



IPSec callback e DHCP su IPSec



Funkwerk Solution - IPSec Callback:

Assicurare la raggiungibilità di due Peer per la creazione di una connessione tramite Internet

L'utilizzo dei DynDNS permette a due Peer di creare una connessione tramite Internet anche nel caso di utilizzo di indirizzi IP dinamici. Il servizio DynDNS non è però in grado di controllare se un Peer è effettivamente online e neanche fare in modo che il Peer, in caso di necessità, possa creare una connessione Internet. A partire dalla Software Release 6.2.5 questo limite è superato grazie alla disponibilità dell'IPSec Callback. Una chiamata ISDN al Peer segnala il proprio stato di online e la disponibilità alla creazione di un Tunnel. Se il terminale remoto non ha al

momento una connessione Internet, la chiamata ISDN fa in modo che crei questa connessione. Per assicurare la reciproca raggiungibilità, è possibile configurare sul Gateway due differenti modalità. La Figura 1 mostra il metodo dell'operazione dal punto di vista del Gateway situato nella sede centrale. In modalità attiva, il Router locale invia una chiamata ISDN al terminale remoto per fare in modo che questi crei un Tunnel IPSec. Se il dispositivo è configurato in modalità passiva, reagisce semplicemente alla chiamata ISDN in entrata ed inizia a creare, se necessario, il Tunnel IPSec verso il Peer.

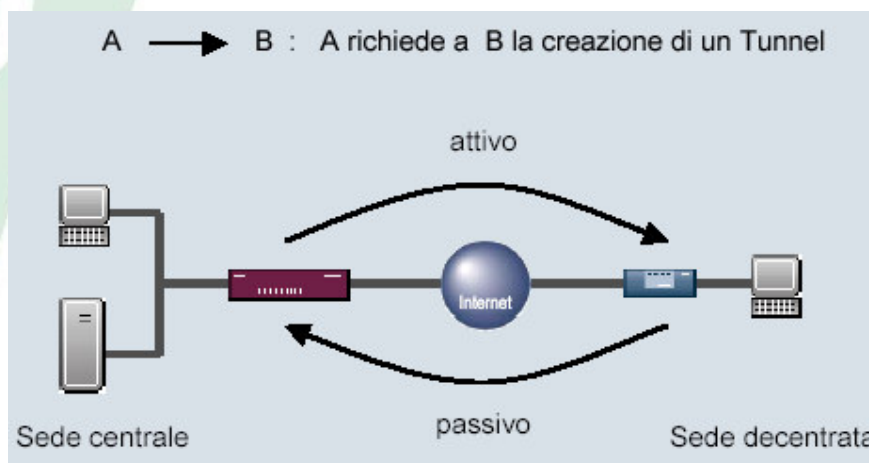


Figura 1: Modalità per l'IPSec Callback



Funkwerk Solution - DHCP over IPSec: Connessione di Host virtuali

Il Dial-in di utenti remoti verso la sede centrale avviene normalmente grazie ad un indirizzo IP assegnato dal Service Provider in modo dinamico. Questo indirizzo viene utilizzato come indirizzo di invio per tutti i pacchetti dati inviati dall'Host remoto. In alcuni casi può essere necessario dare a questi pacchetti un indirizzo IP della rete aziendale, ad esempio per essere in grado di assegnare diritti di accesso. Questo vale per tutti gli scenari nei quali esiste una appartenenza sulla base dell'indirizzo IP e che sono limitati all'ambito interno. Il collaboratore esterno di una società che si collega alla rete aziendale utilizzando l'indirizzo IP assegnatogli dal Provider, non

avrebbe possibilità alcuna di accedere ai dati. Con la funzionalità "DHCP over IPSec" è ora possibile assegnare all'Host remoto, al momento del Dial-in, un indirizzo IP dall'ambito degli indirizzi della rete aziendale. L'Host remoto appare quindi come se fosse un Host virtuale nella rete aziendale (Figura 1). Un IPSec Tunnel permette ora di creare una connessione tra l'Host remoto ed il Gateway VPN. All'Host remoto viene assegnato un indirizzo IP dal Pool della rete aziendale. A questo scopo è possibile utilizzare un Server DHCP dedicato o il Router Bintec.

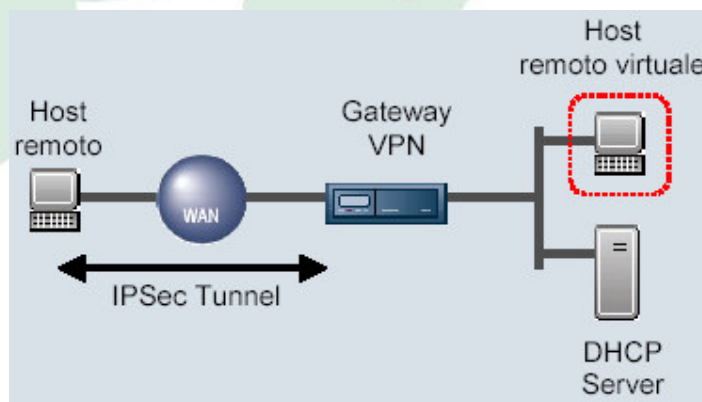


Figura 1: Configurazione DHCP tramite Tunnel IPSec



Funkwerk Solution - SCEP: Richiesta e Download automatico di certificati per dispositivi Bintec

Grazie all'installazione di certificati digitali, è possibile assegnare una chiave pubblica ad una persona in modo univoco e comprovabile. Ad esempio, l'installazione di certificati digitali è molto diffusa nelle VPN IPsec o nelle infrastrutture PKI. A partire dalla Release 6.3.1, Bintec supporta il protocollo SCEP (Simple Certificate

Enrollment Protocol) che permette una pubblicazione sicura di certificati. Ciò significa che il dispositivo Bintec non solo è in grado di inviare alla Certificate Authority (CA) la richiesta di un certificato PKCS#10, ma può anche, dopo la firma da parte della CA, eseguire automaticamente il Download del certificato e memorizzarlo nella configurazione del dispositivo (Figura 1).

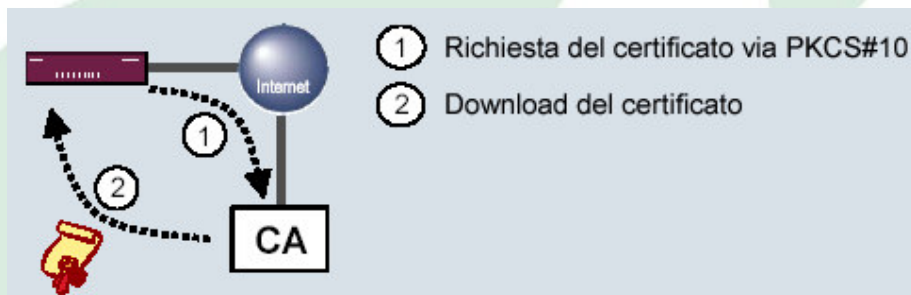


Figure 1: Certificate request and issue using SCEP

Lo stato del Router Bintec durante il cosiddetto processo di "Enrollment" può venire salvato temporaneamente sul dispositivo. Se il dispositivo Bintec dovesse eseguire il Reboot durante la richiesta ed assegnazione del certificato, lo stato del processo di Enrollment non verrebbe perso e potrebbe venire continuato, nella posizione appropriata, dopo il Reboot.