

Wireless e innovazione

*Il Cloud WiFi
e la sicurezza
delle WLAN*

The background is a complex, abstract composition in shades of red and orange. It features numerous overlapping elements: large, semi-transparent numbers (0-9) scattered throughout; circular motifs resembling stylized eyes or lenses, some with internal patterns; and intricate, repeating geometric patterns that resemble a grid or a series of interconnected nodes. The overall effect is one of digital complexity and data visualization.

Avvertenze

Pubblicato nel 2016

Tutti i marchi contenuti in questo white paper sono registrati e di proprietà delle relative società. Tutti i diritti sono riservati. Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale.

Copyright Reportec – 2016

www.reportec.it

Indice

Wireless e innovazione	4
Il Cloud WiFi e le reti WLAN a supporto del business	6
L'emergenza della sicurezza	6
Il Cloud WiFi	9
Sette requisiti per un Cloud WiFi a prova di business	10
Le soluzioni di Fortinet	13
Fortinet Secure Access Cloud	13
La gestione "gratuita" con FortiCloud	15
Gli access point FortiAP-S	16
L'Infrastruttura Secure Access	17
Con Virtual Cell basta interferenze	17
La sicurezza con Fortinet Connect e FortiGate	20
L'Infrastruttura Secure Access Integrata	21
Una sicurezza a tutto tondo	21
Access point FortiAP	23



Wireless e innovazione

Il Cloud WiFi e la sicurezza delle WLAN

Dinamicità e multicanalità stanno cambiando l'approccio delle aziende verso i propri mercati. Protagoniste di questa trasformazione sono le reti wireless. Osserviamo le persone intorno a noi al bar, in una stazione o sui mezzi pubblici: la maggioranza di esse sta fissando il display del proprio smartphone o digitando sullo stesso. Una buona percentuale consulta email o messaggi di lavoro. Basta questo a dimostrare quanto importante sia l'approccio verso i dispositivi mobili, che hanno ormai raggiunto livelli di diffusione elevatissimi.

Secondo IDC, nel 2015 metà dei dispositivi mobili (smartphone, tablet e notebook) venduti alle imprese erano smartphone e solo poco meno di metà saranno ancora nel 2020, allorquando dovrebbe aggiungersi una piccola percentuale di wearable device.

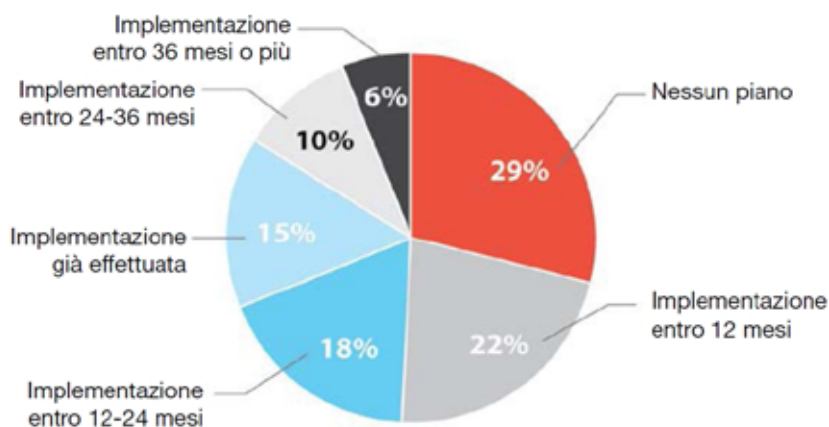
Sempre gli analisti IDC sostengono (dati diffusi a giugno 2016), che in Italia nel 2015 la forza lavoro mobile era costituita da 9,9 milioni di unità, pari al 44% del totale, mentre nel 2020 arriverà a milioni di unità: il 74%.

L'organizzazione aziendale risente delle nuove modalità operative, cambiando i modelli di conseguenza, ne è un esempio importante la crescita dei progetti di smart working che prevedono la realizzazione di spazi per il co-working in azienda. La rete deve necessariamente supportare queste nuove esigenze che si stanno posizionando alla base dell'innovazione nelle imprese. La connessione wireless diventa un imperativo.

Oggi sono sempre più le imprese che stanno implementando infrastrutture completamente wireless in azienda. Più precisamente, secondo lo studio Network Purchase Intention realizzato da ZK Research nel 2015, circa il 70% delle imprese interpellate avevano già implementato (15%) un'infrastruttura di rete "completamente" wireless o hanno espresso l'intenzione di implementarla entro il 2018, dove per completamente s'intende una rete wireless cui si collega più del 90% dei dispositivi client.

C'è poi un'ulteriore tendenza in atto che pone il wireless sotto i riflettori: si tratta dell'IoT (Internet of Things). Siamo solo agli inizi di

Quali sono i piani aziendali per passare a un luogo di lavoro completamente wireless?



Le imprese sono alla ricerca di infrastrutture solo wireless

quella che si prospetta come una vera rivoluzione. Ci sono molte imprese che stanno sviluppando progetti e applicazioni IoT. La maggior parte sono grandi imprese che hanno fatto da apripista, ma delle medie sta crescendo e, presto, arriverà l'ondata delle piccole, cui gli operatori telco, in primis, forniranno soluzioni chiavi in mano, anche gestite.

Alle reti aziendali, dunque, saranno connessi anche numerosi dispositivi che nulla hanno a che vedere con pc, stampanti e altri dispositivi tipicamente informatici, appartenendo alla variegata categoria della operational technology. Sensori connessi alle catene di montaggio, telecamere di videosorveglianza, dispositivi per il monitoraggio sanitario, sonde tra le più disparate rappresentano e sempre più rappresenteranno un mondo interconnesso per la maggior parte attraverso reti wireless. Gli analisti di ZK Research prevedono che nel 2020 ci saranno oltre 50 miliardi di dispositivi connessi.

