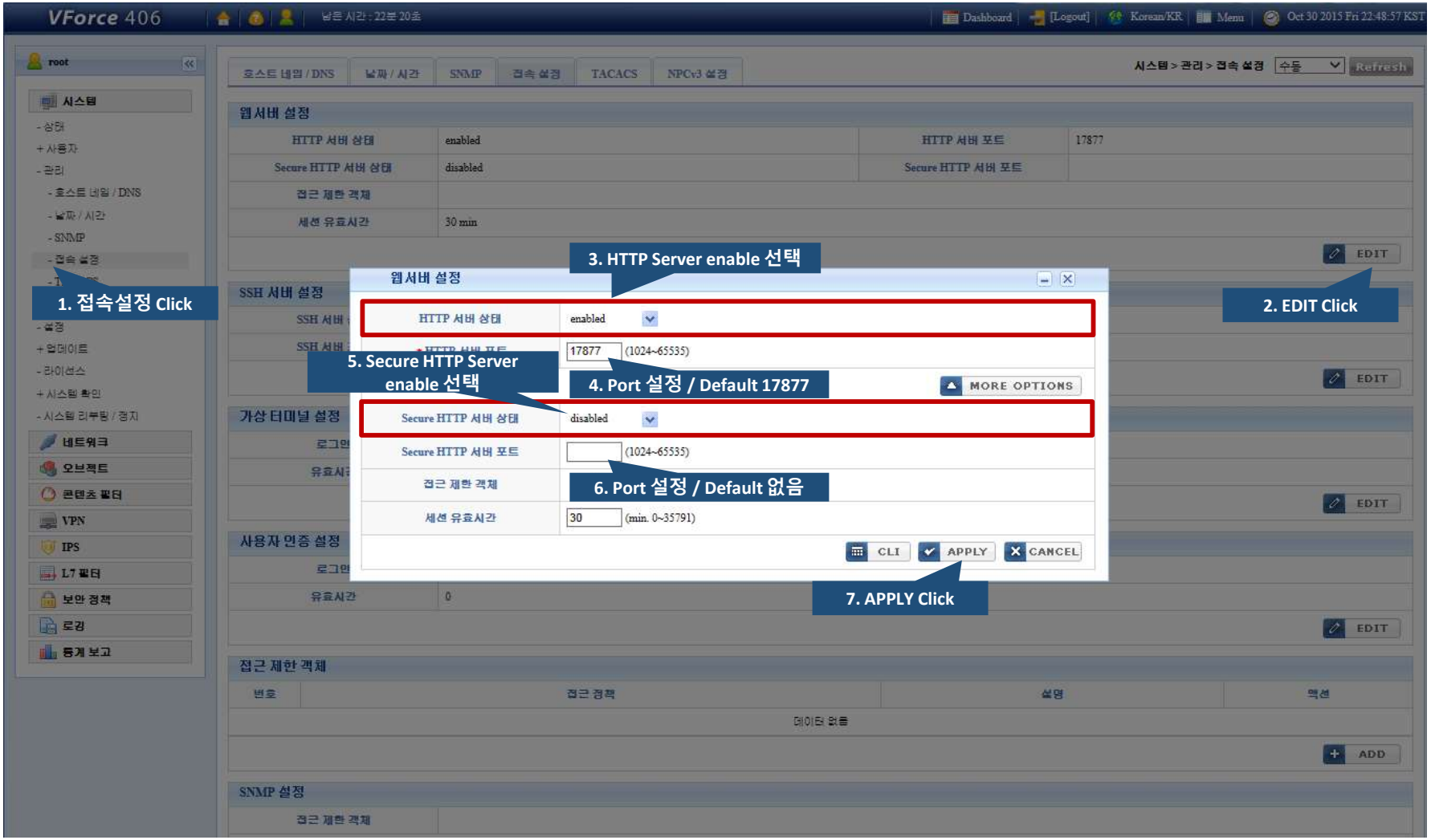
4-2 WebUI 시스템 설정

http / https – SSH 접속 설정



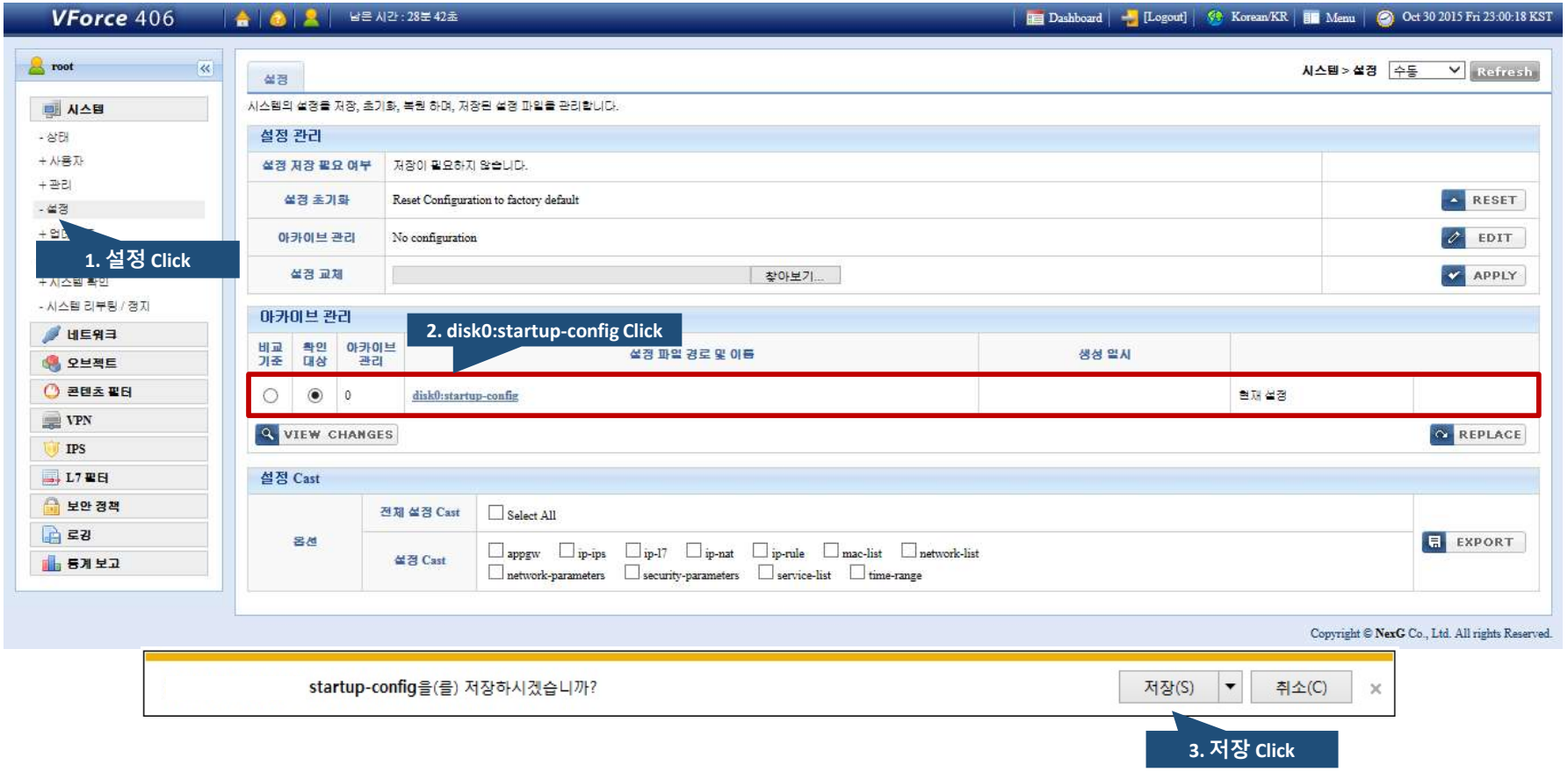
4-2 WebUI 시스템 설정

http / https – WebUI 및 SSL 접속 설정



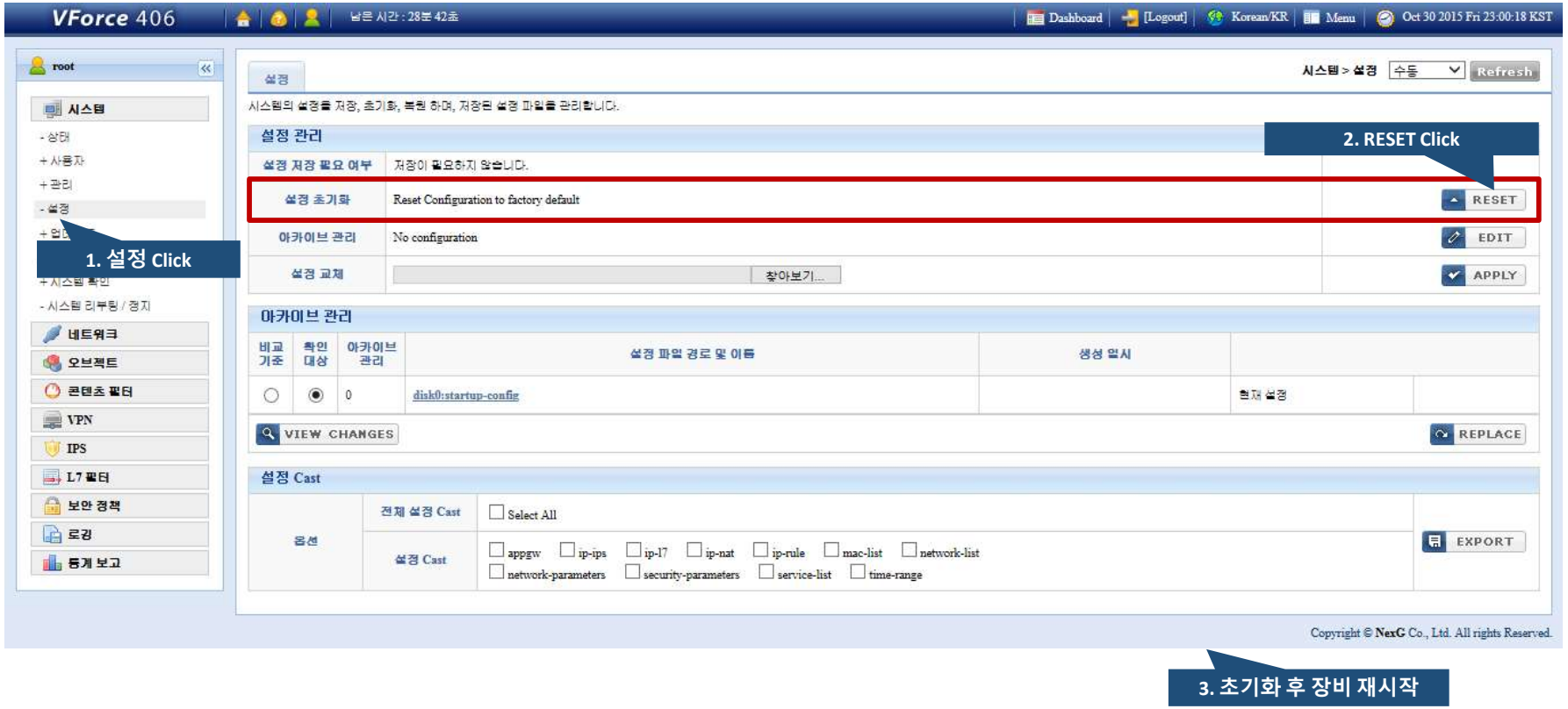
4-2 WebUI 시스템 설정

http / https – 설정 백업



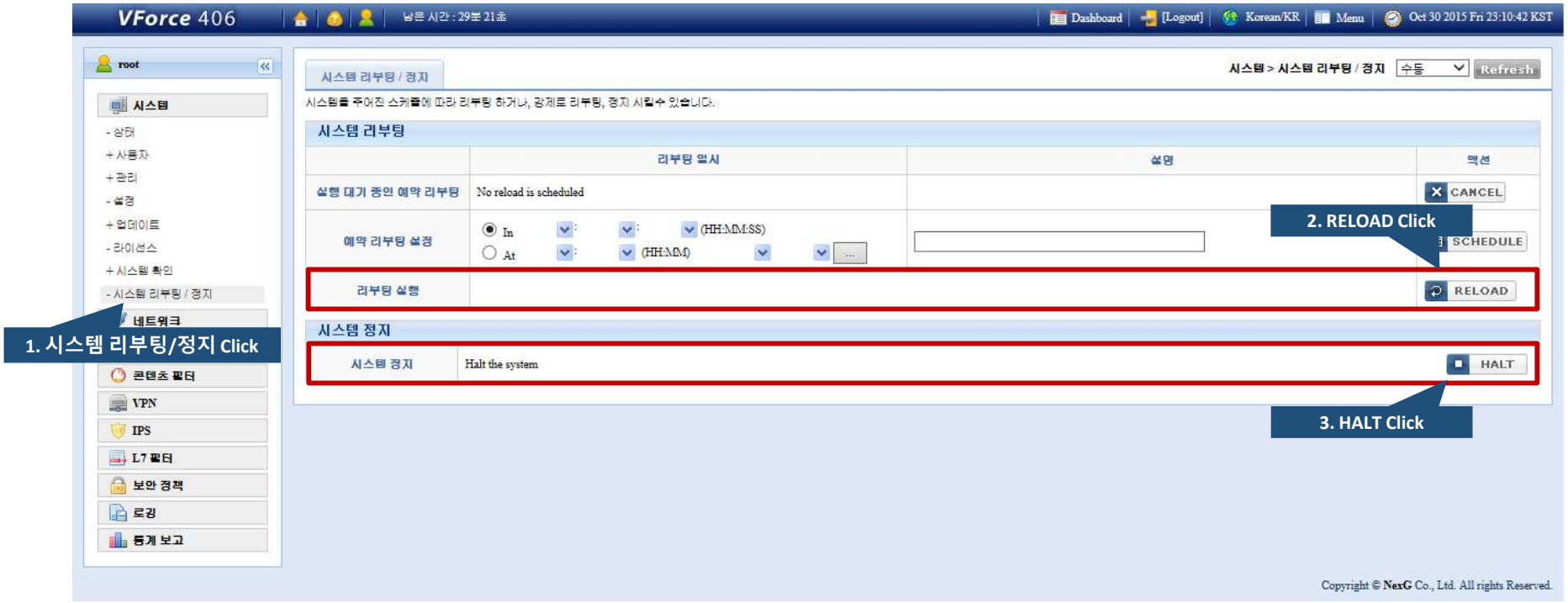
4-2 WebUI 시스템 설정

http / https – 설정 초기화



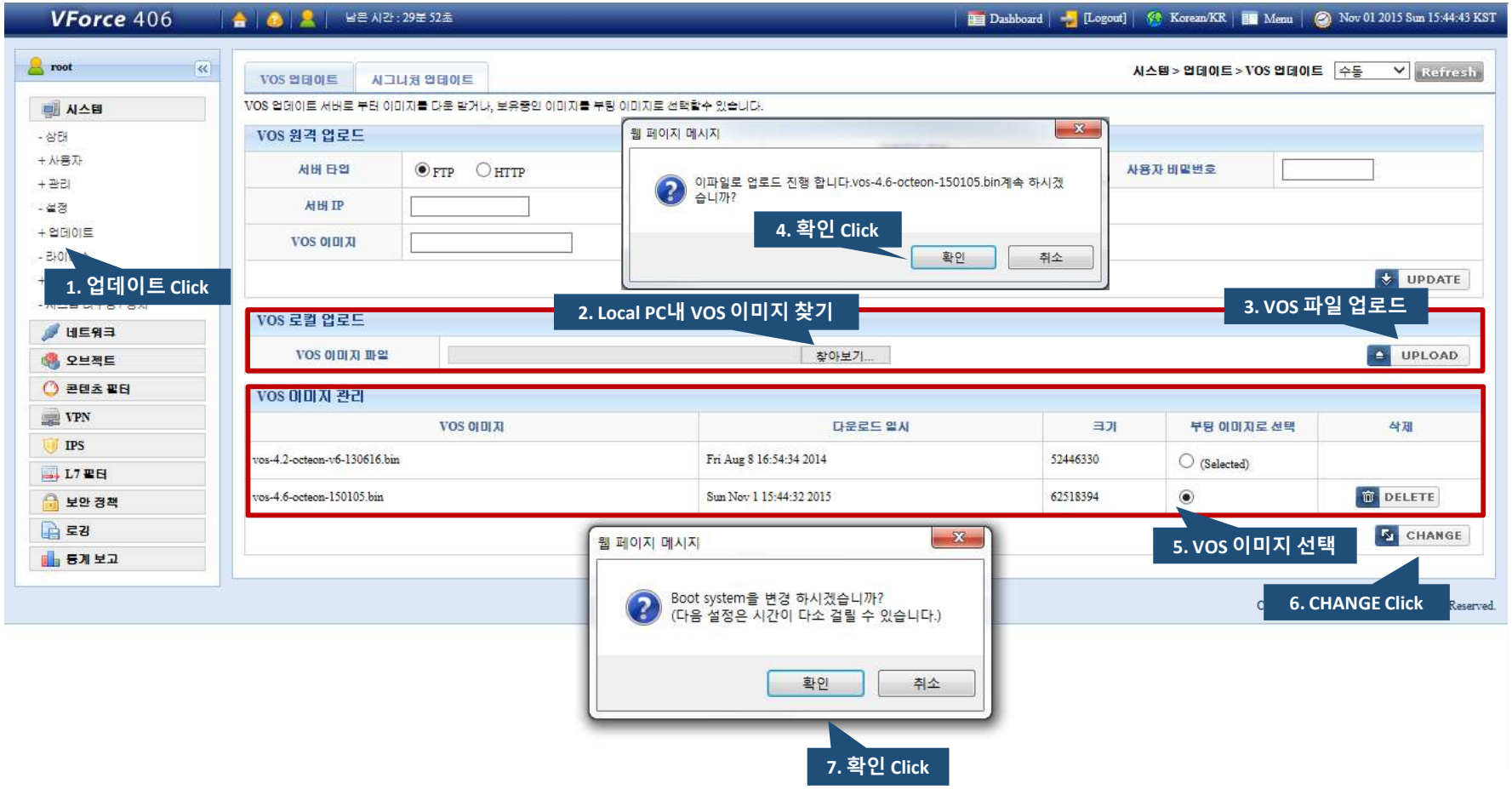
4-2 WebUI 시스템 설정

http / https – 시스템 재시작



4-2 WebUI 시스템 설정

http / https – VOS 업그레이드



5 네트워크 설정

5-1 CLI 네트워크 설정 명령어
5-2 WebUI 인터페이스 설정
5-3 WebUI 라우팅 설정

5-1 CLI 네트워크 설정 명령어

com1 (115200) – Interface IP 설정(고정IP)

```
vforce# configure terminal
vforce(config)# int eth1
vforce (config-if)# ip address 192.168.1.1/24 link-timeout 5 3 icmp
192.168.1.254
vforce (config-if)# end
vforce#
```

회선 연결 장비가 Hang상태로 통신이 불가능 할 때 회선 링크를 강제로 끊는 기능
link-timeout 5 3 icmp 192.168.1.254 : icmp로 5초 주기로 3회 시도, 3회 check fail 일 경우 해당 인터페이스 Down

com1 (115200) – Interface IP 설정(DHCP)

```
vforce# configure terminal
vforce(config)# int eth1
vforce (config-if)# ip address dhcp link-timeout 5 3 icmp
vforce (config-if)# end
vforce #
```

회선 연결 장비가 Hang상태로 통신이 불가능 할 때 회선 링크를 강제로 끊는 기능
link-timeout 5 3 icmp : icmp로 5초 주기로 3회 시도, 3회 check fail 일 경우 해당 인터페이스 Down

com1 (115200) – Interface IP 설정(PPPoE)

```
vforce# configure terminal
vforce(config)# int eth1
vforce (config-if)# pppoe user nexg password test1234
vforce (config-if)# ip address pppoe link-timeout 5 3 icmp
vforce (config-if)# end
vforce#
```

pppoe ID 및 Password 입력

회선 연결 장비가 Hang상태로 통신이 불가능 할 때 회선 링크를 강제로 끊는 기능
link-timeout 5 3 icmp : icmp로 5초 주기로 3회 시도, 3회 check fail 일 경우 해당 인터페이스 Down

com1 (115200) – 라우팅 설정(static / 고정IP, dhcp, pppoe)

```
vforce# configure terminal
vforce(config)# ip route 0.0.0.0/0 1.1.1.1
vforce(config)# ip route 0.0.0.0/0 eth1 dhcp
vforce(config)# ip route 0.0.0.0/0 eth1 pppoe
```

