

# Configurar un túnel IPsec entre un Cisco VPN 3000 Concentrator y NG de punto de control un Firewall

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configurar el concentrador VPN 3000](#)

[Configure NG de punto de control](#)

[Verificación](#)

[Verifique la comunicación de la red](#)

[Vea el estado del túnel en NG de punto de control](#)

[Vea el estado del túnel en el concentrador VPN](#)

[Troubleshooting](#)

[Resumen de la red](#)

[Depuración del punto de control NG](#)

[Depuración del concentrador de VPN](#)

[Información Relacionada](#)

## Introducción

Este documento muestra cómo configurar un túnel IPsec con claves previamente compartidas para comunicarse entre dos redes privadas. En este ejemplo, las redes de comunicación son la red privada 192.168.10.x dentro del Cisco VPN 3000 Concentrator y la red privada 10.32.x.x dentro del Firewall de la última generación del punto de verificación (NG).

## prerrequisitos

### Requisitos

- Tráfico por dentro del concentrador VPN y del interior NG de punto de control a Internet — representado aquí por las redes 172.18.124.x — debe fluir antes de comenzar esta configuración.
- Los usuarios deben ser familiares con el IPSec Negotiation. Este proceso se puede analizar

en cinco pasos, incluyendo dos fases del Internet Key Exchange (IKE). Un túnel IPsec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPsec. En la Fase 1 IKE, las entidades pares IPsec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que autentican a los pares, un túnel seguro se crea con el Internet Security Association and Key Management Protocol (ISAKMP). En la fase 2 IKE, los pares IPsec utilizan el túnel seguro y autenticado para negociar IPsec SA transforman. La negociación de la política compartida determina el modo en que se establece el túnel IPsec. Se crea el túnel IPsec, y los datos se transfieren entre los pares IPsec basados en los parámetros de IPsec configurados en el IPsec transforman los conjuntos. El túnel IPsec termina cuando los IPsec SAs son borrados o cuando caduca su vigencia.

## Componentes Utilizados

Esta configuración fue desarrollada y probada con estas versiones de software y hardware:

- Concentrador VPN de la serie 3000 3.5.2
- NG de punto de control Firewall

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:

**Nota:** El esquema de IP Addressing usado en esta configuración no es legalmente routable en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

## Configuraciones

### Configurar el concentrador VPN 3000

Complete estos pasos para configurar el concentrador VPN 3000:

1. Vaya al **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPsec LAN-to-LAN (IPsec de LAN a LAN)** para configurar a la sesión LAN a LAN. Fije las opciones para autenticación y los algoritmos IKE, clave previamente compartida, IP Address de Peer, y los parámetros de red local y remota. Haga clic en Apply (Aplicar). En esta configuración, la autenticación fue fijada mientras que el ESP-MD5-HMAC y el cifrado fueron fijados como 3DES.
2. Vaya al **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPsec > IKE Proposals (Propuestas IKE)** y fije los parámetros obligatorios. Seleccione la propuesta IKE IKE-3DES-MD5 y verifique los parámetros seleccionados para la oferta. El tecleo **se aplica** para configurar a la sesión LAN a LAN. Éstos

son los parámetros para esta configuración:

3. Vaya al **Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Administración de tráfico) > Security Associations (Asociaciones de seguridad)**, seleccione IPsec SA creado para la sesión, y verifique los parámetros IPsec SA elegidos para la sesión LAN a LAN. En esta configuración el nombre de la sesión LAN a LAN era "punto de verificación," así que IPsec SA fue creado automáticamente como "L2L: Punto de verificación." Éstos son los parámetros para este SA:

## [Configure NG de punto de control](#)

Los objetos de red y las reglas se definen en NG de punto de control para componer la directiva que pertenece a la configuración VPN que se configurará. Esta directiva entonces está instalada con NG de punto de control el editor de políticas para completar NG de punto de control el lateral de la configuración.