È una rivincita per le WLAN (Wireless Local Area Network), che hanno avuto una vita difficile in Italia, dove la loro installazione era sostanzialmente vietata o vincolata fin quasi alla fine degli anni Novanta. Le prestazioni erano penalizzate dal blocco di alcune frequenze e anche a livello internazionale lo sviluppo degli standard ha sempre viaggiato a rilento, ampiamente surclassato da quello relativo alle reti cablate. Oggi, però, non è più necessario scegliere fra i vantaggi del wireless e le prestazioni di Ethernet: LAN e WLAN sono ormai comparabili.

Questo non significa che tutte le reti wireless siano uguali e che non ci siano criticità da considerare nell'implementazione di un'infrastruttura, la quale deve evidentemente garantire affidabilità e sicurezza, senza aggravare i costi operativi. Non dimenticando, inoltre, che, a seconda dei casi, può essere richiesta un'elevata scalabilità.





Il Cloud WiFi e le reti WLAN a supporto del business

Sono dunque due i requisiti basilari di un'infrastruttura wireless per reti enterprise che siano affidabili: la gestibilità e la sicurezza.

Le prime implementazioni WiFi "appiattivano" le differenze, proponendo tipologie e topologie standardizzate, senza considerare che contesti di dimensioni e settori diversi non sono assimilabili: se già esistono differenze importanti da un negozio familiare e un grande magazzino, è facile figurarsi come lo stesso WiFi non possa funzionare in un campus universitario, in un grattacielo di uffici o in un ospedale. Sono quindi nate nuove architetture e topologie, che, normalmente, mantengono l'interoperabilità con dispositivi esistenti.

Secondo le esigenze e gli scenari di utilizzo, potranno risultare migliori reti impostate diversamente: in pratica sono quattro le "variabili" da considerare in modo da realizzare reti:

- con o senza controller;
- gestite on premise o in cloud;
- basate su canali multi-cella o a singola cella;
- con gestione e sicurezza delle applicazioni integrata o separata.

Tali variabili dovranno trovare posto in un'equazione che soddisfi le esigenze specifiche di ciascuna azienda, sempre considerando centrali i temi della gestibilità e della sicurezza. Oggi sono disponibili diverse soluzioni per realizzare reti wireless, alcune decisamente evolute rispetto le prime installazioni. Nel seguito si approfondiranno quelle proposte da Fortinet. Prima di esaminare l'evoluzione, soprattutto in chiave cloud, delle WLAN si evidenzieranno le problematiche legate alla sicurezza, che influenzano le scelte tecnologiche anche in termini di topologia di rete.

L'emergenza della sicurezza

Quello della sicurezza è un tema centrale: la continua crescita delle minacce che incombono su data center e applicazioni, comunicazioni e infrastrutture di rete rende indispensabile una sicurezza



end-to-end che assicuri la massima protezione. Un'infrastruttura wireless deve essere all'altezza di tale compito.

In azienda ne sono coscienti. Infatti, la sensibilità verso i rischi informatici è aumentata in seguito alla crescita degli attacchi e all'eco mediatica che ne è conseguita. Il risultato è che i responsabili delle imprese sono consapevoli di quanto sia importante poter contare su un'infrastruttura sicura e affidabile.

Lo confermano i risultati di una recente survey condotta dalla società di ricerca Lightspeed GMI: ben il 79% degli intervistati si aspetta un'architettura integrata capace di gestire le minacce alla sicurezza informatica ed offrire al contempo un accesso sicuro alla rete. Però, pur comprendendo di aver bisogno di un'infrastruttura di sicurezza end-to-end, i responsabili IT delle imprese ritengono ancora l'adozione di una soluzione integrata un'operazione complessa da configurare, distribuire e gestire. È un atteggiamento comprensibile, perché sono effettivamente molte le violazioni alla sicurezza che sfruttano errori di configurazione, spesso riconducibili a prodotti con sistemi di controllo e gestione diversi. D'altro canto un approccio olistico alla sicurezza è sempre più fondamentale.

La stessa indagine è stata effettuata anche l'anno precedente e da allora poco è cambiato: la sicurezza delle reti wireless era ed è considerata un aspetto problematico. Gli utenti si aspettano una capacità di accesso WiFi capillare per tutti i dispositivi, sia per uso personale sia professionale, anche perché il BYOD è ormai una procedura aziendale consolidata. A tal proposito, l'indagine "Mobile Business Mobility" effettuata nel 2016 da ZK Research ha rilevato che l'82% delle aziende supporta l'utilizzo sul posto di lavoro di dispositivi consumer (anche da 3 a 5 dispositivi per utente, comprese molte realtà verticali a stretta regolamentazione, come il settore sanitario e i servizi finanziari. In più, è emerso che la maggior parte di tali dispositivi può essere connessa solo via wireless. Lo studio Lightspeed mostra che la pratica del BYOD in Emea è più ridotta e, comunque maggiormente controllata dall'IT aziendale che nel resto del mondo. Conseguenza, secondo gli analisti



di una scarsa fiducia nei confronti dei comportamenti accorti da parte degli utenti.

Del resto sono proprio questi ultimi a rappresentare il punto debole della catena. Si temono soprattutto gli attacchi mirati, tant'è che, se la perdita dei dati dei clienti e aziendali costituisce il rischio principale per la maggioranza, al secondo posto si colloca lo spionaggio aziendale, che per il 24% degli IT decision maker è invece considerato il pericolo primario.

