Configurando Vários VPN Clients em um Concentrador Cisco VPN 3000 Usando NAT-Traversal

Índice

Introdução

Este documento mostra como configurar um NAT-T entre Clientes de VPN Cisco localizados atrás de um dispositivo PAT/NAT e um Concentrador de VPN Cisco. O NAT-T pode ser usado entre clientes VPN e um concentrador VPN, ou entre concentradores atrás de um dispositivo NAT/PAT. O NAT-T pode igualmente ser usado ao conectar a um Cisco IOS ® Software running e ao PIX Firewall do roteador Cisco; contudo, estas configurações não são discutidas neste documento.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco VPN 3000 Concentrator 4.0(1)B
- Clientes Cisco VPN: 3.6.1 e 4.0(3) Rel
- Cisco PIX Firewall (dispositivo PAT), versão 6.3(3)

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Há Clientes VPN nos dois PCs (10.10.10.2 e 10.10.10.3) atrás do firewall PIX. Nesse cenário, o PIX está simplesmente sendo usado como dispositivo PAT e conduz o PAT nesses endereços para 171.69.89.78. Qualquer dispositivo que possa ter conexões internas múltiplas de PAT pode ser usado aqui. O endereço público do VPN 3000 Concentrator é 172.16.172.50. O exemplo seguinte demonstra como configurar os clientes e o concentrador de modo que o NAT-T seja usado durante a negociação de IKE.

Convenções

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

Informações de Apoio

Após a conclusão da negociação NAT-T, o iniciador pode usar qualquer porta aleatória do tipo User Datagram Protocol (UDP) (Y). A porta de destino deve ser UDP 4500, como em UDP (Y, 4500) e o respondedor usa UDP (4500, Y). Todas as negociações subsequentes do Internet Key Exchange (IKE) e rekeying são feitas nestas portas. Durante negociações NAT-T, ambos os ipsec peer negociam as portas UDP e igualmente determinam se são atrás de um dispositivo NAT/PAT. O ipsec peer atrás do dispositivo NAT/PAT envia o pacote keepalive IPsec-sobre-UDP NAT ao ipsec peer que não é atrás de um dispositivo NAT/PAT. O NAT-T encapsula tráfego IPSec em datagramas UDP usando a porta 4500, fornecendo assim dispositivos NAT com informações sobre a porta. O NAT-T detecta automaticamente qualquer dispositivo NAT e, quando necessário, encapsula somente o tráfego de IPSec.

Ao executar o IPsec sobre a tradução NAT no VPN 3000 concentrator, o IPsec sobre o TCP toma a primeiros precedência, então NAT-T, e então IPsec sobre o UDP. À revelia, o NAT-T é desligado. É necessário ativar NAT-T usando uma caixa de seleção localizada em NAT Transparency, sob a configuração de IPSec que está dentro de Tunneling Protocols. Ainda, para um túnel de LAN para LAN, você deve ligar o NAT-T no campo IPSec NAT-T nas configurações de LAN para LAN.

Para usar o NAT-T, você deve completar os passos a seguir:

1. Abra a porta 4500 em qualquer firewall que você tenha configurado em frente a um concentrador de VPN.
2. Defina novamente as configurações IPSec e UDP anteriores, usando a porta 4500 em uma porta diferente.
3. Escolha o **Configuração > Interfaces > Ethernet**, e escolha as segundas ou terceiras opções para o parâmetro Política de Fragmentação.Estas opções permitem que o tráfego viaje através dos dispositivos NAT que não apoiam a fragmentação de IP; não impedem a operação de dispositivos NAT que apoia a fragmentação de IP.

Configure o PIX

A saída de configuração relevante para o PIX é mostrado aqui:

Firewall de PIX

```
pix501(config)#
: Saved
:
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 171.69.89.78 255.255.254.0
ip address inside 10.10.10.1 255.255.255.0
...
global (outside) 1 interface nat (inside) 1 0.0.0.0
0.0.0.0 0 0 ... route outside 0.0.0.0 0.0.0.0
171.69.88.1 1 http server enable http 10.10.10.2
255.255.255.255 inside ...
Cryptochecksum:6990adf6e0e2800ed409ae7364eecc9d : end
[OK]
```

Configurar o VPN 3000 Concentrator

Esta mesma configuração presume que o VPN 3000 Concentrator já esteja configurado para conectividade de IP e que as conexões de VPN padrão (não-NAT-T) já estejam estabelecidas.

