White Paper

Sicurezza Wireless con Cyberoam

"**Fault tolerant**" e sicurezza sono ormai un Must per le reti Wireless di ogni azienda e organizzazione che affidano sempre più spesso la trasmissione dei propri dati a reti costruite con architettura IEEE802.11 reti locali Wireless (**WLan**).

Ovviamente l'utilizzo di queste reti pone agli IT Manager delle problematiche quali:

- necessità di garantire la sicurezza della connessione;
- necessità dell'erogazione del servizio anche ad utenti diversi di quelli a dominio (Guest);
- difesa dagli attacchi informatici;
- sicurezza dell'architettura aziendale e dei dati in essa contenuti;
- rispetto della privacy;
- conformità alle normative;
- controllo e monitoraggio della navigazione;
- scelta della tecnologia a garanzia di sicurezza.

Punti fondamentali per la sicurezza in ambiente Wireless

Mentre la sicurezza è importante per tutte le reti, le WLAN meritano una particolare considerazione, in quanto sono soggette ad un livello molto più elevato di rischio. In primo luogo, dal momento che le reti wireless possono estendersi oltre il normale perimetro di un'organizzazione, la sicurezza fisica risulta di fatto molto meno efficace se confrontata con una rete cablata. In secondo luogo, abusare della disponibilità più o meno legale di una rete wireless è diventato abbastanza semplice vista l'enorme quantità di strumenti di "**hacking wireless**" disponibili in internet. Infine, la conoscenza ormai diffusa dei protocolli 802.11 e la proliferazione dei dispositivi di connessione, unita alla scarsa applicazione delle regole, consentono, ai malintenzionati o più semplicemente agli approfittatori, di accedere alle reti aziendali esponendole ai rischi a cui questa pratica le espone.

Ad onor del vero le reti WIFI sono soggette a diversi regolamenti quali **PCI, HIPAA, SOX**. Le transazioni eseguite con carta di credito sono sottoposte al rispetto dello **Standard PCI** al fine di mitigare le probabilità di furto delle credenziali, del numero della carta e più in generale di frode. Tutti coloro che utilizzano per la loro attività le carte di credito devono mettere a disposizione dell'utenza un'infrastruttura informatica sicura, atta a proteggere e cifrare i dati dei titolari della carta. Hanno l'obbligo di monitorare e testare periodicamente il loro network in modo da continuare a garantire il giusto livello di sicurezza.

La "**Health Insurance Portability e Accountability Act**" (**HIPAA**), è stata creata dal

congresso americano nel 1996 proprio per porre le regole relative alla sicurezza all'interno delle reti informatiche in ambiente sanitario, con particolare riferimento ai settori amministrativi e tecnici in modo da garantire l'integrità e la riservatezza dei dati dei pazienti, soprattutto in caso d'impiego di reti wireless che sono notoriamente più vulnerabili.

L'aumento della disponibilità degli strumenti **di hacking wireless** facilmente rintracciabili in internet espone le reti wireless ad un livello di rischio molto più elevato di quello a cui sono esposte le reti cablate.

Infine, le aziende pubbliche sono soggette al "**Sarbanes-Oxley Act**" (**SOX**) e a misure analoghe anche al di fuori degli Stati Uniti (prima solo aziende multinazionali ora anche tutte quelle aziende che intraprendono o intendono iniziare attività internazionali). Il **SOX** richiede alle aziende di mantenere e valutare periodicamente le proprie strutture tecnologiche e le procedure per l'informativa finanziaria in modo da valutare l'efficacia stessa delle strutture poste al controllo interno, che sono di fatto la vera garanzia della correttezza di tutto il processo aziendale. In quest'ottica la sicurezza della rete informatica è parte fondamentale della revisione e del controllo. Anche in Italia tutte le norme che erano alla base del **DPS** (documento programmatico della sicurezza) sono legge, anche se è decaduto l'obbligo di compilazione del DPS, per cui un atteggiamento come quello sopra descritto consente di fornire sicurezza agli utenti nel rispetto delle normative che non possono essere trascurate.

La protezione delle reti LAN senza fili, una continua sfida alla sicurezza

In questa sezione, proveremo a focalizzarci sugli "**obiettivi di sicurezza**" relativi ad un'architettura informatica realizzata in Wireless e proveremo ad accettare e a vincere alcune delle sfide che incontreremo man mano che procediamo nel discorso.
Come ogni altro sistema informatico, anche una LAN wireless deve accondiscendere ad alcune regole basilari e tipiche di ogni rete costruita per fornire connettività all'utenza privata o pubblica che sia. Proviamo a vedere insieme quali sono queste regole base:

- **Riservatezza:** è necessario garantire che la comunicazione possa essere letta solo dagli interessati e da nessun altro se non espressamente autorizzato.
- **Integrità:** è necessario garantire che i dati in transito raggiungano la loro naturale destinazione senza poter in alcun modo venire modificati in modo casuale o ancor peggio intenzionale.
- **Disponibilità:** è necessario garantire che i dispositivi e gli utenti autorizzati possano accedere correttamente e nel tempo alla rete e alle risorse a cui sono destinati.
- **Controllo:** è obbligatorio procedere ad un controllo sulla navigazione degli utenti connessi con registrazione degli orari, dei siti visitati e delle risorse impegnate attraverso la compilazione di apposito Log da rendere disponibile alle autorità competenti.
- **Tutela:** tutelare la propria integrità aziendale/personale fisica/morale da malfattori o approfittatori che possono usare la struttura informatica a proprio vantaggio. Tale tutela può avvenire tramite la messa in campo di apparati H/W e S/W tesi alla navigazione limitata/controllata e all'utilizzo autorizzato delle risorse.

Vediamo di seguito quali sono le principali categorie di attacco informatico (**Threat**) a cui la nostra Wlan può essere sottoposta:

- **Denial of Service;** nella sicurezza informatica **DoS**, scritto con la maiuscola al primo e terzo posto, è la sigla di **denial of service**, letteralmente negazione del servizio. Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio stesso. Oltre al senso primario di denial of service, come azione deliberata, ci si può riferire ad esso come azione accidentale, in seguito per esempio ad una errata configurazione.
- **Eavesdropping;** così definita l'attività di un malintenzionato il quale monitora il traffico di rete in modalità silente allo scopo di venire in possesso di credenziali, password o dati sensibili da cui trarne un proprio beneficio.
- **Man-in-the-Middle;** in crittografia, l'attacco dell'uomo in mezzo, meglio conosciuto come man in the middle attack, **MITM** o **MIM** è un tipo di attacco nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte, ovvero un attaccante. L'attaccante deve essere in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime.

- **Masquerading;** è rappresentato da un malintenzionato che impersona in modo improprio un utente autorizzato, in modo da usare le credenziali sottratte per delinquere.
- **Message Modification;** è un attacco realizzato tramite la parziale cancellazione di un messaggio originale, la sua riscrittura ed il successivo inoltro.
- **Message Replay;** l'attaccante monitora passivamente le trasmissioni e ritrasmette i messaggi, agendo come se fosse l'utente legittimo.
- **Misappropriation;** l'attaccante ruba o fa uso non autorizzato di un servizio o di un'applicazione.
- **Traffic Analysis;** l'attaccante monitora passivamente le trasmissioni e identifica i modelli di comportamento e di comunicazione degli utenti per riutilizzarli in seguito per trarne vantaggio (social engineering).

La maggior parte delle minacce rivolte contro le reti wireless coinvolgono un attaccante che ha accesso al collegamento radio tra i vari dispositivi wireless.
Una volta acceduto alla rete, la tipologia di attacco da portare varierà a seconda del vero scopo del malintenzionato, come descritto nella tabella sopra riportata. La minor difficoltà con la quale si può avere accesso al collegamento mette in evidenza le differenze

più significative tra le problematiche di protezione che esistono tra una rete wireless e le reti cablate.
La relativa facilità di intercettazione delle trasmissioni all'interno di una rete wireless consente di inserire o modificare i dati in modo che questi appaiano inviati da una fonte autentica.
Per violare invece una rete cablata, un attaccante ha bisogno di accedere fisicamente alla rete o da locale o da remoto per essere in grado di compromettere sistemi che di solito non sono presenti su una rete wireless. In una Wlan un utente malintenzionato deve semplicemente essere connesso alla rete, non è necessario che sia all'interno dell'azienda ma è sufficiente che sia fuori magari in cortile o all'interno del parcheggio. Alcuni usano antenne direzionali altamente sensibili, in grado di estendere la distanza effettiva da cui l'attacco viene portato ben al di là quindi delle distanze standard dichiarate che sarebbero necessarie a connettersi.
Un problema, spesso sottovalutato ma grave e da tenere in considerazione, è che un attacco portato ad una Wlan cela molto spesso il vero obiettivo che potrebbe essere la rete cablata aziendale a cui la Wlan è connessa.
Per questo motivo la rete wireless deve essere protetta anche contro quelle minacce che di solito parrebbero non riguardarle.
Un'altra minaccia comune, riferibile alle reti wireless, è il dispiegamento dei dispositivi di connessione non autorizzati. Se un malintenzionato si connettesse ad un punto di accesso (AP) configurato come parte dell'infrastruttura di rete dell'organizzazione ma installato provvisoriamente per risolvere un problema specifico e non più rimosso senza seguire le normali procedure di sicurezza, avrebbe la possibilità di usufruire di una formidabile "**backdoor**" dell'intera rete cablata. Ciò gli consentirebbe di bypassare sia la sicurezza perimetrale che tutti quei meccanismi come firewall e policy aziendali. Inoltre, ogni qualvolta che un client aziendale si connette anche inavvertitamente, il dispositivo canaglia avrà la possibilità di manipolarne i dati.