È importante osservare che la sicurezza delle reti WiFi è sempre stata concentrata sull'accesso. Gli attuali standard di crittografia e autenticazione WiFi (WPA2, 802.1X e così via) sono in buona parte riconosciuti come robusti meccanismi per il controllo degli accessi WiFi. Occorre, però, un livello di sicurezza superiore, perché l'accesso fraudolento ai sistemi è molto più sofisticato che in passato e i cyber criminali adottano tecniche che superano l'accesso diretto utilizzando come ponti email e siti Web.

In sintesi, il sondaggio mostra una richiesta crescente di accesso wireless e di una maggiore sicurezza. Le grandi imprese ne hanno preso atto e stanno incrementando la distribuzione delle soluzioni di sicurezza al proprio interno. In particolare, considerando le reti WLAN come l'elemento più vulnerabile per l'accesso, gli investimenti si sono concentrati su architetture di sicurezza più estese. Il risultato rilevato dal sondaggio è un mix più equilibrato di metodi per sicurezza implementato nel 2016 rispetto al 2015.

Più in dettaglio, gli analisti di Lightspeed hanno osservato che le implementazioni dei sistemi per la protezione dalle intrusioni sono aumentate del 45% e del 60% sono cresciute quelle per il riconoscimento delle applicazioni.



LA METODOLOGIA DELLA SURVEY DI LIGHTSPEED GMI

Gli analisti di Lightspeed GMI hanno coinvolto 1300 decisori appartenenti al mondo dell'information technology (ITDM) in 11 paesi nel mondo e operanti in diversi settori, che comprendono manifatturiero, telecomunicazioni, servizi finanziari, istruzione, pubblica amministrazione e altri. Le aziende selezionate sono clienti di tutti i principali fornitori di apparecchiature WLAN. Il campione è composto per il 33,2% da aziende che hanno da 500 a 1500 dipendenti; per il 21,5% aziende da 2501 a 4999 dipendenti; per il 20,4% da aziende con 5000 o più dipendenti; per il 19,9% da aziende da 1501 a 2500 dipendenti; per il 4,9% da aziende da 250 a 500 dipendenti.





Il Cloud WiFi

Come prima accennato, una delle scelte da compiere, quando si vuole installare o rimodernare una rete WiFi è decidere se basarla su controller tradizionali o meno.

Oggi, infatti, sono ormai diffuse sul mercato soluzioni basate su servizi gestiti in cloud, che consentono di non installare i costosi e onerosi, in termini di gestione, controller.

In ambienti ad alta densità, con centinaia o migliaia di access point installati i controller sono probabilmente necessari, ma le imprese che hanno pochi punti di accesso wireless nonché quelle molto distribuite, che pure hanno pochi access point per sede, devono valutare i vantaggi offerti dalle soluzioni WiFi gestite nel cloud, che consentono ai clienti di acquistare solo gli access point, potendo fare a meno di controller o server di gestione.

Non è un caso, infatti che tali soluzioni siano nate soprattutto per sgravare le aziende molto distribuite dall'onere dei numerosi controller da installare.

I vantaggi non si fermano qui, anche considerando che queste soluzioni sono più recenti, quindi nate nell'epoca della user experience, con tutto ciò che ne consegue in termini di interfacce semplificate e maggiore gestibilità.

Un altro beneficio consiste nella flessibilità, tipica del cloud, che in questo caso, per un'azienda significa poter iniziare con un solo access point per poi crescere in base alle sopravvenute esigenze. Tuttavia, il cloud può non essere un salto qualitativo completo, anche se riduce la complessità e i costi. La maggior parte delle soluzioni Cloud WiFi, però, deludono in termini di contenuti e sicurezza delle applicazioni. Esse, infatti, non spostano i paradigmi delle reti wireless basate su controller: semplicemente spostano questi ultimi fisicamente dall'azienda al data center del provider. Il che introduce anche problematiche, a cominciare da un potenziale point of failure dell'infrastruttura wireless, qualora la connessione con il cloud dovesse cadere. Inoltre, anche la sicurezza è fornita nel cloud, ma i punti di accesso restano ovviamente on



premise, aprendo il fronte a nuove vulnerabilità.

Affinché una soluzione Cloud WiFi possa rispondere alle esigenze di un'impresa è necessario che risponda a una serie di attributi, soprattutto per realizzare una infrastruttura completamente wireless.

Sette requisiti per un Cloud WiFi a prova di business

Coerentemente con quanto finora esposto, la gestibilità va messa in primo piano: occorre un sistema di management completo per il provisioning di aggiornamenti e configurazioni degli access point. I controller, on premise o in cloud sono efficacissimi, ma l'evoluzione delle minacce informatiche, come prima illustrato, pongono l'esigenza di superare le forme di controllo basiche, a beneficio di una console unica la gestione di sicurezza e infrastruttura sull'intera rete. Un sistema di gestione in grado di scalare a piacere.

Il secondo requisito riguarda il provisioning, che, essendo in cloud, non deve prevedere interventi manuali. In pratica, ancora una volta a beneficio delle imprese molto distribuite, deve essere possibile distribuire nuovi access point da remoto, ovunque nel mondo, senza dover ricorrere al supporto tecnico locale. Per esempio, dovrebbe bastare collegare l'apparato, che, una volta online, viene registrato automaticamente nel cloud, scaricando le configurazioni predefinite per quella specifica azienda insieme al firmware più recente.

Terzo punto fondamentale è la visibilità granulare delle applicazioni. È fondamentale riconoscere il traffico che attraversa la rete e distinguere tra quello che è sensibile ai tempi di latenza o richiede larga banda. La molteplicità di servizi che oggi usano la rete rende ancora più necessario poter gestire al meglio la QoS (Quality of Service) sulle reti wireless.

Questo vale anche per svolgere gli adeguati e sempre più sofisticati controlli di sicurezza e, a tal riguardo, è fondamentale che le configurazioni eseguite nel cloud scaricano le relative policy negli access point in tempo reale.

