Nways Manager

# Guía del usuario de Nways VPN Manager

GA10-5244-00

Nways Manager

# Guía del usuario de Nways VPN Manager

GA10-5244-00

**Nota**

Antes de utilizar esta información y el producto al que da soporte,
asegúrese de leer la información general del Apéndice A, “Avisos” en la página 69.

**Primera edición (mayo 1999)**

Esta edición es aplicable a IBM Nways VPN Manager.

Solicite las publicaciones a través de un representante de IBM o la sucursal de IBM de su localidad. En la dirección que figura más abajo no hay existencias de publicaciones.

Al final de esta publicación se proporciona un formulario para los comentarios del lector. Si faltara dicha hoja, puede dirigir sus comentarios a:

IBM, S.A.
National Language Solutions Center
Avda Diagonal 571
08029
Barcelona
España

# Contenido


**Capítulo 1. Introducción . . . . . 1**
Acerca de VPN Manager . . . . . 1
Soporte de hardware . . . . . 1
Requisitos previos de hardware y software . . . . 1

**Capítulo 2. Introducción a las VPN . . . 3**
Tunelización Layer-2 . . . . . 3
Terminología . . . . . 3
Tunelización obligatoria . . . . . 3
Tunelización voluntaria . . . . . 3
Protocolos de tunelización Layer-2 . . . . . 4
Posibilidades de la tunelización Layer-2 . . . . 4
Tunelización IPSec . . . . . 5
Terminología . . . . . 5
Tunelización de extremo a extremo . . . . . 6
Tunelización de pasarela a pasarela . . . . . 6
Gestión de claves . . . . . 6
Gestión de datos . . . . . 6
Posibilidades de la tunelización IPSec . . . . . 7
Políticas . . . . . 7
Relaciones entre los componentes de la política 7
LDAP . . . . . 8
Interacciones entre dispositivos . . . . . 9

**Capítulo 3. Utilización de VPN List Manager . . . . . 11**
Acerca de VPN List . . . . . 11
Acerca del panel de información de VPN List Manager . . . . . 11
Prioridades de las acciones de control . . . . . 12
Información . . . . . 12
Valores del archivo de anotaciones cronológicas 12
Restaurar lista . . . . . 13
Contraseña . . . . . 14
Cambiar contraseña . . . . . 14
Acerca del panel Lista de dispositivos de VPN . . 14
Dispositivos . . . . . 14
Detalles . . . . . 15
Imprimir . . . . . 16

**Capítulo 4. VPN Monitor . . . . . 17**
Ventana VPN Monitor . . . . . 17
Panel Árbol de navegación . . . . . 17
Panel de información . . . . . 18
Área de mensajes . . . . . 18
Funciones de VPN Monitor . . . . . 18
Supervisión . . . . . 18
Notificación de sucesos . . . . . 18
Control operativo . . . . . 18
Resolución de problemas . . . . . 19
Arranque de aplicaciones . . . . . 19

**Capítulo 5. Carpeta general de VPN Monitor . . . . . 21**
Identificación . . . . . 21
Administración . . . . . 21

**Capítulo 6. Carpeta Estado global de VPN Monitor . . . . . 23**
Resumen . . . . . 23
Niveles . . . . . 23
Túneles . . . . . 23
Clientes . . . . . 23
Política . . . . . 23
Sucesos . . . . . 24

**Capítulo 7. Carpeta Túneles de VPN Monitor . . . . . 25**
Carpeta Túneles Layer-2 . . . . . 25
Carpeta Activa . . . . . 25
Carpeta Túneles anteriores . . . . . 27
Carpeta Túneles IPSec . . . . . 28
Carpeta Túneles activos . . . . . 28

**Capítulo 8. Carpeta Clientes de VPN Monitor . . . . . 37**
Carpeta Sesiones Layer-2 . . . . . 37
Carpeta Sesiones activas . . . . . 37

**Capítulo 9. Carpeta Calidad de servicio de VPN Monitor . . . . . 41**
Carpeta RSVP . . . . . 41
Panel Sesiones . . . . . 41
Panel Mensajes PATH del emisor . . . . . 41
Panel Mensajes RESV en sentido inverso . . . . 43

**Capítulo 10. Carpeta Políticas de VPN Monitor . . . . . 45**
Carpeta Dispositivo . . . . . 45
Carpeta Condiciones . . . . . 45

**Capítulo 11. Carpeta Sucesos de VPN Monitor . . . . . 55**
Carpeta Autentificación de Layer-2 . . . . . 55
Panel Estadísticas . . . . . 55
Panel Anotaciones cronológicas de errores de túnel . . . . . 55
Panel Anotaciones cronológicas de los errores de sesión . . . . . 56
Carpeta Cifrado/Autentificación de IPSec . . . . . 56
Panel Estadísticas . . . . . 56
Panel Anotaciones cronológicas de errores de IPSec . . . . . 56

**Capítulo 12. Carpeta operativa de VPN Monitor . . . . . 59**
Carpeta Túneles . . . . . 59
Panel Tamaño de tablas . . . . . 59
Panel Desactivar túneles Layer-2 . . . . . 59
Panel Desactivar túneles de control IPSec . . . . 60
Panel Desactivar túneles de usuario IPSec . . . 60
Carpeta Clientes . . . . . 60
Panel Desactivar sesiones Layer-2 . . . . . 60
Carpeta Políticas . . . . . 61
Panel Habilitar/Inhabilitar políticas . . . . . 61
Panel Volver a cargar políticas de dispositivos . 61
Carpeta LDAP . . . . . 61
Carpeta Rupturas . . . . . 62

**Capítulo 13. Carpeta Pruebas de VPN Monitor . . . . . 65**
Panel Prueba de política . . . . . 65
Carpeta Pruebas de Layer-2 . . . . . 66
Panel Prueba de conexión de Layer-2 . . . . . 66
Panel Prueba del tiempo de respuesta de Layer-2 66
Panel Sondeo remoto . . . . . 67

**Apéndice A. Avisos . . . . . 69**
Marcas registradas . . . . . 70

# Capítulo 1. Introducción

En este capítulo se proporciona una breve descripción de VPN Manager, se enumeran los componentes de hardware de IBM a los que da soporte y se listan los requisitos de hardware y de software para la utilización de VPN Manager.

## Acerca de VPN Manager

Nways VPN Manager proporciona supervisión, notificación de sucesos, resolución de problemas, control operativo y funciones de arranque de aplicaciones para la implantación por parte de IBM de redes privadas virtuales.

## Soporte de hardware

La versión 2.0 de Nways VPN Manager proporciona supervisión y control operativo para las características de VPN implantadas en los siguientes dispositivos:

- Direccionador multiprotocolo IBM 2210 Nways
- Programa de utilidad IBM 2212 Access
- Conector multiacceso IBM 2216 Nways
- Programa de utilidad IBM Network

## Requisitos previos de hardware y software

Nways VPN Manager requiere la versión 2.0 de Nways Element Manager para una de las siguientes plataformas:

- AIX
- HP-UX
- Windows NT

Puesto que los requisitos mínimos de hardware para Nways Element Manager superan a los requisitos para Nways VPN Manager, no hay requisitos de hardware adicionales.

# Capítulo 2. Introducción a las VPN

Una *Red privada virtual* (VPN) proporciona a los usuarios finales un medio para transportar con seguridad información desde una intranet a través de una red IP pública como interred. Una VPN puede estar compuesta de túneles Layer-2, túneles IPSec y políticas. Los túneles Layer-2 proporcionan características de VPN para usuarios de marcación remota. Los túneles IPSec proporcionan posibilidades de VPN para usuarios IP. Las Políticas proporcionan control de acceso para los recursos.

En este capítulo se proporciona una visión general de:

- Tunelización Layer-2
- Tunelización IPSec
- Políticas

## Tunelización Layer-2

Los protocolos de tunelización Layer-2 pueden transportar con seguridad el tráfico privado del protocolo PPP (Point-to-Point Protocol - Protocolo Punto a Punto) a través de una red IP pública. Existen tres protocolos de tunelización Layer-2 que utilizan dos modelos de red. Los tres protocolos de tunelización Layer-2 son L2TP (Layer-2 Tunneling Protocol - Protocolo de Tunelización Layer-2), L2F (Layer-2 Forwarding - Reenvío de Layer-2) y PPTP (Point-to-Point Tunneling Protocol - Protocolo de Tunelización Punto a Punto). Los dos modelos de red son la Tunelización obligatoria y la Tunelización voluntaria.

### Terminología

Un *Servidor de acceso a redes* (NAS) es un dispositivo conectado a una estructura de red conmutada, como una *Red Telefónica Pública Conmutada* (PSTN) o una *Red Digital de Servicios Integrados* (RDSI) y contiene un sistema final PPP (Punto a Punto). Un NAS que es capaz de iniciar un túnel L2TP se conoce como *Concentrador de Acceso a L2TP* (LAC). El NAS es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. Una pasarela es un dispositivo susceptible de terminación PPP que maneja el extremo del servidor de la comunicación. Una pasarela también se conoce como *Servidor de red L2TP* (LNS). La pasarela es el iniciador de las llamadas salientes y el receptor de las llamadas entrantes.

### Tunelización obligatoria

La Tunelización obligatoria permite a los Clientes de marcación que no tienen el software de tunelización habilitado, iniciar una sesión PPP que se encapsula desde el Servidor de acceso a redes (NAS) hasta la Red corporativa. En este modelo, la sesión PPP se encuentra entre el Cliente y la Pasarela y el Túnel se encuentra entre el NAS y la Pasarela.

### Tunelización voluntaria

Por otro lado, la Tunelización voluntaria requiere que los Clientes de marcación estén habilitados para la tunelización. En este modelo, el Cliente se conecta

inicialmente a su suministrador de servicio para obtener acceso a la interred. Una vez establecida la conexión con el suministrador de servicio, el Cliente crea un Túnel Layer-2 hasta la Pasarela y a continuación una Sesión PPP de extremo a extremo a través del Túnel que se acaba de establecer. En este modelo, la Sesión PPP y el Túnel se encuentran entre el Cliente y la Pasarela.

## Protocolos de tunelización Layer-2

La tunelización Layer-2 utiliza los siguientes protocolos:

**L2TP** El Protocolo de tunelización Layer-2, es un protocolo de seguimiento de estándares IETF (Internet Engineering Task Force) que ha evolucionado a partir del protocolo L2F (Layer-2 Forwarding - Reenvío de Layer-2) y el protocolo PPTP (Point-to-Point Tunneling Protocol - Protocolo de Tunelización Punto a Punto). L2TP utiliza el puerto UDP 1701 conocido públicamente para su diálogo inicial de mensajes de control de túnel y tiene la posibilidad de escoger puertos de origen UDP en ambos lados de la conexión. UDP también se utiliza como transporte de paquetes para paquetes PPP tunelizados. L2TP utiliza ambos modelos de red, la Tunelización obligatoria y la Tunelización voluntaria.

**L2F** El Protocolo de Reenvío de Layer-2 es un protocolo de tunelización Layer 2 no basado en estándares implantado originariamente por Cisco Systems. Utiliza el puerto UDP 1701 conocido públicamente (fijo) para la transmisión de túnel y mensajes de control de llamadas y de túnel, así como para el transporte de paquetes PPP tunelizados desde NAS hasta la pasarela. L2F utiliza el modelo de Tunelización obligatoria.

**PPTP** El Protocolo de Tunelización Punto a Punto es otro protocolo de tunelización Layer 2 no basado en estándares implantado originariamente por Microsoft en sus plataformas Windows 95 y Windows NT. PPTP utiliza TCP para abrir estructuras de control de túneles y de sesiones. Después del establecimiento de la sesión, los paquetes PPP se encapsulan utilizando la Encapsulación de direccionamiento genérica (GRE). PPTP utiliza el modelo de red de Tunelización voluntaria.

## Posibilidades de la tunelización Layer-2

Los protocolos de Tunelización Layer-2 pueden proporcionar de manera directa o indirecta autentificación, cifrado y compresión.

Los protocolos de Tunelización Layer-2 pueden proporcionar directamente Autentificación de túneles e indirectamente Autentificación de usuarios. La Autentificación de túneles se realiza entre el NAS y la pasarela. La Autentificación de usuarios se realiza mediante el protocolo básico Punto a Punto.

Los protocolos de Tunelización Layer-2 pueden proporcionar indirectamente Cifrado de datos. Todos los protocolos de Tunelización Layer-2 pueden transportar datos cifrados a nivel de aplicaciones. L2TP se puede utilizar con IPSec, que puede realizar el Cifrado de los datos. PPTP puede utilizar el recurso MPPE (Microsoft Point-to-Point Encryption).

Los protocolos de Tunelización Layer-2 pueden proporcionar indirectamente Compresión de datos. Los protocolos de Tunelización Layer-2 realizan esto mediante la utilización del Protocolo básico Punto a Punto que tiene la capacidad de Compresión de datos.

## Tunelización IPSec

IPSec es un estándar IETF (Internet Engineering Task Force) que define un mecanismo de túnel para transportar con seguridad el tráfico IP a través de una red IP pública. Los túneles IPSec se implantan mediante dos túneles. Existe un túnel de gestión de claves IPSec y un túnel de gestión de datos IPSec. Un Túnel de gestión de claves IPSec se conoce a menudo como Túnel de fase 1 o Túnel IKE (intercambio de claves de Internet) y es un Túnel de control para uno o varios túneles de datos de usuario de fase 2 IPSec. Los Túneles IPSec se suelen implantar en un modelo de red de extremo a extremo o de pasarela a pasarela.

## Terminología

*Autentificación* es la capacidad de saber si los datos recibidos son los mismos que los enviados, así como si el supuesto emisor es de hecho el emisor real. El Método de autentificación de IPSec puede ser una clave compartida previamente y entrada manualmente o una firma digital. Además de la autentificación, las firmas digitales garantizan que el mensaje está asociado exclusivamente con el emisor y que el destinatario no puede falsificarlo. Message Digest 5 (MD5: generación aleatoria de 128 bits) y Secure Hash Algorithm (SHA: generación aleatoria de 160 bits) son los utilizados comúnmente en el modelo de autentificación de Túneles IPSec.

*Integridad* es la propiedad de garantizar la transmisión de los datos desde el origen hasta el destino sin alteración no detectada. Hashed Message Authentication Code Message Digest 5 (HMAC-MD5: generación aleatoria de 2x128 bits) y Hashed Message Authentication Code Message Secure Hash Algorithm (HMAC-SHA: generación aleatoria de 2x160) son los que se utilizan comúnmente en el modelo de integridad de IPSec.

