

FNS

(Fundamental Network Security)

Ch13. VPN

/

hjlee@dongseo.ac.kr
<http://kowon.dongseo.ac.kr/~hjlee>
<http://crypto.dongseo.ac.kr>

2005-12-06
<http://kowon.dongseo.ac.kr/~hjlee>
1

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

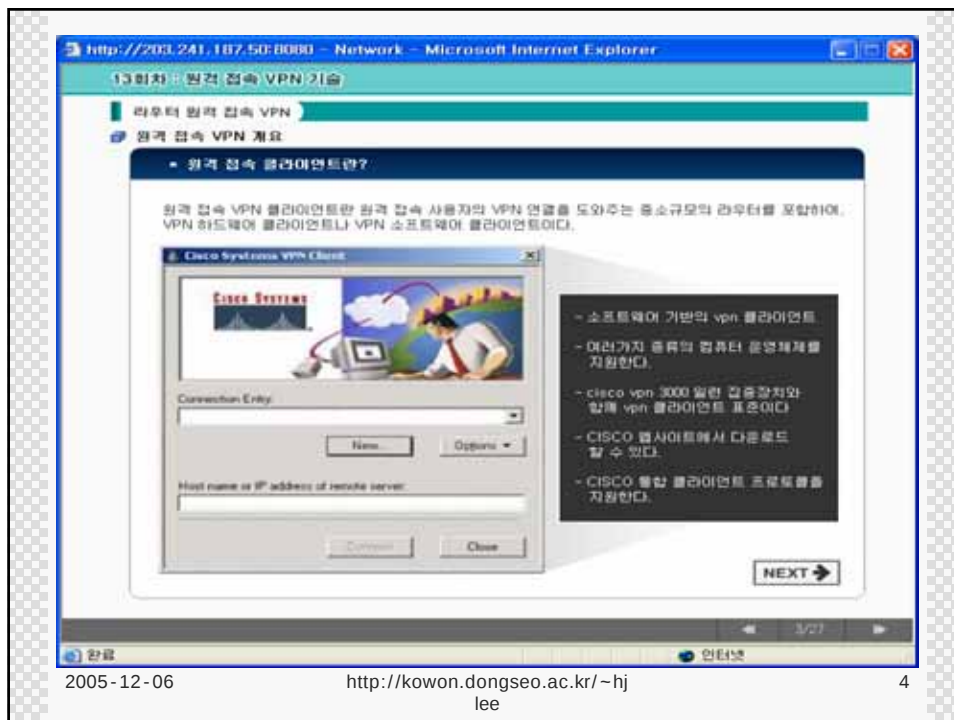
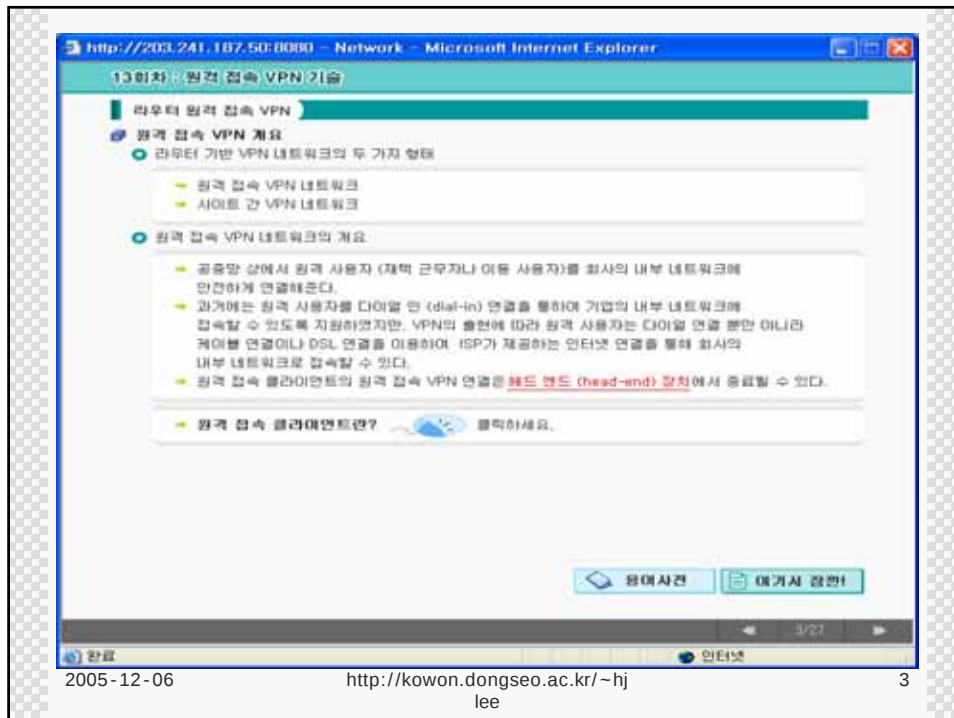
13회차 - 원격 접속 VPN 기술