L'autenticazione degli utenti su specifici SSID è il quarto requisito





da soddisfare, affinché il personale IT possa creare profili di accesso separati per diversi gruppi all'interno dell'azienda: per esempio per definire policy diverse tra studenti, insegnanti e personale ATA in una scuola.

Un gruppo che viene tipicamente trattato a parte è quello dei "guest", per i quali occorre sia previsto (quinto punto) un captive portal apposito.

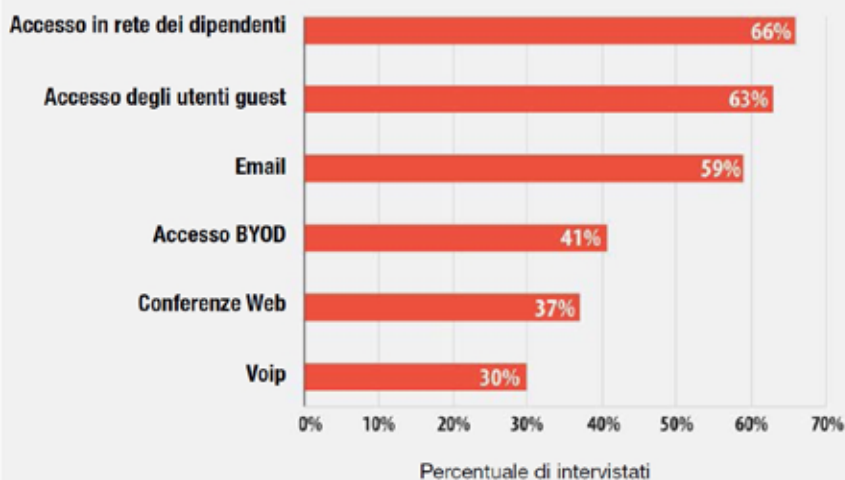
L'indagine Network Purchase Intention di ZK Research, cui si è già fatto riferimento, poneva l'accesso di utenti guest al secondo posto fra le applicazioni che le aziende intendevano implementare su WLAN.

La rete WiFi dovrebbe consentire la configurazione di SSID senza limiti quantitativi.

Il sesto attributo è nuovamente legato alla sicurezza, per la quale, come detto, non basta il controllo accessi, ma occorre poter analizzare lo stato e l'utilizzo delle applicazioni layer 7, in modo da consentire l'impostazione di un modello gestionale predittivo. È opportuno monitorare utilizzo e consumo di banda delle applicazioni e da parte di chi. Informazioni che servono per la sicurezza e per attività di manutenzione preventiva e programmazione.

La richiesta di un accesso guest

Quale delle seguenti applicazioni secondo lei sarà implementata in azienda tramite LAN wireless nei prossimi 12 mesi? (selezionare tutte le voci corrispondenti.)



Per ultimo, ma non ultimo, il settimo punto riguarda la capacità di supportare una sicurezza pensata per infrastrutture di rete completamente wireless.

Si tratta di supportare le evoluzioni evidenziate in incipit. Secondo gli analisti di ZK Research la sicurezza rappresenta l'ostacolo principale nella diffusione dell'IoT.

Un sistema di sicurezza completo non può fermarsi all'autenticazione, come avviene per la maggioranza delle Cloud WiFi, e deve,

invece, comprendere intrusion prevention e tutte le soluzioni che occorrono per mitigare la crescente ondata di minacce cyber. La soluzione Cloud WiFi di Fortinet, che analizziamo in seguito, prevede funzioni di sicurezza avanzata integrate direttamente nell'hardware dell'access point, il che evita di dover installare in cloud le diverse soluzioni per la sicurezza che occorrerebbero.



Le soluzioni di Fortinet

Fortinet mette a disposizione delle imprese tre ipotesi alternative d'infrastruttura wireless, tutte basate su gestibilità e sicurezza, permettendo di scegliere la soluzione che meglio si addice alle esigenze di ciascuna organizzazione.

In particolare Secure Access cloud è una soluzione Cloud WiFi che permette di abbinare i vantaggi di un passaggio da Capex a Opex, con la rapidità di gestione in cloud e l'efficienza necessaria per le imprese distribuite.

L'infrastruttura Secure Access di Fortinet fornisce scalabilità e distribuzione LAN wireless risultando una soluzione in grado di fornire alti vantaggi qualitativi in condizioni di alta densità e forte utilizzo di messaggi voce e video. Fornisce inoltre un ampio portfolio di servizi di sicurezza a livello di applicazione, che consentono alle aziende di potenziare il framework di sicurezza esistente con i più recenti sistemi di protezione dalle minacce sempre in evoluzione. Infine, la soluzione Secure Access integrata unisce in un'unica piattaforma la gestione dell'infrastruttura wireless e cablata senza la necessità di appliance separate. Una sola interfaccia e la garanzia che la WLAN supporti tutte le policy di sicurezza e fornisca un apporto in termini di efficienza operativa e TCO.

Fortinet Secure Access Cloud

Fortinet raccomanda la soluzione Secure Access Cloud, In particolare a piccole e medie imprese e ad aziende distribuite. Si tratta di una soluzione WiFi cloud, che si basa sul servizio di provisioning e gestione FortiCloud e su una nuova classe di Access point (AP) appartenenti alla serie FortiAP-S. A distinguerla è il fatto di unire le stesse capacità di network security tipicamente presenti nelle soluzioni WLAN aziendali gestite da controller dotati di servizi supplementari per la sicurezza.

