

Cisco VPN 3000 Concentrator with VPN Client Release 3.5 이상에서 TCP를 통한 IPSec 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN 3000 Concentrator 구성](#)

[단계별 지침](#)

[VPN 클라이언트 구성](#)

[VPN 3000 Concentrator에서 연결 확인](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 문서에서는 TCP(Transmission Control Protocol)를 통한 IPSec(IP Security)을 구성하는 방법에 대해 설명합니다. 이렇게 하면 VPN 클라이언트가 표준 ESP(Encapsulating Security Protocol), 프로토콜 50(Protocol 50) 또는 인터넷 키 교환(IKE, UDP(User Datagram Protocol) 500)이 작동하지 않거나 기존 방화벽 규칙을 수정하는 경우에만 작동할 수 있는 환경에서 작동할 수 있습니다. IPSec over TCP는 TCP 패킷 내에서 IKE 및 IPSec 프로토콜을 모두 캡슐화하고 NAT(Network Address Translation) 및 PAT(Port Address Translation) 디바이스와 방화벽을 통해 보안 터널링을 활성화합니다.

참고: IPSec over TCP는 프록시 기반 방화벽에서 작동하지 않습니다.

IPSec over TCP는 VPN 소프트웨어 클라이언트 및 VPN 3002 하드웨어 클라이언트 모두에서 작동합니다. Concentrator 기능은 클라이언트 전용 기능입니다. LAN-to-LAN 연결에는 작동하지 않습니다.

VPN 3000 Concentrator는 데이터를 교환하는 클라이언트를 기반으로 표준 IPSec, IPSec over TCP, IPSec over UDP를 동시에 지원할 수 있습니다.

한 번에 하나의 터널을 지원하는 VPN 3002 하드웨어 클라이언트는 표준 IPSec, IPSec over TCP 또는 IPSec over UDP를 사용하여 연결할 수 있습니다.

[사전 요구 사항](#)

[요구 사항](#)

VPN 3000 Concentrator의 공용 인터페이스를 구성해야 합니다. IPSec over TCP는 이더넷 2의 공용 인터페이스에서만 지원됩니다. 자세한 내용은 [Cisco VPN 클라이언트 릴리스 정보](#)를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 3000 Concentrator 버전 3.5 이상
- VPN Client 버전 3.5 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팀 표기 규칙](#)을 참조하십시오.

VPN 3000 Concentrator 구성

단계별 지침

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

1. Configuration(컨피그레이션) > User Management(사용자 관리) > Groups(그룹) > Add Group(그룹 추가)으로 이동하여 VPN Concentrator에 그룹 이름과 비밀번호를 생성합니다. 완료 시 Add(추가)를 클릭합니다

The screenshot shows the 'Add' page for creating a new group in the VPN 3000 Concentrator. The breadcrumb navigation is 'Configuration | User Management | Groups | Add'. A text box explains that the 'Inherit?' checkbox is used to inherit values from the base group. Below this, there are tabs for 'Identity', 'General', 'IPSec', 'Mode Config', 'Client FW', 'FW Client', and 'PPTP/L2TP'. The 'Identity Parameters' section contains a table with the following fields:

Attribute	Value	Description
Group Name	rtvpn	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

At the bottom of the form are 'Add' and 'Cancel' buttons.

2. 3.5 이전 버전의 VPN 클라이언트 사용자가 동일한 그룹을 사용하고 있거나 VPN 클라이언트에서 IPSec over UDP를 사용하는 경우 Client Config(클라이언트 컨피그레이션) 탭 아래에서 IPSec over UDP(IPSec over UDP)를 선택합니다

Client Configuration Parameters			
Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.
Microsoft Client Parameters			
Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	255.255.255.255	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.