이번 강의의 학습목표를 살펴본도록 하겠습니다.

학 습 목 표

- 원격 접속 VPN 기술의 개념에 대하여 설명할 수 있다.
- 원격 접속 VPN의 두 가지 유형에 대하여 설명할 수 있다.
- VPN 서비스를 위한 터널링 기술과 터널링 프로토콜에 대하여 설명할 수 있다.
- 시스코 Easy VPN 서버와 클라이언트 (remote)를 설명할 수 있다.
- 원격 접속 VPN의 연결 과정을 설명할 수 있다.
- 시스코 Easy VPN 서버 설정 방법을 설명할 수 있다.

2005-12-06
<http://kowon.dongseo.ac.kr/~hjlee>
2



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 2[습]

라우터 원격 접속 VPN

원격 접속 VPN 개요

원격 접속 클라이언트란?

- 특징
 - 인스톨하기 쉽다.
 - 어플리케이션과 리모트 사이트에서 pc에 의해 사용됨 플랫폼으로부터 독립적이다.
 - 비용이 저렴하다.



Support Cisco Utility Client Protocol

← PRE Close X

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 5

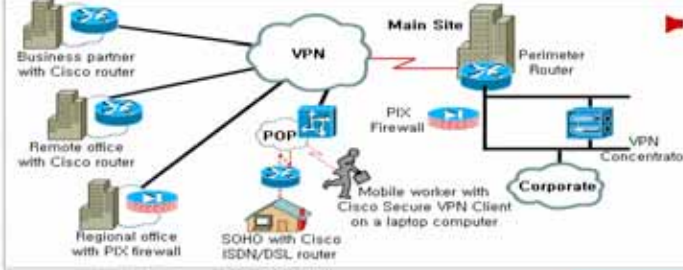
http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 2[습]

라우터 원격 접속 VPN

원격 접속 VPN의 유형

- 클라이언트 구동 (Client-Initiated) 원격 접속 VPN
 - 원격 사용자가 VPN 클라이언트나 웹 브라우저를 이용하여, 공중망을 거쳐 회사의 내부 네트워크로 보안 터널을 설정하는 원격 접속 VPN이다.
- NAS 구동 (NAS-Initiated) 원격 접속 VPN
 - 원격 사용자는 ISP의 NAS (Network Access Server)로 다이얼 인 접속을 하고, NAS에서 회사의 내부 네트워크로 보안 터널을 설정하는 원격 접속 VPN이다.



대거서 접근

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 6

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 기술

라우터 원격 접속 VPN

VPN 터널링 기술과 터널링 프로토콜

- 원격 접속 VPN을 위한 보안 터널
 - VPN 연결을 이용하여 정보를 전송하기 위해서는 보안 터널이 필요하다.
 - 네트워크에 터널링 프로토콜을 구현함으로써 원격 접속 VPN 서비스를 제공할 수 있는 다양한 기술이 개발되어 있다.

같은 터널링이란?

터널링이란 공중을 상에서 오직 사실상의 속한 사용자만을 위한 데이터 전송을 수행하는 것을 말한다. 네트워크에서는 공중을 내의 라우팅 노드가 터널링 기술을 통해 전송되는 데이터가 사실상의 데이터인지 또는 어떤 의미를 가지고 있는 데이터인지 모르게 데이터를 전송한다.

