Configurando um túnel VPN de site a site entre o roteador VPN Cisco RV320 Gigabit Dual WAN e o adaptador de serviços integrados Cisco 500 Series

Objetivo

Uma VPN (Virtual Private Network) existe como uma tecnologia amplamente usada para conectar redes remotas a uma rede privada principal, simulando um link privado na forma de um canal criptografado em linhas públicas. Uma rede remota pode se conectar a uma rede principal privada como se ela existisse como parte da rede principal privada sem preocupações com a segurança devido a uma negociação em duas fases que criptografa o tráfego VPN de uma forma que somente os terminais VPN sabem como descriptografá-lo. Este guia curto fornece um exemplo de projeto para a construção de um túnel de VPN IPsec site a site entre um Cisco 500 Series Integrated Services Adapter e um Cisco RV Series Router.

Dispositivos aplicáveis

Roteadores Cisco RV Series (RV320) Adaptadores de serviços integrados Cisco 500 Series (ISA570)

Versão de software

4.2.2.08 [Cisco RV0xx Series VPN Routers]

Pré-configuração

Diagrama de Rede A seguir, há uma topologia de VPN site a site.



Um túnel VPN IPsec site a site é configurado e estabelecido entre o Cisco RV Series Router no escritório remoto e o Cisco 500 Series ISA no escritório central.

Com essa configuração, um host na LAN 192.168.1.0/24 no escritório remoto e um host na LAN 10.10.10.0/24 no escritório central podem se comunicar com segurança através da VPN.

Conceitos principais

Internet Key Exchange (IKE)

O Internet Key Exchange (IKE) é o protocolo usado para configurar uma associação de segurança (SA) no conjunto de protocolos IPsec. O IKE baseia-se no protocolo Oakley, na Internet Security Association e no Key Management Protocol (ISAKMP) e usa uma troca de chaves Diffie-Hellman para configurar um segredo de sessão compartilhada, a partir do qual as chaves criptográficas são derivadas.

Internet Security Association and Key Management Protocol (ISAKMP)

A Internet Security Association and Key Management Protocol (ISAKMP) é usada para negociar o túnel VPN entre dois pontos terminais VPN. Ele define os procedimentos para autenticação, comunicação e geração de chave, e é usado pelo protocolo IKE para trocar chaves de criptografia e estabelecer a conexão segura.

Internet Protocol Security (IPsec)

IP Security Protocol (IPsec) é um conjunto de protocolos para proteger as comunicações IP, autenticando e criptografando cada pacote IP de um fluxo de dados. O IPsec também inclui protocolos para estabelecer a autenticação mútua entre agentes no início da sessão e a negociação de chaves criptográficas a serem usadas durante a sessão. O IPsec pode ser usado para proteger os fluxos de dados entre um par de hosts, gateways ou redes.

Dicas de design

Topologia de VPN — Uma topologia de VPN ponto a ponto significa que um túnel IPsec seguro está configurado entre o site principal e o site remoto.

As empresas frequentemente exigem vários locais remotos em uma topologia de vários locais e implementam uma topologia VPN hub-and-spoke ou uma topologia VPN full mesh. Uma topologia VPN hub-and-spoke significa que os locais remotos não exigem comunicação com outros locais remotos, e cada local remoto estabelece apenas um túnel IPsec seguro com o local principal. Uma topologia VPN de malha completa significa que os locais remotos exigem comunicação com outros locais remotos locais remotos, e cada local remoto, e cada local remoto estabelece apenas um túnel IPsec seguro com o local principal. Uma topologia VPN de malha completa significa que os locais remotos exigem comunicação com outros locais remotos, e cada local remoto estabelece um túnel IPsec seguro com o local principal e todos os outros locais remotos. **Autenticação VPN** — O protocolo IKE é usado para autenticar peers VPN ao estabelecer um túnel VPN. Existem vários métodos de autenticação IKE, e a chave pré-compartilhada é o método mais conveniente. A Cisco recomenda a aplicação de uma chave pré-compartilhada forte.

Criptografia VPN — Para garantir a confidencialidade dos dados transportados pela VPN, os algoritmos de criptografia são usados para criptografar o payload dos pacotes IP. DES, 3DES e AES são três padrões de criptografia comuns. O AES é considerado o mais seguro quando comparado ao DES e ao 3DES. A Cisco recomenda a aplicação de criptografia AES-128 bits ou superior (por exemplo, AES-192 e AES-256). No entanto, algoritmos de criptografia mais fortes exigem mais recursos de processamento de um roteador. **Endereçamento IP de WAN dinâmica e DDNS (Dynamic Domain Name Service)** — O túnel VPN precisa ser estabelecido entre dois endereços IP públicos. Se os roteadores WAN receberem endereços IP estáticos do ISP (Provedor de serviços de Internet), o túnel VPN poderá ser implementado diretamente usando endereços IP públicos estáticos. No entanto, a maioria das pequenas empresas usa serviços de Internet de banda larga econômicos, como DSL ou cabo, e recebe endereços IP dinâmicos de seus ISPs. Nesses casos, o Dynamic Domain Name Service (DDNS) pode ser usado para mapear o endereço IP dinâmico para um FQDN (nome de domínio totalmente qualificado).

