Configurando o IPsec sobre o TCP em um Cisco VPN 3000 concentrator com VPN client versão 3.5 e mais tarde

Índice

Introdução

Este documento descreve como configurar a Segurança IP (IPsec) sobre o Transmission Control Protocol (TCP). Isto permite um cliente VPN de operar-se em um ambiente em que o protocolo encapsulating security padrão (ESP, 50 pés do protocolo) ou o intercâmbio de chave de Internet (IKE, User Datagram Protocol (UDP) 500) não pode funcionar, ou pode funcionar somente com alteração às regras existentes do Firewall. O IPsec sobre o TCP encapsula o IKE e protocolos IPSec dentro de um pacote de TCP, e permite o Tunelamento seguro com o Network Address Translation (NAT) e os dispositivos e os Firewall da tradução de endereço de porta (PAT).

Nota: O IPsec sobre o TCP não trabalha com firewall baseado em proxy.

O IPsec sobre o TCP trabalha com o cliente do software de VPN e o VPN 3002 Hardware Client. É um cliente à característica do concentrador somente. Não trabalha para conexões de LAN para LAN.

O VPN 3000 concentrator pode simultaneamente apoiar o IPSec padrão, o IPsec sobre o TCP, e o IPsec sobre o UDP, com base no cliente com que ele dados de trocas.

O VPN 3002 Hardware Client, que apoia um túnel de cada vez, pode conectar usando o IPSec padrão, o IPsec sobre o TCP, ou o IPsec sobre o UDP.

Pré-requisitos

Requisitos

A interface pública do VPN 3000 concentrator deve ser configurada. O IPsec sobre o TCP é apoiado somente na interface pública nos Ethernet 2. Refira os Release Note do Cisco VPN Client para mais informação.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 3.5 ou mais recente do VPN 3000 concentrator
- Versão 3.5 ou mais recente do cliente VPN

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

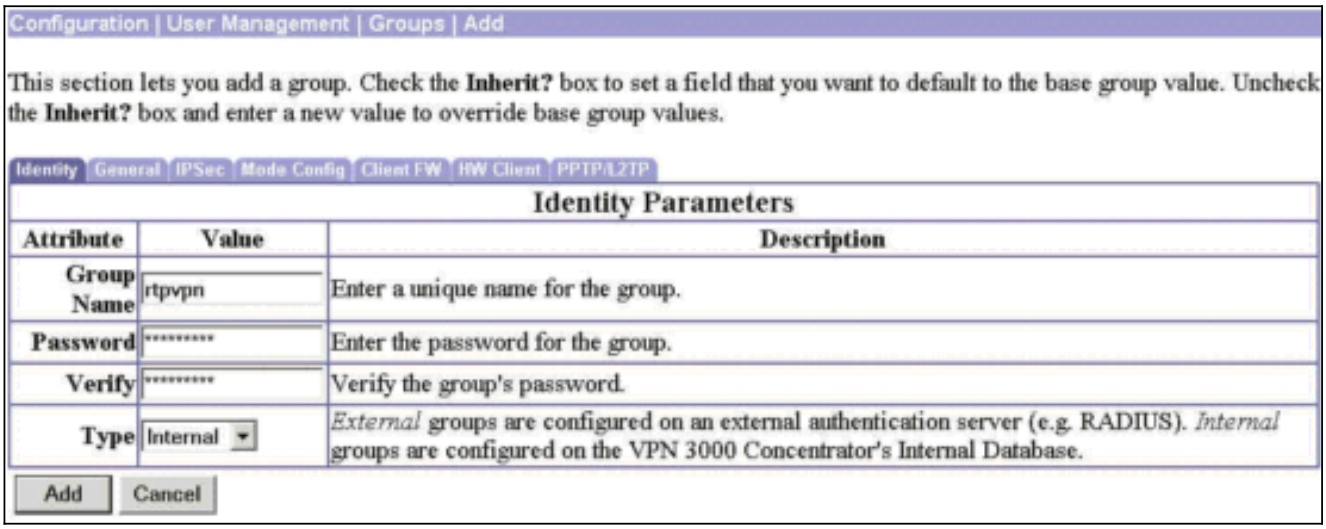
Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar o VPN 3000 Concentrator

