PROTEZIONE DELLA RETE WIRELESS

COME PROTEGGERE LA TUA RETE CASALINGA DAGLI INTRUSI

BOGDAN BOTEZATU
E-THREATS ANALYSIS AND COMMUNICATION TEAM

ITALIAN TRANSLATION
FABIO GINEX

HOME USERS

bitdefender

Indice

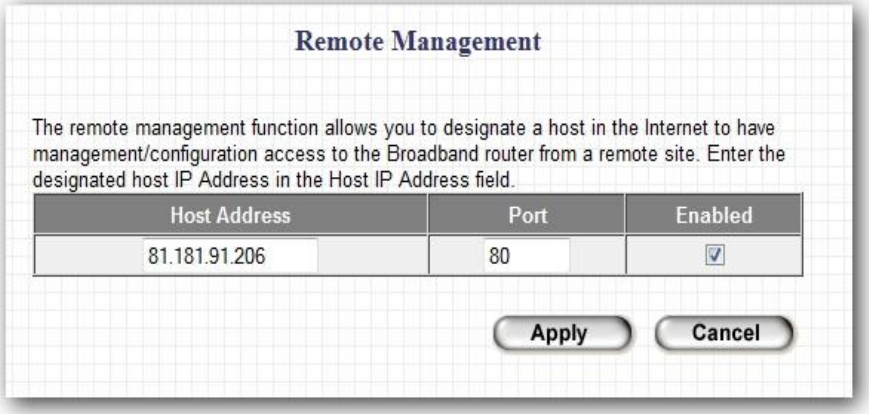
Perché le reti wireless al posto delle reti cablate?

Le comunicazioni radio sono il modo migliore per coprire aree di grandi dimensioni senza dover investire nel cablaggio, per effettuare cambiamenti strutturali quando si tratta di edifici o di eliminare il disordine. Tuttavia, il wireless è continuamente messo in discussione per quanto riguarda la sicurezza poichè l'informazione, anche se spesso è criptata, fluisce liberamente sotto forma di onde radio ed è pubblicamente disponibile a chiunque si trovi nella zona di copertura.

La seguente guida vi mostrerà le migliori prassi da seguire per l' utilizzo delle reti wireless, oltre a come proteggere il router di casa o gli access point per impedire ad altri di abusare della vostra rete.

Alcuni dei vantaggi più evidenti dell'implementazione di una rete wireless 802.11 b / g / n a casa o in piccoli uffici sono il basso costo di acquisto di hardware wireless (access point o router e schede di rete wireless), la facilità di implementazione (non c'è bisogno di forare pareti o di stendere i cavi) e la libertà di movimento propria di una soluzione senza fili. La presenza di adattatori wireless per notebook, netbook e per alcuni telefoni cellulari, ha contribuito anche alla maggiore diffusione delle comunicazioni wireless.

Nonostante le informazioni tra il client e l'access point o il router scorrano liberamente e siano accessibili da qualsiasi altro client nella zona di copertura, una rete wireless ben configurata è completamente sicura.



La gestione in remoto ti permette di definire a quali IP è permesso l'accesso all'interfaccia di amministrazione.

Di preciso, che cosa ha bisogno di una maggiore sicurezza?

Per impostazione predefinita, i router e gli access point vengono venduti con poche o nessuna impostazione di sicurezza attivata. La maggior parte dei router e access point dispongono di una pagina di amministrazione basata su browser che è disponibile accedendo all'IP del dispositivo tramite un browser. Al momento di accedervi, il dispositivo richiede un nome utente predefinito e la password, che solitamente è la stessa per ogni modello, ed è disponibile pubblicamente su Internet.

Accessi amministrativi e log-in remoti

La maggior parte dei dispositivi wireless possono funzionare fin da subito, senza ulteriore configurazione, grazie alla moltitudine di tecnologie e funzionalità implementate per facilitare la diffusione, anche fra i normali consumatori con poche competenze tecniche. L'errore più comune riscontrato tra gli utenti è il fatto di lasciare il dispositivo "*così com'è*" perché risulta funzionante in ogni caso. Invece, è assolutamente obbligatorio cambiare la password subito dopo che il dispositivo è stato collegato e acceso.