Para permitir mais cedo o NAT-T em uma liberação do VPN 3000 concentrator do que a versão 4.1, escolha **configurações > sistema > Tunneling Protocols > IPsec > transparência de NAT**, a seguir verifique o **IPsec sobre a** opção **NAT-T no** concentrador segundo as indicações do exemplo abaixo. Por padrão, a opção NAT-T está desativada.

Para permitir o NAT-T em uma versão 4.1 e mais recente do concentrador VPN, navegue à mesma janela Transparência do NAT escolhendo a **configuração > o Tunelamento e a Segurança > o IPsec > a transparência de NAT**.

Configurar o VPN Client

Para usar o NAT-T, selecione Enable Transparent Tunneling. O exemplo a seguir demonstra isso em um VPN Cliente posterior à versão 4.0.

Nota: A mesma opção de configuração está disponível no VPN Client versão 3.x.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

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

A informação adicional de Troubleshooting pode ser encontrada no Troubleshooting de Segurança IP - Compreendendo e usando comandos debug.

Verificar a configuração do PIX

Esses comandos são usados para verificar a configuração PIX:

- **xlate da mostra** — Segundo as indicações da saída abaixo, o PIX está usando portas de origem diferentes para os dois clientes VPN, mas as portas do destino são as mesmas. Todos os pacotes de dados IPSec são distribuídos usando a porta de UDP 4500. As Negociações de modificação de chave subsequente igualmente usam as mesmas portas de origem e de destino.`pix501(config)# show xlate 3 in use, 4 most used PAT Global 171.69.89.78(1025) Local 10.10.10.3(4500) PAT Global 171.69.89.78(1026) Local 10.10.10.2(4500) PAT Global 171.69.89.78(4) Local 10.10.10.2(500)`
- **mostra arp** — Use este comando indicar a tabela do Address Resolution Protocol (ARP) e determinar se as requisições ARP estão sendo processadas.`pix501(config)# show arp outside 171.69.88.3 00d0.0132.e40a outside 171.69.88.2 00d0.0133.3c0a outside 171.69.88.1 0000.0c07.ac7b inside 10.10.10.3 0050.dabb.f093 inside 10.10.10.2 0001.0267.55cc pix501(config)#`

Estatísticas do VPN Client

Uma vez que o túnel VPN é estabelecido, clicar com o botão direito no fechamento amarelo e escolha o **estado**. Um indicador similar é mostrado abaixo. Observe que a porta do túnel é UDP 4500, o que prova que você está utilizando o NAT-T.

Estatísticas do concentrador de VPN

Conclua estes passos:

1. No concentrador VPN, escolha o **administração > sessão de administrador**.A sessão do VPN Client pode ser vista em Remote Access Sessions (Sessões de acesso remoto). O exemplo abaixo mostra as sessões dos dois clientes depois que estabeleceram um túnel de IPsec ao concentrador VPN. Ambos estão usando o endereço IP público 171.69.89.78 e foram atribuídos a 40.1.1.1 e 40.1.1.2, respectivamente.
2. Clique duas vezes em um nome de usuário de cliente.As estatísticas de IPSec/IKE são mostradas, como visto no exemplo a seguir. A porta de origem de UDP usada pelo cliente é a 1029 e a porta de destino é a 4500.

Troubleshooting

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

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

Nota: A informação de Troubleshooting adicional PIX pode ser encontrada no Troubleshooting de Segurança IP - compreendendo e usando comandos debug.

