Wi-Fi ENTERPRISE

LA QUARTA GENERAZIONE

ALFACOD®

FORTINET

MERU®

Nel 2015 Fortinet, leader nel mondo della Cybersecurity e già impegnata nelle soluzioni di Networking Wi-Fi, decide di acquisire Meru Networks, per dare una risposta più completa al grande tema della Cybersecurity e un'offerta di Networking di altissimo livello.

Chi è Meru Networks

Meru Networks è un'azienda americana, nata nel 2002 a Stanford in California, da un gruppo di imprenditori indiani trasferitisi negli Stati Uniti per studiare. I fondatori di Meru Networks, convinti delle loro innovative e brillanti idee sullo sviluppo della tecnologia Wi-Fi, decisero appunto nel 2002 di fondare l'azienda che è stata in seguito quotata in borsa, al Nasdaq.

Primo obiettivo di Meru Networks era quello di ovviare ai problemi tipici del Wi-Fi. Gli ingegneri di Meru avevano visto che il Wi-Fi, così com'era all'epoca, 11 megabit, 802.11b, aveva dei difetti intrinseci che si sarebbero manifestati sicuramente, e aggravati, con l'aumentare del numero di device, di access point e di applicazioni. Hanno quindi cercato di immaginare che cosa sarebbe successo nell'arco dei successivi 10 anni nel mondo della tecnologia Wi-Fi. Hanno pensato ad un prodotto che ovviasse ai problemi esistenti, rimanendo però fedeli allo standard del Wi-Fi 802.11. L'obiettivo era quello di comportarsi in maniera diversa rispetto a tutti gli altri attori del mercato Wi-Fi di quel periodo, pur rimanendo negli standard.

I punti di forza delle soluzioni Fortinet-Meru si apprezzano quando si usa qualcosa in più della semplice connettività, come la voce, i video o certe applicazioni dati che non possono sopportare neppure micro interruzioni, pena la disconnessione dal server. Fortinet-Meru si rivela straordinaria soprattutto quando si connettono in uno stesso luogo un numero elevato di dispositivi Wi-Fi.

Fortinet-Meru è sempre stata riconosciuta, a livello mondiale, come "visionario tecnologico".

Wi-Fi di 4a generazione

Gartner Group, importantissimo centro studi internazionale, ha classificato il mondo del Wi-Fi in generazioni: Fortinet-Meru è collocata nella generazione più avanzata di tutte. Sempre secondo Gartner, il Wi-Fi di 3a generazione è quello utilizzato dai principali attori di mercato; quello di Fortinet-Meru invece è classificato, già dal 2010, Wi-Fi di 4a generazione. Nelle pagine successive ne esaminiamo i motivi.

Quali sono i problemi tipici del Wi-Fi non appena si abbandona il classico scenario di un access point e un client? Cosa non funziona?

In futuro sempre più dispositivi Wi-Fi dovranno integrarsi alle reti. Già dal 2011 abbiamo assistito ad un'importante svolta nel mondo della connettività: sempre meno connessioni cablate, sempre più connessioni radio. Stiamo assistendo ad un cambiamento epocale. Molta strumentazione informatica non è più dotata di porta Ethernet (oltre il 70% - fonte Gartner); quindi non può più essere connessa via cavo con il server in cui si trovano le varie applicazioni e deve, invece, essere collegata via radio. Un'ondata massiccia di connessioni con nuovi dispositivi sta invadendo le reti Wi-Fi.

Il fenomeno iOS e Android sta dando una forte spinta al bisogno di approfondimento e di utilizzo di reti Wi-Fi di quarta generazione.

Il manager che lo utilizza cerca di rendere più profittevoli le attività che svolge all'interno della rete aziendale. Questo "end point" ha bisogno della connettività e la connettività può essere soltanto wireless. In questo caso è proprio la necessità dei manager a chiedere all'ICT ampia connettività.

Wi-Fi tradizionale: onde, disturbo e comunicazione non lineare

Il problema principale che Meru individuò nel Wi-Fi tradizionale, è che tutte le onde radio generate dagli Access Point e dai client, se concentrate in uno specifico ambiente, come un magazzino, un negozio o un ufficio, non sono assolutamente coordinate tra loro. Questo può essere rappresentato allegoricamente dall'immagine di una superficie d'acqua in cui le onde concentriche, prodotte dalle gocce, si scontrano tra loro, sovrapponendosi.

