Router IOS como Easy VPN Server usando el ejemplo de configuración del profesional de la configuración

Contenido

Introducción

Este documento describe cómo configurar a un router del ® del Cisco IOS como servidor fácil VPN (EzVPN) usando el Cisco Configuration Professional (Cisco CP) y el CLI. La función Easy VPN Server permite a un usuario final remoto comunicarse mediante IP Security (IPsec) con cualquier gateway de Red privada virtual (VPN) de Cisco IOS. Las políticas IPSec administradas de manera centralizada se envían al dispositivo cliente mediante el servidor, lo que minimiza la configuración que debe realizar el usuario final.

Para más información sobre el Easy VPN Server refiera a la sección del Easy VPN Server de la biblioteca de la guía de configuración de la conectividad segura, Cisco IOS Release 12.4T.

prerrequisitos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 1841 Router con el Cisco IOS Software Release 12.4(15T)
- Versión 2.1 de Cisco CP

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.

Instale Cisco CP

Realice estos pasos para instalar Cisco CP:

1. Descargue Cisco CP V2.1 del centro del software de Cisco (clientes registrados solamente) y instalelo en su PC local.La última versión de Cisco CP se puede encontrar en el sitio web de Cisco CP.
2. Inicie Cisco CP de su PC local a través **Start > Programs >** el **Cisco Configuration Professional (CCP)** y elija a la **comunidad** que tiene el router que usted quiere configurar.
3. Para descubrir el dispositivo que usted quiere configurar, resaltar al router y el tecleo **descubre**.

Nota: Para la información sobre los modelos y las versiones del IOS del router Cisco que son compatibles a Cisco CP v2.1, refiera a la sección compatible de las versiones del Cisco IOS.

Nota: Para la información sobre los requisitos PC que ejecuta Cisco CP v2.1, refiera a la sección de los requisitos del sistema.

Configuración del router para ejecutar Cisco CP

Realice estos pasos para la configuración para ejecutar Cisco CP en un router Cisco:

1. Conecte con su router que usa Telnet, SSH, o a través de la consola.Ingrese al modo de configuración global que usa este comando:`Router(config)#`**`enable`** `Router(config)#`
2. Si el HTTP y el HTTPS se habilitan y se configuran para utilizar los números del puerto no estándar, usted puede saltar este paso y utilizar simplemente el número del puerto configurado ya.Habilite el router HTTP o al servidor HTTPS que usa estos comandos del Cisco IOS Software:`Router(config)#` **`ip http server`** `Router(config)#` **`ip http secure-server`** `Router(config)#` **`ip http authentication local`**
3. Cree a un usuario con el nivel de privilegio 15:`Router(config)#` **`username`** *`<username>`* **`privilege 15 password 0`** *`<password>`* **Nota:** ***<username>*** y ***<password>*** *del* reemplace con el nombre de usuario y contraseña que usted quiere configurar.
4. Configuración SSH y Telnet para la conexión local y el nivel de privilegio 15.`Router(config)#` **`line vty 0 4`** `Router(config-line)#` **`privilege level 15`** `Router(config-line)#` **`login local`** `Router(config-line)#` **`transport input telnet`** `Router(config-line)#` **`transport input telnet ssh`** `Router(config-line)#` **`exit`**
5. Registro local (opcional) del permiso para soportar la función de supervisión del registro:`Router(config)#` **`logging buffered 51200 warning`**

Requisitos

Este documento asume que el router Cisco está completamente - operativo y configurado para permitir que Cisco CP realice los cambios de configuración.

