Configuración de un Túnel VPN de Sitio a Sitio entre Cisco RV320 Gigabit Dual WAN VPN Router y Cisco 500 Series Integrated Services Adapter

Objetivo

Una red privada virtual (VPN) existe como una tecnología ampliamente utilizada para conectar redes remotas a una red privada principal, simulando un enlace privado en forma de canal cifrado a través de líneas públicas. Una red remota puede conectarse a una red principal privada como si existiera como parte de la red principal privada sin problemas de seguridad debido a una negociación de dos fases que cifra el tráfico VPN de una manera que sólo los terminales VPN sepan cómo descifrarlo.

Esta breve guía proporciona un diseño de ejemplo para construir un túnel VPN IPsec de sitio a sitio entre un Cisco 500 Series Integrated Services Adapter y un Cisco RV Series Router.

Dispositivos aplicables

Routers · de la serie RV de Cisco (RV320) Adaptadores de servicios integrados · Cisco serie 500 (ISA570)

Versión del software

·4.2.2.08 [Cisco RV0xx Series VPN Routers]

Preconfiguración

Diagrama de la red A continuación se muestra una topología VPN de sitio a sitio.



Se configura y establece un túnel VPN IPsec de sitio a sitio entre el router de la serie RV de Cisco en la oficina remota y el ISA de la serie 500 de Cisco en la oficina principal. Con esta configuración, un host en LAN 192.168.1.0/24 en la oficina remota y un host en LAN 10.10.10.0/24 en la oficina principal pueden comunicarse entre sí de forma segura a través de VPN.

Conceptos básicos

Intercambio de claves de Internet (IKE)

Internet Key Exchange (IKE) es el protocolo utilizado para configurar una asociación de seguridad (SA) en el conjunto de protocolos IPsec. IKE se basa en el protocolo Oakley, la Asociación de seguridad de Internet y el protocolo de administración de claves (ISAKMP), y utiliza un intercambio de claves Diffie-Hellman para configurar un secreto de sesión compartido, del que se derivan claves criptográficas.

Asociación de seguridad de Internet y protocolo de gestión de claves (ISAKMP)

La Asociación de seguridad de Internet y el protocolo de gestión de claves (ISAKMP) se utilizan para negociar el túnel VPN entre dos terminales VPN. Define los procedimientos de autenticación, comunicación y generación de claves, y es utilizado por el protocolo IKE para intercambiar claves de cifrado y establecer la conexión segura.

Seguridad de protocolo de Internet (IPsec)

IP Security Protocol (IPsec) es un conjunto de protocolos para proteger las comunicaciones IP mediante la autenticación y el cifrado de cada paquete IP de un flujo de datos. IPSec también incluye protocolos para establecer la autenticación mutua entre agentes al comienzo de la sesión y la negociación de claves criptográficas que se utilizarán durante la sesión. IPSec se puede utilizar para proteger los flujos de datos entre un par de hosts, gateways o redes.

Consejos de diseño

Topología VPN: una topología VPN punto a punto significa que se configura un túnel IPsec seguro entre el sitio principal y el sitio remoto.

Las empresas a menudo requieren varios sitios remotos en una topología de varios sitios e implementan una topología VPN de hub y radio o una topología VPN de malla completa. Una topología VPN hub-and-spoke significa que los sitios remotos no requieren comunicación con otros sitios remotos, y cada sitio remoto sólo establece un túnel IPsec

seguro con el sitio principal. Una topología VPN de malla completa significa que los sitios remotos requieren comunicación con otros sitios remotos, y cada sitio remoto establece un túnel IPsec seguro con el sitio principal y todos los demás sitios remotos.

Autenticación VPN: el protocolo IKE se utiliza para autenticar a los peers VPN al establecer un túnel VPN. Existen varios métodos de autenticación IKE, y la clave previamente compartida es el método más conveniente. Cisco recomienda aplicar una clave previamente compartida sólida.

