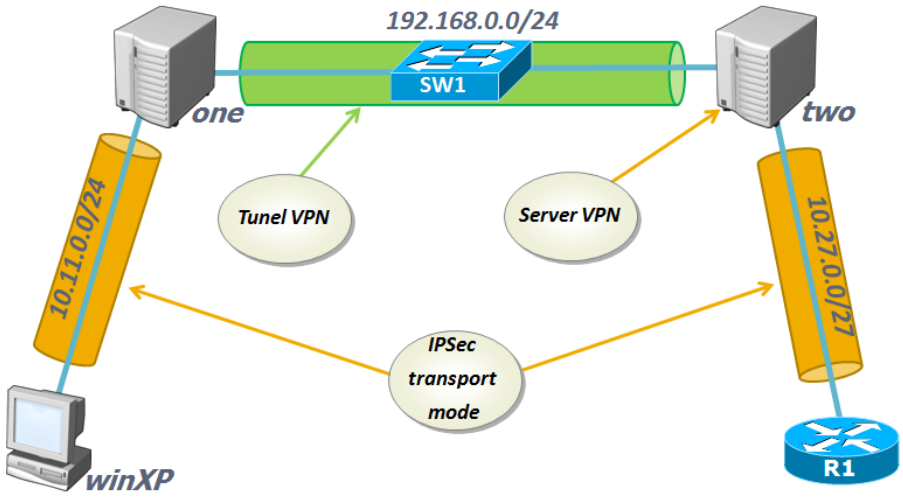
Laborator 4 – VPN şi IPSec

➢ Topologie



Toate calculatoarele din topologie au instalat programul Wireshark. După fiecare configuraţie verificaţi modul în care este trimis traficul (criptat vs. necriptat).

Pentru a putea rezolva acest laborator trebuie modificată din VMWare interfaţa Network Adapter 2 de pe calculatorul „two”, astfel încât aceasta să folosească adaptorul VMNet1(Host-only).

➢ Configurări de bază

1. [1 punct] Configuraţi pe calculatoarele “one” şi “two” rolul de Routing and Remote Access pentru a putea avea acces la serviciile de rutare şi de VPN. Pentru a putea testa conectivitatea între echipamente dezactivaţi Windows Firewall pe toate calculatoarele din reţea.

2. [1 punct] Configuraţi rute statice pe echipamentele din reţea pentru a avea conectivitate punct la punct între calculatorul “winXP” şi router-ul R1. Verificaţi accesând de pe calculatorul winXP prin telnet router-ul R1, folosiţi utilizatorul “cisco” şi parola “cisco”.

➢ IPSec

3. [1 punct] Configuraţi pe serverul “one” o regulă de IPSec prin care să forţaţi criptarea traficului de tip ICMP provenit de la calculatorul „winXP”. Pentru autentificare folosiţi cheia partajată “microsoft”, metoda de criptare pentru trafic este DES iar integritatea traficului se va asigura folosind MD5.

4. [1 punct] Configuraţi o regulă IPSec pentru calculatorul „winXP” astfel încât tot traficul de tip ICMP având ca destinaţie calculatorul „one” să fie acceptat de către destinaţie.

➢ VPN Server

5. [1 punct] Pe calculatorul “two” permiteţi doar porturi de tip PPPT şi L2TP/IPSec pentru accesul remote la acest server şi limitaţi numărul acestora la două pentru fiecare protocol.

6. [1 punct] Configuraţi calculatorul „one” astfel încât acesta să devină client de VPN pentru calculatorul „two”. Trebuie configurată o parolă pentru contul Administrator pentru a putea realiza această conexiune şi trebuie permis accesul în mod implicit din tab-ul Dial-in, pe calculatorul “two”.

7. [1 punct] Configuraţi calculatorul “two” astfel încât să primească doar conexiune folosind protocolul L2TP/IPSec pentru accesul remote şi cheia partajată pentru IPSec “microsoft”. Configuraţi această cheie şi pe calculatorul one şi verificaţi funcţionalitatea conexiunii.

8. [1 punct] Asignarea de adrese IP pentru noi clienţi de VPN poate fi făcută de server sau de un alt server de DHCP din reţea. Configuraţi serviciul de DHCP integrat cu rolul Routing and Remote Access astfel încât clientul să primească adrese IP din spaţiul 10.12.0.1 – 10.12.0.100.

9. [1 punct] Configuraţi utilizatorul Administrator astfel încât politica de acces remote să se stabilească prin serviciul NPS (Network Policy Server). Configuraţi folosind NPS o nouă politică Network Policies prin care să permiteţi accesul în intervalul orar 8-22 pentru orice utilizator.

10. [1 punct] Folosind rute statice permanente asiguraţi-vă că tot traficul spre reţeaua 10.27.0.0/24 trece prin interfaţa de VPN. Aplicaţi un filtru pe interfaţa de VPN folosind NPS astfel încât aceasta să nu accepte pachete de tip ICMP. Pentru verificare trebuie să refaceţi conexiunea de VPN dintre calculatoarele “two” şi “one”.

Pentru configuraţia curentă analizaţi care tip de trafic este criptat. Accesaţi router-ul R1 folosind calculatorul winXP şi calculatorul “one”, analizaţi traficul folosind Wireshark de pe calculatorul “two”.

➢ Advanced IPSec

11. [1 punct] Configuraţi router-ul R1 astfel încât acesta să primească doar trafic criptat pentru traficul de tip ICMP provenit din reţeaua locală. Pentru autentificare folosiţi cheia partajată “cisco”.

12. [1 punct] Configuraţi calculatorul „two” astfel încât să cripteze pachetele ICMP cu destinaţia calculatoarele din reţeaua 10.27.0.0/24. Pentru autentificare folosiţi cheia partajată “cisco”.