

Tecnologie e soluzioni per far rendere al meglio la struttura informatica della piccola e media azienda: dai trucchi per l'installazione della rete ai dispositivi di storage, dalla sicurezza aziendale all'integrazione tra i network dati, voce e videosorveglianza.

Di Simone Zanardi

L'UFFICIO NELLA RETE



Nell'ultimo numero di *PC Professionale* abbiamo presentato una guida alle tecnologie e alle soluzioni che permettono di trasformare un ambiente domestico in una casa digitale; questo mese vogliamo affrontare con un approccio analogo l'ambiente professionale, con particolare attenzione agli uffici di piccole e medie dimensioni. In questi ambiti l'infrastruttura informatica rappresenta sempre più il centro nevralgico non solo per le comunicazioni interne ed esterne, ma anche per gli stessi processi aziendali. Si pensi ad esempio alla gestione documentale, o all'organizzazione della forza lavoro che opera in mobilità, o ancora ai rapporti con clienti e fornitori. Senza considerare, per l'appunto, la convergenza delle comunicazioni che porta sempre più applicazioni (telefonia, videosorveglianza, reti di computer) a insistere su un'unica struttura di network.

NEL DVD Articoli di approfondimento su Nas e videosorveglianza

In momenti di congiuntura economica non proprio brillante come quelli che stiamo vivendo, gli investimenti in nuove tecnologie vanno affrontati con estrema cautela, soprattutto da parte delle realtà medio-piccole, che non hanno certo il budget delle grandi enterprise. È quindi importante non farsi cogliere dai facili entusiasmi derivanti da prospettive di soluzioni futuristiche senza tenere conto dei tempi e dei metodi di rientro negli investimenti, ma d'altro canto bisogna saper riconoscere quelle innovazioni che permettono di rendere il business più efficiente e, di conseguenza, di ridurre i costi.

Oggi ogni ufficio deve progettare la

propria struttura informatica partendo dal cardine della connettività a Internet, ormai indispensabile anche per le attività che non direttamente si occupano di informatica. L'accesso alla Rete serve non solo per reperire informazioni, ma anche per gestire le comunicazioni con i partner e la forza lavoro interna che si muove sul territorio, o ancora per interagire con il pubblico e i clienti finali. Per poter condividere l'accesso al Web da tutti i dispositivi e al contempo consentire ad essi di comunicare tra di loro è poi necessaria una struttura Lan (*Local Area Network*) ben progettata e organizzata, una Lan che chiaramente non può fare a meno di una sezione wireless,

se non altro per fornire connettività ai dispositivi mobili di ultima generazione come smartphone e tablet.

A partire da una struttura di base consolidata, l'amministratore del sistema informatico può puntare all'ottimizzazione, consolidando ad esempio i server (in questo senso i Nas, server di rete dedicati allo storage, ma non solo, possono rappresentare una soluzione ideale per le Pmi), verificando l'opportunità di unificare le comunicazioni audio e voce e rafforzando la sicurezza della rete.

Nelle prossime pagine indagheremo tutti questi aspetti, guidandovi passo-passo nella progettazione di un ufficio sempre più moderno ed efficiente.

Internet via satellite, un'alternativa per la connessione al Web in aree particolarmente disagiate a causa del persistente fenomeno del digital divide.



Internet, l'alternativa wireless

Quando si parla di connessioni a Internet per reti aziendali, anche di piccole dimensioni, si dà per scontato che l'accesso alla Rete esterna sia deputato a tecnologie basate sul cavo: Adsl, Hdsl o fibra ottica. In realtà anche nelle realtà business è bene tenere in considerazione i collegamenti senza fili. In primo luogo, perché essi rappresentano un'alternativa ormai disponibile a cifre più che abbordabili quando la banda larga via cavo non è disponibile: il digital divide è un problema non ancora del tutto risolto nel nostro Paese, soprattutto in zone parzialmente disagiate come le comunità montane. In questi casi un provider che sfrutta le tecnologie HyperLan/Wi-Fi o satellitare rappresenta la soluzione ideale. Anche le reti cellulari di nuova generazione possono offrire una valida alternativa al cavo, ma in questo caso il nostro consiglio è quello di valutarle soprattutto in un'ottica di canale di fail-over, ovvero come accesso a Internet che resti in stand-by e subentri in caso di guasti sulla linea di collegamento principale. Sul mercato esistono ormai numerosi router ai quali è possibile collegare una normale chiavetta Usb 3/4G.



CABLAGGIO E INFRASTRUTTURA

Per il cablaggio di una rete aziendale si ricorre tipicamente a due tecnologie: i cavi in rame e la fibra ottica. I primi hanno il pregio della versatilità e della relativa semplicità nella posa, i secondi offrono prestazioni superiori soprattutto quando le distanze salgono oltre il centinaio di metri.

Nell'ambito dei piccoli e medi uffici sono rari i casi in cui il ricorso alla fibra sia necessario, a meno che l'azienda si sviluppi all'interno di edifici particolari, ad esempio con due unità separate a discreta distanza. C'è poi da considerare il fattore prestazioni: con l'avvento sul rame della tecnologia Gigabit Ethernet prima e 10 Gigabit Ethernet, la fibra ottica non rappresenta più un grande vantaggio competitivo in questo senso.

Il wireless è invece un complemento che non ci si può più permettere di ignorare, come vedremo nelle prossime pagine. Ricordiamo sin d'ora che la posa dei cavi in rame non è sempre agevole: se siete tra i fortunati a disporre di un edificio aziendale moderno dotato ad esempio di pavimenti flottanti, far scorrere i cavi tra le varie postazioni e il centro-stella può non rappresentare un eccessivo problema, ma in caso contrario potreste scontrarvi con muri (letteralmente) invalicabili. Un esempio classico è l'installazione della rete in un edificio storico, dove può essere vietata qualsiasi opera di carattere murario. In questi casi il Wi-Fi può venire in vostro soccorso grazie all'estrema semplicità di installazione. Fatta questa presenza il nostro consiglio è comunque quello di raggiungere quante più postazioni possibili con il

cavo, la soluzione non solo più performante ma anche più affidabile.

