Configuration d'un tunnel VPN site à site entre le routeur VPN double WAN Gigabit Cisco RV320 et l'adaptateur de services intégrés Cisco 500

Objectif

Un réseau privé virtuel (VPN) existe en tant que technologie largement utilisée pour connecter des réseaux distants à un réseau privé principal, simulant une liaison privée sous la forme d'un canal crypté sur des lignes publiques. Un réseau distant peut se connecter à un réseau principal privé comme s'il faisait partie du réseau principal privé sans problème de sécurité en raison d'une négociation en deux phases qui chiffre le trafic VPN d'une manière que seuls les points d'extrémité VPN savent comment le déchiffrer.

Ce guide rapide fournit un exemple de conception pour la construction d'un tunnel VPN IPsec site à site entre un adaptateur de services intégrés de la gamme Cisco 500 et un routeur de la gamme Cisco RV.

Périphériques pertinents

Routeurs · gamme Cisco RV (RV320) · adaptateurs de services intégrés de la gamme Cisco 500 (ISA570)

Version du logiciel

·4.2.2.08 [Routeurs VPN de la gamme Cisco RV0xx]

Préconfiguration

Diagramme du réseau La topologie VPN site à site est présentée ci-dessous.



Un tunnel VPN IPsec site à site est configuré et établi entre le routeur Cisco RV du bureau distant et l'ISA de la gamme Cisco 500 du bureau principal.

Avec cette configuration, un hôte du réseau local 192.168.1.0/24 au bureau distant et un hôte du réseau local 10.10.10.0/24 au bureau principal peuvent communiquer entre eux en toute sécurité via un réseau privé virtuel.

Concepts de base

IKE (Internet Key Exchange)

Internet Key Exchange (IKE) est le protocole utilisé pour configurer une association de sécurité (SA) dans la suite de protocoles IPsec. IKE s'appuie sur le protocole Oakley, Internet Security Association et le protocole ISAKMP (Key Management Protocol) et utilise un échange de clés Diffie-Hellman pour configurer un secret de session partagé, à partir duquel les clés cryptographiques sont dérivées.

ISAKMP (Internet Security Association and Key Management Protocol)

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est utilisé pour négocier le tunnel VPN entre deux points d'extrémité VPN. Il définit les procédures d'authentification, de communication et de génération de clés et est utilisé par le protocole IKE pour échanger des clés de chiffrement et établir la connexion sécurisée.

Sécurité du protocole Internet (IPsec)

IP Security Protocol (IPsec) est une suite de protocoles permettant de sécuriser les communications IP en authentifiant et en chiffrant chaque paquet IP d'un flux de données. IPsec inclut également des protocoles pour établir l'authentification mutuelle entre les agents au début de la session et la négociation des clés cryptographiques à utiliser pendant la session. IPsec peut être utilisé pour protéger les flux de données entre deux hôtes, passerelles ou réseaux.

Conseils de conception

Topologie VPN - Une topologie VPN point à point signifie qu'un tunnel IPsec sécurisé est configuré entre le site principal et le site distant.

Les entreprises ont souvent besoin de plusieurs sites distants dans une topologie multisite et mettent en oeuvre une topologie VPN en étoile ou une topologie VPN à maillage global. Une topologie VPN en étoile signifie que les sites distants n'ont pas besoin de communication avec d'autres sites distants et que chaque site distant établit uniquement un tunnel IPsec sécurisé avec le site principal. Une topologie VPN à maillage global signifie que les sites distants doivent communiquer avec d'autres sites distants, et chaque site distant établit un tunnel IPsec sécurisé avec le site principal et tous les autres sites distants.

Authentification VPN - Le protocole IKE est utilisé pour authentifier les homologues VPN lors de l'établissement d'un tunnel VPN. Il existe différentes méthodes d'authentification IKE et la clé pré-partagée est la méthode la plus pratique. Cisco recommande l'application d'une clé forte prépartagée.

Cryptage VPN - Pour garantir la confidentialité des données transportées sur le VPN, des algorithmes de chiffrement sont utilisés pour chiffrer la charge utile des paquets IP. DES, 3DES et AES sont trois normes de cryptage courantes. AES est considéré comme le plus sécurisé par rapport aux DES et 3DES. Cisco recommande vivement l'application d'un cryptage AES-128 bits ou supérieur (par exemple, AES-192 et AES-256). Cependant, des algorithmes de chiffrement plus puissants nécessitent davantage de ressources de traitement de la part d'un routeur.

Dynamic WAN IP Addressing and Dynamic Domain Name Service (DDNS) : le tunnel VPN doit être établi entre deux adresses IP publiques. Si les routeurs WAN reçoivent des adresses IP statiques du fournisseur d'accès à Internet (FAI), le tunnel VPN peut être mis en oeuvre directement à l'aide d'adresses IP publiques statiques. Cependant, la plupart des petites entreprises utilisent des services Internet haut débit économiques tels que la DSL ou le câble et reçoivent des adresses IP dynamiques de leurs FAI. Dans de tels cas, le service DDNS (Dynamic Domain Name Service) peut être utilisé pour mapper l'adresse IP dynamique à un nom de domaine complet (FQDN).

