NOKIA

D211

PROTEZIONE DEI DATI

NOKIA

Sommario

1. INTRODUZIONE

La nuova scheda radio a modalità multipla Nokia D211 è la soluzione ideale per gli utenti di dispositivi mobili che desiderano accedere alla rete aziendale durante i loro spostamenti. Le informazioni trasferite spesso sono d'importanza critica per un'azienda e come tali devono rimanere riservate. La protezione ha quindi un ruolo importante nell'utilizzo della Nokia D211 per i servizi ad accesso remoto.

In questo documento verrà indicato come affrontare il problema della protezione quando si utilizza una scheda radio Nokia D211. Dopo aver introdotto le nozioni di base sulla protezione Internet, verranno illustrate alcune architetture di riferimento che consentono un accesso protetto a una rete aziendale su reti GPRS (General Packet Radio Service) e su reti WLAN (Wireless Local Area Networks).

2. ARCHITETTURE PER L'ACCESSO REMOTO

2.1 ACCESSO REMOTO TRAMITE MODEM

Fino a poco tempo fa, i servizi di accesso remoto venivano perlopiù implementati mediante linee dedicate, modem di accesso remoto o server di accesso remoto. La connessione viene stabilita utilizzando la rete telefonica pubblica e il noto protocollo PPP (Point-to-Point Protocol), disponibile in quasi tutte le applicazioni terminale. La connessione viene stabilita usando un telefono fisso o un terminale senza filo. Il server di accesso remoto esegue l'autenticazione dell'utente tramite una password. In genere non sono coinvolti altri meccanismi di protezione.

La scheda radio D211 offre due alternative per l'accesso remoto: dati GSM e HSCSD (High Speed Circuit Switched Data). In questa configurazione, la rete GSM protegge i dati dell'utente sulla connessione. In tal modo l'accesso senza filo non richiede ulteriori misure precauzionali e può essere utilizzato come un modem di accesso remoto. Generalmente la connessione di accesso remoto viene stabilita tramite la funzionalità di accesso remoto di Microsoft Windows.

2.2 ACCESSO INTERNET PROTETTO (GPRS, WLAN)

Le nuove tecnologie Internet senza filo, quali GPRS e WLAN, offrono un modo più veloce e conveniente per accedere ai dati aziendali. I nuovi meccanismi di accesso richiedono alcuni miglioramenti alla piattaforma dei servizi aziendali di accesso remoto per garantire la riservatezza dei dati.

Nella figura 1 sono illustrate le architetture di accesso Internet e di accesso remoto La differenza principale consiste nel fatto che, anziché una rete telefonica, le tecnologie GPRS e WLAN utilizzano la dorsale Internet come gateway per la rete aziendale. I dati dell'utente sono trasmessi dalla rete cellulare alla rete aziendale tramite la rete Internet, non protetta, usando i protocolli Internet.

La rete Internet pubblica è esposta a numerosi rischi di protezione. La debolezza principale risiede nel fatto che, a differenza di quanto avviene in una connessione di accesso remoto con il protocollo PPP, i pacchetti Internet sono leggibili da chiunque abbia accesso alla rete. Poiché i pacchetti IP tendono a seguire lo stesso percorso, tutti i pacchetti risultano esposti a potenziali intrusioni. Le funzioni di protezione delle reti GPRS e WLAN non sono sufficienti a garantire la riservatezza. Per creare un sistema di accesso remoto altamente affidabile, è possibile combinare l'accesso senza filo con una soluzione di protezione Internet end-to-end.

Nota: Per un accesso GPRS/WLAN protetto, Nokia consiglia di utilizzare una soluzione VPN (Virtual Private Network, rete privata virtuale) a livello IP, già ampiamente adottata.

Nei seguenti paragrafi verrà illustrato come utilizzare questa tecnologia per l'accesso GPRS, per la connettività aziendale LAN senza filo e per la connettività dei singoli utenti.