Registros de clientes VPN

No PC em que o cliente VPN é instalado, abra o Log Viewer antes de estabelecer uma conexão ao concentrador VPN. Esta saída de registro destaca as mensagens específicas do NAT-T.

```
1      21:06:48.208  10/18/02  Sev=Info/6   DIALER/0x63300002
Initiating connection.
2      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100002
Begin connection process
3      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100004
Establish secure connection using Ethernet
4      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100026
Attempt connection with server "172.16.172.50"
42     21:07:42.326  10/18/02  Sev=Info/6  IKE/0x6300003B
Attempting to establish a connection with 172.16.172.50.
43     21:07:42.366  10/18/02  Sev=Info/4  IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID, VID, VID)
 to 172.16.172.50
44     21:07:42.716  10/18/02  Sev=Info/5  IKE/0x6300002F
Received ISAKMP packet: peer = 172.16.172.50
45     21:07:42.716  10/18/02  Sev=Info/4  IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID, VID, NAT-D, NAT-D, VID, VID)
from 172.16.172.50 46 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload =
12F5F28C457168A9702D9FE274CC0100 47 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer is a
Cisco-Unity compliant peer 48 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload
= 09002689DFD6B712 49 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 50
21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload =
AFCAD71368A1F1C96B8696FC77570100 51 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer
supports DPD 52 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload =
90CB80913EBB696E086381B5EC427B1F 53 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer
supports NAT-T 54 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload =
4048B7D56EBCE88525E7DE7F00D6C2D3C0000000 55 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer
supports IKE fragmentation payloads 56 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID
payload = 1F07F70EAA6514D3B0FA96542A500306 57 21:07:42.757 10/18/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D) to 172.16.172.50
58 21:07:42.767 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50
59 21:07:42.767 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR)
from 172.16.172.50 60 21:07:42.767 10/18/02 Sev=Info/4 CM/0x63100015 Launch xAuth application 61
21:07:42.967 10/18/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 62 21:07:59.801 10/18/02
Sev=Info/4 CM/0x63100017 xAuth application returned 63 21:07:59.801 10/18/02 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50 64 21:08:00.101
10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 65 21:08:00.101
10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.16.172.50 66 21:08:00.101 10/18/02 Sev=Info/5 IKE/0x63000071 Automatic NAT Detection Status:
Remote end is NOT behind a NAT device This end IS behind a NAT device 67 21:08:00.101 10/18/02
Sev=Info/4 CM/0x6310000E Established Phase 1 SA. 1 Phase 1 SA in the system 68 21:08:00.111
10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50
69 21:08:00.111 10/18/02 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to
concentrator 70 21:08:00.111 10/18/02 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco
Integrated Client, Capability= (Centralized Protection Policy). 71 21:08:00.111 10/18/02
Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50 72
21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 73
```

21:08:00.122 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50 74 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 40.1.1.1 75 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 76 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 77 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc. /VPN 3000 Concentrator Version 3.6.1.Rel built by vmurphy on Aug 29 2002 18:34:44 78 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D **MODE_CFG_REPLY: Attribute = Recieved and using NAT-T port number , value = 0x00001194** 79 21:08:00.132 10/18/02 Sev=Info/4 CM/0x63100019 Mode Config data received 80 21:08:00.142 10/18/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 172.16.172.50, GW IP = 172.16.172.50 81 21:08:00.142 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50 82 21:08:00.142 10/18/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 172.16.172.50 83 21:08:00.142 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50 84 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 85 21:08:00.172 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 86 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 87 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 18 seconds, setting expiry to 86382 seconds from now 88 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 89 21:08:00.182 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 90 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 91 21:08:00.182 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50 92 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000058 **Loading IPsec SA (Message ID = 0x347A7363 OUTBOUND SPI = 0x02CC3526 INBOUND SPI = 0x5BEEBB4C)** 93 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000025 **Loaded OUTBOUND ESP SPI: 0x02CC3526** 94 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000026 **Loaded INBOUND ESP SPI: 0x5BEEBB4C** 95 21:08:00.182 10/18/02 Sev=Info/4 CM/0x6310001A **One secure connection established** 96 21:08:00.192 10/18/02 Sev=Info/6 DIALER/0x63300003 **Connection established.** 97 21:08:00.332 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 98 21:08:00.332 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 99 21:08:00.332 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 100 21:08:00.332 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50 101 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000058 Loading IPsec SA (Message ID = 0x2F81FB2D OUTBOUND SPI = 0x3316C6C9 INBOUND SPI = 0x6B96ED76) 102 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000025 **Loaded OUTBOUND ESP SPI: 0x3316C6C9** 103 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000026 **Loaded INBOUND ESP SPI: 0x6B96ED76** 104 21:08:00.342 10/18/02 Sev=Info/4 CM/0x63100022 **Additional Phase 2 SA established.** 105 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 106 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 107 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x2635cc02 into key list 108 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 109 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x4cbbee5b into key list 110 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 111 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0xc9c61633 into key list 112 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 113 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x76ed966b into key list 114 21:08:10.216 10/18/02 Sev=Info/6 IKE/0x63000054 Sent a ping on the Public IPSec SA 115 21:08:20.381 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:HEARTBEAT) to 172.16.172.50 116 21:08:20.381 10/18/02 Sev=Info/6 IKE/0x63000052 Sent a ping on the IKE SA

Registros do VPN Concentrator

Para ver entra o concentrador VPN, escolhem a **monitoração > o log filtrável de eventos**, e selecionam as **classes de evento IKE, IKEDBG, IKEDECODE**, e **IPSECDBG** com gravidades 1 a 13.

```
2835 10/20/2002 20:22:42.390 SEV=8 IKEDECODE/0 RPT=8190 171.69.89.78
  Exchange Type :Oakley Quick Mode
  Flags         :1   (ENCRYPT )
  Message ID    : 1b050792
```