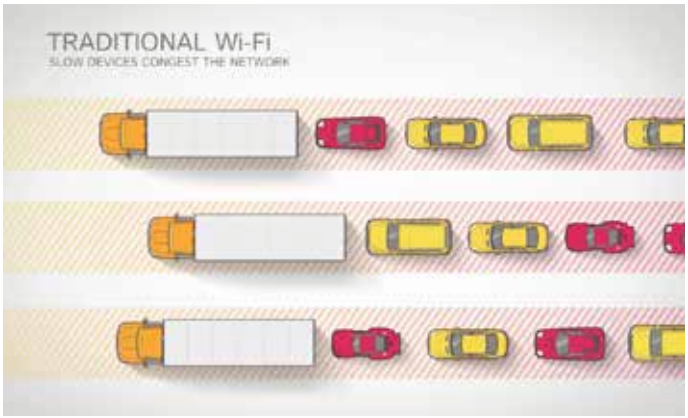
Ciò significa disturbarsi, creare interferenza, distruggersi, perché non esiste coordinamento tra tutte queste trasmissioni. Se, ad esempio, si posiziona un primo access point in un punto e un altro a 50m di distanza, con client che gravitano loro intorno, ognuno di essi trasmette in maniera totalmente indipendente. Essi creano disturbi, interferenze e una condizione di instabilità. In alcuni momenti possono non verificarsi collisioni e in questi casi la comunicazione funziona benissimo, in altri momenti invece no. In presenza di collisioni, assistiamo ad un temporaneo peggioramento della prestazione. Finché si tratta di scaricare un'email o di vedere una pagina web ci si può accontentare, ma quando si devono fornire servizi, con garanzia di buon funzionamento, tutto ciò rappresenta un grandissimo problema.

Il problema di interferenza sul canale tra access point e client, è simile a ciò che succede in una stanza in cui tutti urlano e nessuno capisce con chiarezza. Questa è una tipica difficoltà riscontrata sulle reti Wi-Fi ordinarie; l'altra grossa problematica è rappresentata dal passaggio da una cella ad un'altra: il cosiddetto roaming. Nel Wi-Fi tradizionale il roaming è sempre un evento traumatico; alcuni client sono più adatti a compiere questa operazione, altri meno. A volte il roaming richiede svariati secondi. In un ambiente affollato in cui è necessario servire tanti utenti, tipicamente vengono create svariate celle (tanti AP); il che significa tantissime operazioni di roaming a mano a mano che i client si spostano; è questo il momento in cui si perdono più facilmente le connessioni. E' inutile aggiungere che questa tipologia di reti è difficilmente espandibile nel tempo.

Il Wi-Fi tradizionale ha un comportamento non lineare e non brillante al crescere del numero degli utenti. Con un access point e un'unica cella radio su cui si collegano 3 o 4 utenti, le cose sono semplici da gestire e tutto procede facilmente. Lo scarso numero di dispositivi trova facile connettività e traffico libero. Già si notano cambiamenti caricando sulla stessa cella 10 o 20 client; le prestazioni totali dell'access point decrescono immediatamente. Ogni client "ruba", per così dire, agli altri una porzione di accesso, perchè aumen-

tando i client ci sono maggiori collisioni da gestire.