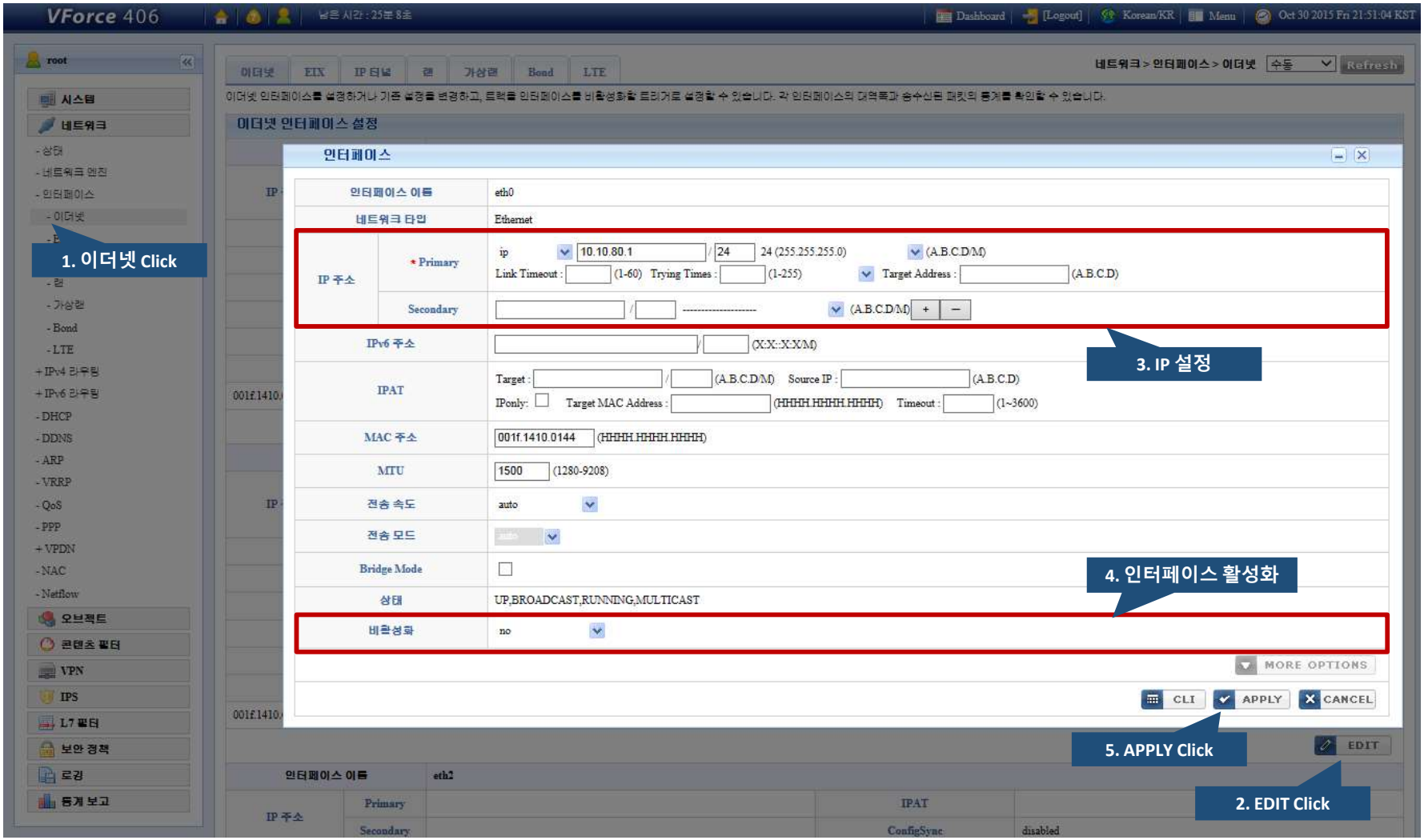
고정IP일 경우 라우팅 설정

dhcp일 경우 라우팅 설정

pppoe일 경우 라우팅 설정

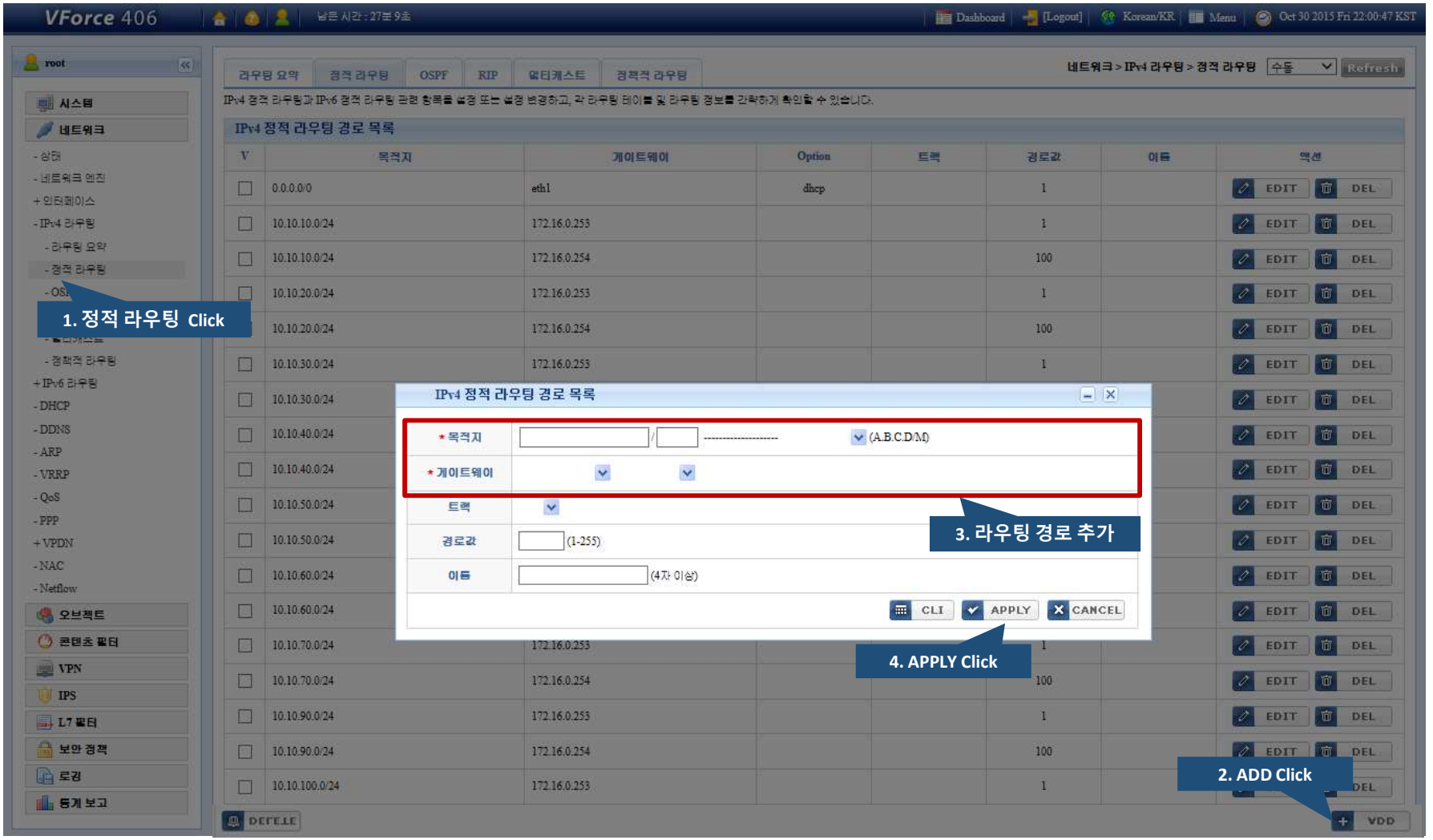
5-2 WebUI 인터페이스 설정

http / https – 인터페이스 설정



5-3 WebUI 라우팅 설정

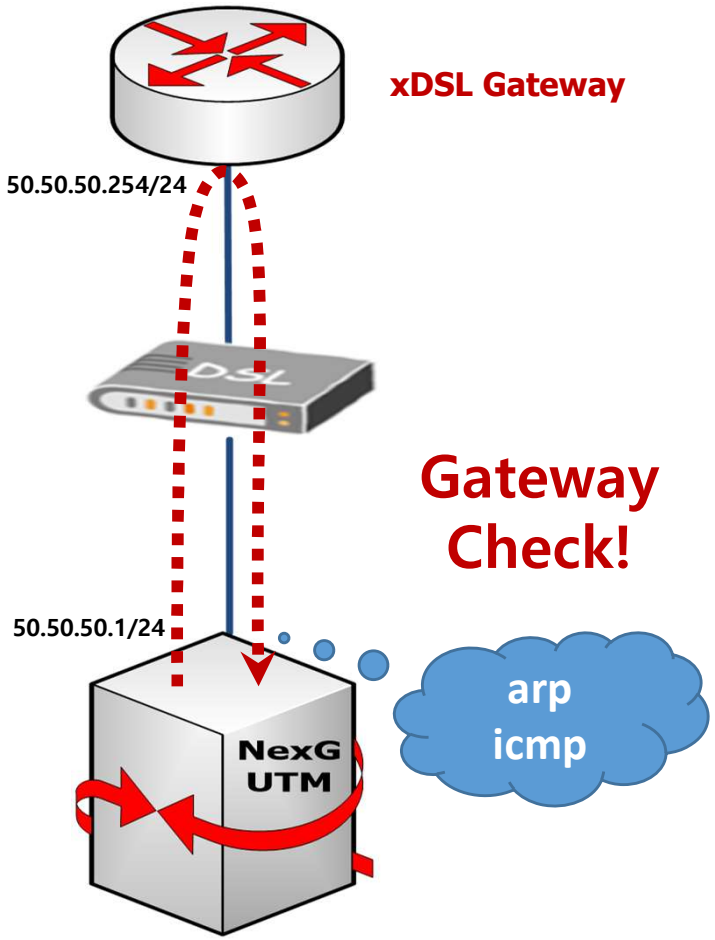
http / https – Static 라우팅 설정



6 시스템 기능 상세

6-1 인터페이스 상태 감시 / Link-timeout

Link-timeout 구성도 예시



com1 (115200) – Link-timeout 설정 예

```
interface eth1
 ip address dhcp link-timeout 5 3 arp ----------▶ DHCP link-timeout 설정
!
interface eth2
 ip address 50.50.50.1/24 link-timeout 5 3 arp 50.50.50.254
!                                  └-------▶ 고정IP link-timeout 설정
vforce#  sh int eth2
Interface eth1
  Hardware is Ethernet, address is 0090.fb18.4138 (bia 0090.fb18.4138)

  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 0
  <UP,BROADCAST,RUNNING,MULTICAST>
  Link-timeout ARP status UP, check interval 2, total 2, success 1, error 0

Speed 1000Base-T
  inet 50.50.50.1/24 broadcast 50.50.50.255
!
```

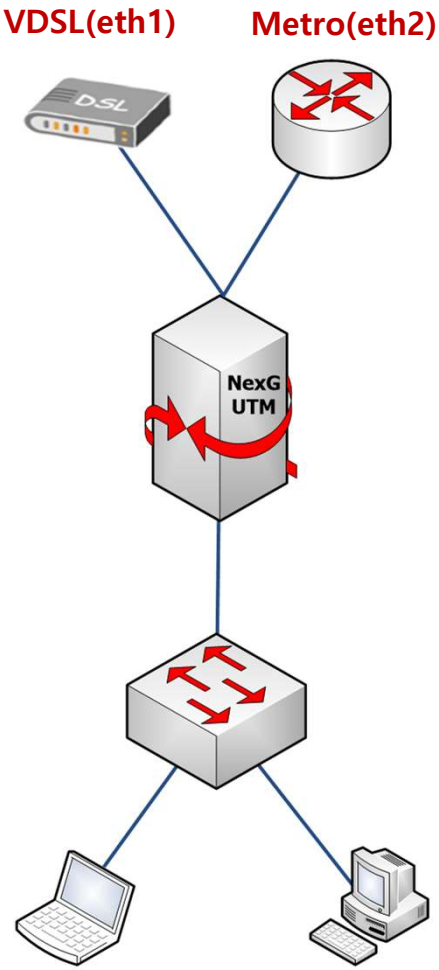
- ❖ **IP 주소 : Address / Mask / Link-timeout(옵션)**
- ❖ **Link-tiemout : line protocol 상태를 체크**

5초당 1번씩 Target 으로 지정된 IP로 ICMP를 체크하며 3번의 응답이 없을 시 장애로 판단하여 회선을 강제로 끊는 옵션

- 권장 값 1: Link-timeout 5 3 arp (VDSL,Metro 고속 회선)
- 권장 값 2 : link-timeout 10 3 icmp (ADSL 저속 회선 또는 손실이 많은 회선)

6-2 정적 라우팅 / Static

구성도 예시



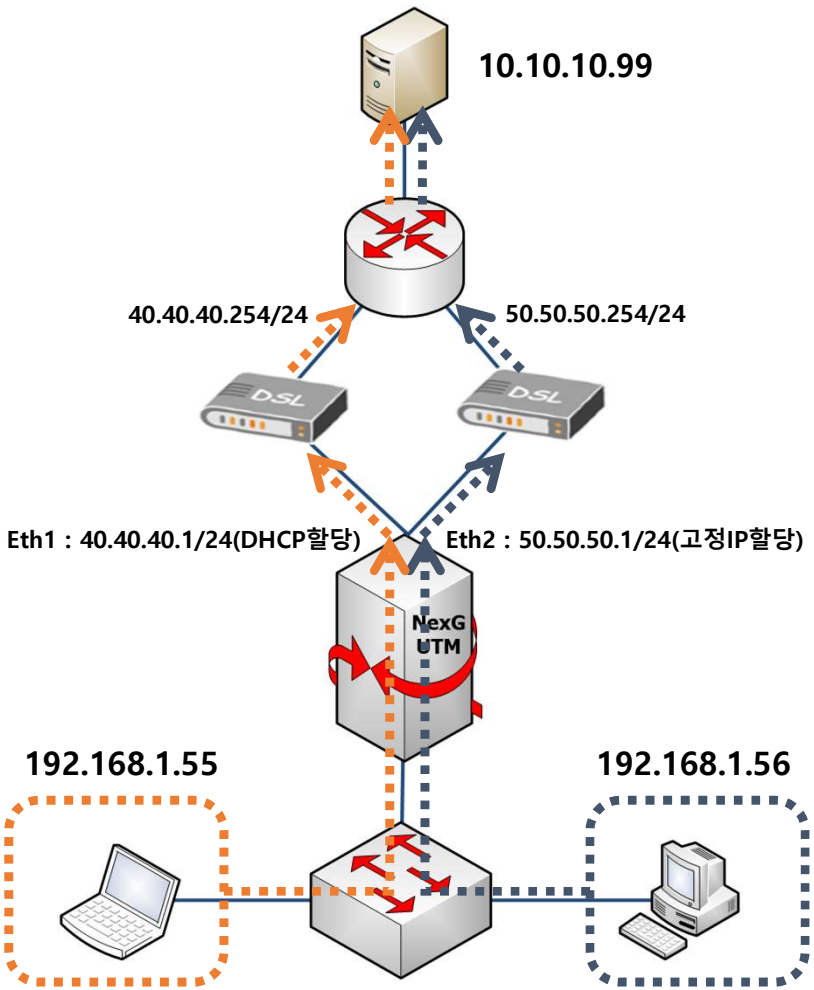
com1 (115200) – Static Routing 설정 예

```
vforce# sh run int eth1
interface eth1
 ip address dhcp link-timeout 5 3 icmp
vforce# sh run int eth2
interface eth2
 ip address 50.50.50.1/24 link-timeout 2 2 arp 50.50.50.254
vforce# conf t
vforce(config)# ip route 0.0.0.0/0 eth1 dhcp -----> DHCP 인터페이스 디폴트
vforce(config)# ip route 0.0.0.0/0 eth1 pppoe -----> PPPoE 인터페이스 디폴트
vforce(config)# no ip route 0.0.0.0/0 eth1 pppoe ----> 라우팅 삭제 명령어
(vforceconfig)# ip route 0.0.0.0/0 50.50.50.254 eth2 -> GW 인터페이스 지정 설정
vforce(config)# ip route 50.50.50.50.250/32 50.50.50.254 10
                                          --------> Static AD 값 설정
```

```
VForce# sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
* 생략 *
Gateway of last resort is 50.50.50.254 to network 0.0.0.0
S*      0.0.0.0/0 [1/0] via 50.50.50.254, eth2
                  [1/0] via 40.40.40.254, eth1
C       10.100.3.0/24 is directly connected, eth3
C       40.40.40.0/24 is directly connected, eth1
C       50.50.50.0/24 is directly connected, eth2
C       127.0.0.0/8 is directly connected, lo
C       192.168.1.0/24 is directly connected, eth0
```

6-2 정적 라우팅 / Static

PBR 구성도 예시



com1 (115200) – PBR 설정 예

- **PBR 구문 형식**

ip route policy [policy_num] **table** [table_num] **source** [source] **destination** [destination] [gateway] [출력 Interface명] [dhcp]

- Destination 이 없으면 0.0.0.0/0(any) 네트워크가 생략되어 있음(생략 가능)
- policy (번호) : PBR 우선 순위 (라우팅의 AD 값과 비슷함)
- table (번호) : PBR 의 목적지 주소와 GW 아이피 주소 및 인터페이스

- **터널 연결용 PBR 설정 예시**

vforce# sh run ip route policy
ip route policy 1 table 1 source eth1 eth1 dhcp ------▶ *유동IP PBR 설정*
ip route policy 2 table 2 source eth2 50.50.50.254 eth2 -▶ *고정IP PBR 설정*

Destination 생략 / 목적지 0.0.0.0/0(any)

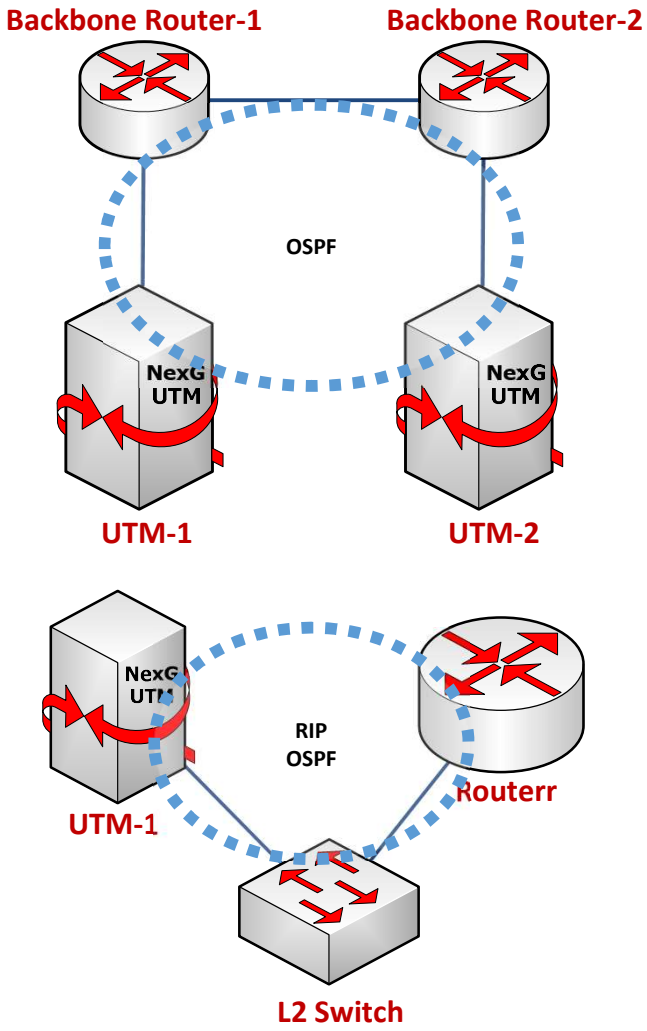
- **일반적인(사용자용) PBR 설정 예시**

vforce# sh run ip route policy
ip route policy 3 table 3 source 192.168.1.55/32 destination
10.10.10.99/32 eth1 dhcp ----------▶ *192.168.1.55 eth1 경유 PBR 설정*
ip route policy 4 table 4 source 192.168.1.56/32 destination
10.10.10.99/32 50.50.50.254 eth2------▶ *192.168.1.56 eth2 경유 PBR 설정*

- ❖ 터널 협상을 위한 정책 기반 라우팅(Policy Based Routing) 설정
- ❖ 회선이 2개 이상일 경우 PBR 설정 필수(안정적인 터널 연결을 위해)
- ❖ Default Routing(0.0.0.0/0) 보다 상위에 동작함
- ❖ 의미 : Source 가 eth1 에서 발생되는 트래픽 은 eth1 G/W 으로 보내도록 설정함.

6-3 동적 라우팅 / RIP, OSPF

구성도 예시



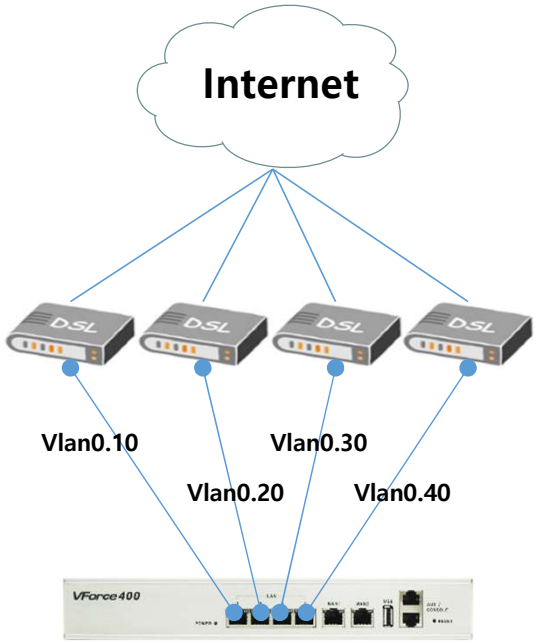
com1 (115200) – RIP, OSPF 설정 예

```
VForce# conf t
VForce (config)# router rip
VForce(config-router)# network 192.168.0.0/16
VForce(config-router)# router ospf 100
VForce(config-router)# network 192.168.0.0/16
VForce(config-router)# redistribute static
VForce(config-router)# end
VForce#
VForce# sh run router rip
router rip
 network 192.168.223.0/24
.

VForce## sh run router ospf
router ospf 100
 redistribute connected
 network 192.168.0.0/16 area 0
```

```
VForce# sh ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B – BGP

Network                  Next Hop        Metric From     If              Time
Rc 192.168.0.0/161                       eth0

*B-UTM-1# sh ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri     State           Dead Time       Address         Interface
192.168.223.1   1       Full/Backup     00:00:40        192.168.223.1   eth0
```

6-4 Interface(1) / LAN Interface Vlan 설정

Vlan 구성도 예시

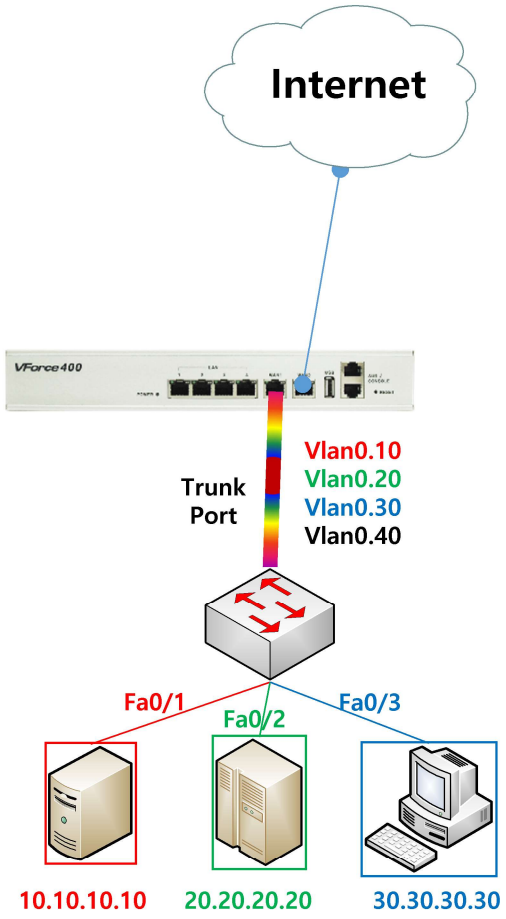


com1 (115200) – Vlan 설정 예

```
vlan database ---------- Vlan 생성
 vlan 10
 vlan 20
 vlan 30
 vlan 40
!
interface eth0
 switchport ---------- L2 모드로 동작
 switchport mode trunk ---------- Trunk 포트 동작 설정
 switchport trunk allowed vlan all ---------- 모든 Vlan 허용
!
interface lan1 ---------- Eth0의 1번 포트 설정
 speed 100 duplex full
 switchport ---------- L2 모드로 동작(기본값)
 switchport access vlan 10 ---------- Vlan 지정
!
interface vlan0.10 ---------- Vlan0.10번 인터페이스 생성
 description wan 1
 ip address dhcp link-timeout 5 3 icmp ---------- IP 설정
```

6-5 Interface(1) / LAN Interface Vlan 설정

Trunk 구성도 예시

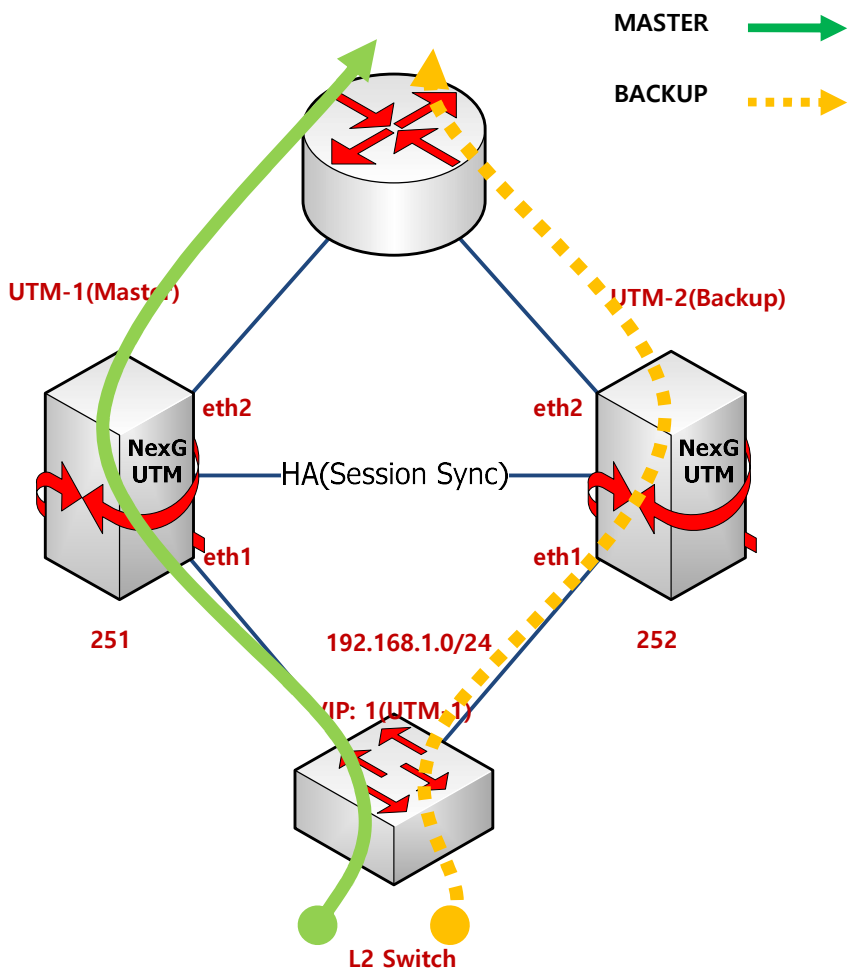


com1 (115200) – Trunk 설정 예

```
vlan database ----------> Vlan 생성
 vlan 10
 vlan 20
 vlan 30
 vlan 40
!
interface eth1
 switchport ----------> L2 모드로 동작
 switchport mode trunk ----------> Trunk 포트 동작 설정
 switchport trunk allowed vlan all ----------> 모든 Vlan 허용
!
interface vlan0.10 ----------> Vlan0.10번 인터페이스 생성
 ip address 10.10.10.1/24 ----------> IP 설정
!
interface vlan0.20 ----------> Vlan0.20번 인터페이스 생성
 ip address 20.20.20.1/24 ----------> IP 설정

interface vlan0.30 ----------> Vlan0.30번 인터페이스 생성
 ip address 30.30.30.1/24 ----------> IP 설정
```