*Confidencialidad* es la propiedad de comunicarse de modo que los destinatarios previstos saben qué se ha enviado pero las personas no autorizadas no pueden determinar qué se ha enviado. IPSec utiliza la Encapsulación y el Cifrado para garantizar la Confidencialidad. El paquete de datos IP original está encapsulado en un paquete de datos IPSec. La Carga útil y la Cabecera IP originales están encapsuladas en Modalidad de túnel, que es la que suelen utilizar las puertas de acceso. En cambio, sólo la Carga original está encapsulada en la Modalidad de transporte, que utilizan habitualmente los sistemas principales. El Cifrado de datos estándar (DES - cifrado de 56 bits), Cifrado de datos triple estándar (DES-3 - cifrado de 3x56 bits) y el Recurso de máscara de datos comerciales (CMDF - cifrado de 40 bits) se suelen utilizar en el modelo de cifrado de IPSec.

Una *Asociación de seguridad* (SA) es una relación entre un conjunto determinado de conexiones de red que establece un conjunto de información de seguridad compartida. Las Asociaciones de seguridad se negocian basándose en claves secretas, algoritmos criptográficos, algoritmos de autentificación y modalidades de encapsulación. IKE utiliza el protocolo de acuerdo de claves Diffie-Hellman (Grupo-1: claves de 768 bits, Grupo-2: claves de 1024 bits) para generar un Secreto compartido, es decir, una clave, entre las dos entidades IPSec. Debe observarse que IKE se conocía anteriormente como ISAKMP / Oakley (Asociación de Seguridad de Internet y protocolo de Gestión de claves / Protocolo Oakley). La duración de una SA se especifica mediante una duración en segundos o una duración en Kbytes.

## Tunelización de extremo a extremo

La Tunelización de extremo a extremo IPSec permite a un Sistema principal IP de un extremo de la red comunicarse con seguridad con un sistema principal IP del otro extremo de la red. Este modelo es similar a un modelo de sistemas homólogos (de igual a igual) específico y requiere que los sistemas principales IP estén habilitados para IPSec. El Túnel IPSec está formado por un Túnel de gestión de claves y un Túnel de gestión de datos entre los dos sistemas principales IP.

## Tunelización de pasarela a pasarela

La Tunelización de pasarela a pasarela permite que uno o varios sistemas principales IP de un extremo de la red se comuniquen con seguridad con uno o varios sistemas principales del otro extremo de la red. Este modelo es similar a un modelo de sistemas heterogéneos, en el que las puertas de acceso deben estar habilitadas para IPSec pero ninguno de los sistemas principales IP necesita estar habilitado para IPSec. El túnel IPSec está formado por un Túnel de gestión de claves y uno o varios Túneles de gestión de datos entre las dos puertas de acceso. Las Puertas de acceso se conectan a través de su Interfaz pública y protegen a una o varias Interfaces privadas que hay tras ellas. Una interfaz privada puede ser una Subred IP, un rango de direcciones IP o una dirección IP individual.

## Gestión de claves

Un Túnel de gestión de claves IPSec se conoce a menudo como túnel IKE (Intercambio de Claves de Internet) o Túnel IPSec de fase 1 y es un túnel de control para uno o varios túneles de datos de usuarios IPSec de fase 2. El Túnel de gestión de claves IPSec se negocia en la Modalidad principal, que utiliza un intercambio de seis mensajes o en la Modalidad agresiva, que utiliza un intercambio de tres mensajes. La negociación implica la autentificación de las entidades, el establecimiento de un Secreto compartido y el establecimiento de parámetros para la Asociación de seguridad. Después de la conclusión satisfactoria de la negociación, el Túnel de gestión de claves IPSec utiliza una única Asociación de seguridad (SA) bidireccional para la comunicación. A lo largo de la duración de un determinado Túnel de gestión de claves IPSec, la SA puede caducar y crearse una nueva.

## Gestión de datos

Un Túnel de gestión de datos IPSec se conoce a menudo como Túnel de datos de usuario de fase 2 IPSec o Túnel IPSec y se utiliza para transportar con seguridad el tráfico IP. El Túnel de gestión de datos IPSec se negocia en la Modalidad rápida, que utiliza un intercambio de tres mensajes. La negociación implica el intercambio de identidades, la decisión de si se aplicará o no una nueva Prevención de repetición, la generación de una clave si es necesario el Secreto perfecto de reenvío, el acuerdo sobre el manejo futuro de No copiar bit de fragmento y el establecimiento de parámetros para la Asociación de seguridad. Los parámetros de seguridad pueden constar de los atributos de proceso AH (Cabecera de autentificación) y/o ESP (Carga de seguridad encapsulada). Mientras que tanto AH como ESP proporcionan la integridad de los paquetes y la autentificación del origen de datos, sólo ESP proporciona cifrado. Los Túneles de gestión de datos IPSec utilizan una o varias SA de entrada y una o varias SA de salida. A lo largo de la duración de un determinado Túnel de gestión de datos IPSec, las SA pueden expirar y crearse otras nuevas. Durante este período de transición, hay realmente

dos SA (una con un estado de ACTUAL y otra con un estado CADUCANDO) para cada SA de entrada original.

### Posibilidades de la tunelización IPSec

La tunelización IPSec puede proporcionar directamente autentificación, cifrado y control de integridad.

La autentificación se realiza para cada un túnel y opcionalmente para cada paquete. En IKE, la autentificación del túnel entre sistemas homólogos se realiza mediante una clave compartida previamente o una firma digital.

La autentificación de paquetes se realiza mediante el proceso de ESP o AH mediante el algoritmo HMAC-MD5 o HMAC-SHA. El cifrado se realiza opcionalmente para cada paquete mediante el proceso ESP. El cifrado de paquetes utiliza el algoritmo DES, DES-3 o CMDF.

El control de integridad se realiza opcionalmente para cada paquete. El control de integridad se puede realizar mediante el proceso de AH o ESP y utiliza el algoritmo HMAC-MD5 o HMAC-SHA.

## Políticas

Una Política consta de un Perfil y una Acción. El Perfil define un conjunto de atributos para el origen y destino de una conexión. La Acción es en realidad un conjunto de acciones o subpolíticas que se utilizan para la Gestión de claves de IPSec, la Gestión de datos de IPSec, los servicios diferenciados y RSVP. Cuando se debe establecer una conexión, se busca una coincidencia en los Perfiles de la política definida. Si se encuentra una coincidencia de perfil, se intercambian propuestas de acción. Si la fase de propuesta finaliza de manera satisfactoria, se establece la conexión y se crea una instancia actual de la política definida. Se pueden crear varias instancias de política a partir de una única política definida.

### Relaciones entre los componentes de la política

Una política VPN debe contener una Condición de política que conste de un Período de validez, un Perfil de tráfico y como mínimo una Acción de política. El componente Período de validez se puede utilizar en varias políticas, pues no contiene información específica de dispositivos. La definición del componente Perfil de tráfico es exclusiva de la Política, puesto que contiene información específica de dispositivos de la Dirección IP. Las definiciones de los componentes Acción de gestión de claves y Propuesta de gestión de claves de la Acción IPSec se pueden utilizar en varias Políticas, ya que ninguna contiene información específica de dispositivos. La definición del componente Acción de gestión de datos de la Acción IPSec es exclusiva de la Política y contiene información específica de dispositivos de la Dirección IP. Las definiciones de los componentes Acción de gestión de datos, Propuesta de gestión de datos, Transformación de cabecera de autentificación (AH) y Transformación de carga de seguridad encapsulada (ESP) de la Acción IPSec pueden estar en varias Políticas, ya que ninguno de ellos contiene información específica de dispositivos. Las definiciones de los componentes Acción de servicios diferenciales y la Acción RSVP se pueden utilizar en varias Políticas, ya que ninguno contiene información específica de dispositivos. La siguiente tabla muestra las relaciones entre los componentes de una Política VPN.

| Componente de la Política | Relación |
|---|---|
| Condiciones de la política | La política debe contener un período de validez y un perfil de tráfico |
| Período de validez | Pueden compartirlo varias políticas |
| Perfil de tráfico | Exclusivo para la política salvo el Perfil de todo el tráfico |
| Acciones de la política | La política debe contener como mínimo una acción |
| Acción IPSec | Debe contener una clave y una acción de gestión de datos |
| Acción de gestión de claves (KM) | Pueden compartirla varias políticas |
| Propuesta de gestión de claves (KM) | Pueden compartirla varias acciones de gestión de claves |
| Acción de gestión de datos (DM) | Exclusiva de la política (contiene información de la dirección IP) |
| Propuesta de gestión de datos (DM) | Pueden compartirla varias acciones de gestión de datos |
| Transformación AH | Pueden compartirla varias Propuestas de gestión de datos |
| Transformación ESP | Pueden compartirla varias Propuestas de gestión de datos |
| Acción de servicios diferenciales | Pueden compartirla varias políticas |
| Acción RSVP | Pueden compartirla varias políticas |

## LDAP

El protocolo LDAP *(Light Weight Directory Access Protocol)* es un estándar de directorios de interred que ha evolucionado a partir del protocolo DAP (Directory Access Protocol) X.500 y es capaz de proporcionar a los dispositivos de clientes libre acceso a los servidores de directorios de intranet/interred. El protocolo proporciona esta posibilidad al transferir intercambios basados en texto, a partir de un esquema entre un cliente y un servidor a través de TCP/IP. El Cliente y el Servidor pueden dar soporte a uno o varios esquemas, que se utilizan para definir un conjunto de objetos relacionados.

La iniciativa DEN (Directory-Enabled Networking - Red habilitada para directorios) ha identificado LDAP en su especificación como el mecanismo que se utilizará para acceder a la información. DEN empezó en 1997 y actualmente da soporte a varios proveedores como IBM, Microsoft, Cisco Systems y Netscape. El objetivo es proporcionar una especificación de modelo de información para un directorio integrado que almacena información acerca de usuarios, dispositivos de red y aplicaciones. En el ámbito de las redes, DEN se considera actualmente una pieza clave en la creación de redes inteligentes, en las que productos de diversos proveedores pueden almacenar y recuperar datos relacionados con la topología y la configuración desde un Servidor LDAP.

Desde una perspectiva VPN, una Aplicación de configuración de políticas y los Dispositivos VPN son Clientes LDAP que se comunican con un servidor LDAP. La Aplicación de configuración de políticas interactúa con el servidor LDAP para crear, actualizar y suprimir políticas VPN. Los dispositivos VPN interactúan con el servidor LDAP para recuperar sus políticas VPN. Los intercambios entre los Clientes LDAP y el Servidor LDAP se basan en un Esquema de política que define los objetos o datos que se utilizan para representar una política VPN.

## Interacciones entre dispositivos

La Aplicación de configuración de políticas se utiliza para definir Políticas VPN para todos los Dispositivos VPN. Las políticas VPN se almacenan en un Servidor LDAP y a continuación se descargan en los dispositivos VPN durante la inicialización, después de la petición de la Aplicación de configuración de políticas o después de la petición de una Aplicación VPN Monitor.

# Capítulo 3. Utilización de VPN List Manager

Este capítulo contiene los siguientes apartados:

- Acerca de VPN List
- Panel de información de VPN List Manager
- Lista de dispositivos de VPN

## Acerca de VPN List

Nways VPN List permite visualizar una lista de dispositivos cuyo mantenimiento lo realiza un servicio de Nways llamado VPN List Manager. Este servicio recibe dispositivos de los usuarios de esta aplicación y de las bases de datos NetView y OpenView. Para añadir a la lista dispositivos de NetView u OpenView, éstos deben pasar una prueba de filtro que verifica que el dispositivo da soporte a la Red Privada Virtual, tal como lo ha implantado IBM. Esta aplicación se puede utilizar para añadir dispositivos a la lista, agregando dispositivos a una lista de dispositivos de usuarios a la que pueden acceder todos los clientes de VPN List Manager. Esto resulta útil en el caso de dispositivos que son desconocidos para NetView y OpenView o que no pasen la prueba de filtro implantada en este release de VPN List Manager.

Esta aplicación permite al usuario controlar VPN List Manager . Puede restaurar la lista de VPN List Manager o añadirle dispositivos, accediendo a su lista añadida manualmente o comprobando si existen nuevos dispositivos en la base de datos NetView u OpenView que pueden haber cambiado. La capacidad de un dispositivo de pasar la prueba de filtro puede variar debido a las actualizaciones de software realizadas desde la primera vez que se realizó la prueba de filtro.

La aplicación muestra una lista de dispositivos en forma de tabla que permite desplazarse por ella, buscar dispositivos y clasificarlos. A pulsar el botón sobre un dispositivo de la lista, se pueden ver más detalles sobre éste y arrancar la aplicación VPN Monitor para ver información de VPN específica de dicho dispositivo.

## Acerca del panel de información de VPN List Manager

Este panel contiene las siguientes secciones:

- Información
- Valores del archivo de anotaciones cronológicas
- Restaurar VPN Manager List
- Contraseña
- Cambiar contraseña

Para colocar una sección en el área visualizable del panel, pulse el botón una vez sobre el nombre de la sección en la lista de selección que se encuentra en el lado izquierdo del panel.

## Prioridades de las acciones de control

VPN List Manager sólo realizará una acción cada vez desde este panel. Si se solicitan varios cambios en este panel, VPN List Manager seguirá la siguiente jerarquía para determinar qué acciones va a realizar:

1. Cambio de contraseña
2. Cambio de estado del registro cronológico
3. Restaurar lista

## Información

Esta sección contiene los campos siguientes:

**Nombre de sistema principal de VPN List Manager:**
El nombre de sistema principal del sistema en el que se ejecuta VPN List Manager.

**Dirección IP de VPN List Manager:**
La dirección IP del sistema en el que se ejecuta VPN List Manager.

**Versión de VPN List Manager:**
La versión de VPN List Manager que se está ejecutando.

**VPN List iniciado en:**
La fecha y la hora en la que se inició VPN List Manager.

**Hora actual en VPN List Manager:**
La fecha y la hora actual del sistema en el que se ejecuta VPN List Manager.

**Número de dispositivos:**
El número actual de dispositivos cuyo mantenimiento lo realiza VPN List Manager.

Compárelo con el número de dispositivos que utiliza este cliente. Si los números no coinciden, utilice el botón **Renovar** en el panel Lista de dispositivos VPN para renovar la lista de clientes de VPN List Manager.