In altre parole, mentre nelle soluzioni tradizionali il controllo del traffico provenienti da tutti gli access viene convogliato verso dispositivi centralizzati sulla LAN, per poi spesso farlo tornare indietro,





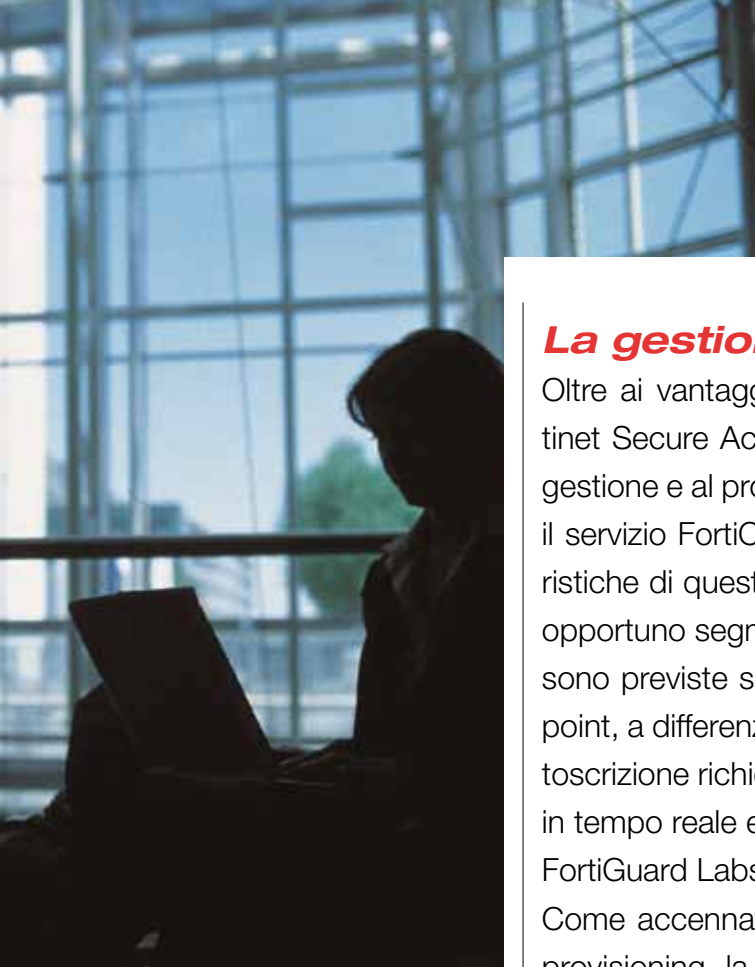
Fortinet Secure Access Cloud non necessita di tali “deviazioni” ed elimina così i conseguenti tempi di latenza, oltre che il consumo di banda. Oltre ad essere penalizzante e complicata, questa pratica inibisce anche la visibilità sul comportamento di utenti e client, poiché elaborare la sicurezza in più passaggi attraverso dispositivi diversi richiede la mappatura da un’appliance di sicurezza alla successiva e questo sui intere VLAN, non di singole sessioni.

Spesso alcune installazioni, per esempio, nel settore retail o in quello alberghiero, si tendono a dividere i tipi di traffico, distinguendo tra quello “guest” e quello aziendale, per ridurre la penalizzazione delle prestazioni dovute ai controlli di sicurezza: in pratica, il traffico guest viene indirizzato direttamente da e verso Internet, senza applicare controlli. Un approccio non ideale. Né lo è il canalizzare all’esterno il traffico diretto verso Internet, controllando solo il traffico interno alla rete aziendale. Di fatto, la sofisticazione degli attacchi richiede un grado di controllo molto maggiore su tutte le tipologie di traffico.

Con la serie FortiAP-S, tutto il traffico proveniente da qualunque tipo di utente può essere protetto e controllato indipendentemente dalla sua natura. Un’opzione che oltre a essere quella più efficiente ed economicamente vantaggiosa, è anche la più sicura e meno complessa.

Questo è reso possibile grazie alle caratteristiche degli access point FortiAP-S, che includono funzioni di sicurezza avanzate integrate nell’hardware dello stesso AP. Per questo sono dotati di memoria extra e di potenza di elaborazione doppia rispetto a quella del tipico access point semplice, consentendo di effettuare l’elaborazione dei controlli per la sicurezza (dal layer 2 a quello 7 della pila OSI) in tempo reale direttamente alla periferia della rete, non nel cloud o nella LAN aziendale. Questa elaborazione in un singolo passaggio, oltre a essere molto efficiente, permette l’implementazione di policy definite per utente e per dispositivo in modo molto granulare e mantiene visibilità completa sul comportamento a livello di sessione.





La gestione “gratuita” con FortiCloud

Oltre ai vantaggi tecnologici prima evidenziati, la soluzione Fortinet Secure Access Cloud ne fornisce altri significativi legati alla gestione e al provisioning in cloud effettuato da Fortinet attraverso il servizio FortiCloud. Prima di entrare nel dettaglio delle caratteristiche di quest'ultimo e degli access point che lo supportano, è opportuno segnalare anche una peculiarità di tipo economico: non sono previste sottoscrizioni per la gestione legate a ogni access point, a differenza di altre offerte presenti sul mercato. L'unica sottoscrizione richiesta è quella usuale per le funzionalità di sicurezza in tempo reale e cioè relative agli aggiornamenti regolari forniti dai FortiGuard Labs.

Come accennato, FortiCloud è il servizio basato sul cloud per il provisioning, la gestione delle configurazioni e l'analisi delle linee di prodotti FortiGate, FortiWiFi, FortiAP e per la serie FortiAP-S. Consente di inizializzare via cloud l'intera rete wireless, centralizzando visibilità e controllo, evitando i costi relativi al controller WLAN e alla strumentazione di gestione.

Gestito da Fortinet, mette a disposizione delle aziende un dashboard singolo per la gestione d'infrastruttura e sicurezza dell'intera rete e offre scalabilità di rete illimitata con tutti i vantaggi che derivano dalla gestione centralizzata.