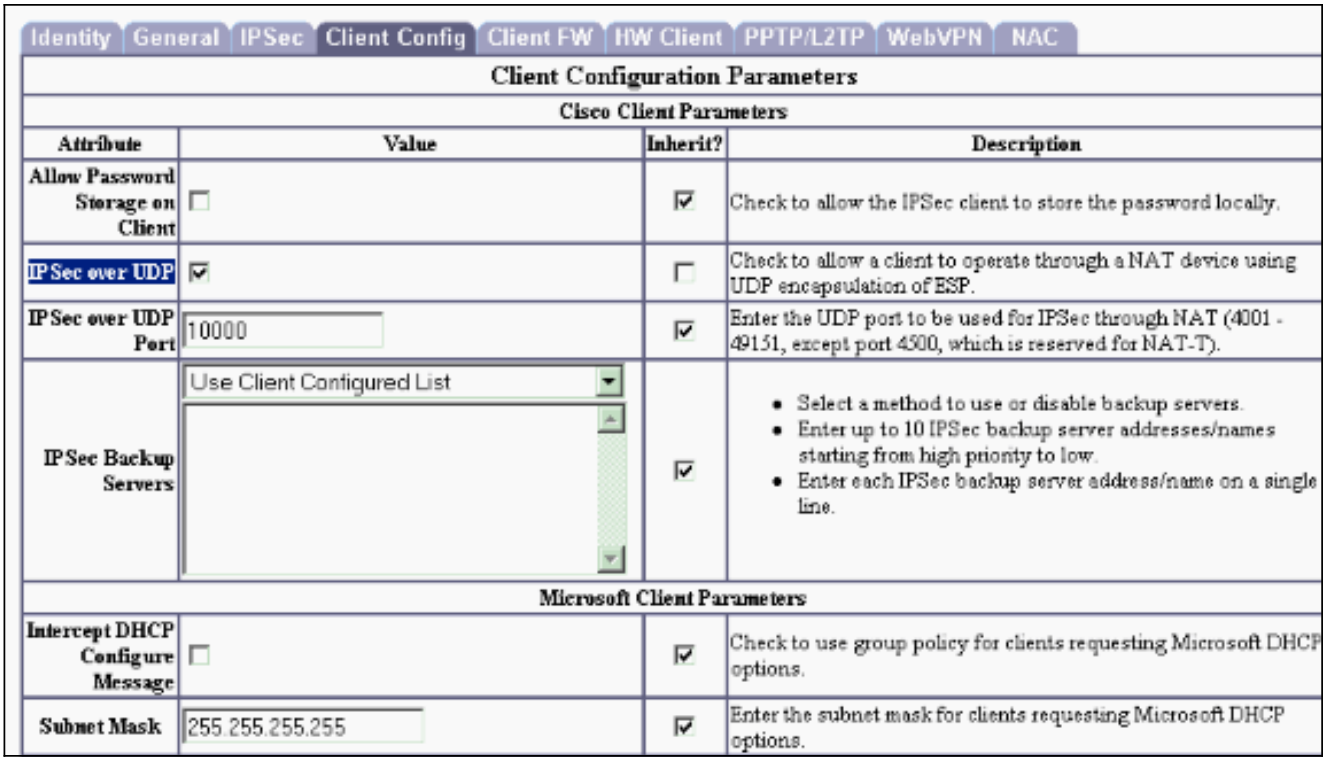
Instruções passo a passo

Termine estas etapas para configurar o VPN 3000 concentrator.

