VPN L’esercitazione dimostrativa del funzionamento delle liste di accesso FOR-NAT.

Le liste di accesso per incanalare il traffico criptato (FOR-VPN) non sono state impostate, quindi non c’è la comunicazione tra la Sede e la Filiale.
E’ stato aggiunto un Router-in-Internet che simula qualsiasi risorsa di Internet ed è raggiungibile sia dalla Sede che dalla Filiale

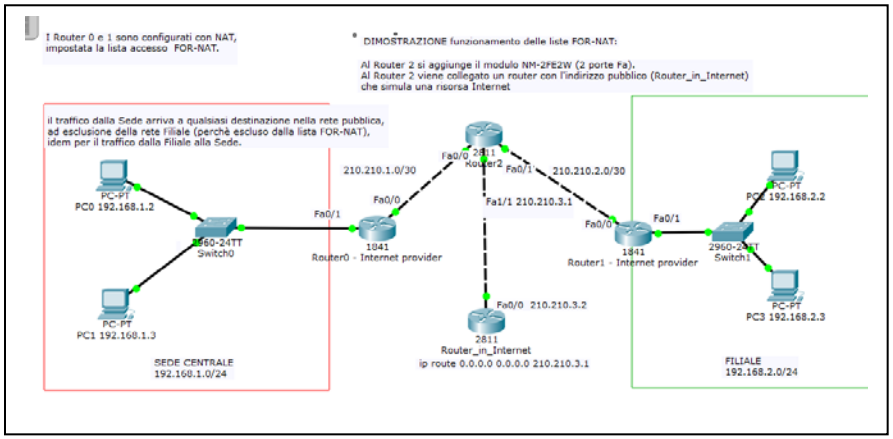
Router 0

ip access-list extended FOR-NAT
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.1.0 0.0.0.255 any

Router 1

ip access-list extended FOR-NAT
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.1.0 0.0.0.255 any

il traffico dalla Sede arriva a qualsiasi destinazione nella rete pubblica, ad esclusione della rete Filiale (perchè escluso dalla lista FOR-NAT), idem per il traffico dalla Filiale alla Sede.



Router 2

interface FastEthernet0/0
description VersoSede
ip address 210.210.1.1 255.255.255.252
!
interface FastEthernet0/1
description VersoFiliale
ip address 210.210.2.1 255.255.255.252
!
interface FastEthernet1/1
description RisorsaInternet
ip address 210.210.3.1 255.255.255.252

I Router 0 e 1 sono configurati con NAT, impostata la lista accesso FOR-NAT.

DIMOSTRAZIONE funzionamento delle liste FOR-NAT:

Al Router 2 si aggiunge il modulo NM-2FE2W (2 porte Fa).
Al Router 2 viene collegato un router con l'indirizzo pubblico (Router_in_Internet) che simula una risorsa Internet

il traffico dalla Sede arriva a qualsiasi destinazione nella rete pubblica, ad esclusione della rete Filiale (perchè escluso dalla lista FOR-NAT), idem per il traffico dalla Filiale alla Sede.