Nel firmware degli access point FortiAP-S è compresa la funzionalità di registrazione in FortiCloud, in modo da consentire un provisioning senza interventi manuali: una volta installati, gli access point rilevano la presenza di FortiCloud al quale si connettono, effettuando automaticamente il proprio provisioning. Risulta altresì semplificato il provisioning anche di altri dispositivi Fortinet per la sicurezza, collocati presso sedi remote prive di personale IT competente.

FortiCloud, una volta installato opera come soluzione unificata in grado di gestire gli access point WiFi e il panorama globale di sicurezza presso ogni sede remota: dal rilevamento di AP non autorizzati, alla gestione degli accessi degli utenti guest, fino alla



reportistica sull'utilizzo delle applicazioni e all'analisi delle minacce, fornendo visibilità completa sulla qualità di servizio offerto ai clienti.



Gli access point FortiAP-S

La serie FortiAP-S garantisce accesso wireless sicuro in ambienti interni con una gamma di AP 802.11ac 3x3 MIMO a radio doppia e a radio singola. Alcuni modelli sono dotati di antenne interne, altri di antenne esterne che consentono maggiore flessibilità direzionale e copertura ad ampio raggio per ambienti esterni ed interni. Caratteristiche e funzionalità principali integrate negli access point FortiAS-S sono:

- Provisioning senza interventi manuali.
- Capacità di sopravvivenza alle interruzioni WAN.
- Application Control e scansione antivirus.
- Air Monitor
- Soppressione di AP non autorizzati e WIDS.
- Facilità di assegnazione policy.
- IPS.
- Antimalware.
- Web URL Filtering.
- Application Control.

Il supporto alla sicurezza con FortiCloud



Gli access point FortiAP-S



L'Infrastruttura Secure Access

L'Infrastruttura Secure Access di Fortinet si distingue da altre implementazioni di reti wireless per il modo in cui vengono gestiti i canali di frequenza. Un approccio esclusivo che semplifica la distribuzione degli access point e aumenta la scalabilità. Più precisamente, la gestione innovativa dello spettro consente di “superare” gli ostacoli che generano le interferenze tipiche dei luoghi con grandi dimensioni, come centri congressi, stadi, magazzini e campus ospedalieri o universitari. L'infrastruttura risulta così ideale per la realizzazione di reti largamente distribuite e per grandi aziende alle prese con il proliferare dei dispositivi utilizzati da ciascun dipendente.

Peraltro anche realtà più piccole, come le scuole, dalla materna alle superiori, che hanno spesso carenza di personale e che possono così distribuire una rete wireless scalabile e sicura con costi contenuti.

La soluzione mette a disposizione un set completo di servizi per la sicurezza, che possono aggiungersi all'eventuale di information security esistente. Più precisamente, Fortinet Infrastructure Secure Access comprende componenti switch, WLAN (precedentemente Meru Networks) e le soluzioni di sicurezza integrate nell'appliance. FortiGate, comprendenti anche funzionalità di Application Control granulare.

La componente wireless consiste in una rete WiFi on-premise a elevate prestazioni realizzabile con un'ampia gamma di access point in grado di supportare l'esclusiva architettura Virtual Cell di Fortinet.

Con Virtual Cell basta interferenze

Come accennato, grazie all'innovativa gestione dello spettro non è più necessario preoccuparsi delle interferenze tra diversi canali. Questo porta notevoli vantaggi e risparmi, perché, per esempio, non occorre gestire le pianificazioni dei canali oppure perché elimina il bisogno di sopralluoghi per l'installazione di nuovi access



point o per effettuare modifiche e neanche per estendere l'infrastruttura: se si vuole aumentare copertura e capacità in un'area specifica, basta aggiungere fisicamente gli access point dove necessario. Non ci sono interferenze, non serve regolare potenza e canale. Non bisogna, in buona sostanza, ridefinire la rete.

Questo è possibile perché la tecnologia Virtual Cell consente alle radio degli access point di operare su un singolo canale, presentandosi ai client come una radio sola, ovunque si trovino, e realizzando un unico livello di copertura esteso a tutta la struttura.

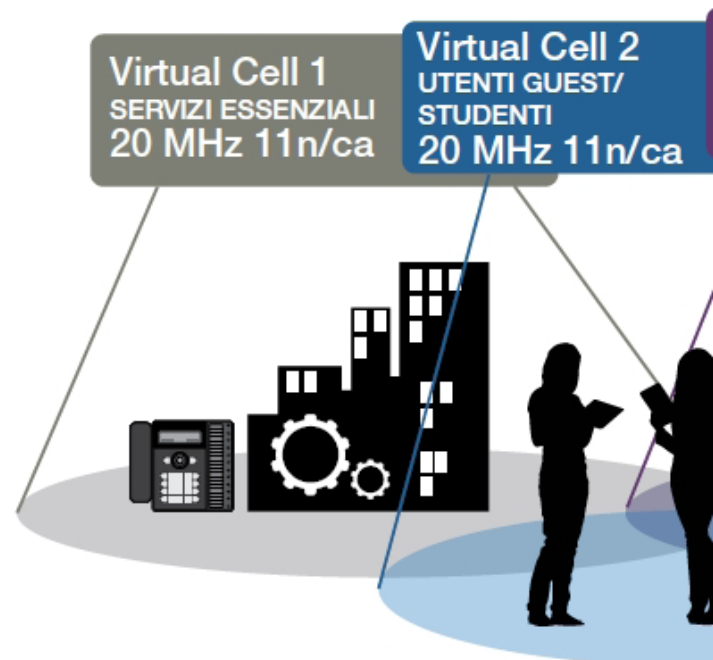
Qualora si voglia aumentare la capacità in maniera significativa è possibile configurare più Virtual Cell, assegnando a ognuna un diverso canale. È possibile sia estendere tale sistema a tutta la struttura sia limitarlo a una zona contenuta, dove occorre supportare un volume maggiore di connessioni.

