==========

Come realizzare una connessione VPN con Windows XP

Una rete privata virtuale tra PGP7 e Windows XP

by Emanuele –DiABlO– Zerbin

==========

La seguente procedura è stata testata su una macchina dove girava Windows XP Professional V.2002 senza alcun Service Pack.

Cliccate su Start, selezionate il Pannello di Controllo, cliccate su "Prestazioni e Manutenzione" (per la visualizzazione avanzata) e poi su "Strumenti di Amministrazione". Selezionate "Criteri di Protezione Locali", cliccate con il pulsante destro su "Criteri di Protezione IP su Computer Locale" e dal menù che appare scegliete "Gestisci Elenchi Filtri IP e Operazioni Filtro"; nella finestra che appare cliccate su Aggiungi.

Specificate un nome a voi comprensibile nella casella "Nome" (per esempio *PC1-su-PC2*), cliccate su "Aggiungi", poi su "Avanti". Come "Indirizzo di Origine" lasciate selezionata la voce "Indirizzo IP" e cliccate su "Avanti"; in "Indirizzo di Destinazione" selezionate

- "**Nome DNS Specifico**" se la macchina a cui vi volete connettere in vpn possiede un ip statico associato ad un dns; in questo caso inserite il nome host nella casella che appare, ciccate su "Avanti" e nella finestra "Avviso di Protezione" scegliete il pulsante "Si"
- "**Indirizzo IP Specifico**" se la macchina di destinazione possiede si un indirizzo IP statico, ma non un DNS; in questo caso inserite l'indirizzo IP nella casella che appare
- "**Subnet IP Specifica**" se la macchina a di destinazione non possiede un IP statico ma voi siete a conoscenza del range di variazione dell'IP dinamico (*es. macchina di destinazione connessa in dial-up con Libero con pop a Udine: l'IP varia da 151.25.0.0 a 151.25.254.254; nella casella "Indirizzo IP" inserirete 151.25.0.0 e in "Subnet Mask" 255.255.0.0*)

cliccate su "Avanti". In "Selezionare un Tipo di Protocollo" scegliete "Qualsiasi" e cliccate su "Avanti", selezionate la casella "Modifica Proprietà" e cliccate su "Fine".
Nella finestra "Proprietà – Filtro" assicuratevi che la casella "Speculare…" sia attivata e cliccate su "Ok". Nella finestra "Elenco Filtri IP" cliccate su "Ok".

Selezionate la seconda pagina ("Gestione Operazioni Filtro") della finestra "Gestisci Elenchi IP e Azioni Filtro", cliccate su "Aggiungi" e poi su "Avanti". Nella casella "Nome" inserite un titolo appropriato (per esempio *Cripto PC1-PC2*), cliccate su "Avanti", selezionate la casella "Negozia protezione", cliccate su "Avanti", selezionate "Non comunicare con i computer che non supportano IPSec", cliccate ancora su "Avanti", selezionate "Personalizzata" e cliccate sul pulsante "Impostazioni".
Nella finestra che appare selezionate la casella "Integrità Dati e Indirizzi senza Crittografia (AH)" e nel modulo associato scegliete "SHA1"; selezionate poi la casella "Integrità Dati con Crittografia (ESP)": nel modulo "Algoritmo di Integrità" scegliete "SHA1", mentre in "Algoritmo di Crittografia" scegliete "3DES"; lasciate deselezionate le altre caselle e cliccate su "Ok".
Cliccate su "Avanti", selezionate la casella "Modifica Proprietà" e cliccate su "Fine"
Nella finestra "Proprietà – Cripto PC1-PC2" deselezionate la casella "Accetta Comunicazioni non Protette…" e selezionate invece "PFS (Perfect Forward Secrecy)", cliccate su "Ok" e su "Chiudi" nella finestra "Gestisci Elenchi".

Cliccate con il pulsante destro su "Criteri di Protezione IP su Computer Locale", selezionate "Crea Criterio di Protezione IP": nella finestra che appare cliccate sul pulsante "Avanti", scegliete un nome per il vostro nuovo criterio di protezione (es. *IPSec PC1-PC2*), cliccate su "Avanti" e togliete la scelta "Attiva la Regola di Risposta Predefinita", cliccate ancora su "Avanti", lasciate selezionate la casella "Modifica Proprietà" e cliccate su "Fine".

Nel modulo "Regole di Protezione IP" della finestra "Proprietà – IPSec PC1-PC2" lasciate deselezionata la casella "<Dinamico>" e cliccate sul pulsante "Aggiungi", cliccate "Avanti" e selezionate "Questa regola non specifica un tunnel", cliccate "Avanti", lasciate selezionata l'opzione "Tutte le Connessioni di Rete" e cliccate ancora su "Avanti". Ora selezionate l'opzione "Utilizza questa stringa per proteggere…" e nel modulo sottostante inserite la parola chiave che è stata assegnata nella configurazione di PGP per il vostro computer; cliccate ancora su "Avanti". Nello spazio "Elenchi Filtri IP" selezionate la voce creata da voi (*PC1-su-PC2*), cliccate su "Avanti", nello spazio "Operazioni Filtro" selezionare il criterio creato da voi (*Cripto PC1-PC2*) e cliccate su "Avanti", lasciate selezionata la casella "Modifica Proprietà" e cliccate su "Fine".
Nella finestra "Proprietà – Nuova Regola" controllate che sia tutto come volete (se mi avete seguito fino qui dovrebbe esserlo) e selezionate "Ok". Nella finestra "Proprietà – IPSec PC1-PC2" cliccate su "Chiudi".

Abbiamo quasi finito. Nella finestra principale "Impostazioni Protezione Locale", nella sezione di destra, selezionate con il pulsante destro la nuova regola (*IPSec PC1-PC2*) e dal menù scegliete "Assegna".

Se possedete un router e/o un firewall (sia hardware che software) occorrerà aprire la porta UDP 500 sia in ingresso che in uscita.

==========

AVVERTENZE

- provare con dei ping la connessione IPSec fra le macchine
- se qualcosa non va, abilitare il logging (per sapere come si fa riferitevi alla piccola appendice alla fine di questa guida)
- per eseguire la connessione digitare dalla console (*Start > Esegui > cmd*) **ping -t host**, dove "host" corrisponde al nome dns del computer a cui vi volete connettere in vpn (quindi quello dove sarà installato PGP7); per un po' di tempo troverete visualizzato "Negoziazione IP in corso...", poi, se tutto è correttamente impostato, leggerete la normale risposta ai ping.

==========

Appendice – Abilitazione del Logging (dalla guida Microsoft)

" *To enable debug logging by IKE*
From the Windows desktop, click Start, click Run, and type regedt32 in the text box. Click OK. This starts the Registry Editor.
Navigate to HKEY_LOCAL_MACHINE on Local Machine.
Navigate to the following location: System\CurrentControlSet\Services\PolicyAgent.
Double-click PolicyAgent.
If the Oakley key doesn't exist, on the Edit menu, click Add Key.
Enter the Key Name (case sensitive): Oakley.

Leave Class blank, and click OK.
Select the new key, Oakley.
On the Edit menu, click Add Value.
Enter the Value Name (case sensitive): EnableLogging
Select Data Type: REG_DWORD and click OK.
Enter value 1
Click Hex as the Radix. Click OK
Exit from the Registry Editor.
At the Windows 2000 command prompt, type net stop policyagent, then type net start policyagent to restart the IPSec related services.
il file di log è \WINNT\debug\Oakley.log ”

==========

sabato 4 settembre 2004