Endereçamento IP da LAN — O endereço de rede IP da LAN privada de cada site não deve ter sobreposições. O endereço de rede IP da LAN padrão em cada local remoto deve sempre ser alterado.

Dicas de configuração

Lista de verificação de pré-configuração

Etapa 1. Conecte um cabo Ethernet entre o RV320 e seu DSL ou modem a cabo e conecte um cabo Ethernet entre o ISA570 e seu DSL ou modem a cabo.

Etapa 2. Ligue o RV320 e conecte PCs, servidores e outros dispositivos IP internos às portas LAN do RV320.

Etapa 3. Ligue o ISA570 e conecte PCs, servidores e outros dispositivos IP internos às portas LAN do ISA570.

Etapa 4. Certifique-se de configurar os endereços IP da rede em cada site em sub-redes diferentes. Neste exemplo, a LAN do escritório remoto está usando 192.168.1.0 e a LAN do escritório central está usando 10.10.10.0.

Etapa 5. Certifique-se de que os PCs locais possam se conectar aos respectivos roteadores e com outros PCs na mesma LAN.

Identificando a conexão WAN

Você precisará saber se o ISP fornece um endereço IP dinâmico ou um endereço IP estático. O ISP geralmente fornece um endereço IP dinâmico, mas você deve confirmá-lo antes de concluir a configuração do túnel VPN site a site.

Configurando o túnel VPN IPsec Site-to-Site para RV320 no escritório remoto

Etapa 1. Vá para **VPN > Gateway-to-Gateway** (consulte a imagem)

r.) Insira um nome de túnel, como o escritório remoto.

b.) Defina Interface como WAN1.

c.) Defina o modo de chave como IKE com chave pré-compartilhada.

d.) Insira o endereço IP local e o endereço IP remoto.

A imagem a seguir mostra a página Gateway para Gateway do Roteador VPN WAN Dual Gigabit RV320:

CISCO RV320 Gi	gabit Dual WAN VPN R	louter		
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	Keying Mode:	IKE with Preshared key	V	
Gateway to Gateway Client to Gateway	Enable:	V		
PPTP Server	Local Group Setup			
 Certificate Management 	Local Security Gateway Type:	IP Only		~
► Log	IP Address:	0.0.0.0		
User Management	Local Security Group Type:	Subnet	V	
Wizard	IP Address:	192.168.1.0		
	Subnet Mask:	255.255.255.0		
	Remote Group Setup			
	Remote Security Gateway Type:	IP Only		¥
	IP Address 🗸 :			
	Remote Security Group Type:	Subnet	Y	
	IP Address:			
© 2013 Cisco Systems, Inc. All Ri	ghts Reserved.			

Etapa 2. Configurar as definições do túnel IPSec (ver imagem)

- r.) Defina Encryption como 3DES.
- b.) Defina Authentication como SHA1.
- c.) Verifique o segredo perfeito para encaminhamento.

d.) Configure a *chave pré-compartilhada* (precisa ser a mesma em ambos os roteadores).

A seguir, mostra a configuração de IPSec (Fase 1 e 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 🗸	
Phase 2 SA Lifetime:	600	sec (Range: 120-28800, Default: 3600)
Minimum Preshared Key Complexity:	Enable	
Preshared Key:	Aa1234567890!@#\$%^&*()_+	
Preshared Key Strength Meter:		
Advanced +		

Note: Lembre-se de que as configurações de túnel IPsec em ambos os lados do túnel VPN IPsec site a site devem corresponder. Se existirem discrepâncias entre as Configurações de Túnel IPsec do RV320 e do ISA570, ambos os dispositivos falharão ao negociar a chave de criptografia e não conseguirão se conectar.

Etapa 3. Clique em Salvar para concluir a configuração.

Configurando o túnel de VPN IPsec site a site para ISA570 no escritório principal

Etapa 1. Vá para VPN > Políticas IKE (consulte a figura)

r.) Defina *Encryption* como ESP_3DES.

- b.) Defina Hash como SHA1.
- c.) Defina Authentication como Pre-shared Key.
- d.) Defina D-H Group como Group 2 (1024 bits).