Le situazioni di Denial of Service (**DoS**) sono, come abbiamo detto, una grave minaccia da cui le reti wireless si devono proteggere. In caso di attacco si trovano inondate di pacchetti IP (un utente malintenzionato invia un gran numero di messaggi a una velocità elevata per impedire alla rete wireless il delivery del traffico legittimo).
E' anche possibile disturbare l'apparato WIFI tramite la trasmissione radio di una frequenza uguale o vicina a quella utilizzata per lo scambio dati per renderlo inutilizzabile. Un fenomeno simile "**Jamming**" si verifica spesso involontariamente, ad esempio, forni a microonde, telefoni cordless e altri dispositivi trasmissivi in tecnologia wireless possono inavvertitamente rendere le reti wireless inutilizzabili. La negazione delle normali condizioni di servizio può anche essere causata dalla manipolazione del protocollo di trasmissione, che può ingannare i dispositivi con richieste improprie costringendoli magari alla sconnessione o al rifiuto a fornire l'accesso agli utenti.

Architetture sicure per Wireless LAN

Di seguito analizzeremo quali sono le modalità per avere architetture Wlan sicure e quali sono i loro limiti. Descriveremo prima, molto rapidamente, le modalità WEP, WPA e WPA2 che sono state progettate appositamente per proteggere i dati a livello del collegamento fisico durante la trasmissione tra gli utenti e l'Access Point.

Wired Equivalent Privacy (WEP); in telecomunicazioni e crittografia il **Wired Equivalent Privacy** (**WEP**, dall'inglese *privacy equivalente alla rete cablata*) è parte dello standard IEEE 802.11 (ratificato nel 1999) e in particolare è quella parte dello standard che specifica il protocollo utilizzato per rendere sicure le trasmissioni radio delle reti Wi-Fi. WEP è stato progettato per fornire una sicurezza comparabile a quelle delle normali reti LAN cablate. Seri difetti sono stati scoperti nella particolare implementazione dell'algoritmo crittografico utilizzato per rendere sicure le comunicazioni. Questo ha reso necessaria una revisione del WEP che adesso viene considerato un sottoinsieme del più sicuro standard Wi-Fi Protected Access (WPA) rilasciato nel 2003 e facente parte dell'IEEE 802.11i (conosciuto come WPA2) definito nel giugno del 2004. Il WEP viene ritenuto il minimo indispensabile per impedire a un utente casuale di accedere alla rete locale.

Wi-Fi Protected Access(WPA); Wi-Fi Protected Access (**WPA** e **WPA 2**) è un programma di certificazione amministrato dall'alleanza del Wi-Fi come forma di protezione dei dati scambiati in una rete di computer wireless. Il protocollo è stato creato in risposta alle numerose falle che i ricercatori hanno trovato nel sistema di sicurezza precedente, il Wired Equivalent Privacy (WEP), sebbene una ricerca condotta nel 2008 abbia portato alla luce dei difetti anche nell'implementazione del WPA. Questo protocollo implementa la maggior parte dello standard IEEE 802.11i e intende essere una soluzione intermedia, atta a sostituire il protocollo WEP mentre lo standard 802.11i veniva ultimato. Nella fattispecie, il protocollo TKIP (*Temporal Key Integrity Protocol*), fu incluso nel WPA. Il protocollo TKIP cambia dinamicamente la chiave in uso e la combina con un vettore di inizializzazione (IVS) di dimensione doppia rispetto al WEP (in modo da rendere vani gli attacchi simili a quelli previsti per il WEP) e può essere implementato nelle schede di interfaccia wireless pre-WPA, che cominciarono ad essere distribuite nel 1999, attraverso un aggiornamento del firmware. Siccome i cambiamenti richiedono meno modifiche sul client che sull'access point, molti access point costruiti prima del 2003 non possono essere aggiornati per supportare il WPA con TKIP. La successiva certificazione WPA2 indica conformità con un protocollo avanzato che

implementa pienamente lo standard. Questo protocollo avanzato non può funzionare su alcune vecchie schede wireless. I prodotti che hanno completato con successo la fase di test da parte dell'alleanza per il Wi-Fi per la conformità con il protocollo possono esibire il marchio WPA.