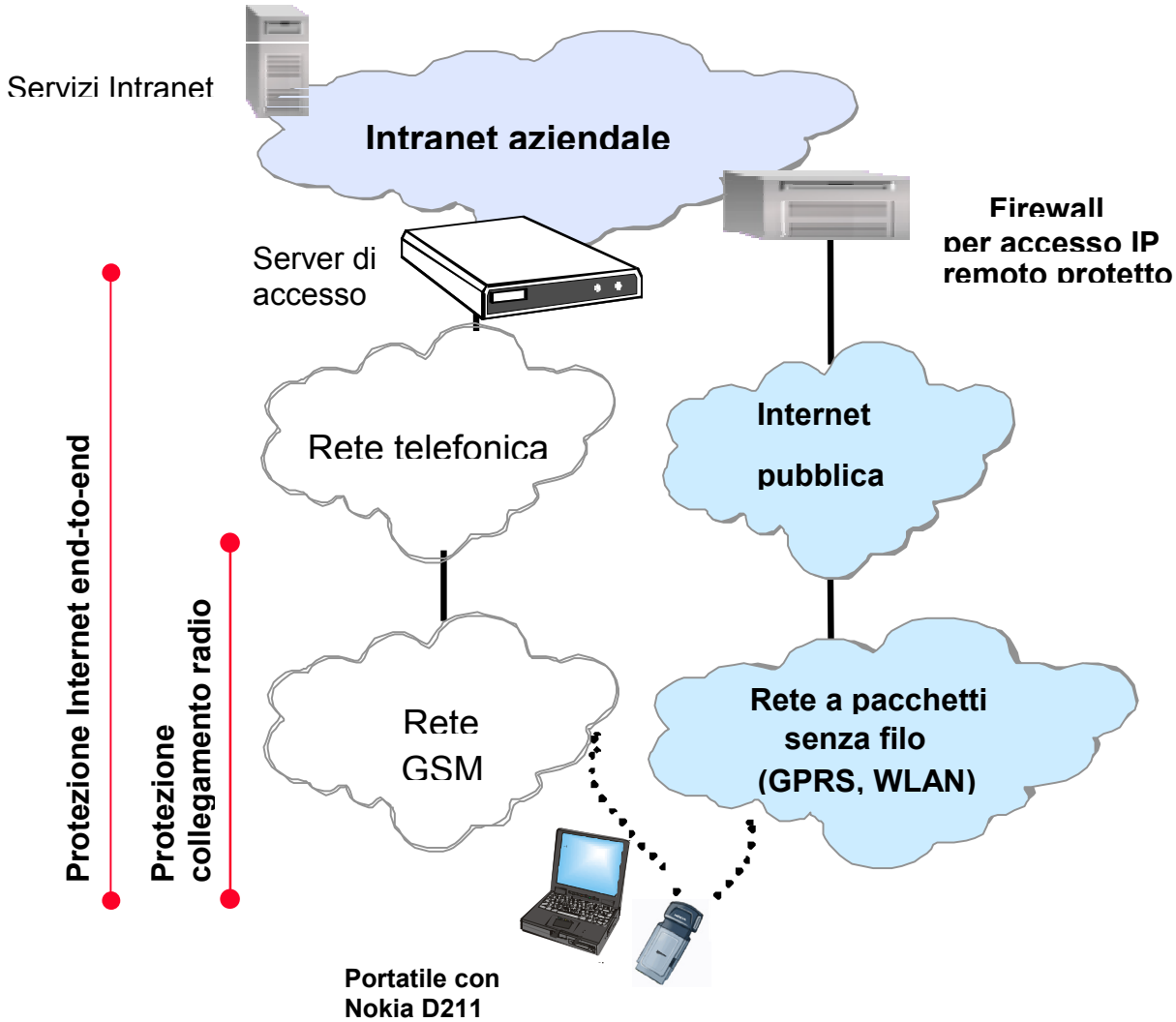


Figura 1: Meccanismi alternativi di accesso remoto: accesso remoto e accesso Internet

2.2.1 Requisiti per la protezione Internet

Al fine di garantire la protezione dei dati e della rete aziendale, una soluzione di protezione Internet dovrebbe includere le seguenti funzioni critiche:

- Controllo dell'accesso alla rete aziendale con restrizioni per gli utenti non autorizzati.
- Utilizzo della crittografia per impedire a chiunque la lettura o la copia dei dati durante il loro spostamento su Internet. La crittografia dei viene utilizzata per proteggere i dati da utenti non autorizzati mediante codifica dei contenuti. Esistono diversi metodi di crittografia, che si differenziano tra loro principalmente per gli algoritmi.
- Autenticazione per verificare che i dati provengano dall'origine dichiarata.

La tecnologia VPN è ampiamente usata per connettere LAN aziendali tra i diversi siti o partner commerciali esterni alla rete aziendale.

2.2.2 La tecnologia VPN in breve

Nella figura 2 è illustrata una configurazione VPN tipica. La stessa tecnologia e la stessa piattaforma possono essere impiegate per fornire un accesso remoto protetto per utenti di reti GPRS e LAN senza filo.