I cavi Ethernet in sé sono di tipo *twisted pair* (a coppie incrociate); si tratta di cavi del diametro di circa 4 mm che si suddividono in categorie, indicanti la qualità costruttiva e la banda passante che sono in grado di supportare. Considerate esclusivamente cablaggi Cat5e (sino a 100 MHz) e Cat6 (250 MHz) o superiori: i primi possono gestire le connessioni Gigabit Ethernet, i secondi garantiscono ulteriore affidabilità su collegamenti a 1.000 Mbps e 10 Gbps.

Nella scelta dello switch, il dispositivo che convoglia tutte le linee di collegamento verso un punto centrale, il fattore essenziale da considerare per la Pmi è la velocità e numero delle porte, quest'ultimo chiaramente proporzionale ai punti rete da attivare nell'ufficio; in quest'ottica è bene non essere avari, dotandosi di porte libere in previsione di un'eventuale espansione della rete. Lo standard minimo di velocità deve essere il Gigabit Ethernet.

Un altro fattore di distinzione per gli switch è il livello operativo. I dispositivi di "livello 2" agiscono sui singoli collegamenti, quelli di livello 3 possono operare sul protocollo IP in modo analogo a un router.

Per la maggior parte delle applicazioni da piccolo e medio ufficio, un layer 2 è più che sufficiente: per eventuali problematiche di segmentazione di rete e gestione delle priorità di traffico può essere sufficiente il supporto per le Vlan e per gli standard 802.1p (*Class Of Service*).

CONSIGLI PRATICI: un network future-proof

➔ Non lesinate in punti rete

Al momento di progettare i punti rete del network, assicuratevi di portare una linea collegamento a ogni scrivania o postazione di lavoro, anche quelle in cui al momento non sono previste apparecchiature informatiche. Se volete essere ancor più previdenti predisponete un paio di porte per postazione. Non scordatevi di collocare qualche porta di rete anche in corrispondenza dei punti sensibili per un'eventuale struttura di videosorveglianza.

➔ La scelta dei cavi

Oltre che per categoria, i cavi *twisted pair* possono essere catalogati in base alle differenze costruttive: i cablaggi Utp (*Unshielded Twisted Pair*) sono i più diffusi e sono essenzialmente costituiti da quattro coppie di fili racchiuse in un involucro esterno in plastica. Sono adeguati alla maggior parte degli impieghi. I cavi Stp (*Shielded Twisted Pair*) e Ftp (*Foiled Twisted Pair*) utilizzano lo stesso schema ma sono muniti di una schermatura esterna in rame o altro materiale per proteggere le trasmissioni da interferenze esterne. Sono consigliabili solo nei casi in cui il cablaggio Ethernet scorra parallelamente e a stretto contatto con linee elettriche, trasformatori o apparati radio che possono disturbare le trasmissioni.

➔ Lo switch è il centro della rete

Abbiamo già detto che le connessioni a 1 Gbps sono più che adeguate per le reti di piccole dimensioni, ma se il vostro budget lo consente, optate comunque per uno switch che supporti uno o due canali 10 Gbps (eventualmente tramite moduli in fibra o su rame opzionali). Potrebbero tornare utili per fornire un canale ad altissima velocità verso il server. Se avete intenzione di spostare in futuro la struttura telefonica o di videosorveglianza su rete IP, potrebbe essere il caso di investire immediatamente su uno switch con supporto all'alimentazione PoE (alimentazione dei terminali su cavo di rete).



Uno switch con connessioni su rame a 10 Gbps: massime performance per la connessione al server.



WIRELESS

Abbilitare la rete aziendale all'accesso wireless non è più un'opzione, ma una necessità. Oltre a costituire uno strumento per sfruttare al meglio la mobilità dei notebook, le connessioni radio permettono di agganciare alla Lan quei dispositivi che non dispongono di connettività Ethernet (smartphone e tablet) e sono perfette per gestire gli accessi ospite in caso di visite di personale esterno.

Rispetto alle reti domestiche, spesso un singolo access point può non essere sufficiente, non solo per problemi di copertura, ma anche per la gestione di un numero elevato di

terminali. In molti casi, dunque, la soluzione ideale per un piccolo o medio ufficio è un sistema di gestione centralizzato, in cui i singoli punti di accesso svolgano il ruolo di semplici interfacce radio demandando il management a un dispositivo centrale. I vantaggi di una gestione centralizzata sono innumerevoli: in primo luogo, la sicurezza della struttura wireless

risponde a dei criteri unificati, per cui all'aggiunta di un nuovo punto di accesso questo eredita automaticamente i parametri di protezione già impostati. Dal punto di vista della mobilità, poi, la gestione centralizzata consente di attivare meccanismi di roaming in modo che un terminale possa passare dalla zona di copertura di un access point ad un'altra in modo trasparente e senza la necessità di ri-autenticarsi sulla rete.

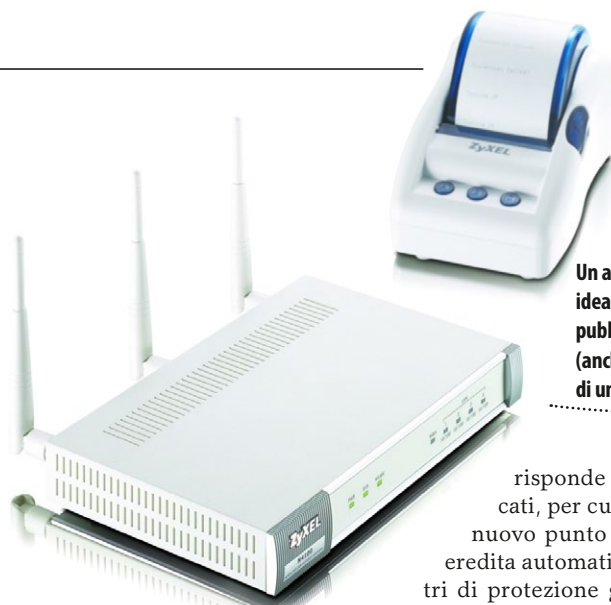
Se per il vostro ufficio un sistema centralizzato con punti di accesso multipli è sovradimensionato, potete ricorrere a un singolo access point professionale; pur non offrendo i servizi peculiari dei sistemi fin qui esaminati, questi dispositivi dispongono di altre funzioni sconosciute ai modelli consumer.

Dal punto di vista della sicurezza, in installazioni wireless professionali difficilmente ci si può accontentare di una protezione a password condivisa. Il sistema di accessi deve essere invece organizzato in account personali. La tecnologia Wi-Fi prevede in questi casi l'interazione con un server di autenticazione già presente in rete a cui interfacciarsi tramite il protocollo 802.1x. In assenza di questo servizio, molti access point integrano un database interno di utenti locali.