Allo stesso modo, è importante proteggere il pannello amministrativo per evitare che un soggetto non autorizzato possa manomettere le impostazioni di rete e/o eseguire alcune azioni come cancellare il log degli accessi, con lo scopo di non lasciar traccia durante la connessione alle reti altrui.

Al fine di minimizzare ulteriormente l'intrusione nel pannello di amministrazione, il proprietario del dispositivo wireless dovrebbe anche disattivarne l'accesso remoto. La maggior parte dei router e access point consente ad un utente autorizzato di modificare le impostazioni del dispositivo - anche se non sono nello stesso edificio - semplicemente digitando nel browser l'indirizzo IP.

Questa caratteristica si rivela preziosa per gli amministratori di sistema che devono risolvere un problema di connettività a tarda notte, dato che permette loro di accedere dal comfort della propria casa, ma espone anche il router a chiunque cerchi di accedere all'indirizzo IP associato con l'interfaccia pubblica del dispositivo.

Se il router non accetta la creazione di un elenco di indirizzi IP di fiducia autorizzati ad accedere al pannello di amministrazione, è consigliabile disattivare l'interfaccia di amministrazione remota.


MAC Address Filtering Table
It allows to entry 20 sets address only.

NO.	MAC Addres	Comment	Select
1	00:1f:e1:9b:4f:2b	Lori's Dell	☐
2	00:23:4d:c1:5a:62	Bogdan's Dell	☐
3	00:0e:2e:f4:06:0b	Kappa's PC	☐
4	00:24:d6:51:9d:06	Bog's Dell	☐
5	00:21:63:28:c1:39	Cati's Laptop	☐

Delete Selected | Delete All | Reset

Il filtro MAC assicura che il router accetti solo client già segnalati come affidabili.

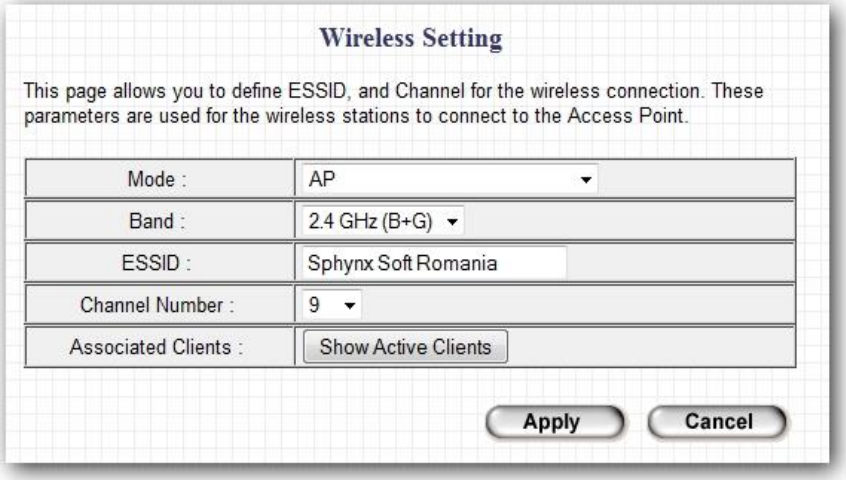
Crittografia del traffico wireless

Oltre a proteggere l'area di amministrazione del dispositivo wireless, grande attenzione dovrebbe essere prestata al collegamento senza fili stesso. Abbiamo accennato in precedenza in questo documento che, a differenza delle infrastrutture formate da reti cablate, che trasportano il segnale tra router e computer - una rete di per sé affidabile - il segnale wireless copre vasti spazi, che sono limitati solo dalla potenza di trasmissione. A seconda della zona di copertura, ci possono essere decine di computer che tentano di connettersi alla rete senza autorizzazione o, ancora peggio, intromettersi nel flusso di informazioni che scorre in chiaro.