1. Cree los dos objetos de red para NG de punto de control la red y la red del concentrador VPN que cifrarán el tráfico interesante. Para crear los objetos, seleccione **Manage > Network Objects**, después seleccione **New > Network**. Ingrese la información de red apropiada, después haga clic la **AUTORIZACIÓN**. Estos ejemplos muestran la configuración de los objetos de red llamados CP\_inside (la red interna del NG de punto de control) y el CONC\_INSIDE (la red interna del concentrador VPN).
2. Vaya a **Manage > Network Objects** y seleccionando **New > Workstation** para crear los objetos de estación de trabajo para los dispositivos VPN, NG de punto de control y el concentrador VPN. **Nota:** Usted puede utilizar NG de punto de control el objeto de estación de trabajo creado durante la configuración del punto de control inicial NG. Seleccione las opciones para fijar el puesto de trabajo como el gateway y dispositivo VPN interoperable, después haga clic la **AUTORIZACIÓN**. Estos ejemplos muestran la configuración de los objetos llamados cisco cp (NG de punto de control) y CISCO\_CONC (concentrador VPN 3000):
3. Vaya a **Manage > Network Objects > Edit** para abrir la ventana de Propiedades de la estación de trabajo para NG de punto de control el puesto de trabajo (cisco cp en este ejemplo). Seleccione la **topología de las** opciones en el lado izquierdo de la ventana, después seleccione la red para ser cifrado. El tecleo **edita** para fijar las propiedades de la interfaz. En este ejemplo, el CP\_inside es la red interna del NG de punto de control.
4. En la ventana de pPropiedades de la interfaz, seleccione la opción para señalar el puesto de trabajo como interno, después especifique la dirección IP apropiada. Haga clic en OK. Las selecciones de topología mostradas señalan el puesto de trabajo como interno y especifican los IP Addresses detrás de la interfaz del CP\_inside:
5. De la ventana de Propiedades de la estación de trabajo, seleccione la interfaz exterior en NG de punto de control eso lleva hacia fuera a Internet, después hace clic **editan** para fijar las propiedades de la interfaz. Seleccione la opción para señalar la topología como externo, después haga clic la **AUTORIZACIÓN**.
6. De la ventana de Propiedades de la estación de trabajo en NG de punto de control, el **VPN** selecto de las opciones en el lado izquierdo de la ventana, entonces selección los parámetros IKE para encriptación y algoritmos de autenticación. El tecleo **edita** para configurar las propiedades IKE.
7. Fije las propiedades IKE para hacer juego las propiedades en el concentrador VPN. En este ejemplo, seleccione la opción de encriptación para el **3DES** y la opción del picado para el

## MD5.

8. Seleccione la opción de autenticación para los **Secretos previamente compartidos**, después haga clic **editan los secretos** para fijar la clave previamente compartida para ser compatible con la clave previamente compartida en el concentrador VPN. El tecleo **edita** para ingresar su clave como se muestra, después hace clic el **conjunto, AUTORIZACIÓN**.
9. De la ventana de las propiedades IKE, haga clic **avanzado...** y cambie estas configuraciones: No reelija como candidato la opción para **Support aggressive mode (Admitir modo agresivo)**. Seleccione la opción para el **intercambio de claves del soporte para las subredes**. Cuando le acaban, **AUTORIZACIÓN** del tecleo, **AUTORIZACIÓN**.
10. Vaya a **Manage > Network Objects > Edit** para abrir la ventana de Propiedades de la estación de trabajo para el concentrador VPN. **Topología** selecta de las opciones en el lado izquierdo de la ventana para definir manualmente el dominio VPN. En este ejemplo, el CONC\_INSIDE (la red interna del concentrador VPN) se define como el dominio VPN.
11. **El VPN** selecto de las opciones en el lado izquierdo de la ventana, entonces selecciona el **IKE** como el esquema de encriptación. El tecleo **edita** para configurar las propiedades IKE.
12. Fije las propiedades IKE para reflejar la configuración actual en el concentrador VPN. En este ejemplo, fije la opción de encriptación para el **3DES** y la opción del picado para el **MD5**.
13. Seleccione la opción de autenticación para los **Secretos previamente compartidos**, después haga clic **editan los secretos** para fijar la clave previamente compartida. El tecleo **edita** para ingresar su clave como se muestra, después hace clic el **conjunto, AUTORIZACIÓN**.
14. De la ventana de las propiedades IKE, haga clic **avanzado...** y cambie estas configuraciones: Seleccione al grupo Diffie-Hellman apropiado para las propiedades IKE. No reelija como candidato la opción para **Support aggressive mode (Admitir modo agresivo)**. Seleccione la opción para el **intercambio de claves del soporte para las subredes**. Cuando le acaban, **AUTORIZACIÓN** del tecleo, **AUTORIZACIÓN**.
15. Seleccione el **Rules (Reglas) > Add Rules (Agregar reglas) > Top (Superiores)** para configurar las reglas de encriptación para la directiva. En la ventana de editor de políticas, inserte una regla con la fuente como el CP\_inside (red interna del NG de punto de control) y destino como CONC\_INSIDE (red interna del concentrador VPN). Los valores establecidos para el **servicio = ningunos**, **acción = cifran**, y **pista = registro**. Cuando usted ha agregado la sección de la acción del cifrar de la regla, haga clic con el botón derecho del ratón la **acción** y selecciónela **Edit Properties**.
16. Seleccione el **IKE** y el tecleo **editan**.
17. En la ventana de las propiedades IKE, cambie las propiedades para estar de acuerdo con el concentrador VPN transforman. Fije la opción de la transformación al **Encryption + Data Integrity (ESP)**. Fije el algoritmo de encriptación al **3DES**. Fije la integridad de los datos al **MD5**. Fije el gateway de peer permitido para hacer juego el concentrador VPN (CISCO\_CONC). Cuando haya finalizado, haga clic en **OK (Aceptar)**.
18. Después de que NG de punto de control se configure, salve la directiva y la **directiva** selecta **> instala** para habilitarla. La ventana de instalación visualiza las notas de progreso mientras que se compila la directiva. Cuando la ventana de instalación indica que la instalación de regulación es completa, tecleo **cercano** para acabar el procedimiento.