Cifrado VPN: para garantizar la confidencialidad de los datos transportados a través de VPN, se utilizan algoritmos de cifrado para cifrar la carga útil de los paquetes IP. DES, 3DES y AES son tres estándares de cifrado comunes. AES se considera el más seguro en comparación con DES y 3DES. Cisco recomienda encarecidamente aplicar cifrado AES-128 bits o superior (por ejemplo, AES-192 y AES-256). Sin embargo, los algoritmos de cifrado más fuertes requieren más recursos de procesamiento de un router.

Dirección IP de WAN dinámica y servicio dinámico de nombres de dominio (DDNS): el túnel VPN debe establecerse entre dos direcciones IP públicas. Si los routers WAN reciben direcciones IP estáticas del proveedor de servicios de Internet (ISP), el túnel VPN se puede implementar directamente mediante direcciones IP públicas estáticas. Sin embargo, la mayoría de las pequeñas empresas utilizan servicios de Internet de banda ancha rentables como DSL o cable, y reciben direcciones IP dinámicas de sus ISP. En estos casos, se puede utilizar el servicio de nombres de dominio dinámicos (DDNS) para asignar la dirección IP dinámica a un nombre de dominio completo (FQDN).

Dirección IP LAN: la dirección de red IP LAN privada de cada sitio no debe tener superposiciones. La dirección de red IP de LAN predeterminada en cada sitio remoto siempre debe cambiarse.

Consejos de Configuración

Lista de comprobación previa a la configuración

Paso 1. Conecte un cable Ethernet entre el RV320 y su módem DSL o por cable y conecte un cable Ethernet entre el ISA570 y su módem DSL o por cable.

Paso 2. Encienda el RV320 y, a continuación, conecte PC internos, servidores y otros dispositivos IP a los puertos LAN del RV320.

Paso 3. Active ISA570 y, a continuación, conecte PC internos, servidores y otros dispositivos IP a los puertos LAN del ISA570.

Paso 4. Asegúrese de configurar las direcciones IP de red en cada sitio en diferentes subredes. En este ejemplo, la LAN de oficina remota utiliza 192.168.1.0 y la LAN de oficina principal utiliza 10.10.10.0.

Paso 5. Asegúrese de que los PC locales pueden conectarse a sus respectivos routers y con otros PC de la misma LAN.

Identificación de la conexión WAN

Deberá saber si el ISP proporciona una dirección IP dinámica o una dirección IP estática. El ISP normalmente proporciona una dirección IP dinámica, pero debe confirmarlo antes de completar la configuración del túnel VPN de sitio a sitio.

Configuración del Túnel VPN IPsec de Sitio a Sitio para RV320 en la Oficina Remota

Paso 1. Vaya a VPN > Gateway-to-Gateway (consulte la imagen)

r.) Introduzca un nombre de túnel, como RemoteOffice.

b) Establezca la interfaz en WAN1.

c.) Establezca Keying Mode en IKE con la clave previamente compartida.

d.) Introduzca la dirección IP local y la dirección IP remota.

La siguiente imagen muestra la página Puerta de enlace a puerta de enlace del router VPN Dual WAN RV320 Gigabit:

CISCO RV320 Gi	gabit Dual WAN VPN F	Router		
Getting Started System Summary	Gateway to Gateway			
▶ Setup	Add a New Tunnel			
▶ DHCP	Tunnel No.	2		
System Management Port Management	Tunnel Name:			
▶ Firewall	Interface:	WAN1	¥	
VPN Summary Gateway to Gateway	Keying Mode:	IKE with Preshared key	~	
Client to Gateway VPN Passthrough PPTP Server	Local Group Setup			
 Certificate Management 	Local Security Gateway Type:	IP Only		v
 Log SSL VPN 	IP Address:	0.0.0.0		
User Management	Local Security Group Type:	Subnet	¥	
Wizard	IP Address:	192.168.1.0		
	Subnet Mask:	255.255.255.0		
	Remote Group Setup			
	Remote Security Gateway Type:	IP Only		V
	IP Address 🗸 :			
	Remote Security Group Type:	Subnet	V	
	IP Address:			
© 2013 Cisco Systems, Inc. All Ri	ights Reserved.			