Para toda la información sobre cómo comenzar a usar Cisco CP, refiera a la introducción con el Cisco Configuration Professional.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección, le presentan con la información para configurar las configuraciones básicas para un router en una red.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Cisco CP - Configuración del Easy VPN Server

Realice estos pasos para configurar al router del Cisco IOS como Easy VPN Server:

1. Elija el > Security (Seguridad) de la **configuración** > el **VPN** > el **Easy VPN Server** > **crean el Easy VPN Server** y hacen clic al **Asisitente del Easy VPN Server del lanzamiento** para configurar al router del Cisco IOS como Easy VPN Server:
2. Haga clic **después** para proceder con la configuración del **Easy VPN Server**.
3. En la ventana resultante, una **interfaz virtual** será configurada como parte de la configuración del Easy VPN Server. Proporcione la **dirección IP de la interfaz del túnel virtual** y también elija el **método de autentificación** usado para autenticar a los clientes VPN. Aquí, las **claves previamente compartidas** son el método de autentificación usado. Tecleo **después**:
4. Especifique el **algoritmo de encripción, el algoritmo de autenticación y el método del intercambio de claves** que se utilizará por este router al negociar con el dispositivo remoto. Una política IKE predeterminada está presente en el router que puede ser utilizado si procede. Si usted quiere agregar una nueva política IKE, haga click en Add
5. Proporcione el **algoritmo de encripción**, el **algoritmo de autenticación**, y el **método del intercambio de claves** como se muestra aquí, después haga clic la **AUTORIZACIÓN**:
6. **La política IKE predeterminada** se utiliza en este ejemplo. Como consecuencia, elija la política IKE predeterminada y haga clic **después**.
7. En la nueva ventana, los detalles **determinados de la transformación** deben ser proporcionados. El conjunto de la transformación especifica el **cifrado** y los **algoritmos de autenticación** usados para proteger los **datos en el VPN hacen un túnel**. El tecleo **agrega** para proporcionar estos detalles. Usted puede agregar cualquier número de conjuntos

Transform según las necesidades cuando usted tecleo **agrega** y proporciona los detalles.**Nota: El valor por defecto CP transforma el conjunto** está presente por abandono en el router cuando está configurado usando **Cisco CP**.

8. Proporcione la **transformación los** detalles **determinados** (**cifrado y algoritmo de autenticación**) y haga clic la **AUTORIZACIÓN**.
9. **El valor por defecto transforma el valor por defecto** nombrado **conjunto CP transforma el conjunto** se utiliza en este ejemplo. Como consecuencia, elija el valor por defecto transforman el conjunto y hacen clic **después**.
10. En la nueva ventana, elija el servidor en el cual las directivas del grupo serán configuradas que pueden ser **Local** o **RADIUS** o **Local y RADIUS**. En este ejemplo, utilizamos al **servidor local** para configurar las directivas del grupo. Elija el **Local** y haga clic **después**.
11. Elija el servidor que se utilizará para la autenticación de usuario en esta nueva ventana que pueda ser **Local solamente** o **RADIUS** o **Local solamente y RADIUS**. En este ejemplo utilizamos al **servidor local** para configurar los credenciales de usuario para la autenticación. Aseegurese la casilla de verificación al lado de la **autenticación de usuario del permiso** se marca. Elija el **Local solamente** y haga clic **después**.
12. El tecleo **agrega** para crear una nueva directiva del grupo y para agregar a los usuarios remotos en este grupo.
13. En la **ventana de la política del grupo del agregar**, proporcione el nombre del grupo en el espacio preven el **nombre de este grupo** (**Cisco** en este ejemplo) junto con la **clave previamente compartida**, y la información de la **agrupación IP** (la **dirección IP que comienza** y **dirección IP de la terminación**) como se muestra y la **AUTORIZACIÓN del** tecleo.**Nota:** Usted puede crear a una nueva agrupación IP o utilizar a una agrupación IP existente si presente.
14. Ahora elija la nueva **directiva del grupo** creada con el nombre **Cisco** y después haga clic la casilla de verificación al lado del **temporizador de inactividad de la configuración** como se requiere en la orden para configurar el **temporizador de inactividad**. Haga clic en Next (Siguiente).
15. Habilite **Cisco que hace un túnel el Control Protocol** (cTCP) si procede. Si no, haga clic **después**.
16. Revise el **resumen de la configuración**. Haga clic en Finish (Finalizar).
17. En la **configuración de la entrega a la ventana del router**, el tecleo **entrega** para entregar la configuración al router. Usted puede hacer clic en **para salvar para clasifiar** para salvar la configuración como archivo en el PC.
18. **La ventana de estado de la salida del comando** muestra el estatus de la salida de los comandos al router. Aparece como **configuración entregada al router**. Haga clic en OK.
19. Usted puede ver el Easy VPN Server creado recientemente. Usted puede editar al servidor existente eligiendo **edita el Easy VPN Server**. Esto completa la configuración del Easy VPN Server en el router del Cisco IOS.