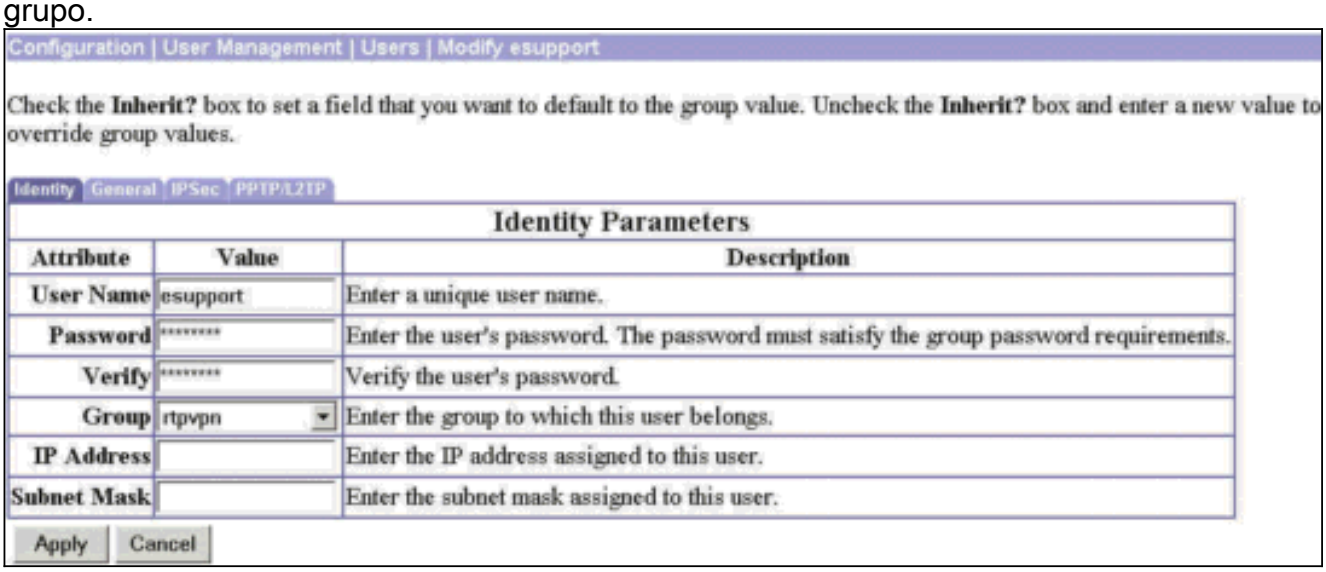
1. Vá ao **grupo do configuração > gerenciamento de usuário > grupos > adicionar** e crie um nome do grupo e uma senha no concentrador VPN. O clique **adiciona** em cima da conclusão.



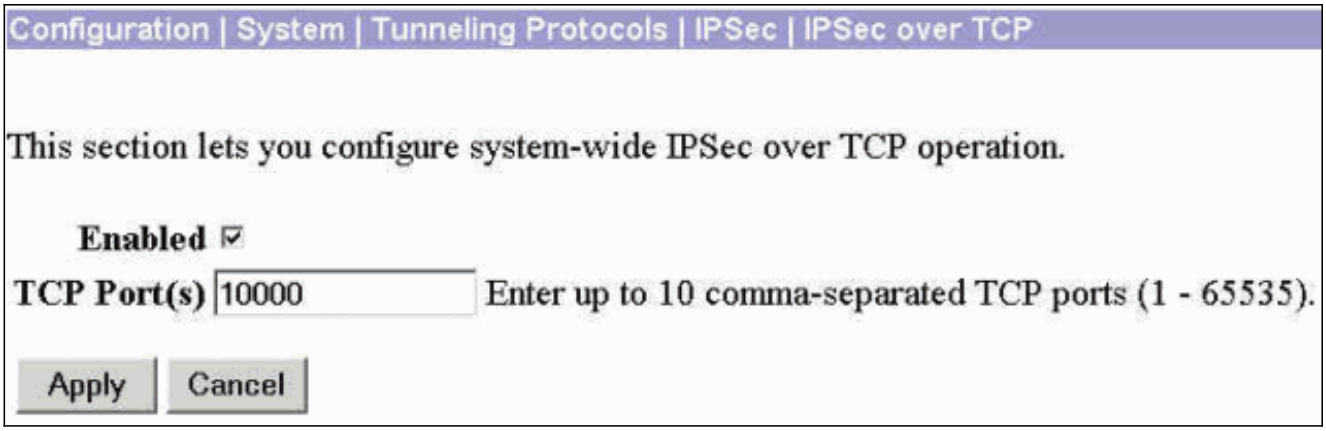
2. Se o mesmo grupo está sendo usado por usuários em versões do cliente VPN mais cedo de 3.5, ou se você está usando o IPsec sobre o UDP no cliente VPN, a seguir selecione o **IPsec sobre o UDP** sob o guia de configuração do cliente.



3. Vá ao **Configuração > Gerenciamento de Usuário > Usuários > Modify Esupport**. Se você está usando a autenticação interna, crie um usuário para autenticar ao grupo. Atribua então o usuário a esse
grupo.