**Número de clientes:**
El número de clientes que se han registrado en VPN List Manager para recibir avisos de actualización cuando se modifica la lista. Los cambios pueden proceder de otros clientes o ser el resultado de la notificación a VPN List Manager por parte de OpenView o Netview de que se ha descubierto o añadido un nuevo dispositivo.

**Notificar estado a este cliente:**
Indica si este cliente va a recibir actualizaciones de VPN List Manager cuando se modifica la lista.

Los clientes registran las actualizaciones al inicializar la aplicación VPN Manager. El estado debe ser *habilitado*. Si el estado no es *habilitado*, indica que existe un problema en la conexión con VPN List Manager. Vuelva a visualizar el panel Lista de dispositivos VPN y regrese al panel de control de VPN List Manager para ver si el estado ha cambiado.

## Valores del archivo de anotaciones cronológicas

Esta sección contiene los campos siguientes:

**Estado actual del registro cronológico:**

Indica si VPN List Manager está registrando sus actividades en un archivo. Para cambiar este estado es necesario que los usuarios escriban la contraseña actual y pulsen el botón sobre **Aplicar** para activar el cambio.

Si se está creando el archivo de anotaciones cronológicas, éste se llamará vpnlist.log y se ubicará con los demás archivos de anotaciones cronológicas de Nways Manager.

## Restaurar lista

Esta sección contiene los campos siguientes:

**Estado actual de los dispositivos del sistema:**

Indica si VPN List Manager ha podido acceder a la base de datos NetView u OpenView (del sistema) de los dispositivos que List Manager mantiene.

Los valores posibles son los siguientes:

**Error en la carga**

Indica que VPN List Manager no ha podido ponerse en contacto con la base de datos del sistema y por lo tanto no ha podido cargar la lista de dispositivos.

**Desconocido**

Indica que VPN List Manager no conoce el estado de la base de datos del sistema. Esto indica la existencia de un problema en VPN List Manager.

**Cargado**

Es el estado normal, que indica que el sistema ha respondido a la petición de dispositivos de VPN List Manager. Indica que VPN List Manager ha añadido a su lista de manera satisfactoria los dispositivos que son compatibles con VPN.

**A la espera de una respuesta del sistema**

Indica que VPN List Manager todavía no ha añadido ningún dispositivo de la base de datos del sistema. El sistema todavía está reuniendo información sobre dispositivos de la red y transferirá la información sobre dispositivos a VPN List Manager cuando la tarea haya finalizado.

**Carga en proceso...**

Indica que el sistema está transfiriendo actualmente información sobre los dispositivos a VPN List Manager.

**Estado actual de los dispositivos de usuario**

Indica el estado de los dispositivos que los usuarios han añadido manualmente a VPN List Manager.

Los valores posibles son los siguientes:

**Error en la carga**

Indica que VPN List Manager no ha podido cargar el archivo de usuario especificado. Esto indica la existencia de un problema en el archivo de usuario.

**Desconocido**

Indica que VPN List Manager no conoce el estado del archivo de usuario. Esto indica la existencia de un problema en VPN List Manager.

**Cargado**

Es el estado normal cuando VPN List Manager ha leído el archivo de usuario. Indica que VPN List Manager ha añadido de manera satisfactoria los dispositivos del archivo de usuario a su lista de dispositivos.

**Carga en proceso...**

Indica que VPN List Manager está leyendo actualmente el archivo de usuario.

**Restaurar lista**

Permite renovar o añadir elementos a la lista actual de dispositivos. Para restaurar la lista, debe escribir la contraseña actual. Pulse el botón **Aplicar** para restaurar la lista con el tipo de restauración seleccionado.

## Contraseña

Esta sección contiene el campo siguiente:

**Contraseña actual:**

Los usuarios deben escribir una contraseña válida para que VPN List Manager pueda realizar cambios en las listas de dispositivos. Los cambios efectuados en las listas de dispositivos de VPN List Manager afectarán a otros clientes que utilicen este VPN List Manager y deben realizarse con cuidado.

La contraseña por omisión es **OK**.

## Cambiar contraseña

Esta sección contiene los campos siguientes:

**Cambiar contraseña**

Para poder realizar esta acción es necesario escribir la contraseña actual. Debe escribir la contraseña dos veces para su confirmación. Cuando haya escrito la nueva contraseña, pulse el botón **Aplicar** para cambiar la contraseña actual.

# Acerca del panel Lista de dispositivos de VPN

El panel Lista de dispositivos de VPN contiene las secciones siguientes:

- Dispositivos
- Detalles
- Imprimir

## Dispositivos

Esta sección contiene los campos y botones siguientes:

**Tabla de dispositivos**

La tabla de dispositivos muestra información sobre los dispositivos de la lista actual de dispositivos de VPN List Manager en forma de tabla, que le permite buscar información, desplazarse a través de la información y seleccionar dispositivos individuales.

Al seleccionar una fila de la tabla pulsando sobre ésta mientras el puntero se encuentra sobre los datos de la fila, se actualiza el resto de la información mostrada en el panel, para reflejar la fila seleccionada.

La selección de una columna de la tabla clasifica la tabla en orden ascendente o descendente, basándose en los datos de la columna seleccionada.

La doble pulsación sobre una fila realiza la misma función que el botón **Monitor**, iniciando la aplicación VPN Monitor para el dispositivo.

La tabla muestra las siguientes columnas:

**Nombre de dispositivo**
El nombre que el usuario o la plataforma de gestión de la red han proporcionado al dispositivo.

**Dirección IP**
La dirección IP del dispositivo

**Tipo de dispositivo**
El tipo de dispositivo de este dispositivo.

**Campos de búsqueda**
Los campos de búsqueda utilizan el asterisco (*) como carácter comodín. El carácter comodín se puede utilizar al principio de un campo, al final, o en ambos. El comodín no se puede utilizar en la serie de búsqueda. Puede buscar dispositivos por su nombre de dispositivo, por su dirección IP o por ambos.

**Nombre de dispositivo**
El nombre que se desea buscar.

**Dirección IP**
La dirección IP que se desea buscar.

**Botón de búsqueda**
Ejecuta una búsqueda sirviéndose de la información que se encuentra en la fila superior de la vista actual de la lista.

**Botón de búsqueda Siguiente**
Ejecuta una búsqueda sirviéndose de la información entrada en la fila que hay a continuación de la fila seleccionada actualmente en la vista actual de la lista.

## Detalles

Esta sección contiene los campos y botones siguientes:

**Número total de dispositivos de la lista:**
Indica el número total de dispositivos de la lista visualizada actualmente.

**Nombre de dispositivo:**
El nombre del dispositivo actual definido por el usuario.

**Dirección IP:**
La dirección IP del dispositivo actual.

**Nombre comunitario de lectura:**
El nombre comunitario de acceso de lectura de SNMP para el dispositivo actual. El dispositivo puede tener varios niveles de acceso para la lectura y escritura. Este es el nombre asociado con el acceso de sólo lectura.

**Nombre comunitario de escritura**
El nombre comunitario de acceso de escritura de SNMP para el dispositivo actual. El dispositivo puede tener varios niveles de acceso para la lectura y escritura. Es el nombre asociado con el acceso de lectura-escritura.

**Tipo de dispositivo:**
El tipo de dispositivo del dispositivo actual.

**Botón Añadir:**
Al pulsar sobre este botón, se añaden nuevos dispositivos a la lista utilizando la información entrada.

**Botón Cambiar:**
Cambia los atributos de los dispositivos que se han añadido manualmente a la lista. Utilice la plataforma de gestión del sistema para efectuar cambios en los dispositivos que el sistema ha añadido a la lista.

**Botón Suprimir:**
Suprime los dispositivos que se han añadido manualmente a la lista. Para suprimir los dispositivos añadidos por el sistema, utilice la plataforma de gestión del sistema.

**Botón Monitor:**
Inicia la aplicación VPN Monitor en el dispositivo actual.

## Imprimir

Esta sección le permite imprimir la información mostrada en la lista. Puede escribir texto de cabecera y pie de página que se incluirá en todas las páginas impresas.

Esta sección muestra los campos y botones siguientes:

**Cabecera:**
Escriba el texto de cabecera que desea imprimir en la parte superior de cada página.

**Pie de página:**
Escriba el texto de pie de página que desea imprimir en la parte inferior de cada página.

**Botón Imprimir**
Al pulsar este botón se visualiza una lista de selección de impresoras. Seleccione una impresora para dar formato a la salida para el tipo de impresora correcto.

**Nota:** Si no se ha definido ninguna impresora en el sistema, la función de impresión no podrá dar formato a la lista de dispositivos, volverá al panel Lista de dispositivos VPN y responderá con el mensaje:

```
Impresión cancelada
```

# Capítulo 4. VPN Monitor

VPN Monitor proporciona supervisión, notificación se sucesos, resolución de problemas, control operativo y funciones de arranque de aplicaciones para los dispositivos compatibles con VPN de la red y para las VPN que utilicen dichos dispositivos.

Este apartado incluye información sobre la ventana VPN Manager. Contiene las secciones siguientes:

- Ventana VPN Monitor
- Funciones de VPN Monitor

## Ventana VPN Monitor

La ventana VPN Monitor consta de tres partes:

- Árbol de navegación
- Panel de información
- Área de mensajes

### Panel Árbol de navegación

El árbol de navegación es una estructura jerárquica que permite ver el rango de información de gestión acerca del dispositivo gestionado.

#### Iconos

El árbol de navegación utiliza varios iconos para representar los recursos supervisados:

**Carpeta** Recurso de nivel superior que representa uno o varios elementos dependientes. Por ejemplo, la carpeta situada en la parte superior del árbol generalmente representa al propio dispositivo. Otras carpetas de los siguientes niveles pueden representar información de configuración o información sobre errores.

En cada carpeta hay elementos que forman parte de la carpeta global de información. El estado indicado para una carpeta se calcula a partir de los estados de los elementos dependientes inmediatos. Pulse sobre el signo más (+) situado junto a una carpeta para ver y utilizar los elementos de la carpeta.

**Página** Recurso dependiente que consta tan sólo de información, como por ejemplo, información de configuración. Este recurso puede permitir que el usuario efectúe cambios o no permitirlo, según el elemento, el dispositivo que se está gestionando y los derechos de acceso del usuario.

#### Navegación

Para expandir carpetas, pulse sobre el signo más (+) situado junto al icono para mostrar los elementos dependientes.

Para contraer carpetas, pulse sobre el signo menos (–) situado junto al icono para ocultar los elementos dependientes.

### Panel de información

El panel de Información muestra información acerca de la función seleccionada en el panel Árbol de Navegación. Desde este panel se pueden realizar todas las funciones de VPN Monitor.

### Área de mensajes

El Área de mensajes muestra información de estado de la aplicación VPN Monitor.

## Funciones de VPN Monitor

VPN Monitor proporciona las siguientes funciones:

- Supervisión
- Notificación de sucesos
- Control operativo
- Resolución de problemas
- Arranque de aplicaciones

En el resto de este apartado se describe cómo utilizar estas funciones para gestionar VPN y la ubicación de las funciones en el árbol de navegación.

### Supervisión

VPN Monitor muestra información acerca de varias facetas de la red, entre las que se incluyen túneles, clientes y políticas. El Capítulo 6, Carpeta Estado global de VPN Monitor proporciona información general acerca del estado de los elementos de la red VPN. Para visualizar más información, utilice el Capítulo 7, Carpeta Túneles de VPN Monitor, el Capítulo 8, Carpeta Clientes de VPN Monitor, el Capítulo 10, Carpeta Políticas de VPN Monitor y el Capítulo 9, Carpeta Calidad de servicio de VPN Monitor.

Estas carpetas le proporcionan información importante acerca del estado de los elementos de la red.

### Notificación de sucesos

Para proporcionar información adicional acerca de VPN, la aplicación VPN Monitor proporciona anotaciones cronológicas y contadores de los sucesos que se producen en la red. Éstos se muestran en el Capítulo 11, Carpeta Sucesos de VPN Monitor.

La Carpeta Sucesos muestra contadores y registros cronológicos para los éxitos y fracasos de la sesión y el túnel Layer-2 y para los éxitos y fracasos de cifrado y del túnel IPSec.

### Control operativo

La aplicación VPN Monitor también permite controlar los túneles, clientes y políticas de la estación de trabajo de gestión. Mediante la utilización del Capítulo 12, Carpeta operativa de VPN Monitor, puede habilitar o inhabilitar los túneles IPSec y Layer-2, habilitar e inhabilitar clientes y renovar las políticas.

## Resolución de problemas

Puede averiguar el origen de los problemas de conectividad de la red; la aplicación VPN Monitor proporciona diversas herramientas en el Capítulo 13, Carpeta Pruebas de VPN Monitor que le ayudan a comprobar la conectividad potencial, los efectos de las nuevas políticas antes de implantarlas en la red y el tiempo total de transmisión para un túnel específico o para un sistema principal específico.

## Arranque de aplicaciones

La aplicación VPN Monitor proporciona la posibilidad de arrancar algunas aplicaciones que le ayudan a gestionar la red, entre las que se incluyen:

- Telnet
- JMA del dispositivo supervisado
- Navegador MIB
- Navegador Web

# Capítulo 5. Carpeta general de VPN Monitor

La Carpeta general de VPN Monitor proporciona información sobre los Dispositivos VPN de la red. Contiene dos elementos dependientes:

- Identificación
- Administración

## Identificación

El panel Identificación proporciona información general que describe el dispositivo VPN seleccionado. Contiene los siguientes campos, que contienen información recuperada de la MIB del dispositivo.

**Descripción**
Una descripción del dispositivo.

**Identificación de dispositivo**
El identificador de objeto del sistema (SYSOID) para el dispositivo.

**Contacto**
La información de contacto contenida en la MIB del dispositivo. Los usuarios autorizados pueden modificar esta información desde el panel Identificación.

**Nombre de dominio**
El nombre del dominio IP utilizado por el dispositivo. Los usuarios autorizados pueden modificar esta información desde el panel Identificación.

**Ubicación**
La información sobre la ubicación del dispositivo. Los usuarios autorizados pueden modificar esta información desde el panel Identificación.