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

## [Verifique la comunicación de la red](#)

Para probar la comunicación entre las dos redes privadas, usted puede iniciar un ping a partir de la una de las redes privadas a la otra red privada. En esta configuración, un ping fue enviado NG de punto de control del lateral (10.32.50.51) a la red del concentrador VPN (192.168.10.2).

## [Estado del túnel de la visión en NG de punto de control](#)

Para ver el estado del túnel, vaya al editor de políticas y seleccione el **Window (Ventana) > Sytem Status (Estado del sistema)**.

## [Vea el estado del túnel en el concentrador VPN](#)

Para verificar el estado del túnel en el concentrador VPN, vaya al **Administration (Administración) > Administer sessions (Administrar sesiones)**.

Bajo sesiones LAN a LAN, seleccione el nombre de la conexión para el punto de verificación para ver los detalles en los SA creados y el número de paquetes transmitidos/recibidos.

## [Troubleshooting](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

**Nota:** El tráfico no debe ser PATed a través del túnel IPsec usando el IP Address público del concentrador VPN (interfaz exterior). Si no, el túnel falla. Así pues, la dirección IP usada para PATing debe ser un direccionamiento con excepción del direccionamiento configurado en la interfaz exterior.

## [Resumen de la red](#)

Cuando el múltiplo adyacente, las redes internas se configura en el dominio del cifrado en el punto de verificación, el dispositivo puede resumir automáticamente las redes con respecto al tráfico interesante. Si el concentrador VPN no se configura para hacer juego, el túnel es probable fallar. Por ejemplo, si las redes internas de 10.0.0.0 /24 y de 10.0.1.0 /24 se configuran para ser incluidas en el túnel, estas redes se pueden resumir a 10.0.0.0 /23.

## [Depuración del punto de control NG](#)

Para ver los registros, seleccione el **Window (Ventana) > Log Viewer (Visor de registro)**.

## [Depuración del concentrador de VPN](#)

Para habilitar los debugs en el concentrador VPN, vaya al **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases)**. Permita al AUTH, al AUTHDBG, al IKE, al IKEDBG, al IPSEC, y al IPSECDBG para que la gravedad registre como 1 - 13. Para ver los debugs, seleccione el **Monitoring (Monitoreo) > Filterable Event Log (Registro de eventos filtrables)**.