A imagem a seguir mostra Políticas IKE:

Multin Small Business					
Configuration Wizards Status Networking Firewall Security Services 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	IKE Policies IKE Policies Add Delete Name Defaultike rv320	Encryption AES_256 3DES IKE Policy - Name: Encryption: Hash: Authenticatio D-H Group:	Hash SHA1 Add/Edit IV320 ESP_3DES * • SHA1 O MD5 on: • Pre-shared Key O RSA_SIC Group 2 (1024bits) •	Authentication PPE SHAPE FEEE	D-H Group group_2 group_2
L2TP Server VPN Passthrough Users Device Management	Save Cancel			OK Cancel	

Etapa 2. Vá para VPN > Conjuntos de transformação IKE (consulte a figura)

- r.) Defina Integrity como ESP_SHA1_HMAC.
- b.) Defina Encryption como ESP_DES.

O seguinte mostra Conjuntos de transformação IKE:

Configuration Wizards	Transform Sets		
Status	Transform Sate		
Networking			
Firewall	Name	Integrity	Encryption
Security Services	DefaultTrans	ESP_SHA1_HMAC	ESP_AES_256
 VPN Status IPsec VPN Status SSL VPN Status SSL VPN Status Site-to-Site IPsec Policies IKE Policies IRSE Policies IFsec Remote Access SSL Remote User Access Teleworker VPN Client L2TP Server 	I IV320	ESP_SHA1_HMAC Transform Set - Add/Edit Name: IV320 ESP Integrity: O ESP_MD5_HMAC Encryption: ESP_3DES	ESP_3DES
VPN Passthrough	Save Cancel		OK Cancel

Etapa 3. Vá para VPN > Políticas IPsec > Adicionar > Configurações básicas (consulte a figura)

- r.) Insira uma Descrição, como RV320.
- b.) Defina Ativar política IPsec como Ativado.
- c.) Defina Remote Type (Tipo remoto) como Static IP (IP estático).
- d.) Endereço remoto de entrada.
- e.) Defina Authentication Method como Pre-Shared Key.
- f) Defina a interface WAN como WAN1.

- g.) Defina Local Network como DEFAULT_NETWORK.
- h) Defina Remote Network como RV320.

A imagem a seguir mostra as configurações básicas das políticas de IPsec:

Small Business cisco ISA500 Series Co	nfiguration Utility	
Configuration Wizards	IPsec Policies	
Status Networking Firewall Security Services VPN VPN Status IPsec VPN Status SSL Remote Access IPsec Remote Access SSL Remote User Access Teleworker VPN Client L2TP Server VPN Passthrough	Enable VPN: Psec Policies - Add/Edit Basic Settings Advanced Settings Vame · Description: · V320 · Psec Policy Enable: · Description: · V320 · Psec Policy Enable: · On Off · Remote Type: Static IP * Remote Address: 10.10.12 · Authentication Method: · Pre-Shared Key · Certificate Local Certificate: Local Certificate: default * · VAN Interface: WAN1 * · Local network: DEFAULT_NETWORK *	IKE N320
Users		

Etapa 4. Vá para **VPN > Políticas IPsec > Adicionar > Configurações avançadas** (veja a figura) r.) Defina *IKE Policy* e *IKE Transform Sets* respectivamente para aqueles criados nas Etapas 1 e 2.

b.) Defina SA-Lifetime como 0 hora 5 min 0 s.

c.) Click OK.

O seguinte mostra as Configurações avançadas das políticas de IPsec:

ululu Small Business cisco ISA500 Series Col	nfiguration l	Jtility					
Configuration Wizards	IPsec Polici	ies	-				
Status Networking	Enable VPN:	IPsec Policies - Add/Edit Basic Settings Advanced	d Settings VPN	Failover		Help	
Security Services	Add X	Windows Networking (Net BIOS) Broadcast: O On On Off			Help IKE rv320	^	
 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	Save Cancel	Access Control : Apply NAT Policies: Translated Local Netwo Translated Remote Ne IKE Policy: Transform: SA-Lifetime:	Zone LAN WAN DMZ GUEST SSLVPN VOICE On ork: - Sele rv320 0	Access Setting Permit Deny Permit Deny Permit Deny Permit Deny Permit Deny Permit Deny Permit Deny Off Ct an address object - KE Policy Link Transform Link Hour 5 Min 0 Sec	(Range: 3 minutes to	24 hours) 💙	rv320
Users						OK Cancel	

Etapa 5. Conectar o túnel VPN IPsec site a site (consulte a figura)

- r.) Defina Enable VPN (Ativar VPN) como On (Ativado).
- b.) Clique no botão Connect (Conectar).

A imagem a seguir mostra o botão 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	/ 🗙 🖉