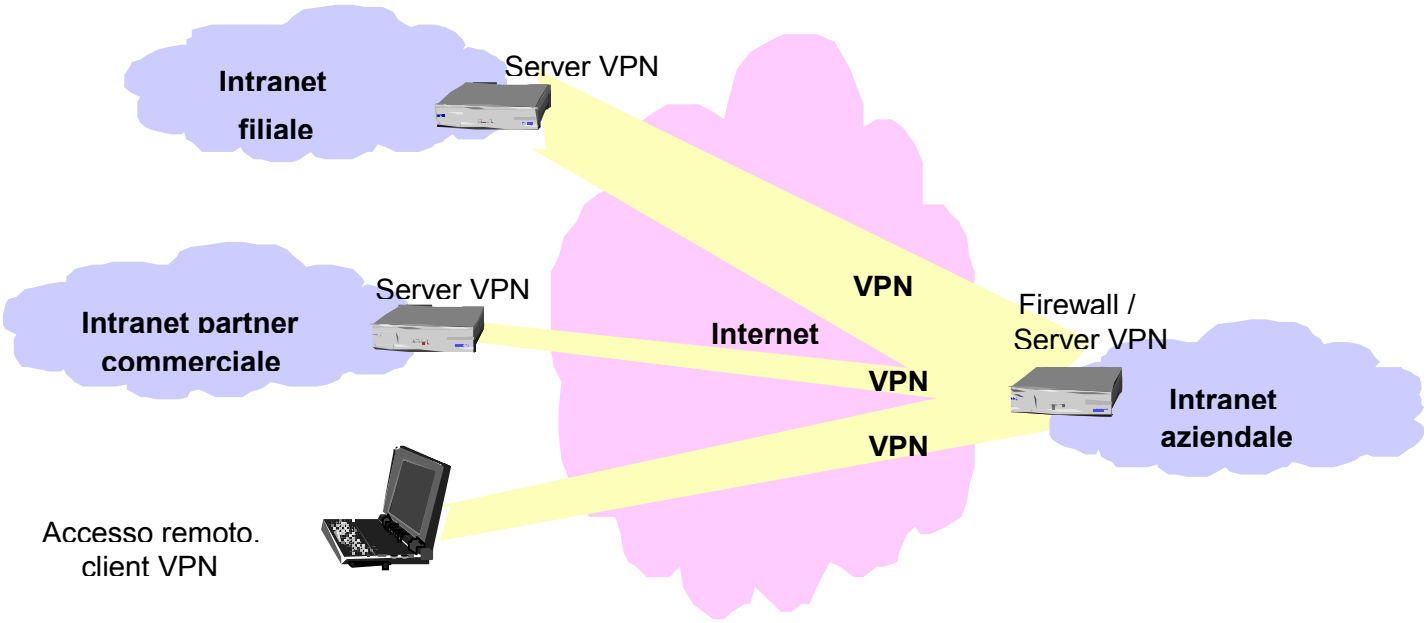


Figura 2: Rete privata virtuale

La soluzione VPN si compone di un server di rete e di un software client. Il server VPN protegge da comunicazioni indesiderate o non autorizzate all'interno o all'esterno della rete protetta. Tutto il traffico verso la rete privata viene fatto passare dal server VPN. Viene creato un tunnel tra il terminale e il server VPN e i dati dell'utente vengono autenticati, crittografati e trasmessi mediante il tunnel all'host.

La rete VPN ha il vantaggio di proteggere le informazioni trasmesse da e verso la rete Intranet e di impedire l'accesso non autorizzato. Le reti VPN non mantengono collegamenti

permanenti tra punti terminali. Quando si rende necessaria, viene creata una connessione tra un terminale e la rete aziendale, che verrà poi eliminata una volta chiusa. Il client stabilisce il tunnel protetto e la rete autentica l'utente remoto. Tramite l'autenticazione utente vengono confermate le identità di tutti gli utenti remoti. L'accesso alla rete aziendale è concesso solo dopo il completamento dell'autenticazione. Sono disponibili diversi meccanismi di autenticazione alternativi, quali password, token di protezione memorizzati, ad esempio, su schede smart e certificati.

Il tunnelling end-to-end protegge la trasmissione dati da attacchi alla protezione. I client e i server VPN spesso dispongono anche di un firewall incorporato. Un cosiddetto firewall "personale" filtra i dati in ingresso e rende possibili le connessioni Internet solo da host predefiniti. In tal modo si possono prevenire intrusioni nel terminale remoto.

La crittografia integrata rende praticamente impossibile la lettura dei dati da parte di utenti non autorizzati. La maggior parte dei dispositivi VPN negozia automaticamente l'utilizzo dei più elevati algoritmi di crittografia e autenticazione dati tra le parti che effettuano la comunicazione. La crittografia è trasparente per tutte le applicazioni che utilizzano i protocolli IP, quali la posta elettronica e i browser Web. L'unica conseguenza significativa è rappresentata dal fatto che l'incapsulamento VPN comporta l'invio di una piccola quantità di dati aggiuntivi sulla connessione senza filo.

2.2.3 Dispositivi VPN commerciali

Sul mercato è presente un'ampia gamma di soluzioni VPN commerciali. Un gateway di protezione VPN potrebbe essere adatto per le seguenti categorie: router VPN ad alte prestazioni, firewall, hardware VPN integrato e software VPN economico. La crittografia dei pacchetti è normalmente inclusa nei router, sia come software aggiuntivo che come scheda a circuiti supplementare. Quest'ultima è la soluzione ideale per situazioni che richiedono una maggiore velocità di trasmissione dei dati. La combinazione di tunnelling, crittografia e firewall è probabilmente la soluzione migliore per reti di piccole dimensioni con basso volume di traffico.

Nella maggior parte dei casi, è il responsabile IT dell'azienda che sceglie e amministra il sistema VPN. La gamma di prodotti disponibili è ampia. Il criterio fondamentale per scegliere la soluzione appropriata è la capacità richiesta, ovvero il numero di utenti che effettuano l'accesso remoto. La rete VPN normalmente deve effettuare una conversione dello schema di indirizzi IP tra la rete aziendale e la rete dell'operatore. Si consiglia quindi di scegliere una soluzione che supporti la conversione degli indirizzi di rete (NAT, Network Address Translation).