6-6 Interface(2) / Trunk(802.1q) 설정

VRRP 구성도 예시



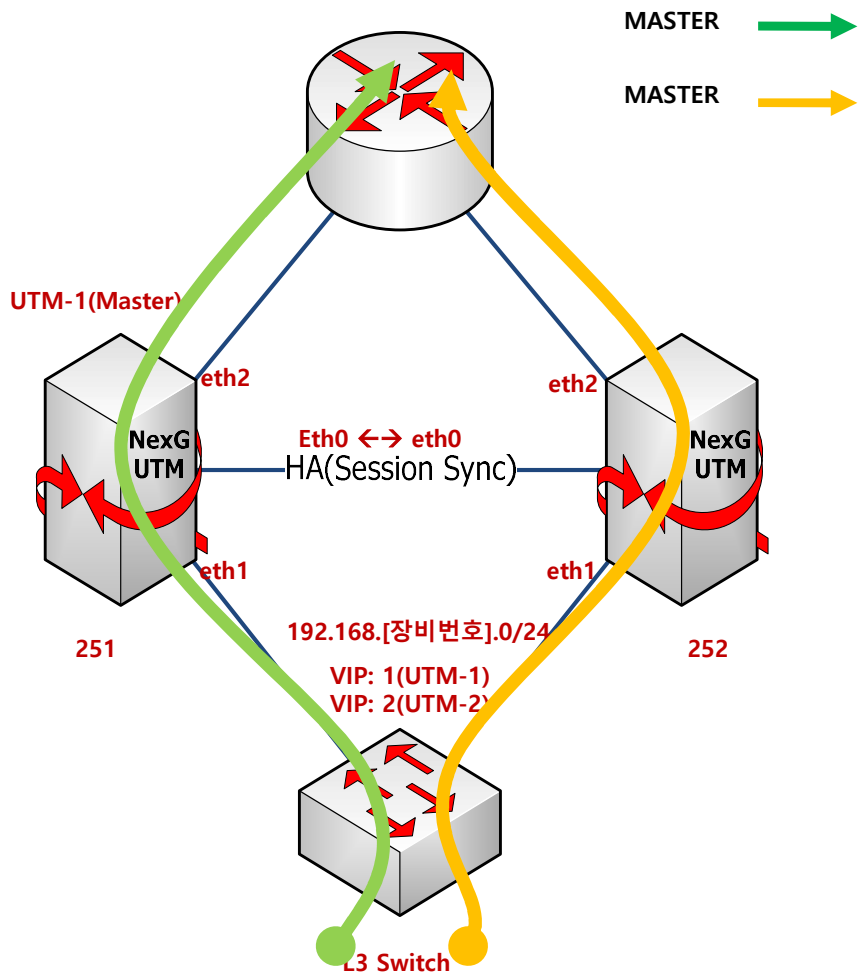
com1 (115200) – VRRP 설정 예

```
< 1호기 >
VForce-1# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 250
 advertisement-interval 3
 enable


< 2호기 >
VForce-2# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 240
 advertisement-interval 3
 enable
```

```
VForce-1# sh vrrp brief
VrID  Interface  State    Priority   AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Master   250/250    3            TRUE     eth2/100/UP

VForce-2# sh vrrp brief
VrID  Interface  State    Priority   AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Backup   240/240    3            TRUE     eth2/100/UP
```

6-6 VRRP(1) / Master - Standby

Multi VRRP 구성도 예시



com1 (115200) – Multi VRRP 설정 예

< 1호기 >

```
VForce-1# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 250
 advertisement-interval 3
 enable
```

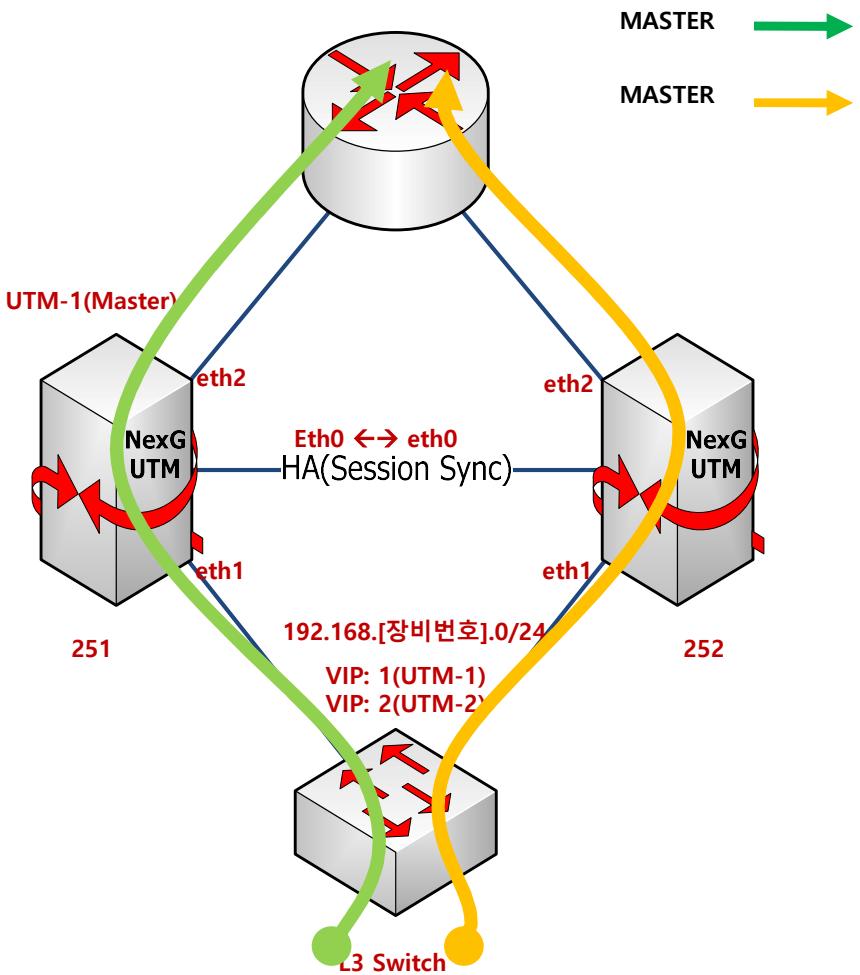
< 2호기 >

```
VForce-2# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 240
 advertisement-interval 3
 enable
```

```
B-UTM-1# sh vrrp brief
VrID  Interface  State    Priority   AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Master   250/250    3            TRUE     eth2/100/UP
20    eth1       Backup   200/200    3            TRUE     eth2/100/UP

B-UTM-2# sh vrrp brief
VrID  Interface  State    Priority   AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Backup   200/200    3            TRUE     eth2/100/UP
20    eth1       Master   250/250    3            TRUE     eth2/100/UP
```

6-6 VRRP(2) / Master - Master(Multi VRRP)

Multi VRRP 구성도 예시



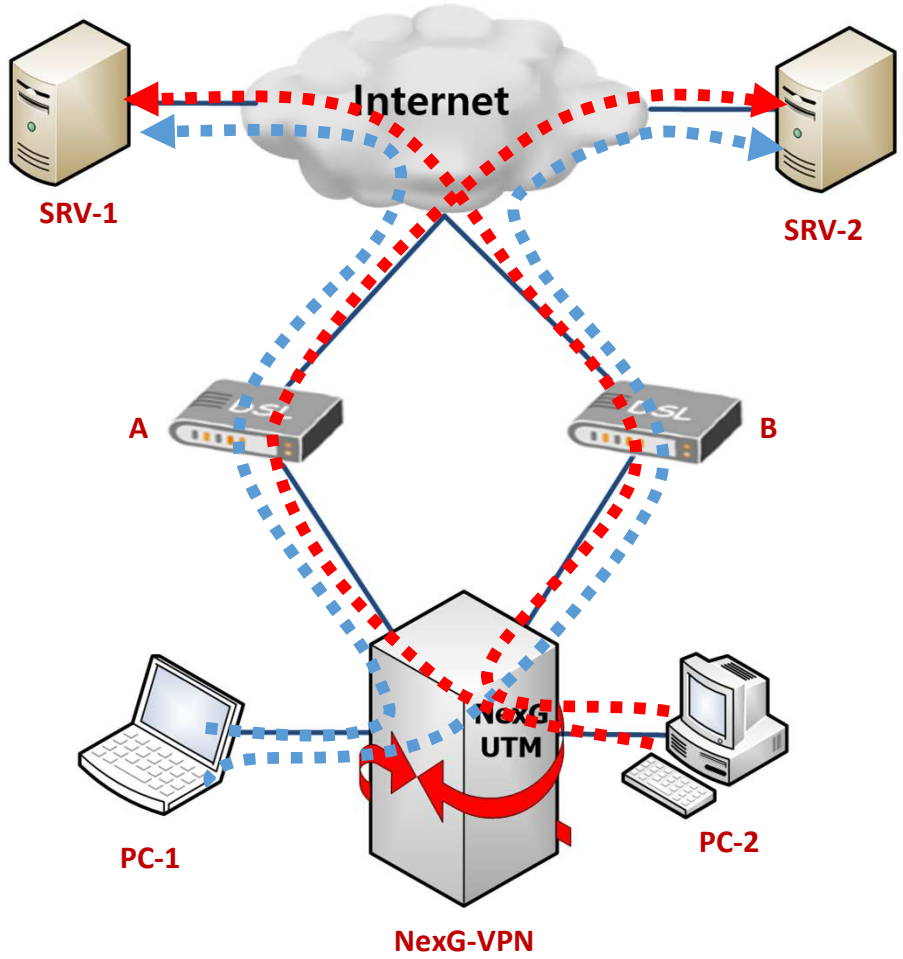
com1 (115200) – Multi VRRP 설정 예

```
< 1호기 >
VForce-1# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 250
 advertisement-interval 3
 enable


< 2호기 >
VForce-2# sh run router vrrp
!
router vrrp 10 eth1
 virtual-ip 192.168.1.1 backup
 circuit-failover eth2 100
 priority 240
 advertisement-interval 3
 enable
```

```
B-UTM-1# sh vrrp brief
VrID  Interface  State     Priority     AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Master    250/250      3            TRUE     eth2/100/UP
20    eth1       Backup    200/200      3            TRUE     eth2/100/UP

B-UTM-2# sh vrrp brief
VrID  Interface  State     Priority     AD-Interval  Preempt  Circuit-Failover
-------------------------------------------------------------------------------
10    eth1       Backup    200/200      3            TRUE     eth2/100/UP
20    eth1       Master    250/250      3            TRUE     eth2/100/UP
```

6-7 ECMP(Equal Cost Multipath Protocol)

ECMP 구성도 예시



com1 (115200) – ECMP 설정 예

```
vforce# show run ip route
!
ip route 0.0.0.0/0 eth1 dhcp
ip route 0.0.0.0/0 eth2 dhcp
!
```

Default Routing의 AD값을 Equal Cost로 설정

✓ PC-1 경로

1: PC-1: A > SRV-1

2: PC-1: B > SRV-2

✓ PC-2 경로

3: PC-2: B > SRV-1

4: PC-2: A > SRV-2

6-8 NTP(Network Time Protocol)

com1 (115200) – NTP 설정

```
VForce# sh run clock
ntp server 203.252.0.211 prefer
ntp server 203.248.240.140
ntp server 210.98.16.100
ntp server 210.98.16.101
clock timezone KST 9
```

(1) : 시간 관련 설정 보기
(2) : 주 NTP 서버 아이피 설정()
(2) : NTP 서버 아이피 설정(time.bora.net)
(2) : NTP 서버 아이피 설정(time.kriss.re.kr)
(3) : NTP 서버 아이피 설정(time2.kriss.re.kr)
(4) : 장비 표준시 설정(한국 표준시)

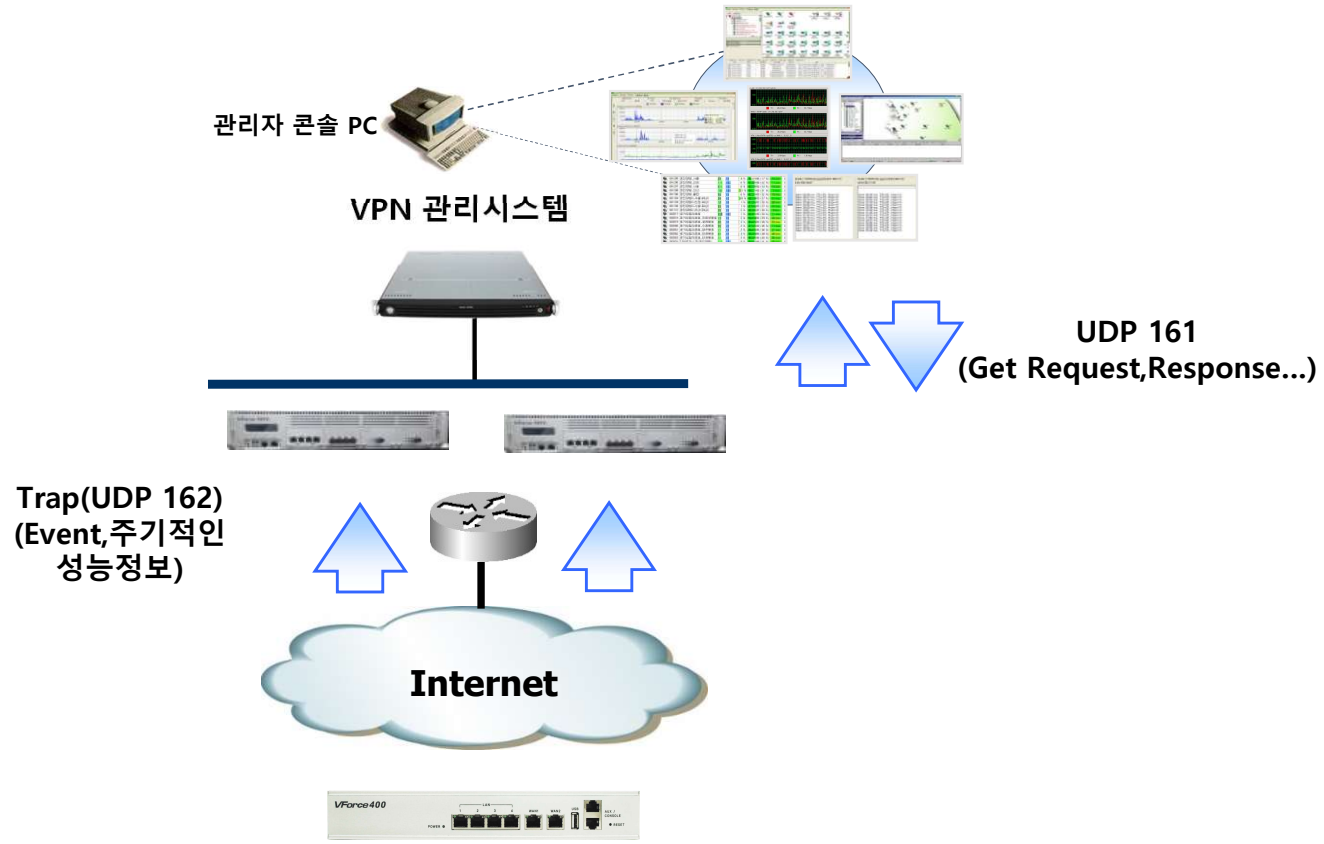
```
VForce# sh ntp associations
   address          ref clock       st   when   poll   reach   delay   offset    disp
 ~203.252.0.211     123.140.16.100   2    143    1024   377     0.0     0.0       18.7
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

com1 (115200) – NTP 서버 시간 가져오기

```
VForce# clock ntpdate 203.248.240.140
VForce# sh clock
Wed Jul 22 14:53:02 KST 2009
```

(1) : NTP 서버 시간 즉시 가져오기
(2) : 현재 시간 보기
(3) : 현재 시간

6-9 SNMP(Simple Network Management Protocol)



com1 (115200) – SNMP	
snmp-server source {Source Binding IP/INTERFACE} snmp-server host {NMS 서버} traps version 2c nexg snmp-server community nexg rw snmp-server info interval 1	(1) : SNMP Source Binding (2) : Trap 설정 (3) : Community 설정 (4) : Trap 전송 주기 설정(1분)

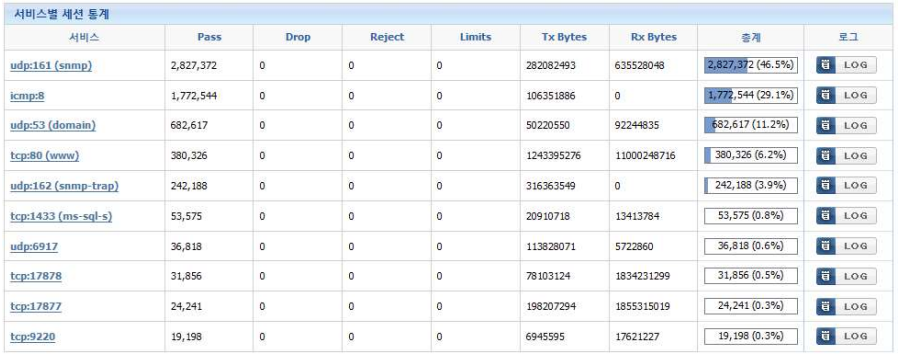
7 방화벽(정책) 설정

7-1 방화벽 & NAT Overview

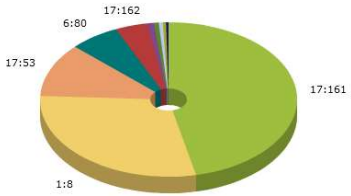
✓ **Stateful Inspection Firewall 지원**
- Rule, Session 개수에 무관한 성능 보장
- 다양한 NAT 기능 지원(1:1, N:1, M:N, Static NAT, Excluded NAT, ECMP NAT, Double NAT)
- 직관적인 객체 관리기능 지원 (IP Address, Service, Time)
- 정책별 세션 제한 기능 지원
- 장비 자체 통계 리포트 지원(출발지/목적지 IP별, 서비스별, 정책별)
- Dashboard를 통한 시스템 상태 모니터링 지원(Concurrent Session, New Session, Concurrent Log)

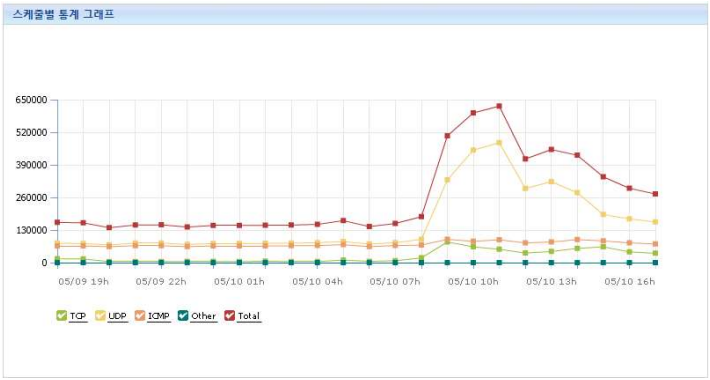
✓ **HA(High Availability)**
- Active-Active, Active-Standby, Clustering HA 지원 (Without L4)
- Dynamic Routing / VRRP를 이용한 Full-Mash Firewall 지원

✓ **인증**
- ID/PASSWORD 기반 인증, OTP(One-Time Password), TACAS+, RADIUS 지원
- Privilege를 이용한 ID별 권한 설정

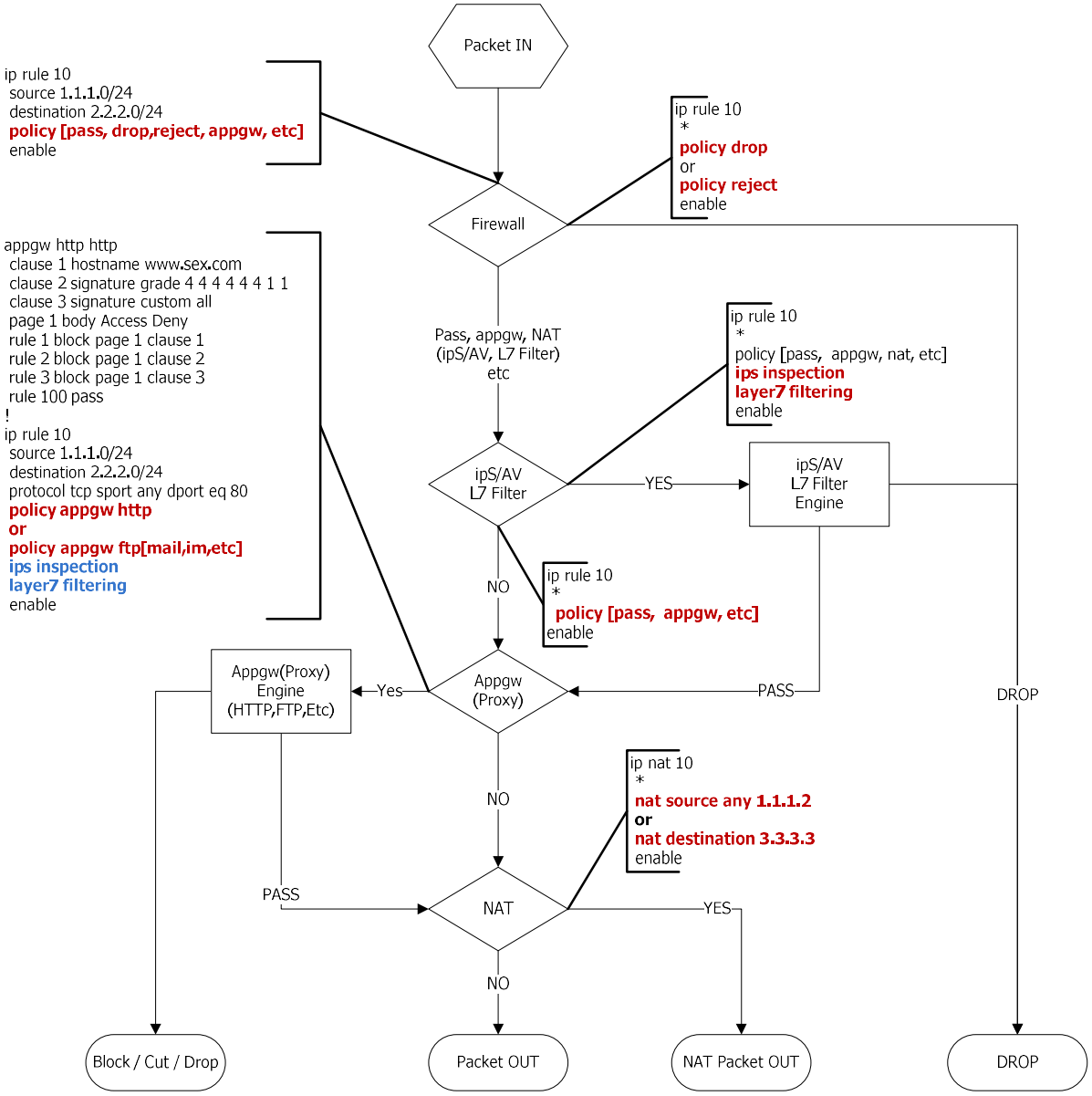

서비스별 세션 통계

서비스	Pass	Drop	Reject	Limits	Tx Bytes	Rx Bytes	총계	로그
udp:161 (snmp)	2,827,372	0	0	0	282082493	635528048	2,827,372 (46.5%)	LOG
icmp:8	1,772,544	0	0	0	106351886	0	1,772,544 (29.1%)	LOG
udp:53 (domain)	682,617	0	0	0	50220550	92244835	682,617 (11.2%)	LOG
tcp:80 (www)	380,326	0	0	0	1243395276	11000248716	380,326 (6.2%)	LOG
udp:162 (snmp-trap)	242,188	0	0	0	316363549	0	242,188 (3.9%)	LOG
tcp:1433 (ms-sql-s)	53,575	0	0	0	20910718	13413784	53,575 (0.8%)	LOG
udp:6917	36,818	0	0	0	113828071	5722860	36,818 (0.6%)	LOG
tcp:17878	31,856	0	0	0	78103124	1834231299	31,856 (0.5%)	LOG
tcp:17877	24,241	0	0	0	198207294	1855315019	24,241 (0.3%)	LOG
tcp:9220	19,198	0	0	0	6945595	17621227	19,198 (0.3%)	LOG





7-2 방화벽 정책 흐름(Flow)



PASS

ip rule 10
*
policy **pass**
enable

DROP

ip rule 10
*
policy **drop**
enable

HTTP APPGW

ip rule 10
*
policy **appgw http**
enable

FTP APPGW

ip rule 10
*
policy **appgw ftp**
enable

DNAT

ip nat 10
*
nat destination a.b.c.d
enable

SNAT

ip nat 10
*
nat source eth1 a.b.c.d
enable

NO NAT

ip nat 9
source host 1.1.1.1
destination host 2.2.2.2
no nat
enable

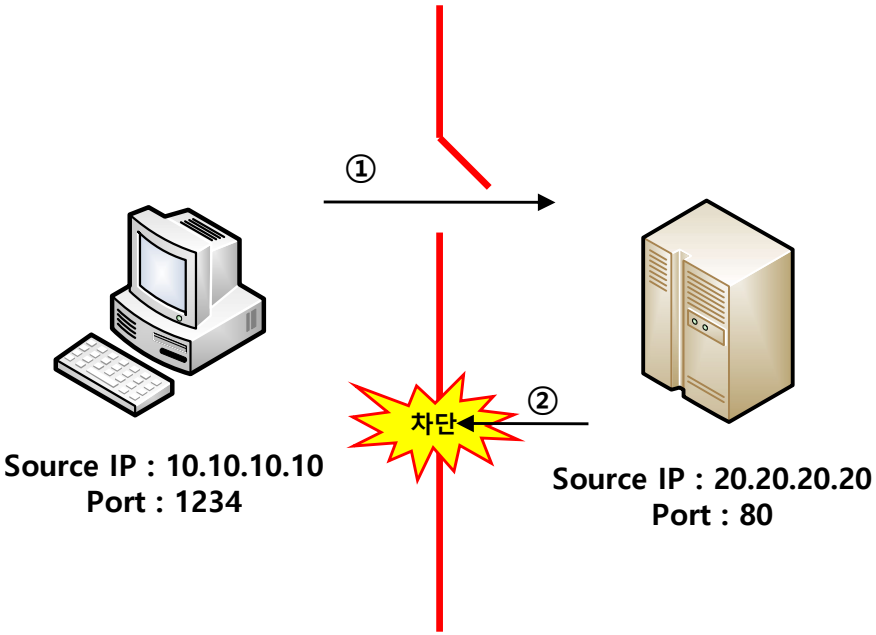
Double NAT

ip nat 20
source host 1.1.1.1
destination host 2.2.2.2
nat source any 1.1.1.3
nat destination 2.2.2.4
enable

7-3 Stateful Inspection 동작 방식

Stateless(ACL) 방식

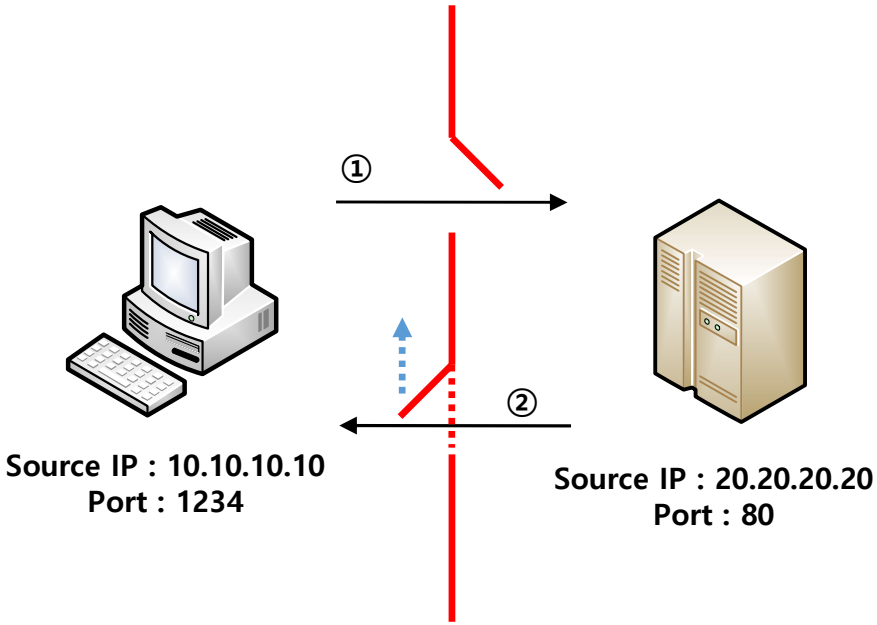
PASS : 10.10.10.10/32 → 20.20.20.20/32



• 라우터, 스위치에서 ACL을 설정 Packet Filtering
• 각 Packet의 SRC, DST / IP, Port에 대한 단순 Filtering
• Return Packet Flow에 대한 별도의 rule 설정 필요

Statefull 방식

PASS : 10.10.10.10/32 → 20.20.20.20/32



• 관리 운용의 편의성 증가
• Packet filtering에 비해 부하 증가
• Returned Packet Flow에 대한 Rule 자동 생성

7-3 Stateful Inspection 동작 방식

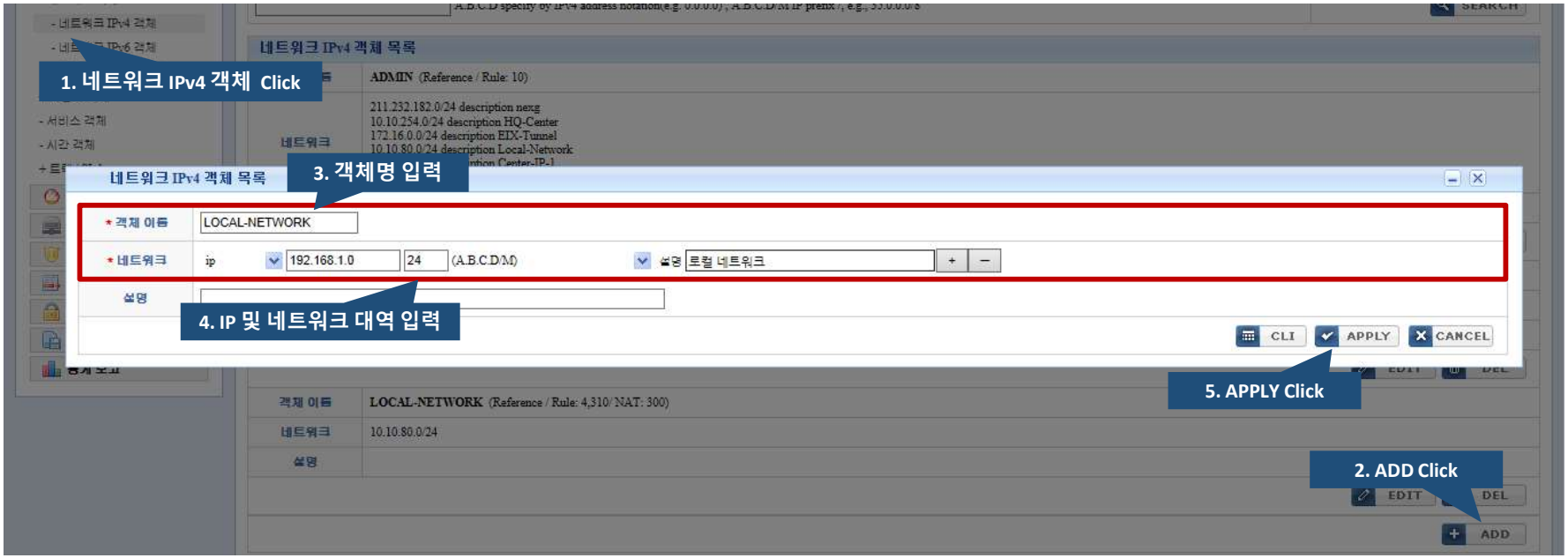
com1 (115200) – 네트워크 객체 설정