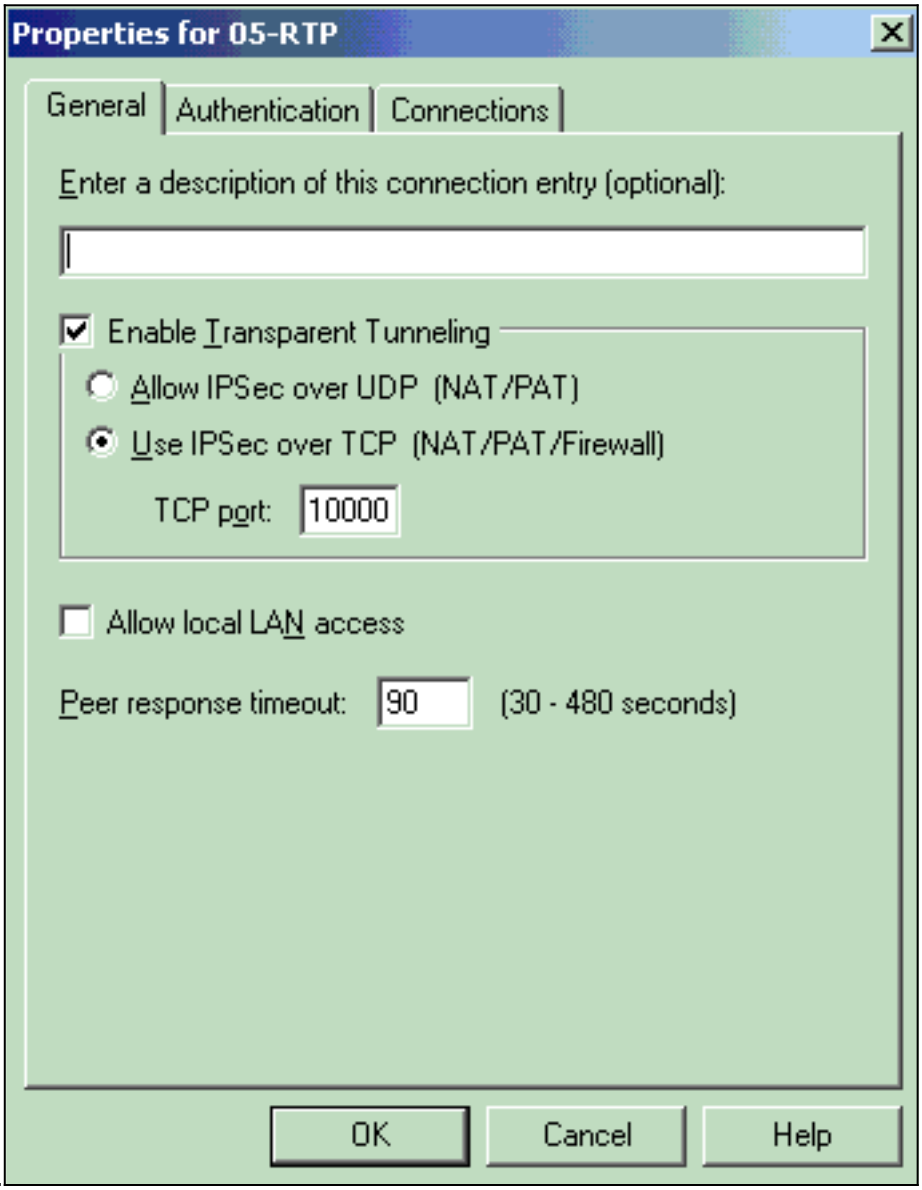
4. Vá à **configuração** > ao **Tunelamento e à Segurança** > à **transparência de NAT** e selecione o **IPsec sobre a opção de TCP**Entre até as portas 10, usando uma vírgula para separar as portas. Você não precisa de usar espaços. A porta padrão é 10,000. A escala é 1 a 65,635.Se você entra em uma porta bem conhecida (tal como a porta 80 (HTTP) ou a porta 443 (HTTPS), o sistema indica um aviso que o protocolo associado com essa porta já não trabalhe na interface pública. A consequência é que você pode já não usar um navegador para controlar o VPN 3000 concentrator através da interface pública. Para resolver este problema, reconfigure o Gerenciamento HTTP/HTTPS às portas diferentes.Você deve configurar a porta TCP no cliente VPN assim como no concentrador VPN. A configuração de cliente deve incluir pelo menos uma das portas que você se ajusta para o concentrador VPN aqui.