3. Configuration(구성) > User Management(사용자 관리) > Users(사용자) > Modify Support(지원 수정)로 이동합니다. 내부 인증을 사용하는 경우 그룹에 인증할 사용자를 생성합니다. 그런 다음 해당 그룹에 사용자를 할당합니다

Configuration | User Management | Users | Modify esupport

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters		
Attribute	Value	Description
User Name	esupport	Enter a unique user name.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	rtvpn	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Apply Cancel

4. Configuration(컨피그레이션) > Tunneling and Security(터널링 및 보안) > NAT Transparency(NAT 투명도)로 이동하여 IPsec over TCP 옵션을 선택합니다. 포트를 구분하려면 쉽표를 사용하여 최대 10개의 포트를 입력합니다. 공백을 사용할 필요가 없습니다. 기본 포트는 10,000입니다. 범위는 1~65,635입니다. 잘 알려진 포트(예: 포트 80(HTTP) 또는 포트 443(HTTPS))를 입력하면 해당 포트와 연결된 프로토콜이 공용 인터페이스에서 더 이상 작동하지 않는다는 경고가 표시됩니다. 따라서 공용 인터페이스를 통해 더 이상 브라우저를 사용하여 VPN 3000 Concentrator를 관리할 수 없습니다. 이 문제를 해결하려면 HTTP/HTTPS 관리를 다른 포트로 재구성하십시오. VPN 클라이언트 및 VPN Concentrator에서 TCP 포트를 구성해야 합니다. 클라이언트 컨피그레이션에는 여기에 VPN Concentrator에 대해 설정한 포트 중 하나 이상이 포함되어야 합니다

Configuration | System | Tunneling Protocols | IPsec | IPsec over TCP

This section lets you configure system-wide IPsec over TCP operation.

Enabled

TCP Port(s) Enter up to 10 comma-separated TCP ports (1 - 65535).

VPN 클라이언트 구성

VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. 옵션 > 등록 정보로 이동합니다. General(일반) 탭에서 Enable Transparent Tunneling(투명 터널링 활성화)을 선택하고 Use IPsec over TCP(NAT/PAT/Firewall)를 선택합니다

Properties for 05-RTP

General | Authentication | Connections

Enter a description of this connection entry (optional):

Enable Transparent Tunneling

Allow IPsec over UDP (NAT/PAT)

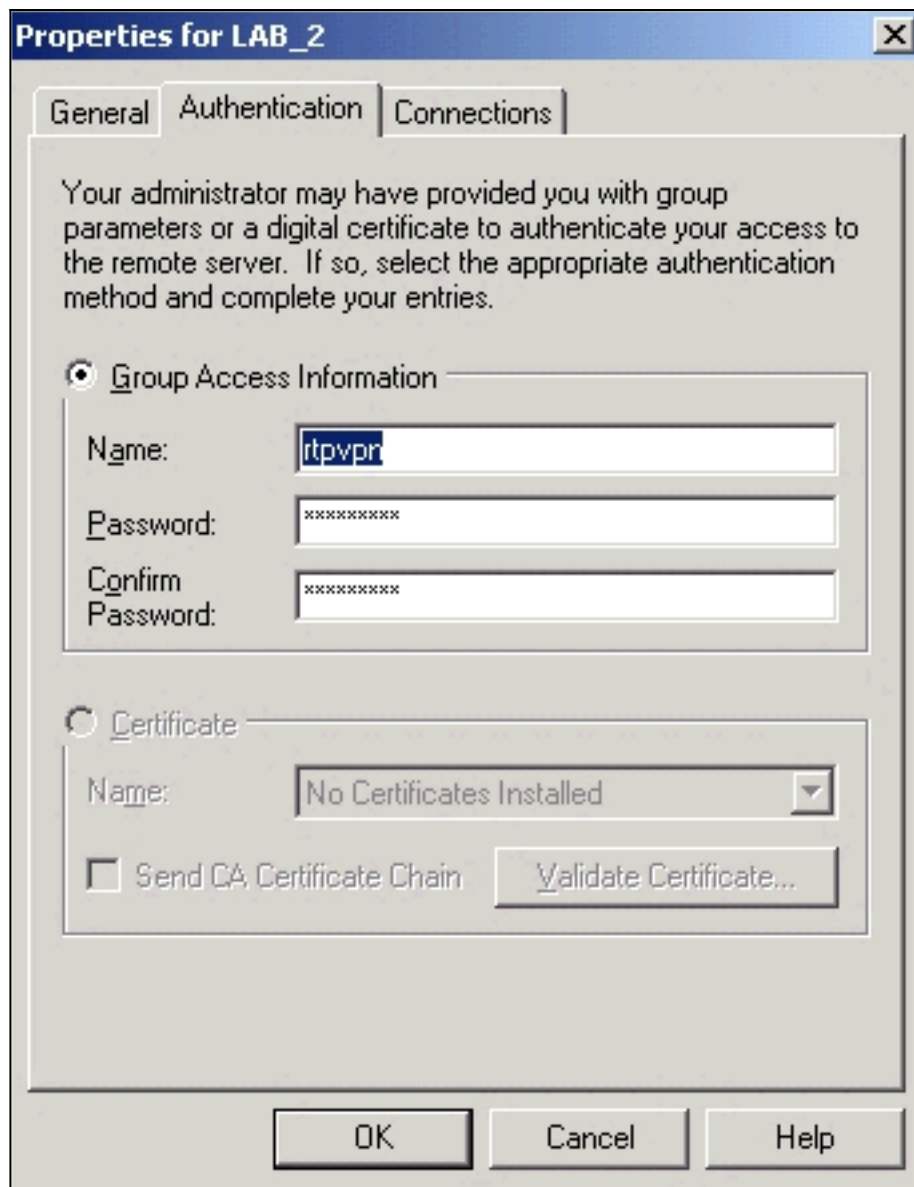
Use IPsec over TCP (NAT/PAT/Firewall)