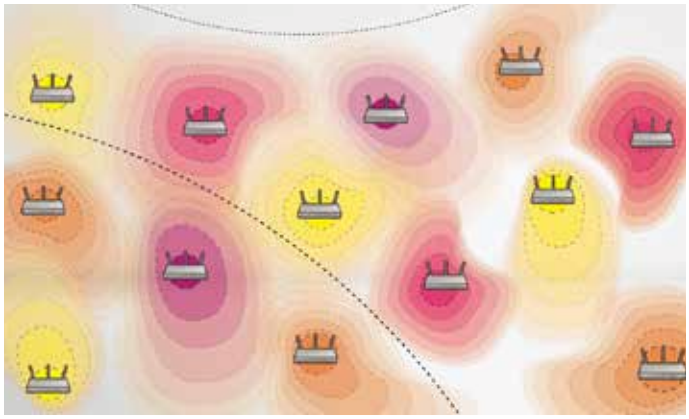
Il Wi-Fi "tradizionale", pensato agli inizi degli anni 2000, nello standard 802.11 è strutturato esattamente come un hub. Chi ha dimestichezza con le vecchie reti ethernet ricorderà la cosa. Prima dell'avvento dello switch si usavano gli hub per connettere le workstation al nodo di rete e si verificava il problema appena descritto. I PC creavano una grande quantità di collisioni e al crescere degli utenti peggioravano drasticamente le performance del sistema. Questo concetto può essere raffigurato da un incrocio, che permette un passaggio sciolto di vetture quando il traffico è basso, ma congestionandosi il traffico, si può arrivare fino alla paralisi.



Panoramica storica del Wi-Fi

Il Wi-Fi è nato negli anni '90, senza uno standard, spinto da operatori importanti quali Proxi, Lucent, Aironet e Symbol, tecnologie radio di proprietà in sistemi radio proprietari. Questo scenario si è evoluto nel tempo, con l'obiettivo di poter connettere alle reti dispositivi di terze parti. Coloro che hanno però scritto lo standard 802.11 non avevano minimamente la visione dell'impressionante sviluppo che il mobile computing avrebbe avuto: hanno quindi creato le specifiche in funzione di traffici scarsi. Alcune aziende come Cisco e HP decisero di portare comunque il Wi-Fi in un ambito più professionale, anche se inizialmente era nato per un mercato consumer. Finché si installavano pochi access point, tutto andava bene, ma con l'aumentare del numero di client che dovevano essere serviti, si è cercato di trovare una soluzione per coordinare meglio le nuove reti, già di cospicue dimensioni. La soluzione, che è identificata appunto come Wi-Fi di 3ª generazione, ha preso il nome di "centralizzazione": alle celle radio viene aggiunta una controller per fare il management centralizzato delle configurazioni e inviare alcuni suggerimenti agli access point, in modo da attenuare i loro conflitti. Di che suggerimenti parliamo? Prima di tutto di evitare che tutti gli access point stiano sullo stesso canale.

Nel Wi-Fi tradizionale esiste una regola fondamentale: non mettere mai 2 access point vicini sullo stesso canale, altrimenti si disturbano. Nel Wi-Fi di seconda generazione, con access point privi di controller, le configurazioni di ciascuno di essi, venivano fatte manualmente, impostando i canali 1, 6 e 11. I 3 canali, che su 2,4 GHz si possono usare senza sovrapposizioni e senza disturbo reciproco, purtroppo sono soltanto 3. Ecco uno dei grandi problemi. Quindi solo 3 canali sui quali sincronizzare tutti gli access point, ma ricordando che access point sincronizzati sullo stesso canale non devono sovrapporre il segnale, altrimenti nasce un conflitto, una interferenza. É facile intuire che in presenza di tanti access point il lavoro di configurazione deve essere meticoloso e se mutano le condizioni ambientali, la configurazione deve essere rifatta.



Grazie alla controller centralizzata di terza e quarta generazione, invece il tutto avviene in maniera automatica. Quindi, la prima cosa che fanno i sistemi di 3ª generazione, è distribuire i canali su frequenze diverse. La seconda cosa che fanno è la riduzione della potenza delle celle radio in caso di disturbo, in modo tale da allontanare virtual-

mente gli access point. Questa è la soluzione che i competitor di Fortinet-Meru hanno pensato di adottare quando nello stesso ambiente gli access point fanno fatica a lavorare in modo coordinato. Malgrado questo stratagemma, le prestazioni wireless sono ancora spesso imprevedibili: la qualità della voce, per esempio, è piuttosto povera e quando avviene un passaggio di cella il rischio di perdita di dati è ancora molto alto.

Fortinet-Meru ha ritenuto che questa non fosse la strada giusta ed ha attuato un approccio completamente diverso.