Un esempio di antenna Wi-Fi direzionale, utile alla creazione di un ponte radio per collegare due segmenti di rete cablata.



Un access point con stampante, ideale per creare un hot spot pubblico e fornire accessi (anche a pagamento) ai clienti di un'attività commerciale.



I nuovi terminali in ufficio

Tablet e smartphone non possono più essere ignorati nella progettazione di una struttura informatica efficiente per l'azienda. Oltre a fornire agli utenti di apparati mobili un'adeguata modalità di accesso tramite connessione wireless, è necessario impostare delle policy aziendali che permettano di far interagire questi apparati con il resto del network.

Nella maggior parte dei casi la soluzione più efficace

per consentire questa interazione è l'utilizzo delle piattaforme di sincronizzazione basate sul cloud: lo scambio dei dati diretto con smartphone e tablet non è infatti sempre agevole, soprattutto se si parla di dispositivi Apple, ma con qualche semplice accorgimento la rete aziendale può essere configurata per rendere semplice la vita anche agli utenti mobili. Un classico esempio in questo senso è l'impiego di un servizio di cloud storage come Dropbox (in versione professionale per team) o Amazon S3. Impostando sulla Lan una zona di condivisione dei file questi divengono immediatamente accessibili da smartphone e tablet, anche da remoto.

Sul fronte della posta elettronica la filosofia cardine da adottare prevede che un singolo utente possa accedere alla propria casella da più di un dispositivo, trovando le missive sempre sincronizzate. Esistono numerose soluzioni per raggiungere questo scopo, la più pratica in questo ambito certo quella di ricorrere a un servizio di posta che supporti lo standard Imap per gestire centralmente la posta sul server.

Per quanto concerne infine le applicazioni business disponibili per tablet e smartphone, una disamina estesa esula dagli scopi di questo articolo, ma ci è sufficiente ricordare la presenza di numerose suite per la gestione di documenti office (file di testo, fogli di calcolo, presentazioni PowerPoint e Pdf), per il controllo dei computer e per l'accesso alla rete aziendale tramite Vpn. Su ogni numero di PC Professionale potete trovare una rassegna delle più interessanti app per smartphone e tablet, anche dedicate alla produttività in azienda.



CONSIGLI PRATICI: wireless sicuro

Queste soluzioni sono ideali anche per la gestione degli accessi occasionali: se ad esempio si vuole fornire accesso a un utente ospite è sufficiente creare un account temporaneo che può essere quindi disattivato al termine della sessione. Al contrario, un sistema a chiave precondivisa (Psk, PreShared Key) costringe in tali casi a disabilitare la protezione di rete o a cambiare la chiave al termine della sessione con utenti ospiti.

Altra caratteristica diffusa negli access point professionali è la possibilità di definire Ssid virtuali multipli: in questo modo a partire da una sola stazione base si creano di fatto due o più reti wireless, ciascuna dotata di proprie caratteristiche di sicurezza e policy di accesso.

Un caso particolare di accesso wireless è quello necessario per collegare due edifici non adiacenti, ad esempio il magazzino con gli uffici. In queste situazioni la tecnologia consente di installare un ponte radio, in modo da unire due tratte di rete cablate. Molto spesso è consigliabile il ricorso ad antenne direzionali: gli access point "tradizionali" sono infatti generalmente forniti con antenne omnidirezionali, che coprono in modo uniforme tutta l'area circostante. Per un ponte radio è più efficace un'antenna direttiva, che indirizzi, la potenza di trasmissione verso un determinato punto, aumentando la portata in quella direzione. Esistono varie antenne direttive che possono essere installate sugli access point professionali, ciascuna adatta a specifiche esigenze di collegamento.

In ambito aziendale spesso la soluzione più efficace per l'accesso Wi-Fi è l'impiego di più access point gestiti centralmente.



→ Utilizzate autenticazione 802.1x e non Psk

L'autenticazione degli utenti tramite password precondivisa (Psk, *Pre Shared Key*) è più che adeguata ai contesti residenziali e alle realtà di piccolissime dimensioni, ma mostra tutti i suoi limiti in ambito business. Il problema principale risiede nella necessità di dover assegnare una chiave di accesso comune a tutti gli utenti della Wlan. Se dovete fornire accesso temporaneo (ad esempio a un ospite) siete costretti a comunicare la Psk che al termine della sessione diviene quindi insicura e obsoleta. Un sistema di autenticazione 802.1x si basa invece su account di utenti e gruppi di lavoro, proprio come avviene tradizionalmente nei sistemi informatici di condivisione delle risorse: un account è quindi dotato di proprio userid e password, che potete attivare anche per brevi intervalli di tempo ed eliminare senza alcuna ripercussione sugli altri utenti. La protezione 802.1x richiede in linea di principio un server di autenticazione esterno già presente sulla rete, ma le piattaforme wireless professionali offrono in alternativa un database interno riservato all'autenticazione dei client radio.

→ Definite più reti wireless virtuali

Molte piattaforme di accesso professionali consentono di definire reti senza fili virtuali multiple: pur appoggiandosi sulla stessa struttura fisica, ogni wireless Lan virtuale è caratterizzata da un proprio identificativo Ssid e può essere configurata con specifiche regole di sicurezza. Potete ad esempio creare una prima rete wireless riservata ai dipendenti e dalla quale è possibile accedere a tutto il network, e una seconda Wlan virtuale per gli ospiti con "vista su Internet" ma non al server di produzione riservato.

→ Vpn: protezione al massimo

In caso di applicazioni particolarmente riservate che non possono essere confinate alla sola sezione cablata del network, potete ricorrere ai tunnel Vpn (*Virtual Private Network*) anche come sistema di protezione delle connessioni radio. Questo sistema costituisce di fatto una doppia barriera di sicurezza: un primo livello agisce sul collegamento fisico, il secondo interviene sui layer di rete e superiori per un'ulteriore fase di autenticazione e cifratura dei dati. Alcune piattaforme wireless presenti sul mercato offrono profili Vpn specifici per la cifratura delle trasmissioni senza fili. Nelle prossime pagine potete trovare ulteriori dettagli sulle Vpn.