Configuración de CLI

Configuración del router

```
Router#show run Building configuration... Current
configuration : 2069 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption hostname
Router boot-start-marker boot-end-marker no logging
buffered enable password cisco !---AAA enabled using aaa
```

```
newmodel command. Also AAA Authentication and
Authorization are enabled---! aaa new-model ! ! aaa
authentication login ciscocp_vpn_xauth_ml_1 local aaa
authorization network ciscocp_vpn_group_ml_1 local ! !
aaa session-id common ip cef ! ! ! ! ip domain name
cisco.com ! multilink bundle-name authenticated ! ! !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and Policy details
are hidden as the default values are chosen. crypto
isakmp policy 1 encr 3des authentication pre-share group
2 crypto isakmp keepalive 10 ! crypto isakmp client
configuration group cisco key cisco123 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1 match
identity group cisco client authentication list
ciscocp_vpn_xauth_ml_1 isakmp authorization list
ciscocp_vpn_group_ml_1 client configuration address
respond virtual-template 1 ! ! !--- Configuration for
IPsec policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set ESP-3DES-SHA
esp-3des esp-sha-hmac ! crypto ipsec profile
CiscoCP_Profile1 set security-association idle-time
86400 set transform-set ESP-3DES-SHA set isakmp-profile
ciscocp-ike-profile-1 ! ! ! !--- RSA certificate
generated after you enable the !--- ip http secure-
server command. crypto pki trustpoint TP-self-signed-
1742995674 enrollment selfsigned subject-name cn=IOS-
Self-Signed-Certificate-1742995674 revocation-check none
rsakeypair TP-self-signed-1742995674 !--- Create a user
account named cisco123 with all privileges. username
cisco123 privilege 15 password 0 cisco123 archive log
config hidekeys ! ! !--- Interface configurations are
done as shown below---! interface Loopback0 ip address
10.10.10.10 255.255.255.0 ! interface FastEthernet0/0 ip
address 10.77.241.111 255.255.255.192 duplex auto speed
auto ! interface Virtual-Template1 type tunnel ip
unnumbered Loopback0 tunnel mode ipsec ipv4 tunnel
protection ipsec profile CiscoCP_Profile1 ! !--- VPN
pool named SDM_POOL_1 has been defined in the below
command---! ip local pool SDM_POOL_1 192.168.1.1
192.168.1.254 !--- This is where the commands to enable
HTTP and HTTPS are configured. ip http server ip http
authentication local ip http secure-server ! ! ! !
control-plane ! line con 0 line aux 0 !--- Telnet
enabled with password as cisco. line vty 0 4 password
cisco transport input all scheduler allocate 20000 1000
! ! ! ! end
```

Verificación

Easy VPN Server - comandos show

Use esta sección para confirmar que su configuración funciona correctamente.

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.`Router#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status 10.77.241.111 172.16.1.1 QM_IDLE 1003 0 ACTIVE`

- **muestre IPSec crypto sa** — Muestra todo el SA de IPSec actual en un par.
```
Router#show crypto ipsec sa interface: Virtual-Access2 Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0) current_peer 172.16.1.1 port 1086 PERMIT, flags={origin_is_acl,} #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28 #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 2 local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0 current outbound spi: 0x186C05EF(409732591) inbound esp sas: spi: 0x42FC8173(1123844467) transform: esp-3des esp-sha-hmac
```

Troubleshooting

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte información importante en los comandos debug antes de ejecutar los comandos debug.

Información Relacionada

- IPSec Negotiation/IKE Protocols
- Guía de inicio rápido del Cisco Configuration Professional
- Páginas de Soporte de Productos de Cisco - Routers
- Soporte Técnico y Documentación - Cisco Systems