터널링 프로토콜 표준

- IPSec (IP Security): IETF RFC 2401
- SSL (Secure Sockets Layer): IETF RFC 2246
- TLS (Transport Layer Security): IETF RFC 2246
- L2TP (Layer 2 Tunneling Protocol): IETF RFC 2661
- PPTP (Point-to-Point Tunneling Protocol): Microsoft
- MPPE (Microsoft Point-to-Point Encryption): Microsoft

[여기서 보기](#)

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 7

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

시스코 Easy VPN

- Easy VPN 서버
 - 시스코 IOS 라우터와 PIX 방화벽, 그리고 VPN 3000 집중기 (concentrator) 등이 사이트 간 VPN이나 원격 접속 VPN 서비스를 제공하는 VPN 헤드 앤드 장치로 동작할 수 있게 한다.
 - 시스코 IOS 릴리즈 (Release) 12.2(8)T Easy VPN 서버는 시스코 VPN 클라이언트 릴리즈 3.x 소프트웨어 클라이언트와 하드웨어 클라이언트를 지원한다.
- Easy VPN 리모트
 - 시스코 IOS 라우터와 PIX 방화벽, VPN 3000 하드웨어나 소프트웨어 클라이언트가 원격 VPN 클라이언트로 동작할 수 있게 한다.

[여기서 보기](#)

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 8

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13페이지: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

- Easy VPN 연결 과정
 - Easy VPN 연결 설정 과정

제 1 단계: VPN 클라이언트, IKE Phase 1 시작

제 2 단계: VPN 클라이언트, IKE SA 제안

제 3 단계: Easy VPN 서버, IKE SA 제안 수락

제 4 단계: Easy VPN 서버, 사용자 인증/확인

제 5 단계: 모드 설정 과정 수행

제 6 단계: RRI (Reverse Route Injection) 과정 수행

제 7 단계: IKE quick 모드 (quick mode) 수행 및 IPSec SA 완료

대기시간 종료!

완료 인터넷

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 9

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13페이지: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

- Easy VPN 연결 과정
 - 제 1 단계: VPN 클라이언트, IKE Phase 1 시작
 - VPN 클라이언트의 인증 수행 방법에 대하여 고려할 필요가 있다.
 - 공유 키 (pre-shared key)를 사용할 경우, VPN 클라이언트는 **AM (aggressive mode)** 모드로 구동된다.
 - 디지털 인증서를 사용할 경우, VPN 클라이언트는 **MM (main mode)** 모드로 구동된다.

Easy 리모트 VPN 클라이언트 3.x가 설치된 원격지 PC

IOS 라우터 12.0(T Easy VPN 서버)

원래사건 대기시간 종료!

완료 인터넷

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 10

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 2 단계: VPN 클라이언트, IKE SA 제안

- VPN 클라이언트는 Easy VPN 서버로 여러 개의 IKE 제안 (proposal)을 전송함으로써 SA 설정을 시도한다.
- IKE 제안은 VPN 클라이언트에서의 수동 설정 작업을 줄이기 위하여 아래의 몇 가지 항목을 조합하여 이루어진다.
 - 암호화 (encryption)와 해시 알고리즘 (hash algorithms)
 - 인증 방법 (authentication method)
 - Diffie-Hellman 그룹 크기 (group size)

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 11

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 3 단계: Easy VPN 서버, IKE SA 제안 수락

- Easy VPN 서버는 자신의 목록 내용과 일치하는 제안을 검색한다.
 - 서버의 제안 목록 중 첫 번째로 일치하는 제안을 수락한다.
 - 안전성에 높은 제안일수록 Easy VPN 서버 제안 목록의 위쪽에 위치한다.
- IKE SA가 성공적으로 확립된다.
- 이로써 장치 인증 단계가 끝나고 사용자 인증 단계가 시작된다.

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 12

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 4 단계: Easy VPN 서버, 사용자 인증/확인

- Easy VPN 서버가 Xauth 로 설정되어 있을 경우, VPN 클라이언트는 username/password challenge를 기다린다.
 - 사용자는 username과 password를 입력한다.
 - 입력된 username/password 정보를 AAA를 이용하여 확인한다.
- Easy VPN 서버는 모든 사용자 인증을 수행하도록 설정되어야 한다.

Easy 리모트 VPN 클라이언트 3.x가 설치된 원격지 PC

IOS 라우터 12.0T Easy VPN 서버

username/password challenge

username/password

AAA 관리

완료

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 13

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 - 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 5 단계: 모드 설정 과정 수행

- Easy VPN 서버에서의 인증 과정이 성공적으로 이루어질 경우, VPN 클라이언트는 Easy VPN 서버에게 나머지 설정 파라미터를 요구한다.
 - 모드 설정 과정 시작
 - IP 주소, DNS, 터널링 정보 등과 같은 나머지 파라미터가 VPN 클라이언트로 다운로드 된다.
- IP 주소만이 그룹 프로파일에 필요한 파라미터이며, 다른 모든 파라미터는 건락 사항이다.