Length : 52
2838 10/20/2002 20:22:42.390 SEV=8 IKEDBG/0 RPT=9197 171.69.89.78
RECEIVED Message (msgid=1b050792) with payloads :
HDR + HASH (8) + NONE (0)
total length : 48
2840 10/20/2002 20:22:42.390 SEV=9 IKEDBG/0 RPT=9198 171.69.89.78
Group [ciscovpn] User [vpnclient2]
processing hash
2841 10/20/2002 20:22:42.390 SEV=9 IKEDBG/0 RPT=9199 171.69.89.78
Group [ciscovpn] User [vpnclient2]
loading all IPSEC SAs
2842 10/20/2002 20:22:42.390 SEV=9 IKEDBG/1 RPT=793 171.69.89.78
Group [ciscovpn] User [vpnclient2]
Generating Quick Mode Key!
2843 10/20/2002 20:22:42.390 SEV=9 IKEDBG/1 RPT=794 171.69.89.78
Group [ciscovpn] User [vpnclient2]
Generating Quick Mode Key!
2844 10/20/2002 20:22:42.400 SEV=4 IKE/173 RPT=41 171.69.89.78
Group [ciscovpn] User [vpnclient2]
NAT-Traversal successfully negotiated! IPSec traffic will be encapsulated to pass through NAT devices. 2847 10/20/2002 20:22:42.400 SEV=7 IKEDBG/0 RPT=9200 171.69.89.78 Group [ciscovpn] User [vpnclient2] Loading host: Dst: 172.16.172.50 Src: 40.1.1.2 2849 10/20/2002 20:22:42.400 SEV=4 IKE/49 RPT=63 171.69.89.78 Group [ciscovpn] User [vpnclient2] Security negotiation complete for User (vpnclient2) Responder, Inbound SPI = 0x350f3cb1, Outbound SPI = 0xc74e30e5 2852 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/6 RPT=309 IPSEC key message parse - msgtype 1, Len 704, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state 320, label 0, pad 0, spi c74e30e5, encrKeyLen 24, hashKe yLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 2856 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1137 Processing KEY_ADD msg! 2857 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1138 key_msghdr2secassoc(): Enter 2858 10/20/2002 20:22:42.400 SEV=7 IPSECDBG/1 RPT=1139 No USER filter configured 2859 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1140 KeyProcessAdd: Enter 2860 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1141 KeyProcessAdd: Adding outbound SA 2861 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1142 KeyProcessAdd: src 172.16.172.50 mask 0.0.0.0, DST 40.1.1.2 mask 0.0.0.0 2862 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1143 KeyProcessAdd: FilterIpsecAddIkeSa success 2863 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/6 RPT=310 IPSEC key message parse - msgtype 3, Len 376, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state 32, label 0, pad 0, spi 350f3cb1, encrKeyLen 24, hashKey Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 2866 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1144 Processing KEY_UPDATE MSG! 2867 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1145 Update inbound SA addresses 2868 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1146 key_msghdr2secassoc(): Enter 2869 10/20/2002 20:22:42.400 SEV=7 IPSECDBG/1 RPT=1147 No USER filter configured 2870 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1148 KeyProcessUpdate: Enter 2871 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1149 KeyProcessUpdate: success 2872 10/20/2002 20:22:42.400 SEV=8 IKEDBG/7 RPT=63 IKE got a KEY_ADD MSG for SA: SPI = 0xc74e30e5 2873 10/20/2002 20:22:42.400 SEV=8 IKEDBG/0 RPT=9201 pitcher: rcv KEY_UPDATE, spi 0x350f3cb1 2874 10/20/2002 20:22:42.400 SEV=4 IKE/120 RPT=63 171.69.89.78 Group [ciscovpn] User [vpnclient2] PHASE 2 COMPLETED (msgid=1b050792) 2875 10/20/2002 20:22:42.430 SEV=8 IKEDECODE/0 RPT=8191 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47 Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : cf9d1420 Length : 52 2882 10/20/2002 20:22:42.430 SEV=8 IKEDBG/0 RPT=9202 171.69.89.78 RECEIVED Message (msgid=cf9d1420) with payloads : HDR + HASH (8) + NONE (0) total length : 48 2884 10/20/2002 20:22:42.430 SEV=9 IKEDBG/0 RPT=9203 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 2885 10/20/2002 20:22:42.430 SEV=9 IKEDBG/0 RPT=9204 171.69.89.78 Group [ciscovpn] User [vpnclient2] loading all IPSEC SAs 2886 10/20/2002 20:22:42.430 SEV=9 IKEDBG/1 RPT=795 171.69.89.78 Group [ciscovpn] User [vpnclient2] Generating Quick Mode Key! 2887 10/20/2002 20:22:42.440 SEV=9 IKEDBG/1 RPT=796 171.69.89.78 Group [ciscovpn] User [vpnclient2] Generating Quick Mode Key! 2888 10/20/2002 20:22:42.440 SEV=4 IKE/173 RPT=42 171.69.89.78 **Group [ciscovpn] User [vpnclient2] NAT-Traversal successfully negotiated! IPSec traffic will be encapsulated to pass through NAT devices.** 2891 10/20/2002 20:22:42.440 SEV=7 IKEDBG/0 RPT=9205 171.69.89.78 Group [ciscovpn] User [vpnclient2] Loading subnet: DST: 0.0.0.0 mask: 0.0.0.0 Src: 40.1.1.2 2893 10/20/2002 20:22:42.440 SEV=4 IKE/49 RPT=64 171.69.89.78 Group [ciscovpn] User [vpnclient2] Security negotiation complete for User (vpnclient2) Responder, Inbound SPI = 0x2a2e2dcd, Outbound SPI = 0xf1f4d328 2896 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/6 RPT=311 IPSEC key message parse - msgtype 1, Len 704, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state