NAS E BACKUP

I Nas (*Network Attached Storage*) sono server ideali per la piccola azienda. Offrono la maggior parte dei servizi indispensabili per la gestione di un rete locale, inclusi i processi di backup dei dispositivi, permettono di accedere a risorse condivise sia sulla Lan che da remoto, se opportunamente dimensionati presentano un'ottima affidabilità in termini di resistenza ai guasti. Sfruttando protocolli di comunicazione standard non sono soggetti a problemi di compatibilità con i sistemi operativi dei terminali e sono disponibili in un ampio range di caratteristiche e prezzi.

Anche se il vostro ufficio dispone già di uno o più server per applicazioni aziendali, email o servizi Ftp, un Nas può insomma rappresentare uno degli investimenti più sicuri per espandere in tutta sicurezza la capacità di immagazzinamento dati della struttura informatica senza dover intervenire sui server di produzione. I Nas montano tipicamente due o più dischi e possono essere configurati in modalità Raid (*Redundant Array of Independent Disks*) differenti per ottimizzare affidabilità o prestazioni. Un sistema Raid di livello

0 effettua lo *striping* sulle unità, suddividendo i dati sui vari dischi e offrendo il massimo delle prestazioni a scapito dell'affidabilità (in caso di guasto su di un disco tutti i dati vengono perduti). Al contrario, il *mirroring* (o Raid 1), massimizza l'affidabilità introducendo uno o più volumi che replicano il contenuto dell'unità in uso, pronti a subentrarvi in caso di guasti; la robustezza si ottiene in questo caso a scapito dello spazio su disco effettivamente utilizzabile che risulta dimezzato.

Se si dispone di almeno 3 dischi, il miglior compromesso è sicuramente rappresentato da un'architettura Raid 5: si tratta di un sistema che distribuisce i dati sulle diverse unità conservando la ridondanza necessaria a ricostruire i dati in caso di guasti; nel caso ad esempio di 3 dischi da 2 TByte l'uno, lo spazio utile a disposizione è pari a 4 TB, ma nell'eventualità di danneggiamento di un disco il sistema è in grado di ricostruire tutti i dati del file system. I sistemi Raid più evoluti permettono inoltre di sostituire a caldo eventuali dischi guasti, senza alcuna interruzione di servizio. I Nas aziendali integrano al loro interno completi meccanismi

di gestione dei permessi e delle quote, ma possono appoggiarsi a una struttura di autenticazione preesistente; sono inoltre dotati di un server Ftp integrato per un accesso remoto delle risorse.

Sul fronte backup, i Nas offrono numerose modalità di copia sicura dei dati. In primo luogo, possono fungere da destinazione per i processi di copia lanciati dai software appositi installati sui terminali aziendali. Molti Nas sono forniti con software di backup per personal computer, a volte sviluppati dalla stessa azienda che produce il server, in altri casi di terze parti. Verificate sempre il numero di licenze fornite con il prodotto. Nel caso dei sistemi Apple, molti Nas supportano il servizio *Time Machine* per la copia di sicurezza dei sistemi Mac.

Oltre a gestire il backup da Pc, i Nas possono a loro volta effettuare copie di sicurezza dei dati immagazzinati su altri server di storage presenti in rete (attraverso il protocollo standard Rsync o tramite soluzioni proprietarie) o direttamente su dischi e memorie collegate direttamente al Nas tramite porte Usb o eSata.

I Nas offrono un numero sempre maggiore di funzioni e servizi, tanto da essere ormai paragonabili a server completi.



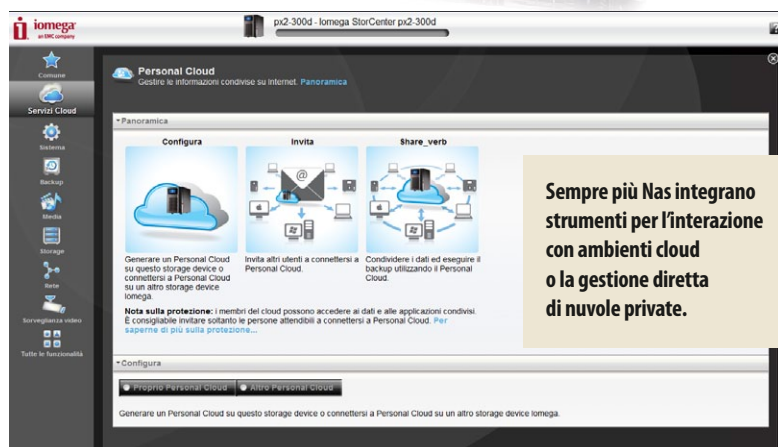
Gruppi di continuità

Sebbene non strettamente legato al networking, l'impianto elettrico costituisce le fondamenta su cui si posa l'intera struttura informatica di un ufficio. Spesso preoccupandosi di fornire un'adeguata protezione alla rete attraverso firewall e antivirus ci si dimentica una delle principali cause di interruzione di servizio che può colpire una struttura It: il blackout. I disturbi all'alimentazione elettrica (blackout, ma anche variazioni improvvise di tensione e distorsioni in frequenza) rischiano non solo di bloccare il vostro lavoro, ma possono anche danneggiare in modo irreparabile dispositivi del valore di diverse migliaia di euro, oltre a comportare la perdita di dati sensibili. I gruppi di continuità, o Ups (*Uninterruptible Power Supply*) mettono al riparo i dispositivi da questi disturbi, fornendo un'autonomia variabile che permette in caso di blackout di continuare a lavorare o perlomeno di arrestare correttamente le unità operative. Per mettere al riparo la vostra struttura da problemi di natura elettrica, vi consigliamo dunque vivamente di ricorrere a un gruppo di continuità, perlomeno per i sistemi vitali alla produzione come i server principali.

Un gruppo di continuità può salvare l'integrità dei vostri dati.



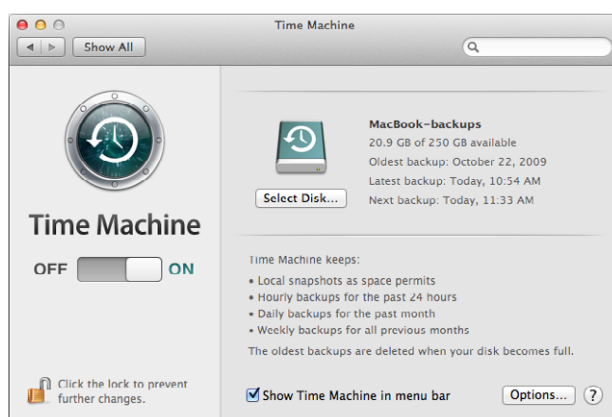
In ambito business esistono Nas per tutte le esigenze e le tasche, a partire dai modelli desktop con due dischi sino ad arrivare alle unità rack.