**Tiempo activo**
El tiempo transcurrido desde que el dispositivo se inició o reinició por última vez.

**Servicios del sistema**
Número que representa las prestaciones del dispositivo.

**Funciones de servicio del sistema**
Texto descriptivo de las prestaciones representadas por el número de Servicios del sistema.

## Administración

El panel Administración muestra los parámetros SNMP que VPN Monitor utiliza para comunicarse con el dispositivo. Los usuarios autorizados pueden modificar esta información desde el panel Administración.

El panel Administración contiene los siguientes campos:

**Dirección IP**
La dirección IP utilizada para peticiones SNMP

**Nombre comunitario (Lectura)**
El nombre comunitario SNMP utilizado para peticiones de Lectura.

**Nombre comunitario (escritura)**
El nombre comunitario SNMP utilizado para peticiones de Escritura.

**Puerto remoto**
El puerto del dispositivo utilizado para las peticiones SNMP.

**Tiempo de espera excedido (ms)**
El valor de tiempo de espera excedido, en milisegundos, utilizado para peticiones SNMP.

**Reintentos**
El número de reintentos utilizados para peticiones SNMP.

**Intervalo de sondeo**
El intervalo de sondeo, en milisegundos, utilizado para peticiones SNMP.

# Capítulo 6. Carpeta Estado global de VPN Monitor

La carpeta Estado global de VPN Monitor muestra el proceso VPN del dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Resumen

## Resumen

El panel Resumen proporciona información de resumen acerca del proceso VPN del dispositivo seleccionado. Contiene las siguientes secciones:

- Niveles
- Túneles
- Clientes
- Política
- Sucesos

### Niveles

La sección de niveles proporciona información sobre el código de protocolo y las MIB utilizadas por el dispositivo. Contiene los siguientes campos:

**Versión MIB de Layer-2**
La versión de la MIB de Layer-2 utilizada por el dispositivo.

**Versión de protocolo de Layer-2**
La versión del código de protocolo de Layer-2 utilizada por el dispositivo.

**Versión MIB de IPSec**
La versión de la MIB de IPSec utilizada por el dispositivo.

**Versión MIB de política**
La versión de la MIB de política utilizada por el dispositivo.

### Túneles

La sección Túneles proporciona información sobre el número de túneles Layer-2 e IPSec que están activos actualmente en este dispositivo.

### Clientes

La sección Clientes muestra el número de sesiones Layer-2 que están activas actualmente en este dispositivo.

### Política

La sección Política proporciona información sobre la política VPN utilizada actualmente por el dispositivo. Contiene los siguientes campos:

**Tiempo activo de la política**
El tiempo activo del código de componente de la Política actual.

**Tiempo activo del dispositivo**
El tiempo activo del dispositivo.

**Hora actual del dispositivo**
La hora actual utilizada por el dispositivo.

**Horas respecto a UTC**
La diferencia entre la hora utilizada por el dispositivo y la UTC (hora universal coordinada) actual.

**Origen de configuración actual**
El origen de la configuración de la Política actual.

**Estado de carga de la política**
El resultado del último intento de cargar una política.

## Sucesos

La sección Sucesos proporciona información sobre los sucesos supervisados por VPN Monitor para este dispositivo. Contiene los siguientes campos:

**Éxitos de túnel Layer-2**
El número de túneles Layer-2 activados de manera satisfactoria para este dispositivo.

**Errores de túnel Layer-2**
El número de túneles Layer-2 para este dispositivo que se han intentado activar sin éxito.

**Éxitos de sesión Layer-2**
El número de sesiones Layer-2 activadas de manera satisfactoria para este dispositivo.

**Errores de sesión Layer-2**
El número de intentos no satisfactorios de activar una sesión Layer-2 para este dispositivo.

**Autentificaciones de IPSec de entrada**
El número de autentificaciones de IPSec de entrada realizadas de manera satisfactoria.

**Errores de autentificación de IPSec de entrada**
El número de intentos fallidos de autentificaciones de IPSec de entrada.

**Descifrados de IPSec de entrada**
El número de descifrados de IPSec de entrada realizados de manera satisfactoria.

**Errores de descifrado de IPSec de entrada**
El número de intentos fallidos de descifrados de IPSec de entrada.

**Autentificaciones de salida de IPSec**
El número de autentificaciones de IPSec de salida realizadas de manera satisfactoria.

**Errores de autentificación de IPSec de salida**
El número de intentos fallidos de autentificaciones de IPSec de salida.

**Cifrados de IPSec de salida**
El número de cifrados de IPSec de salida realizados de manera satisfactoria.

**Errores de cifrado IPSec de salida**
El número de intentos fallidos de cifrados de IPSec de salida.

# Capítulo 7. Carpeta Túneles de VPN Monitor

La carpeta Túneles de VPN Monitor contiene información sobre el estado de los túneles Layer-2 e IPSec utilizados por el dispositivo seleccionado. Esta carpeta contiene los siguientes elementos dependientes:

- Carpeta Túneles Layer-2
- Carpeta Túneles IPSec

## Carpeta Túneles Layer-2

La carpeta Túneles Layer-2 proporciona información sobre los túneles Layer-2 anteriores y activos del dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Panel Túneles activos
- Panel Túneles anteriores

### Carpeta Activa

La carpeta Túneles Layer-2 Activos proporciona información para todos los túneles Layer-2 activos asociados con el dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Panel Estado
- Panel Atributos
- Panel Estadísticas
- Panel Puntos finales

#### Panel Estado

El panel Estado proporciona información sobre el estado de los Túneles Layer-2 activos asociados con el dispositivo seleccionado. Contiene los siguientes campos:

**Túnel** El número de índice del túnel.

**Estado** El estado del túnel: activo o destruir. Los usuarios autorizados pueden modificar este valor desde la vista Estado.

**Tipo** El tipo de túnel: L2TP, L2F o PPTP.

**Sistema principal remoto**
El nombre del sistema principal asociado con este túnel

**Tiempo activo**
El tiempo que el túnel ha estado activo.

**Sesiones activas**
El número de sesiones activas asociadas con este túnel.

**Sesiones anteriores**
El número de sesiones previamente activas asociadas con este túnel.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles Layer-2. Los usuarios autorizados pueden modificar este valor desde la vista Estado.

## Panel Atributos

El panel Atributos proporciona información sobre los atributos de un túnel seleccionado. Contiene los siguientes campos:

**Identificación de control local**
La identificación de control local para el túnel.

**Identificación de control similar**
La identificación de control similar para el túnel.

**Estado de control**
El estado de control del túnel.

**Tiempos de espera excedidos de control**
El número de tiempos de espera excedidos de control registrados para este túnel.

**Sistema principal remoto**
El nombre del sistema principal remoto asociado con este túnel.

**Nombre de proveedor remoto**
El nombre del proveedor del sistema principal remoto.

**Versión de firmware remoto**
La versión del firmware que se ejecuta en el sistema principal remoto.

**Versión de protocolo remoto**
La versión de protocolo utilizada por el sistema principal remoto.

**Conexión inicial**
Indica si el túnel lo ha generado el sistema principal local.

**Ventana de paquetes de recepción local**
El tamaño de la ventana de paquetes de recepción utilizada por el sistema principal local.

**Ventana de paquetes de recepción remota**
El tamaño de la ventana de paquetes de recepción utilizada por el sistema principal remoto.

**Siguiente secuencia de envío**
El valor del siguiente número de secuencia de envío.

**Siguiente secuencia de recepción**
El valor del siguiente número de secuencia de recepción.

## Panel Estadísticas

El panel Estadísticas proporciona estadísticas acerca del túnel Layer-2 especificado. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos a través de este túnel.

**Paquetes de entrada**
El número de paquetes recibidos a través de este túnel.

**Paquetes de entrada descartados**
El número de paquetes descartados durante la recepción a través de este túnel.

**Bytes de salida**
El número de bytes enviados a través de este túnel por el sistema principal local.

**Paquetes de salida**
El número de paquetes enviados a través de este túnel por el sistema principal local.

**Paquetes de salida descartados**
El número de paquetes descartados durante el envío a través de este túnel por el sistema principal local.

### Panel Puntos finales

El panel Puntos finales proporciona información acerca del punto final de un túnel seleccionado. Contiene los siguientes campos:

**Dirección IP remota**
La dirección IP remota asociada con el túnel seleccionado.

**Dirección IP local**
La dirección IP local del túnel seleccionado.

**Puerto de origen**
El puerto del sistema principal local asociado con este túnel.

**Puerto de destino**
El puerto del sistema principal remoto asociado con este túnel.

## Carpeta Túneles anteriores

La carpeta Túneles Layer-2 anteriores proporciona información de resumen y estadísticas para los túneles Layer-2 anteriores especificados, asociados con el dispositivo seleccionado. El número de entradas anteriores para las que se visualiza información se puede especificar desde el panel Resumen. La carpeta Túneles Layer-2 anteriores contiene los siguientes elementos dependientes:

- Panel Resumen
- Panel Estadísticas

### Panel Resumen

El panel Resumen proporciona información sobre un túnel Layer-2 activo previamente seleccionado. Contiene los siguientes campos:

**Orden** El orden en el que ha finalizado el túnel.

**Túnel** El índice del túnel.

**Tipo** El tipo de túnel: L2TP, L2F, PPTP.

**Sistema principal remoto**
El nombre del sistema principal remoto asociado con el túnel.

**Dirección IP remota**
La dirección IP remota asociada con el túnel.

**Puerto remoto**
El puerto remoto asociado con el túnel.

**Dirección IP local**
La dirección IP local asociada con el túnel.

**Puerto local**
El puerto local asociado con el túnel.

**Sesiones totales**
El número total de sesiones activas que han utilizado el túnel.

**Tiempo activo del túnel**
El tiempo que el túnel ha estado activo.

### Panel Estadísticas

El panel Estadísticas proporciona información acerca de la utilización de un túnel anterior. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos a través de este túnel por el dispositivo supervisado.

**Paquetes de entrada**
El número de paquetes recibidos a través de este túnel por el dispositivo supervisado.

**Paquetes de entrada descartados**
El número de paquetes descartados durante la recepción a través de este túnel por el dispositivo supervisado.

**Bytes de salida**
El número de bytes enviados a través de este túnel por el dispositivo supervisado.

**Paquetes de salida**
El número de paquetes enviados a través de este túnel por el dispositivo supervisado.

**Paquetes de salida descartados**
El número de paquetes descartados por el dispositivo supervisado durante el envío a través de este túnel.

## Carpeta Túneles IPSec

La carpeta Túneles de control IPSec proporciona información sobre los túneles IPSec activos y anteriores del dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Carpeta Túneles activos
- Carpeta Túneles anteriores

## Carpeta Túneles activos

La carpeta Túneles IPSec activos proporciona información sobre los túneles de control IPSec y túneles de datos de usuario activos. Contiene los siguientes elementos dependientes:

- Carpeta Túneles de control IPSec
- Carpeta Túneles de datos de usuario IPSec

### Carpeta Túneles de control IPSec

La carpeta Túneles de control IPSec proporciona información acerca de los túneles de control IPSec activos asociados con el dispositivo seleccionado. Contiene los siguientes paneles:

- Estado
- Atributos
- Estadísticas
- Proceso

**Estado:** El panel Estado proporciona información sobre el Estado de un túnel de control IPSec seleccionado. Contiene los siguientes campos:

**Túnel** El número de índice del túnel seleccionado.

**Estado** El estado del túnel: activo o destruir. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Identificación**
La identificación del túnel seleccionado.

**Nombre remoto**
El nombre remoto del túnel.

**Dirección remota**
La dirección IP remota del túnel.

**Nombre local**
El nombre local del túnel.

**Dirección local**
La dirección IP local del túnel.

**Tiempo activo**
El tiempo que el túnel ha estado activo.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles de control IPSec activos. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Atributos:** El panel Atributos proporciona información sobre los atributos del túnel de control IPSec seleccionado. Contiene los siguientes campos:

**Modalidad de negociación**
La modalidad utilizada por el túnel de control IPSec seleccionado para negociar nuevas conexiones con sistemas principales remotos.

**Duración en segundos de SA**
La duración en segundos de la asociación de seguridad del túnel.

**Porcentaje del umbral de renovación de SA**
El porcentaje del umbral de renovación de la asociación de seguridad.

**Renovaciones totales de SA**
El número de renovaciones de la asociación de seguridad realizadas.

**Estadísticas:** Este panel proporciona estadísticas acerca del túnel de control IPSec seleccionado. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos a través de este túnel por el dispositivo supervisado.

**Paquetes de entrada**
El número de paquetes recibidos a través de este túnel por el dispositivo supervisado.

**Paquetes de entrada suprimidos**
El número de paquetes descartados durante la recepción a través de este túnel por el dispositivo supervisado.

**Bytes de salida**
El número de bytes enviados a través de este túnel por el dispositivo supervisado.

**Paquetes de salida**
El número de paquetes enviados a través de este túnel por el dispositivo supervisado.

**Paquetes de salida suprimidos**
El número de paquetes descartados por el dispositivo supervisado durante el envío a través de este túnel.

**Proceso:** Este panel proporciona información sobre el proceso relacionado con el túnel de control IPSec seleccionado. Contiene los siguientes campos:

**Notificaciones de entrada**
El número de notificaciones recibidas a través de este túnel.

**Propuestas de entrada**
El número de propuestas recibidas a través de este túnel.

**Propuestas de entrada no válidas**
El número de propuestas recibidas a través de este túnel que no han sido válidas.

**Propuestas de entrada rechazadas**
El número de propuestas recibidas a través de este túnel que se han rechazado.

**Supresiones de entrada de SA**
El número de supresiones de la asociación de seguridad recibidas a través de este túnel.

**Notificaciones de salida**
El número de notificaciones enviadas a través de este túnel.

**Propuestas de salida**
El número de propuestas enviadas a través de este túnel.

**Propuestas de salida no válidas**
El túnel de propuestas enviadas a través de este túnel que no han sido válidas.

**Propuestas de salida rechazadas**
El número de propuestas enviadas a través de este túnel que se han rechazado.

**Supresiones de salida de SA**
El número de supresiones de asociaciones de seguridad enviadas a través de este túnel.

## Carpeta Túneles de datos de usuario IPSec activos

Esta carpeta proporciona información acerca de los túneles de datos de usuario IPSec activos asociados con el dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Panel Estado
- Panel Atributos
- Panel Estadísticas
- Panel Puntos finales
- Panel Índices de protección de seguridad

**Panel Estado:** Este panel proporciona información sobre el estado del túnel de datos de usuario IPSec seleccionado. Contiene los siguientes campos:

**Túnel** El número de índice del túnel seleccionado.

**Estado** El estado del túnel seleccionado: activo o destruir. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Dirección IP remota**
La dirección IP remota del túnel.