Fortinet-Meru ritiene infatti che il vero problema stia proprio nella mancanza di coordinamento tra tutti gli attori che operano all'interno dell'infrastruttura radio. Fortinet-Meru sostiene che, anziché selezionare canali diversi e ridurre le potenze, si possa agire in un altro modo: si sincronizzano tra loro tutte le trasmissioni in modo che avvengano in istanti diversi e che quindi non ci sia mai una trasmissione contemporanea ad un'altra, che possa creare collisione. Analizzando una rete Fortinet-Meru si noterà una sola onda alla volta, e non varie nello stesso istante che possono provocare cancellazioni e disturbi. Gli access point Fortinet-Meru sono tra loro coordinati e non andranno mai a infastidirsi l'uno con l'altro. Inoltre gli access point Fortinet-Meru, utilizzando parametri propri dello standard 802.11, sono in grado di comunicare ai client il momento in cui ciascuno di essi può trasmettere, un po' come se dicessero ad un client: "tu puoi parlare da quest'istante a quest'istante, dopo fai silenzio", e ad un'altro: "tu puoi parlare da questo istante a quest'altro istante" e così a tutti i client che si trovano nel medesimo ambiente. Grazie alle reti Fortinet-Meru e alla sua tecnologia, centinaia o migliaia di client riusciranno a parlare uno per volta senza darsi fastidio.

Con questa soluzione si potrebbe pensare ad un rallentamento delle prestazioni, perché mentre nelle altre reti tutti parlano contemporaneamente, nella rete Fortinet-Meru si parla uno alla volta. Non è così. In realtà il numero di megabit per secondo che si possono gestire in una rete sincronizzata come quella Fortinet-Meru, è uguale a quello di una rete non sincronizzata. Grazie a questa sincronizzazione ci sono invece molti benefici aggiunti, che mostreremo.

Gartner ritiene che Fortinet-Meru sia il leader della nuova generazione di Wi-Fi. La quarta.

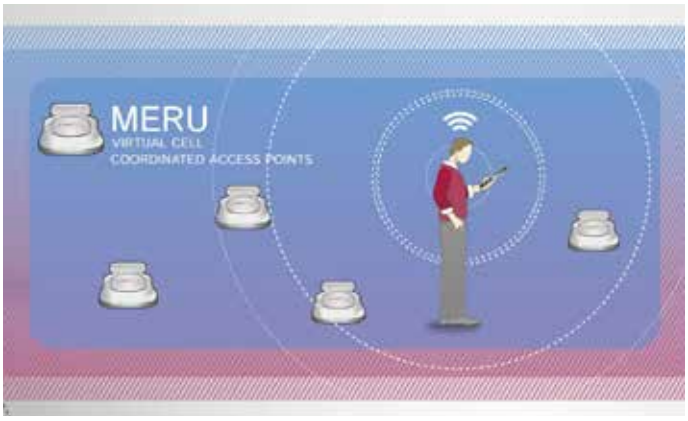
Questa nuova generazione si contraddistingue principalmente per 3 elementi caratteristici:

Primo elemento: Single Channel (canale unico). Fortinet-Meru può configurare tutti i propri access point sul medesimo canale. In tal modo facilita molto la vita dei client, che essendo sincronizzati non si disturbano. Gli access point, anche vicini, non parlano tra loro; in realtà è la controller a monte che impartisce gli ordini, evitando che i client si disturbino. Per fare un esempio, ipotizziamo una rete di 50 access point Fortinet-Meru. Anche gli access point vicini tra loro, che trasmettono sullo stesso canale, non si disturberanno reciprocamente, poiché è compito della controller gestire il traffico degli access point che costituiscono l'infrastruttura.

Secondo elemento: Air Time Fairness ("Fairness" = equità, "Air Time": è il tempo a disposizione sull'interfaccia radio). Fortinet-Meru offre a tutti i client la stessa quantità di tempo di trasmissione. Nel Wi-Fi tradizionale di 3a generazione non è così. Nel Wi-Fi tradizionale c'è una gara, una piccola contesa tra i client per cercare di avere accesso al mezzo. A Fortinet-Meru non piace questo sistema. Utilizzando sempre il protocollo dello standard 802.11, dà in sostanza la stessa quantità di tempo a tutti i device. Quindi ci saranno dei client che hanno la capacità di andare molto veloci e in quell'intervallo di tempo trasmetteranno una quantità elevata di dati e dei

client che andranno più lentamente e nello stesso periodo di tempo trasmetteranno meno dati, ma senza prevaricazioni.