Easy 리모트 VPN 클라이언트 3.x가 설치된 원격지 PC

IOS 라우터 12.0T Easy VPN 서버

파라미터 요청

모드 설정을 통한 시스템 파라미터 다운로드

완료

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 14

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 5 단계: RRI (Reverse Route Injection) 과정 수행

- Easy VPN 클라이언트의 IP 주소를 파악한 Easy VPN 서버는 어떤 적절한 VPN 터널을 통해 패킷을 전송해야 할지를 결정해야 한다.
 - RRI는 Easy VPN 서버 상에 각각의 VPN 클라이언트 내부 IP 주소에 대한 정적 경로 (static route)를 생성한다.
 - RRI는 VPN 클라이언트를 지칭하는 crypto map에 할당되어야 해야 한다.
- RRI는 라우팅 정보를 분배하기 위해 이미 사용되고 있는 GRE 터널에 적용되는 crypto map에는 할당되어 있을 필요가 없다.

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 15

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 연결 과정

제 7 단계: IKE quick 모드 (quick mode) 수행 및 IPSec SA 완료

- VPN 클라이언트에 설정 파라미터가 성공적으로 수신된 후, IPSec SA 설정 협상을 위한 IKE quick 모드가 수행된다.
- IPSec SA 설정이 끝남으로써 VPN 연결 과정이 완료된다.

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 16

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Easy VPN 서버 설정 작업 순서

- 시스코 라우터 상에 Easy VPN 서버를 설정하기 위해 사용되는 작업 순서는 일반적으로 다음과 같다.

- 작업 1: IP address pool 설정
- 작업 2: Group policy lookup 설정
- 작업 3: 원격 접속 VPN 클라이언트를 위한 ISAKMP policy 설정
- 작업 4: 모든 설정을 위한 group policy 정의
- 작업 5: Transform set 설정
- 작업 6: RRI를 이용한 dynamic crypto map 설정
- 작업 7: Dynamic crypto map에 모든 설정 적용
- 작업 8: 라우터 외부 인터페이스에 dynamic crypto map 적용
- 작업 9: IKE DPD (dead peer detection) 활성화
- 작업 10: Xauth 설정

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 17

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

작업 1: IP address pool 설정

- 로컬 IP 주소 풀이 사용 중이라면, 원격 VPN 클라이언트에 대한 새로운 풀을 생성해야 한다.
- ip local pool 명령어를 사용한다.

```
Router(config)#ip local pool {default | pool-name low-ip-address [high-ip-address]}
```

로컬 IP 주소 풀 그룹을 설정한다.

작업 2: Group policy lookup 설정

- Group policy lookup 설정은 두 단계를 통해 이루어진다.
- 모든 `aaa new-model` 명령어를 사용하여 AAA 기능을 설정한다.
- 다음으로 group policy lookup을 활성화 한다. 이를 위한 명령어는 `aaa authorization network list-name local group radius`이다.

[대가시 보기!](#)

작업 3: 원격 접속 VPN 클라이언트를 위한 ISAKMP policy 설정

- 라우터에 연결할 모든 Easy VPN 리모트 클라이언트에 대한 ISAKMP policy를 설정한다.
- ISAKMP policy 설정 작업을 위해서는 표준 ISAKMP 설정 명령어를 사용한다.

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 18

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

작업 4: 모드 설정을 위한 group policy 정의

- 사용자는 비록 연결 (connection) 별로 오직 하나의 그룹에 속할 수 있지만, 서로 다른 정책 요구 사항을 가지고 특정 그룹에 속할 수도 있다.
- 모드 설정을 통해 VPN 클라이언트로 전달할 정책 속성 (policy attribute)을 정의하기 위해서 아래의 단계를 수행한다.
 - 그룹 프로파일 정의
 - 비드 공유 키 설정
 - DNS 서버 설정
 - WINS 서버 설정
 - DNS 도메인 설정
 - 로컬 IP 주소 풀 설정
- Group policy 정의 설정 명령어 클릭하세요.