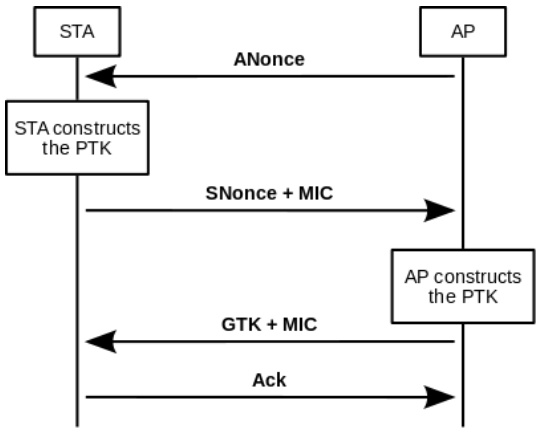
Wi-Fi Protected Access 2(WPA2); IEEE 802.11i (conosciuto anche come **WPA2**) è uno standard sviluppato dalla IEEE specificamente per fornire uno strato di sicurezza alle comunicazioni basate sullo standard IEEE 802.11. Il documento è stato ratificato il 24 giugno 2004 e rappresenta un superset (estensione) del precedente standard Wired Equivalent Privacy (WEP) che aveva dimostrato di essere soggetto a errori concettuali di progetto. Prima dello standard 802.11i la Wi-Fi Alliance aveva introdotto il Wi-Fi Protected Access (WPA), che è anch'esso un sottoinsieme delle specifiche 802.11i. Il WPA era stato introdotto per tamponare l'emergenza sicurezza dovuta al WEP e rappresenta solamente uno standard transitorio, mentre l'802.11i veniva terminato e perfezionato. La Wi-Fi Alliance ha deciso di chiamare le specifiche 802.11i con il nome di WPA2, per rendere semplice all'utente comune l'individuazione delle schede basate sul nuovo standard. L'802.11i utilizza come algoritmo crittografico l'Advanced Encryption Standard (AES) a differenza del WEP e del WPA che utilizzano l'RC4. L'architettura dell'802.11i utilizza i seguenti componenti: IEEE 802.1x per autenticare (può essere utilizzato il protocollo EAP o un server di autenticazione) il protocollo RSN per tenere traccia delle associazioni e il CCMP per garantire la confidenzialità, l'integrità dei dati e la certezza del mittente. Il processo di autenticazione avviene mediante un four-way handshake.

Il four way handshake; Il processo four way handshake (che può essere tradotto con stretta di mano a quattro vie) parte da due considerazioni. AP deve autenticarsi e la chiave di sessione utilizzata per cifrare i messaggi deve ancora essere calcolata. Per primo EAP dovrebbe scambiare la sua chiave privata (PMK) con AP. Ma questa chiave va rivelata il meno possibile e solo su un canale sicuro dato che è la parola chiave che protegge tutte le comunicazioni e quindi entra in funzione il four way handshake. Per prima cosa EAP trasmette ad AP una chiave temporanea PTK. La PTK è generata concatenando PMK, AP nonce (ANonce), STA nonce (Snonce) AP MAC address e STA MAC address. Il prodotto viene inviato a una funzione crittografica di hash.

Il protocollo utilizza la chiave temporanea GTK per decrittare il traffico multicast.

Evoluzione temporale del Four way handshake

- Nonce: Numero pseudo casuale
- AP: Access Point
- STA : Station Client



Evoluzione temporale del Four way handshake

1. AP invia il valore nonce a STA (ANonce). Ora il client ha tutti i dati per generare la PTK. (Prima mano)
2. STA invia il valore nonce (SNonce) ad AP con in più il MIC. (Seconda mano)
3. AP invia GTK e un numero sequenziale insieme a un altro MIC. Il numero sequenziale viene utilizzato per indicare il primo pacchetto

cifrato da allora. (Terza mano)
4. STA invia la conferma ad AP. (Quarta mano)

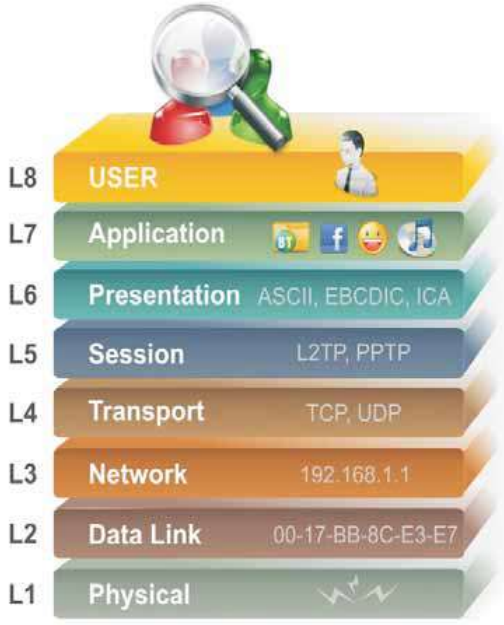
Una volta che la PTK viene recuperata viene subito divisa nelle cinque chiavi:

1. EAPOL-Key Encryption Key (KEK) - La chiave utilizzata per fornire confidenzialità per alcune informazioni addizionali spedite al client (come la GTK)
2. EAPOL-Key Confirmation Key (KCK) - La chiave utilizzata per calcolare il MIC sull'EAPOL Key message
3. Temporal Key (TK) - La chiave utilizzata per cifrare e decifrare l'attuale traffico wireless unicast.
4. MIC Tx Key - La chiave utilizzata per calcolare il MIC sul traffico unicast trasmesso dall'AP
5. MIC Rx Key - La chiave utilizzata per calcolare il MIC sul traffico unicast trasmesso dall'STA.