Terzo elemento: Virtual Port. Ogni client che si connette a una rete Fotinet-Meru, ha a disposizione un access point (AP) virtuale a lui dedicato, che viene generato da qualsiasi AP fisico in cui il client passerà. Ogni volta che gli AP fisici ricevono una richiesta di associazione di un client, producono un access point virtuale.



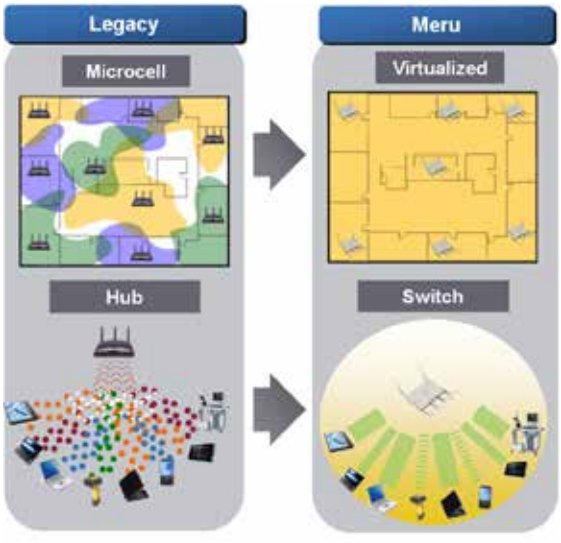
Facendo così, si riporta la situazione alle condizioni di quando fu scritto lo standard in cui si prevedeva un access point per un solo client. La condizione è ideale perché quel client non deve gareggiare per guadagnarsi il canale; lui si ritiene l'unico associato in quel momento a quell'access point. Con questo "trucco" si inganna il client, dando allo stesso la possibilità di trasmettere quando ne ha voglia. Sarà quindi la controller a sincronizzare tra loro tutti i Virtual Access.

WLAN Virtualizzata

Gli access point di una rete Fortinet-Meru lavorano tutti su un unico canale, permettendo in tal modo una facile pianificazione della stessa (immagine sotto). In una situazione tradizionale si dovrebbero assegnare i canali 1, 6 e 11. Con Fortinet-Meru è tutto molto più facile: si decide, per esempio, che il canale 6 è il più pulito e sgombro, dopo aver fatto la dovuta indagine preliminare?

Allora si metteranno quindi tutti gli access point sul medesimo canale e qualora ci accorgessimo, a posteriori, che è presente un buco di copertura per Fortinet-Meru sarebbe semplice rimediare. Sarebbe sufficiente aggiungere un altro access point e metterlo sullo stesso canale. Nel caso di un Wi-Fi tradizionale di 3a generazione, quando si attiva un access point aggiuntivo si deve prestare grande attenzione al canale che gli viene assegnato, perché potrebbe andare a disturbare tutti gli altri che gli stanno attorno.

Facilità di design e quindi di installazione, eliminando molti problemi.



Un'altra caratteristica interessante è il mantenimento di potenza. Dal momento che gli access point Fortinet-Meru non vengono ridotti in potenza, trasmettono sempre al 100% delle loro possibilità, contrariamente a quello che accade con reti di 3a generazione, con controllo sull'algoritmo di gestione della potenza automatizzata, in cui spesso, lo stesso algoritmo costringe gli access point a ridurre al 50% la potenza, per non creare disturbi. Ciò si traduce in un raggio di copertura più ridotto. In un caso del genere, allora, per coprire la medesima area, con Fortinet-Meru si possono risparmiare fino al 30% di access point rispetto ad una soluzione tradizionale.