L'interoperabilità standardizzata tra dispositivi VPN diversi garantisce l'interoperabilità tra client VPN e numerosi server VPN. L'interoperabilità della scheda radio Nokia D211 è stata verificata con i principali prodotti server e client VPN. È possibile consultare un elenco dettagliato dei prodotti verificati all'indirizzo: www.nokia.com.

2.2.4 Firewall personale

Firewall personale è un software dotato di un insieme di regole che permette o nega il traffico di rete tramite un computer. Monitora o controlla le applicazioni con lo scopo di proteggerle da cavalli di troia e keylogger. Viene impiegato principalmente per migliorare la protezione

quando si utilizza un client VPN. Un firewall personale controlla l'accesso al PC dell'utente. Quando un computer portatile viene utilizzato in una rete non protetta, è necessario che il livello di protezione sia molto alto. Tutti i tentativi di connessione al computer devono infatti essere negati. Quando il modulo di gestione del firewall individua un intruso, segnala al software di bloccare l'indirizzo IP dell'hacker. Dato che il firewall controlla la trasmissione a livello dello stack TCP/IP della rete, gli hacker non sono in grado di circumnavigare un blocco nel firewall. Questo tipo di protezione deve essere attivata sempre e in qualsiasi luogo.

2.3 PROTEZIONE A LIVELLO APPLICATIVO PER LA NAVIGAZIONE INTERNET

Alcune applicazioni Internet, quali i browser Web, offrono un livello di protezione aggiuntivo. Le ultime versioni di Netscape e Internet Explorer utilizzano protocolli di protezione a livello applicativo, quali TLS (Transport Layer Security) e SSL (Secure Socket Layer), che garantiscono la protezione dei dati degli utenti tra l'applicazione client e il server. Questi meccanismi sono utilizzati su ampia scala ad esempio per le transazioni elettroniche e bancarie su Internet.

La protezione a livello applicativo assicura un livello di protezione aggiuntivo che può essere utilizzato per l'accesso a Internet nei casi in cui non siano coinvolte informazioni aziendali riservate e il terminale mobile non contenga informazioni riservate. In questi casi è possibile utilizzare la scheda radio Nokia D211 senza servizi VPN. I meccanismi di protezione a livello applicativo non proteggono però il terminale mobile da attacchi esterni. Inoltre il livello di crittografia è spesso inferiore rispetto a una connessione VPN.

Nota: in caso di applicazioni con dati aziendali, si consiglia di utilizzare sempre il tunnelling VPN end-to-end. La protezione a livello applicativo offrirà quindi un livello di protezione aggiuntivo rispetto a quello già garantito dal tunnelling VPN.

3. ACCESSO GPRS PROTETTO ALLA RETE AZIENDALE

La rete GPRS standard offre protezione durante la connessione, ma non garantisce alcuna soluzione di protezione Internet end-to-end per l'accesso mobile a una LAN aziendale. In questo tipo di rete sono assicurate due funzioni di protezione: *autenticazione del sottoscrittore* e *crittografia dei dati*. Le procedure di autenticazione degli utenti in GPRS sono simili a quelle della rete GSM. Tutte le funzioni di protezione si basano sulla chiave segreta Ki, presente sia sulla carta SIM (Subscriber Identity Module) che nel registro delle ubicazioni degli operatori. In GPRS, i dati e i segnali vengono crittografati tra il terminale e Internet.