```
VForce(config)#network-list range 192.168.1.1 192.168.1.100
VForce(config)#network-list local 192.168.1.0/24
VForce(config)#network-list server 192.168.1.200
!
VForce# sh run ip rule 100
ip rule 100
 source network-list range
 source network-list local
 destination network-list server
 policy pass
 enable
```

(1) : network-list 의 range 객체 정의
(2) : network-list 의 local 객체 정의
(3) : network-list 의 server의 객체 정의

(4) : network-list 의 range 객체 적용
(5) : network-list 의 local 객체 적용
(6) : network-list 의 server의 객체 적용

http / https – 네트워크 객체 설정



7-4 WebUI 네트워크 객체 설정

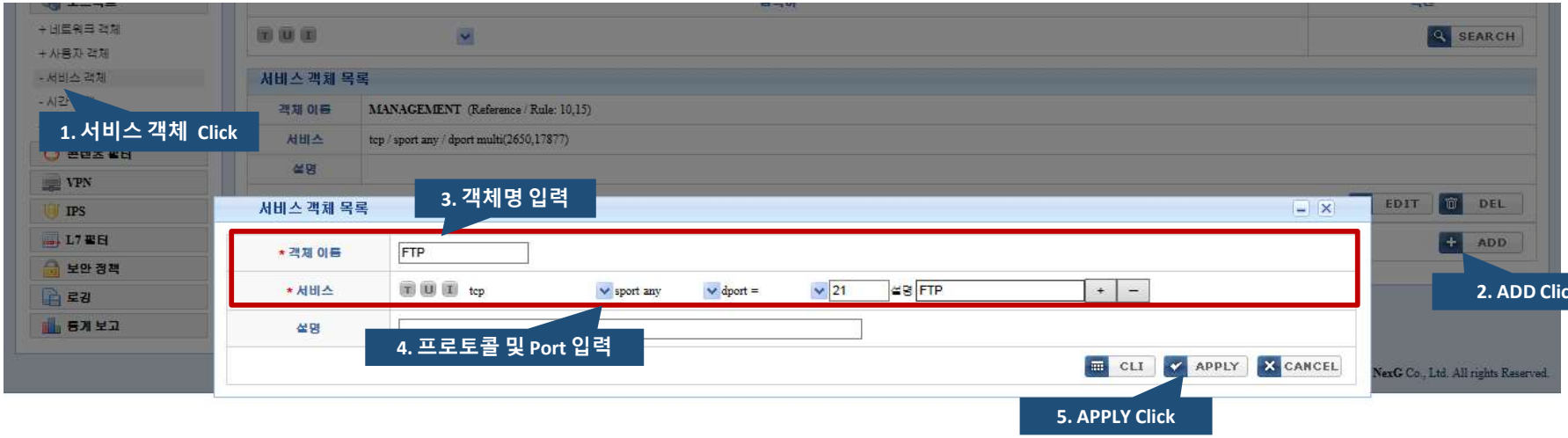
com1 (115200) – 네트워크 객체 설정

```
VForce(config)#service-list test icmp
VForce(config)#service-list test tcp sport any dport eq 80 description http
VForce(config)#service-list test tcp sport any dport eq 53 description dns
VForce(config)#service-list test udp sport any dport eq 53 description dns
!
VForce#sh run ip rule 9999
 source network-list local
 destination network-list server
 service-list test
 policy pass
 enable
```

(1) : service-list의 test 객체 정의

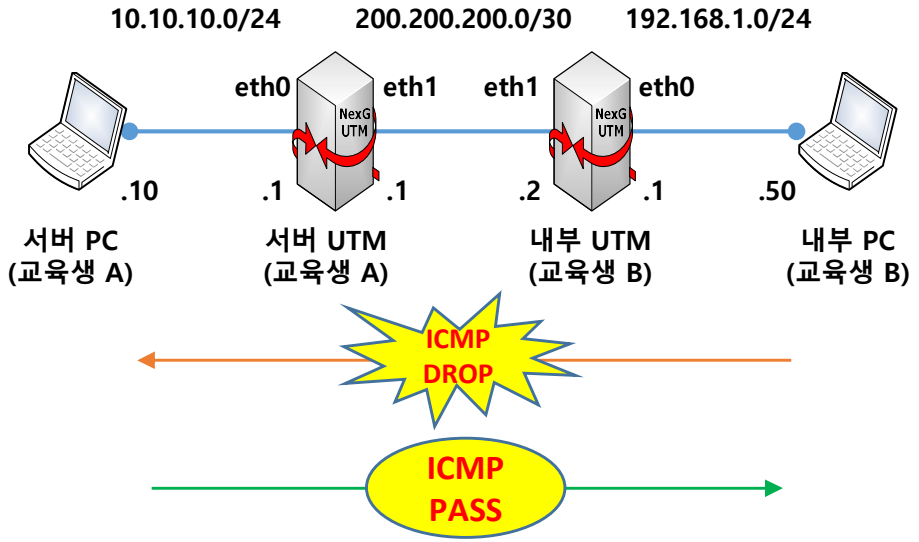
(2) : service-list 객체 적용 예

http / https – 서비스 객체 설정



7-5 WebUI 네트워크 객체 설정

방화벽 구성도 예시



com1 (115200) – 방화벽 설정

```
vforce# conf t
*vforce(config)# ip rule 100
*vforce(config-ip-rule)# description TEST rule
*vforce(config-ip-rule)# source 192.168.1.0/24
*vforce(config-ip-rule)# destination 10.10.10.10/32
*vforce(config-ip-rule)# protocol icmp
*vforce(config-ip-rule)# policy drop
*vforce(config-ip-rule)# log connections ---------▶ 방화벽 Log를 남김
*vforce(config-ip-rule)# enable
*vforce(config-ip-rule)# end
*vforce
```

✓ Protocol 지정이 되지 않으면 모든 Protocol을 의미함.

✓ **Session Log 보기**

```
vforce# show logging
5 Lines:
Index  Time          Proto  Policy Rule  Type  Src          Dst          Spt-c  Dpt-t  Bytes  Packets  R_Src    R_Dst    R_Spt-c  R_Dpt-t  R_Bytes  R_Packets  Count
000000 04-05 16:34:10 icmp   drop   20    n/a   192.168.1.50  10.10.10.10  0      8      0      0        0.0.0.0  0.0.0.0  0        0        0        0          5
000001 04-05 16:34:21 icmp   drop   20    n/a   192.168.1.50  10.10.10.10  0      8      0      0        0.0.0.0  0.0.0.0  0        0        0        0          5
```

7-7 방화벽 설정 예

EX) 단방향 허용(PASS)	EX) 양방향 허용(PASS)
ip rule 11 source 192.168.1.0/24 destination 10.10.10.0/24 policy pass enable	ip rule 12 source 192.168.1.0/24 destination 10.10.10.0/24 policy pass bi-direction enable

EX) Application Gateway 정책	EX) Application Gateway 정책
ip rule 13 source 192.168.1.0/24 destination 10.10.10.0/24 policy appgw [정책 객체 이름] enable	ip rule 13 source 192.168.1.0/24 destination 10.10.10.0/24 policy appgw http enable

EX) 단방향 차단(DROP)	EX) 양방향 차단(DROP)
ip rule 13 source 192.168.1.0/24 destination 10.10.10.0/24 policy drop or policy reject enable	ip rule 14 source 192.168.1.0/24 destination 10.10.10.0/24 policy drop bi-direction or policy reject bi-direction enable

EX) Application Gateway 정책	EX) Application Gateway 정책
ip rule 13 source 192.168.1.0/24 destination 10.10.10.0/24 policy appgw ftp enable	ip rule 13 source 192.168.1.0/24 destination 10.10.10.0/24 policy appgw im enable

7-8 방화벽 설정 옵션

방화벽 룰(Rule) 매칭(Matching) 조건

```
ip rule 100
 source  host 192.168.1.55
 source  host 192.168.1.56
 destination host 168.126.63.1
 destination host 168.126.63.2
 protocol icmp
 protocol tcp sport any dport eq 53
 protocol tcp sport any dport eq 80
 protocol udp sport any dport eq 53
 policy pass
 enable
```

출발지 host IP 가 192.168.1.55 또는
출발지 host IP 가 192.168.1.56 이면서
목적지 host IP 가 168.126.63.1 또는
목적지 host IP 가 168.126.63.2 이면서
프로토콜이 icmp 또는
tcp 프로토콜 목적지 포트가 53 번 또는
udp 프로토콜 목적지 포트가 80 번 또는
udp 프로토콜 목적지 포트가 53 번 일때
패킷을 통과 시킴

- ✓ **방화벽 rule 정책에서 같은 항목과는 or 조건 다른 항목과는 and 조건 처리**
- ✓ **출발지 IP 에서 목적지로 IP로 통신 할 때 해당 프로토콜 및 포트 번호만 허용**
- ✓ **역방향으로 목적지 IP 에서 패킷이 생성되어 출발지 IP로 들어오는 패킷은 방화벽 허용 룰이 없기 때문에 차단됨**

방화벽 룰(Rule) 번호(Sequence) 일괄 변경

```
UTM-1(config)# ip rule resequence start 100 increment 100
```

rule 전체를 100 부터 시작해서 100씩 증가 하도록 변경 설정

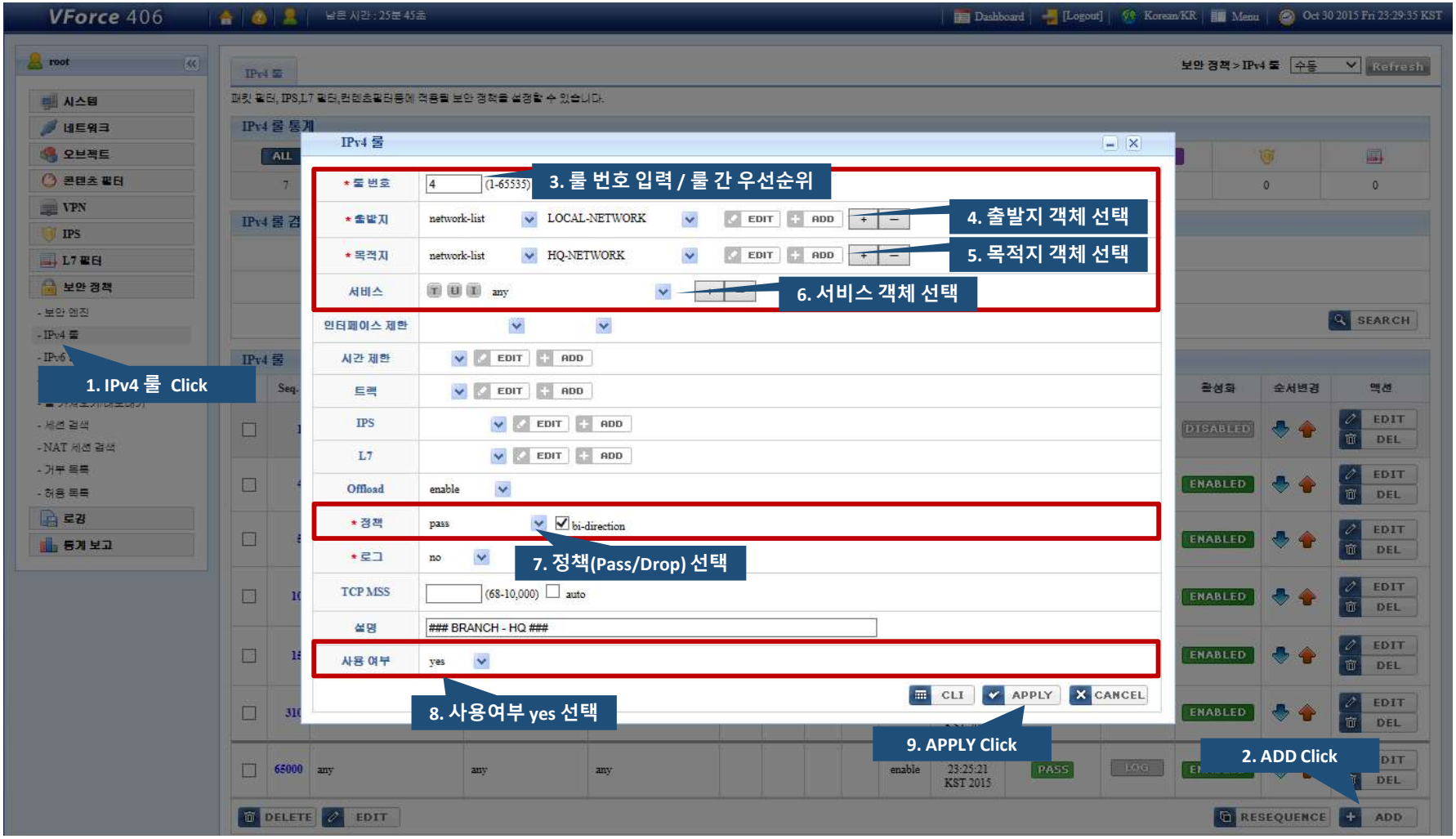
방화벽 룰(Rule) 옵션

```
ip rule 110
 source 192.168.1.0/24
 destination any
 protocol tcp sport any dport eq 80
 inbound interface eth1
 policy appgw http
 log connections
 session-limit 100000
 layer7 filtering
 ips inspection
 enable
```

패킷이 들어오는 인터페이스를 지정 하고 싶을 경우 설정
방화벽 정책 설정 (pass, drop, reject, appgw, etc)
해당된 룰에 걸린 패킷 정보를 로그를 남기고 싶을 경우 설정
해당 방화벽 룰에서 출발지 아이피별 세션 제한을 설정
해당 방화벽 룰의 L7 Filter 를 적용 (policy 옵션이 없을 경우 기본 정책 0 번)
해당 방화벽 룰의 IPS 정책 적용 (policy 옵션이 없을 경우 기본 정책 0번)

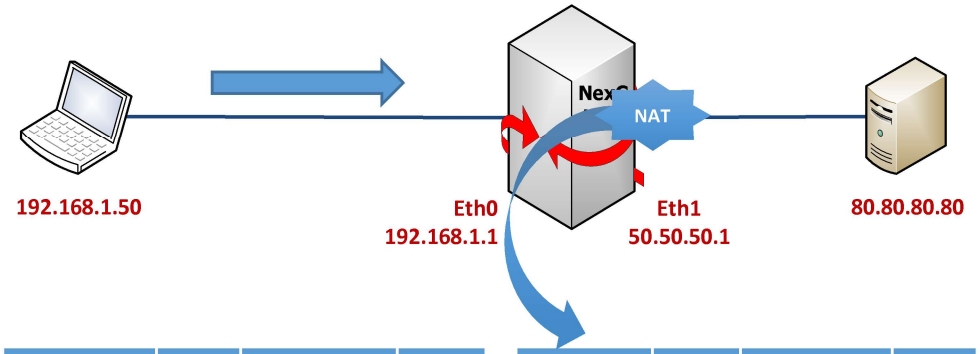
7-9 WebUI 방화벽 설정

http / https – 방화벽 설정



7-10 NAT 설정 실습

NAT 구성도 예시(SNAT)



출발지 IP	Port	목적지 IP	Port
192.168.1.50	2900	80.80.80.80	80

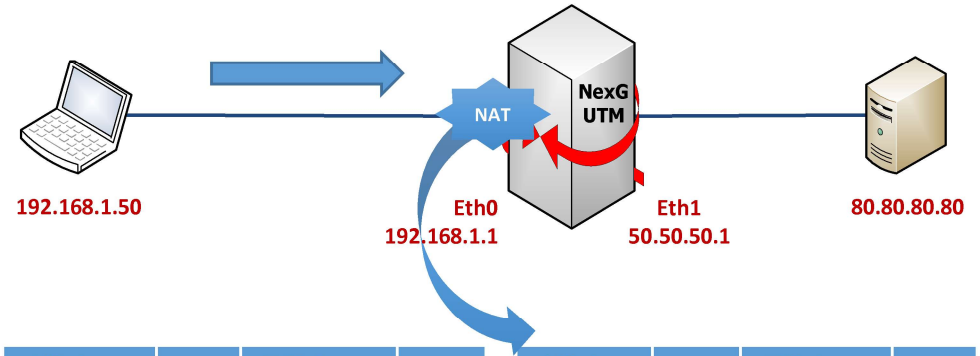
출발지 IP	Port	목적지 IP	Port
50.50.50.1	2900	80.80.80.80	80

com1 (115200) – Source NAT 설정

```
vforce#
vforce#config t
vforce(config)#ip nat 100 ----------> NAT Rule 번호
vforce(config-ip-nat)#source host 192.168.1.50 ----------> 출발지 IP 설정
vforce(config-ip-nat)#destination host 80.80.80.80 ----------> 목적지 IP 설정
vforce(config-ip-nat)#nat source eth1 auto ----------> NAT IP/인터페이스 설정
vforce(config-ip-nat)#enable ----------> NAT 활성화
vforce(config-ip-nat)#end
vforce#
```

✓ *Source NAT : 최종 경로를 선택후 패킷이 나갈때 Source IP를 변경 함.*

NAT 구성도 예시(DNAT)



출발지 IP	Port	목적지 IP	Port
192.168.1.50	2900	80.80.80.80	80

출발지 IP	Port	목적지 IP	Port
50.50.50.1	2900	80.80.80.80	80

com1 (115200) – Destination NAT 설정