Altro effetto molto importante, conseguente alla generazione di una Virtual Port per ogni client, ovvero un access point personalizzato, è che il client non si accorge che sta facendo roaming, cioè un passaggio di cella. La controller Fortinet-Meru, nel momento in cui si accorge che un tablet in Wi-Fi o un terminale portatile si sta spostando, quindi il proprio segnale sta lasciando il primo access point e si sta muovendo sul successivo, sposta la virtual port da un access point all'altro in maniera automatica. Il device che prima riceveva le risposte dal primo access point ad un certo punto, su decisione presa dalla controller, riceverà le risposte dall'altro access point.

Il client non si accorge assolutamente di nulla, credendo di essere ancora attaccato all'access point originario, ma cambiando fisicamente cella. Di conseguenza il client in questione non inizierà mai un processo di roaming; si sposterà e crederà di essere attaccato ad un unico gigantesco access point in qualsiasi zona della rete.

E sulla telefonia VoIP questo si nota ancora di più. Anche i telefoni migliori impiegano 100 millisecondi per fare roaming. Si può pensare che 100 millisecondi non siano un tempo elevato, ma chi conosce il funzionamento del Voice Over IP (VOIP) sa che i pacchetti di voce vengono mandati ogni 20 millisecondi. Quindi se ho un buco di 100 millisecondi, perdo 3-4-5 pacchetti di voce. Se addirittura, il tempo, invece di 100 millisecondi, fosse ancora maggiore, si rischierebbe la caduta della connessione. Sapete invece quanto impiega Fortinet-Meru ad effettuare lo spostamento di un client VOIP, che non è costretto a fare la scansione dei canali e una nuova autenticazione, da una cella fisica ad un'altra? Impiega in totale dai 3 ai 5 millisecondi.

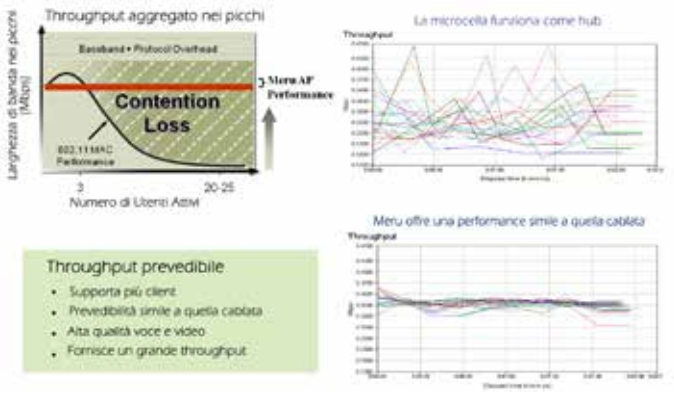
Semplicemente, il client vede che il segnale scende leggermente e poi risale immediatamente, ma si vede sempre associato allo stesso access point. Questo vale anche per i client peggiori, che potrebbero impiegare fino a 4 secondi per fare il passaggio di cella; perché il client non farà mai un vero roaming, ma sarà la controller Fortinet-Meru a spostare il suo access point virtualizzato su tutti gli access point fisici all'interno dell'area. L'altra cosa importante delle reti Fortinet-Meru a singolo canale è rappresentata dal fatto che permette una crescita di capacità, cioè di utenti che si possono associare, e di Mb/sec, maggiore di qualsiasi altra soluzione. Facciamo l'esempio di una sala convegni o di un'aula universitaria, in cui potremmo avere facilmente 200-300 persone e dove, magari, ognuna di queste potrebbe avere più di 1 dispositivo Wi-Fi (PC, smartphone, iPad, ecc.). In una situazione normale dovremmo riempire la sala di tante micro celle, tanti access point, ognuno su un canale diverso (fermo restando che i canali disponibili sono tre: 1, 6 e 11) e ognuno che cerca di prendersi qualche client. Però è pericoloso inserire tanti access point in uno spazio fisicamente ristretto: c'è un limite. Più ne inserisco e più disturbo. In pratica esiste una specie di tetto, approssimativamente di 200 client, che non è possibile superare. Anche i migliori competitor di Fortinet-Meru, quando si trovano a gestire una situazione di alta densità, pur mettendo tantissimi access point nella stanza, non gestiscono più di 200 client.

Channel Layering

Come si comporta una rete Fortinet-Meru?