Sempre più Nas supportano poi la sincronizzazione dello storage con servizi *cloud-based*, utili non solo ad effettuare una copia dei dati su postazioni remote al riparo da guasti catastrofici che possono bloccare la struttura locale, ma anche per semplificare l'accesso alle risorse, anche da parte di dispositivi mobili come smartphone e tablet. Da citare infine i numerosi servizi avanzati, a partire dalla possibilità di gestire un piccolo sito Web, ad esempio a uso interno dell'azienda, passando

per l'utilizzo come piattaforma di registrazione video in accoppiata con un sistema di sorveglianza basato su IP, sino ad arrivare ai moduli evoluti per il controllo diretto della posta e l'analisi antivirus dei file salvati. Per una disamina dettagliata di alcune soluzioni Nas presenti sul mercato e adatte per l'utilizzo in ambito Pmi vi rimandiamo alla rassegna apparsa sul numero 254 di *PC Professionale* e riproposto in formato digitale sul Dvd allegato a questo numero della rivista.

Time Machine, il servizio Apple per il backup dei sistemi Mac, supportato dalla maggior parte dei Nas in commercio.



CONSIGLI PRATICI: scegliere il Nas

→ Il numero di slot è importante

Esistono Nas per ogni esigenza, ma uno dei parametri più importanti nella scelta di un server di storage resta il numero di dischi supportati. Per un'utenza business la configurazione minima da noi consigliata è quella a quattro dischi, che consente di configurare architetture Raid dotate di ridondanza senza eccessivo spreco di capacità. Un esempio classico è il Raid 5 che con quattro dischi di dimensioni fisse utilizza la capacità di tre moduli ma regge il guasto di una singola unità senza perdita di dati. Con un Raid 5 di tre dischi più *hot spare*, la capacità è quella di due unità, ma il sistema può gestire il guasto di due moduli.

→ Verificate i servizi software

Sebbene tutti i Nas di ultima generazione supportino la maggior parte dei servizi di base indispensabili per le aziende di piccole e medie dimensioni, è sempre bene verificare con attenzione che il sistema gestisca le funzioni su cui la vostra struttura di rete si fonda. Se ad esempio volete utilizzare il Nas anche come espansione *diretta* dello storage di un server pre-esistente, verificate le funzionalità iScsi, mentre per un'interazione con il cloud controllate quali sono i servizi online supportati. In caso di integrazione con altri Nas, i protocolli di sincronizzazione come Rsync divengono indispensabili.

→ Non dimenticate la ridondanza

Nella maggior parte dei casi il Nas è destinato a conservare alcuni dei file più sensibili della vostra struttura informatica. In questi casi, è importante alzare al massimo l'affidabilità di questo apparato, non solo proteggendosi dai guasti sui dischi tramite opportune architetture Raid ridondanti, ma optando per modelli con doppio alimentatore e sistema operativo replicato su due moduli di memoria, in modo da poter sopravvivere a ogni genere di guasto.

→ Non scordate i "pezzi di ricambio"

In caso di guasto a un disco un Nas opportunamente configurato può continuare a operare senza interruzione di servizio. In queste situazioni è però opportuno essere pronti a sostituire immediatamente l'unità guasta, in modo da non rischiare un secondo fail che potrebbe risultare catastrofico. È buona norma quindi acquistare in anticipo e conservare un hard disk extra compatibile con il Nas pronto per la sostituzione.

LA TELEFONIA SU IP

L'argomento IP telephony riferito alla piccola e media azienda è sempre spinoso: se le grandi realtà enterprise sono abituate a investimenti anche massicci sulle infrastrutture in un'ottica di maggiore efficienza e rientro degli investimenti, le piccole realtà faticano spesso a percepire come reali i vantaggi che derivano da un cambiamento radicale effettuato su un servizio ormai dato per scontato come quello telefonico. In realtà esiste uno spazio di competitività per la telefonia su IP anche nella piccola e media azienda, soprattutto se questa si trova nella situazione di dover comunque mettere mano alla propria struttura di comunicazione.

Al centro di un impianto di IP telephony c'è sempre un centralino, o Pbx; questo è tipicamente rappresentato da un computer con a bordo un software opportuno, o da un'applicazione preconfigurata per fungere da gestore della rete. I telefoni sono analoghi a quelli tradizionali,

Un terminale dual-mode: telefono IP e tradizionale in un'unica soluzione.



Centralino e terminali VoIP permettono di trasformare la struttura telefonica aziendale integrandola con quella It.



ma si collegano alla rete tramite normali cavi Ethernet o in modalità Wi-Fi. Possono essere sostituiti da altri terminali con opportuno software a bordo (personal computer, tablet o smartphone). È anche possibile riutilizzare i vecchi terminali analogici tramite adattatori. Molti IP Pbx possono interagire con i centralini tradizionali affiancandoli per un passaggio graduale dell'azienda al VoIP, oltre a sfruttare le linee tradizionali in uscita.

I vantaggi che un impianto telefonico basato su IP può apportare a un'azienda, anche di piccole dimensioni, risiedono innanzitutto nell'abbattimento dei costi per le chiamate effettuate da sedi remote o telelavoratori e nella

drastica riduzione di quelli legati alle comunicazioni a lunga distanza: nel primo caso, infatti, il traffico voce viaggia sull'infrastruttura Internet e quindi, salvi i costi di connettività alla Rete, risulta gratuito. Per quanto concerne le chiamate internazionali verso numeri telefonici tradizionali, il trasporto su IP può essere sfruttato per gran parte della tratta e convogliato su reti tradizionali solo nell'ultimo segmento.