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 19

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Group policy 정의 설정 명령어

Remote client

vpngate1

Group: vpn-remote-access
Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150

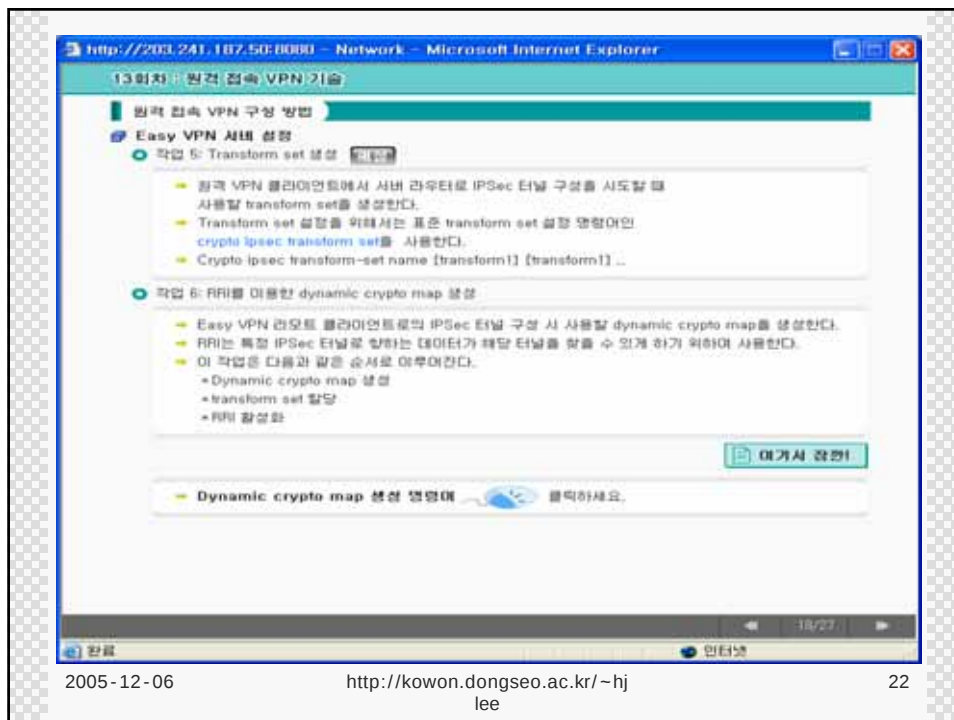
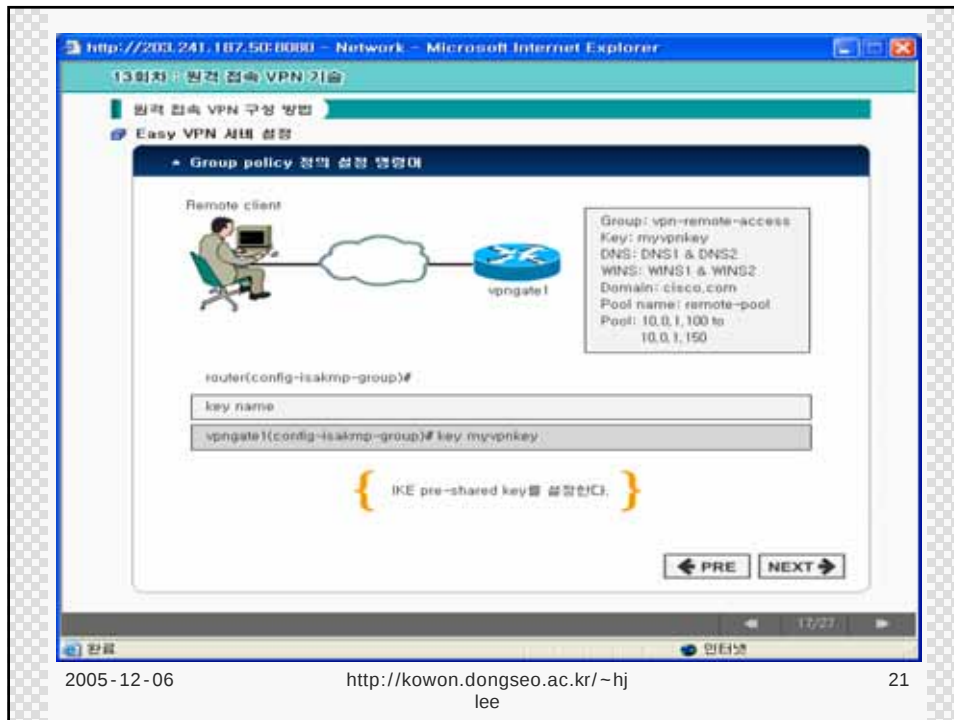
```

router(config)#
crypto isakmp client configuration group (group-name default)
vpngate1(config)# crypto isakmp client configuration group
vpn-remote-access
vpngate1(config-isakmp-group)#
  