Questo è il motivo per cui il proprietario del router wireless è obbligato a impostare una solida linea di difesa tramite la crittografia della connessione utilizzando una chiave pre-condivisa. Al fine di mantenere i prezzi verso il basso e ridurre la complessità di implementazione, i dispositivi wireless sono generalmente dotati di due protocolli di cifratura, ossia Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA / WPA2).

Entrambi i protocolli si basano su una misura di autenticazione a un fattore sotto forma di chiavi precondivise che agiscono come password, ma sono diversi in termini di sicurezza. WEP esiste dal 1997, quando faceva parte del protocollo 802.11, ma è ormai diventato obsoleto a causa di alcuni gravi difetti che lo rendono facilmente raggirabile. WPA e WPA2 forniscono un livello di sicurezza valido mantenendo il lavoro di configurazione al minimo, il che li rende la migliore scelta per le reti wireless domestiche.

Ci sono casi in cui l'uso del WPA è impossibile - soprattutto quando l'infrastruttura di rete è costruita attorno a vecchi hardware che sono stati acquistati prima dell'introduzione degli standard. Se il dispositivo non supporta il WPA, il primo passo da fare è verificare tramite il produttore se non vi è alcun aggiornamento del firmware che possa includere il supporto WPA.



La trasmissione del SSID comunica agli utenti la presenza di una rete wireless nelle vicinanze. Potenziali attacchi possono essere in grado di sfruttare questo elemento.

Anche se non è disponibile alcun aggiornamento firmware, si dovrebbe comunque scegliere WEP piuttosto che lasciare la connessione non crittografata, ma bisogna tenere presente che si rischia di esporre i dati ad un potenziale intruso e che sarebbe più saggio spendere circa 30 - 40 euro per comprare un nuovo router wireless che supporta in modo nativo WPA/WPA2.

Impostare i criteri d'accesso secondo il MAC (Media Access Control)

Un metodo secondario per filtrare eventuali intrusi è quello di definire le politiche riguardanti l'identità dei computer che tentano di connettersi alla rete wireless. La maggior parte dei router SOHO e access point supportano il controllo degli accessi basato sul MAC, ovvero il router accetta solo connessioni provenienti da un elenco predefinito di clienti che si identificano con i MAC delle schede wireless.

Alcune schede wireless consentono all'utente di modificare l'indirizzo MAC quando necessario. Questo significa che il filtraggio MAC da solo non è una soluzione efficace per tenere a bada gli intrusi. Tuttavia, è una precauzione in più che, insieme ad una solida chiave WPA pre-condivisa, aumenterà la sicurezza della rete wireless.

I passaggi sopra elencati sono il mezzo più comune per assicurare una rete e prevenire altri utenti non autorizzati (come vicini di casa o dirottatori WLAN) di connettersi ad essa. Nella sezione seguente discuteremo di come nascondere la rete, in modo da renderla inaccessibile ad eventuali intrusi che vogliano forzarla.

La trasmissione del SSID comunica agli utenti la presenza di una rete wireless nelle vicinanze. Potenziali attacchi possono essere in grado di sfruttare questo elemento.

Arrestare il broadcast di SSID

Al fine di consentire all'utente di riconoscere una rete wireless da un'altra, router e access point trasmettono automaticamente il proprio nome (noto anche come *ESSID/SSID* o *Service Set ID*. Anche se utile per il proprietario della rete, questo metodo è comodo anche per potenziali utenti esterni, perché in pratica il router "urla" continuamente per richiamare l'attenzione della sua presenza. Disabilitare l'SSID broadcast permetterà al router (con tutti i client ad esso collegati) di rimanere invisibile a chi non è consapevole del fatto che vi sia un trasmettitore wireless attivo nella zona.

Ridurre al minimo la trasmissione

Proprio come qualsiasi dispositivo radio, l'access point/router è in grado di coprire un'area che è proporzionale alla potenza del trasmettitore incorporato. Il valore predefinito di fabbrica è più che sufficiente a coprire una casa e anche parte degli spazi pubblici circostanti, come ad esempio scale o il marciapiede di fronte alla casa, il che significa che chiunque dotato di un netbook o laptop può tentare di forzare la rete. Ridurre al minimo la potenza di trasmissione può garantire effettivamente che il router non trasmetta al di là di vostra proprietà, rendendo così impossibile lo sniffing della rete.