Fortinet-Meru ha la possibilità di servire i primi 200 client sul canale 1, altri 200 sul canale 6 e altri 200 sul canale 11. Questi 3 "strati" non si disturbano tra loro perché sono su 3 canali diversi, come insegna la regola del Wi-Fi. Si fa quindi il cosiddetto channel layering. Si possono quindi agevolmente triplicare le capacità di rete. In un Wi-Fi tradizionale, all'aumentare del numero degli access point, non si aumenta proporzionalmente la capacità, ma in realtà si ha un abbattimento delle performance anche del 20-30% sulla maggior parte degli access point. Fondamentalmente, l'aggiunta di access point causerà la perdita di prestazioni di quelli già presenti.

Nei grafici dello schema sottostante, vengono riportati i risultati a confronto di test reali fatti su access point tradizionali e access point Fortinet-Meru. In questo test si vedono 20 client associati ad un access point. Quello che si nota con grande evidenza, nel grafico relativo ad una rete tradizionale, è l'andamento difforme di ogni client: in certi momenti buone prestazioni, in altri momenti pessime. Alcuni client, addirittura, hanno sempre basse prestazioni perché non riescono mai a vincere la contesa di banda con gli altri. Se si fa una media della velocità di questo insieme di traffico considerando le varie prestazioni, risulta bassa, intorno ai 2 Mb.



La controller di Fortinet-Meru, invece, avendo il controllo della situazione, ordinerà a tutti i client il momento esatto in cui possono trasmettere e quello in cui non farlo. Tutti quanti avranno un trattamento equo. Come si vede espresso dal grafico, tutte le prestazioni si assomigliano; la media è più alta, mancando collisioni, non ci sono momenti d'inefficienza; lo stesso singolo access point può distribuire al meglio il traffico.

Fortinet-Meru ritiene inoltre di dare il meglio in situazioni mission critical. Che cosa vuol dire?

Quando le applicazioni non sono di semplice connettività dati, ma sono composte da video, voce e altro, e quando il numero di device che si connette alla rete diventa quantitativamente importante, Fortinet-Meru ritiene di avere dei plus insiti nella propria tecnologia.

La tecnologia Fortinet-Meru è brevettata e per questo motivo è unica.

Per i competitor è difficile seguire Fortinet-Meru sulla stessa strada. È ovvio che in presenza di un uso leggero del Wi-Fi, come succedeva fino a pochi anni fa, forse Fortinet-Meru non avrebbe fatto la differenza. Fino a qualche tempo fa, in effetti, il numero degli utilizzatori era talmente esiguo che, anche in presenza di reti mal costruite, le pecche non sarebbero emerse più di tanto. Ora è diverso. Sempre più utenti usano il Wi-Fi e per operazioni sempre più importanti. Hanno un tablet in mano e si chiedono come mai nella propria azienda il Wi-Fi funzioni così male. Oggi sono i "decision maker" che vogliono che il Wi-Fi funzioni. Secondo Fortinet-Meru, il Wi-Fi deve garantire la stessa affidabilità delle reti cablate. Gli EDP manager di tutte le grandi realtà sono o saranno misurati anche sul buon funzionamento del Wi-Fi e sulle prestazioni costanti nel tempo.

Con Fortinet-Meru esiste quindi la possibilità di garantire finalmente tutto questo con sicurezza, affidabilità e alte prestazioni per qualsiasi tipo di applicazione dedicata a: retail, logistica, manufacturing, fiere, stadi, scuole, hotel, ospedali e grandi spazi commerciali. L'uso massiccio di tablet e smartphone sta accelerando l'utilizzo delle reti Wi-Fi. Sempre di più, i dipendenti e i collaboratori di una azienda vogliono utilizzare i propri device Wi-Fi nelle reti aziendali. Una tendenza ormai frequente negli Stati Uniti e in pieno sviluppo anche da noi. Questo provoca di solito grandi mal di pancia agli EDP Manager, perché non

essendo dispositivi acquistati dall'azienda, non sono configurati secondo le politiche di sicurezza aziendali e metterli in rete potrebbe significare un rischio o comunque un disturbo.