```

{ 모드 설정을 위한 group policy 정의 }

NEXT

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 20



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Dynamic crypto map 생성 방법

Remote client



Crypto map name/sequence#
dynmap 1

```

router(config)#
crypto dynamic-map dynamic-map-name dynamic-seq-num
vpngate1(config)# crypto dynamic-map dyn-map 1
vpngate1(config-crypto-map)#

```

{ Dynamic map 설정하기 }

NEXT →

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 23

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13화차: 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Dynamic crypto map 생성 방법

Remote client



Transform set name
vpntransform

```

router(config-crypto-map)#
set transform-set transform-set-name {transform-set-name2
transform-set-name6}
vpngate1(config-crypto-map)# set transform-set vpntransform
vpngate1(config-crypto-map)#

```

{ Dynamic map에 이면에 설정한 transform-set 적용하기 }

← PRE NEXT →

완료 인터넷

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 24

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Dynamic crypto map 생성 명령어

```

router(config-crypto-map)#
reverse route
Vpngate1(config-crypto-map)#reverse-route

```

Reverse-route 명령어를 사용하여 Reverse Route Injection을 enable 한다.

PRE Close X

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 25

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

작업 7: Dynamic crypto map에 모드 설정 적용

- Dynamic crypto map에 모드 설정을 적용하는 것은 다음과 같은 단계를 통해 이루어진다.
 - 모드 설정 요구 (Mode Configuration Request)에 응답할 수 있도록 라우터를 설정한다.
 - 그를 정책에 대한 IKE querying을 활성화 한다.
 - Dynamic crypto map에 변경 사항을 적용한다.

대거서 끝!

Dynamic crypto map에 모드 설정 적용 명령어

작업 8: 라우터 외부 인터페이스에 dynamic crypto map 적용

- 새로운 dynamic crypto map을 Easy VPN 서버 라우터의 외부 인터페이스에 적용한다.
- Easy VPN 서버 라우터의 외부 인터페이스를 serial 0/0이라 할 경우의 명령어는 다음과 같다.

Dynamic crypto map을 라우터 인터페이스에 적용 명령어	<pre> Router(config)#interface serial 0/0 Router(config-if)#crypto map map-name </pre>
---------------------------------------	--

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 26

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Dynamic crypto map을 모드 설정 적용 설명서



Remote client

```

router(config)#
crypto map map-name client configuration address (initiate i, respond)
vpngate1(config)# crypto map dynmap client configuration address respond

```

- 모드 설정 요구 (Mode Configuration Request)에 응답할 수 있도록 라우터를 설정한다
- 이 작업은 라우터로 하여금 모드 설정을 시작하거나 모드 설정 요구에 응답하도록 하는 것이다. VPN 클라이언트는 응답 정보 (respond keyword)가 필요하다.
- initiate 키워드는 vpn remote client 3.x 버전 이전에 사용되어진다.

NEXT

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 27

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Dynamic crypto map을 모드 설정 적용 설명서



Remote client

```

router(config)#
crypto map map-name isakmp authorization list list-name
vpngate1(config)# crypto map dynamic isakmp authorization list
vpn-remote-access

```

{ 그룹 정책에 대한 IKE querying을 활성화 한다. }

PRE NEXT

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 28

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 시범 실행

작업 9: IKE DPD 활성화

- VPN 클라이언트 대신, 시스코 IOS VPN 게이트웨이로 하여금 IKE DPD 메시지를 전송할 수 있도록 한다.
- 연결 커넥션에 트래픽이 없을때 keepalive를 보내서 연결의 상태를 모니터링한다.
- 명령어 형식은 다음과 같다.

IKE DPD 활성화 명령어

클릭하세요.

작업 10: Xauth 설정

- Easy VPN 시범 라우터 상의 Xauth 설정은 다음과 같은 단계를 통해 이루어진다.
 - AAA login 인증을 활성화 한다.
 - Xauth 타입아웃 값을 설정한다.
 - Dynamic crypto map에 대한 IKE Xauth를 활성화 한다.