Paso 2. Configuración de la configuración del túnel IPSec (consulte la imagen)

- r.) Establezca *Encryption* en 3DES.
- b) Establezca Authentication en SHA1.
- c.) Marque Perfect Forward Secrecy.
- d.) Configure la *clave precompartida* (debe ser la misma en ambos routers).

A continuación se muestra la configuración IPSec (Fase 1 y 2):

IPSec Setup		
Phase 1 DH Group:	Group 2 - 1024 bit 🗸	
Phase 1 Encryption :	3DES 🗸	
Phase 1 Authentication:	SHA1	
Phase 1 SA Lifetime:	600	sec (Range: 120-86400, Default: 28800)
Perfect Forward Secrecy:	✓	
Phase 2 DH Group:	Group 2 - 1024 bit 🗸	
Phase 2 Encryption:	3DES 🗸	
Phase 2 Authentication:	SHA1 V	
Phase 2 SA Lifetime:	600	sec (Range: 120-28800, Default: 3600)
Minimum Preshared Key Complexity:	Enable	
Preshared Key:	Aa1234567890!@#\$%^&*()_+	
Preshared Key Strength Meter:		
Advanced +		

Nota: Tenga en cuenta que la configuración del túnel IPsec en ambos lados del túnel VPN IPsec de sitio a sitio debe coincidir. Si existe alguna discrepancia entre la Configuración de Túnel IPSec del RV320 y el ISA570, ambos dispositivos no podrán negociar la clave de cifrado y no podrán conectarse.

Paso 3. Haga clic en Guardar para completar la configuración.

Configuración del Túnel VPN IPSec de Sitio a Sitio para ISA570 en la Oficina Principal

Paso 1. Vaya a VPN > IKE Policies (consulte la imagen)

r.) Establezca *Encryption* en ESP_3DES.

- b) Establezca Hash en SHA1.
- c.) Establezca Authentication en Pre-shared Key.
- d.) Establezca Grupo D-H en Grupo 2 (1024 bits).

La siguiente imagen muestra las políticas IKE:

ututh Small Business	nfiguration L Itility				
Configuration Wizards	IKE Policies				
Status	IKE Policies				
Networking	Add X Delete				
Firewall		Encryption	Hash	Authentication	D-H Group
Security Services	Defaultike	AFS 256	9441		aroup 2
VPN		3DES IKE Policy - Ar	1d/Edit	Help	group_2
 VPN Status IPsec VPN Status SSL VPN Status Stet-to-Site IPsec Policies IRE Policies Transform Sets IPsec Remote Access SSL Remote User Access Teleworker VPN Client 12TE Server 		Name: Encryption: Hash: Authentication D-H Group: Lifetime:	rv320 ESP_3DES ▼ ③ SHA1 ○ MD5 : ○ Pre-shared Key ○ RSA_SI Group 2 (1024bits) ▼ ○ Hour 5 Min ○ Sec (F	IG Range: 3 minutes to 24 hours)	
VPN Passthrough	Save Cancel			OK Cancel	
Device Management					
Device Management					

Paso 2. Vaya a VPN > Conjuntos de transformación IKE (consulte la imagen)

r.) Establezca Integrity en ESP_SHA1_HMAC.

b) Establezca *Encryption* en ESP_DES.

