

[Home](#) | [TechNet nel mondo](#) [Ricerca avanzata](#)

- Il programma TechNet Subscription
- Prodotti e tecnologie
- Soluzioni IT
- Eventi
- Sicurezza
- Supporto
- IT Community
- Newsletter
- Siti correlati

Installazione di una rete privata virtuale (VPN) con Windows 2000

Anche se l'espressione "rete privata virtuale" (VPN, Virtual Private Networking) ha un significato piuttosto ampio, la maggior parte degli esperti la utilizza per riferirsi alla creazione di un tunnel privato in una rete pubblica, ad esempio Internet. Grazie a una rete VPN i dati viaggiano tra computer attraverso una rete pubblica in modo protetto mediante l'incapsulamento dei pacchetti con un'intestazione contenente informazioni per il routing. Windows 2000 supporta i protocolli di tunneling del livello 2 (livello di collegamento dati - link layer), ad esempio PPTP e L2TP, che incapsulano i dati in una struttura PPP prima che possano essere trasmessi via cavo. Sono inoltre supportati i protocolli di tunneling del livello 3 (livello di rete - network layer), ad esempio IPsec. Tali protocolli incapsulano i pacchetti IP prima che vengano trasmessi.

Contenuti

Scenari VPN

È possibile sfruttare le caratteristiche delle reti VPN in diversi modi. Lo scenario più usuale è rappresentato dall'accesso da parte di un utente remoto alla rete aziendale tramite un tunnel VPN. Un altro scenario è rappresentato da un ufficio remoto che si connette alla rete aziendale mediante una connessione permanente o una connessione VPN remota a richiesta. Inoltre, è possibile eseguire il deployment delle reti VPN in una extranet per poter comunicare in modo protetto con i partner aziendali. Nel presente articolo verrà descritta l'installazione di una VPN nel primo scenario presentato, nel quale un utente remoto si connette alla rete aziendale tramite un tunnel VPN.



Configurazione di un server Windows 2000 per la rete VPN

Per configurare un server VPN, è necessario che il computer disponga di almeno due interfacce di rete. Per configurare un server Windows 2000 per le reti VPN, utilizzare la procedura seguente:

1. Aprire la console Routing e Accesso remoto in Strumenti di amministrazione.
2. Fare clic con il pulsante destro del mouse sul server e quindi scegliere *Configura e abilita Routing e Accesso remoto*.
3. Verrà avviata la Configurazione guidata server di Routing e Accesso remoto. Fare clic su Avanti.
4. Selezionare *Server configurato manualmente*, come mostrato nella figura 1, e quindi fare clic su Avanti.
5. Fare clic su Fine per completare la configurazione guidata.

Se il browser in uso non supporta frame non ancorati (inline), [fare clic qui](#) per la visualizzazione in una pagina distinta.

Figura 1 Abilitazione della rete VPN nel server

Non utilizzare l'opzione *Server VPN*. Configurazione guidata server di Routing e Accesso remoto non consente il routing, come spiegato nell'articolo della Microsoft Knowledge Base [Q2433](#). Questa opzione configura il server per le connessioni VPN in ingresso e protegge il server mediante filtri che lasciano passare solo il traffico PPTP o L2TP. Se ciò è quello che si desidera non vi è motivo di preoccuparsi. Tuttavia, è opportuno ricordare che l'utilizzo di questa opzione fa in modo che Routing e Accesso remoto blocchi tutti i pacchetti che non siano riferibili ai protocolli PPTP e L2TP.

Prima che gli utenti possano stabilire connessioni VPN al server, è necessario eseguire un'ulteriore operazione. Occorre assegnare agli utenti le autorizzazioni di connessione appropriate per l'accesso alla rete. A tal fine è possibile accordare agli utenti autorizzazioni di accesso remoto in Criteri di accesso remoto, come illustrato nella figura 2, oppure configurare autorizzazioni di connessione per ogni utente in Utenti e computer di Active Directory.

Se il browser in uso non supporta frame non ancorati (inline), [fare clic qui](#) per la visualizzazione in una pagina distinta.

Figura 2 Autorizzazioni di accesso remoto

Per impostazione predefinita, il numero di porte VPN create varia a seconda se si sceglie l'opzione *Server configurato manualmente*, nel qual caso vengono create solo cinque porte PPTP e cinque porte L2TP, o se si sceglie l'opzione *Server VPN*: in questo caso vengono create 128 porte PPTP e 128 porte L2TP. È sempre possibile regolare il numero di porte nella configurazione di Routing e Accesso remoto selezionando Porte e poi Proprietà.