TCP port:

Allow local LAN access

Peer response timeout: (30 - 480 seconds)

2. Authentication(인증) 탭에서 클라이언트에 그룹 이름 및 비밀번호를 구성합니다



[VPN 3000 Concentrator에서 연결 확인](#)

VPN 300 Concentrator의 Monitoring > **Sessions** 영역은 TCP를 통한 IPSec 및 UDP를 통한 IPSec에 대해 동일한 그룹을 가진 사용자의 연결을 확인합니다.

Monitoring | Sessions Wednesday, 05 December 2001 10:39:01
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	1	3	3	20	26

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
esupport	rtpvpn	64.102.55.209	172.18.124.217	IPSec/UDP	3DES-168	Dec 05 10:38:06	0:00:58	22416	1536
esupporttcp	rtpvpn	172.18.124.241	172.18.124.218	IPSec/TCP	3DES-168	Dec 05 10:39:02	0:00:02	64	72

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show** 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오](#).

Configuration(컨피그레이션) > System(시스템) > **Events(이벤트)** > Classes(클래스)에서 레벨 1~13에 대해 AUTH, AUTHDBG, AUTHDECODE, IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE에 대한 디버그를 활성화합니다.

```
1203 12/05/2001 11:40:54.220 SEV=9 IKEDBG/0 RPT=5347 172.18.124.241
Group [rtpvpn] User [esupporttcp]
processing SA payload
```

```
1204 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5035 172.18.124.241
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 696
```

```
1207 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5036 172.18.124.241
Proposal Decode:
Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40
```

```
1211 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5037 172.18.124.241
```

Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 28

1213 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5038 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1216 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5039 172.18.124.241
Proposal Decode:
Proposal # : 1
Protocol ID : IPCOMP (4)
#of Transforms: 1
Spi : 5D 82
Length : 34

1220 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5040 172.18.124.241
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : LZS (3)
Length : 24

1222 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5041 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1224 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5042 172.18.124.241
Proposal Decode:
Proposal # : 2
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1228 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5043 172.18.124.241
Transform # 1 Decode for Proposal # 2:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 28

1230 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5044 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1233 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5045 172.18.124.241
Proposal Decode:
Proposal # : 2
Protocol ID : IPCOMP (4)
#of Transforms: 1
Spi : D8 44
Length : 34

1237 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5046 172.18.124.241
Transform # 1 Decode for Proposal # 2:
Transform # : 1
Transform ID : LZS (3)
Length : 24