```
vforce#
vforce#config t
vforce(config)#ip nat 110 ----------> NAT Rule 번호
vforce(config-ip-nat)#source host 192.168.1.50 ----------> 출발지 IP 설정
vforce(config-ip-nat)#destination host 80.80.80.80 ----------> 목적지 IP 설정
vforce(config-ip-nat)#nat destination 80.80.80.81 ----------> NAT IP/인터페이스 설정
vforce(config-ip-nat)#enable ----------> NAT 활성화
vforce(config-ip-nat)#end
vforce#
```

✓ *Destination NAT : 패킷이 들어 오면 바로 Destination IP를 변경 함*

7-11 NAT 설정 예

EX) SNAT(PAT – Interface 1개)

```
ip nat 15
 source 192.168.1.0/24
 destination any
 nat source eth1 auto
 enable
```

패킷이 eth1로 나갈 때 eth1 인터페이스 IP로 NAT

EX) SNAT(PAT-Interface 2개)

```
ip nat 16
 source 192.168.1.0/24
 destination any
 nat source eth1 auto eth2 auto
 enable
```

패킷이 eth1, eth2로 나갈 때 eth1, eth2 인터페이스 IP로 NAT

EX) SNAT(M:N / Range)

```
ip nat 21
 source 192.168.1.0/24
 destination any
 nat source range 1.1.1.1 1.1.1.100
 enable
```

패킷이 eth1로 나갈 때 eth1 인터페이스 IP로 NAT

EX) SNAT(M:N / Network)

```
ip nat 22
 source 192.168.1.0/24
 destination any
 nat source eth1 1.1.1.2/31
 enable
```

패킷이 eth1, eth2로 나갈 때 eth1, eth2 인터페이스 IP로 NAT

EX) SNAT(PAT – IP 지정)

```
ip nat 17
 source 192.168.1.0/24
 destination any
 nat source eth2 50.50.50.1
 enable
```

EX) SNAT(1:1 Source NAT)

```
ip nat 18
 source 192.168.1.0/24
 destination any
 nat source eth1 211.231.231.0/24
 enable
```

EX) SNAT(Backup SNAT)

```
ip nat 23
 source 192.168.1.0/24
 destination any
 nat source eth1 auto eth2 auto eix0
1.1.1.1
 enable
```

EX) SNAT(Double NAT)

```
ip nat 24
 source host 192.168.1.55
 destination host 212.233.211.3
 nat source any 212.233.213.4
 nat destnation 192.168.1.3
 enable
```

EX) DNAT(Destination NAT)

```
ip nat 19
 source any
 destination interface eth1
 nat destination 192.168.1.55
 enable
```

EX) DNAT(Destination Port NAT)

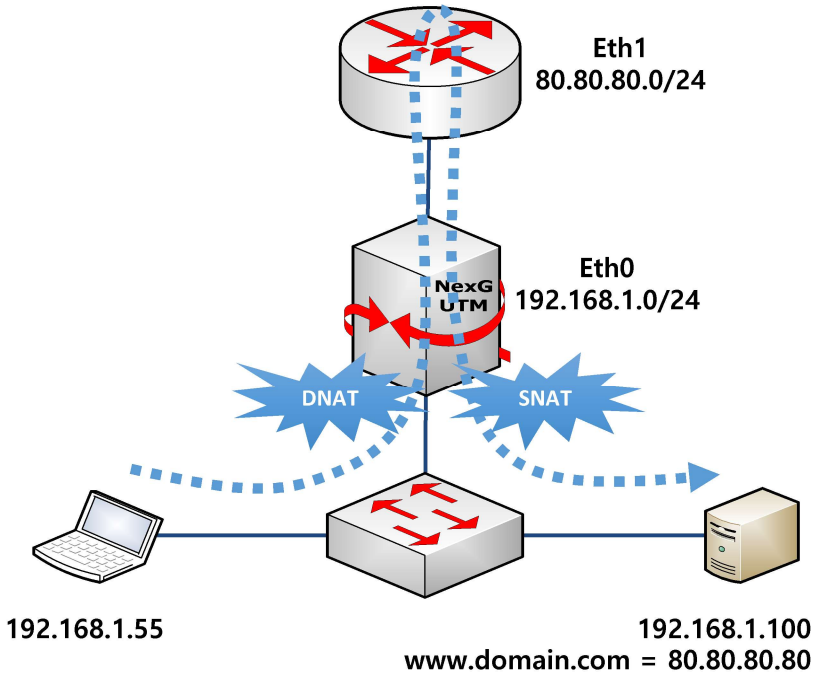
```
ip nat 20
 source any
 destination interface eth2
 protocol tcp sport any dport eq 80
 nat destination 192.168.1.55 port 8080
 enable
```

EX) DNAT(Exclusive SNAt)

```
ip nat 25
 source host 192.168.1.55
 destination any
 no nat
 enable
```

7-12 NAT 설정 심화(1) / Double NAT

Double NAT 구성도 예시



com1 (115200) – Double NAT 설정

```
vforce# conf t
*vforce(config)# ip rule 100
*vforce(config-ip-rule)# description TEST rule
*vforce(config-ip-rule)# source 192.168.1.0/24
*vforce(config-ip-rule)# destination 10.10.10.10/32
*vforce(config-ip-rule)# protocol icmp
*vforce(config-ip-rule)# policy drop
*vforce(config-ip-rule)# log connections --------▶ 방화벽 Log를 남김
*vforce(config-ip-rule)# enable
*vforce(config-ip-rule)# end
*vforce
```

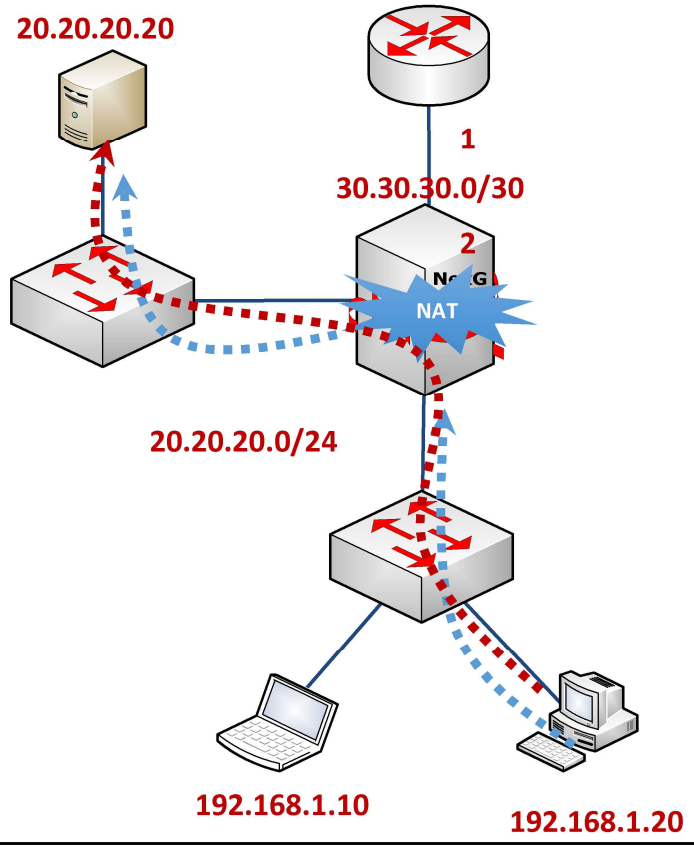
✓ *Protocol 지정이 되지 않으면 모든 Protocol을 의미*

✓ 사설 IP를 사용하는 내부 네트워크에 웹서버 운영시(1:1 NAT 설정) 사설 IP 사용하는

✓ PC가 도메인으로 웹 서버 접속 시 Source IP와 Destination IP를 NAT 변경 해야 정상 접속 가능

7-12 NAT 설정 심화(2) / NO NAT

No NAT 구성도 예시



No nat 설정 필요

```
ip rule 100
 source 192.168.1.0/24
 destination any
 policy pass
 enable
!
ip nat 90
 source 192.168.1.0/24
 destination 20.20.20.0/24
 no nat ← (1)
 enable
!
ip nat 100
 source 192.168.1.0/24
 destination any
 nat source any 30.30.30.2
 enable
!
```

(1) No nat룰이 없을 시 서버로 갈때 NAT 적용

No nat 설정 불필요

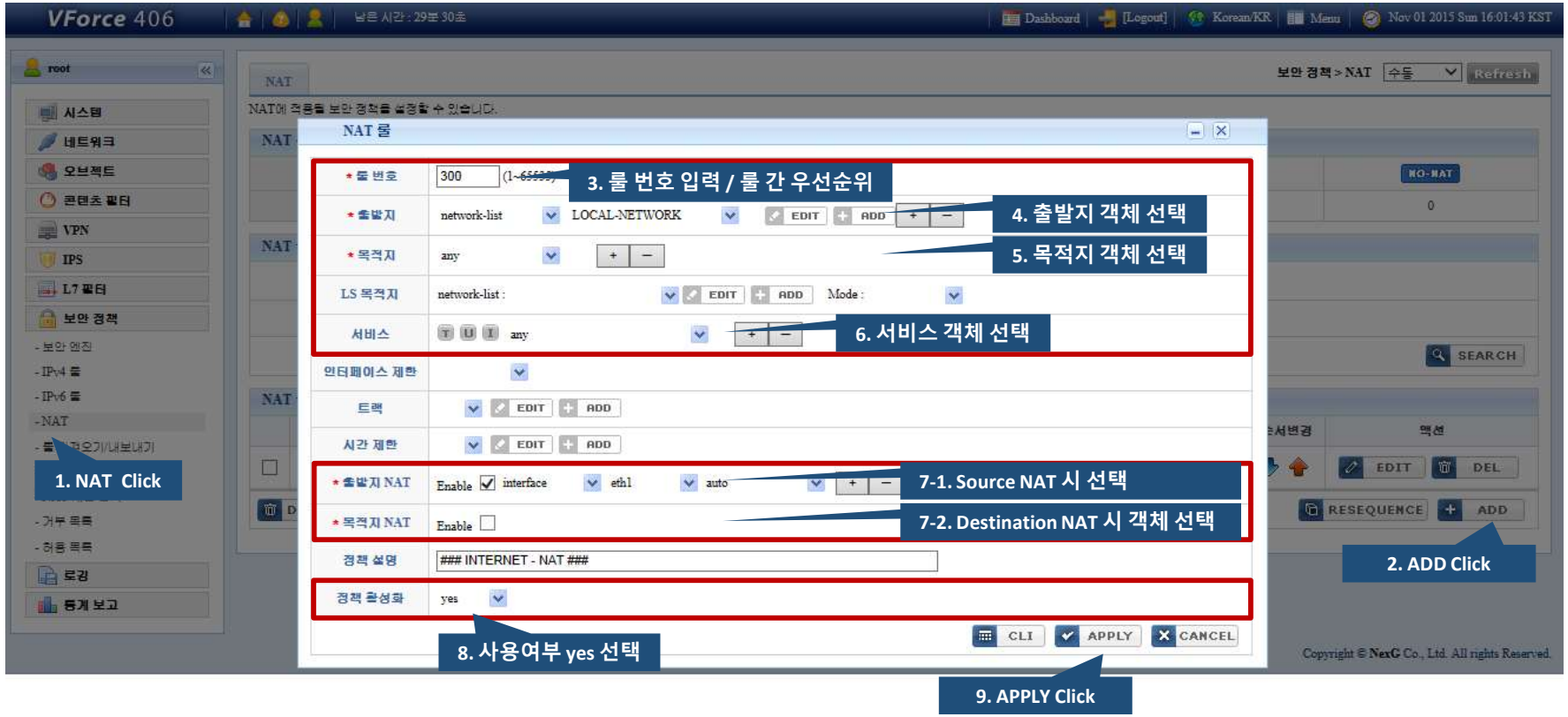
```
ip rule 100
 source 192.168.1.0/24
 destination any
 policy pass
 enable
!
ip nat 100
 source 192.168.1.0/24
 destination any
 nat source eth1 30.30.30.2← (2)
 enable
!
```

(2) 패킷이 eth1 인터페이스 나갈때만 NAT 적용 (No nat룰이 없어도 서버로 갈 때 NAT 적용 안됨)

✓ 라우팅 설정

```
B-UTM-1# sh ip route
!
S*      0.0.0.0/0 [1/0] via 30.30.30.1, eth1
C       192.168.1.0/24 is directly connected, eth0
C       20.20.20.0/24 is directly connected, eth2
```

7-13 WebUI NAT 설정

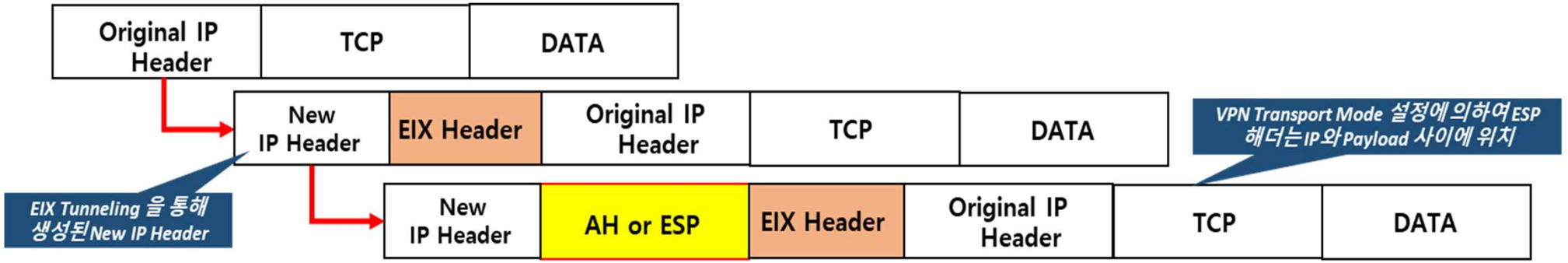


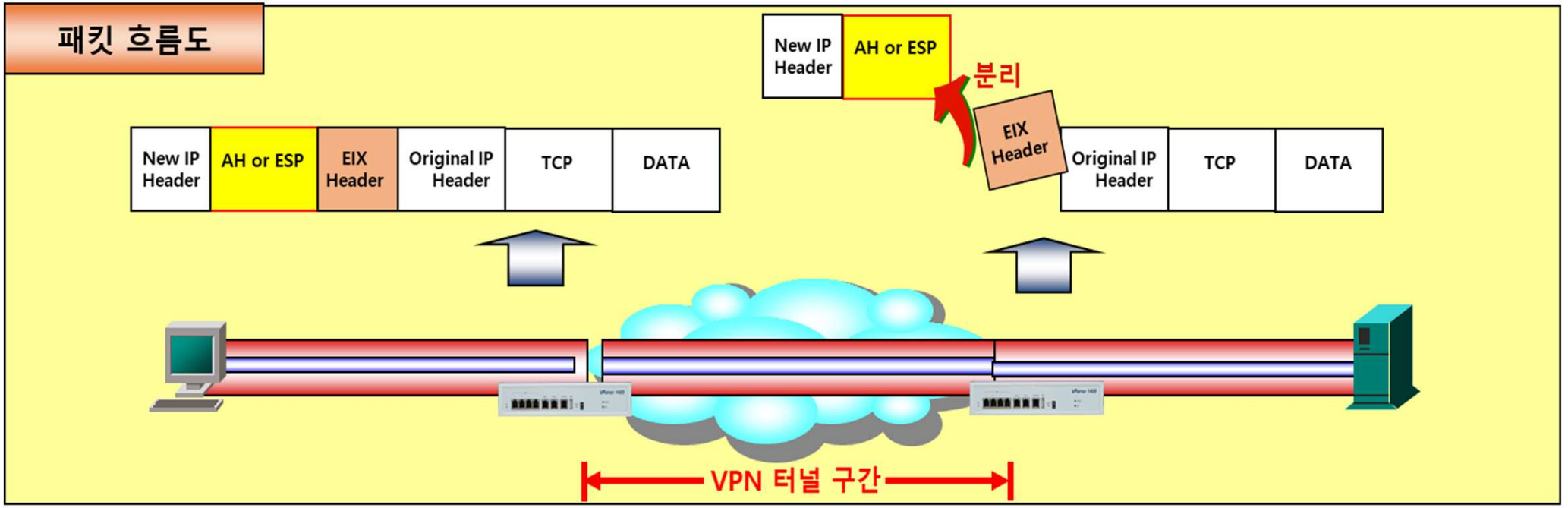
8 EIX VPN

8-1 EIX VPN 개념
8-2 EIX VPN 실습

8-1 EIX(EtherIP eXtended) VPN개념(1)

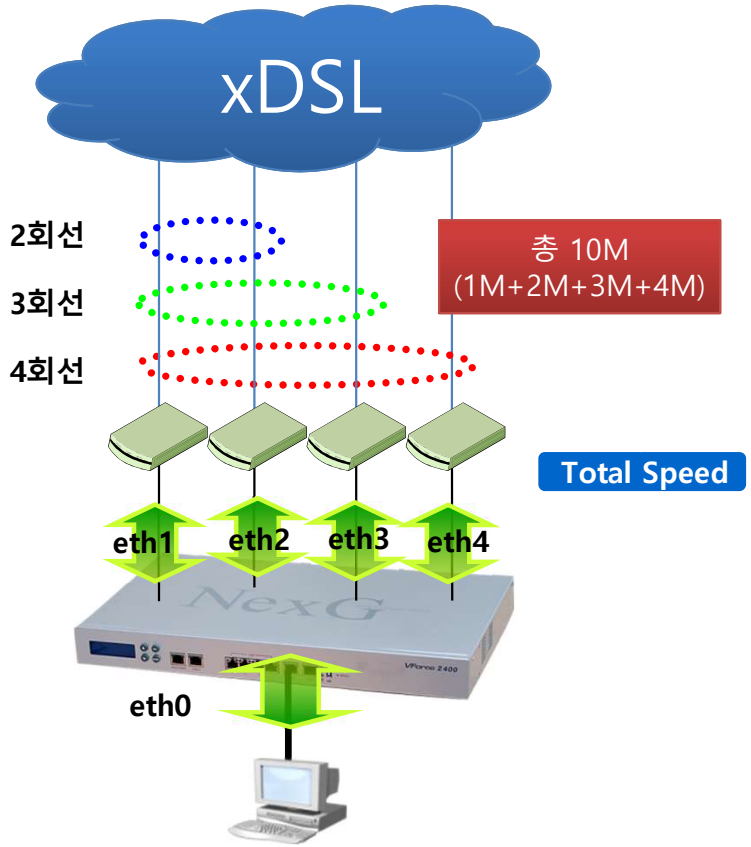
✓ EIX VPN은 확장된 EtherIP를 이용하여 가상의 포인트 to 포인트 연결을 제공하므로 두 Peer간에 라우팅 프로토콜을 사용 가능하게 해준다.





8-2 EIX(EtherIP eXtended) VPN 개념(2)

EIX VPN 구성도 예시(1)



※ xDSL 1회선당 평균 속도
- ➲ Upload 512Kbps
- ➲ Download 3Mbps

※ xDSL 4회선 Bonding 속도
- ➲ Upload 2Mbps
- ➲ Download 10Mbps

EIX Interface 설정 예