Nota Se i client VPN passano attraverso un router o un firewall, accertarsi che, se si utilizza il protocollo PPTP, la porta TCP 1723 e il protocollo IP con ID 47 (GRE, Generic Routing Encapsulation) siano autorizzati a passare attraverso il router o il firewall. Se si utilizza il protocollo L2TP, è necessario aprire la porta UDP 500 (IKE), l'ID protocollo 50 (IPSec ESP) e l'ID protocollo 51 (IPSec AH).



Configurazione dei client

Per connettersi a un server VPN situato presso la rete aziendale, è innanzitutto necessario assicurarsi di essere connessi a Internet avendo composto il numero del provider ISP, a meno che non si disponga di una connessione dedicata a Internet (ad esempio, DSL) per la quale non occorre comporre alcun numero. La connessione a Internet immette nello stesso backbone mondiale di Internet a cui è connesso il server VPN aziendale. È quindi possibile stabilire una seconda connessione per creare un tunnel VPN.

A tal fine, seguire la procedura descritta di seguito:

1. Fare clic sul pulsante Start, scegliere Impostazioni, Rete e connessioni remote e selezionare Crea nuova connessione per avviare Connessione guidata di rete.
2. Nella schermata Tipo di connessione di rete selezionare *Connessione a una rete privata attraverso Internet*, come illustrato nella figura 3.

3. Nella schermata Rete pubblica è possibile configurare la connessione affinché componga automaticamente il numero del provider ISP prima di stabilire la seconda connessione al server VPN aziendale. Questa opzione va utilizzata solo se si dispone un modem analogico o ISDN per comporre il numero del provider ISP e connettersi a Internet.
4. Attenersi alle istruzioni visualizzate sullo schermo per completare la procedura guidata.

Se il browser in uso non supporta frame non ancorati (inline), [fare clic qui](#) per la visualizzazione in una pagina distinta.

Figura 3 Tipo di connessione di rete

Per impostazione predefinita, quando si utilizza questa connessione è possibile digitare solo il nome utente e la password. Per aggiungere l'opzione relativa al dominio, fare clic su Proprietà e nella scheda Opzioni selezionare la casella *Includi dominio di accesso Windows* come mostrato nella figura 4.