Le ultime due chiavi (MIC Rx/Tx) sono usate solo se la rete sta utilizzando TKIP per crittografare i dati.

La soluzione Cyberoam

Abbiamo precedentemente visto quali sono gli attacchi principali alla sicurezza delle reti WIFI e le modalità attraverso le quali i protocolli e gli standard internazionali provano a proteggere le strutture informatiche partendo dalla modalità di accesso. Proviamo ora a vedere come ogni It Manager può proteggere la sua rete utilizzando prodotti altamente tecnologici quali **Cyberoam**.
Cyberoam realizza soluzioni di security complete contro le minacce Internet esistenti e future fornendo alle reti e ai dispositivi aziendali un elevato livello di protezione da virus, worm, trojan, spyware, phishing, pharming e molto altro.
Le soluzioni di gestione unificata degli attacchi (**UTM**, ovvero Unified Threat Management) sono pensate in linea con le necessità delle aziende di dotarsi di piattaforme unificate, facili da gestire e in grado di assicurare prestazioni ottimali a fronte degli investimenti in sicurezza. La flessibilità e la vasta gamma delle appliance **Cyberoam** le rende inoltre adatte sia alle strategie delle piccole e medie aziende sia a quelle delle organizzazioni di maggiori dimensioni.
Grazie all'approccio **UTM** alla gestione unificata degli attacchi, le appliance **Cyberoam** riuniscono in una sola piattaforma numerose funzionalità di protezione come Firewall, VPN, gateway antivirus, anti-malware, anti-spam, intrusion prevention system, filtraggio dei contenuti e gestione della disponibilità della banda e dei multiple link.
Per iniziare a capire come **Cyberoam** approcci queste problematiche è necessario partire da una considerazione fondamentale che è quella



attorno alla quale gira l'intera filosofia con cui **Cyberoam** realizza le sue soluzioni. Attorno e all'interno di ogni architettura non può esistere sicurezza se non si parte da colui attorno al quale ruota tutto: **l'utente**. **Cyberoam** ha inserito sopra il livello 7 della pila OSI un nuovo livello, l'ottavo, il livello utente. Facendo convergere tutte le policy di rete attraverso questo livello è possibile riparametrizzare ogni divieto o autorizzazione su base utente facendo in modo di erogare i servizi solo a chi servono e quando servono e nel contempo in caso di attacco poter arrivare immediatamente all'individuazione dell'origine del problema eliminandolo. Tutto questo nel rispetto delle normative. E' possibile realizzare tutto ciò sia con reti tradizionali che WIFI per cui partendo dalle soluzioni di livello 2 sino a quelle di livello 7 passando tutte dall'utente che origina l'accesso. Questo straordinario e per certi aspetti rivoluzionario modo di vedere le cose pone **Cyberoam** in prima fila tra i players del mercato distinguendolo tra quella stretta cerchia di "**Innovatori"**.
Per questo motivo, al centro del progetto di sicurezza di **Cyberoam,** c'è il "**Layer-8 "Identity Based Firewall** " che aiuta a fortificare le architetture Wireless LAN security esistenti.

"**Identity Based Firewall**" di **Cyberoam**, costituisce il nucleo funzionale dell'UTM assicurando la possibilità di segmentare la rete wireless dividendola così per i dipendenti e per gli ospiti (diversi SSID e diverse VLan). L'amministratore è così in grado di creare un "**profilo comune**" per tutti coloro che accederanno in modalità ospite, attraverso la rete WIFI, rilasciando le sole credenziali di accesso. I profili precedentemente generati garantiranno la navigazione o l'accesso alle risorse predisposte per gli ospiti senza impattare sulla struttura informatica aziendale. Inoltre, può sempre definire accessi autorizzati alla rete aziendale a server extranet / DMZ in base all'identità dell'utente.

Cyberoam consente l'integrazione con i vari servizi di autenticazione quali, Active Directory, LDAP e RADIUS in modo da garantire che i suoi UTM "**Identity Based Firewall**" non siano di ostacolo all'operatività aziendale. Accetta infine l'autenticazione in modalità trasparente come il "**Single Sign On**" in modo da permettere l'accesso anche agli utenti che utilizzano questo protocollo di autenticazione.