Adressage IP LAN - L'adresse réseau IP LAN privée de chaque site ne doit pas comporter de chevauchement. L'adresse réseau IP LAN par défaut de chaque site distant doit toujours être modifiée.

Conseils de configuration

Liste de contrôle de préconfiguration

Étape 1. Connectez un câble Ethernet entre le RV320 et son modem DSL ou câble, et un câble Ethernet entre le ISA570 et son modem DSL ou câble.

Étape 2. Mettez le routeur RV320 sous tension, puis connectez les ordinateurs, les serveurs et les autres périphériques IP internes aux ports LAN du routeur RV320.

Étape 3. Mettez le ISA570 sous tension, puis connectez les ordinateurs, les serveurs et les autres périphériques IP internes aux ports LAN du ISA570.

Étape 4. Assurez-vous de configurer les adresses IP réseau de chaque site sur différents sous-réseaux. Dans cet exemple, le réseau local du bureau distant utilise 192.168.1.0 et le réseau local du bureau principal utilise 10.10.10.0.

Étape 5. Assurez-vous que les PC locaux sont en mesure de se connecter à leurs routeurs respectifs et à d'autres PC sur le même réseau local.

Identification de la connexion WAN

Vous devez savoir si votre FAI fournit une adresse IP dynamique ou une adresse IP statique. Le FAI fournit généralement une adresse IP dynamique, mais vous devez le

Configuration du tunnel VPN IPsec site à site pour RV320 sur le site distant

Étape 1. Accédez à VPN > Gateway-to-Gateway (voir l'image)

a.) Entrez un nom de tunnel, tel que RemoteOffice.

b.) Définissez l'interface sur WAN1.

c.) Définissez le mode de clé sur IKE avec la clé prépartagée.

d.) Saisissez Local IP Address (Adresse IP locale) et Remote IP Address (Adresse IP distante).

L'image suivante présente la page Passerelle de routeur VPN double WAN Gigabit RV320 :

cisco RV320 Gig	gabit Dual WAN VPN F	Router	
Getting Started System Summary	Gateway to Gateway		
▶ Setup	Add a New Tunnel		
▶ DHCP	Tunnel No.	2	
 System Management 	Tunnel Name:		
Port Management	runner Name.		
▶ Firewall	Interface:	WAN1	/
▼ VPN	Kevina Mode:	IKE with Preshared key	
Summary Gateway to Gateway Client to Gateway	Enable:	V	
VPN Passthrough PPTP Server	Local Group Setup		
Certificate Management	Local Security Gateway Type:	IP Only	¥
► Log	IP Address:	0.0.0.0	
► SSL VPN	Local Security Group Type:	Subnet	
Wizord			
Wizaru	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	·
	IP Address:		
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.		

Étape 2. Configurer les paramètres du tunnel IPSec (voir l'image)

- a.) Définissez Encryption sur 3DES.
- b.) Définissez Authentication sur SHA1.
- c.) Cochez Parfect Forward Secrecy.
- d.) Configurez la *clé prépartagée* (doit être identique sur les deux routeurs).

L'exemple suivant illustre la configuration IPSec (phases 1 et 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: Gardez à l'esprit que les paramètres de tunnel IPsec des deux côtés du tunnel VPN IPsec site à site doivent correspondre. S'il existe des différences entre les paramètres de tunnel IPsec du RV320 et de l'ISA570, les deux périphériques ne négocieront pas la clé de chiffrement et ne se connecteront pas.

Étape 3. Cliquez sur Enregistrer pour terminer la configuration.

Configuration du tunnel VPN IPsec site à site pour ISA570 au bureau principal

Étape 1. Accédez à VPN > IKE Policies (voir l'image)

a.) Définissez Encryption sur ESP_3DES.

b.) Définissez Hash sur SHA1.

c.) Définissez Authentification sur Clé pré-partagée.

d.) Définissez Groupe D-H sur Groupe 2 (1 024 bits).