Alcuni router e access point SOHO d'alto profilo possiedono le impostazioni software per ridurre la potenza di trasmissione della scheda di rete WLAN. Non esiste un valore sicuro pre-calcolato per offrire il miglior rapporto tra sicurezza e prestazioni.

Il Firewall BitDefender individua automaticamente reti non sicure e raccomanda all'utente le azioni da intraprendere.

Quando si modifica la potenza di uscita della WLAN, bisogna tenere presente che l'aumento della potenza di trasmissione può attirare ospiti non indesiderati alla WLAN. Al contrario, riducendo troppo la potenza di trasmissione si rischia di ridurre drasticamente le prestazioni della rete in termini di trasferimento dati.

La potenza di trasmissione può essere controllata anche sui dispositivi che non hanno questa opzione integrata nel firmware. Basta rimuovere l'antenna del dispositivo (o una delle antenne, se il dispositivo senza fili ne possiede più di una) affinché il segnale sia abbastanza basso per scoraggiare l'intercettazione, ma sufficiente per un rendimento elevato all'interno della casa.

Anche il posizionamento fisico del router influisce sulla copertura. Come regola generale, non porre mai il router wireless o l'access point vicino a una finestra che si affaccia su luoghi pubblici, perché le onde radio si propagano meglio attraverso il vetro che attraverso il cemento.

Rischi dell'utilizzazione e della connessione a reti non protette

Come regola generale, le reti non protette significano guai. Con poche eccezioni, quando cioè si rivoltano contro l'"invasore", le reti non protette sono una notevole fonte di perdita di dati per il proprietario.

Le reti domestiche si basano **sulla fiducia**: non ci sono costosi meccanismi di autenticazione messi in atto per ridurre al minimo l'accesso ad una risorsa o un altra. Al contrario, gli utenti domestici tendono a rendere il tutto a disposizione del pubblico, in modo che le informazioni di un computer siano disponibili ad altre macchine in famiglia.

Condivisioni di rete con privilegi di lettura e scrittura o in possesso di informazioni private (documenti ed immagini, per esempio, per citarne solo alcuni) sono i punti deboli più incontrati nella rete domestica.

Nel momento in cui gli utenti non autorizzati si connettono correttamente a una rete non protetta, hanno accesso alle condivisioni di rete, il che significa che possono copiare foto di famiglia, documenti o file multimediali come giochi e film. Se queste condivisioni di rete sono scrivibili, l'attaccante può cancellare il contenuto della cartella, o anche piantare un malware camuffato da file innocente e attendere che l'utente lo esegua.

Il **packet sniffing** e l'intercettazione del traffico sono altri aspetti da valutare quando si parla di intrusioni in rete. In base alla progettazione, il traffico di rete fluisce liberamente tra tutti i computer. E' il computer che decide quale tipo di traffico processare e quale scartare perché le informazioni specifiche non erano destinate ad esso. Un intruso camuffato da "elemento della rete" può ascoltare tutto il traffico utilizzando strumenti speciali e di processarlo alla ricerca di conversazioni IM, dati di login che non sono stati inviati tramite connessioni SSL e così via.

Il **Sidejacking** è una forma di packet sniffing, ma è molto più efficiente delle intercettazioni senza un obiettivo specifico alla ricerca di nomi utente e password inviate in chiaro. Questo tipo di attacco intercetta cookies scambiati tra gli utenti autenticati e rispettivi siti web. L'attacco è efficace anche contro i servizi web che utilizzano l'autenticazione SSL per crittografare nome utente e password prima di inviarle al server. Una volta che il cookie cade nelle mani sbagliate, può essere utilizzato per l'autenticazione ad un servizio di web proprio come l'utente originale, senza che quest'ultimo nemmeno sappia che c'è qualcun altro che sta utilizzando l'account.

