

Configuración de un Concentrador VPN 5000 de Cisco con autenticación externa en un servidor IAS RADIUS de Microsoft Windows 2000.

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración del concentrador VPN 5000 de Cisco](#)

[Configure al servidor de RADIUS de IAS del Microsoft Windows 2000](#)

[Verifique el resultado](#)

[Configure el cliente VPN](#)

["Registros del concentrador"](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe los procedimientos usados para configurar un concentrador del Cisco VPN 5000 con la autenticación externa a un Internet Authentication Server del Microsoft Windows 2000 (IAS) con el RADIUS.

Nota: El Challenge Handshake Authentication Protocol (CHAP) no trabaja. Utilice solamente el protocolo password authentication (PAP). Refiera al Id. de bug Cisco [CSCdt96941](#) ([clientes registrados solamente](#)) para otros detalles.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Versión concentrador software 6.0.16.0001 del Cisco VPN 5000

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Configuración del concentrador VPN 5000 de Cisco

```
VPN5001_4B9CBA80
VPN5001_4B9CBA80> show config Enter Password: Edited
Configuration not Present, using Running [ General ]
EthernetAddress = 00:02:4b:9c:ba:80 DeviceType = VPN
5001 Concentrator ConfiguredOn = Timeserver not
configured ConfiguredFrom = Command Line, from Console
EnablePassword = Password = [ IP Ethernet 0 ] Mode =
Routed SubnetMask = 255.255.255.0 IPAddress =
172.18.124.223 [ IP Ethernet 1 ] Mode = Off [ IKE Policy
] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ]
BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet
= 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0 [
RADIUS ] BindTo = "ethernet0" ChallengeType = PAP
PAPAuthSecret = "pappassword" PrimAddress =
"172.18.124.108" Secret = "radiuspassword" UseChap16 =
Off Authentication = On [ Logging ] Level = 7 Enabled =
On Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

Configure al servidor de RADIUS de IAS del Microsoft Windows 2000

Estos pasos le dirigen con una configuración de servidor de RADIUS simple de IAS del Microsoft Windows 2000.

1. Bajo propiedades IAS del Microsoft Windows 2000, los **clientes** selectos y crean a un nuevo cliente. En este ejemplo, una entrada nombrada VPN5000 se crea. La dirección IP del concentrador del Cisco VPN 5000 es 172.18.124.223. Bajo la casilla desplegable de Client Vendedor, seleccione **Cisco**. El secreto compartido es el secreto en la sección del [RADIUS] de la configuración del [concentrador VPN](#).
2. Bajo propiedades de la política de acceso remoto, seleccione a **Grant que el Permiso de acceso remoto** bajo "si un usuario hace juego las condiciones" sección y después hace clic **edita el perfil**.
3. Haga clic la lengüeta de la autenticación y asegúrese que esa solamente **autenticación Unencrypted (PAP, SPAP)** está seleccionado.
4. Seleccione la ficha Avanzadas, el tecleo **agrega** y selecciona **específico del vendedor**.
5. Conforme al cuadro de diálogo polivalente de la información de atributo para el atributo específico del proveedor, el tecleo **agrega** para ir al cuadro de diálogo Vendor Specific Attribute Information. Selecto **ingrese Vendor Code (Código de proveedor)** y ingrese **255** en el rectángulo adyacente. Siguiente, seleccione **sí. Él conforma** y el **atributo de la**

configuración del teclado.

6. Conforme al cuadro de diálogo de la configuración VSA (conforme a RFC), ingrese **4** para el número de atributo Vendedor-asignado, ingrese la **cadena** para el formato de atributo, y ingrese el **RTP-grupo** (nombre del grupo VPN en el concentrador del Cisco VPN 5000) por el valor de atributo. Haga Click en OK y relanza el paso 5.
7. Conforme al cuadro de diálogo de la configuración VSA (conforme a RFC), ingrese **4** para el número de atributo Vendedor-asignado, ingrese la **cadena** para el formato de atributo, y ingrese el **cisco123** (el secreto compartido con el cliente) por el valor de atributo. Haga clic en OK.
8. Usted ve que el atributo específico del proveedor contiene dos valores (grupo y contraseña de VPN).
9. Bajo sus propiedades del usuario, haga clic el dial-in tab y asegúrese de que el **acceso del control con la política de acceso remoto** está seleccionado.

Verifique el resultado

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre a Visualizaciones de estadísticas del radio** las estadísticas de paquete para la comunicación entre el concentrador VPN y el servidor del RADIUS predeterminado identificados por la sección RADIUS.
- **muestre los config del radio** — Muestra las configuraciones actuales para los parámetros de RADIUS.

Ésta es la salida del **comando show radius statistics**.

```
VPN5001_4B9CBA80>show radius statistics RADIUS Stats Accounting Primary Secondary Requests 0 na Responses 0 na Retransmissions 0 na Bad Authenticators 0 na Malformed Responses 0 na Packets Dropped 0 na Pending Requests 0 na Timeouts 0 na Unknown Types 0 na Authentication Primary Secondary Requests 3 na Accepts 3 na Rejects 0 na Challenges 0 na Retransmissions 0 na Bad Authenticators 0 na Malformed Responses 0 na Packets Dropped 0 na Pending Requests 0 na Timeouts 0 na Unknown Types 0 na VPN5001_4B9CBA80>
```

Ésta es la salida del **comando show radius config**.

```
RADIUS      State      UDP  CHAP16
Authentication  On        1812 No
Accounting      Off        1813 n/a
Secret          'radiuspassword'

Server      IP address      Attempts  AcctSecret
Primary     172.18.124.108      5      n/a
Secondary   Off
```

Configure el cliente VPN

Este procedimiento le dirige con la configuración del cliente VPN.

1. Del cuadro de diálogo del cliente VPN, seleccione la ficha de configuración. Después, del Cliente-prompt VPN para el cuadro de diálogo secreto, ingrese el secreto compartido bajo el

servidor VPN. El secreto compartido cliente VPN es el valor ingresado para la contraseña de VPN del atributo 5 en el concentrador VPN.

2. Después de que usted ingrese el secreto compartido, le indican para una contraseña y un secreto de autenticación. La contraseña es su contraseña de radius para ese usuario, y el secreto de autenticación es el secreto de la autenticación PAP en la sección del `[RADIUS]` del [concentrador VPN](#).

“Registros del concentrador”

```
Notice 4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar
Debug 4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108
Debug 4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contacting
server
Notice 4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108.
Debug 4088.8 seconds Client's local broadcast address = 172.18.124.255
Notice 4088.8 seconds User assigned IP address 10.1.1.1
Info 4094.49 seconds Command loop started from 10.1.1.1 on PTY2
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco](#)
- [Página de soporte del concentrador VPN 5000 de Cisco](#)
- [Página de soporte para Cisco VPN 5000 Client](#)
- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)