L'image suivante montre les stratégies IKE :

Small Business LISA500 Series Col	nfigu	uration Utility					, and the second se	
Configuration Wizards	IKE	Policies						
Status	IKE	Dolicios						
Networking								
Firewall	1	PAdd 👗 Delete						
Security Services		Name	Encr	ption		Hash	Authentication	D-H Group
VPN		Defaultike	AES_	256		SH01	PRE SHARE	group_2
✓ VPN Status		rv320	3DE	IKE Policy - A	dd/Edit		Help	group_2
IPsec VPN Status				Name:	rv320			
SSL VPN Status				Encryption:	ESP 3D	FS 💌		
				Encryption.	0			
IPsec Policies				Hash:	SHA1	⊖ MD5		
Transform Sets				Authenticatior	n: 💿 Pre-s	hared Key 🔘 RSA_SI	G	
IPsec Remote Access				D-H Group:	Group 2	(1024bits) 🔽		
SSL Remote User Access								
Teleworker VPN Client				Lifetime:	0 Hou	5 Min 0 Sec (F	Range: 3 minutes to 24 hours)	
L2TP Server			_					
VPN Passthrough	Sav	ve Cancel						
							OK Cancel	
					_			
Users								
Device Management								

Étape 2. Accédez à VPN > IKE Transform Sets (voir l'image)

- a.) Définissez Integrity sur ESP_SHA1_HMAC.
- b.) Définissez Encryption sur ESP_DES.
- La figure suivante illustre les jeux de transformation IKE :

Small Business			
Configuration Wizards			
Status	Transform Sets		
Networking	Transform Sets		
Firewall			
Populity Continent	Name	Integrity	Encryption
Security Services	DefaultTrans	ESP_SHA1_HMAC	ESP_AES_256
VPN	I rv320	ESP_SHA1_HMAC	ESP_3DES
 VPN Status IPsec VPN Status SSL 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 		Transform Set - Add/Edit * Name: IV320 ESP Integrity: ESP_MD5_HMAC • Encryption: ESP_3DES •	ESP_SHA1_HMAC
VPN Passthrough	Save Cancel		Cancel

Étape 3. Accédez à VPN > Stratégies IPsec > Ajouter > Paramètres de base (voir l'image)

- a.) Entrez une description, telle que RV320.
- b.) Définissez Activer la stratégie IPsec sur Activé.
- c.) Définissez Remote Type sur Static IP.
- d.) Saisissez l'adresse distante.
- e.) Définissez Authentication Method sur Pre-Shared Key.
- f) Définissez l'interface WAN sur WAN1.
- g.) Définissez Réseau local sur DEFAULT_NETWORK.

h) Définissez Remote Network sur RV320.

L'image suivante montre les paramètres de base des stratégies IPsec :

Small Business cisco ISA500 Series Co	nfiguration l	Jtility	
Configuration Wizards	IPsec Polic	ies	
Configuration Wizards Status Networking Firewall Security Services VPN VPN Status IPsec VPN Status SSL VPN Status VPN Passthrough	IPsec Polici IPsec Policie Add X Name rv320	Ies Psec Policies - Add/Edit Pescic Settings Advanced Settings VPN Failover Pesciption: rv320 Pescription: rv320 Presc Policy Enable: ● On Off Remote Type: Static IP ♥ Remote Address: 10.10.10.2 Authentication Method: ● Pre-Shared Key	IKE IV320
Users			

Étape 4. Accédez à **VPN > Stratégies IPsec > Ajouter > Paramètres avancés** (voir l'image) a.) Définissez respectivement *la stratégie IKE* et les *jeux de transformation IKE* sur ceux créés aux

étapes 1 et 2.

b.) Définissez SA-Lifetime à 0 Heure 5 min 0 sec.

c.) Click OK.

L'exemple suivant illustre les paramètres avancés des stratégies IPsec :

Small Business cisco ISA500 Series Cor	nfiguration l	Jtility					
Configuration Wizards	IPsec Polic	ies					
Status Networking	Enable VPN:	IPsec Policies - Add/Edit				Help	
Firewall Security Services	Psec Policie	Windows Networking (Net BIOS) Broadcast:	On Off	wover		^	
VPN	Name	Access Control :	Zone	Access Setting			IKE
▼ VPN Status	□ rv320		LAN	Permit Deny			rv320
IPsec VPN Status			WAN	Permit Deny			
SSL VPN Status			DMZ	Permit Deny			
IPsec Policies			GUEST	Permit Deny			
IKE Policies			SSLVPN	Permit Deny			
Transform Sets			VOICE	Permit Deny			
IPsec Remote Access							
 SSL Remote User Access 		Apply NAT Policies:	🔿 On 🤅	Off			
Teleworker VPN Client			Coloct	an address object			
LZTP Server		Translated Local Netwo	ork:	all autress object - 💌			
VEN Fassinough		Translated Remote Ne	twork: - Select	an address object – 💌			
	Save Cancel	IKE Policy:	rv320 💌	IKE Policy Link			
		Transform:	rv320 🔽	Transform Link			
		SA-Lifetime:	0 Ho	our 5 Min 0 Sec	(Range: 3 minutes to	24 hours) 💙	
						OK Cancel	
Users							

Étape 5. Connecter le tunnel VPN IPsec site à site (voir l'image) a.) Définissez *Enable VPN* sur On.

- b.) Cliquez sur le bouton Connect.

L'image suivante montre le bouton Connect :

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