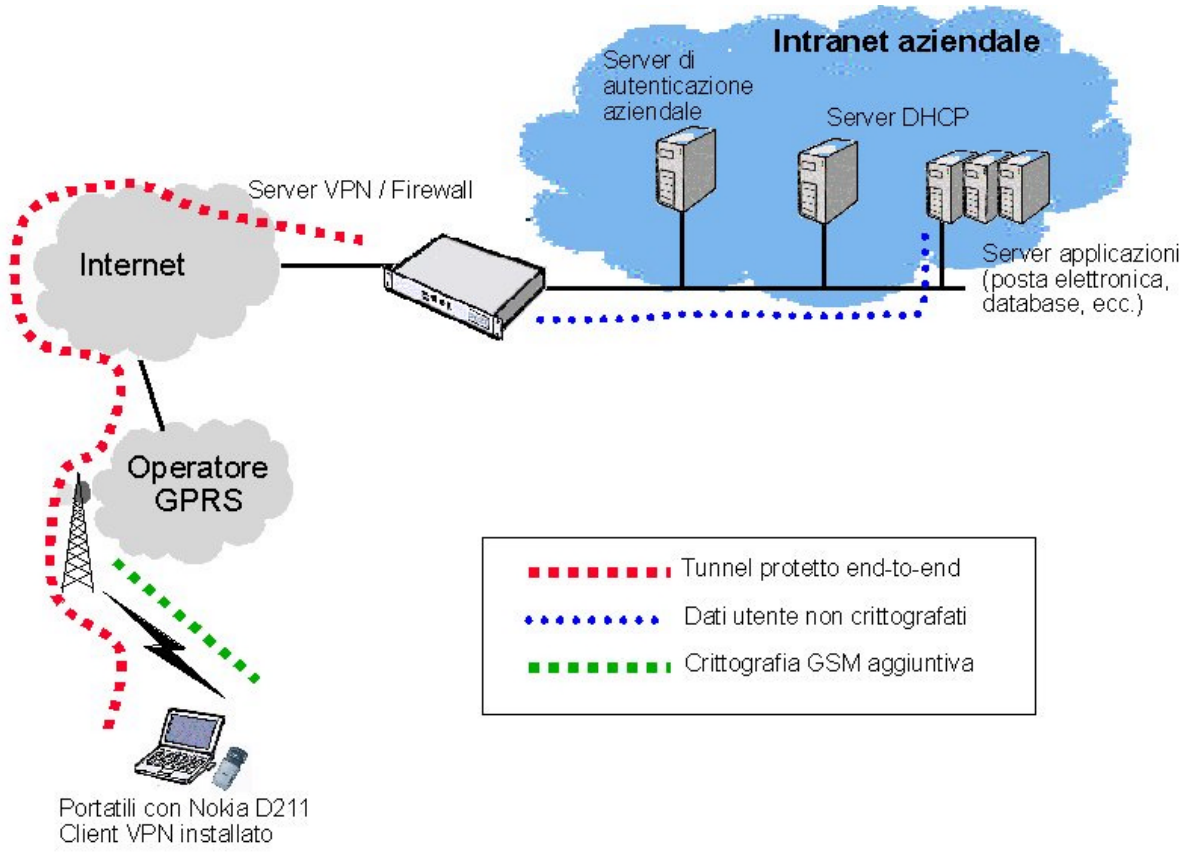
Nota: per le connessioni GPRS con la scheda radio Nokia D211 per scopi aziendali si consiglia di utilizzare una soluzione di protezione VPN che garantisce autenticazione e crittografia dei dati end-to-end.

Una soluzione VPN non è necessaria se GPRS viene utilizzato per applicazioni non riservate, ad esempio la navigazione su Internet. Normalmente il servizio VPN viene fornito dall'IM aziendale o dall'operatore di telefonia mobile. Il sistema, illustrato nella figura 2, funziona come indicato di seguito:

1. L'utente attiva la connessione GPRS.

2. La rete GPRS esegue l'autenticazione del terminale mobile con la carta SIM e viene stabilito un collegamento GPRS senza fili protetto con Internet (crittografia GPRS).
3. L'utente esegue il client VPN sul terminale mobile, stabilendo un tunnel IP con crittografia end-to-end con la rete aziendale (crittografia dati Internet).

Questa soluzione è estremamente affidabile e protetta, in quanto tutto il traffico viene crittografato dal terminale mobile al server VPN aziendale e VPN offre un livello di protezione elevato. L'utente può eccedere alla Intranet da qualunque rete di operatori GPRS.



Accesso GPRS remoto

Figura 3: accesso GPRS protetto ai dati aziendali

In alternativa, è possibile utilizzare una connessione dedicata dalla rete GPRS dell'operatore di telefonia mobile alla Intranet aziendale, escludendo completamente la rete pubblica Internet. In questo modello, il terminale mobile non richiede alcun client VPN. Le funzioni di protezione della rete GPRS assicurano protezione dei dati tra il terminale e il fulcro della rete GPRS. L'operatore di telefonia mobile stabilisce quindi un tunnel protetto tra la propria rete la rete aziendale. Con questo approccio, il cliente aziendale deve fidarsi dell'operatore di telefonia mobile che offre il tunnelling protetto. Non sono molti gli operatori di telefonia mobile che offrono questo tipo di soluzione per grandi aziende. Per informazioni dettagliate, rivolgersi al proprio operatore di telefonia mobile.

4. ACCESSO SICURO A LAN SENZA FILO

Le LAN senza filo vengono solitamente utilizzate in uffici, abitazioni o zone di accesso pubblico, quali hotel, aeroporti e così via. Consentono agli utenti di spostarsi con flessibilità all'interno dell'ufficio e delle sale riunioni o lavorare dalla propria abitazione, avendo sempre a disposizione le ultime informazioni della rete aziendale. Analogamente alle reti GPRS, anche le reti LAN utilizzano la dorsale Internet. Di conseguenza, la stessa piattaforma di accesso remoto VPN protetta che supporta GPRS supporta anche le LAN senza filo. Per la connessione alla rete aziendale, gli utenti della scheda radio Nokia D211 possono scegliere tra collegamenti LAN senza filo o GPRS, quindi utilizzare la stessa configurazione VPN.

Le WLAN possono incorrere in rischi di protezione nel momento in cui i segnali radio escono dall'edificio dell'azienda. Questi rischi possono essere evitati utilizzando l'autenticazione e la crittografia adeguate.