Configurar o VPN Client

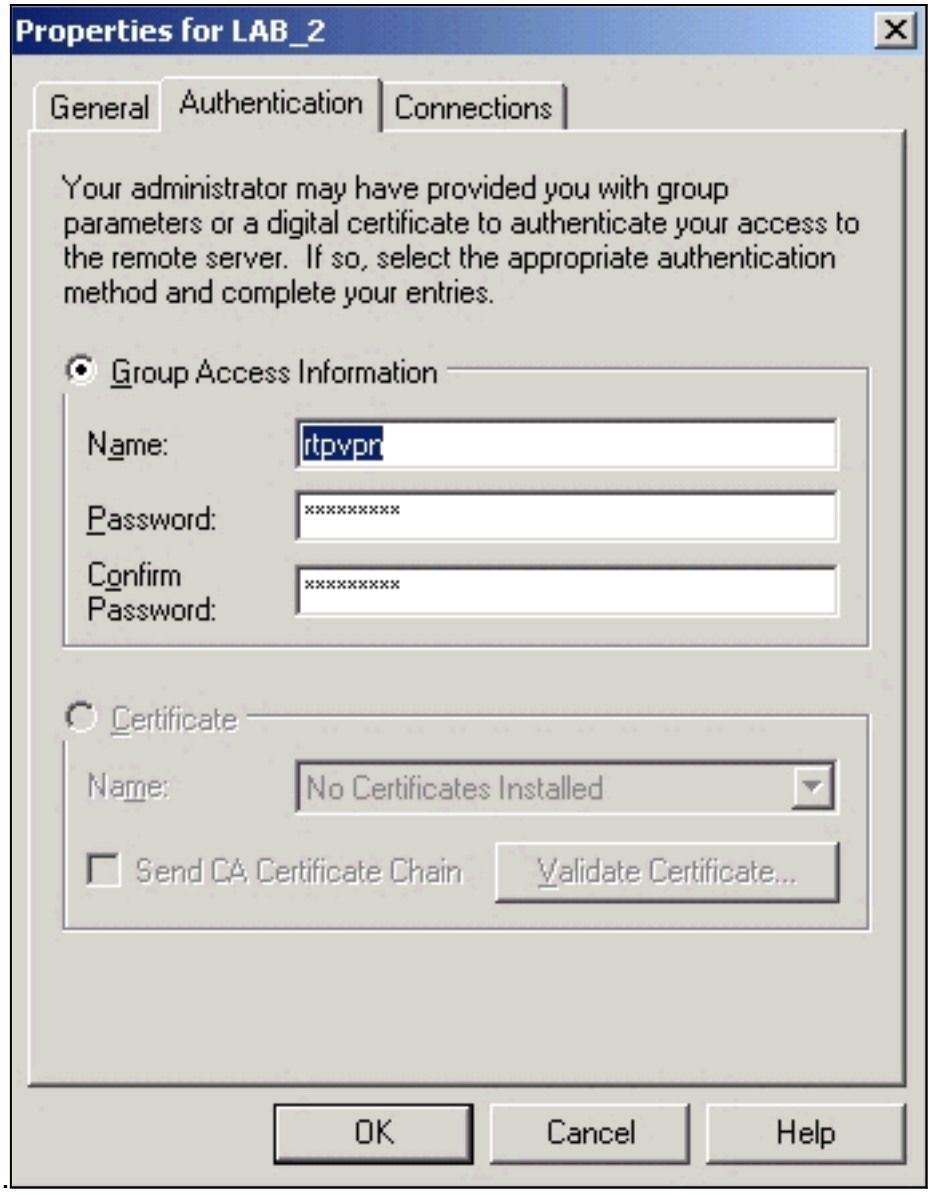
Termine estas etapas para configurar o cliente VPN.

1. Vá ao **opções > propriedades**. Sob o tab geral, a verificação **permite o Tunelamento transparente** e escolhe o **IPsec do uso sobre TCP (NAT/PAT/Firewall)**.



2. Sob a aba da autenticação, configurar um nome do grupo e uma senha no

cliente.



Verifique as conexões no VPN 3000 concentrator

A área do **monitoramento > sessões no** VPN 3000 concentrator verifica a conexão de usuários com o mesmo grupo para o IPsec sobre o TCP e o IPsec sobre o UDP.

Monitoring | Sessions — Wednesday, 05 December 2001 10:39:0

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 --All--

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

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

Permita debuga para o **AUTH, AUTHDBG, AUTHDECODE, IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE** para os níveis 1 a 13 sob o **configuração > sistema > eventos > classes**.

```
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 constucting 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 [rtpvpn] 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 [rtpvpn] 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 [rtpvpn] User [esupporttcp]
processing hash

1424 12/05/2001 11:40:54.250 SEV=9 IKEDBG/0 RPT=5359 172.18.124.241
Group [rtpvpn] 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 [rtpvpn] 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 [rtpvpn] 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 [rtpvpn] 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 [rtpvpn] 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: FilterIpsecAddIkeSa 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
```

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de Suporte do Cisco VPN Client
- Página de suporte do IPSec
- Suporte Técnico e Documentação - Cisco Systems