Le reti non protette possono facilmente essere un canale giusto per **vari scopi illegali**. In genere, i cyber-criminali decidono di utilizzare le reti aperte per ordinare i prodotti utilizzando carte di credito rubate, per agire illegalmente in spazi privati o per scaricare illegalmente musica, film o software via P2P, al fine di camuffare la propria identità dietro l'indirizzo IP di una rete non protetta. Se la polizia decide di perseguire l'autore del reato, in realtà finiranno per perseguire lo sprovveduto proprietario della rete aperta. In altri casi, i cyber criminali utilizzano reti wireless non protette per inviare grandi quantità di spam a nome del proprietario della rete, che probabilmente porterà ad ulteriori indagini o anche alla cessazione dell'abbonamento Internet.

Connettersi a reti non protette è altrettanto pericoloso, perché il traffico in chiaro che scorre tra te e il router o access point può essere facilmente intercettato da persone malintenzionate collegate sulla stessa rete. Si rischia di esporre le condivisioni di rete che sono state configurate per la rete di casa o persino rimanere infettati da worm vari provenienti da altri sistemi in rete.

Suggerimenti sulla sicurezza durante l'accesso agli hotspot

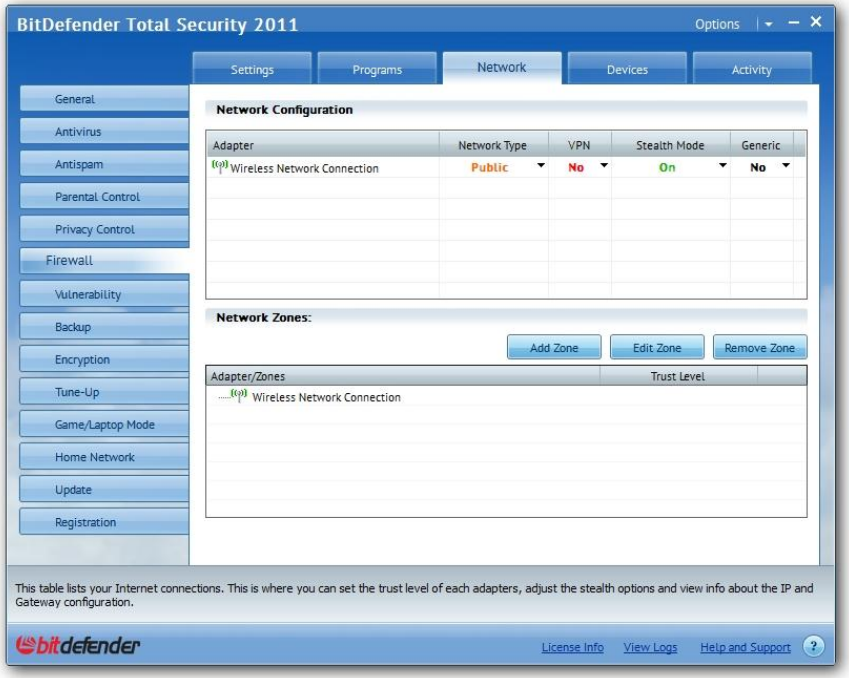
I punti d'accesso potrebbero presto divenire molto diffusi con parchi, internet cafè e aeroporti in grado di fornire l'accesso gratuito a Internet.

Tuttavia, la connessione a un hotspot non protetto può portare più problemi che soddisfazioni, se non è stato preso un livello minimo di precauzione. Qui ci sono alcune linee guida per aiutarvi a stare al sicuro durante la navigazione in incognito.

Ogni volta che si è in roaming in una rete non protetta, ricordati che non sai chi sono i tuoi vicini. Si può tentare di eseguire le scansioni delle porte al fine di individuare le vulnerabilità sfruttabili, e entrare nella sicurezza locale. Al fine di minimizzare i rischi, è necessario installare un firewall in grado di filtrare i tentativi di connessione alla rete esterna.

Le reti pubbliche non sono adatte per lo scambio di informazioni sensibili. Esiste il rischio che uno o più utenti che condividono lo stesso punto d'accesso cerchino di curiosare fra il traffico di rete proveniente da, e verso, altri computer alla ricerca di informazioni preziose quali nomi utente, password, interessanti conversazioni di messaggistica instantanea o, meglio ancora, autenticazioni e-banking. Si consiglia di prestare particolare attenzione a quali servizi si utilizzano durante la connessione hotspot e di evitare di eseguire login per quanto possibile.

