

Esercizio 22

Esercizio 1

Scopo dell'esercizio è la configurazione di una politica IPsec in ogni computer della rete di modo che il traffico dati TCP dal suo PC alla porta 21 del server Mendrisio e viceversa (canale di controllo FTP) sia autenticato e cifrato.

Come metodo di autenticazione vengono adoperati dei Certificati (rilasciati al computer). Come metodo di cifratura scelga l'algoritmo 3DES e per la funzione di Hash SHA-1.

Prima di iniziare l'esercizio si procuri il certificato per il computer (tramite Servizio Certificati).

Verifichi la Security Association del canale IPsec tramite **ipsecmon** e verifichi tramite Ethereal che il canale di controllo FTP è cifrato.