```
interface eix0
 eix destination 1.1.1.1
 eix destination 1.1.1.2
 eix destination 1.1.1.3
 eix destination 1.1.1.4
 eix destination 1.1.1.5
 eix destination 1.1.1.6
 eix source eth1
 eix source eth2
 eix source eth3
 eix source eth4
 ip address 172.16.1.1/16
```

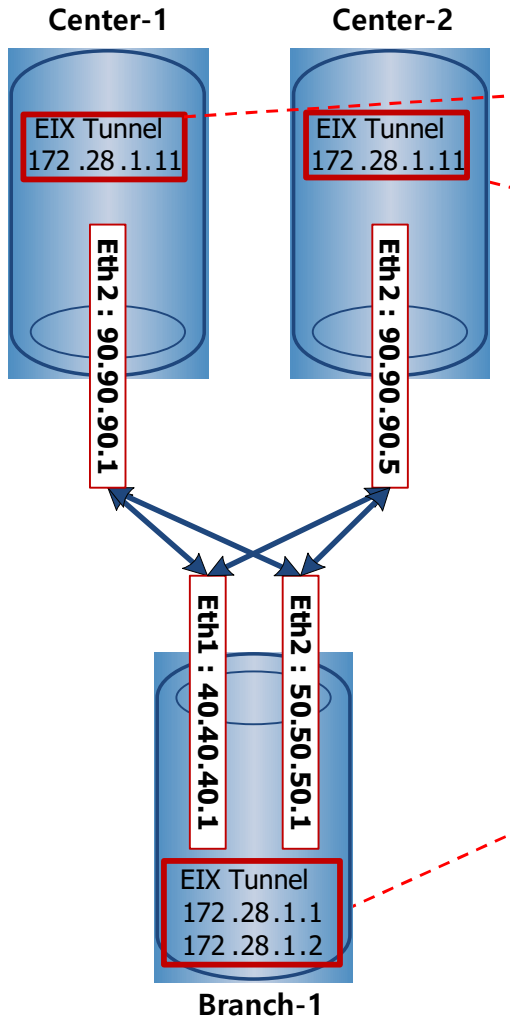
EIX Source Interface 추가

EIX 터널 IP

✓ **EIX (EtherIP eXtended) / EIX over IPSec**
- **ADSL/VDSL 회선 Bonding**
- **다른 속도 Bonding 에 강점**
- **RTT 고려하여 Packet**

8-2 EIX(EtherIP eXtended) VPN 개념(3)

EIX VPN 구성도 예시(2)



EIX Session 및 Tunnel 테이블

Center-1# sh eix tunnel

Identity	Peer IP	Status
66:69:78:18:41:37	172.28.1.11	up(2/2)

고정IP link-timeout 설정

Center-1# sh eix session

Local	Remote	Status	Upload	Download	RTT	Tunnel
90.90.90.1	40.40.40.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:37
90.90.90.1	50.50.50.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:37

Center-2# sh eix tunnel

Identity	Peer IP	Status
66:69:78:18:41:37	172.28.1.11	up(2/2)

Center-2# sh eix session

Local	Remote	Status	Upload	Download	RTT	Tunnel
90.90.90.5	40.40.40.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:37
90.90.90.5	50.50.50.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:37

Branch-1# sh eix tunnel

Identity	Peer IP	Status
66:69:78:18:42:8b	172.28.1.2	up(2/2)
66:69:78:18:41:fb	172.28.1.1	up(2/2)

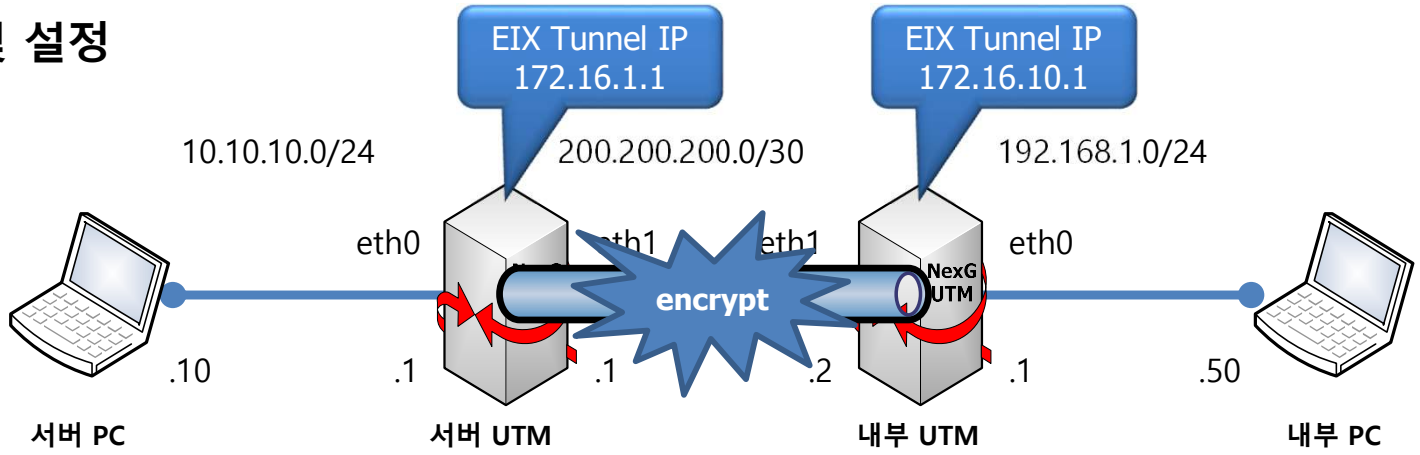
Branch-1# sh eix session

Local	Remote	Status	Upload	Download	RTT	Tunnel
40.40.40.1	90.90.90.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:fb
50.50.50.1	90.90.90.1	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:41:fb
40.40.40.1	90.90.90.5	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:42:8b
50.50.50.1	90.90.90.5	up	1.0Mbps	1.0Mbps	0ms	66:69:78:18:42:8b

- 가상의 포인트 투 포인트 연결을 제공하므로 두 Peer간에 라우팅 프로토콜을 사용 가능하게 해준다.
- 일반 라우팅이 가능해져 PBR 적용도 사용할 수 있게 한다.
- GRE Tunneling 방식과 유사

8-3 EIX VPN 실습

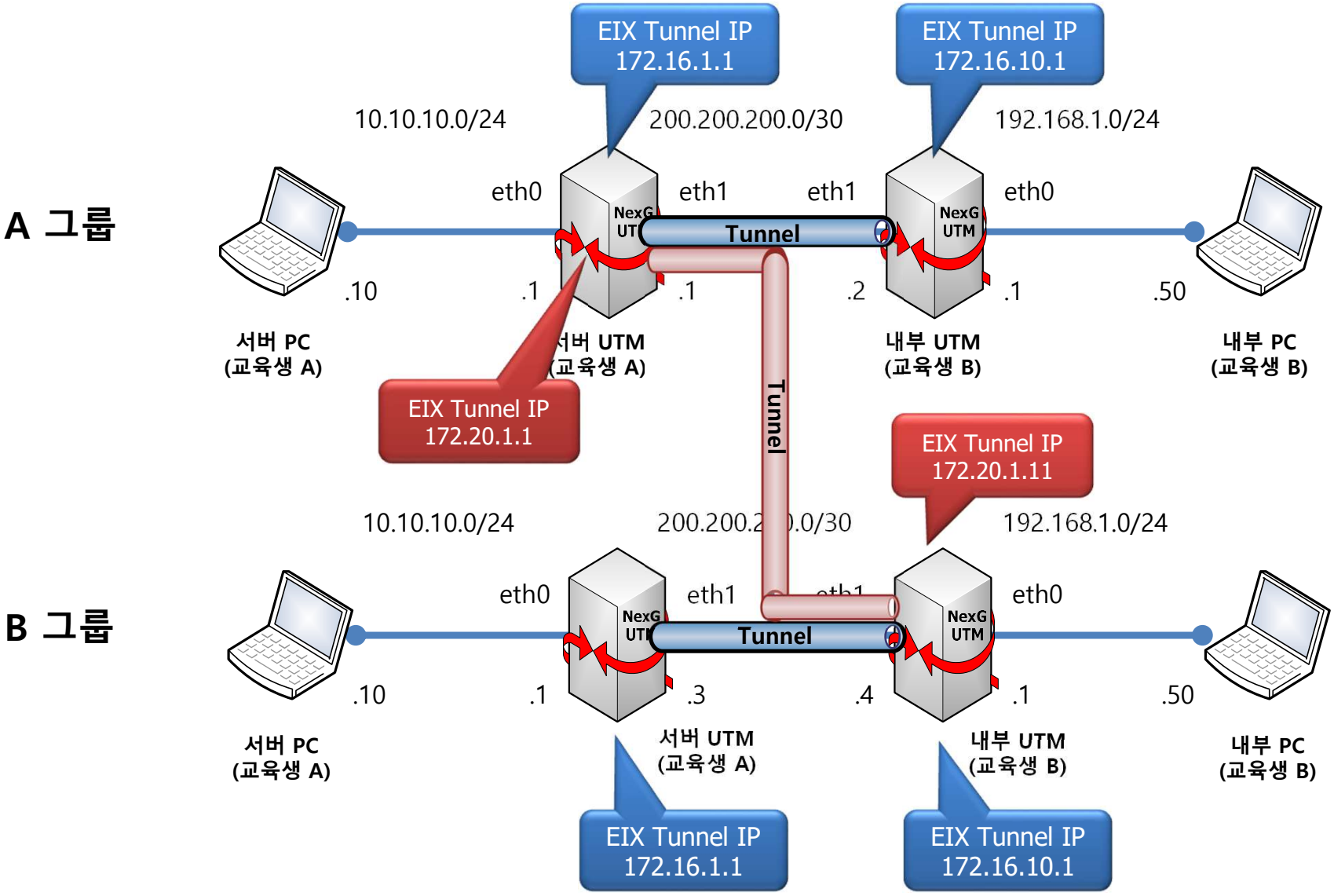
◆ 구성 및 설정



센터	설명
interface eix0	(1) : EIX 인터페이스
eix source eth1	(2) : 센터 WAN IP 또는 인터페이스
eix dpd-timeout 5	(3) : EIX DPD
ip address 172.16.1.1/24	(4) : 센터 EIX 터널 IP
!	
security parameters	
remote-secret test id-type fqdn id branch-1	(5) : 지점 local-identity 값
!	
crypto tunnel center	(6) : 센터 IPsec 설정
priority 255	(7) : VPN 설정 객체 우선 순위
local-identity fqdn center-1	(8) : 센터 인증 Key 값(로컬 ID)
local-secret test	(9) : 지점 인증 Key 그룹명(로컬 secret)
transforms esp aes-128 sha1	(10) : 암호화 종류
ipsec-mode transport	(11) : IPsec Transport Mode
source 200.200.200.1	(12) : 센터 WAN IP
destination any	(13) : 지점 통신 할 대역 any
protocol etherip	(14) : EIX 패킷만 VPN 암호화
enable	(15) : 동작 시작
!	
ip route 192.168.1.0/24 172.16.10.1	(16) : 센터 지점간 통신 하기 위한 라우팅

지점	설명
interface eix0	(1) : EIX 인터페이스
eix destination 200.200.200.1	(2) : 센터 WAN IP
eix source eth1	(3) : 지점 WAN IP 또는 인터페이스
eix dpd-timeout 5	(4) : EIX DPD
ip address 172.16.10.1/24	(5) : 센터 EIX 터널 IP
!	
security parameters	
remote-secret test id-type fqdn id center-1	(6) : 센터 local-identity 값
!	
crypto tunnel branch	(7) : 지점 IPsec 설정
priority 255	(8) : VPN 설정 객체 우선 순위
local-identity fqdn branch-1	(9) : 지점 인증 Key 값(로컬 ID)
local-secret test	(10) : 센터 인증 Key 그룹명(로컬 secret)
transforms esp aes-128 sha1	(11) : 암호화 종류
ipsec-mode transport	(12) : IPsec Transport Mode
source 200.200.200.2	(13) : 지점 WAN IP
destination 200.200.200.1	(14) : 센터 WAN IP
protocol etherip	(15) : EIX 패킷만 VPN 암호화
enable	(16) : 동작 시작
!	
ip route 10.10.10.0/24 172.16.1.1	(17) : 센터 지점간 통신 하기 위한 라우팅

8-4 EIX VPN 실습 (Multi-EIX)

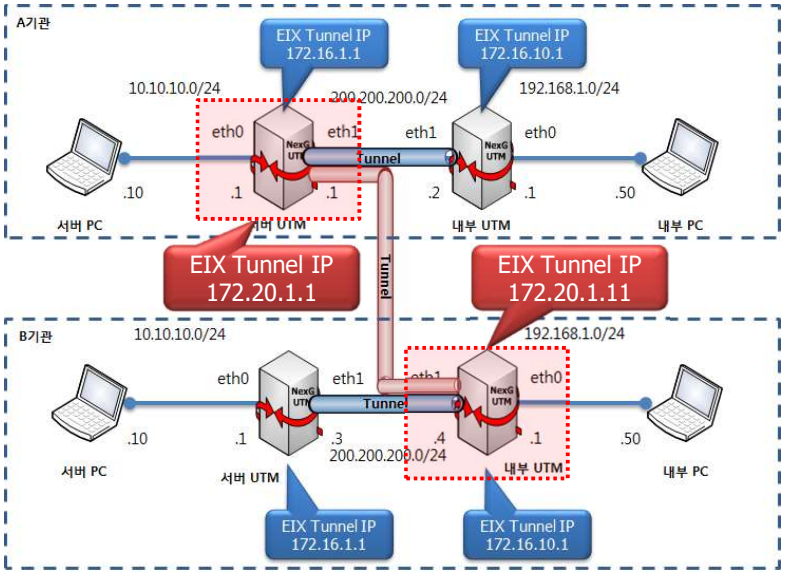


8-4 EIX VPN 실습 (Multi-EIX)

센터 설정 정보

```
security parameters
 mode-type2
 remote-secret test id-type fqdn id B기관ID enable

interface eix[1~255]
 eix source eth1
 eix class-id <1~255>
 eix dpd-timeout 10
 ip address 172.20.1.1/24

crypto tunnel Center
--- 생략 ---
enable

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn A기관ID
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
destination host 200.200.200.4
 protocol etherip
 enable
```

EIX인터페이스 번호는 장비끼리 동일할 필요 없음



지점 설정 정보

```
security parameters
 mode-type2
 remote-secret test id-type fqdn id A기관ID enable

interface eix[1~255]
 eix destination 200.200.200.1
 eix source eth1
 eix class-id <1~255>
 eix dpd-timeout 10
 ip address 172.20.1.11/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn B기관ID
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination host 200.200.200.1
 protocol etherip
 enable
```

옵션 type 1 : Quicksecpm Type 2 : Strongswan

FQDN ID 설정

양 장비 간 Class-ID 동일 (Default 값 :0)

FQDN ID 설정

터널 확인

```
VForcer# show eix tunnel all
Interface eix0: Total 1 tunnel.

Identity        Peer IP        Status      Uptime
6669.7842.16c0  172.16.1.11    up(1/1)     18:42:00
```

기존 터널 상태

```
Interface eix10: Total 1 tunnel.

Identity        Peer IP        Status      Uptime
6669.7855.3638  172.20.1.11    up(1/1)     18:40:26
```

신규 터널 상태

터널 확인

```
*VForcer# show eix tunnel all
Interface eix0: Total 1 tunnel.

Identity        Peer IP        Status      Uptime
6669.7842.16c0  172.16.1.1     up(1/1)     18:42:00

Interface eix10: Total 1 tunnel.

Identity        Peer IP        Status      Uptime
6669.7855.3638  172.20.1.1     up(1/1)     18:40:26
```

9 Trouble Shooting

9-1 패스워드 복구

U-Boot Mode : 패스워드 복구

U-Boot 1.1.1 (Development build) (Build time: Jul 15 2008 - 21:13:03) ---> *장비 전원 리부팅*
CUST_VF2400 board revision major:2, minor:0, serial #: VF24000800023
OCTEON CN31XX-NSP revision: 2, Core clock: 500 MHz, DDR clock: 266 MHz
(532 Mhz data rate)
Hareware Monitor: Winbond w83792d.
Programming Vitesse switch .... done.
Disabling switch port ..... done. ---> *Ctrl + c 키 입력 하여 boot 모드 진입*
DRAM: 1024 MB
Flash: 8 MB
Clearing DRAM..... done
BIST check passed.
Starting PCI
PCI Status: PCI 32-bit
PCI BAR 0: 0x08000000, PCI BAR 1: Memory 0x00000000 PCI 0x00000000
Net: octeth0, octeth1, octeth2
 Bus 0 (CF Card): OK
VF406# <INTERRUPT>
VF406# $(bootcmd) single ---> *비밀번호 복구 명령어 입력*
reading vos.bin
* ############################부팅 생략
############################*
INIT[194]: logd will be started
The loading might take a while to process... Wait a moment
Please press Enter to activate this console. ---> *비밀번호 없이 로그인 가능*
NexG VOS Software, Version 4.2-r22029 10/06/09 11:56:19
UTM-1> ---> *저장 가능 모드로 진입하기 위한 명령어 입력*
UTM-1> restore pri
UTM-1# ---> *패스워드 변경*
*UTM-1 (config)# username root secret admin1234
*UTM-1 (config)# end ---> *변경된 설정 저장*
*UTM-1# wr
Building configuration...
[OK] ---> *장비 리부팅*
UTM-1# reload
Proceed with reload? [yes/no] y

9-2 실시간 트래픽 확인

Bwm 명령어 : 실시간 트래픽량 확인

vforce# start-shell
/media/disk0 # **bwm -u bits -d**

Bandwidth Monitor v0.5 (delay 1.000s); press 'ctrl-c' to end this

/ iface	Rx	Tx	Total
eth0:	22.24 Mb/s	2.01 Mb/s	24.25 Mb/s
eth1:	6.31 Kb/s	4.49 Kb/s	10.79 Kb/s
eth2:	1.95 Mb/s	21.80 Mb/s	23.75 Mb/s
eth3:	0.00 b/s	0.00 b/s	0.00 b/s
lo:	0.00 b/s	0.00 b/s	0.00 b/s
* 생 략 *			
eix0:	0.00 b/s	0.00 b/s	0.00 b/s
vlan0.1:	0.00 b/s	0.00 b/s	0.00 b/s
total:	24.20 Mb/s	23.79 Mb/s	47.99 Mb/s

UTM-1# start-shell
/media/disk0 # **bwm -u bits -I eth0,eth1,eth2**

Bandwidth Monitor v0.5 (delay 1.000s); press 'ctrl-c' to end this

iface	Rx	Tx	Total
eth0:	5.92 Kb/s	0.00 Kb/s	5.92 Kb/s
eth1:	0.00 Kb/s	0.00 Kb/s	0.00 Kb/s
eth2:	0.00 Kb/s	0.00 Kb/s	0.00 Kb/s
total:	5.93 Kb/s	0.00 Kb/s	5.93 Kb/s

-u : bytes, bits, packets, errors / -d : K 또는 M 용량 자동 계산 출력 /
-I : 인터페이스

과다 트래픽 발생(TX/RX)시 외부 공격으로 의심되며, 원인 분석을 위하여 해당 트래픽 분석이 필요함

9-3 실시간 패킷 캡처(1)

tcpdump 명령어 : 실시간 패킷 캡처	tcpdump 명령어 : 이상 패킷 수집 & 전송
UTM-1# **start-shell** /media/disk0 # **tcpdump -ni eix0 port 80** device eth0 entered promiscuous mode tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes 23:25:38.568120 IP 192.168.1.55.2798 > 211.233.29.229.80: P 3205412440:3205412782(342) ack 2151009431 win 46425 23:25:38.577304 IP 211.233.29.229.80 > 192.168.1.55.2798: . 1:1301(1300) ack 342 win 8576 23:25:38.586830 IP 192.168.1.55.2798 > 211.233.29.229.80: . ack 4038 win 46440 23:25:39.252951 IP 211.115.115.77.80 > 192.168.1.55.2786: F 1576423558:1576423558(0) ack 1063176899 win 7504 23:25:39.253054 IP 211.115.115.77.80 > 192.168.1.55.2783: F 1579788893:1579788893(0) ack 1951857196 win 7504 23:25:39.253126 IP 192.168.1.55.2786 > 211.115.115.77.80: . ack 1 win 46425 23:25:39.253217 IP 192.168.1.55.2783 > 211.115.115.77.80: . ack 1 win 46425 23:25:39.260046 IP 211.115.115.77.80 > 192.168.1.55.2784: F 1678655931:1678655931(0) ack 840783774 win 7504 23:25:39.260216 IP 192.168.1.55.2784 > 211.115.115.77.80: . ack 1 win 46292 23:25:39.294091 IP 211.115.115.77.80 > 192.168.1.55.2787: F 1615723517:1615723517(0) ack 251283718 win 7504 23:25:39.294192 IP 211.115.115.77.80 > 192.168.1.55.2808: F 1614937698:1614937698(0) ack 1603444436 win 7504 23:25:39.294248 IP 192.168.1.55.2787 > 211.115.115.77.80: . ack 1 win 46425 23:25:39.294289 IP 211.115.115.77.80 > 192.168.1.55.2782: F 1628110907:1628110907(0) ack 1311185782 win 7504 예) ***# tcpdump -i eth0 –pn 'tcp[tcpflags] & (tcp-rst|tcp-syn) != 0'*** ***# tcpdump -i eth0 –pn 'tcp[tcpflags] & (tcp-rst|tcp-syn) != 0' and dst host 서버 IP*** ***# tcpdump –i eth0 –pn 'tcp[tcpflags] & tcp-syn != 0'*** ***# tcpdump -ni eth0 tcp[13] = 0***	UTM-1# start-shell /media/disk0 # **/media/disk0 # tcpdump -ni eth0 host 192.168.1.55 -s0 -w virus.cap** tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes **[캡쳐 중지시 CTRL + C]** 158 packets captured 158 packets received by filter 0 packets dropped by kernel /media/disk0 # exit UTM-1# sh disk0:/ -#- --type-- nlen ---length--- --------date/time-------- name **1 File 9 5725238 Mon Jul 27 09:24:28 2009 virus.cap** UTM-1# **copy disk0:/virus.cap ftp://192.168.1.55/** !!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! 5725238 bytes transferred *(1): Application 문제 또는 Virus 패킷을 수집 하고 싶을 때는 들어오는 인터페이스에서 패킷 덤프를 실행* *(2): 패킷덤프는 최대한 필요한 부분만 필터링 하여 수집* *(3): tcpdump 에서 –s0 옵션을 선택하여 패킷의 전체를 캡춰* *(4): tcpdump 에서 –w [파일이름] 옵션을 선택하여 파일로 저장* *(5): 해당된 파일을 FTP를 통하여 전송 Wireshark 또는 기타 프로그램으로 패킷 분석*

9-3 실시간 패킷 캡처(2)

Tcpdump Command Line Options(1)	
-A	Print frame payload in ASCII
-c <count>	Number : 제시된 수의 패킷을 받은 후 종료한다.
-D	List available interfaces
-e	출력되는 각각의 행에 대해서 link-level 헤더를 출력한다. 즉 맥어드레스를 함께 출력한다.
-F <file>	filter 표현의 입력으로 파일을 받아들인다. 커맨드라인에 주어진 추가의 표현들은 모두 무시된다.
-G <n>	Rotate the dump file every n seconds
-i <iface>	어느 인터페이스를 경유하는 패킷들을 잡을지 지정한다. 지저되지 않으면 시스템의 인터페이스 리스트를 뒤져서 가장 낮은 번호를 가진 인터페이스를 선택한다(이 때 loopback은 제외된다).
-K	Don't verify TCP checksums
-L	List data link types for the interface
-n	모든 주소들을 변환하지 않는다(port, host address 등등) 이것은 DNS lookup을 피할 수 있다.
-p	인터페이스를 promiscuous mode로 두지 않는다.

Tcpdump Command Line Options(2)	
-q	프로토콜에 대한 정보를 덜 출력한다. 따라서 출력되는 라인이 좀 더 짧아진다.
-r <file>	패킷들을 '-w'옵션으로 만들어진 파일로 부터 읽어 들인다. 파일에 "-" 가 사용되면 표준 입력을 통해서 받아들인다.
-s <len>	Capture up to **len** bytes per packet
-S	TCP sequence번호를 상대적인 번호가 아닌 절대적인 번호로 출력한다.
-t	출력되는 각각의 라인에 시간을 출력하지 않는다.
-v[v[v]]	좀 더 많은 정보들을 출력한다. (VVV 더 많은정보)
-w <file>	캡춰한 패킷들을 분석해서 출력하는 대신에 그대로 파일에 저장한다.
-x	각각의 패킷을 헥사코드로 출력한다.
-X	Print frame payload in hex and ASCII
-y <type>	Specify the data link type
-Z <user>	Drop privileges from root to user

9-3 실시간 패킷 캡처(3)

tcpdump 명령어 : 예제

tcpdump -ni eth0 host 192.168.1.50 → *출발지 / 목적지 상관 없이 host IP 에 대해서 캡처*

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
13:53:45.230457 IP 192.168.1.50.53781 > 10.100.44.12.53: 54765+[|domain]

13:53:45.232036 IP 10.100.44.12.53 > 192.168.1.50.53781: 54765[|domain]

13:53:45.233220 IP 192.168.1.50.4979 > 211.234.239.58.80: S
837107015:837107015(0) win 65535 <mss 1460,nop,nop,sackOK>
13:53:45.243336 IP 211.234.239.58.80 > 192.168.1.50.4979: S
2928507481:2928507481(0) ack 837107016 win 5840 <mss 1300>
13:53:45.243610 IP 192.168.1.50.4979 > 211.234.239.58.80: . ack 1 win 65535

13:53:45.256042 IP 211.234.239.58.80 > 192.168.1.50.4979: . ack 373 win 6432
13:53:45.256672 IP 211.234.239.58.80 > 192.168.1.50.4979: F 475:475(0) ack 373 win 6432

13:53:45.257404 IP 192.168.1.50.4979 > 211.234.239.58.80: F 373:373(0) ack 476 win 65061
```

tcpdump -ni eth0 net 192.168.1.0/24 → *Network 대역을 지정 하여 캡처*

tcpdump -ni eth0 src net 192.168.1.0/24 → *출발지를 지정한 network 대역을 캡처*

tcpdump -ni eth0 host 192.168.1.50 and port 80 → *출발지 호스트와 사용 포트를 지정 하여 캡처*

tcpdump -ni eth0 host 192.168.1.50 and port 80 or port 53 → *출발지 호스트 목적지 포트 2개 지정 하여 캡처*

tcpdump -ni eth0 port 80 -X → *80 포트 사용 패킷 캡쳐중 Hex 값으로 패킷 표시*

tcpdump -ni eth0 port 80 -X -s0 → *80 포트 사용 패킷 캡쳐중 Hex 값으로 전체 패킷에 대해 표시*

tcpdump -ni eth0 dst port 80 → *목적지 포트 지정 하여 패킷 캡쳐*

9-4 실시간 로그 확인

명령어 : terminal monitor	
*UTM-1# **terminal monitor ? ← (1)** appgw Application level gateway ips Start monitoring IPS logs ipsec Start monitoring IPsec logs l7filter Start monitoring l7filter logs session Start monitoring session logs system Start monitoring sytem logs	*기능별 실시간 로그 옵션* *; 이벤트 발생 시 실시간 로그 메시지 출력*

< 실시간 시스템 로그 : terminal monitor system>

```
Center-vpn# ter monitor system
Center-vpn# 071750: Feb 27 18:56:27 quicksecpm: <6> IKE SA destroyed from '10.10.20.54', remote identity 'C=kr, CN=branch-1'
071752: Feb 27 18:56:43 quicksecpm: <6> IKEv2 SA [Responder rekey] negotiation completed
071763: Feb 27 18:56:43 quicksecpm: <6> IKE SA negotiation done from '10.10.20.54', remote identity 'C=kr, CN=branch-1'
071764: Feb 27 18:56:43 quicksecpm: <6> IKE SA negotiations: 3898 done, 3898 successful, 0 failed
071765: Feb 27 18:56:57 IPSECD: <3> 861::timeout limit exceeded, terminate session. (tid:0)(in:0)(seld:1697231440)375:403, cur_time = Fri Feb 27 18:56:57 2015
, pSession->m_Timeout = Fri Feb 27 18:56:50 2015
071766: Feb 27 18:56:57 IPSECD: <6> 861::closing tunnel for 861-3
071767: Feb 27 18:56:58 IPSECD: <6> 861::ipsecd-line for 861-3 terminated.
071768: Feb 27 18:56:58 IPSECD: <6> disconnect_count : 0
071769: Feb 27 18:56:59 quicksecpm: <6> Policy rules reloaded
071770: Feb 27 18:56:59 ntpd: <6> Deleting interface #29 vpn8613, 172.61.3.1#123, interface stats: received=0, sent=0, dropped=0, active_time=101 secs
071771: Feb 27 18:56:59 ntpd: <6> peers refreshed
```

< 실시간 세션 로그 : terminal monitor session >

```
Center-vpn# terminal monitor session
Center-vpn#
Index  Time          Proto     Policy Rule  Type  Src           Dst           Spt-c  Dpt-t  Bytes     Packets    R_Src         R_Dst         R_Spt-c R_Dpt-t R_Bytes    R_Packets  Count  Duration-time
050190 02-27 18:58:07 icmp      pass   65000 open      10.254.254.15   10.10.20.53     0      8      0         0          10.10.20.53     10.254.254.15   0       0       0          0          1      -
050191 02-27 18:58:08 icmp      pass   65000 close     10.254.254.15   10.10.20.53     0      8      60        1          10.10.20.53     10.254.254.15   0       0       60         1          1      0000:00:01
```