Le condivisioni di rete sono un altro aspetto critico che deve essere preso in considerazione quando ci si collega ad altre reti, in quanto si corre il rischio di esporre involontariamente dati privati a persone non autorizzate. Ricordatevi sempre di disattivare le condivisioni prima di connettervi ad un punto d'acesso.



BitDefender nasconde automaticamente il computer dalle altre postazioni presenti nella rete quando il profilo di rete è impostato su "Pubblico"

Come BitDefender vi può aiutare?

BitDefender ha introdotto il modulo firewall nel 2001, diventando così il primo antivirus al mondo con un funzione firewall integrata. I prodotti 2011 di BitDefender - Internet Security e Total Security - dispongono di un firewall ottimizzato per venire incontro alle esigenze di sicurezza in ambienti wireless non protetti.

Al fine di facilitare la configurazione, il firewall BitDefender viene fornito con quattro tipi di rete pre impostati : Sicura, Home/Office, Pubblica e Non Sicura.

Ancor di più, se collegato a reti pubbliche, il firewall attiva automaticamente la modalità Stealth, che nasconde automaticamente il computer da altri sistemi nella rete, riducendo così al minimo le possibilità di essere intercettati dal malware o dagli hacker.

Anche quando usato dalla comodità della propria rete, il firewall può risultare utile, in quanto ha una funzione che visualizza una notifica ogni volta che un computer si collega alla rete.

Ciò è particolarmente importante per aiutare a individuare se i sistemi che si connettono alla rete in realtà appartengono a utenti conosciuti o vi è stato un tentativo riuscito di hacking.

Le informazioni e i dati presenti in questo documento rappresentano l'attuale opinione di BitDefender ® sugli argomenti trattati al momento della pubblicazione. Questo documento e le informazioni presenti non devono essere interpretati in alcun modo come impegno o accordo di qualsiasi sorta per BitDefender.

Sebbene ogni precauzione sia stata presa nella preparazione di questo documento, l'editore, gli autori e i collaboratori non si assumono alcuna responsabilità per eventuali errori e/o omissioni. Tantomeno si assumono responsabilità per eventuali danni derivanti dall'uso delle informazioni contenute nel presente documento. Inoltre, le informazioni qui presenti sono soggette a modifiche senza preavviso. BitDefender, l'editore, gli autori e i collaboratori non garantiscono la pubblicazione di ulteriori documenti relativi ai contenuti qui presenti, o la pubblicazione di qualsiasi altra informazione futura.

Questo documento e i dati contenuti al suo interno sono solo a scopo informativo.

BitDefender, l'editore, gli autori e i collaboratori non forniscono alcuna garanzia, espressa, implicita o per legge, per quanto riguarda le informazioni contenute in questo documento.

Il contenuto del documento può non essere adatto per ogni tipo di situazione. Nel caso in cui assistenza a livello professionale fosse richiesta, si prega di richiedere la consulenza di un professionista. BitDefender, l'editore, gli autori e i collaboratori non sono responsabili per danni derivanti da questo documento.

Il fatto che un individuo o organizzazione, il lavoro di un singolo o collettivo, compresi materiali stampati, documenti elettronici, siti web, ecc... siano indicati in questo documento come una citazione e/o fonte di informazioni non implica che BitDefender, l'editore, gli autori e i collaboratori condividono le informazioni o le raccomandazioni che queste persone, organizzazioni, opere individuali o collettive, compresi i materiali stampati, documenti elettronici, siti web, ecc possono fornire. Informiamo i lettori che BitDefender, l'editore, gli autori e i collaboratori non possono garantire l'accuratezza delle informazioni qui presentate dopo la data di pubblicazione, includendo, ma non limitandosi a indirizzi Web e collegamenti internet elencati nel documento, i quali potrebbero essere stati modificati o rimossi fra il momento in cui questo lavoro è stato scritto e pubblicato, ed è il momento in cui viene letto.

bitdefender