**Dirección IP local**
La dirección IP local del túnel.

**Tiempo activo**
El tiempo que el túnel ha estado activo.

**Renovaciones totales de la asociación de seguridad**
El número total de renovaciones de la asociación de seguridad realizadas.

**Asociaciones de seguridad actuales**
El número de asociaciones de seguridad actuales.

**Asociaciones de seguridad caducadas**
El número de asociaciones de seguridad caducadas.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles de datos de usuario IPSec activos. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Panel Atributos:** Este panel proporciona información sobre los atributos del túnel de datos de usuario IPSec seleccionado. Contiene los siguientes campos:

**Identificación**
El número de índice del túnel.

**Túnel de control**
El número de índice del túnel de control IPSec asociado con este túnel de datos de usuario IPSec.

**Tipo de clave**
El tipo de clave del túnel.

**Modalidad de encapsulación**
La modalidad de encapsulación del túnel.

**Duración en segundos de la asociación de seguridad**
La duración en segundos de la asociación de seguridad del túnel.

**Porcentaje del umbral de renovación de la asociación de seguridad**
El porcentaje del umbral de renovación de la asociación de seguridad.

**Cifrado de SA de entrada**
El tipo de cifrado de entrada utilizado para este túnel.

**Autentificación de SA de entrada**
El algoritmo de autentificación de entrada utilizado para este túnel.

**Cifrado de SA de salida**
El tipo de cifrado de salida utilizado para este túnel.

**Autentificación de SA de salida**
El algoritmo de autentificación de salida utilizado para este túnel.

**Panel Estadísticas:** Este panel proporciona estadísticas de uso para el túnel de datos de usuarios IPSec seleccionado. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos a través de este túnel.

**Reinicios de contador de bytes de entrada**
El número de veces que el contador de bytes se ha reiniciado.

**Bytes descomprimidos de entrada**
El número de bytes descomprimidos recibidos a través de este túnel.

**Reinicios de bytes descomprimidos de entrada**
El número de veces que el contador de bytes descomprimidos de entrada se ha reiniciado.

**Paquetes de entrada**
El número de paquetes recibidos a través de este túnel.

**Paquetes de entrada suprimidos**
El número de paquetes suprimidos durante la recepción a través de este túnel.

**Autentificaciones de entrada**
El número de autentificaciones de entrada realizadas para este túnel.

**Errores de autentificación de entrada**
El número de autentificaciones de entrada para este túnel que no se han realizado satisfactoriamente.

**Descifrados de entrada**
El número de descifrados de entrada realizados para este túnel.

**Errores de descifrado de entrada**
El número de descifrados de entrada para este túnel que no se han realizado satisfactoriamente.

**Bytes de salida**
El número de bytes enviados a través de este túnel.

**Reinicios de contador de bytes de salida**
El número de veces que se ha reiniciado el contador de bytes de salida.

**Bytes descomprimidos de salida**
El número de bytes descomprimidos enviados a través de este túnel.

**Reinicios de bytes descomprimidos de salida**
El número de veces que se ha reiniciado el contador de bytes descomprimidos de salida.

**Paquetes de salida**
El número de paquetes enviados a través de este túnel.

**Paquetes de salida suprimidos de salida**
El número de paquetes suprimidos durante la transmisión a través de este túnel.

**Autentificaciones de salida**
El número de autentificaciones de salida realizadas para este túnel.

**Errores de autentificaciones de salida**
El número de autentificaciones de salida para este túnel que no se han realizado satisfactoriamente.

**Cifrados de salida**
El número de cifrados de salida realizados para este túnel.

**Errores de cifrados de salida**
El número de cifrados de salida para este túnel que no se han realizado satisfactoriamente.

**Panel Puntos finales:** Este panel proporciona información sobre los puntos finales del túnel seleccionado. Contiene los siguientes campos:

**Nombre local**
El nombre local del túnel.

**Tipo local**
El tipo de direccionamiento local: subred o rango.

**Protocolo local**
El protocolo local del túnel.

**Máscara de subred local**
La máscara de subred local utilizada para el túnel.

**Dirección IP baja local**
La dirección IP baja local para el túnel.

**Dirección IP alta local**
La dirección IP alta local para el túnel.

**Puerto local**
El puerto local utilizado por el túnel.

**Nombre remoto**
El nombre remoto del túnel.

**Tipo remoto**
El tipo de direccionamiento remoto: subred o rango.

**Protocolo remoto**
El protocolo remoto del túnel.

**Máscara de subred remota**
La máscara de subred remota utilizada para el túnel.

**Dirección IP baja remota**
La dirección IP baja remota para el túnel.

**Dirección IP alta remota**
La dirección IP alta remota para el túnel.

**Puerto remoto**
El puerto remoto utilizado por el túnel.

**Panel Índices de protección de seguridad:** Este panel proporciona información acerca del índice de protección de seguridad (SPI) utilizado por el túnel. Contiene los siguientes campos:

**SPI** El índice de protección de seguridad utilizado por el túnel.

**Dirección**
La dirección de tráfico a la que se está aplicando el SPI: entrada o salida.

**Valor** El valor del SPI.

**Protocolo**
El protocolo usado por el SPI.

## Carpeta Túneles de datos de usuario IPSec anteriores

Esta carpeta proporciona información sobre los túneles de datos de usuario IPSec que han dejado de estar activos. Contiene los siguientes paneles:

- Panel Resumen
- Panel Estadísticas

**Panel Resumen:** Este panel proporciona información de resumen acerca de los túneles de datos de usuario IPSec anteriores. Contiene los siguientes campos:

**Orden** El orden en el que ha finalizado el túnel.

**Identificación**
La identificación del túnel.

**Dirección IP remota**
La dirección IP remota utilizada por el túnel.

**Dirección IP local**
La dirección IP local utilizada por el túnel.

**Tiempo activo**
El tiempo que el túnel ha estado activo.

**Renovaciones totales de SA**
El número de renovaciones asociación de seguridad realizadas para este túnel.

**SA totales**
El número total de asociaciones de seguridad para este túnel.

**Panel Estadísticas:** Este panel proporciona estadísticas de uso para un túnel de datos de usuario IPSec activo previamente. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos a través de este túnel.

**Reinicios de contador de bytes de entrada**
El número de veces que se ha reiniciado el contador de bytes de entrada.

**Bytes descomprimidos de entrada**
El número de bytes descomprimidos recibidos a través de este túnel.

**Reinicios de bytes descomprimidos de entrada**
El número de veces que el contador de bytes descomprimidos de entrada se ha reiniciado.

**Paquetes de entrada**
El número de paquetes recibidos a través de este túnel.

**Paquetes de entrada suprimidos**
El número de paquetes suprimidos durante la recepción a través de este túnel.

**Autentificaciones de entrada**
El número de autentificaciones de entrada realizadas para este túnel.

**Errores de autentificación de entrada**
El número de autentificaciones de entrada para este túnel que no se han realizado satisfactoriamente.

**Descifrados de entrada**
El número de descifrados de entrada realizados para este túnel.

**Errores de descifrados de entrada**
El número de descifrados de entrada para este túnel que no se han realizado satisfactoriamente.

**Bytes de salida**
El número de bytes enviados a través de este túnel.

**Reinicios de contador de bytes de salida**
El número de veces que se ha reiniciado el contador de bytes de salida.

**Bytes descomprimidos de salida**
El número de bytes descomprimidos enviados a través de este túnel.

**Reinicios de bytes descomprimidos de salida**
El número de veces que se ha reiniciado el contador de bytes descomprimidos de salida.

**Paquetes de salida**
El número de paquetes enviados a través de este túnel.

**Paquetes de salida suprimidos**
El número de paquetes suprimidos durante la transmisión a través de este túnel.

**Autentificaciones de salida**
El número de autentificaciones de salida realizadas para este túnel.

**Errores de autentificaciones de salida**
El número de autentificaciones de salida para este túnel que no se han realizado satisfactoriamente.

**Cifrados de salida**
El número de cifrados de salida realizados para este túnel.

**Errores de cifrados de salida**
El número de cifrados de salida para este túnel que no se han realizado satisfactoriamente.

# Capítulo 8. Carpeta Clientes de VPN Monitor

La carpeta Clientes de VPN Monitor proporciona información sobre las sesiones Layer-2. Contiene las siguientes subcarpetas:

- Sesiones Layer-2

## Carpeta Sesiones Layer-2

Esta carpeta proporciona información sobre las sesiones Layer-2 para el dispositivo seleccionado. Contiene las siguientes subcarpetas:

- Sesiones activas
- Sesiones anteriores

### Carpeta Sesiones activas

Esta carpeta proporciona información sobre las sesiones Layer-2 activas para el dispositivo seleccionado. Contiene los siguientes paneles:

- Estado
- Estadísticas

#### Carpeta Estado

Esta carpeta proporciona información de estado sobre una sesión Layer-2 seleccionada. Contiene los siguientes paneles:

- Estado
- Atributos
- Estadísticas

**Panel Estado:** Este panel proporciona información sobre el estado de una sesión Layer-2 seleccionada. Contiene los siguientes campos:

**Túnel** El índice del túnel utilizado por la sesión seleccionada.

**Sesión** El índice de la sesión.

**Estado** El estado de la sesión: activa o destruir. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Tiempo activo de la sesión**
El tiempo que la sesión ha estado activa.

**BPS de conexión**
La velocidad de la conexión en bits por segundo.

**Método de autentificación**
El método de autentificación utilizado por esta sesión.

**Cifrado/Descifrado**
El indicador de cifrado/descifrado para esta sesión. Verdadero indica que el cifrado y descifrado se están utilizando para la sesión, Falso indica que no se están utilizando.

**Destruir todas las sesiones**
El desencadenante para destruir todas la sesiones Layer-2. Los usuarios autorizados pueden modificar este valor desde el panel Estado.

**Panel Atributos:** Este panel enumera los atributos de la sesión seleccionada. Contiene los siguientes campos:

**Nombre remoto**
El nombre remoto de la sesión.

**Estado de línea**
El estado de línea de la sesión.

**Identificación local**
La identificación local de la sesión.

**Identificación remota**
La identificación remota de la sesión.

**Número de dispositivo**
El número del dispositivo que utiliza la sesión.

**Número de serie**
El número de serie del dispositivo que utiliza la sesión.

**Tipo de portador**
El tipo de portador que utiliza la sesión: digital or analógico.

**Tipo de trama**
El tipo de trama que utiliza la sesión: síncrona o asíncrona.

**Ventana de paquetes locales**
El tamaño de la ventana de paquetes locales.

**Ventana de paquetes remotos**
El tamaño de la ventana de paquetes remotos.

**Tiempos de espera excedidos**
El número de tiempos de espera excedidos que se han producido durante esta sesión.

**Siguiente secuencia de envío**
El valor del siguiente número de secuencia de envío.

**Siguiente secuencia de recepción**
El valor del siguiente número de secuencia de recepción.

**PPD remoto**
La duración del retardo del proceso de paquetes remotos.

**Panel Estadísticas:** Este panel proporciona información estadística para la sesión Layer-2 seleccionada. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos.

**Bytes de entrada descomprimidos**
El número de bytes descomprimidos recibidos.

**Paquetes de entrada**
El número de paquetes recibidos.

**Paquetes de entrada descartados**
El número de paquetes descartados durante la recepción.

**Bytes de salida**
El número de bytes enviados.

**Bytes de salida descomprimidos**
El número de bytes descomprimidos enviados.

**Paquetes de salida**
El número de paquetes enviados.

**Paquetes de salida descartados**
El número de paquetes descartados durante el envío.

## Carpeta Sesiones Layer-2 anteriores

Esta carpeta proporciona información sobre las sesiones Layer-2 anteriores del dispositivo seleccionado. Contiene los siguientes elementos dependientes:

- Panel Resumen
- Panel Estadísticas

**Panel Resumen:** Este panel proporciona información de resumen acerca de una sesión Layer-2 seleccionada del dispositivo elegido. Contiene los siguientes campos:

**Orden** El orden en el que ha finalizado la sesión.

**Túnel** El índice del túnel utilizado por la sesión.

**Sesión** El índice de la sesión activa previamente.

**Método de autentificación**
El método de autentificación utilizado por la sesión.

**Cifrado/Descifrado**
El indicador de cifrado/descifrado para la sesión. Verdadero indica que se ha utilizado el cifrado/descifrado para la sesión, Falso indica que no se ha utilizado.

