Obiettivi:

- **creare il tunnel VPN site-to-site in tre passi (NAT, ISAKMP, IPSec);**
- **impostare il NAT;**
- **impostare il tunnel ISAKMP;**
- **impostare il tunnel IPSec.**

VPN

Site-to-site

IMPOSTAZIONE NAT per far uscire i pacchetti dalla Lan in Internet

Router 1 (vedi la topologia di rete con due sedi aziendali lontane, collegate tramite Internet)

Si ricorda di salvare con ***wr mem*** e controllare con ***show run***

```
enable
conf t
show run  //vediamo la configurazione generica di Fa0/0 e Fa0/1
```

IMPOSTAZIONE LISTA ACCESSI di nome FOR-NAT (di tipo Extended, non di tipo Standard):
si scrive: l'IP rete di partenza con wild card al posto di netmask e l'IP rete di arrivo con wild card.
Tutti i pacchetti dalla LAN Filiale alla LAN Sede **non devono** uscire con NAT in Internet, ma devono essere introdotti nel tunnel cifrato,
quindi escluderemo (**deny**) la "rotta Filiale-Sede" dal NAT, ma permetteremo **(permit)** di uscire con NAT a tutti i pacchetti che vanno dalla LAN Filiale in qualsiasi altra direzione **(any)**

```
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)#deny ip 192.168.2.0  0.0.0.255  192.168.1.0  0.0.0.255
Router(config-ext-nacl)#permit ip  192.168.2.0  0.0.0.255  any
Router(config-ext-nacl)#exit
```

INDICHEREMO l'interfaccia per la lista FOR-NAT, è l'interfaccia esterna Fa 0/0

```
Router(config)#ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
Router(config)#exit
Router#wr mem
```

Impostazione NAT:

```
interface FastEthernet0/0
description outside
ip nat outside

interface FastEthernet0/1
description inside
ip nat inside
```

Router 0

```
Enable  !  conf t  ! show run  //vediamo la configurazione generica di Fa0/0 e Fa0/1
```

LISTA ACCESSI di nome FOR-NAT:
si scrive: l'IP rete di partenza con wild card al posto di netmask e l'IP rete di arrivo con wild card
Tutti gli invii degli pacchetti dalla LAN Sede alla LAN Filiale **non devono** uscire con NAT in Internet, ma devono essere introdotti nel tunnel cifrato,
quindi escluderemo (**deny**) la "rotta Sede-Filiale" dal NAT, ma permetteremo **(permit)** di uscire con NAT a tutti i pacchetti che vanno dalla LAN Sede in qualsiasi altra direzione **(any)**

```
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)#deny ip  192.168.1.0  0.0.0.255  192.168.2.0  0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.1.0  0.0.0.255  any
Router(config-ext-nacl)#exit
Router(config)#exit
Router#wr mem
!
```

Impostazione NAT:

```
interface FastEthernet0/0
description outside
ip nat outside

interface FastEthernet0/1
description inside
ip nat inside
```

INDICHEREMO l'interfaccia per la lista FOR-NAT, è l'interfaccia esterna Fa 0/0

```
Router#conf t
Router(config)#ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
Router(config)#exit
Router#wr mem
```

PROVE Finita l'impostazione NAT, verifichiamo il ping da un PC al router di confine, cioè, "provider"
Dalla filiale all'ISP 210.210.2.1 :
PC2 (poi PC3) Scheda Desktop- Command Prompt ping 210.210.2.1 - va a buon fine
Dalla sede all'ISP 210.210.1.1 :
PC0 (poi PC1) Scheda Desktop- Command Prompt ping 210.210.1.1 - va a buon fine

IMPOSTAZIONE VPN sul router 0 I FASE

1) **Router#conf t**

Router(config)#crypto isakmp policy 1 *// indichiamo la politica con tutti i parametri del protocollo IKE per instaurare la connessione "tecnologica", cioè, il tunnel ISAKMP* (IKE Internet Key Exchange, RFC 2409). Le funzioni di IKE: 1.negoziazione dei parametri di sicurezza; 2. Autenticazione; 3.scambio delle chiavi; 4.gestione delle chiavi (dopo lo scambio) . IKE è costituito da 3 protocolli, tra cui ISAKMP) (Internet Security Association and Key Management Protocol) che specifica un'architettura per lo scambio di messaggi tra IPSec peer

Router(config-isakmp)#**encryption 3des** *//algoritmo di crittografia*
Router(config-isakmp)#**hash md5** *//algoritmo di hash*
Router(config-isakmp)#**authentication pre-share** //per autenticazione usare la chiave pre-share *("precedentemente condivisa",* algoritmo Diffie-Hellman*)*
Router(config-isakmp)#**group 2** *// indica il gruppo di Diffie-Hellman*
Router(config-isakmp)#**end**

2) Impostazione chiave di autenticazione pre-share "**cisco**" e dell'Ip esterno del router-**peer** (partner in filiale) Router#conf t
Router(config)#crypto isakmp key **cisco** address **210.210.2.2**

IMPOSTAZIONE VPN router 0 II FASE

Il protocollo IPSec comprende 3 protocolli, tra cui IKE (per negoziazione dei parametri di sicurezza, autenticazione e distribuzione delle chiavi) **e ESP** (Encapsulating Security Payload, per confidenzialità ed autenticazione dei pacchetti)

Indichiamo i parametri per IPSec-tunnel

A transform set is a combination of security protocols and algorithms that define how the security appliance protects data. Hashed Message Authentication Codes (HMAC) method to ensure the identity of the sender, and to ensure that the message has not been modified in transit.

1) **Il set di parametri "transform-set" di nome TS: usare algortimo crittografico 3des, algoritmo Hash md5 e Hmac** per autenticazione e integrità del messaggio (Hmac è obbligatorio per IPSec)

Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac

2) **Creare la lista di accesso al VPN**, cioè quale traffico deve essere criptato. Ci interessa in traffico dalla Sede (rete 192.168.1.0) diretto alla filiale (rete 192.168.2.0)

Router(config)#ip access-list extended **FOR-VPN** *//chiamiamo la lista FOR-VPN*
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#end

3) Creare la cripto mappa

Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 210.210.2.2 *//il nostro peer-router , della filiale, 210.210.2.2*
Router(config-crypto-map)#set transform-set TS *//usare il transform-set dei parametri di nome TS*
Router(config-crypto-map)#match address FOR-VPN *//deve essere criptato il traffico della lista FOR-VPN*
Router(config-crypto-map)#exit

3) **Ultimo passo: legare la cripto mappa ad una interfaccia.** Quale? – quella esterna, **Fa 0/**
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#wr mem

RIPETERE FASE I e FASE II per il Router 1 , da cambiare solo gli IP