9-5 세션 상태 모니터링

Show ip session 명령어 : 세션 확인

vforce# show ip session | match 192.168.1. ----------→ *Match filtering을 이용하여 192.168.1.과 일치하는 세션 출력*

tcp ESTABLISHED 3587 192.168.1.161:2147(40.40.40.1:2147) - 207.46.110.94:80 rule=403 nat=403 tx=486/101948 rx=260/95109 ASSURED
tcp ESTABLISHED 3537 192.168.1.54:62187(40.40.40.1:62187) - 211.45.26.66:33 rule=410 nat=403 tx=984/43033 rx=553/31341 ASSURED
tcp ESTABLISHED 3503 192.168.1.54:62186(40.40.40.1:62186) - 211.45.26.66:33 rule=410 nat=403 tx=1248/55137 rx=820/50810 ASSURED
udp 19 192.168.1.225:32768(40.40.40.1:32768) - 192.168.1.52:514 rule=130nat=403 tx=9546/1937838 rx=0/0 NOREPLY
tcp ESTABLISHED 3596 192.168.1.107:1075(40.40.40.1:1075) - 210.126.140.34:80 rule=399 nat=403 tx=11326/2059791 rx=11191/2183426 ASSURED
tcp CLOSE 3 192.168.1.106:64013 - 208.80.152.2:80 rule=403 tx=10/602 rx=9/1214 ASSURED
tcp SYN_SENT 8 192.168.1.106:64057 - 72.51.37.237:8899 rule=410 tx=3/152 rx=0/0 NOREPLY
tcp ESTABLISHED 3310 192.168.1.106:61932 - 192.168.1.17:445 rule=130 tx=150/11483 rx=227/234323 ASSURED
tcp SYN_SENT 7 192.168.1.106:64058 - 66.199.250.170:8911 rule=410 tx=3/152 rx=0/0 NOREPLY
tcp LAST_ACK 8 192.168.106:64112 - 211.233.79.69:80 rule=403 tx=6/1161 rx=5/1116 ASSURED

1. (40.40.40.1:2147) : Source NAT 된 IP 와 Port 정보

2. udp 19 : 해당 세션 테이블 보관 시간

3. TCP 상태 : SYN_SENT(Syn 패킷 전송후), ESTABLISHED(데이터 통신 상태), LAST_ACK(FIN 패킷 전송후), CLOSE(최종 FIN ACK 응답후)

4. ASSURED : 세션이 정상적으로 연결된 상태

9-6 로그(Log) 분석(1)

네트워크 : Link-timeout 실패할 경우

< 센터 >

```
center# sh run interface eth2
!
interface eth2
 ip address 2.2.2.1/24 link-timeout 5 3 icmp 2.2.2.2
```

G/W(2.2.2.2)를 5초 주기로 3회 icmp 체크함
; 3회 모두 check 실패 시 해당 인터페이스(eth2)를 강제 Down 시킴

< 지점 >

```
branch# sh run int eth2
!
interface eth2
 ip address 3.3.3.1/24 link-timeout 5 3 icmp 3.3.3.3
```

G/W(2.2.2.2)를 5초 주기로 3회 icmp 체크함
; 3회 모두 check 실패 시 해당 인터페이스(eth2)를 강제 Down 시킴

에러 로그

< 센터 >

```
000611: Nov  3 08:15:00 NSM: <6> Interface eth2 ICMP check failed (0/1/3) (suc/err/try)
000612: Nov  3 08:15:06 NSM: <6> Interface eth2 ICMP check failed (0/2/3) (suc/err/try)
000613: Nov  3 08:15:12 NSM: <6> Interface eth2 ICMP check failed (0/3/3) (suc/err/try)
000614: Nov  3 08:15:12 NSM: <6> Interface eth2 link status going DOWN. now update RIB.
```

회선 G/W Health Check 시 icmp 3회 모두 fail
; 회선 점검 필요

< 지점 >

```
000479: Nov  3 08:04:05 NSM: <6> Interface eth2 ICMP check failed (0/1/3) (suc/err/try)
000481: Nov  3 08:04:10 NSM: <6> Interface eth2 ICMP check failed (0/2/3) (suc/err/try)
000482: Nov  3 08:04:16 NSM: <6> Interface eth2 ICMP check failed (0/3/3) (suc/err/try)
000483: Nov  3 08:04:16 NSM: <6> Interface eth2 link status going DOWN. now update RIB.
```

회선 G/W Health Check 시 icmp 3회 모두 fail
; 회선 점검 필요

9-6 로그(Log) 분석(2)

네트워크 : VPN 회선 점검

< 센터 >

```
center# show dhcp eth1

DHCP Interface eth1
 Interface IP : 10.10.20.159 netmask 255.255.255.0
 Lease Time   : 86400 seconds (76296 seconds are left)
 Gateway IP   : 10.10.20.1
 Server ID   : 10.10.20.2
 DNS #0       : 154.10.6.11
 DNS #1       : 164.124.101.2
!
vforce# ping 168.126.63.1 repeat 1000
```

KT DNS로 Ping 1000개 전송 테스트

< 지점 >

```
branch# show dhcp eth1

DHCP Interface eth1
 Interface IP : 10.10.20.160 netmask 255.255.255.0
 Lease Time   : 86400 seconds (76296 seconds are left)
 Gateway IP   : 10.10.20.1
 Server ID   : 10.10.20.2
 DNS #0       : 154.10.6.11
 DNS #1       : 164.124.101.2
!
vforce# ping 168.126.63.1 repeat 1000
```

KT DNS로 Ping 1000개 전송 테스트

에러 로그

< 센터 / 지점 >

```
Vforce# ping 168.126.63.1 repeat 1000

Type escape sequence to abort.
Sending 1000, 36-byte ICMP Echos to 168.126.63.1, timeout is 0.950 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 2/3/8 ms
```

< Ping 명령어 옵션 >

168.126.63.1 : 목적지 IP
Source : interface 또는 IP
Repeat : Ping 개수
Size : Packet Size

Ping Loss 확인 (Ping Loss 발생 시 Counter가 올라감)
; ping loss 다량 발생 시 회선 점검 필요

Round-trip Time(RTT)값을 통하여 간단한 회선 속도 확인

9-6 로그(Log) 분석(3)

네트워크 : 방화벽에 차단될 경우

< 센터 >

```
center# sh run ip rule 1
!
ip rule 1
 source any
 destination any
 policy drop
 log connections
 enable
!
```

방화벽 룰을 Default Drop로 설정

< 지점 >

```
branch# ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 36-byte ICMP Echos to 1.1.1.1, timeout is 0.950 seconds:
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms
```

센터로 Ping TEST

에러 로그

< 센터 >

Center# show logging session(저장로그 확인) 및 terminal monitor session(실시간 확인)

```
000015 11-03 08:26:17 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000016 11-03 08:26:18 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000017 11-03 08:26:19 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000018 11-03 08:26:20 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000019 11-03 08:26:21 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000020 11-03 08:26:25 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000021 11-03 08:26:26 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000022 11-03 08:26:27 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000023 11-03 08:26:28 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
000024 11-03 08:26:29 icmp drop 1 n/a 1.1.1.2 1.1.1.1 0 8 0 0 0.0.0.0
```

해당 ICMP 방화벽 룰에 의해 Drop 됨
; 적법한 사용자의 IP라면, 방화벽을 통해 해당 IP 와 서비스를 허용해야 함

9-6 로그(Log) 분석(4)

IPSec VPN : remote-id(fqdn)이 서로 일치하지 않을 경우

< 센터 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id branch enable
!
crypto tunnel center
 priority 255
 local-identity fqdn center
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
!
```

< 지점 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center-1 enable
!
crypto tunnel branch
 priority 255
 local-identity fqdn branch
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination host 1.1.1.1
 protocol etherip
 enable
!
```

에러 로그

< 센터 >

000466: Nov 3 07:10:00 iked: <6> 08[IKE] no IKE config found for 1.1.1.1...1.1.1.2, sending NO_PROPOSAL_CHOSEN ------> ***NO_PROPOSAL_CHOSEN***

<지점>

000453: Nov 3 07:18:53 iked: <6> 15[IKE] initiating IKE_SA b(1.1.1.2-1.1.1.1)[2] to 1.1.1.1

000454: Nov 3 07:18:53 iked: <6> 02[IKE] received NO_PROPOSAL_CHOSEN notify error ----------> ***NO_PROPOSAL_CHOSEN***

IPSec VPN Parameter 값을 서로 일치 시켜 문제 해결

**** IPSec VPN 설정 관련 Parameter 값이 일치하지 않을 경우 대부분 NO_PROPOSAL_CHOSEN 와 같은 동일 Log 출력***

9-6 로그(Log) 분석(5)

IPSec VPN : PSK이 서로 일치하지 않을 경우

< 센터 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id branch enable
!
crypto tunnel center
 priority 255
 local-identity fqdn center
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
!
```

< 지점 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center enable
!
crypto tunnel branch
 priority 255
 local-identity fqdn branch
 auth-key admin
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination host 1.1.1.1
 protocol etherip
 enable
!
```

에러 로그

< 센터 >

000466: Nov 3 07:10:00 iked: <6> 08[IKE] no IKE config found for 1.1.1.1...1.1.1.2, sending NO_PROPOSAL_CHOSEN ------> ***NO_PROPOSAL_CHOSEN***

<지점>

000453: Nov 3 07:18:53 iked: <6> 15[IKE] initiating IKE_SA b(1.1.1.2-1.1.1.1)[2] to 1.1.1.1

000454: Nov 3 07:18:53 iked: <6> 02[IKE] received NO_PROPOSAL_CHOSEN notify error ----------> ***NO_PROPOSAL_CHOSEN***

IPSec VPN Parameter 값을 서로 일치 시켜 문제 해결

**** IPSec VPN 설정 관련 Parameter 값이 일치하지 않을 경우 대부분 NO_PROPOSAL_CHOSEN 와 같은 동일 Log 출력***

9-6 로그(Log) 분석(6)

IPSec VPN : 암호화 알고리즘이 서로 일치하지 않을 경우

< 센터 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id branch enable
!
crypto tunnel center
 priority 255
 local-identity fqdn center
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
!
```

< 지점 >

```
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center enable
!
crypto tunnel branch
 priority 255
 local-identity fqdn branch
 auth-key admin
 transforms esp aes-256 sha-512
 ipsec-mode transport
 source interface eth1
 destination host 1.1.1.1
 protocol etherip
 enable
!
```

에러 로그

< 센터 >

```
000359: Nov  3 07:55:14 iked: <6> 15[IKE] 1.1.1.2 is initiating an IKE_SA
000360: Nov  3 07:55:14 iked: <6> 16[IKE] IKE_SA c(1.1.1.1-0.0.0.0/0)[5] established between 1.1.1.1[center]...1.1.1.2[branch]
000361: Nov  3 07:55:14 iked: <6> 16[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ
000362: Nov  3 07:55:14 iked: <6> 16[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
000363: Nov  3 07:55:14 iked: <6> 16[CHD] no acceptable proposal found
```

센터와 지점 간 무결성 알고리즘이 다름

<지점>

```
000453: Nov  3 08:04:08 iked: <6> 15[IKE] initiating IKE_SA b(1.1.1.2-1.1.1.1)[3] to 1.1.1.1
000454: Nov  3 08:04:08 iked: <6> 02[CHD] establishing CHILD_SA b(1.1.1.2-1.1.1.1){1}
000455: Nov  3 08:04:08 iked: <6> 01[IKE] IKE_SA b(1.1.1.2-1.1.1.1)[3] established between 1.1.1.2[branch]...1.1.1.1[center]
000456: Nov  3 08:04:08 iked: <6> 01[CHD] received NO_PROPOSAL_CHOSEN notify, no CHILD_SA built
```

NO_PROPOSAL_CHOSEN

IPSec VPN Parameter 값을 서로 일치 시켜 문제 해결

9-6 로그(Log) 분석(4)

IPSec VPN : eix ip가 같은 대역이 아닐 경우

< 센터 >

```
interface eix0
 eix source eth1
 eix with-ipsec
 ip address 172.16.0.1/16
!
```

< 지점 >

```
interface eix0
 eix destination 1.1.1.1
 eix source eth1
 eix with-ipsec
 ip address 172.17.0.2/16
!
```

에러 로그

< 센터 >

```
Center# sh eix tu
Total 1 tunnel.

Identity          Peer IP       Status      Uptime
6669.7823.5868    0.0.0.0       up(1/1)     00:01:10
```

EIX IP를 동일 대역으로 일치 시켜 문제 해결

< 지점 >

```
Branch# sh eix tu
Total 1 tunnel.

Identity          Peer IP       Status      Uptime
6669.7823.94fa    0.0.0.0       up(1/1)     00:01:17
```

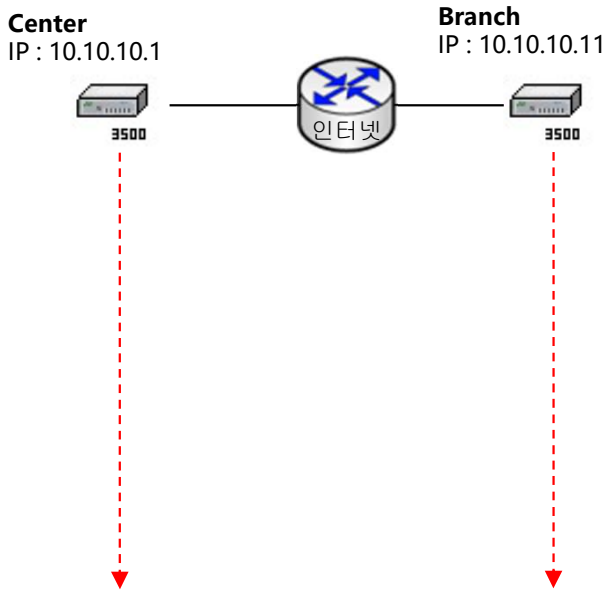
센터 / ATM지점 모두 EIX Tunnel IP가 정상적으로 올라오지 않음

9-6 로그(Log) 분석(4)

Quicksec 동작 시 (Mode Type 1)

센터 설정 정보

```
security parameters
 dpd-timeout 10!
 remote-secret test id-type fqdn id branch_1 enable

interface eix0
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.1/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn center
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
security parameters
 dpd-timeout 10
 remote-secret test id-type fqdn id center enable

interface eix0
 eix destination 10.10.10.1
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.11/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn branch_1
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination host 10.10.10.1
 protocol etherip
 enable
```

설정이 없거나,
PSK/Fqdn ID 값이 다를 경우

센터 로그

```
001968: Jul  5 14:20:04 quicksecpm: <6> IPsec SA [Initiator] negotiation failed:
001970: Jul  5 14:20:04 quicksecpm: <6>   Local IKE peer  10.10.10.1:500 ID center (fqdn)
001971: Jul  5 14:20:04 quicksecpm: <6>   Remote IKE peer 10.10.10.11:500 ID branch_1 (fqdn)
001973: Jul  5 14:20:04 quicksecpm: <6>   Message: Timed out (65540)
001974: Jul  5 14:20:04 quicksecpm: <6> IPsec SA negotiations: 60 done, 31 successful, 29 failed
001975: Jul  5 14:20:04 quicksecpm: <7> SAD: deleting IPsec SAs by peer handle 0000001e
001977: Jul  5 14:20:04 quicksecpm: <6> IPsec SA destroyed: Inbound SPI:      | Outbound SPI:
001978: Jul  5 14:20:04 quicksecpm: <6>                    ESP    [55819b41] | [4bc01eb2]
001979: Jul  5 14:20:04 quicksecpm: <7> SAD: 00000001 destroyed
001980: Jul  5 14:20:04 quicksecpm: <7> SAD: deleting IPsec SAs by peer handle 0000001e
001981: Jul  5 14:20:04 quicksecpm: <7>
001982: Jul  5 14:20:04 quicksecpm: <7> IKE SA destroyed:
001983: Jul  5 14:20:04 quicksecpm: <7>   Initiator SPI 30073f7e eb0fcb98 Responder SPI
6572a484 9cc41809
001984: Jul  5 14:20:04 quicksecpm: <6> IKE SA destroyed from '10.10.10.11', remote identity
'branch_1'
```

지점 로그

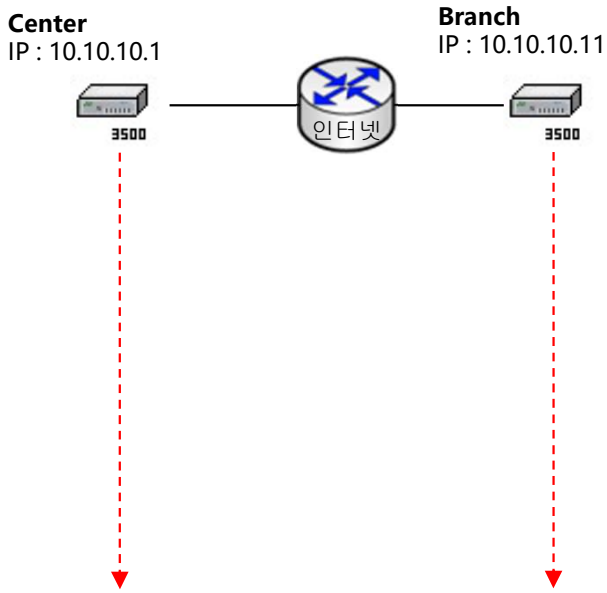
```
008673: Jul  5 14:05:52 quicksecpm: <6> IKEv2 SA [Initiator] negotiation failed:
008674: Jul  5 14:05:52 quicksecpm: <6>
008675: Jul  5 14:05:52 quicksecpm: <6>   Local IKE peer  10.10.10.11:500 ID branch_1 (fqdn)
008676: Jul  5 14:05:52 quicksecpm: <6>   Remote IKE peer 10.10.10.1:500 ID center (fqdn)
008677: Jul  5 14:05:52 quicksecpm: <6>
008678: Jul  5 14:05:52 quicksecpm: <6> IKE SA negotiation failed to '10.10.10.1', remote identity
'center'
008679: Jul  5 14:05:52 quicksecpm: <6>   Message: Authentication failed (24)
008680: Jul  5 14:05:52 quicksecpm: <6>   Reason:
008681: Jul  5 14:05:52 quicksecpm: <6>     Remote ID mismatch
008682: Jul  5 14:05:52 quicksecpm: <6> IKE SA negotiations: 475 done, 3 successful, 472 failed
```

9-6 로그(Log) 분석(4)

Quicksec 동작 시 (Mode Type 1)

센터 설정 정보

```
security parameters
 dpd-timeout 10!
 remote-secret test id-type fqdn id branch_1 enable

interface eix0
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.1/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn center
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
security parameters
 dpd-timeout 10
remote-secret test id-type fqdn id center enable

interface eix0
 eix destination 10.10.10.1
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.11/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn branch_1
 local-secret test
 transforms esp aes-256 sha1
 ipsec-mode transport
 source interface eth1
 destination host 10.10.10.1
 protocol etherip
 enable
```

암호화 방식 상이함

센터 로그

003036: Jul 5 14:41:19 quicksecpm: <6> IPsec SA [Responder] negotiation failed:
003037: Jul 5 14:41:19 quicksecpm: <6>
003038: Jul 5 14:41:19 quicksecpm: <6> Local IKE peer 10.10.10.1:500 ID center (fqdn)
003039: Jul 5 14:41:19 quicksecpm: <6> Remote IKE peer 10.10.10.11:500 ID branch_1 (fqdn)
003041: Jul 5 14:41:19 quicksecpm: <6> Message: No proposal chosen (14)
003042: Jul 5 14:41:19 quicksecpm: <6> Reason:
003043: Jul 5 14:41:19 quicksecpm: <6> Encryption algorithm mismatch
003044: Jul 5 14:41:19 quicksecpm: <6> IKE transform attribute mismatch (possible key size mismatch).
003045: Jul 5 14:41:19 quicksecpm: <6> IPsec SA negotiations: 105 done, 47 successful, 58 failed

지점 로그

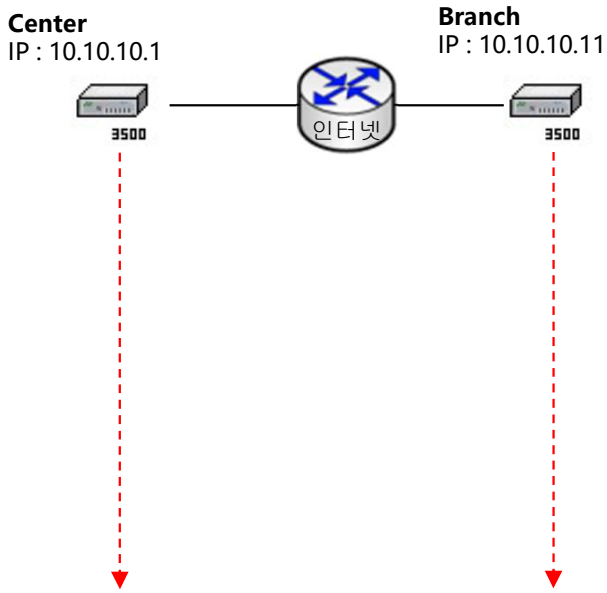
009966: Jul 5 14:41:17 quicksecpm: <4> Authenticated notification `No proposal chosen' (14) from 10.10.10.1:500 for protocol None. Initiator SPI c9686d00 8573f20d Responder SPI 60aac330 dfa62cfa
009968: Jul 5 14:41:17 quicksecpm: <6> IPsec SA [Initiator] negotiation failed:
009970: Jul 5 14:41:17 quicksecpm: <6> Local IKE peer 10.10.10.11:500 ID branch_1 (fqdn)
009971: Jul 5 14:41:17 quicksecpm: <6> Remote IKE peer 10.10.10.1:500 ID center (fqdn)
009973: Jul 5 14:41:17 quicksecpm: <6> Message: No proposal chosen (14)
009974: Jul 5 14:41:17 quicksecpm: <6> IPsec SA negotiations: 534 done, 6 successful, 528 failed

9-6 로그(Log) 분석(4)

Quicksec 동작 시 (Mode Type 1)

센터 설정 정보

```
security parameters
 dpd-timeout 10!
 remote-secret test id-type fqdn id branch_1 enable

interface eix0
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.1/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn center
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
security parameters
 dpd-timeout 10
remote-secret test id-type fqdn id center enable

interface eix0
 eix destination 10.10.10.1
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.11/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn branch_1
 local-secret test
 transforms esp aes-128 md5
 ipsec-mode transport
 source interface eth1
 destination host 10.10.10.1
 protocol etherip
 enable
```

암호화 방식 상이함

센터 로그

003090: Jul 5 14:43:39 quicksecpm: <6> IPsec SA [Responder] negotiation failed:
003092: Jul 5 14:43:39 quicksecpm: <6> Local IKE peer 10.10.10.1:500 ID center (fqdn)
003093: Jul 5 14:43:39 quicksecpm: <6> Remote IKE peer 10.10.10.11:500 ID branch_1 (fqdn)
003095: Jul 5 14:43:39 quicksecpm: <6> Message: No proposal chosen (14)
003096: Jul 5 14:43:39 quicksecpm: <6> Reason:
003097: Jul 5 14:43:39 quicksecpm: <6> Integrity algorithm mismatch
003098: Jul 5 14:43:39 quicksecpm: <6> IPsec SA negotiations: 110 done, 47 successful, 63 failed

지점 로그

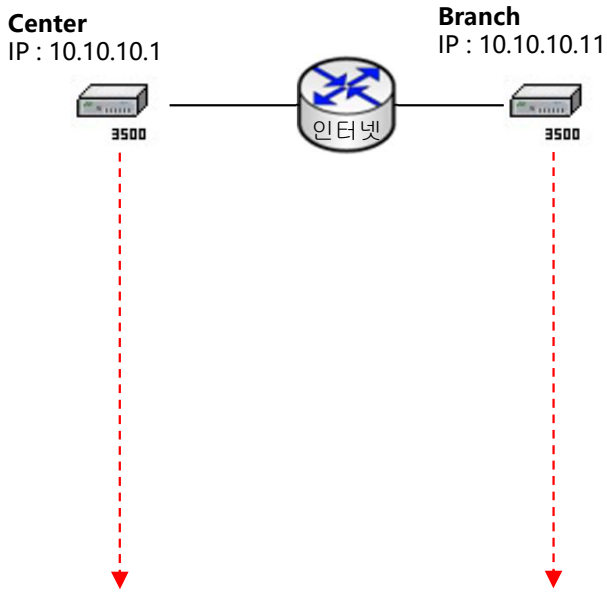
*VForce# 010013: Jul 5 14:43:37 quicksecpm: <4> Authenticated notification `No proposal chosen' (14) from 10.10.10.1:500 for protocol None. Initiator SPI c9686d00 8573f20d Responder SPI 60aac330 dfa62cfa
010015: Jul 5 14:43:37 quicksecpm: <6> IPsec SA [Initiator] negotiation failed:
010017: Jul 5 14:43:37 quicksecpm: <6> Local IKE peer 10.10.10.11:500 ID branch_1 (fqdn)
010018: Jul 5 14:43:37 quicksecpm: <6> Remote IKE peer 10.10.10.1:500 ID center (fqdn)
010020: Jul 5 14:43:37 quicksecpm: <6> Message: No proposal chosen (14)
010021: Jul 5 14:43:37 quicksecpm: <6> IPsec SA negotiations: 539 done, 6 successful, 533 failed

9-6 로그(Log) 분석(4)

Quicksec 동작 시 (Mode Type 1)

센터 설정 정보