La riduzione dei costi di chiamata non è comunque l'unico vantaggio competitivo dell'IP telephony nei confronti dei sistemi tradizionali: basandosi sul protocollo IP le comunicazioni telefoniche possono sfruttare la rete informatica, dimezzando di fatto i costi di gestione e manutenzione della struttura. Se dovete predisporre una nuova postazione di lavoro potete così stendere un solo cavo per collegare entrambi gli impianti, così come possono essere unificati i sistemi di protezione

Anche il fax passa dall'IP

Uno dei motivi per cui molte aziende restano legate alla telefonia analogica è il fax, strumento oggi francamente obsoleto ma spesso ancora utilizzato nei rapporti con fornitori e clienti. Quando un'azienda approccia le soluzioni VoIP, nella maggior parte dei casi essa è già pronta a sostituire al proprio interno lo strumento Fax con documenti digitali o digitalizzati da inviare via e-mail. Il problema si pone quando si ha che fare con terze parti non così evolute. Fortunatamente, esistono oggi numerosi servizi online che permettono di creare un numero di fax virtuale interamente gestito su reti IP e, più specificamente, tramite e-mail. In ingresso, chiunque voglia inviare un fax all'azienda non deve cambiare in nessun modo il procedimento: utilizzando una qualsiasi macchina fax, indirizza i documenti al numero telefonico virtuale come se si trattasse di un normale contatto. Il servizio online riceve la trasmissione, converte automaticamente i documenti in formato elettronico e li invia a una casella di posta elettronica assegnata all'utente. Questo riceve quindi i file in email e può decidere se stamparli come avrebbe fatto una normale macchina fax o se conservarli direttamente in formato elettronico.

Grazie ai servizi di fax online, è possibile inviare e ricevere facsimili utilizzando una casella email.

The screenshot shows the MESSAGENET website interface. At the top, there's a navigation bar with 'Voip', 'Fax', 'Sms', and 'Mobile' tabs. Below this, a banner reads 'Oggi. Ricevi e invia fax con email e web.' and lists benefits: 'Economico ed ecologico', 'Facile e veloce come l'email', 'Affidabile e sicuro', and 'Mantieni il tuo numero'. There are three main service boxes: 'faxin' (receiving faxes via email), 'faxout' (sending faxes via email or Microsoft Office), and 'freefax' (receiving faxes via email). Each box has an 'Attiva' button.



Esistono numerosi client VoIP per smartphone e tablet, su tutte le principali piattaforme mobili.

(firewall, gruppi di continuità). Bisogna poi considerare la totale indipendenza del numero telefonico (e quindi della postazione di lavoro) dalla locazione fisica: essendo il terminale di IP telephony un apparato di rete, esso può essere spostato in modo trasparente sulla struttura.

Un dipendente può ad esempio accedere al proprio profilo da casa utilizzando un personal computer ma anche un tablet o uno smartphone dotato di apposito client e conservando tutte le impostazioni e le informazioni che ritroverebbe sulla scrivania. Per raggiungerlo è sufficiente comporre il numero che lo identifica in azienda, sia che si tratti di una chiamata interna sia che questa provenga da fuori. Allo stesso modo, il telelavoratore può effettuare chiamate come se fosse in ufficio, con eventuali costi addebitati direttamente all'azienda.

La portabilità si estende anche ai numeri geografici: un'azienda può ad esempio acquistare un'estensione con prefisso teletestivo di Roma ma ricevere le chiamate presso la sede di Milano, senza alcun addebito aggiuntivo a carico del chiamante.



La tecnologia VoIP si presta anche all'utilizzo in ambito di conferenze a partecipanti multipli.



CONSIGLI PRATICI: VoIP al massimo

→ Acquistate estensioni geografiche

Un centralino IP per il piccolo e medio ufficio permette di ricevere ed effettuare chiamate sia verso altri sistemi IP telephony sia verso numeri telefonici tradizionali (fissi o cellulari). Per questi ultimi il Pbx si può appoggiare a delle linee telefoniche classiche presenti in ufficio o a servizi Itsp (*Internet Telephony Service Provider*). Un Itsp fornisce al cliente un account di accesso al proprio proxy Sip; attraverso il proxy Internet si interfaccia con la Pstn (la rete telefonica classica) permettendo di raggiungere tutte le utenze tradizionali. Un'ulteriore servizio offerto dagli Itsp è la fornitura di uno o più numeri telefonici geografici: senza un numero di questo tipo il servizio IP può contattare la rete tradizionale ma non essere raggiunto da essa. Una volta acquistati, i numeri forniti dall'Itsp possono essere sfruttati dal Pbx per interfacciare le estensioni locali, impostando opportuni meccanismi di inoltro delle linee in ingresso e uscita.

→ Impostate un piano Lcr

I sistemi di *Least Cost Routing* (Lcr) implementati nella maggior parte dei Pbx IP anche di fascia bassa, permettono di indicare quale account o provider Itsp utilizzare per le chiamate in uscita in base al numero chiamato. In questo modo è possibile ridurre i costi delle telefonate ad esempio sfruttando il VoIP per le chiamate a lunga distanza (tipicamente quelle che consentono un risparmio maggiore) e la linea tradizionale per quelle nazionali. L'Lcr consente inoltre di indirizzare direttamente sulle linee classiche quelle numerazioni che non sono gestibili dalla telefonia su IP (numeri di emergenza e contatti non geografici come ad esempio 144/166, 84X, 199, 709, 899).

→ La segreteria telefonica in email

Uno degli esempi più diffusi di interazione tra sistema telefonico IP e struttura informatica è la voice mail, ovvero la casella di segreteria telefonica abbinata a un numero IP che viene gestita dall'apparato di posta elettronica: i messaggi lasciati dal chiamante sono così inoltrati automaticamente all'indirizzo email dell'utente, come allegati in formato audio.

→ Sfruttate le funzioni lvr

I Pbx più evoluti dispongono di sistemi lvr (*Interactive Voice Response*) per la creazione di risponditori automatici interattivi; il chiamante può così essere guidato attraverso una serie di menu vocali con cui interagisce tramite la pressione dei tasti del suo apparecchio. L'impiego più elementare è un risponditore automatico da attivare negli orari di chiusura, ma un lvr può essere utilizzato anche per deviare le chiamate verso il reparto o l'estensione interna più appropriata. In alcuni casi il risponditore consente di registrare messaggi che possono poi essere rediretti automaticamente a una casella di voicemail specifica.