320, label 0, pad 0, spi f1f4d328, encrKeyLen 24, hashKe yLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 2900 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1150 Processing KEY_ADD MSG! 2901 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1151 key_msghdr2secassoc(): Enter 2902 10/20/2002 20:22:42.440 SEV=7 IPSECDBG/1 RPT=1152 No USER filter configured 2903 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1153 KeyProcessAdd: Enter 2904 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1154 KeyProcessAdd: Adding outbound SA 2905 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1155 KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, DST 40.1.1.2 mask 0.0.0.0 2906 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1156 KeyProcessAdd: FilterIpsecAddIkeSa success 2907 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/6 RPT=312 IPSEC key message parse - msgtype 3, Len 376, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state 32, label 0, pad 0, spi 2a2e2dcd, encrKeyLen 24, hashKey Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 2910 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1157 Processing KEY_UPDATE MSG! 2911 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1158 Update inbound SA addresses 2912 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1159 key_msghdr2secassoc(): Enter 2913 10/20/2002 20:22:42.440 SEV=7 IPSECDBG/1 RPT=1160 No USER filter configured 2914 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1161 KeyProcessUpdate: Enter 2915 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1162 KeyProcessUpdate: success 2916 10/20/2002 20:22:42.440 SEV=8 IKEDBG/7 RPT=64 IKE got a KEY_ADD MSG for SA: SPI = 0xf1f4d328 2917 10/20/2002 20:22:42.440 SEV=8 IKEDBG/0 RPT=9206 pitcher: rcv KEY_UPDATE, spi 0x2a2e2dcd 2918 10/20/2002 20:22:42.440 SEV=4 IKE/120 RPT=64 171.69.89.78 Group [ciscovpn] User [vpnclient2] PHASE 2 COMPLETED (msgid=cf9d1420) 2919 10/20/2002 20:22:44.680 SEV=7 IPSECDBG/1 RPT=1163 IPSec Inbound SA has received data! 2920 10/20/2002 20:22:44.680 SEV=8 IKEDBG/0 RPT=9207 pitcher: recv KEY_SA_ACTIVE spi 0x2a2e2dcd 2921 10/20/2002 20:22:44.680 SEV=8 IKEDBG/0 RPT=9208 KEY_SA_ACTIVE no old rekey centry found with new spi 0x2a2e2dcd, mess_id 0x0 2922 10/20/2002 20:22:47.530 SEV=9 IPSECDBG/18 RPT=828 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2923 10/20/2002 20:22:47.530 SEV=9 IPSECDBG/18 RPT=829 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2924 10/20/2002 20:22:48.280 SEV=9 IPSECDBG/17 RPT=668 Received an IPSEC-over-NAT-T NAT keepalive packet 2925 10/20/2002 20:22:52.390 SEV=9 IPSECDBG/17 RPT=669 **Received an IPSEC-over-NAT-T NAT keepalive packet** 2926 10/20/2002 20:22:52.720 SEV=7 IPSECDBG/1 RPT=1164 IPSec Inbound SA has received data! 2927 10/20/2002 20:22:52.720 SEV=8 IKEDBG/0 RPT=9209 pitcher: recv KEY_SA_ACTIVE spi 0x19fb2d12 2928 10/20/2002 20:22:52.720 SEV=8 IKEDBG/0 RPT=9210 KEY_SA_ACTIVE no old rekey centry found with new spi 0x19fb2d12, mess_id 0x0 2929 10/20/2002 20:22:56.530 SEV=9 IPSECDBG/18 RPT=830 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2930 10/20/2002 20:22:56.530 SEV=9 IPSECDBG/18 RPT=831 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2931 10/20/2002 20:22:58.300 SEV=8 IKEDECODE/0 RPT=8192 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3 Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : d4a0ec25 Length : 76 2938 10/20/2002 20:22:58.300 SEV=8 IKEDBG/0 RPT=9211 171.69.89.78 RECEIVED Message (msgid=d4a0ec25) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 2940 10/20/2002 20:22:58.300 SEV=9 IKEDBG/0 RPT=9212 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 2941 10/20/2002 20:22:58.300 SEV=9 IKEDBG/0 RPT=9213 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 2942 10/20/2002 20:22:58.300 SEV=8 IKEDECODE/0 RPT=8193 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 28 2948 10/20/2002 20:22:58.300 SEV=9 IKEDBG/41 RPT=336 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received keep-alive of type Altiga keep-alive, not the negotiated type 2950 10/20/2002 20:22:58.310 SEV=8 IKEDECODE/0 RPT=8194 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3 Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : d196c721 Length : 84 2957 10/20/2002 20:22:58.310 SEV=8 IKEDBG/0 RPT=9214 171.69.89.78 RECEIVED Message (msgid=d196c721) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80 2959 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9215 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 2960 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9216 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 2961 10/20/2002 20:22:58.310 SEV=8 IKEDECODE/0 RPT=8195 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : DPD R-U-THERE (36136) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 32 2967 10/20/2002 20:22:58.310 SEV=9 IKEDBG/36 RPT=92 171.69.89.78 Group [ciscovpn] User [vpnclient1] Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x2d932552) 2969 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9217 171.69.89.78 Group [ciscovpn] User [vpnclient1] constructing blank hash 2970 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9218 171.69.89.78 Group [ciscovpn] User [vpnclient1] constructing qm hash 2971 10/20/2002 20:22:58.310 SEV=8 IKEDBG/0 RPT=9219 171.69.89.78 SENDING Message (msgid=d678099) with payloads : HDR + HASH (8) + NOTIFY (11) total length : 80 2973 10/20/2002 20:23:02.400 SEV=8 IKEDECODE/0 RPT=8196 171.69.89.78

ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47 Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : 317b646a Length : 76 2980 10/20/2002 20:23:02.400 SEV=8 IKEDBG/0 RPT=9220 171.69.89.78 RECEIVED Message (msgid=317b646a) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 2982 10/20/2002 20:23:02.400 SEV=9 IKEDBG/0 RPT=9221 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 2983 10/20/2002 20:23:02.400 SEV=9 IKEDBG/0 RPT=9222 171.69.89.78 Group [ciscovpn] User [vpnclient2] Processing Notify payload 2984 10/20/2002 20:23:02.400 SEV=8 IKEDECODE/0 RPT=8197 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A Length : 28 2990 10/20/2002 20:23:02.400 SEV=9 IKEDBG/41 RPT=337 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received keep-alive of type Altiga keep-alive, not the negotiated type 2992 10/20/2002 20:23:02.410 SEV=9 IPSECDBG/17 RPT=670 Received an IPSEC-over-NAT-T NAT keepalive packet 2993 10/20/2002 20:23:05.530 SEV=9 IPSECDBG/18 RPT=832 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2994 10/20/2002 20:23:05.530 SEV=9 IPSECDBG/18 RPT=833 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2995 10/20/2002 20:23:08.310 SEV=9 IPSECDBG/17 RPT=671 Received an IPSEC-over-NAT-T NAT keepalive packet 2996 10/20/2002 20:23:12.420 SEV=9 IPSECDBG/17 RPT=672 Received an IPSEC-over-NAT-T NAT keepalive packet 2997 10/20/2002 20:23:14.530 SEV=9 IPSECDBG/18 RPT=834 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2998 10/20/2002 20:23:14.530 SEV=9 IPSECDBG/18 RPT=835 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2999 10/20/2002 20:23:18.330 SEV=8 IKEDECODE/0 RPT=8198 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3 Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : f6457474 Length : 76 3006 10/20/2002 20:23:18.330 SEV=8 IKEDBG/0 RPT=9223 171.69.89.78 RECEIVED Message (msgid=f6457474) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3008 10/20/2002 20:23:18.330 SEV=9 IKEDBG/0 RPT=9224 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 3009 10/20/2002 20:23:18.330 SEV=9 IKEDBG/0 RPT=9225 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 3010 10/20/2002 20:23:18.330 SEV=8 IKEDECODE/0 RPT=8199 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 28 3016 10/20/2002 20:23:18.330 SEV=9 IKEDBG/41 RPT=338 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received keep-alive of type Altiga keep-alive, not the negotiated type 3018 10/20/2002 20:23:18.330 SEV=9 IPSECDBG/17 RPT=673 Received an IPSEC-over-NAT-T NAT keepalive packet 3019 10/20/2002 20:23:22.430 SEV=8 IKEDECODE/0 RPT=8200 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47 Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : 358ae39e Length : 76 3026 10/20/2002 20:23:22.430 SEV=8 IKEDBG/0 RPT=9226 171.69.89.78 RECEIVED Message (msgid=358ae39e) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3028 10/20/2002 20:23:22.430 SEV=9 IKEDBG/0 RPT=9227 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 3029 10/20/2002 20:23:22.430 SEV=9 IKEDBG/0 RPT=9228 171.69.89.78 Group [ciscovpn] User [vpnclient2] Processing Notify payload 3030 10/20/2002 20:23:22.430 SEV=8 IKEDECODE/0 RPT=8201 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A Length : 28 3036 10/20/2002 20:23:22.430 SEV=9 IKEDBG/41 RPT=339 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received keep-alive of type Altiga keep-alive, not the negotiated type 3038 10/20/2002 20:23:22.430 SEV=9 IPSECDBG/17 RPT=674 Received an IPSEC-over-NAT-T NAT keepalive packet 3039 10/20/2002 20:23:23.530 SEV=9 IPSECDBG/18 RPT=836 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3040 10/20/2002 20:23:23.530 SEV=9 IPSECDBG/18 RPT=837 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3041 10/20/2002 20:23:28.340 SEV=9 IPSECDBG/17 RPT=675 Received an IPSEC-over-NAT-T NAT keepalive packet 3042 10/20/2002 20:23:32.440 SEV=9 IPSECDBG/17 RPT=676 Received an IPSEC-over-NAT-T NAT keepalive packet 3043 10/20/2002 20:23:32.530 SEV=9 IPSECDBG/18 RPT=838 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3044 10/20/2002 20:23:32.530 SEV=9 IPSECDBG/18 RPT=839 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3045 10/20/2002 20:23:38.360 SEV=8 IKEDECODE/0 RPT=8202 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3 Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : fa8597e6 Length : 76 3052 10/20/2002 20:23:38.360 SEV=8 IKEDBG/0 RPT=9229 171.69.89.78 RECEIVED Message (msgid=fa8597e6) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3054 10/20/2002 20:23:38.360 SEV=9 IKEDBG/0 RPT=9230 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 3055 10/20/2002 20:23:38.360 SEV=9 IKEDBG/0 RPT=9231 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 3056 10/20/2002 20:23:38.360 SEV=8 IKEDECODE/0 RPT=8203 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 28 3062