Xauth 설정 명령어

클릭하세요.

원격 vpn 클라이언트 접속하기

접속화면 보기

클릭하세요.

완료

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 29

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 시범 실행

IKE DPD 활성화 명령어

```

router(config)#
crypto isakmp keepalive secs retries
vpngate1(config)# crypto isakmp keepalive 20 10

```

{ Keepalive를 20초로 설정하고 만일 응답이 없다면 10초후에 다시 시도한다. }

Close X

완료

2005-12-06 <http://kowon.dongseo.ac.kr/~hjlee> 30

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Xauth 설정 설명

Remote client



```

router(config)#
aaa authentication login list-name method1 [method2]
vpngate1(config)# aaa authentication login vpusers local

```

{ Vpn 클라이언트의 AAA login 인증을 활성화 한다. }

NEXT

2005-12-06 http://kowon.dongseo.ac.kr/~hj lee 31

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

원격 접속 VPN 구성 방법

Easy VPN 서버 설정

Xauth 설정 설명

Remote client



```

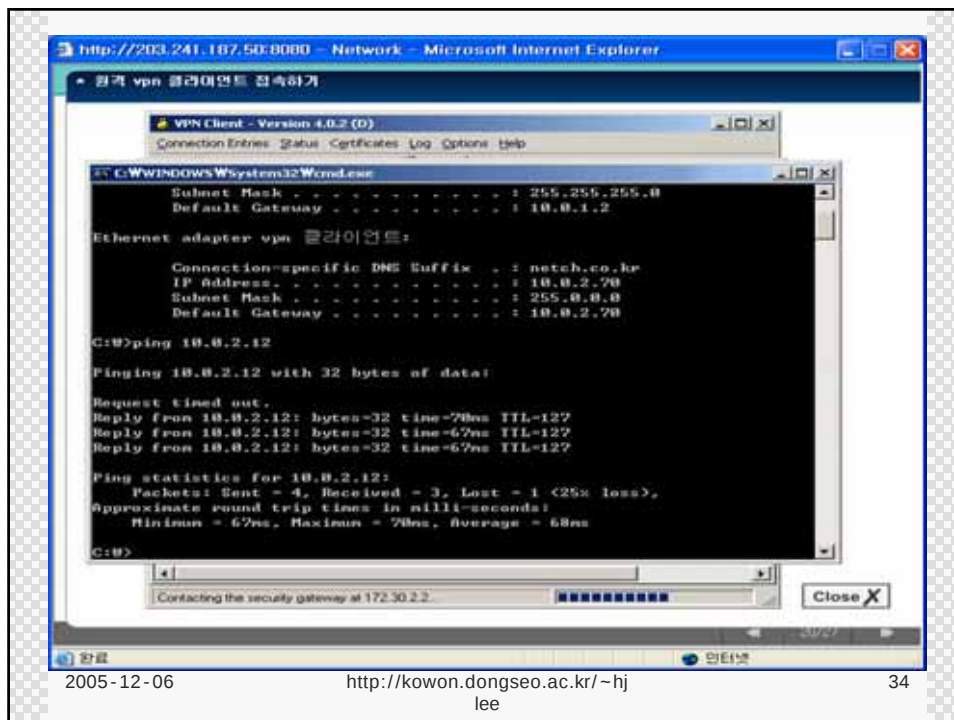
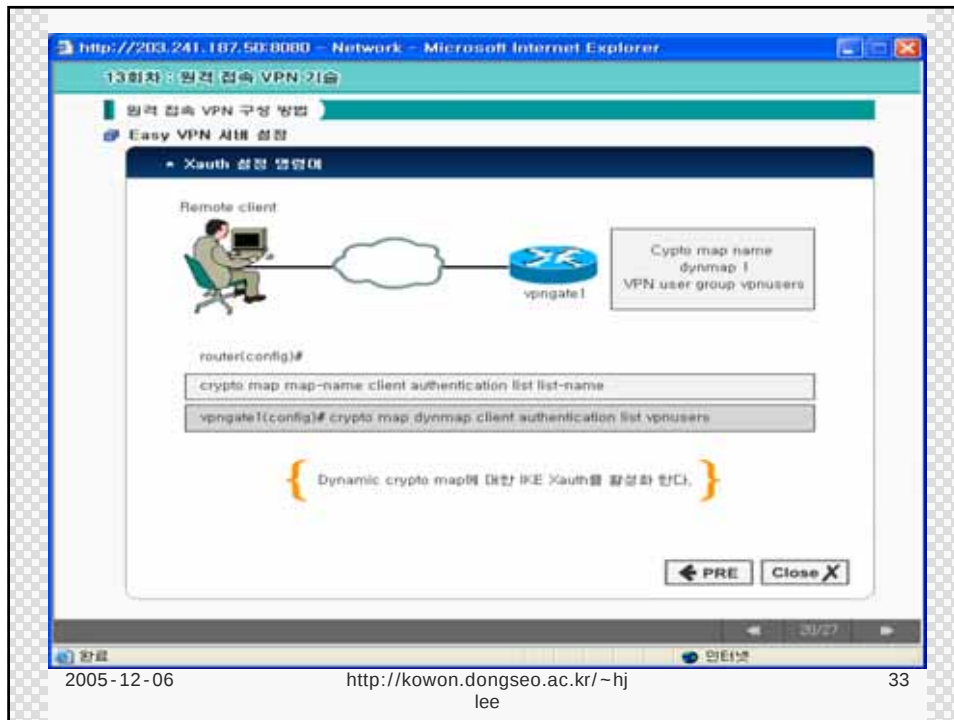
router(config)#
crypto isakmp xauth timeout seconds
vpngate1(config)# crypto isakmp xauth timeout 20