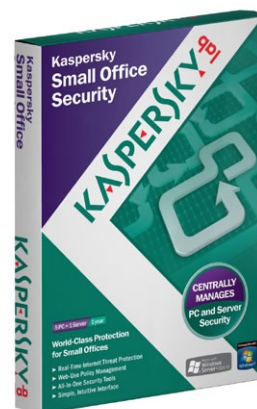
→ Ottimizzate la qualità di servizio

Una delle critiche più diffuse ai sistemi di IP telephony riguarda la qualità delle chiamate. Gran parte dell'effettiva resa audio del VoIP è da imputare al tipo di connessione a Internet di cui dispone l'impianto: al momento di sottoscrivere un contratto di accesso verificate non solo la velocità massima in downstream (ovvero per i trasferimenti dati da Internet verso la vostra rete), ma anche quella in upstream (altrettanto importante in ambito telefonico) e la velocità minima garantita sulla vostra linea di accesso. A livello di apparati, potete invece agire sulle policy di accesso a Internet del router e sulla Lan vera e propria. Sul router definite delle regole di priorità per l'accesso alla banda verso la rete esterna.

LA SICUREZZA IN RETE



Le appliance Utm forniscono protezione unificata dagli attacchi provenienti da Internet.



Un pacchetto software comprensivo di antivirus protegge l'azienda da minacce provenienti dall'interno.

In queste pagine abbiamo ripetuto più volte come non abbia più senso ipotizzare una rete informatica che non sia strettamente interconnessa con Internet. Questa apertura verso la Rete globale espone chiaramente la struttura aziendale a una serie estesa di minacce provenienti dal Web ed è quindi indispensabile includere la sicurezza tra i punti chiave da tenere in considerazione al momento della progettazione. In realtà, l'approccio alla sicurezza in un ambiente informatico delicato come quello aziendale va ben al di là dell'acquisto di un singolo dispositivo: si tratta di ideare e realizzare un piano

di protezione completo e organico, che parta dal training degli impiegati e passi per la definizione di policy di comportamento e di accesso alle risorse.

L'approccio organico deve riguardare anche i dispositivi e le soluzioni tecnologiche: concentrarsi unicamente sulla protezione dagli attacchi esterni (firewall) o sulla salvaguardia dei singoli Pc (antivirus personali) è estremamente limitativo e inefficace, così come lo è pensare che le minacce possano provenire solo dall'esterno senza considerare le potenziali debolezze costituite dagli utenti stessi della Lan.

Il mercato dei dispositivi si sta muovendo in tal senso, come dimostrano le appliance Utm (*Unified Threat Management*, protezione unificata dalle minacce) proposte oggi non solo dalle aziende che producono storicamente apparati di rete, ma anche dai principali produttori di antivirus; si tratta di dispositivi hardware che proteggono la struttura interna a tutti i livelli, verificando il traffico in entrata e uscita e assicurandosi al contempo che i personal computer siano aggiornati per affrontare le ultime minacce.

In questi dispositivi sono inclusi gli elementi essenziali per una protezione



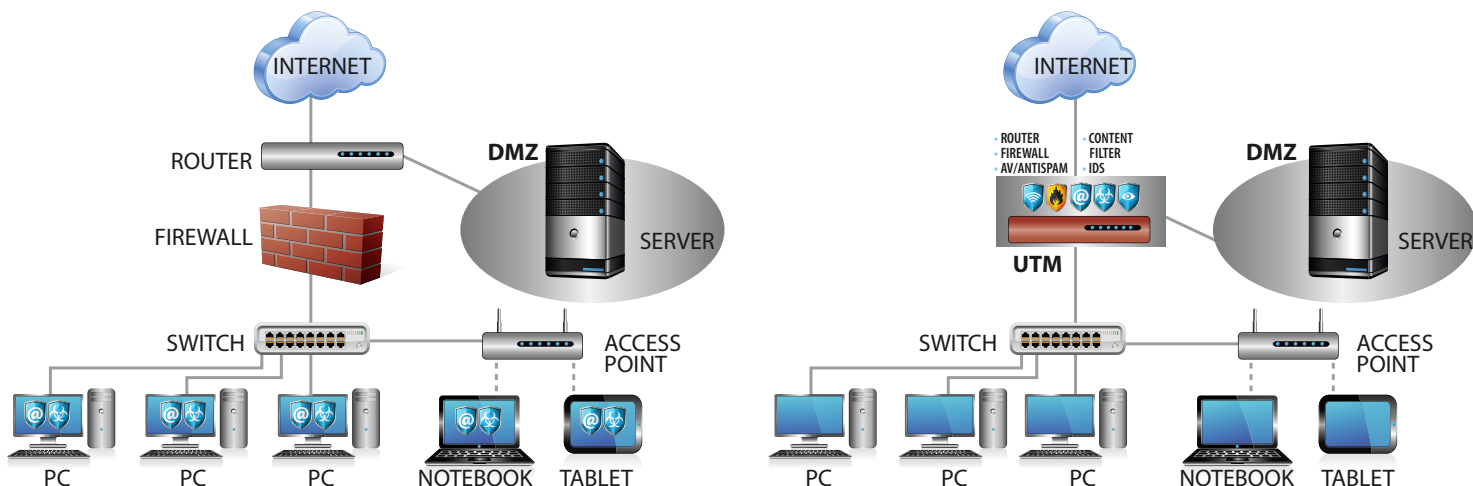
Sicurezza informatica e fisica

Il sistema di sorveglianza dell'ufficio può essere integrato con la struttura IP grazie alle videocamere di ultima generazione nate all'insegna della convergenza. Proprio come nel caso dell'IP telephony, la videosorveglianza su IP presenta un buon numero di vantaggi rispetto a quella tradizionale, in primo luogo la convergenza della struttura di cablaggio già citata nelle applicazioni telefoniche che permette di ridurre considerevolmente i costi di installazione e manutenzione della struttura aziendale. Gli impianti di sorveglianza di fascia alta consentono di gestire un parco telecamere esteso attraverso un server centrale che si occupa di tutte le funzioni di coordinamento tra i terminali e dei servizi di allarme e di registrazione. Anche dotandovi di una singola videocamera professionale potete comunque essere certi di disporre di un sistema di sorveglianza autonomo, dal momento che questi dispositivi integrano tutte le funzioni indispensabili per la gestione delle policy di sicurezza, con meccanismi di *motion detection* per il rilevamento del movimento nell'area inquadrata, possibilità di definire un calendario orario in cui lo stato di allerta deve essere mantenuto attivo, connettori I/O per interfacciarsi direttamente con allarmi e sensori e servizi per l'invio di immagini e notifiche via email o Ftp. Tra i parametri di scelta di una videocamera di sorveglianza su IP, ricordiamo le opzioni di collegamento al network (i modelli dotati di semplice interfaccia Ethernet richiedono la stesura di un cavo fino al punto di installazione mentre dispositivi predisposti per le connessioni WiFi possono comunicare con la Lan in modalità wireless), il supporto allo standard Power Over Ethernet per l'alimentazione diretta da cavo Utp e le già citate funzioni di motion detection e invio delle immagini a un server di appoggio. Dal punto di vista ottico, invece, considerate l'angolo



