

CISCO IOS Easy VPN Server



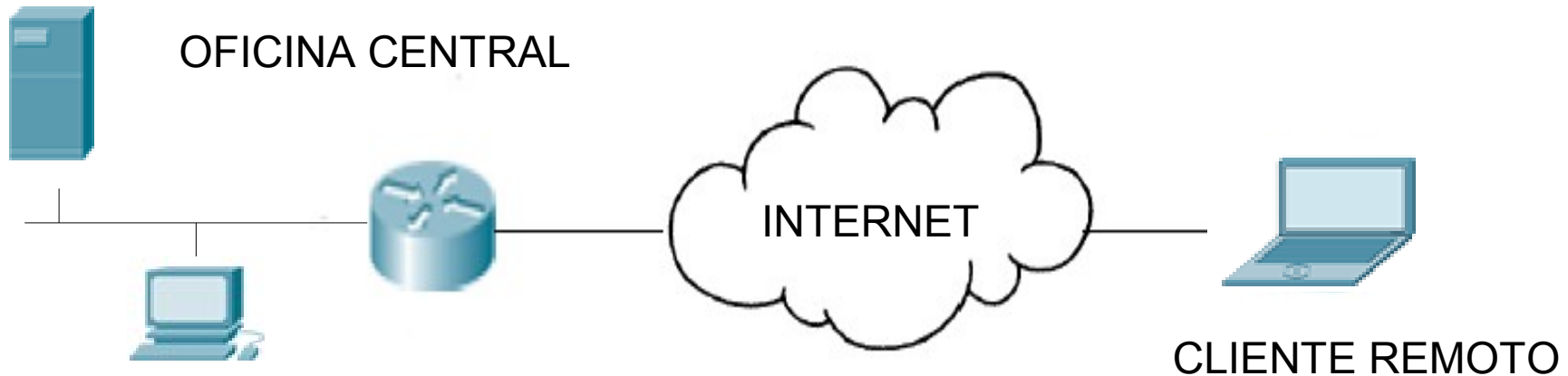
IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Alberto Molina Coballes

Redes de Área Local

Junio 2009

Escenario



- Se quiere implementar una VPN de acceso remoto basada en IPSec
- Se usará un router (IOS 12.4 o posterior) como servidor Easy VPN
- Los clientes necesitan instalar CISCO Easy VPN Client

Tareas a realizar

- I. Crear un pool de direcciones que usarán los clientes que se conecten por VPN
- II. Configurar la autenticación
- III. Configurar la política IKE
- IV. Configurar la política IPSec



I. Crear un pool de direcciones

Paso	Comando	Objetivo
1	<code>r1(config)# ip local pool VPNPOOL 192.168.1.10 192.168.1.19</code>	Se crea un pool de direcciones que permite 10 conexiones concurrentes



II. Configurar la autenticación

Paso	Comando	Objetivo
2	<code>r1(config)# aaa new-model</code>	Activa la funcionalidad aaa (Authentication, Authorization y Accounting)
3	<code>r1(config)# aaa authentication login VPN-USERS local</code>	Defina la lista de métodos de autenticación cuando un usuario hace login (local, RADIUS...)
4	<code>r1(config)# aaa authorization network VPN-GROUP local</code>	Establece los parámetros que restringen el acceso de los usuarios a la red
5	<code>r1(config)# username vpnuser password micontraseña</code>	Se crea una cuenta de usuario que usarán los clientes VPN para autenticarse contra el servidor

III. Configurar las políticas IKE

Paso	Comando	Objetivo
6	<code>r1(config)# crypto isakmp policy 10</code>	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)
7	<code>r1(config-isakmp)# encryption aes 192</code>	Especificar el algoritmo de cifrado a utilizar
8	<code>r1(config-isakmp)# hash sha</code>	Elegir el algoritmo de hash a usar: Message Digest 5 (MD5 [md5]) o Secure Hash Algorithm (SHA [sha]).
9	<code>r1(config-isakmp)# authentication pre-share</code>	Determinar el método de autenticación: pre-shared keys (pre-share), RSA1 encrypted nonces (rsa-encr), o RSA signatures (rsa-slg).

III. Configurar las políticas IKE

Paso	Comando	Objetivo
10	<code>r1(config-isakmp)# group 5</code>	Especificar el identificador de grupo Diffie-Hellman
11	<code>r1(config)# crypto isakmp client configuration group VPN-GROUP</code>	Crea un grupo IKE para los clientes VPN
12	<code>r1(config-isakmp-group)# key SECRETOCOMPATIDO</code>	Establece el secreto compartido para el grupo VPN-GROUP
13	<code>r1(config-isakmp-group)# pool VPNPOOL</code>	Se selecciona el pool de direcciones para los clientes