Il modello di crescita non mette a rischio stabilità e prestazioni, perché l'aggiunta di nuove celle virtuali accanto a quelle già installate non richiede modifiche su queste ultime.

Inoltre, questo sistema risulta comodo per isolare il traffico, per esempio per separare quello degli interni da quello degli ospiti, oppure per garantire maggiore capacità a specifici gruppi di utenti o applicazioni (Voip, videoconferencing, gestionali). Ancora, il sistema permette di isolare e supportare meglio strumentazioni particolari in ambiti come, per esempio, gli ospedali (dove monitor cardiaci, sistemi di tracciamento della posizione o altre funzioni cliniche richiedono attenzioni particolari) o il retail (POS mobili, lettori di bar code o altro).

L'architettura di Virtual Cell presenta un ulteriore elemento d'efficienza, consistente nel roaming

La gestione gruppi con le Virtual Cell



controllato dalla rete, il quale aumenta considerevolmente la qualità e l'affidabilità dei servizi in tempo reale.

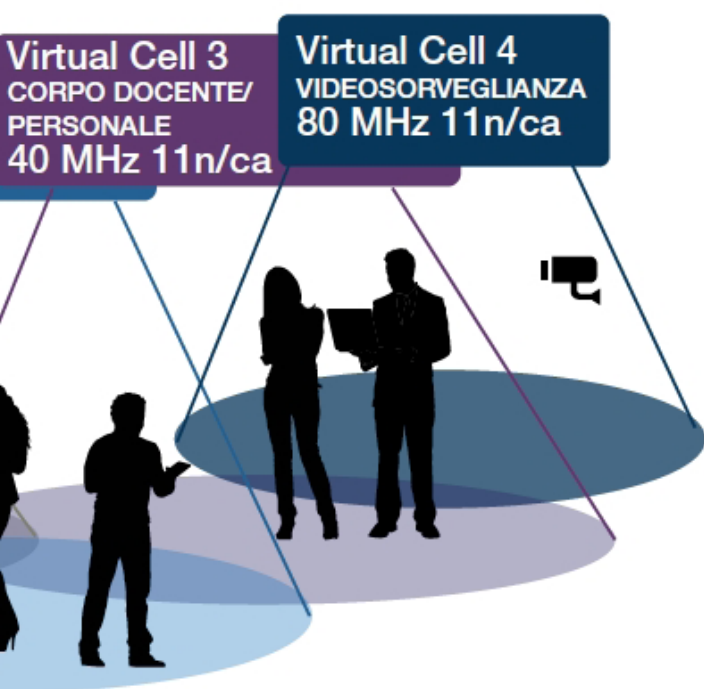
Nelle reti tradizionali, appena il segnale si attenua i client interrogano gli access point, per essere pronti a "spostarsi" su quello disponibile per effettuare il roaming, impegnando di continuo la banda. Con la tecnologia di Fortinet, il roaming è gestito dalla rete, che, oltre alla potenza del segnale è in grado di valutare anche il carico sostenuto da ciascun access point. In pratica, viene emulata la modalità di roaming delle reti cellulari, garantendo il miglior supporto possibile, anche perché il tempo per il roaming risulta di 3 ms invece degli oltre 100 ms usuali). Il sistema consente, inoltre, di gestire al meglio il balancing del traffico sugli AP.

Tale impostazione riduce anche il traffico generato inutilmente dai client fissi, che sfruttano la rete wireless, ma non hanno bisogno di prepararsi ad alcun roaming. Interrogazioni e trasmissioni di servizio vengono ridotte al minimo indispensabile.

Oltre ad aumentare l'affidabilità delle connessioni, l'architettura della Secure Access Infrastructure di Fortinet fornisce diverse opzioni per aumentare la disponibilità. Per esempio la ridondanza

active/ active o active/stand-by a livello di collegamento consente la connessione dei controller a due o più switch di rete tramite porte GbE o 10GbE, a seconda del controller selezionato.

La ridondanza dei controller N+1 consente il backup di cluster fino a cinque controller attivi su un controller in stand-by. Le modifiche alla configurazione dei controller sono sincronizzate tra controller master e slave, garantendo così che, in caso di emergenza, il controller in stand-by contenga sempre una configurazione valida e sicura.





La sicurezza con Fortinet Connect e FortiGate

Fortinet Connect è la soluzione che consente ai dipartimenti IT di effettuare facilmente la segmentazione di utenti o dispositivi client in base al ruolo, attraverso una gestione granulare delle policy in base a tipo di dispositivo, utente, orari e altri criteri. Utilizzando SSID separati con opzioni specifiche di autenticazione è possibile creare profili di accesso separati per individui e gruppi all'interno di un'organizzazione (per esempio corpo docente, studenti e visitatori in una scuola o personale medico, paramedico, amministratori e responsabili delle strutture ospedaliere).

Inoltre, la soluzione supporta più tipi di captive portal per dipendenti e utenti guest, abilitando il provisioning self service per gli ospiti e l'apertura al BYOD, anche grazie a un'ampia vasta gamma di opzioni per l'autenticazione, come social login, autenticazione 802.1x e a due fattori. È poi compatibile con RADIUS, Active Directory, LDAP e altre directory.

Disponibile una API che abilita l'integrazione con piattaforme di provisioning di terze parti: per esempio il registro clienti di un albergo o quello degli studenti in un'università.

La sicurezza in Secure Access Infrastructure è garantita da Cooperative Security Fabric e dalla nota piattaforma FortiGate.