**Tiempo activo**
El tiempo que la sesión ha estado activa.

**Panel Estadísticas:** Este panel proporciona información estadística acerca de una sesión Layer-2 activa previamente en el dispositivo seleccionado. Contiene los siguientes campos:

**Bytes de entrada**
El número de bytes recibidos.

**Bytes de entrada descomprimidos**
El número de bytes descomprimidos recibidos.

**Paquetes de entrada**
El número de paquetes recibidos.

**Paquetes de entrada descartados**
El número de paquetes descartados durante la recepción.

**Bytes de salida**
El número de bytes enviados.

**Bytes de salida descomprimidos**
El número de bytes descomprimidos enviados.

**Paquetes de salida**
El número de paquetes enviados.

**Paquetes de salida descartados**
El número de paquetes descartados durante el envío.

# Capítulo 9. Carpeta Calidad de servicio de VPN Monitor

Esta carpeta proporciona información sobre la calidad de servicio de una sesión seleccionada que utiliza el Protocolo RSVP (Resource Reservation Protocol - Protocolo de Reserva de Recursos). Contiene el siguiente elemento dependiente:

- RSVP

## Carpeta RSVP

Esta carpeta contiene información acerca del protocolo RSVP (Resource Reservation Protocol) utilizado para una sesión seleccionada. Contiene los siguientes paneles:

- Sesiones
- Mensajes PATH del emisor
- Mensajes RESV en sentido inverso

### Panel Sesiones

Este panel proporciona información de RSVP para una sesión seleccionada. Contiene los siguientes campos:

**Índice de sesión**
El índice de la sesión.

**Tipo de sesión**
El tipo de la sesión.

**Protocolo IP**
El protocolo IP utilizado por la sesión.

**Dirección de destino**
La dirección de destino de la sesión.

**Puerto de destino**
El puerto de destino de la sesión.

**Número de emisores**
El número de emisores de la sesión.

**Número de peticiones RSVP recibidas**
El número de peticiones RSVP recibidas por el dispositivo seleccionado.

**Número de peticiones RSVP enviadas**
El número de peticiones RSVP enviadas por el dispositivo seleccionado.

### Panel Mensajes PATH del emisor

Este panel contiene información de rutas para la sesión seleccionada. Contiene los siguientes campos:

**Índice de sesión**
El índice de la sesión.

**Índice de emisor**
El índice del emisor asociado con esta sesión.

**Tipo de sesión**
El tipo de sesión.

**Protocolo IP**
El protocolo IP de la sesión.

**Dirección de destino**
La dirección de destino asociada con esta sesión.

**Puerto de destino**
El puerto de destino asociado con esta sesión.

**Dirección de origen**
La dirección de origen asociada con esta sesión.

**Puerto de origen**
El puerto de origen asociado con esta sesión.

**Identificador de flujo IPv6**
El identificador de flujo IPv6 para esta sesión.

**Dirección de salto anterior**
La dirección IP del salto anterior.

**Handle de interfaz lógica de salto anterior**
El handle de interfaz lógica del salto anterior.

**Último índice de interfaz**
El último índice de interfaz.

**BPS Promedio**
La velocidad media de conexión de esta sesión, en bits por segundo.

**BPS máximo**
La velocidad más alta de conexión de esta sesión, en bits por segundo.

**Máximo de Bytes esperados**
El número máximo de bytes esperados a través de esta conexión.

**Tamaño mínimo de mensaje**
El tamaño mínimo de mensaje utilizado para esta sesión.

**Tamaño máximo de mensaje**
El tamaño máximo de mensaje utilizado para esta sesión.

**Intervalo de mensajes de renovación**
El intervalo con el que se envían los mensajes de renovación para esta sesión.

**Salto anterior es RSVP**
Indica si el salto anterior era un salto RSVP.

**Último cambio de mensaje de la ruta**
La hora en la que se cambió por última vez el mensaje de la ruta.

**Política**
La política asociada con este emisor.

**Último valor TTL**
El último valor del tiempo de vida utilizado para esta sesión.

**Salto no IS detectado**
Indica si se ha detectado un salto no IS para esta sesión.

**Cuenta de saltos**
La cuenta de saltos para esta sesión.

**Ancho de banda de la ruta**
El ancho de banda de la ruta.

**Latencia mínima de la ruta**
La latencia mínima de la ruta.

**Unidad máxima de transmisión**
El tamaño de la MTU (unidad máxima de transmisión) para esta sesión.

**Servicio garantizado**
Indica si el servicio está garantizado para esta sesión.

**Interrupción de servicio**
Indica si se ha producido una interrupción de servicio para esta sesión.

**Alteración temporal de la cuenta de saltos**
La alteración temporal de la cuenta de saltos para esta sesión.

**Alteración temporal del ancho de banda de la ruta**
La alteración temporal del ancho de banda de la ruta para esta sesión.

**Alteración temporal de la latencia mínima de la ruta**
La alteración temporal de la latencia mínima de la ruta para esta sesión.

**Alteración temporal de unidad máxima de transmisión**
La alteración temporal de la unidad máxima de transmisión para esta sesión.

## Panel Mensajes RESV en sentido inverso

Este panel proporciona información sobre los mensajes RESV en sentido inverso para la sesión seleccionada. Contiene los siguientes campos:

**Índice de sesión**
El índice de la sesión.

**Índice de petición**
El índice de la petición.

**Tipo de sesión**
El tipo de la sesión.

**Protocolo IP**
El protocolo IP utilizado para esta sesión.

**Dirección de destino**
La dirección de destino asociada con esta sesión.

**Puerto de destino**
El puerto de destino asociado con esta sesión.

**Dirección de origen**
La dirección de origen asociada con esta sesión.

**Puerto de origen**
El puerto de origen asociado con esta sesión.

**Dirección de salto anterior**
La dirección IP del salto anterior.

**Handle de interfaz lógica de salto anterior**
El handle de la interfaz lógica del salto anterior.

**Último índice de interfaz**
El último índice de la interfaz.

**Calidad de servicio**
La clasificación de calidad de servicio solicitada para esta sesión.

**BPS Promedio**
La velocidad media de esta conexión, en bits por segundo.

**BPS máximo**
La velocidad más alta de conexión, en bits por segundo.

**Máximo de Bytes esperados**
El número máximo de bytes esperados a través de esta conexión.

**Tamaño mínimo de mensaje**
El tamaño mínimo de mensaje utilizado para esta conexión.

**Tamaño máximo de mensaje**
El tamaño máximo de mensaje utilizado para esta conexión.

**Intervalo de mensajes de renovación**
El intervalo de mensajes de renovación para esta conexión.

**Ámbito**
El valor del objeto de ámbito.

**Reserva compartida**
El indicador de reserva compartida.

**Emisores explícitos**
El indicador de emisores explícitos.

**El siguiente salto es RSVP**
Indica si el siguiente salto es un salto RSVP.

**Último cambio**
La hora del último cambio.

**Política**
La política asociada con esta petición.

**Último valor TTL**
El valor del último tiempo de vida recibido.

**Identificador de flujo IPv6**
El identificador de flujo IPv6.

# Capítulo 10. Carpeta Políticas de VPN Monitor

Esta carpeta contiene información sobre las políticas utilizadas para dirigir las conexiones VPN. Contiene los siguientes elementos dependientes:

- Carpeta Dispositivo
- Carpeta Condiciones
- Carpeta Acciones

## Carpeta Dispositivo

La carpeta Dispositivo proporciona información sobre las políticas creadas para un dispositivo seleccionado. Contiene los siguientes paneles:

- Políticas
- Reglas de filtro
- Política para reglas

La carpeta Dispositivo proporciona los mismos campos para las tres vistas de información sobre la política. Dichos campos son:

**Nombre de política**
El nombre de la política.

**Estado** El estado de la política: habilitar o inhabilitar. Los usuarios autorizados pueden modificar este valor desde el panel Políticas.

**Prioridad**
La prioridad de la política.

**Validez**
El indicador de validez para la política.

**Identificación manual de IPSec**
La identificación manual del túnel IPSec.

**Coincidencias**
El número de coincidencias para esta política.

**Período de validez**
El nombre del período de validez para esta política.

**Perfil de tráfico**
El nombre del perfil de tráfico para esta política.

**Acción de gestión de claves**
El nombre de la acción de gestión de claves para esta política.

**Acción de gestión de datos**
El nombre de la acción de gestión de datos para esta política.

**Acción de servicios diferenciales**
El nombre de la acción de servicios diferenciales para esta política.

**Acción RSVP**
El nombre de la acción RSVP para esta política.

### Carpeta Condiciones

La carpeta Condiciones de la política proporciona información sobre los períodos de validez y acciones de política para una política seleccionada. Contiene los siguientes elementos dependientes:

- Panel Períodos de validez
- Carpeta Perfiles de tráfico

## Panel Períodos de validez

El panel Períodos de validez muestra las definiciones de todos los períodos de validez. Contiene los siguientes campos:

**Nombre de período de validez**
El nombre del período de validez.

**Fecha y hora de inicio**
La fecha y la hora de inicio del período de validez.

**Fecha y hora de fin**
La fecha y la hora de finalización del período de validez.

**Máscara de meses**
La máscara utilizada para determinar los meses del período de validez.

**Máscara de días**
La máscara utilizada para determinar los días del período de validez.

**Hora de inicio**
La hora de inicio para el período de validez.

**Hora de fin**
La hora de finalización del período de validez.

## Carpeta Perfiles de tráfico

La carpeta Perfiles de tráfico proporciona información sobre los perfiles de tráfico asociados con una política. Contiene los siguientes paneles:

- Perfiles base
- Perfiles de entrada/salida
- Perfiles de identificación remota

**Panel Perfiles base:** El panel Perfiles base proporciona información sobre los perfiles base asociados con una política. Contiene los siguientes campos:

**Nombre de perfil de tráfico**
El nombre del perfil de tráfico.

**Protocolo bajo**
El número del protocolo de bajo nivel.

**Protocolo alto**
El número del protocolo de alto nivel.

**Dirección IP de origen baja**
La dirección IP de origen baja asociada con este perfil.

**Dirección IP de origen alta**
La dirección IP de origen alta asociada con este perfil.

**Puerto de origen alto**
El puerto alto asociado con este perfil.

**Puerto de origen bajo**
El puerto bajo asociado con este perfil.

**Destino de la dirección IP baja**
El destino de la dirección IP baja.

**Destino de la dirección IP alta**
El destino de la dirección IP alta.

**Puerto de destino bajo**
El número del puerto de destino bajo.

**Puerto de destino alto**
El número de puerto de destino alto.

**Máscara de bytes de tipo de servicio**
La máscara de bytes del tipo de servicio.

**Comparación de tipo de servicio**
El valor de la comparación de bytes del tipo de servicio.

**Tipo de identificación local**
El tipo de identificación local.

**Valor de identificación local**
El valor de la identificación local.

**Nombre de grupo de identificación remota**
El nombre del grupo de identificación remota.

**Perfiles de entrada/salida:** La vista proporciona información sobre los perfiles de entrada/salida. Contiene los siguientes campos:

**Nombre de perfil de tráfico**
El nombre del perfil de tráfico.

**Índice de entrada/salida de perfil de tráfico**
El índice del par de interfaz.

**Dirección IP de entrada**
La dirección IP del tráfico de entrada.

**Dirección IP de salida**
La dirección IP del tráfico de salida.

**Panel Perfiles de identificación remota:** Este panel proporciona información sobre las identificaciones remotas asociadas con un perfil de tráfico. Contiene los siguientes campos:

**Nombre de perfil de tráfico**
El nombre del perfil de tráfico.

**Grupo remoto de perfil de tráfico**
El nombre del grupo remoto.

**Índice** El índice de la identificación remota.

**Tipo** El tipo de identificación remota.

**Valor** El valor de la identificación remota

**Modalidad de autentificación**
La modalidad de autentificación utilizada para esta identificación remota.

## Carpeta Acciones

Esta carpeta proporciona información sobre la gestión de claves IPSec, la gestión de datos IPSec, los servicios diferenciales y el protocolo de reserva de recursos (RSVP). Contiene los siguientes elementos dependientes:

- Carpeta IPSec
- Panel Servicios diferenciales
- Panel RSVP

**Carpeta IPSec:** La carpeta IPSec proporciona información sobre la gestión de claves IPSec y la gestión de datos IPSec. Contiene los siguientes elementos dependientes:

- Carpeta Gestión de claves
- Carpeta Gestión de datos

*Carpeta Gestión de claves:* La carpeta Gestión de claves proporciona información sobre la gestión de claves de IPSec. Contiene los siguientes paneles:

- Acciones
- Propuestas
- Acciones a propuestas
- Sesiones activas

*Panel Acciones:* El panel Acciones proporciona información sobre las acciones de gestión de claves. Contiene los siguientes campos:

**Nombre de acción de gestión de claves**
El nombre de la acción de gestión de claves.

**Modalidad de intercambio**
La modalidad de intercambio.

**Duración en segundos de la SA de conexión**
La duración de la Asociación de seguridad de la conexión en segundos.

**Duración en kilobytes de la SA de conexión**
La duración de la asociación de seguridad de la conexión en kilobytes.

**Función de la política**
La función de la política.

**Porcentaje mínimo de renovación**
El porcentaje mínimo de renovación de la asociación de seguridad.

**Inicio automático**
El indicador de inicio automático: verdadero o falso.

**Coincidencias**
El número de coincidencias para esta acción.

*Panel Propuestas:* Este panel proporciona información sobre las propuestas de gestión de claves. Contiene los siguientes campos:

**Nombre de propuesta de gestión de claves**
El nombre de la propuesta de gestión de claves.

**Método de autentificación**
El método de autentificación utilizado para esta propuesta.

**Algoritmo hash**
El nombre del algoritmo hash utilizado para esta propuesta.

**Algoritmo de cifrado**
El nombre del algoritmo de cifrado utilizado para esta propuesta.

**Identificación de grupo Diffie Hellman**
La identificación del grupo diffie hellman de esta propuesta.

**Duración de SA en segundos**
La duración en segundos de la Asociación de seguridad.

**Duración de SA en kilobytes**
La duración en kilobytes de la Asociación de seguridad.

*Panel Acciones a propuestas:* Este panel proporciona información sobre las acciones de claves y las propuestas de claves. Contiene los siguientes campos:

**Nombre de acción de gestión de claves**
El nombre de la acción de gestión de claves.

**Nombre de propuesta**
El nombre de la propuesta de gestión claves

**Orden de propuesta**
El orden de la propuesta de gestión de claves.

**Detalles de acción**
Un resumen de la información del panel Acción. Para obtener más información, consulte el Panel Acciones.

**Detalles de propuestas**
Un resumen de la información del panel Propuestas. Para obtener más información, consulte el Panel Propuestas.

*Panel Sesiones activas:* Este panel proporciona información sobre las sesiones de gestión de claves activas. Contiene los siguientes campos:

**Nombre de acción**
El nombre de la acción de gestión de claves.

**Orden de creación**
El orden en el que se ha creado esta acción.

**Identificación de túnel KM**
La identificación del túnel de gestión de claves.

**Índice de túnel KM**
El índice del túnel de gestión de claves.

**Detalles de acción**
Un resumen de la información del panel Acción. Para obtener más información, consulte el Panel Acciones.

**Estado** El estado del túnel activo: activo o destruir. Los usuarios autorizados pueden modificar este valor desde el panel Sesiones activas.