1239 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5047 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1241 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5048 172.18.124.241
Proposal Decode:
Proposal # : 3
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1245 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5049 172.18.124.241
Transform # 1 Decode for Proposal # 3:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 28

1247 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5050 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1250 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5051 172.18.124.241
Proposal Decode:
Proposal # : 4
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1254 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5052 172.18.124.241
Transform # 1 Decode for Proposal # 4:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 28

1256 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5053 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1259 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5054 172.18.124.241
Proposal Decode:
Proposal # : 5
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1263 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5055 172.18.124.241
Transform # 1 Decode for Proposal # 5:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 28

1265 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5056 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1268 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5057 172.18.124.241

Proposal Decode:

Proposal # : 5

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : 80 07

Length : 34

1272 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5058 172.18.124.241

Transform # 1 Decode for Proposal # 5:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1274 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5059 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1276 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5060 172.18.124.241

Proposal Decode:

Proposal # : 6

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38

Length : 40

1280 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5061 172.18.124.241

Transform # 1 Decode for Proposal # 6:

Transform # : 1

Transform ID : DES-CBC (2)

Length : 28

1282 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5062 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1285 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5063 172.18.124.241

Proposal Decode:

Proposal # : 6

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : 1A D4

Length : 34

1289 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5064 172.18.124.241

Transform # 1 Decode for Proposal # 6:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1291 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5065 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1293 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5066 172.18.124.241

Proposal Decode:

Proposal # : 7

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38
Length : 40

1297 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5067 172.18.124.241
Transform # 1 Decode for Proposal # 7:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 28

1299 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5068 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1302 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5069 172.18.124.241
Proposal Decode:
Proposal # : 8
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1306 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5070 172.18.124.241
Transform # 1 Decode for Proposal # 8:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 28

1308 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5071 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1311 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5072 172.18.124.241
Proposal Decode:
Proposal # : 9
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1315 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5073 172.18.124.241
Transform # 1 Decode for Proposal # 9:
Transform # : 1
Transform ID : NULL (11)
Length : 28

1317 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5074 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1320 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5075 172.18.124.241
Proposal Decode:
Proposal # : 9
Protocol ID : IPCOMP (4)
#of Transforms: 1
Spi : 7B 9B
Length : 34

1324 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5076 172.18.124.241

Transform # 1 Decode for Proposal # 9:

Transform # : 1
Transform ID : LZS (3)
Length : 24

1326 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5077 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1328 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5078 172.18.124.241
Proposal Decode:
Proposal # : 10
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1332 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5079 172.18.124.241
Transform # 1 Decode for Proposal # 10:
Transform # : 1
Transform ID : NULL (11)
Length : 28

1334 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5080 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1337 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5081 172.18.124.241
Proposal Decode:
Proposal # : 10
Protocol ID : IPCOMP (4)
#of Transforms: 1
Spi : 79 45
Length : 34

1341 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5082 172.18.124.241
Transform # 1 Decode for Proposal # 10:
Transform # : 1
Transform ID : LZS (3)
Length : 24

1343 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5083 172.18.124.241
Phase 2 SA Attribute Decode for Transform # 1:
Encapsulation : Tunnel (1)
Life Time : 2147483 seconds

1345 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5084 172.18.124.241
Proposal Decode:
Proposal # : 11
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40

1349 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5085 172.18.124.241
Transform # 1 Decode for Proposal # 11:
Transform # : 1
Transform ID : NULL (11)
Length : 28

1351 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5086 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: MD5 (1)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1354 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5087 172.18.124.241

Proposal Decode:

Proposal # : 12

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38

Length : 40

1358 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5088 172.18.124.241

Transform # 1 Decode for Proposal # 12:

Transform # : 1

Transform ID : NULL (11)

Length : 28

1360 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5089 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1363 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=666 172.18.124.241

Group [rtpvpn] User [esupporttcp]

processing nonce payload

1364 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=667 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Processing ID

1365 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/11 RPT=115

ID_IPV4_ADDR ID received

172.18.124.217

1366 12/05/2001 11:40:54.230 SEV=5 IKE/25 RPT=58 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Received remote Proxy Host data in ID Payload:

Address 172.18.124.217, Protocol 0, Port 0

1369 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=668 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Processing ID

1370 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/11 RPT=116

ID_IPV4_ADDR_SUBNET ID received

0.0.0.0

0.0.0.0

1371 12/05/2001 11:40:54.230 SEV=5 IKE/34 RPT=36 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Received local IP Proxy Subnet data in ID Payload:

Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

1374 12/05/2001 11:40:54.230 SEV=5 IKE/66 RPT=58 172.18.124.241

Group [rtpvpn] User [esupporttcp]

IKE Remote Peer configured for SA: ESP-3DES-MD5

1376 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5348 172.18.124.241

Group [rtpvpn] User [esupporttcp]

processing IPSEC SA

1377 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5090
IKE Decode of received SA attributes follows:
0000: 80050001 80040001 80010001 00020004
0010: 0020C49B . . .

1380 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5091
IKE Decode of received SA attributes follows:
0000: 80050002 80040001 80010001 00020004
0010: 0020C49B . . .

1383 12/05/2001 11:40:54.230 SEV=8 IKEDBG/0 RPT=5349
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
Phase 2 failure:
Mismatched attr types for class HMAC Algorithm:
Rcv'd: SHA
Cfg'd: MD5

1387 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5092
IKE Decode of received SA attributes follows:
0000: 80050001 80040001 80010001 00020004
0010: 0020C49B . . .

1390 12/05/2001 11:40:54.230 SEV=7 IKEDBG/27 RPT=58 172.18.124.241
Group [rtpvpn] User [esupporttcp]
IPSec SA Proposal # 3, Transform # 1 acceptable

1392 12/05/2001 11:40:54.230 SEV=7 IKEDBG/0 RPT=5350 172.18.124.241
Group [rtpvpn] User [esupporttcp]
IKE: requesting SPI!

1393 12/05/2001 11:40:54.230 SEV=9 IPSECDBG/6 RPT=282
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 58, err 0, type 2, mode 0, state 32, label 0, pad 0,
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0,
hmacAlg 0, lifetype 0, lifetime1 707832, lifetime2 0, dsId 300

1397 12/05/2001 11:40:54.230 SEV=9 IPSECDBG/1 RPT=1062
Processing KEY_GETSPI msg!

1398 12/05/2001 11:40:54.230 SEV=7 IPSECDBG/13 RPT=58
Reserved SPI 1889854019

1399 12/05/2001 11:40:54.230 SEV=8 IKEDBG/6 RPT=58
IKE got SPI from key engine: SPI = 0x70a4e243

1400 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5351 172.18.124.241
Group [rtpvpn] User [esupporttcp]
oakley constructing quick mode

1401 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5352 172.18.124.241
Group [rtpvpn] User [esupporttcp]
constructing blank hash

1402 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5353 172.18.124.241
Group [rtpvpn] User [esupporttcp]
constructing ISA_SA for ipsec

1403 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=669 172.18.124.241
Group [rtpvpn] User [esupporttcp]
constructing ipsec nonce payload

1404 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=670 172.18.124.241
Group [rtpvpn] User [esupporttcp]

constructing proxy ID

1405 12/05/2001 11:40:54.230 SEV=7 IKEDBG/0 RPT=5354 172.18.124.241
Group [rtppvpn] User [esupporttcp]
Transmitting Proxy Id:
Remote host: 172.18.124.217 Protocol 0 Port 0
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

1409 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5355 172.18.124.241
Group [rtppvpn] User [esupporttcp]
constructing qm hash

1410 12/05/2001 11:40:54.240 SEV=12 IKEDECODE/5 RPT=58
IKE Responder sending 2nd QM pkt: msg id = f2a6ce35

1411 12/05/2001 11:40:54.240 SEV=8 IKEDBG/0 RPT=5356 172.18.124.241
SENDING Message (msgid=f2a6ce35) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 152

1414 12/05/2001 11:40:54.250 SEV=8 IKEDECODE/0 RPT=5093 172.18.124.241
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): E7 AC CD 06 A6 74 A7 1A
Responder Cookie(8): 98 3B 37 97 CA 06 BC 18
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : f2a6ce35
Length : 52