Nota: per l'accesso a dati aziendali su LAN senza filo, si consiglia di utilizzare una soluzione VPN end-to-end.

La specifica LAN (IEEE 802.11b) contiene l'algoritmo di protezione WEP (Wired Equivalent Privacy), utilizzabile per l'autenticazione dei terminali nelle LAN senza filo e per la crittografia dei dati sul collegamento radio. Il livello di protezione di WEP non è elevato se confrontato alla protezione IP (VPN). WEP può essere attivato come livello di protezione aggiuntivo per il controllo degli accessi alla LAN senza filo, ad esempio per usi domestici, ma non rappresenta la soluzione ideale per il controllo degli accessi a una rete aziendale o per la protezione di dati riservati.

Alcuni produttori hanno implementato soluzioni proprietarie per migliorare la protezione WEP, ad esempio 802.1x, e ritengono che questi siano sufficienti per garantire la protezione delle reti aziendali. Tuttavia il livello di protezione di queste soluzioni non standard è decisamente inferiore se confrontato con la soluzione VPN end-to-end. La combinazione tra LAN senza filo e VPN con configurazione adeguata è estremamente sicura e rappresenta una soluzione eccellente per tutti gli ambienti WLAN.

4.1 ACCESSO LAN SENZA FILO NEGLI UFFICI

L'ambiente più comune per le implementazioni delle LAN senza filo è rappresentato dagli uffici. Gli utenti possono spostarsi facilmente all'interno dell'ufficio, dalla sala riunioni alla propria postazione e negli edifici confinanti, mantenendo sempre la connessione con la rete. Nella figura 4 è illustrata una configurazione tipica di LAN senza filo protetta utilizzata negli uffici.

I punti di accesso alla LAN senza filo sono separati dalla rete aziendale con un server VPN. Tra il terminale senza filo e il server VPN viene creato un tunnel VPN che protegge le informazioni trasmesse da e verso la Intranet e impedisce gli accessi non autorizzati. L'utente può essere autenticato tramite password o password valida una sola volta, quali token hardware o certificati.

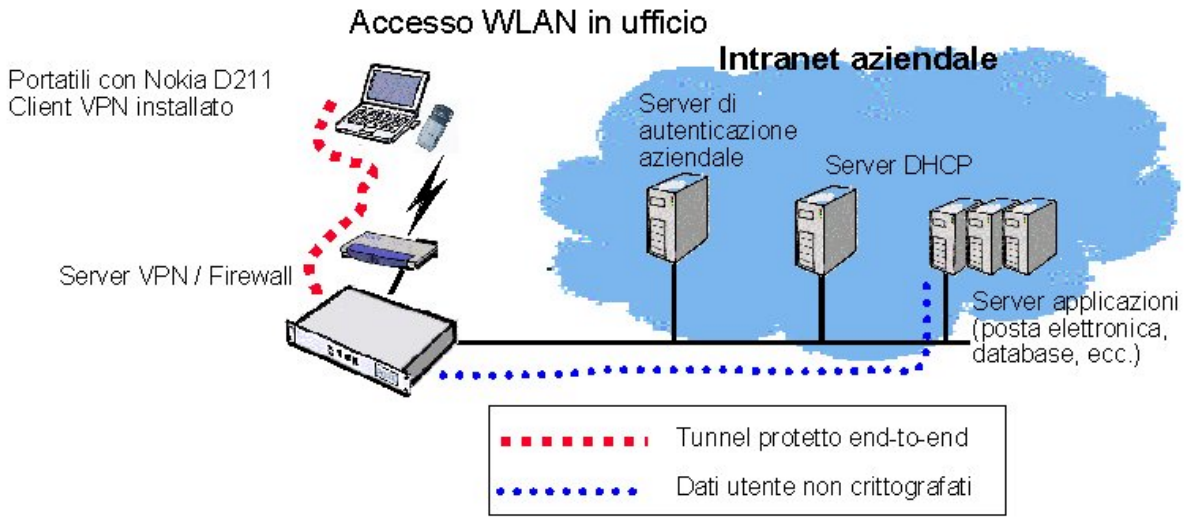


Figura 4: ufficio con LAN senza filo protetta

4.2 ACCESSO REMOTO A LAN SENZA FILO

Gli utenti mobili necessitano spesso di utilizzare i dispositivi LAN senza filo anche al di fuori dell'ufficio. Molti provider di servizi Internet (ISP) e operatori di telefonia mobile forniscono servizi di accesso a WLAN pubblici da aeroporti, hotel e altre ubicazioni pubbliche. Inoltre alcuni utenti dispongono di LAN senza filo anche presso le proprie abitazioni. Gli utenti della scheda radio Nokia D211 possono stabilire una connessione remota protetta con LAN senza filo alla rete aziendale da tutte queste ubicazioni.