*Carpeta Gestión de datos IPSec:* Esta carpeta proporciona información sobre la gestión de datos IPSec. Contiene los siguientes elementos dependientes:

- Panel Acciones
- Panel Propuestas
- Panel Sesiones activas
- Carpeta Transformaciones
- Carpeta Correlaciones

*Panel Acciones:* Este panel proporciona información sobre las acciones de gestión de datos IPSec. Contiene los siguientes campos:

**Nombre de acción de gestión de datos**
El nombre de la acción Gestión de datos.

**Tipo** El tipo de acción: permitir o denegar.

**Dirección IP de inicio de túnel**
La dirección IP de inicio del túnel.

**Dirección IP de fin de túnel**
La dirección IP del final del túnel.

**Tipo de proxy local**
El tipo de proxy local.

**Valor de proxy local**
El valor del proxy local.

**Protocolo de proxy local**
El protocolo del proxy local.

**Puerto de origen de proxy local**
El número del puerto de origen de proxy local.

**Tipo de proxy remoto**
El tipo de proxy remoto.

**Valor de proxy remoto**
El valor del proxy remoto.

**Protocolo de proxy remoto**
El protocolo del proxy remoto.

**Puerto de origen de proxy remoto**
El número del puerto de origen del proxy remoto.

**Porcentaje de umbral de renovación de SA**
El umbral de renovación de la asociación de seguridad.

**Porcentaje mínimo de umbral de renovación de SA**
El umbral de renovación mínimo de la asociación de seguridad.

**Túnel en túnel**
El indicador de túnel en túnel.

**Inicio automático**
El valor del inicio automático: habilitar o inhabilitar.

**No fragmentar el manejo de bits**
El indicador de no fragmentar el manejo de bits.

**Prevención de nueva repetición**
El valor de la prevención de una nueva repetición.

**Coincidencias**
El número de coincidencias para esta acción.

*Panel Propuestas:* Este panel proporciona información sobre las propuestas de Gestión de datos. Contiene los siguientes campos:

**Nombre**
El nombre de la acción Gestión de datos.

**Secreto perfecto de reenvío**
El valor del secreto perfecto del reenvío: habilitar o inhabilitar.

**Identificación de grupo Diffie Hellman**
La identificación del grupo diffie hellman.

*Panel Sesiones activas:* Este panel proporciona información sobre las sesiones Gestión de datos activas. Contiene los siguientes campos:

**Acción Gestión de datos**
El nombre de la acción Gestión de datos.

**Orden de creación**
El orden en el que se ha creado la acción Gestión de de datos.

**Identificación de túnel de Gestión de claves**
La identificación del túnel de Gestión de claves.

**Índice de túnel Gestión de datos**
El índice del túnel Gestión de datos.

**Detalles de la acción Gestión de datos**
Resumen del panel Acción Gestión de datos. Para obtener más información, consulte “Panel Acciones” en la página 49.

**Detalles de la acción Gestión de claves**
Resumen del panel Acción Gestión de claves. Para obtener más información, consulte “Panel Acciones” en la página 48.

*Carpeta Transformaciones:* Esta carpeta proporciona información sobre las transformaciones de la Gestión de datos. Contiene los siguientes paneles:

- Transformaciones AH
- Transformaciones ESP
- Transformaciones IPCOMP

*Panel Transformaciones AH:* Este panel proporciona información sobre las transformaciones de la cabecera de autentificación (AH). Contiene los siguientes campos:

**Nombre de transformación AH**
El nombre de la transformación de cabecera de autentificación.

**Algoritmo de encapsulación**
El algoritmo de encapsulación utilizado por la transformación AH.

**Algoritmo de integridad**
El algoritmo de integridad utilizado por la transformación AH.

**Duración de SA en segundos**
La duración en segundos de la asociación de seguridad.

**Duración de SA en kilobytes**
La duración en kilobytes de la Asociación de seguridad.

*Panel Transformaciones ESP:* Este panel proporciona información sobre las transformaciones ESP (Carga de seguridad de encapsulación). Contiene los siguientes campos:

**Nombre de transformación ESP**
El nombre de la transformación ESP.

**Algoritmo de encapsulación**
El algoritmo de encapsulación utilizado por la transformación ESP.

**Algoritmo de integridad**
El algoritmo de integridad utilizado por la transformación ESP.

**Duración de SA en segundos**
La duración en segundos de la Asociación de seguridad.

**Duración de SA en kilobytes**
La duración en kilobytes de la Asociación de seguridad.

*Panel Transformaciones de IPCOMP:* Este panel proporciona información sobre las transformaciones de IPCOMP. Contiene los siguientes campos:

**Nombre**
El nombre de la transformación de IPCOMP.

**Algoritmo IPCOMP**
El nombre del algoritmo de compresión.

**Algoritmo de proveedor IPCOMP**
El nombre del algoritmo de proveedor.

**Duración de SA**
La duración en segundos de la Asociación de seguridad.

**Duración de SA en kilobytes**
La duración en kilobytes de la Asociación de seguridad.

*Carpeta Correlación:* Esta carpeta proporciona información sobre la correlación entre las Propuestas de gestión de datos IPSec y las transformaciones activas. Contiene los siguientes paneles:

- Correlación de la propuesta de gestión de datos
- Correlación de AH
- Correlación de ESP
- Correlación de IPCOMP

*Panel Correlación de la propuesta de gestión de datos:* Este panel proporciona información sobre las correlaciones de la Propuesta de gestión de datos. Contiene los siguientes campos:

**Nombre de acción**
El nombre de la acción Gestión de datos.

**Nombre de propuesta**
El nombre de la propuesta Gestión de datos.

**Orden de propuesta**
El orden de la propuesta Gestión de datos.

**Detalles de la acción Gestión de datos**
Resumen del panel Acciones de gestión de datos. Para obtener más información, consulte “Panel Acciones” en la página 49.

**Detalles de la propuesta de gestión de datos**
Resumen del panel Propuestas de gestión de datos. Para obtener más información, consulte “Panel Propuestas” en la página 50.

*Panel Correlación de AH:* Este panel proporciona información sobre las correlaciones de AH (cabecera de autentificación). Contiene los siguientes campos:

**Nombre de propuesta**
El nombre de la propuesta Gestión de datos.

**Nombre de transformación AH**
El nombre de la transformación AH.

**Orden de transformación AH**
El orden de la transformación AH.

**Detalles de la acción Gestión de datos**
Resumen del panel Acciones de gestión de datos. Para obtener más información, consulte “Panel Acciones” en la página 49.

**Detalles de transformación AH**
Resumen del panel Transformación AH. Consulte “Panel Transformaciones AH” en la página 51

*Panel Correlación de ESP:* Este panel proporciona información sobre correlaciones de ESP (Encapsulating Security Payload - Encapsulación de la carga de seguridad). Contiene los siguientes campos:

**Nombre de propuesta**
El nombre de la propuesta Gestión de datos.

**Nombre de transformación ESP**
El nombre de la transformación ESP.

**Orden de transformación ESP**
El orden de la transformación ESP.

**Detalles de la acción Gestión de datos**
Resumen del panel Acciones de gestión de datos. Para obtener más información, consulte “Panel Acciones” en la página 49.

**Detalles de transformación de ESP**
Resumen del panel Transformación de ESP. Consulte “Panel Transformaciones ESP” en la página 51

*Panel Correlación de IPCOMP:* Este panel proporciona información sobre correlaciones de IPCOMP. Contiene los siguientes campos:

**Nombre de propuesta**
El nombre de la propuesta Gestión de datos.

**Nombre de transformación IPCOMP**
El nombre de la transformación de IPCOMP.

**Orden de transformación IPCOMP**
El orden de la transformación IPCOMP.

**Detalles de la acción Gestión de datos**
Un resumen del panel Acciones de gestión de datos. Para obtener más información, consulte “Panel Acciones” en la página 49.

**Detalles de Transformación IPCOMP**
Un resumen del panel Transformación IPCOMP. Consulte “Panel Transformaciones de IPCOMP” en la página 51

*Panel Acciones de servicios diferenciales:* Este panel muestra todas las definiciones de las acciones de servicios diferenciales. Contiene los siguientes campos:

**Nombre de acción de servicios diferenciales**
El nombre de la acción de los servicios diferenciales.

**Permiso**
El valor de permiso para la acción: permitir o denegar.

**Prioridad en cola**
La prioridad cola de la acción en la cola.

**Tipo de ancho de banda**
El tipo de ancho de banda de la acción.

**Compartimiento de ancho de banda**
El compartimiento de ancho de banda de la acción.

**Máscara TOS**
La máscara de bytes del tipo de servicio.

**Coincidencia TOS**
La coincidencia de bytes del tipo de servicio.

**Coincidencias**
El número de coincidencias para esta acción.

*Acciones RSVP:* Este panel muestra todas las definiciones de las acciones RSVP. Contiene los siguientes campos:

**Nombre**
El nombre de la acción RSVP.

**Permiso**
El valor de permiso para la acción: permitir o denegar.

**Velocidad máx/Flujo**
La velocidad máxima por flujo en kilobytes.

**Token-Bucket máximo/flujo**
El token-bucket máximo por flujo.

**Duración máxima de flujo**
La duración máxima del flujo en segundos.

**Retardo mínimo**
El retardo mínimo en segundos.

**Acción Servicios diferenciales**
El nombre de la acción de servicios diferenciales.

**Detalles de la acción Servicios diferenciales**
Un resumen del panel Acción de servicios diferenciales. Para obtener más información, consulte “Panel Acciones de servicios diferenciales” en la página 53.

# Capítulo 11. Carpeta Sucesos de VPN Monitor

La carpeta Sucesos de VPN Monitor proporciona datos sobre la notificación de sucesos realizada por VPN Monitor. Contiene los siguientes elementos dependientes:

- Carpeta Autentificación de Layer-2
- Carpeta Autentificación/Cifrado de IPSec

## Carpeta Autentificación de Layer-2

Esta carpeta proporciona información sobre las autentificaciones de Layer-2 realizadas por el dispositivo supervisado. Contiene los siguientes paneles:

- Estadísticas
- Anotaciones cronológicas de los errores de túnel
- Anotaciones cronológicas de los errores de sesión

### Panel Estadísticas

Este panel proporciona estadísticas sobre las autentificaciones de Layer-2 realizadas por el dispositivo supervisado. Contiene los siguientes campos:

**Éxitos de túnel**
El número de túneles Layer-2 que se han activado.

**Errores de túnel**
El número de túneles Layer-2 que no se han podido autentificar y no se han activado.

**Éxitos de sesión**
El número de sesiones Layer-2 que se han activado.

**Errores de sesión**
El número de sesiones Layer-2 que no se han podido autentificar y no se han activado.

### Panel Anotaciones cronológicas de errores de túnel

Este panel proporciona información acerca de los túneles Layer-2 que no se han podido autentificar y por lo tanto no se han abierto. Contiene los siguientes campos:

**Número de errores**
El número de errores.

**Sistema principal**
El sistema principal correspondiente al túnel fallido.

**Dirección IP**
La dirección IP correspondiente al túnel fallido.

**Hora** La hora del error.

## Panel Anotaciones cronológicas de los errores de sesión

Este panel proporciona información acerca de las sesiones Layer-2 que no se han podido autentificar y que por lo tanto no se han abierto. Contiene los siguientes campos:

**Número de errores**
El número de errores

**Identificación de usuario**
La identificación de usuario asociada con el túnel fallido.

**Hora** La hora del error.

# Carpeta Cifrado/Autentificación de IPSec

Esta carpeta proporciona información acerca de los cifrados y autentificaciones de IPSec realizados por el dispositivo supervisado. Contiene los siguientes paneles:

- Estadísticas
- Anotaciones cronológicas de los errores de IPSec

## Panel Estadísticas

Este panel proporciona estadísticas para los cifrados y autentificaciones de IPSec realizados por el dispositivo supervisado. Contiene los siguientes campos:

**Autentificaciones de entrada**
El número de autentificaciones de entrada de IPSec realizadas.

**Errores de autentificación de entrada**
El número de autentificaciones de entrada de IPSec fallidas.

**Descifrados de entrada**
El número de descifrados de entrada de IPSec realizados.

**Errores de descifrado de entrada**
El número de descifrados de entrada de IPSec fallidos.

**Autentificaciones de salida**
El número de autentificaciones de salida de IPSec realizadas.

**Errores de autentificación de salida**
El número de autentificaciones de salida de IPSec fallidas.

**Cifrados de salida**
El número de cifrados de salida de IPSec realizados.

**Errores de cifrados de salida**
El número de cifrados de salida de IPSec fallidos.

## Panel Anotaciones cronológicas de errores de IPSec

Este panel proporciona información sobre los errores de autentificación y cifrado de IPSec. Contiene los siguientes campos:

**Número de errores**
El número de errores.

**Causa** La causa del error.

**Hora** La hora del error.

**Identificación de túnel**
La identificación de túnel fallido.

**SPI de SA**
El Índice de protección de seguridad de la asociación de seguridad del error.

**Dirección IP de origen**
La dirección IP de origen del error.

**Dirección IP de destino**
La dirección IP de destino del error.

# Capítulo 12. Carpeta operativa de VPN Monitor

Esta carpeta proporciona información sobre el funcionamiento del dispositivo supervisado. Contiene los siguientes elementos dependientes:

- Carpeta Túneles
- Carpeta Clientes
- Carpeta Políticas
- Carpeta LDAP
- Carpeta Rupturas

## Carpeta Túneles

Esta carpeta proporciona posibilidades de visualización y operativas para los tamaños de las tablas históricas y de registro cronológico de Layer-2, túneles Layer-2 activos, túneles de control IPSec activos y túneles de usuario IPSec activos. Contiene los siguientes paneles:

- Tamaño de tablas
- Desactivar túneles Layer-2
- Desactivar túneles de control IPSec
- Desactivar túneles de usuario IPSec

### Panel Tamaño de tablas

Este panel proporciona información sobre los tamaños de las tablas de registro cronológico e históricas de Layer-2. Contiene los siguientes campos:

**Tablas históricas de Layer-2**
El número de entradas a conservar para las sesiones y túneles Layer-2 anteriores. Los usuarios autorizados pueden modificar este valor desde el panel Tamaño de tablas.

**Tablas de errores de autentificación de Layer-2**
El número de entradas a conservar en la tabla Errores de autentificación de Layer-2. Los usuarios autorizados pueden modificar este valor desde el panel Tamaño de tabla.

### Panel Desactivar túneles Layer-2

Este panel permite a los usuarios autorizados desactivar los túneles Layer-2. Contiene los siguientes campos:

**Detalles de los túneles Layer-2 activos**
Un resumen del panel Túneles Layer-2 activos.

**Estado** El desencadenante para destruir un túnel individual. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles Layer-2.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles Layer-2.