```
10/20/2002 20:23:38.360 SEV=9 IKEDBG/41 RPT=340 171.69.89.78 Group [ciscovpn] User [vpnclient1]
Received keep-alive of type Altiga keep-alive, not the negotiated type 3064 10/20/2002
20:23:38.360 SEV=9 IPSECDBG/17 RPT=677 Received an IPSEC-over-NAT-T NAT keepalive packet 3065
10/20/2002 20:23:41.530 SEV=9 IPSECDBG/18 RPT=840 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive
packet: success 3066 10/20/2002 20:23:41.530 SEV=9 IPSECDBG/18 RPT=841 171.69.89.78 Xmit IPSEC-
over-UDP NAT keepalive packet: success 3067 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8204
171.69.89.78 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A Next Payload : HASH (8) Exchange Type : Oakley
Informational Flags : 1 (ENCRYPT ) 3073 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8204
171.69.89.78 Message ID : c892dd4c Length : 76 RECEIVED Message (msgid=c892dd4c) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3076 10/20/2002 20:23:42.470 SEV=9
IKEDBG/0 RPT=9233 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 3077
10/20/2002 20:23:42.470 SEV=9 IKEDBG/0 RPT=9234 171.69.89.78 Group [ciscovpn] User [vpnclient2]
Processing Notify payload 3078 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8205 171.69.89.78
Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive
(40500) Spi : C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A Length : 28 3084 10/20/2002
20:23:42.470 SEV=9 IKEDBG/41 RPT=341 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received
keep-alive of type Altiga keep-alive, not the negotiated type 3086 10/20/2002 20:23:42.470 SEV=9
IPSECDBG/17 RPT=678 Received an IPSEC-over-NAT-T NAT keepalive packet 3087 10/20/2002
20:23:48.370 SEV=9 IPSECDBG/17 RPT=679 Received an IPSEC-over-NAT-T NAT keepalive packet 3088
10/20/2002 20:23:50.530 SEV=9 IPSECDBG/18 RPT=842 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive
packet: success 3089 10/20/2002 20:23:50.530 SEV=9 IPSECDBG/18 RPT=843 171.69.89.78 Xmit IPSEC-
over-UDP NAT keepalive packet: success 3090 10/20/2002 20:23:52.470 SEV=9 IPSECDBG/17 RPT=680
Received an IPSEC-over-NAT-T NAT keepalive packet 3091 10/20/2002 20:23:58.380 SEV=8 IKEDECODE/0
RPT=8206 171.69.89.78 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): B6 92 24 F4 96 0A 2D
9E Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3 Next Payload : HASH (8) Exchange Type : Oakley
Informational Flags : 1 (ENCRYPT ) Message ID : 943c7d99 Length : 76 3098 10/20/2002
20:23:58.390 SEV=8 IKEDBG/0 RPT=9235 171.69.89.78 RECEIVED Message (msgid=943c7d99) with
payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3100 10/20/2002
20:23:58.390 SEV=9 IKEDBG/0 RPT=9236 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing
hash 3101 10/20/2002 20:23:58.390 SEV=9 IKEDBG/0 RPT=9237 171.69.89.78 Group [ciscovpn] User
[vpnclient1] Processing Notify payload 3102 10/20/2002 20:23:58.390 SEV=8 IKEDECODE/0 RPT=8207
171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga
keep-alive (40500) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 28 3108
10/20/2002 20:23:58.390 SEV=9 IKEDBG/41 RPT=342 171.69.89.78 Group [ciscovpn] User [vpnclient1]
Received keep-alive of type Altiga keep-alive, not the negotiated type 3110 10/20/2002
20:23:58.390 SEV=9 IPSECDBG/17 RPT=681 Received an IPSEC-over-NAT-T NAT keepalive packet 3111
10/20/2002 20:23:59.530 SEV=9 IPSECDBG/18 RPT=844 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive
packet: success 3112 10/20/2002 20:23:59.530 SEV=9 IPSECDBG/18 RPT=845 171.69.89.78 Xmit IPSEC-
over-UDP NAT keepalive packet: success
```