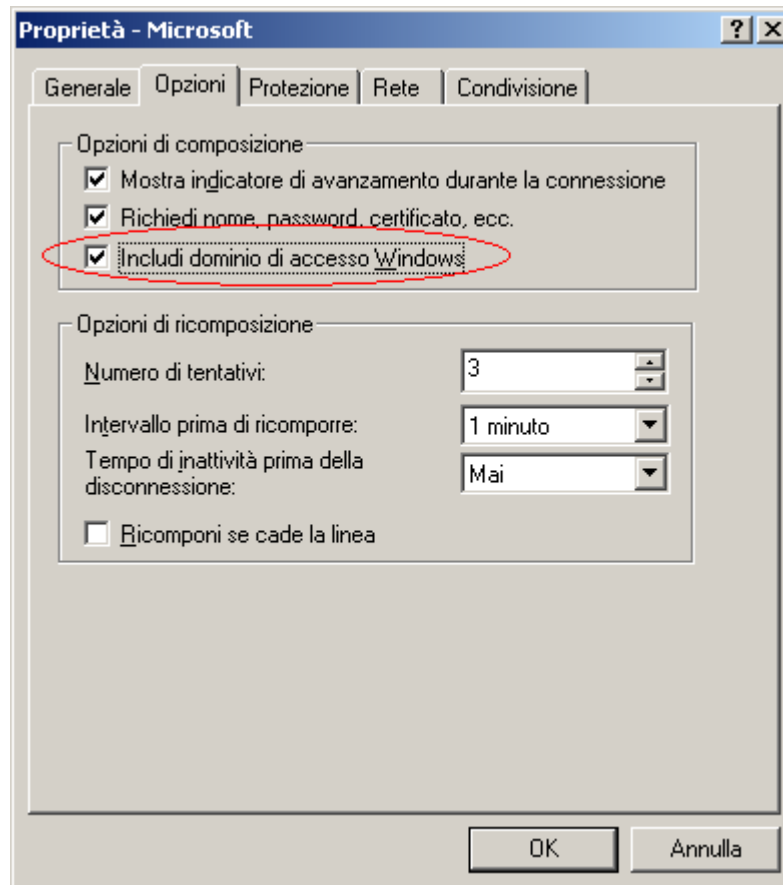


Figura 4 Opzione Includi dominio di accesso Windows



Livelli di crittografia supportati dalle reti VPN

A seconda di come ci si connette al server VPN, viene utilizzata la crittografia MPPE o IPSec. Se ci si connette a un server PPTP, si utilizza la crittografia MPPE, mentre se ci si connette a un server L2TP, si utilizza la crittografia IPSec. Per impostazione predefinita, la rete VPN è configurata automaticamente per un tipo di server, ovvero, prima di tentare l'utilizzo della crittografia MPPE con il protocollo PPTP, si prova a utilizzare la crittografia IPSec con il protocollo L2TP. La crittografia MPPE funziona in modo diverso da quella IPSec. Dato che i pacchetti possono giungere a destinazione fuori sequenza, la crittografia MPPE utilizza un numero di sequenza nell'intestazione per tenere traccia dei pacchetti e modifica la chiave crittografica di ogni pacchetto in base al numero di sequenza. L'utilizzo di una connessione L2TP necessita di certificati IPSec. Se si verificano problemi nello stabilire una connessione VPN, provare a selezionare PPTP come tipo di connessione anziché l'opzione predefinita Automatica. Se si seleziona l'impostazione Automatica e non è possibile negoziare una sessione IPSec, potrebbe dover essere necessario attendere a lungo (fino a 2 minuti) prima che il protocollo PPTP sia nuovamente selezionato automaticamente.

Per la crittografia sono supportate quattro opzioni che è possibile configurare selezionando Modifica profilo nella sezione Proprietà di Criteri di accesso remoto. Nella scheda Crittografia è possibile selezionare Senza crittografia, Livello minimo, Livello avanzato o Livello massimo. L'opzione Livello massimo (128 bit) è disponibile solo se si installa [Windows 2000 High Encryption Pack](#) (è consigliabile installare [Windows 2000 Service Pack 1](#)).

Nella tabella seguente è incluso un confronto tra i vari tipi di crittografia utilizzati per la connessione remota con il protocollo PPTP rispetto al protocollo L2TP su connessioni VPN I

	Connessione remota e protocollo PPTP	Protocollo L2TP su IPSec
Livello minimo	Crittografia MPPE a 40 bit	Crittografia DES a 56 bit

Livello avanzato	Crittografia MPPE a 56 bit	Crittografia DES a 56 bit
Livello massimo	Crittografia MPPE a 128 bit	Crittografia 3DES (tre chiavi a 56 bit)



Informazioni sulla struttura dei pacchetti

Struttura dei pacchetti PPTP

Nella figura 5 che segue viene illustrata la struttura dei pacchetti di dati PPTP quando passano attraverso un tunnel. Viene innanzitutto creata una struttura PPP incapsulando i dati PPP crittografati con un'intestazione (header) PPP. Quindi, la struttura PPP viene incapsulata con un'intestazione GRE. Il pacchetto risultante viene incapsulato con un'intestazione IP, che include informazioni sugli indirizzi IP di origine e di destinazione. Infine, questo datagramma viene incapsulato con l'intestazione e il riempimento (trailer) del livello di collegamento da che variano a seconda della tecnologia in uso. Ad esempio, se si inviano datagrammi IP su rete Ethernet, essi vengono incapsulati con un'intestazione e un riempimento Ethernet, se si invia su una linea telefonica analogica vengono incapsulati con un'intestazione e un riempimento PPP, e così via. Quando i pacchetti raggiungono la destinazione, le intestazioni vengono rimosse una alla volta in ordine inverso. Prima vengono rimossi l'intestazione e il riempimento del livello di collegamento dati, quindi le intestazioni IP, GRE e PPP. Infine vengono decrittografati i dati PPP.

Intestazione del collegamento dati	Intestazione IP	Intestazione GRE	Intestazione PPP	Dati PPP crittografati (IP, IPX, NetBEUI)	Riempimento del collegamento dati
------------------------------------	-----------------	------------------	------------------	---	-----------------------------------

Figura 5 Struttura dei pacchetti PPTP

Struttura dei pacchetti L2TP

La struttura dei pacchetti L2TP è alquanto simile a quella dei pacchetti PPTP per il fatto che le intestazioni vengono aggiunte ai dati PPP. Nella figura 6 viene illustrata la struttura dei pacchetti L2TP. Si noti che tutto ciò che è compreso tra l'intestazione UDP e il riempimento IPsec viene crittografato.

Se il browser in uso non supporta frame non ancorati (inline), [fare clic qui](#) per la visualizzazione in una pagina distinta.

Figura 6 Struttura dei pacchetti L2TP



Una soluzione molto diffusa

Le reti VPN rappresentano un metodo utile per l'accesso protetto alle reti aziendali nell'ambito del tele-lavoro. Risultano inoltre vantaggiose nelle filiali e nelle extranet, dove rappresenta un'estensione protetta della rete LAN su una rete pubblica. Rispetto alle soluzioni di connessione remota tradizionali, le reti VPN si sono molto diffuse di recente grazie alla loro facilità di gestione e al loro ridotto costo di esercizio.



[Note legali](#) [Informativa sulla privacy](#)