## Panel Desactivar túneles de control IPSec

Este panel permite a los usuarios autorizados desactivar los túneles de control IPSec. Contiene los siguientes campos:

**Detalles de los túneles de control IPSec activos**
Un resumen del panel Túneles de control IPSec activos.

**Estado** El desencadenante para destruir un túnel individual. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles de control IPSec.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles de control IPSec.

## Panel Desactivar túneles de usuario IPSec

Este panel permite a los usuarios autorizados desactivar los túneles de usuario IPSec. Contiene los siguientes campos:

**Detalles de los túneles de usuario IPSec activos**
Un resumen del panel Túneles de usuario IPSec activos.

**Estado** El desencadenante para destruir un túnel individual. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles de usuario IPSec.

**Destruir todos los túneles**
El desencadenante para destruir todos los túneles. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar túneles de usuario IPSec.

# Carpeta Clientes

Esta carpeta proporciona posibilidades de visualización y control para las sesiones Layer-2. Contiene los siguientes paneles:

- Desactivar sesiones Layer-2

## Panel Desactivar sesiones Layer-2

Este panel permite a los usuarios autorizados desactivar las sesiones Layer-2. Contiene los siguientes campos:

**Detalles de las sesiones Layer-2 activas**
Un resumen del panel Sesiones Layer-2 activas.

**Estado** El desencadenante para destruir una sesión individual. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar sesiones Layer-2.

**Destruir todas las sesiones**
El desencadenante para destruir todas las sesiones. Los usuarios autorizados pueden modificar este valor desde el panel Desactivar sesiones Layer-2.

## Carpeta Políticas

Esta carpeta proporciona posibilidades de visualización y control para las políticas de dispositivos VPN. Contiene los siguientes paneles:

- Habilitar/Inhabilitar políticas
- Volver a cargar políticas de dispositivos

### Panel Habilitar/Inhabilitar políticas

Este panel permite a los usuarios habilitar o inhabilitar una política de dispositivos seleccionada. Contiene los siguientes campos:

**Detalles de las políticas**
Un resumen del panel Políticas.

**Estado** El desencadenante para habilitar o inhabilitar una política. Los usuarios autorizados pueden modificar este valor desde este panel.

### Panel Volver a cargar políticas de dispositivos

Este panel permite a los usuarios volver a cargar las políticas utilizadas para un dispositivo supervisado. Contiene los siguientes campos:

**Detalles de las definiciones administrativas**
Un resumen de las definiciones administrativas del protocolo LDAP (Lightweight Directory Access Protocol). Para obtener más información, consulte “Panel Parámetros administrativos” en la página 62.

**Detalles de las definiciones operativas**
Un resumen de las definiciones LDAP operativas. Para obtener más información, consulte “Panel Parámetros operativos” en la página 61.

**Volver a cargar políticas**
El desencadenante para volver a cargar las políticas. Los usuarios autorizados pueden volver a cargar las políticas desde este panel.

## Carpeta LDAP

Esta carpeta proporciona posibilidades de visualización y control para los parámetros del protocolo LDAP (Lightweight Directory Access Protocol). Contiene los siguientes paneles:

- Parámetros operativos
- Parámetros administrativos

### Panel Parámetros operativos

Este panel proporciona información sobre los parámetros operativos de LDAP. Contiene los siguientes campos:

**Estado** El estado de la definición: habilitar o inhabilitar.

**Dirección IP del servidor LDAP principal**
La dirección IP del servidor LDAP principal.

**Dirección IP del servidor LDAP secundario**
La dirección IP del servidor LDAP secundario.

**Nivel del servidor LDAP**
El nivel del servidor LDAP.

**Nombre base de la política**
El nombre del objeto base de la política para el dispositivo.

**Puerto** El número de puerto utilizado por el servidor LDAP.

**Tiempo de espera excedido**
El valor del tiempo de espera excedido utilizado por el servidor LDAP.

**Intervalo entre reintentos**
El intervalo entre reintentos utilizado por el servidor LDAP.

**Identificación de usuario**
La identificación de usuario del servidor LDAP.

### Panel Parámetros administrativos

Este panel proporciona control de los parámetros LDAP. Contiene los mismos campos que el panel Parámetros operativos, pero en este panel, los usuarios autorizados pueden modificar el valor de cualquiera de los parámetros.

## Carpeta Rupturas

Esta carpeta proporciona posibilidades de visualización y control para las rupturas VPN. Contiene los siguientes paneles:

- Control de rupturas Layer-2
- Control de rupturas IPSec

### Panel Control de rupturas Layer-2

Este panel proporciona información y control de las rupturas Layer-2 del dispositivo seleccionado. Los usuarios autorizados pueden modificar los valores de todos los campos de este panel. El panel Control de rupturas Layer-2 contiene los siguientes campos:

**Rupturas de inicio de túnel**
El estado del proceso de las rupturas de inicio del túnel: habilitar o inhabilitar.

**Rupturas de paro de túnel**
El estado del proceso de las rupturas de paro del túnel: habilitar o inhabilitar.

**Rupturas de error de autentificación del túnel**
El estado del proceso de las rupturas de error de autentificación del túnel: habilitar o inhabilitar.

**Rupturas de error de autentificación de usuario**
El estado del proceso de las rupturas de error de autentificación de usuario: habilitar o inhabilitar.

### Panel Control de rupturas IPSec

Este panel proporciona información y control de las rupturas IPSec del dispositivo seleccionado. Los usuarios autorizados pueden modificar los valores de todos los campos de este panel. El panel Control de rupturas IPSec contiene los siguientes campos:

**Rupturas de inicio de túnel de control**
El estado del proceso de las rupturas de inicio del túnel de control: habilitar o inhabilitar.

**Rupturas de paro de túnel de control**
El estado del proceso de las rupturas de paro del túnel de control: habilitar o inhabilitar.

**Rupturas de inicio de túnel de datos de usuario**
El estado del proceso de las rupturas de inicio del túnel de datos de usuario: habilitar o inhabilitar.

**Rupturas de paro de túnel de datos de usuario**
El estado del proceso de las rupturas de paro del túnel de datos de usuario: habilitar o inhabilitar.

**Rupturas de errores de autentificación**
El estado del proceso de las rupturas de errores de autentificación: habilitar o inhabilitar.

**Rupturas de errores de descifrado**
El estado del proceso de las rupturas de errores de descifrado: habilitar o inhabilitar.

# Capítulo 13. Carpeta Pruebas de VPN Monitor

Esta carpeta permite a los usuarios probar las políticas, la conectividad y el tiempo de respuesta a y desde sistemas principales. Contiene los siguientes elementos dependientes:

- Panel Prueba de política
- Carpeta Pruebas de Layer-2
- Panel Sondeo remoto

## Panel Prueba de política

Este panel le proporciona la posibilidad de ejecutar pruebas de política y revisar el resultado. Puede iniciar una prueba especificando las direcciones de origen y de destino, los puertos de origen y de destino, el protocolo que se va a utilizar y el tipo de servicio solicitado. Cuando la prueba se ha realizado, se visualizan las políticas y las acciones seleccionadas. El panel Prueba de política contiene los siguientes campos:

**Índice de prueba**
El índice de la prueba.

**Resultado**
El resultado de la prueba.

**Estado** El estado de la entrada de prueba.

**Dirección IP de origen**
La dirección IP de origen que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Puerto de origen**
El puerto de origen que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Dirección IP de destino**
La dirección IP de destino que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Puerto de destino**
El puerto de destino que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Protocolo**
El protocolo que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Byte de TOS**
El byte de tipo de servicio que se va a utilizar en la prueba. Puede modificar este valor aquí.

**Política de claves de gestión**
La política de claves de gestión seleccionada.

**Acción de claves de gestión**
La acción de claves de gestión seleccionada.

**Política de gestión de datos**
La política de gestión de datos seleccionada.

**Acción de gestión de datos**
La acción de gestión de datos seleccionada.

**Política de servicios diferenciales**
La política de servicios diferenciales seleccionada.

**Acción de servicios diferenciales**
La acción de servicios diferenciales seleccionada.

**Política de RSVP**
La política de RSVP seleccionada.

**Acción de RSVP**
La acción de RSVP seleccionada.

# Carpeta Pruebas de Layer-2

Esta carpeta permite comprobar la conectividad y el tiempo de respuesta para los túneles Layer-2. Contiene los siguientes paneles:

- Prueba de conexión de Layer-2
- Prueba del tiempo de respuesta de Layer-2

## Panel Prueba de conexión de Layer-2

Este panel permite comprobar la conectividad potencial de Layer-2 con un sistema principal. Para iniciar la prueba, seleccione el nombre de un sistema principal potencial. Al finalizar la prueba, se muestra la disponibilidad de la conexión. Este panel contiene los siguientes campos:

**Índice de prueba**
El índice de la prueba.

**Sistema principal**
El sistema principal cuya conectividad se va a probar. Puede modificar este valor aquí.

**Resultado**
El resultado de la prueba.

**Tipo de túnel**
El tipo de túnel utilizado para la prueba.

## Panel Prueba del tiempo de respuesta de Layer-2

Este panel permite comprobar el tiempo de respuesta de un sistema principal activo. Para iniciar la prueba, seleccione el nombre de un sistema principal activo. Al finalizar la prueba, se muestra el tiempo de ida y vuelta de un paquete dirigido al sistema principal seleccionado. Este panel contiene los siguientes campos:

**Índice de prueba**
El índice de la prueba.

**Sistema principal**
El sistema principal cuya conectividad se va a comprobar. Puede modificar este valor aquí.

**Resultado**
El resultado de la prueba.

**Tiempo de ida y vuelta**
El tiempo de ida y vuelta del paquete de prueba.

## Panel Sondeo remoto

Esta panel permite comprobar el tiempo de respuesta desde el dispositivo VPN actual hasta otro dispositivo. Para iniciar el sondeo, especifique la dirección IP del sistema principal remoto, el tamaño del paquete y el valor de tiempo de espera excedido que se va a utilizar para la prueba. Al finalizar la prueba, se muestra el tiempo de ida y vuelta de un paquete dirigido al sistema principal. Este panel contiene los siguientes campos:

**Dirección IP**
La dirección IP a sondear. Puede modificar este valor aquí.

**Tamaño de paquete**
El tamaño del paquete que se va a utilizar para el sondeo. Puede modificar este valor aquí.

**Valor de tiempo de espera excedido**
El valor de tiempo de espera excedido que se va a utilizar para el sondeo. Puede modificar este valor aquí.

**Resultado**
El resultado del sondeo.

**Tiempo de sondeo**
El tiempo de ida y vuelta de la prueba.

# Apéndice A. Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los EE.UU. IBM puede no ofrecer los productos, servicios o dispositivos tratados en este documento en otros países. Si desea obtener información sobre los productos y servicios disponibles actualmente en su localidad, consulte a su representante local de IBM.

Las referencias que se hacen en esta publicación a productos, programas y servicios de IBM no implican que IBM tenga la intención de comercializarlos en todos los países en los que realiza operaciones. Las referencias a productos, programas o servicios de IBM no implican que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere los derechos de propiedad intelectual de IBM. Son responsabilidad del usuario la verificación y la evaluación del funcionamiento junto con otros productos, excepto aquéllos expresamente indicados por IBM.

IBM puede tener patentes o solicitudes de patente pendientes que afecten a los temas tratados en este documento. La posesión de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar sus consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Para realizar consultas sobre licencias referentes a la información de doble byte (DBCS), póngase en contacto con el Departamento para la Propiedad Intelectual de IBM de su país, o envíe sus consultas por escrito a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en el que estas disposiciones sean incoherentes con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA ÍNDOLE, TANTO EXPLÍCITAS COMO IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VIOLACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN OBJETIVO CONCRETO. Algunos estados no permiten la exclusión o limitación de garantías ni implícitas ni explícitas en determinadas transacciones, por lo que la exclusión o limitación antes mencionada puede no aplicársele en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información que contiene está sujeta a modificaciones periódicas, las cuales se van incorporando en ediciones posteriores. IBM puede realizar mejoras y/o cambios en los productos y programas descritos en esta publicación en cualquier momento sin previo aviso.

Las referencias que se hacen en esta información a páginas Web que no pertenecen a IBM se proporcionan sólo por conveniencia y no sirven de ningún modo como aval de dichas páginas Web. El material de dichas páginas Web no forma parte del material de este producto de IBM y si utiliza dichas páginas Web es por su cuenta y riesgo.

## Marcas registradas

Los siguientes términos son marcas registradas de IBM Corporation en los EE.UU. y/o en otros países:

| | |
|---|---|
| DB2 | IBM |
| Nways | DB2 Universal Database |

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en los EE.UU. y/o en otros países.

Microsoft, Windows, Windows NT y los logotipos de Windows 95 y Windows 98 son marcas registradas de Microsoft Corporation.

Pentium es una marca registrada de Intel Corporation en los EE.UU. y en otros países.

Netfinity es una marca registrada de Tivoli Systems, Inc. en los EE.UU. y/o en otros países.

UNIX es una marca registrada en los EE.UU. y en otros países bajo licencia exclusiva a través de X/Open Company Limited.

Freelance Graphics es una marca registrada de Lotus Development Corporation en los EE.UU. y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otros fabricantes.

# Hoja de Comentarios

**Nways Manager**
**Guía del usuario de Nways VPN Manager**

**Número de Publicación GA10-5244-00**

**En general, ¿está Ud. satisfecho con la información de este libro?**

| | Muy satisfecho | Satisfecho | Normal | Insatisfecho | Muy insatisfecho |
|---|---|---|---|---|---|
| Satisfacción general | □ | □ | □ | □ | □ |

**¿Cómo valora los siguientes aspectos de este libro?**

| | Muy bien | Bien | Acep-table | Insatisfecho | Muy insatisfecho |
|---|---|---|---|---|---|
| Organización | □ | □ | □ | □ | □ |
| Información completa y precisa | □ | □ | □ | □ | □ |
| Información fácil de encontrar | □ | □ | □ | □ | □ |
| Utilidad de las ilustraciones | □ | □ | □ | □ | □ |
| Claridad de la redacción | □ | □ | □ | □ | □ |
| Calidad de la edición | □ | □ | □ | □ | □ |
| Adaptación a los formatos, unidades, etc. del país | □ | □ | □ | □ | □ |

**Comentarios y sugerencias:**

Nombre

Dirección

Compañía u Organización

Teléfono

**Hoja de Comentarios**
GA10-5244-00

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

GA10-5244-00

Corte o Doble
Por la Línea

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GA10-5244-00