Cyberoam implementa anche un sistema di **IDS/IPS** wireless in grado di identificare tutti gli accessi non autorizzati sulla LAN e prevenire attacchi quali "**man in the middle**". Questo modo di operare rileva immediatamente le reti ad hoc (aggiunta di AP non autorizzati) o altri tentativi di inserimento di apparati Wireless non codificati. Con un sistema IPS integrato, avvisi basati sull'identità utente e relativi report vengono generati ogni volta che si verifica un attacco **DoS/DDoS** oppure qualora venga avviata un'attività di "**backdoor**" o una qualsiasi minaccia agli utenti della rete.

Un filtro di contenuti generato sulla base del "**Layer-8 "Identity Based Firewall** di **Cyberoam** garantisce che tutti gli utenti wireless siano compatibili con la politica di accesso a Internet dell'organizzazione. Il "filtro può essere sincronizzato con la tipologia "**per applicazioni**", in grado di riconoscere e discernere le applicazioni le une dalle altre dividendole

per richiesta di banda, impedendo così l'utilizzo ingiustificato delle risorse poste alla base della capacità di connessione aziendale.

Il trend del **Byod** che significa portare il proprio dispositivo (**BYOD**) chiamato anche portare la propria tecnologia (**BYOT**), portare il proprio telefono (**BYOP**), e portare il proprio PC (**BYOPC**), si riferisce alla politica di consentire ai dipendenti di portare i dispositivi mobili di proprietà personale (computer portatili, tablet e smartphone) al loro posto di lavoro, e di utilizzare questi dispositivi per accedere a informazioni privilegiate e di applicazioni dell'azienda. Il termine è anche usato per descrivere la stessa prassi applicata per gli studenti che utilizzano i dispositivi di proprietà personale in contesti educativi. Questa modalità operativa sta mettendo a dura prova le reti **wi-fi** spingendo in alto la domanda di implementazioni di attrezzature per reti **Wlan** lo rivelano le ultime statistiche di **Infonetics Research** elaborate dopo il sondaggio condotto tra 162 aziende di medie e grandi dimensioni in Nord America.

Cyberoam UTM offre elevate prestazioni di sicurezza basate sul **Level 8 User Identity** sia su reti WLAN che reti cablate

"Grazie all'esplosione dei device mobili e alla domanda di accesso alla rete da questi device, il **Wlan** è già un mercato che fattura 4 miliardi di dollari l'anno e il nostro ultimo sondaggio dimostra che la crescita non si fermerà: prevediamo molte altre implementazioni **Wlan**", spiega **Matthias Machowinski**, directing analyst for enterprise networks and video di **Infonetics**. "Le aziende ci indicano che stanno pianificando importanti potenziamenti della loro copertura wireless e prevedono di far crescere i loro punti di accesso di più del 20% entro il 2015 per supportare i device mobili, la mobilità degli utenti e l'accesso per i visitatori".

Le aziende già mostrano interesse verso la tecnologia **wi-fi** di nuova generazione, con i prodotti per la versione 802.11ac, oppure aggiornano attrezzature preesistenti con la tecnologia 802.11n, la cui penetrazione, secondo le previsioni di **Infonetics**, è destinata più che a raddoppiare entro il 2015. Le aziende intervistate da Infonetics hanno una media di 9.000 device sulle loro reti: questo numero aumenterà del 20% entro il 2015 e la metà sarà costituito da dispositivi mobili.