I sistemi di videosorveglianza moderna stanno gradualmente convergendo su reti IP e sono gestiti tramite personal computer.

di campo (che determina l'ampiezza dell'area inquadrata) e la sensibilità della videocamera: per la videosorveglianza notturna sono indispensabili gruppi ottici in grado di operare in condizioni di scarsa illuminazione (una candela produce circa 1 Lux) o, meglio ancora, modelli night&day che possono operare anche in assenza di luce visibili, sfruttando la gamma infrarossa emessa da illuminatori integrati o unità esterne. Se desiderate infine un dispositivo di sorveglianza a 360 gradi, potete ricorrere ai modelli con PtZ (*Pan Tilt e Zoom*) motorizzato: la rotazione su due assi consente inquadrature ad ampio spettro e può essere comandata anche da remoto. Nel Dvd allegato alla rivista potete trovare una rassegna di soluzioni di sorveglianza IP per l'ufficio.



Rispetto all'approccio tradizionale (sx), un Utm integra in un solo apparato numerose funzioni di protezione.

completa del sistema informatico connesso a Internet: il firewall si occupa di analizzare e filtrare i pacchetti di rete in transito, in modo da bloccare a livello IP trasmissioni dannose o indesiderate in ingresso e uscita; il modulo *Intrusion Detection System* va oltre al livello IP, sfruttando un database aggiornato che contiene un elenco degli attacchi informatici e il relativo schema comportamentale, in modo da riconoscere e bloccare le minacce appena queste si manifestino.

L'antivirus centralizzato analizza il traffico email, Ftp e Web prima che questo possa pervenire ai computer, in modo da neutralizzare sul nascere i contenuti maligni; spesso è abbinato a un motore antispam che identifica le missive fraudolente o indesiderate evitando di intasare i client di posta dei Pc. Ultima, ma non meno importante, è la verifica dello stato dei client: i sistemi più evoluti dispongono di agenti installabili sui singoli personal computer e che si occupano di controllare periodicamente lo stato di aggiornamento di sistema operativo e software di sicurezza; quando un upgrade è disponibile, l'agente si occupa di revisionare i sistemi. Per mantenere inalterata l'efficacia di questi moduli è indispensabile che le appliance siano costantemente aggiornate per disporre delle ultime definizioni di virus, attacchi e frodi; i sistemi sono perciò sempre collegati a un servizio di update del produttore gestito da opportune taskforce con il preciso compito di individuare nuove minacce e metterne a conoscenza il dispositivo in tempo reale.

CONSIGLI PRATICI Vpn client-to-site

La procedura di configurazione di un nuovo tunnel Vpn può essere suddivisa in due fasi:

- **Definizione di una policy IKE (Internet Key Exchange) contenente gli estremi identificativi delle due parti che saranno coinvolte nella comunicazione**
- **Definizione della Security Association che sfrutterà la policy appena creata per generare il tunnel vero e proprio**

FASE 1 Configurare il server Vpn

La configurazione ha sempre inizio sul router Vpn: identificate la sezione relativa alle Vpn e aggiungete un nuovo profilo di connessione, chiamandolo ad esempio *PCprova*. Dovrete innanzitutto indicare i recapiti: nel caso del router è indispensabile essere muniti di un indirizzo fisso che potrà essere contattato dal client remoto. Se il vostro contratto di accesso a Internet fornisce un indirizzo IP pubblico e fisso, potete servirvi di quest'ultimo; in alternativa, ricorrete a un servizio di Ddns (*Dynamic Dns*). Impostate ora il protocollo di autenticazione del terminale: le opzioni disponibili sono due: chiave precondivisa e certificati digitali; in questa guida ci riferiremo per ragioni di semplicità alla prima ipotesi: scegliete una parola chiave di sufficiente robustezza. Oltre alla chiave precondivisa, impostate i parametri della proposta Ike: negoziazione aggressiva o classica, algoritmo di cifratura dei dati (tipicamente Des, 3Des o Aes) e di autenticazione (Sha1 o Md5) e il gruppo Dh da utilizzare. Questi parametri presupporrebbero una buona conoscenza della tecnologia Vpn, ma è possibile procedere anche senza particolari nozioni. Impostate ad esempio una negoziazione classica, con cifratura Aes, autenticazione SHA1 e gruppo DH2, annotando ciascun parametro scelto.

FASE 2 Configurare il server Vpn

La seconda fase di configurazione del tunnel consiste nella definizione della IPSec Sa. Questa associazione sfrutta la Ike appena configurata nella fase 1 per stabilire un tunnel sicuro; indicate quindi nell'apposito spazio che desiderate servirvi della policy *PCprova*. Al momento dell'accesso da remoto, il client Vpn entra a far parte della vostra rete come se si trattasse di un normale terminale locale; per questo dovete indicare un indirizzo IP privato che sarà associato alla macchina virtuale. Se ad esempio la vostra Lan è identificata dagli indirizzi 192.168.0.X, potete riservare al client Vpn l'indirizzo 192.168.0.34 con il quale il terminale sarà raggiungibile dalla Lan. Impostate infine i parametri dell'associazione IPSec: alcuni dei campi sono analoghi alla fase 1, ma non devono necessariamente assumere gli stessi valori. Altri parametri includono il tipo di incapsulamento (tunnel, nel nostro caso) e il protocollo di tunneling (Esp o Ah). Se desiderate che il personal computer remoto possa sfogliare la rete dell'ufficio attraverso le Risorse di rete di Windows, ricordatevi di abilitare il passaggio del protocollo NetBIOS attraverso il tunnel.

Giunti a questo punto, la configurazione del client è relativamente semplice: vi basterà riportare in modo duale tutti i valori impostati sul router: nella fase 1, ricordatevi di indicare l'indirizzo IP pubblico della vostra rete o in alternativa il dominio Ddns che avete configurato.