IV. Configurar la política IPSec

Paso	Comando	Objetivo
14	<code>r1(config)# crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac</code>	Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones
15	<code>r1(config)# crypto dynamic-map VPN-DYNAMIC 10</code>	Crea un crypto map dinámico que se usa cuando la IP del host remoto no se conoce, como es el caso en las VPN de acceso remoto
16	<code>r1(config-crypto-map)# set transform-set VPNSET</code>	Asocia el transform set VPNSET al crypto map dinámico
17	<code>r1(config-crypto-map)# reverse-route</code>	Activa Reverse Route Injection (RRI)

IV. Configurar la política IPSec

Paso	Comando	Objetivo
18	<code>r1(config)# crypto map VPN-STATIC client configuration address respond</code>	Configura un crypto map estático que puede ser asociado a una interfaz
19	<code>r1(config)# crypto map VPN-STATIC client authentication list VPN-USERS</code>	Define el conjunto de usuarios con permisos de autenticación
20	<code>r1(config)# crypto map VPN-STATIC isakmp authorization list VPN-GROUP</code>	Establece el grupo de usuarios y los parámetros de acceso a la red
21	<code>r1(config)# crypto map VPN-STATIC 20 ipsec-isakmp dynamic VPN-DYNAMIC</code>	Asocia el crypto map dinámico creado para los clientes de acceso remoto

IV. Configurar la política IPSec

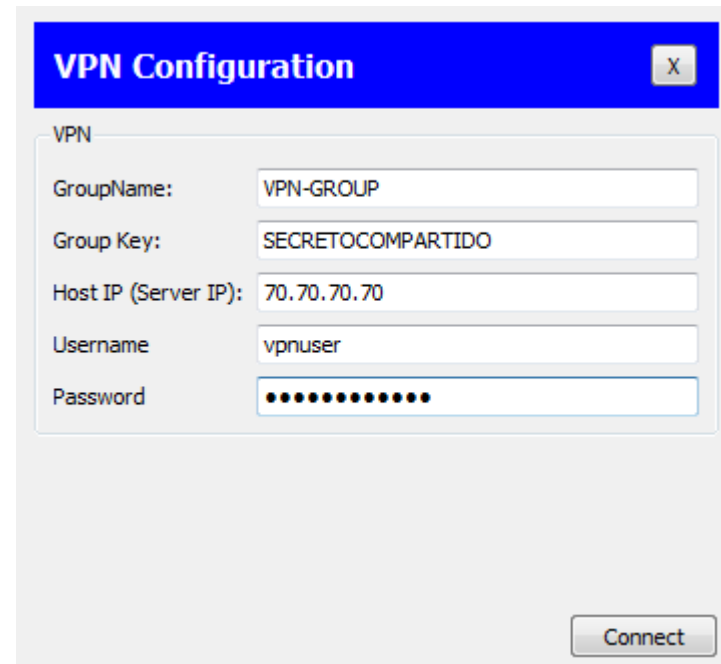
Paso	Comando	Objetivo
22	<code>r1(config)# interface serial 1/0</code>	Accedemos a la configuración de la interfaz por la que se conectarán los clientes VPN
23	<code>r1(config-if)# crypto map VPN-STATIC</code>	Asociamos el crypto map a la interfaz
24	<code>r1# write</code>	Guardamos todos los cambios

Conexión desde el cliente



The image shows the 'Create New VPN Connection Entry' dialog box in the Cisco VPN Client. It has a title bar with a Cisco logo and the text 'VPN Client | Create New VPN Connection Entry'. The dialog is divided into several sections. At the top, there are three text input fields: 'Connection Entry:', 'Description:', and 'Host:'. To the right of these fields is a small cartoon illustration of a person sitting at a desk with a computer. Below the input fields are four tabs: 'Authentication', 'Transport', 'Backup Servers', and 'Dial-Up'. The 'Authentication' tab is selected. Under this tab, there are two radio button options: 'Group Authentication' (which is selected) and 'Certificate Authentication'. Under 'Group Authentication', there are three text input fields: 'Name:', 'Password:', and 'Confirm Password:'. Under 'Certificate Authentication', there is a 'Name:' dropdown menu showing 'powder.uio.no (Microsoft Machine)' and a checkbox labeled 'Send CA Certificate Chain'. At the bottom of the dialog, there are three buttons: 'Erase User Password', 'Save', and 'Cancel'.

CISCO VPN CLIENT



The image shows a 'VPN Configuration' dialog box. It has a blue title bar with the text 'VPN Configuration' and a close button (X). The dialog is divided into two main sections. The top section is labeled 'VPN' and contains several text input fields: 'GroupName:' with the value 'VPN-GROUP', 'Group Key:' with the value 'SECRETOCOMPARTIDO', 'Host IP (Server IP):' with the value '70.70.70.70', 'Username:' with the value 'vpnuser', and 'Password:' with a masked password represented by dots. The bottom section is empty. At the bottom right of the dialog, there is a 'Connect' button.

PACKET TRACERT