Troubleshooting Adicional

O NAT-T encapsula o tráfego IPSec nos datagramas UDP, utilizando a porta 4500. Se o NAT-T não está verificado no concentrador VPN ou se a transparência de NAT não está verificada no cliente VPN, o túnel de IPsec está estabelecido; contudo, você não pode passar nenhuns dados. Para que o NAT-T funcione, você deve ter o NAT-T selecionado no concentrador e o NAT Transparency (sobre UDP) selecionado no cliente.

O exemplo abaixo mostra um tipo de caso no qual NAT-T não foi verificado no concentrador. No cliente, o tunelamento transparente foi verificado. Nesse caso, o túnel IPSec está estabelecido entre o cliente e o concentrador. Porém, como as negociações de porta de túnel IPSec falharam, nenhum dado passa entre o cliente e o concentrador. Dessa forma, os bytes transmitidos e recebidos são zero para as sessões de acesso remoto.

O exemplo a seguir mostra as estatísticas do VPN Client. Observe que a porta de túnel negociada é 0. Há uma tentativa de executar o ping de 192.168.2.251 (interface privada do VPN 3000 Concentrator) e de 172.16.172.50 a partir de um prompt do DOS. Entretanto, estes pings estão falhando, porque não foi negociada nenhuma porta de túnel, e, portanto, os dados de IPSec estão sendo descartados no servidor VPN remoto.

O exemplo abaixo mostra que o cliente VPN está enviando dados criptografados (13 pacotes). Mas o número de pacotes decifrados é zero para o servidor VPN remoto e ele não retornou nenhum dado codificado. Como nenhuma porta de túnel foi negociada, o servidor VPN remoto descarta os pacotes e não envia nenhum dado de resposta.

Informações Relacionadas

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