A continuación se muestran los conjuntos de transformación IKE:

Small Business cisco ISA500 Series	Configuration Utility		
Configuration Wizards Status Networking Firewall	Transform Sets		
Security Services VPN VPN Status	DefaultTrans rv320	Integrity ESP_SHA1_HMAC ESP_SHA1_HMAC	Encryption ESP_AES_256 ESP_3DES
IPsec VPN Status SSL VPN Status SSL VPN Status IPsec Policies IKE Policies Transform Sets IPsec Remote Access SSL Remote User Access Teleworker VPN Client		Transform Set - Add/Edit Name: 17/320 ESP Integrity: ESP_MD5_HMAC • Encryption: ESP_3DES •	ESP_SHA1_HMAC
VPN Passthrough	Save Cancel		OK Cancel

Paso 3. Vaya a VPN > Políticas IPsec > Add > Basic Settings (consulte la imagen)

- r.) Introduzca una descripción, como RV320.
- b) Establezca Activar política IPSec en Activado.
- c.) Establezca Remote Type en Static IP.
- d.) Introducir dirección remota.
- e.) Establezca Authentication Method en Pre-Shared Key.
- f) Establezca WAN Interface en WAN1.
- g) Establezca Red Local en DEFAULT_NETWORK.

h) Establezca Red Remota en RV320.

La siguiente imagen muestra las políticas IPsec Configuración básica:

Small Business cisco ISA500 Series Co	nfiguration Utility	
Configuration Wizards	IPsec Policies	
Status	Enable VPN: IPsec Policies - Add/Edit	Help
Firewall	IPsec Policie Basic Settings Advanced Settings VPN Failover	
Security Services VPN	Name Secretion: IPsec Policy Enable: On Off	IKE
▼ VPN Status IPsec VPN Status	rv320 * Remote Type: Static IP	rv320
SSL VPN Status Site-to-Site IPsec Policies IKE Policies Transform Sets IPsec Remote Access SSL Remote User Access Teleworker VPN Client L2TP Server VPN Passthrough	Remote Address: 10.10.2 * Authentication Method: Pre-Shared Key Key: Aa1234567890!@#\$%^&*() Certificate Local Certificate: default v Remote Certificate: default v WAN Interface: WAN1 v	
	Save Cancel * Remote network: IN320 V	Cancel

Paso 4. Vaya a VPN > Políticas IPsec > Add > Advanced Settings (consulte la imagen)

r.) Establezca *IKE Policy* y *Conjuntos de transformación IKE* respectivamente en los creados en los Pasos 1 y 2.

b) Establezca SA-Lifetime en 0 Hour 5 Min 0 Sec.

c.) Click OK.

A continuación se muestra la configuración avanzada de las políticas IPsec:

Small Business cisco ISA500 Series Col	nfiguration l	Jtility							
Configuration Wizards	IPsec Polic	ies	and the second second						
Status Networking	Enable VPN:	IPsec Policies - Add/Edit Basic Settings Advanced	d Settings	VPN Failo	ver			Help IKE rv320 es to 24 hours)	
Firewall Security Services	Add X	Windows Networking (Net BIOS) Broadcast:	○ On ④ Off			^	IKE		
VPN VPN Status IPsec VPN Status SSL VPN Status Site-to-Site IPsec Policies IKE Policies Transform Sets IPsec Remote Access SSL Remote User Access Teleworker VPN Client L2TP Server VPN Passthrough	Name Acce Apply NAT Translate Translate IKE Policy	Access Control : Apply NAT Policies: Translated Local Netwo Translated Remote Net IKE Policy:	Zone LAN WAN DMZ GUEST SSLVPN VOICE	Access Setting Permit Deny Permit Deny Permit Deny T Permit Deny N Permit Deny N Permit Deny N Permit Deny N Permit Deny N Permit Deny KE Policy Link			IV320		
Unarro		Transform: SA-Lifetime:	[rv320 ▼ 0 Hou	т 5 м	iransform Link	(Range: 3 minutes to	24 hours)	
03613									

Paso 5. Conexión del túnel VPN IPsec de sitio a sitio (consulte la imagen)

r.) Establezca *Enable VPN* en On.

b) Haga clic en el botón **Connect**.

La siguiente imagen muestra el botón Connect (Conectar):

IPsec Policies					
Enable VPN: 💿 O	n O Off				
IPsec Policies					
🕂 Add 🗙 Delete	😵 Refresh				
ers	Local	Remote	IKE	Transform	Configure
.10.10.2	*DEFAULT_NETWORK	rv320	rv320	rv320	/ X \ \