1421 12/05/2001 11:40:54.250 SEV=8 IKEDBG/0 RPT=5357 172.18.124.241
RECEIVED Message (msgid=f2a6ce35) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

1423 12/05/2001 11:40:54.250 SEV=9 IKEDBG/0 RPT=5358 172.18.124.241
Group [rtppvpn] User [esupporttcp]
processing hash

1424 12/05/2001 11:40:54.250 SEV=9 IKEDBG/0 RPT=5359 172.18.124.241
Group [rtppvpn] User [esupporttcp]
loading all IPSEC SAs

1425 12/05/2001 11:40:54.250 SEV=9 IKEDBG/1 RPT=671 172.18.124.241
Group [rtppvpn] User [esupporttcp]
Generating Quick Mode Key!

1426 12/05/2001 11:40:54.260 SEV=9 IKEDBG/1 RPT=672 172.18.124.241
Group [rtppvpn] User [esupporttcp]
Generating Quick Mode Key!

1427 12/05/2001 11:40:54.260 SEV=7 IKEDBG/0 RPT=5360 172.18.124.241
Group [rtppvpn] User [esupporttcp]
Loading subnet:
Dst: 0.0.0.0 mask: 0.0.0.0
Src: 172.18.124.217

1429 12/05/2001 11:40:54.260 SEV=4 IKE/49 RPT=58 172.18.124.241
Group [rtppvpn] User [esupporttcp]
Security negotiation complete for User (esupporttcp)
Responder, Inbound SPI = 0x70a4e243, Outbound SPI = 0x9879d238

1432 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/6 RPT=283
IPSEC key message parse - msgtype 1, len 620, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,

spi 9879d238, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2,
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

1436 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1063
Processing KEY_ADD msg!

1437 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1064
key_msghdr2secassoc(): Enter

1438 12/05/2001 11:40:54.260 SEV=7 IPSECDBG/1 RPT=1065
No USER filter configured

1439 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1066
KeyProcessAdd: Enter

1440 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1067
KeyProcessAdd: Adding outbound SA

1441 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1068
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst
172.18.124.217 mask 0.0.0.0

1442 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1069
KeyProcessAdd: FilterIpssecAddIkeSa success

1443 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/6 RPT=284
IPSEC key message parse - msgtype 3, len 334, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 70a4e243, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2,
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

1447 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1070
Processing KEY_UPDATE msg!

1448 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1071
Update inbound SA addresses

1449 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1072
key_msghdr2secassoc(): Enter

1450 12/05/2001 11:40:54.260 SEV=7 IPSECDBG/1 RPT=1073
No USER filter configured

1451 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1074
KeyProcessUpdate: Enter

1452 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1075
KeyProcessUpdate: success

1453 12/05/2001 11:40:54.260 SEV=8 IKEDBG/7 RPT=58
IKE got a KEY_ADD msg for SA: SPI = 0x9879d238

1454 12/05/2001 11:40:54.260 SEV=8 IKEDBG/0 RPT=5361
pitcher: rcv KEY_UPDATE, spi 0x70a4e243

1455 12/05/2001 11:40:54.260 SEV=4 IKE/120 RPT=58
172.18.124.241
Group [rtpvpn] User [esupporttcp]
PHASE 2 COMPLETED (msgid=f2a6ce35)

1456 12/05/2001 11:40:55.120 SEV=7 IPSECDBG/1 RPT=1076
IPSec Inbound SA has received data!

1457 12/05/2001 11:40:55.120 SEV=8 IKEDBG/0 RPT=5362

pitcher: recv KEY_SA_ACTIVE spi 0x709e5f39

1458 12/05/2001 11:40:55.120 SEV=8 IKEDBG/0 RPT=5363
KEY_SA_ACTIVE no old rekey centry found with new spi
0x709e5f39, mess_id 0x0

관련 정보

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [Cisco VPN 클라이언트 지원 페이지](#)
- [IPSec 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)