L'architettura di una WLAN remota è simile a quella di una WLAN per uffici. L'unica differenza rilevante è rappresentata dal fatto che in ufficio il traffico viene instradato direttamente al server VPN tramite una rete privata. Nel caso di una zona ad accesso pubblico o di una LAN senza filo domestica, i dati dell'utente vengono instradati tramite la rete pubblica Internet. Dal punto di vista della protezione, per entrambi i casi è necessario l'utilizzo di VPN. La stessa configurazione di protezione terminale può essere utilizzata per l'accesso remoto e l'accesso da ufficio. Nella figura 5 è illustrata l'architettura di accesso remoto. L'utente della scheda radio Nokia D211 viene autenticato dalla LAN senza filo pubblica, quindi esegue il client VPN e automaticamente viene stabilito un tunnel protetto alla rete aziendale.

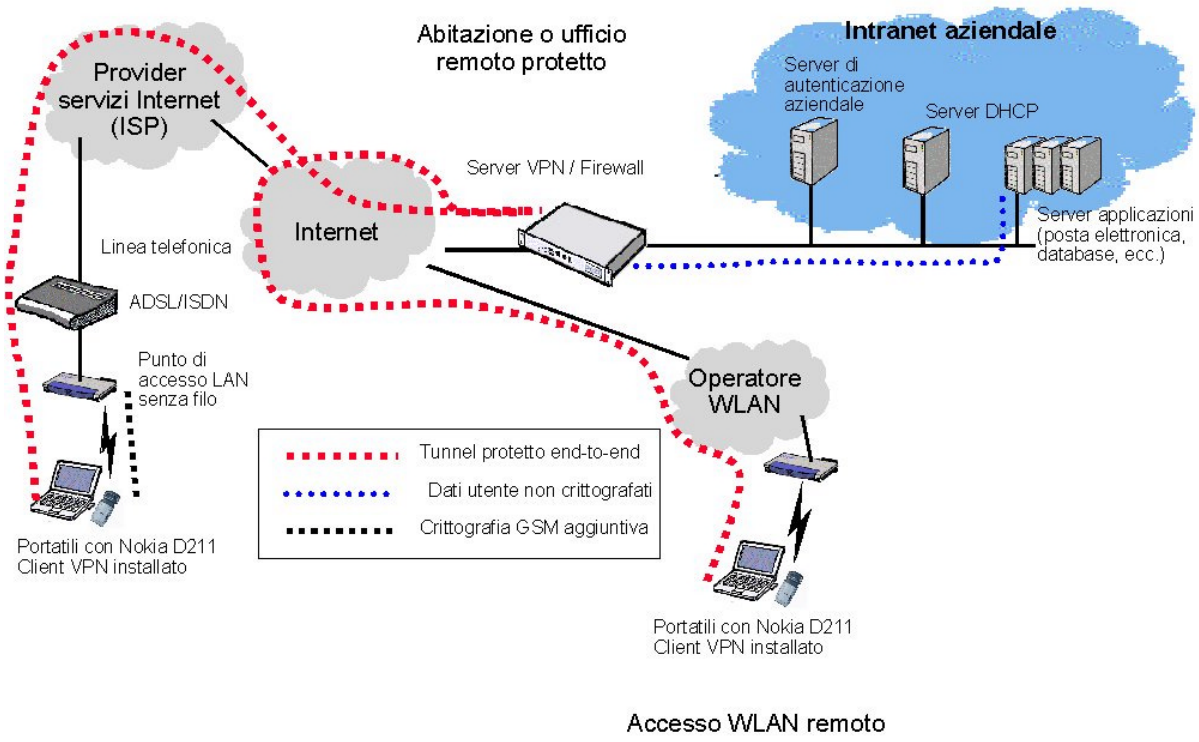


Figura 5: accesso WLAN remoto

5. RIEPILOGO – ACCESSO AZIENDALE PROTETTO CON LA SCHEDA RADIO NOKIA D211

La scheda radio Nokia D211 consente agli utenti di utilizzare la tecnologia convenzionale di accesso remoto (figura 1). Con questa configurazione, il client VPN non è necessario, la connessione viene stabilita tramite le funzioni di accesso remoto standard di Microsoft Windows.

L'architettura di accesso remoto introdotta e illustrata nella figura 6 si compone di due parti principali: il server VPN e il client VPN. Il server VPN aggiunge alla rete aziendale l'accesso Internet e offre accesso protetto alle risorse della rete aziendale da tutte le reti senza fili alternative, GPRS, HSCSD o LAN senza filo. Lo stesso server offre servizi di accesso remoto per tutti i tipi di utenti remoti: persone che lavorano dalla propria abitazione, utenti che fanno uso del roaming GPRS, utenti di LAN senza filo pubbliche e così via. In questo modo i costi di amministrazione si riducono e l'architettura di rete risulta semplificata. In genere l'amministrazione del server VPN è di competenza del reparto IT di una società.

