CISCO Site-to-Site VPN

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Alberto Molina Coballes

Redes de Área Local

Junio 2009

Escenario

- Se quiere implementar una VPN Site-to-Site entre las dos oficinas
- Se creará un túnel IPSEC entre ambas sedes basado en secreto compartido

Tareas a realizar

I. Configurar las políticas IKE
II. Verificar las políticas IKE
III. Configurar IPSec
IV. Configurar Crypto Map

I. Configurar las políticas IKE

- Una política IKE define una combinación de parámetros de seguridad (cifrado, hash, autenticación y DH) que serán usados durante la negociación IKE.
- En ambos nodos deben crearse políticas (tantas como se quieran ordenadas por prioridad) y, al menos, debe existir una igual en los 2 extremos.
- También se deben configurar paquetes IKE keepalives (o paquetes hello) para detectar posibles pérdidas de conectividad.

I. Configurar las políticas IKE

Paso	Comando	Objetivo
1	r1(config)# crypto isakmp policy 1	Crear una nueva política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la más prioridad más alta)
2	r1(config-isakmp)# encryption 3des	Especificar el algoritmo de cifrado a utilizar: 56-bit Data Encryption Standard (DES [des]) o 168-bit Triple DES (3des).
3	r1(config-isakmp)# hash sha	Elegir el algoritmo de hash a usar: Message Digest 5 (MD5 [md5]) o Secure Hash Algorithm (SHA [sha]).
4	r1(config-isakmp)# authentication pre-share	Determinar el método de autenticación: pre-shared keys (pre-share), RSA1 encrypted nonces (rsa-encr), o RSA signatures (rsa-sig).

I. Configurar las políticas IKE

Paso	Comando	Objetivo
5	r1(config-isakmp)# group 2	Especificar el identificador de grupo Diffie-Hellman: 768-bit Diffie-Hellman (1) o 1024-bit Diffie-Hellman (2)
6	r1(config-isakmp)# lifetime 86400	Determinar el tiempo de vide de la Asociación de Seguridad (SA) en segundos. 86400 segundos = 1 día
7	r1(config-isakmp)# exit	Volver al modo de configuración global
Op-cio-nal	r1(config)# cry isakmp keepalive 12 2	Elegir el intervalo de los paquetes hello (por defecto 10 segundos) y el tiempo de reintento cuando un paquete falla.

I. Configurar las políticas IKE

- En función del método de autenticación elegido hay que llevar a cabo una tarea más antes de que IKE e IPSec puedan usar la política creada.
  - RSA signatures: hay que configurar ambos nodos para obtener los certificados de una CA
  - RSA encrypted nonces: cada nodo debe tener en su poder la clave pública del otro nodo
  - Pre-Shared keys:
    1. Establecer la identidad ISAKMP de cada nodo (nombre o IP)
    2. Establecer el secreto compartido en cada nodo.

I. Configurar las políticas IKE

Paso	Comando	Objetivo
9	r1(config)# crypto isakmp identity address	En la oficina central: elegir la identidad ISAKMP (address o hostname) que el router usará en las negociaciones IKE
10	r1(config)# crypto isakmp key misecretocompartido ip_oficina_remota	En la oficina central: establecer el secreto compartido que se usará con el router de la oficina remota
11	r2(config)# crypto isakmp identity address	En la oficina remota: elegir la identidad ISAKMP (address o hostname) que el router usará en las negociaciones IKE
12	r2(config)# crydpto isakmp key misecretocompartido ip_oficina_central	En la oficina remota: establecer el secreto compartido que se usará con el router de la oficina cetral

II. Verificar las políticas IKE

- Para asegurarnos de que la configuración de la política es la que deseamos usar podemos utilizar el siguiente comando:

Paso	Comando	Objetivo
13	r1# show crypto isakmp policy	Comprobar los valores de cada parámetro de seguridad de la política IKE

III. Configurar IPSec

- Tras configurar y verificar la política IKE en cada nodo, hay que configurar IPSec en ambos extremos:

1. Crear Crypto ACL
2. Verificar Crypto ACL
3. Definir el Transform Set
4. Verificar el Transform Set

III. Configurar IPSec

1. Crear Crypto ACL.

Las Crypto ACL se usan para definir el tráfico que será protegido mediante cifrado

Paso	Comando	Objetivo
14	r1(config)# access-list 109 permit ip red_oficina_central red_oficina_remota	En la oficina central: cifrar todo el tráfico IP que salga de la oficina central hacia la oficina remota
15	r2(config)# access-list 109 permit ip red_oficina_remota red_oficina_central	En la oficina remota: cifrar todo el tráfico IP que salga de la oficina remota hacia la oficina central

III. Configurar IPSec

2. Verificar Crypto ACL.

Paso	Comando	Objetivo
16	r1# show access-lists 109	Verificar Crypto ACL

III. Configurar IPSec

3. Definir los Transform Sets

Paso	Comando	Objetivo
17	r1(config)# crypto ipsec transform-set STRONG esp-3des esp-sha-hmac	Esyablece las políticas de seguridad IPSEC que se usarán en las comunicaciones, eligiendo el modo transporte (AH) o túnel (ESP)
18	r1(config-isakmp)# exit	En la oficina remota: cifrar todo el tráfico IP que salga de la oficina remota hacia la oficina central

III. Configurar IPSec

3. Verificar el Transform Set

Paso	Comando	Objetivo
19	r1# show crypto ipsec transform-set	Verificar Transform Set

IV. Configurar Crypto Map

Paso	Comando	Objetivo
20	r1(config)# crypto map NOMBRE 1 ipsec-isakmp	Crear un crypto map de nombre NOMBRE, y establecer el número de secuencia de esta entrada, obligando a usar IKE para establecer SAs.
21	r1(config-crypto-map)# set transform-set STRONG	De los transform sets que se hayan definido, especificar cuál se usara en esta entrada del crypto-map
22	r1(config-crypto-map)# set pfs group 2	Activar Perfect Forward Secrecy
23	r1(config-crypto-map)# set peer dirección-oficina-remota	Definir la dirección del host remoto

IV. Configurar Crypto Map

Paso	Comando	Objetivo
24	r1(config-crypto-map)# match address 109	Establecer el tráfico que se va a cifrar (definido previamente en una ACL)
25	r1(config-crypto-map)# ^Z	Volver al modo privilegiado
26	r1(config)# show crypto map	Verificar la configuración del crypto map

IV. Configurar Crypto Map

Paso	Comando	Objetivo
27	r1(config)# interface XXXX	Entrar al modo de configuración de la interfaz donde se aplicará el crypto map
28	r1(config-if)# crypto map NOMBRE	Aplicar el crypto map a la interfaz física.
29	r1(config-if)#^Z	Volver al modo privilegiado
30	r1#show crypto map interface XXXX	Verificar la asociación de la intnerfaz y el crypto map.

Comprobar el funcionamiento

Paso	Comando	Objetivo
31	r1# show crypto ipsec sa	Mostrar la información de la Asociación de Seguridad para verificar su correcto funcionamiento
32	r1# write	Guardar los cambios. El paso más importante :-)