```
security parameters
 dpd-timeout 10!
 remote-secret test id-type fqdn id branch_1 enable

interface eix0
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.1/24

crypto tunnel test
 priority 255
 ike-algorithms 3des sha1
 local-identity fqdn center
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
security parameters
 dpd-timeout 10
remote-secret test id-type fqdn id center enable

interface eix0
 eix destination 10.10.10.1
 eix source eth1
 eix dpd-timeout 10
 ip address 172.17.1.11/24

crypto tunnel test
 priority 255
 ike-versions 1
 ike-algorithms 3des sha1
 local-identity fqdn branch_1
 local-secret test
 transforms esp aes-128 sha1
 ipsec-mode transport
 source interface eth1
 destination host 10.10.10.1
 protocol etherip
 enable
```

IKE 버전이 다를 경우

센터 로그센터 로그

```
002896: Jul  5 14:38:23 quicksecpm: <6>
002897: Jul  5 14:38:23 quicksecpm: <6> IKEv1 SA [Responder] negotiation failed:
002898: Jul  5 14:38:23 quicksecpm: <6>
002899: Jul  5 14:38:23 quicksecpm: <6>   Local IKE peer  10.10.10.1:500 ID (null)
002900: Jul  5 14:38:23 quicksecpm: <6>   Remote IKE peer 10.10.10.11:500 ID (null)
002901: Jul  5 14:38:23 quicksecpm: <6>
002902: Jul  5 14:38:23 quicksecpm: <6> IKE SA negotiation failed from '10.10.10.11',
remote identity '(null)'
002903: Jul  5 14:38:23 quicksecpm: <6>   Message: No proposal chosen (14)
002904: Jul  5 14:38:23 quicksecpm: <6>   Reason:
002905: Jul  5 14:38:23 quicksecpm: <6>     IKE version mismatch
002906: Jul  5 14:38:23 quicksecpm: <6> IKE SA negotiations: 76 done, 46 successful, 30
failed
002907: Jul  5 14:38:23 quicksecpm: <6>   IKEv1 Error : No proposal chosen
```

지점 로그

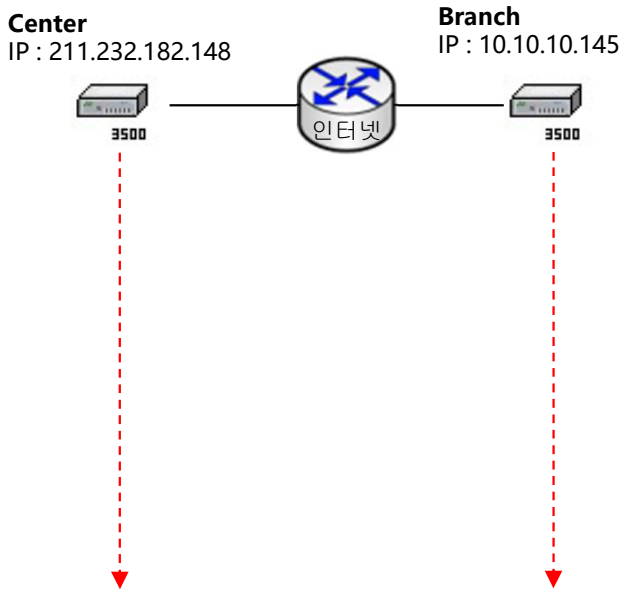
```
009838: Jul  5 14:38:21 quicksecpm: <6> IKEv1 SA [Initiator] negotiation failed:
009839: Jul  5 14:38:21 quicksecpm: <6>
009840: Jul  5 14:38:21 quicksecpm: <6>   Local IKE peer  10.10.10.11:500 ID branch_1 (fqdn)
009841: Jul  5 14:38:21 quicksecpm: <6>   Remote IKE peer 10.10.10.1:500 ID (null)
009842: Jul  5 14:38:21 quicksecpm: <6>
009843: Jul  5 14:38:21 quicksecpm: <6> IKE SA negotiation failed to '10.10.10.1', remote identity
'(null)'
009844: Jul  5 14:38:21 quicksecpm: <6>   Message: No proposal chosen (14)
009845: Jul  5 14:38:21 quicksecpm: <6> IKE SA negotiations: 530 done, 5 successful, 525 failed
009846: Jul  5 14:38:21 quicksecpm: <6>   IKEv1 Error : No proposal chosen
009847: Jul  5 14:38:21 quicksecpm: <7>
009848: Jul  5 14:38:21 quicksecpm: <7> IKE SA destroyed:
009849: Jul  5 14:38:21 quicksecpm: <7>   Initiator SPI df103ab0 0b9bfe51 Responder SPI 00000000
00000000
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
 remote-secret test id-type fqdn id test enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

Fqdn 이 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216181: Dec 14 23:19:28 iked: <6> 14[IKE] 10.10.10.145 is initiating an IKE_SA
216182: Dec 14 23:19:28 iked: <6> 15[IKE] no shared key found for '%any' - 'nexg'
216183: Dec 14 23:19:28 iked: <6> 15[IKE] failed to process auth for other
(211.232.182.148...10.10.10.145)
```

지점 로그

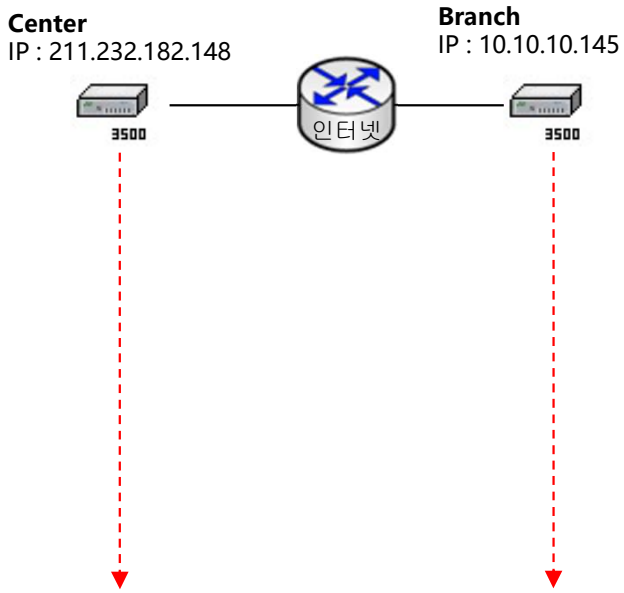
```
*Test-Branch# 001649: Dec 14 23:20:02 iked: <6> 11[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[36] to 211.232.182.148
001650: Dec 14 23:20:02 iked: <6> 10[CHD] establishing CHILD_SA Test(10.10.10.145-
211.232.182.148){3}
001651: Dec 14 23:20:02 iked: <6> 14[IKE] received AUTHENTICATION_FAILED notify error
(10.10.10.145...211.232.182.148
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
 remote-secret test id-type fqdn id @nexg-1 enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

Fqdn 이 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216220: Dec 14 23:25:36 iked: <6> 06[IKE] 10.10.10.145 is initiating an IKE_SA
216221: Dec 14 23:25:36 iked: <6> 07[IKE] no shared key found for '%any' - 'nexg'
216222: Dec 14 23:25:36 iked: <6> 07[IKE] failed to process auth for other
(211.232.182.148...10.10.10.145)
```

지점 로그

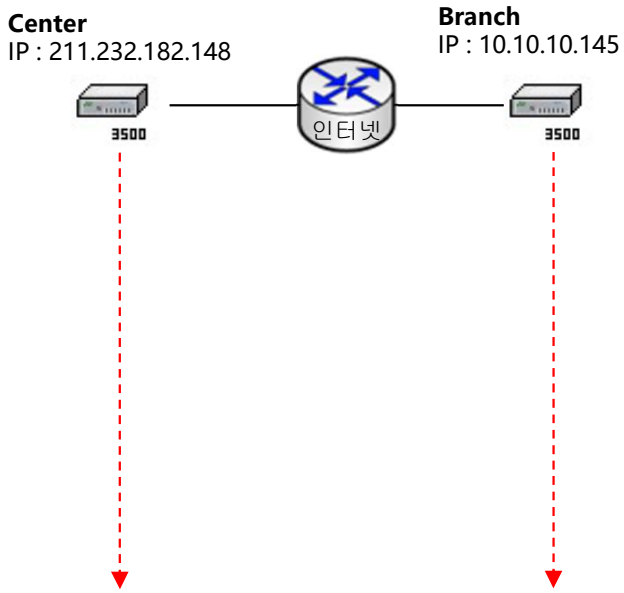
```
*Test-Branch# 001784: Dec 14 23:26:10 iked: <6> 06[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[2] to 211.232.182.148
001785: Dec 14 23:26:10 iked: <6> 09[CHD] establishing CHILD_SA Test(10.10.10.145-
211.232.182.148){1}
001786: Dec 14 23:26:10 iked: <6> 08[IKE] received AUTHENTICATION_FAILED notify error
(10.10.10.145...211.232.182.148)
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
 remote-secret testadmin id-type fqdn id @nexg enable
 !
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

PSK 가 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216243: Dec 14 23:29:20 iked: <6> 10[IKE] 10.10.10.145 is initiating an
IKE_SA
216244: Dec 14 23:29:20 iked: <6> 11[IKE] tried 1 shared key for '%any' - 'nexg', but MAC
mismatched
216245: Dec 14 23:29:20 iked: <6> 11[IKE] failed to process auth for other
(211.232.182.148...10.10.10.145)
```

지점 로그

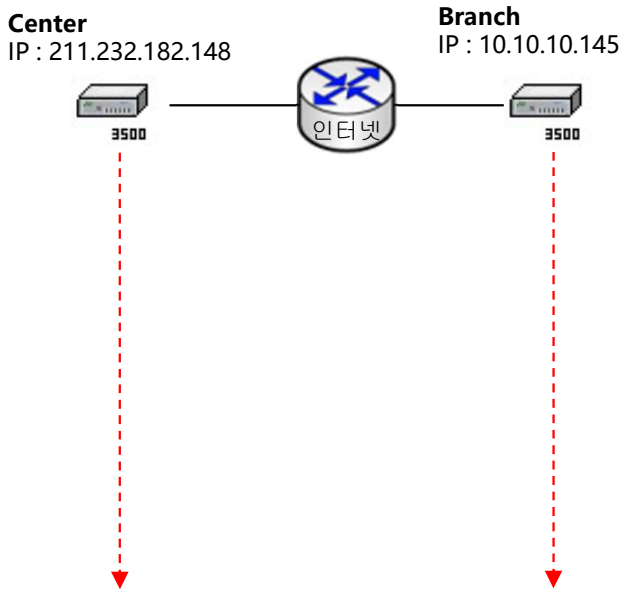
```
*Test-Branch# 001805: Dec 14 23:29:54 iked: <6> 01[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[9] to 211.232.182.148
001806: Dec 14 23:29:54 iked: <6> 06[CHD] establishing CHILD_SA Test(10.10.10.145-
211.232.182.148){1}
001807: Dec 14 23:29:54 iked: <6> 07[IKE] received AUTHENTICATION_FAILED notify error
(10.10.10.145...211.232.182.148)
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
remote-secret admin1234 id-type fqdn id @nexg
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin1234 id-type fqdn id center
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

PSK 가 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216257: Dec 14 23:31:28 iked: <6> 08[IKE] 10.10.10.145 is initiating an IKE_SA
216258: Dec 14 23:31:28 iked: <6> 07[IKE] IKE_SA Test(211.232.182.148-0.0.0.0/0)[24]
established between 211.232.182.148[center#1]...10.10.10.145[nexg]
216259: Dec 14 23:31:28 iked: <6> 07[CHD] CHILD_SA Test(211.232.182.148-0.0.0.0/0){2}
established with SPIs c30fca97_i c35ca9f4_o and TS 211.232.182.148/32[etherip] ===
10.10.10.145/32[etherip]
216260: Dec 14 23:31:28 iked: <6> 06[IKE] deleting IKE_SA Test(211.232.182.148-
0.0.0.0/0)[24] between 211.232.182.148[center#1]...10.10.10.145[nexg]
216261: Dec 14 23:31:28 iked: <6> 06[IKE] IKE_SA deleted
```

지점 로그

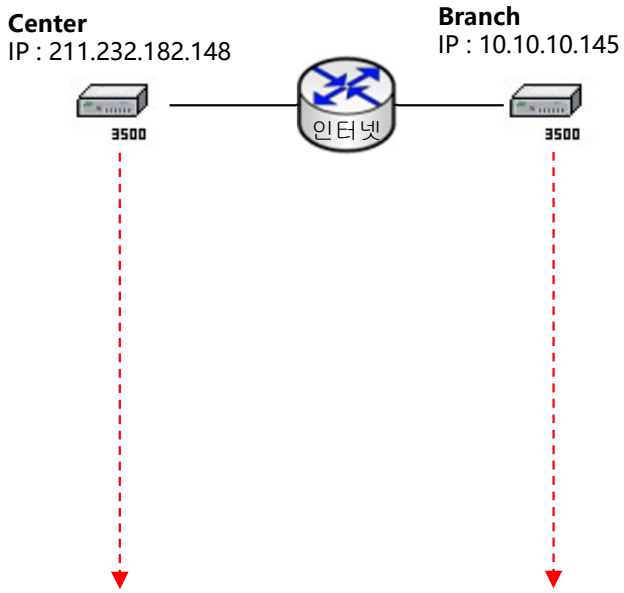
```
*Test-Branch# 001839: Dec 14 23:32:02 iked: <6> 15[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[13] to 211.232.182.148
001840: Dec 14 23:32:02 iked: <6> 05[CHD] establishing CHILD_SA Test(10.10.10.145-
211.232.182.148){1}
001841: Dec 14 23:32:02 iked: <6> 01[IKE] no shared key found for 'nexg' - 'center#1'
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
remote-secret admin1234 id-type fqdn id @nexg
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin!@#$
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
  remote-secret admin12345 id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

PSK 가 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216300: Dec 14 23:36:24 iked: <6> 14[IKE] 10.10.10.145 is initiating an
IKE_SA
216301: Dec 14 23:36:24 iked: <6> 15[IKE] IKE_SA Test(211.232.182.148-0.0.0.0/0)[32]
established between 211.232.182.148[center#1]...10.10.10.145[nexg]
216302: Dec 14 23:36:24 iked: <6> 15[CHD] CHILD_SA Test(211.232.182.148-0.0.0.0/0){9}
established with SPIs c914b1b6_i c1c0ef46_o and TS 211.232.182.148/32[etherip] ===
10.10.10.145/32[etherip]
216303: Dec 14 23:36:24 iked: <6> 05[IKE] deleting IKE_SA Test(211.232.182.148-
0.0.0.0/0)[32] between 211.232.182.148[center#1]...10.10.10.145[nexg]
216304: Dec 14 23:36:24 iked: <6> 05[IKE] IKE_SA deleted
```

지점 로그

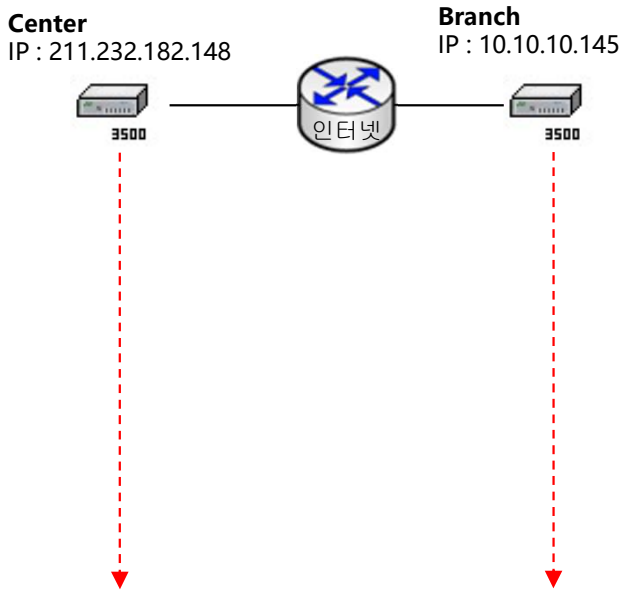
```
*Test-Branch# 002008: Dec 14 23:36:58 iked: <6> 07[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[2] to 211.232.182.148
002009: Dec 14 23:36:58 iked: <6> 12[CHD] establishing CHILD_SA Test(10.10.10.145-
211.232.182.148){1}
002010: Dec 14 23:36:58 iked: <6> 10[IKE] tried 2 shared keys for 'nexg' - 'center#1', but MAC
mismatched
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
remote-secret admin1234 id-type fqdn id @nexg
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin!@#$
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin!@#$ id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 ike-algorithms aes-256 sha-256
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

IKE 알고리즘이 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216349: Dec 14 23:41:18 iked: <6> 05[IKE] 10.10.10.145 is initiating an IKE_SA
216350: Dec 14 23:41:18 iked: <6> 05[CFG] received proposals:
IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
216351: Dec 14 23:41:18 iked: <6> 05[CFG] configured proposals:
IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
216352: Dec 14 23:41:18 iked: <6> 05[IKE] received proposals inacceptable
(10.10.10.145...211.232.182.148)
```

지점 로그

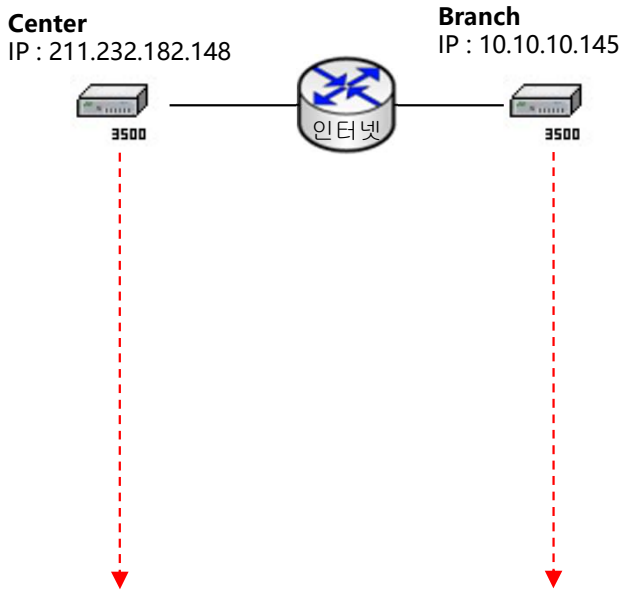
```
*Test-Branch# 002224: Dec 14 23:41:51 iked: <6> 01[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[2] to 211.232.182.148
002225: Dec 14 23:41:52 iked: <6> 05[IKE] received NO_PROPOSAL_CHOSEN notify error
(10.10.10.145...211.232.182.148)
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
remote-secret admin1234 id-type fqdn id @nexg
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin!@#$
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.20.11/24
!
security parameters
 mode type 2
 remote-secret admin!@#$ id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp 3des sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

IPSec 알고리즘이 다를 경우

센터 로그센터 로그

```
*NexG-F/W# 216375: Dec 14 23:43:44 iked: <6> 10[IKE] 10.10.10.145 is initiating an IKE_SA
216376: Dec 14 23:43:44 iked: <6> 10[CFG] received proposals:
IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
216377: Dec 14 23:43:44 iked: <6> 10[CFG] configured proposals:
IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
216378: Dec 14 23:43:44 iked: <6> 10[IKE] received proposals inacceptable
(10.10.10.145...211.232.182.148)
```

지점 로그

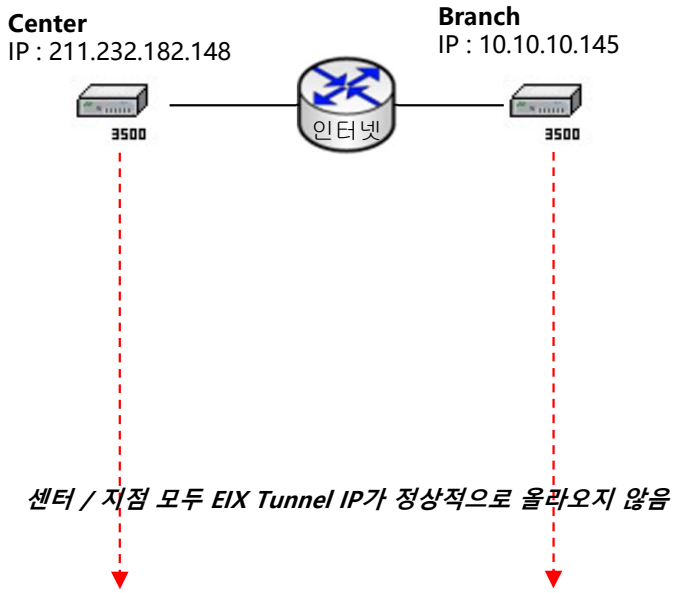
```
002387: Dec 14 23:43:59 ntpd: <6> Listening on routing socket on fd #28 for interface updates
002388: Dec 14 23:44:17 iked: <6> 11[IKE] initiating IKE_SA Test(10.10.10.145-
211.232.182.148)[2] to 211.232.182.148
002389: Dec 14 23:44:18 iked: <6> 13[IKE] received NO_PROPOSAL_CHOSEN notify error
(10.10.10.145...211.232.182.148)
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
interface eix201
 eix source eth1
 eix class-id 201
 ip address 20.20.20.1/24

security parameters
 mode type 2
remote-secret admin1234 id-type fqdn id @nexg
!
crypto tunnel Test
 priority 255
 local-identity fqdn center#1
 auth-key admin!@#$
 transforms esp aes-256 sha-256
 ipsec-mode transport
 source interface eth1
 destination any
 protocol etherip
 enable
```



지점 설정 정보

```
interface eix201
 eix destination 211.232.182.148
 eix source eth2
 eix class-id 201
 ip address 20.20.30.11/24
!
security parameters
 mode type 2
 remote-secret admin!@#$ id-type fqdn id center#1
enable
!
crypto tunnel Test
 priority 255
 local-identity fqdn @nexg
 auth-key admin1234
 transforms esp 3des sha-256
 ipsec-mode transport
 source interface eth2
 destination host 211.232.182.148
 protocol etherip
 enable
```

EIX IP 주소대역이 다를 경우

센터 로그센터 로그

```
NexG-F/Wr# sh eix tu all
Total 1 tunnel.

Identity          Peer IP      Status      Uptime
6669.7823.5868    0.0.0.0      up(1/1)     00:01:10
```

지점 로그

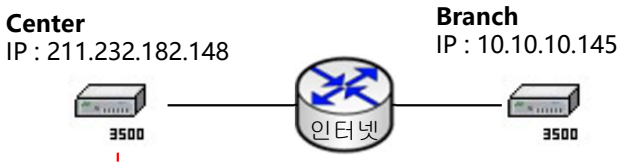
```
Test-Branch# sh eix tu
Total 1 tunnel.

Identity          Peer IP      Status      Uptime
6669.7823.94fa    0.0.0.0      up(1/1)     00:01:17
```

9-6 로그(Log) 분석(4)

StrongSwan 동작 시 (Mode Type 2)

센터 설정 정보

```
center# sh run ip rule 1

ip rule 1
 source any
 destination any
 policy drop
 log connections
 enable
```



지점 테스트

```
branch# ping 211.232.182.148

Type escape sequence to abort.
Sending 5, 36-byte ICMP Echos to
211.232.182.148, timeout is 0.950 seconds:
.....
Success rate is 0 percent (0/5), round-trip
min/avg/max = 0/0/0 ms
```

Ping Loss

센터 로그센터 로그

Center# show logging session(저장로그 확인) 및 terminal monitor session(실시간 확인)

```
000015 11-03 08:26:17 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000016 11-03 08:26:18 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000017 11-03 08:26:19 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000018 11-03 08:26:20 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000019 11-03 08:26:21 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000020 11-03 08:26:25 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000021 11-03 08:26:26 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000022 11-03 08:26:27 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000023 11-03 08:26:28 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
000024 11-03 08:26:29 icmp  drop  1  n/a  10.10.10.145  211.232.182.148  0  8  0  0  0.0.0.0
```

해당 ICMP 방화벽 룰에 의해 Drop 됨
적법한 사용자의 IP라면, 방화벽을 통해 해당 IP 와 서비스를 허용해야 함