FortiGate riunisce le funzionalità di sicurezza singoli, che in altre soluzioni sono supportati da sette dispositivi diversi: firewall, gateway VPN, IPS di rete, DLP, antimalware, Web Filtering e Application Control.

Senza entrare in ulteriori dettagli, è bene osservare che a ciascuna delle suddette funzionalità corrispondono diverse tecnologie per la protezione dei dati e dei sistemi informatici, il cui motore è rappresentato da FortiOS e dai processori sviluppati da Fortinet per le appliance Fortigate, che garantiscono la qualità dei controlli e le prestazioni necessarie al loro svolgimento e al corretto funzionamento della rete.



L'Infrastruttura Secure Access Integrata

Per diverse proprie ragioni, in molte grandi aziende, in particolare quelle distribuite, si è piuttosto restii ad abbandonare la tradizionale architettura di rete wireless basata sui controller. La preoccupazione maggiormente condivisa riguarda l'infrastruttura di sicurezza o, meglio, la possibilità di utilizzare l'infrastruttura di sicurezza aziendale, composta da firewall, IPS di rete, scansione antivirus, Web Filtering, Application Control e via dicendo, anche per il traffico WLAN.

Per questo Fortinet ha sviluppato la soluzione Integrated Secure Access, affinché sia in grado risolvere tutte le problematiche di accesso e cyber security, inserendo la sicurezza di rete all'interno della stessa piattaforma di controllo WLAN e semplificando la gestione di protezione e accessi.

Per questo l'architettura proposta da Fortinet non richiede numerose appliance di terze parti, ma realizza una piattaforma di sicurezza a 360 gradi e di gestione delle WLAN grazie alla combinazione dell'appliance FortiGate e degli access point FortiAP. Un approccio che consente di sottoporre il traffico WLAN a diversi controlli di sicurezza in un singolo passaggio, eliminando il bisogno di effettuare una mappatura della WLAN su varie appliance e riducendo al minimo la latenza dovuta alle analisi di security.

Una sicurezza a tutto tondo

FortiGate opera sia da controller WiFi sia da piattaforma per la network security e, come tale, unisce le funzionalità tipicamente fornite da sette o più dispositivi singoli, tra cui firewall, gateway VPN, IPS di rete, DLP, software antimalware, Web Filtering e Application Control. Il tutto assicurando prestazioni elevate.

Questo "sforzo" è reso oggi necessario dalla crescita ed evoluzione delle minacce, che impongono non solo il controllo degli accessi (funzione base per una WLAN), ma anche scansione mal-





ware, l'integrità degli endpoint e altri tipi di prevenzioni. I cyber attacchi, infatti, riescono a penetrare nella rete attraverso applicazioni comuni, come la mail o un sito Web. Sono sempre più diffusi, per esempio i siti di phishing: siti falsi/mascherati sui quali è relativamente facile finire dopo aver ricevuto una mail che non suscita sospetti, soprattutto a un utente distratto. Il BYOD peggiora le cose, considerando l'eccessiva confidenza delle persone con i propri dispositivi mobili. Altra fonte di accessi potenzialmente pericolosi è l'IoT, le cui applicazioni potrebbero generare grandi moli di traffico.

Le complesse infrastrutture tradizionali di sicurezza, magari basate sul best of breed, cioè un insieme eterogenee di ottime singole soluzioni dedicate ciascuna a specifici controlli, richiedono un instradamento del traffico WLAN attraverso diverse appliance, con un'architettura che è complicato orchestrare.

L'infrastruttura di sicurezza integrata di Fortigate elimina questa complessità e, grazie ai processori proprietari FortiASIC è in grado di supportare tutti i controlli necessari con le prestazioni adeguate, risultando in grado, come certificano laboratori indipendenti e organizzazioni come Gartner, di rilevare contenuti dannosi a velocità multigigabit.

A questo si aggiungono le molteplici funzioni di controllo granulare realizzate dal sistema operativo per la sicurezza FortiOS.

La piattaforma mette a disposizione, inoltre, una serie di tecnologie che forniscono strumenti per configurare efficacemente supporto al BYOD, accesso degli utenti guest, accesso per ruolo e identità, autenticazione e crittografia.





Access point FortiAP

Come spiegato, il traffico WLAN viene sottoposto ai controlli di sicurezza in un unico passaggio, questo è reso possibile dalla configurazione predefinita dei controller che gestiscono gli access point FortiAP, la quale prevede che gli SSID instradino tutto il traffico sul controller wireless FortiGate all'interno di tunnel CAPWAP DTLS o non DTLS, per l'applicazione delle misure di sicurezza, prima di poter passare in Internet o nella LAN aziendale.

Si ottiene così un importante vantaggio in termini di prestazioni, granularità delle policy e visibilità sul comportamento di utenti e dispositivi.

La gamma FortiAP di access point gestiti da controller assicura prestazioni elevate in ambienti interni e accesso wireless all'esterno con un'ampia gamma di AP, che va da 802.11n a radio singola fino a 802.11ac MIMO 3x3 a radio doppia, compresi i modelli a rating massimo.

Il design dei modelli per interni, che ricorda i rilevatori di fumo, consente un posizionamento discreto in aree nelle quali l'estetica è importante, mentre i modelli irrobustiti per esterni sono l'ideale per le condizioni più estreme.

Il provisioning automatico delle risorse radio e le funzionalità di distribuzione senza intervento manuale consentono una rapida implementazione dei FortiAP anche negli uffici remoti e in assenza di FortiGate on-premise. Tutte le funzionalità richieste dalle imprese, quali roaming veloce, supporto maglie e ponti, air monitor, accesso degli utenti guest, rilevamento degli AP non autorizzati, WMM e QoS, sono supportate come standard, senza l'esigenza di acquistare ulteriori licenze specifiche.



Reportec

2016