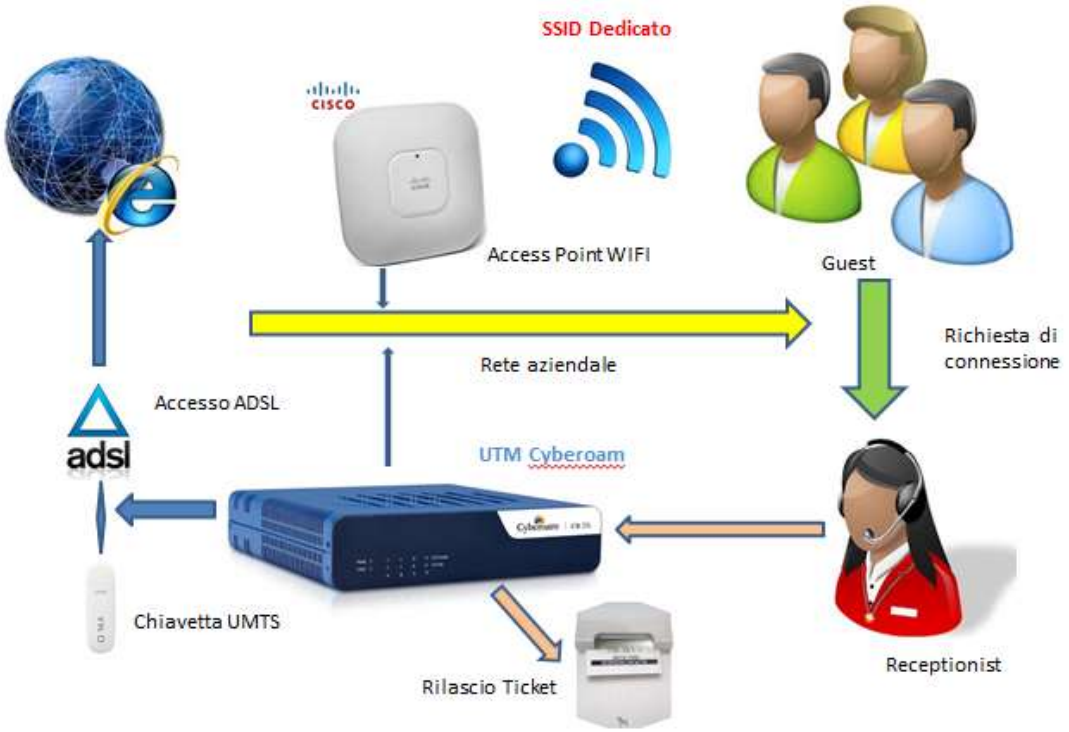
Questo enorme esercito di utenti chiede accessi sicuri a reti aziendali in modalità wireless.
Vediamo come **Cyberoam** affronta il problema.
Ogni qualvolta un utente richiede l'accesso alla rete aziendale da un punto WIFI può essere trattato in due modi diversi:

Utente aziendale

E' un utente della rete aziendale dotato quindi di credenziali e di un proprio profilo per cui durante la procedura di accesso sarà riconosciuto dall'access point a cui si collega in quell'istante (SSID per utenti aziendali) e indirizzato direttamente sulla rete a cui accederà con le sue credenziali. Anche attraverso la rete WIFI **Cyberoam** garantisce lo stesso livello di sicurezza che le policy aziendali prevedono per ogni singolo utente.

Utente Guest

Ci troviamo ora di fronte ad una serie di utenti esterni all'azienda che chiedono alla struttura informatica l'accesso per potersi connettere ad internet, alla propria casella di posta oppure ad applicazioni aziendali. In questo caso cambia tutto in quanto il richiedente non ha credenziali, non ha un profilo che gli consenta di navigare nella rete aziendale in sicurezza ma ciò nonostante deve poter accedere alla struttura. Come fare per garantire al Guest l'accesso, la navigazione sicura e la rimozione di ogni permesso al momento in cui lo user avrà completato il lavoro?
Prima di tutto verifichiamo le modalità di rilascio dei permessi per la navigazione all'interno della rete che possono essere rilasciati in due modalità distinte.
L'apparato UTM **Cyberoam** soddisfa a pieno le richieste degli Utenti Guest tramite il rilascio, da parte dell'operatore, di un ticket contenente user name e password che consentirà, a coloro che ne faranno richiesta, di navigare in Internet secondo le modalità sotto descritte.



Come Funziona

Il cuore della soluzione proposta è costituito dall'apparato UTM **Cyberoam** che offre tutte le funzionalità di Hot Spot necessarie a realizzare quanto richiesto. Quando l'utente accede ai locali dell'azienda, nei quali è installato un access point, si connetterà in automatico ad un portale (**captive portal**) in quanto sarà riconosciuto come utente non appartenente alla rete aziendale e quindi qui dirottato. Il captive portal gli consentirà di richiedere le credenziali necessarie a navigare in Internet. Ovviamente l'utenza Guest sarà connessa in WIFI tramite un SSID dedicato che lo separerà completamente dalla rete aziendale tramite una rete VLan che lo connetterà rigidamente all'UTM **Cyberoam** per la connessione ad internet. La pagina di presentazione del servizio è generata localmente dall'UTM **Cyberoam** e può essere personalizzata con i loghi dell'azienda ospitante e con messaggi predefiniti. Il Captive Portal svolge anche funzioni di statistica dei dati raccolti relativi ai Guest che si sono connessi.

Le credenziali richiese possono essere rilasciate tramite un servizio di **SMS** al quale l'azienda dovrà rivolgersi per il rilascio del servizio (**servizio a pagamento**). Questa modalità di accesso consente la generazione delle credenziali di accesso degli utenti Guest in modo automatico. L'utente riceve direttamente sul telefono la user name e password, che gli consentirà poi, tramite il captive portal, di connettersi ad Internet per un tempo predefinito dalla maschera di richiesta che appare al momento della richiesta delle credenziali. Questa però non è la modalità migliore di richiesta per l'azienda che intende invece rilasciare in proprio le credenziali e le modalità di navigazione ai propri guest per poterli completamente controllare.