Il software client VPN è installato sui PC degli utenti e viene eseguito assieme al software della scheda radio Nokia D211. La stessa configurazione client standard viene utilizzata con GPRS e WLAN. Il client stabilisce automaticamente un tunnel protetto al server VPN della società. Inoltre può essere fornito un firewall personale per la protezione dei PC da attacchi esterni. La società può scegliere il client VPN più adatto alle proprie esigenze, in quanto la scheda radio Nokia D211 è compatibile con tutti i principali client VPN.

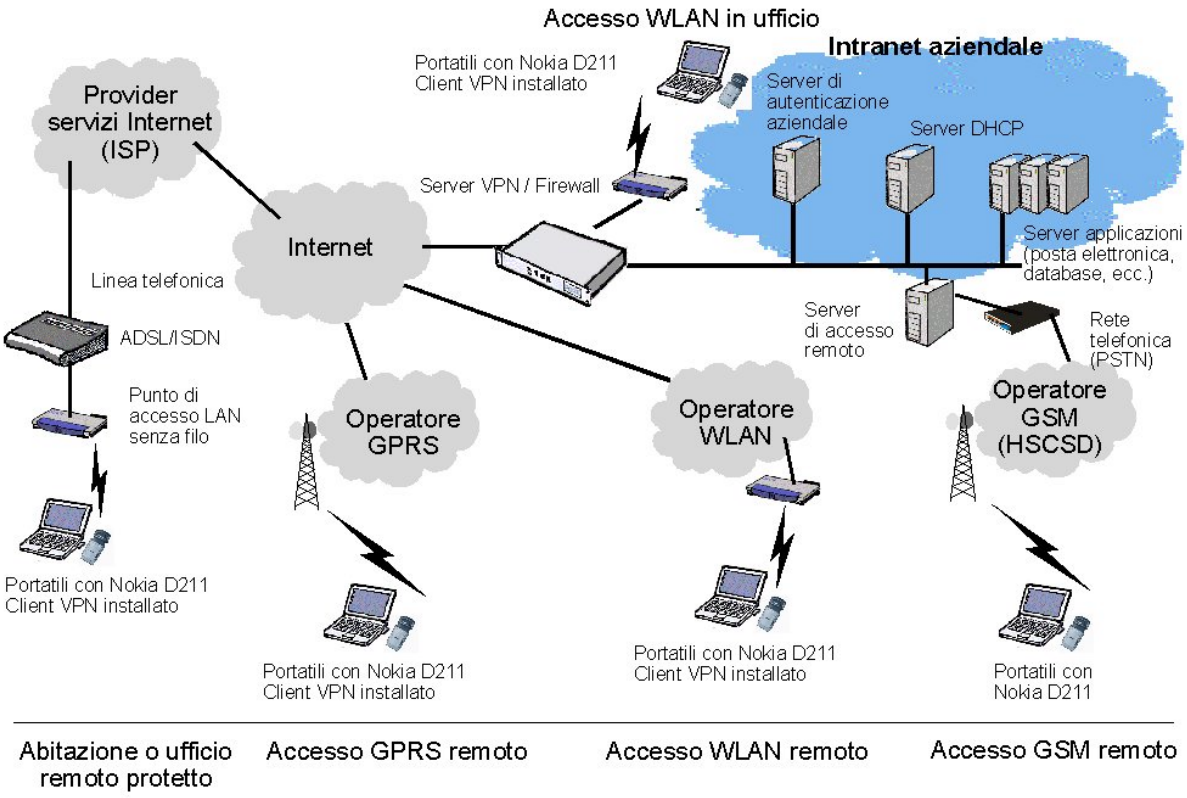


Figura 6: riepilogo dell'architettura protetta di accesso remoto

VPN rappresenta la soluzione ideale per la creazione di un'infrastruttura di comunicazione privata e protetta basata su Internet. L'utilizzo della connettività Internet, di GPRS e WLAN, quando disponibile, offre diversi vantaggi:

- Le reti GPRS e LAN senza filo consentono agli utenti di utilizzare la connessione Internet pubblica. Non è quindi necessario effettuare chiamate interurbane o intercontinentali per accedere direttamente al numero della società.
- L'addebito per le reti WLAN e GPRS è normalmente calcolato in base ai volumi trasmessi e non al tempo di connessione. L'uso della posta elettronica e la navigazione su Internet possono quindi essere molto più convenienti con questo tipo di connessione.
- Grazie a VPN, le società possono fare a meno di pool di modem, costose linee dedicate e server di accesso remoto.
- Un ulteriore risparmio è garantito dalla riduzione dei costi di funzionamento associati al supporto degli utenti remoti.

La scheda radio a modalità multipla Nokia D211 rappresenta un nuovo punto di riferimento per la connettività PC ed è in grado di offrire sia accesso remoto che connettività GRPS e WLAN. Le problematiche di protezione sono state prese in considerazione in fase di progettazione del prodotto. La scheda radio Nokia D211 è stata verificata in relazione all'interoperabilità con il software dei principali produttori di client VPN e con le soluzioni di protezione Internet (IPSEC) incorporate nelle applicazioni Microsoft. Per informazioni dettagliate sulle problematiche di protezione, visitare il sito all'indirizzo: www.nokia.com.