```

{ Xauth 타임아웃 값을 설정한다 }

PRE NEXT

2005-12-06 http://kowon.dongseo.ac.kr/~hj lee 32



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

 지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.

컴퓨터 원격 접속 VPN

원격 접속 VPN은 공용망 상에서 제3의 근무지나 이동 사용자와 같은 원격 사용자를 회사의 내부 네트워크에 안전하게 연결해주는 것이 목표이다.
원격 접속 VPN은 클라이언트-구동 (Client-initiated) 원격 접속 VPN과 NAS 구동 (NAS-initiated) 원격 접속 VPN의 두 가지 유형이 있다.
VPN 연결을 이용하여 정보를 전송하기 위해서는 보안 터널이 필요하다.

원격 접속 VPN 구성 방법

시스코의 원격 접속 VPN 서비스를 제공하기 위해서는 Easy VPN 서버와 Easy VPN 클라이언트가 필요하다. Easy VPN 서버는 시스코 IOS 라우터와 PIX 방화벽, 그리고 VPN 3000 집중기 (concentrator) 등이 서버로 간다. 원격 접속 VPN 서비스를 제공하는 VPN 헤드 엔드 장치로 동작할 수 있게 한다. Easy VPN 클라이언트는 시스코 IOS 라우터와 PIX 방화벽, VPN 3000 하드웨어나 소프트웨어 클라이언트가 원격 VPN 클라이언트로 동작할 수 있게 한다.

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 35

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

13회차 : 원격 접속 VPN 기술

 지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.

Easy VPN 연결 과정

제 1 단계: VPN 클라이언트, IKE Phase 1 시작
제 2 단계: VPN 클라이언트, IKE SA 제안
제 3 단계: Easy VPN 서버, IKE SA 제안 수락
제 4 단계: Easy VPN 서버, 사용자 인증/확인
제 5 단계: 모드 설정 과정 수행
제 6 단계: RRI (Reverse Route Injection) 과정 수행
제 7 단계: IKE 약 모드 (quick mode) 수행 및 IPSec SA 완료

Easy VPN 서버 설정

작업 1: IP address pool 설정
작업 2: Group policy lookup 설정
작업 3: 원격 접속 VPN 클라이언트를 위한 ISAKMP policy 설정
작업 4: 모드 설정을 위한 group policy 할당
작업 5: Transform set 설정
작업 6: RRI를 이용한 dynamic crypto map 설정
작업 7: Dynamic crypto map에 모드 설정 적용
작업 8: 라우터 외부 인터페이스에 dynamic crypto map 적용
작업 9: IKE DPD (dead peer detection) 활성화
작업 10: Xauth 설정

완료

2005-12-06 http://kowon.dongseo.ac.kr/~hjlee 36

End of Lecture



2005-12-06

<http://kowon.dongseo.ac.kr/~hjlee>

37