Per erogare questo servizio è necessaria la presenza di un operatore aziendale in loco che fornirà, dietro richiesta, le credenziali necessarie tramite l'apertura di un ticket che potrà essere dimensionato a seconda delle richieste o della tipologia del Guest, come andremo di seguito a specificare.

Sarà necessario creare un utente amministratore (receptionist) il quale gestirà i permessi di accesso in modalità manuale. L'utente con i seguenti requisiti amministrativi potrà creare utenti singoli o di gruppo inviando le credenziali così ottenute ad una stampante. Tali credenziali saranno consegnate all'utente/gruppo per la navigazione.

La creazione contemporanea di più utenti (Gruppo) soddisfa ad esempio la necessità di un evento da tenersi localmente. L'amministratore può decidere se l'utente/gruppo sarà attivo al primo login effettuato e per un lasso di tempo definito o dal momento della creazione per lo stesso periodo di tempo.

In ogni caso, sia gli utenti guest automatici (SMS) che gli utenti creati manualmente (receptionist), sono gestiti dall' UTM **Cyberoam** come utenti locali. Quando un utente viene generato viene associato al gruppo predefinito Guest ed eredita tutte le proprietà del gruppo. Le proprietà gli consentiranno una navigazione controllata e monitorata con nessun accesso alle risorse della rete aziendale. (Policy aziendali).

Click per scaricare la presentazione.

Tali policy consentiranno all'azienda ospitante di mantenere comunque i propri standard di sicurezza stabiliti limitando la navigazioni ad alcuni siti o a particolari tipologie di siti (**Cyberoam** ragiona per tipologie e classi consentendo l'esclusione o l'inclusione automatica ad Es. dei social network, dei siti sportivi, di quelli porno o a rischio, etc.). La tipologia di navigazione del singolo utente potrà poi essere definita come di seguito:

- Per una o più ore del giorno.
- Per gruppi di ore diverse all'interno dello stesso giorno Es: 8-11,00 e 14,30-17,00.
- Per livello di traffico generato 10Mb in upload e 100 in download.
- In modalità free per un certo lasso di tempo con picco massimo di 1 GB.
- Per applicazioni utilizzate nel caso in cui venga consentito al guest di connettersi ad un servizio aziendale.

N.B: ognuno delle possibilità sopra riportate possono essere utilizzate da sole o in unione con le altre.
In ogni caso al termine del servizio previsto l'utente sarà disconnesso e per poter riaccedere alla rete dovrà effettuare una nuova procedura di richiesta.
Infine L'UTM **Cyberoam** consente un corretto log di tutti gli accessi effettuati dei siti visitati e delle applicazione utilizzate come richiesto dalla legge.

Caratteristica	Descrizione	Benefici
Accesso Wi-Fi in base all'identità presso il Layer 8	⇢ Accesso al Wi-Fi in base all'identità dell'utente ⇢ Policy uniche per dipendenti e ospiti, in base a: - nome utente o gruppo - pianificazione temporale - categorie di accesso al web - limite nel trasferimento dati - disponibilità di banda - policy per le applicazioni presso il Layer 7	⇢ Eliminazione delle lacune nella sicurezza a causa di chiavi pre-condivise in uso nelle aziende ⇢ Maggior sicurezza (accesso a tempo degli utenti ospiti) ⇢ Miglioramento della sicurezza della rete e dei dati

Access point virtuali multipli	Fino a 8 access point virtuali: creazione di reti indipendenti nella stessa area fisica Creazione di zone wi-fi per funzioni o gruppi, con separazione dalle zone per gli utenti ospiti Controllo degli accessi alla rete e a internet da parte degli utenti ospiti	Elevata sicurezza e flessibilità, ad es. raggruppamento dei reparti Vendite, Marketing, Finanziario e Progettazione in zone diverse Prevenzione del data leakage e sicurezza delle risorse di rete sensibili mediante separazione e controllo dell'accesso degli utenti ospiti
Tecnologia MIMO	Uso di MIMO Controllo della banda e della copertura wireless	Maggior throughput Personalizzazione per soddisfare le esigenze del business
Reportistica basata sull'identità presso il Layer 8	Ampie possibilità di logging e reportistica legati al nome utente Tracciamento delle attività degli utenti ospiti e dei dipendenti Scelta tra reportistica installata nell'appliance o log e rapporti centralizzati mediante CCC e iView Cyberoam	Rapida identificazione che accresce la sicurezza Soddisfacimento dei requisiti di legge

Le reti WIFI sono diventate veloci, consentono accessi in modalità mobile e in pratica allargano la connettività aziendale a dismisura, a costi più bassi di quelli necessari per una rete tradizionale, ma non dimentichiamo mai che…

La sicurezza informatica non può passare attraverso compromessi e Cyberoam lo sa.

Cyberoam GOLD PARTNER

Il Tuo EterNet Team

.

EterNet Vitalize your IT