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157  
RECEIVED Message (msgid=0) with payloads :  
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157  
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157  
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157  
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157  
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

**25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3** 26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514  
172.18.124.157 constructing ISA\_SA for isakmp 27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515  
172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total  
length : 84 29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 RECEIVED Message  
(msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 31  
09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with  
payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002  
20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002  
20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA\_KE 35 09/11/2002 20:36:03.630  
SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9  
IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9  
IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9  
IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660  
SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002  
20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send IOS VID 41 09/11/2002 20:36:03.660 SEV=9  
IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version:  
1.0.0, capabilities: 20000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157  
constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send  
Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys

for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157] Starting group lookup for peer 172.18.124.157 54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10 AUTH\_Open() returns 9 55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9 56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH\_PutAttrTable(9, 748174) 57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH\_GroupAuthenticate(9, 2f1b19c, 49c648) 58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH\_BindServer(51a6b48, 0, 0) 59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH\_CreateTimer(51a6b48, 0, 0) 61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018 62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH\_BuildMsg(51a6b48, 0, 0) 63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH\_StartTimer(51a6b48, 0, 0) 64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 30000 65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH\_SndRequest(51a6b48, 0, 0) 66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB\_Decode(3825300, 156) 67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB\_Xmt(51a6b48) 68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 xmit\_cnt = 1 69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB\_Xmt(51a6b48) 70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB\_Match(51a6b48, 3eb7ab0) 71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH\_RcvReply(51a6b48, 0, 0) 72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB\_Decode(3eb7ab0, 298) 73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB\_Rcv(51a6b48) 74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10 AUTH\_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH\_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.157 78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH\_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH\_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 **90** **09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED** 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None 92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157 Keep-alives configured on but peer does not support keep-alives (type = None) 93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH\_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH\_Int\_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157]  
Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group  
[172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask  
255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM  
IsRekeyed old sa not found by addr **114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157**  
**Group [172.18.124.157] IKE Remote Peer configured for SA: L2L: Checkpoint** 115 09/11/2002  
20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157] processing IPSEC SA  
**116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPsec SA**  
**Proposal # 1, Transform # 1 acceptable** 117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536  
172.18.124.157 Group [172.18.124.157] IKE: requesting SPI! 118 09/11/2002 20:36:03.790 SEV=9  
IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 10,  
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 17248580, lifetime2 0, dsId 300 122 09/11/2002  
20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY\_GETSPI msg! 123 09/11/2002 20:36:03.790  
SEV=7 IPSECDBG/13 RPT=10 Reserved SPI 305440147 124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6  
RPT=10 IKE got SPI from key engine: SPI = 0x1234a593 125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0  
RPT=537 172.18.124.157 Group [172.18.124.157] oakley constructing quick mode 126 09/11/2002  
20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank  
hash 127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157]  
constructing ISA\_SA for ipsec 128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157  
Group [172.18.124.157] constructing ipsec nonce payload 129 09/11/2002 20:36:03.800 SEV=9  
IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID **130 09/11/2002**  
**20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id:**  
**Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask**  
**255.255.255.0 Protocol 0 Port 0** 134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541  
172.18.124.157 Group [172.18.124.157] constructing qm hash 135 09/11/2002 20:36:03.800 SEV=8  
IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8)  
+ SA (1) ... total length : 152 137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543  
172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ...  
total length : 48 139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157 Group  
[172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545  
172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9  
IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002  
20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode  
Key! **143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157]**  
**Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0** 146  
**09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security**  
**negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593,**  
**Outbound SPI = 0x0df37959** 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message  
parse - msgtype 1, len 606, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label  
0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0,  
lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140  
Processing KEY\_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141  
key\_msghdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter  
configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157  
09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA 158  
09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,  
dst 10.32.0.0 mask 0.0.127.255 159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146  
KeyProcessAdd: FilterIpsecAddIkeSa success 160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41  
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000, seq 0, err 0, type 2, mode  
1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg  
3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 164 09/11/2002 20:36:03.810 SEV=9  
IPSECDBG/1 RPT=147 Processing KEY\_UPDATE msg! 165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1  
RPT=148 Update inbound SA addresses 166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149  
key\_msghdr2secassoc(): Enter 167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter  
configured 168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter 169  
09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success 170 09/11/2002  
20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY\_ADD msg for SA: SPI = 0x0df37959 171 09/11/2002  
20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY\_UPDATE, spi 0x1234a593 **172 09/11/2002**  
**20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED**  
(msgid=54796f76)

## [Información Relacionada](#)

- [Página de soporte del concentrador de la serie Cisco VPN 3000](#)
- [Página de soporte al cliente Serie Cisco VPN 3000](#)
- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)