Il BYOD è un fenomeno in forte crescita, motivato anche dal fatto che il device personale è molto spesso più moderno e meglio equipaggiato di quello assegnato aziendalmente.La richiesta di poter connettere smartphone o tablet personali all'interno delle imprese, è una domanda che arriva soprattutto da manager, dirigenti, consulenti e che non può essere ignorata dai gestori delle reti aziendali. E' un fenomeno ormai inarrestabile, come segnala anche uno studio di Ernst & Young. Gli operatori del mondo Wi-Fi hanno coniato quest'acronimo BYOD: Bring Your Own Device, ovvero "porta con te il tuo device". Dove? In azienda, in trasferta, a casa. Succederà sempre più spesso; è una cosa di cui sentiremo parlare sempre di più, anche nei messaggi pubblicitari e di marketing.

Cybersecurity

Il Wi-Fi, in pratica, è diventato la base tecnologica di moltissime delle nostre attività quotidiane, sia lavorative che attinenti la sfera privata.

Attraverso la rete Wi-Fi passano miriadi di dati, spesso molto importanti, esposti però ad altrettanti rischi.

Secondo il report Online Trust Alliance 2018, nel solo anno 2017 si sono registrati 159.700 data breaches, ovvero cyber-attacchi andati a segno, più del doppio di quelli portati a termine nel 2016. Il dato più significativo è che il 93% di questi attacchi sarebbe potuto essere neutralizzato, utilizzando le basilari tecnologie e pratiche di Cybersecurity.

Il vero problema in materia di sicurezza informatica è rappresentato dal costante miglioramento delle minacce e dall'utilizzo di tecniche di attacco sempre nuove. Basti pensare all'introduzione di nuovi pericoli come ransomware e cryptolocker, cui si è assistito negli ultimi tempi.

Per questi motivi, una volta messa in piedi un'architettura Wi-Fi estremamente performante come quella Fortinet-Meru, è fondamentale difendere i dati che passano attraverso di essa. Fortinet è da anni leader mondiale nell'ambito della Cybersecurity, non solo grazie alle straordinarie performance delle sue tecnologie hardware o virtuali (firewall, antivirus ecc.), ma anche e soprattutto grazie ad una costante attività di ricerca di nuove minacce e di monitoraggio e diagnostica della "salute" della rete.

Da diversi anni, Fortinet ha costituito un centro di ricerca delle nuove minacce, che lavora costantemente per aggiornare le definizioni di pericoli, quali malware, applicazioni "exploit" e botnet. In questo modo, il centro di ricerca riesce ad aggiornare quotidianamente i propri prodotti, difendendo la rete e, al tempo stesso, prevenendo attacchi futuri. Inoltre, questa costante attività di ricerca, permette a Fortinet di rilasciare continuamente nuove patches per andare ad alzare il livello di sicurezza dei propri prodotti.

Si pensi alla Cybersecurity come ad un muro di cinta difensivo, al quale l'attività di ricerca di Fortinet aggiunge costantemente dei mattoncini per renderlo più alto e solido.

Nessun player del mercato della Cybersecurity può vantare una struttura così ampia, consolidata e reattiva. È anche questo aspetto che rende Fortinet il leader incontrastato del mondo della sicurezza informatica.

Tutte le reti possono essere difese, senza alcuna distinzione, attraverso le soluzioni di Cybersecurity Fortinet, ma è evidente che quelle che sfruttano il Wi-Fi Fortinet-Meru avranno benefici di integrazione maggiori. Questo perché, banalmente, creare un'architettura Wi-Fi e difenderla attraverso tecnologie che "parlano la stessa lingua" sarà molto più facile che mettere in comunicazione due tecnologie che devono prima "interpretarsi".

Utilizzare la tecnologia Fortinet sia per la rete Wi-Fi che per la Cybersecurity significa mettere in piedi il network che meglio di tutti riesce a coniugare potenza di prestazioni e sicurezza, sfruttando la perfetta complementarità delle due tecnologie dello stesso brand. A ciò si aggiunge il vantaggio e la comodità di avere un unico referente con cui relazionarsi e un solo centro di assistenza a cui rivolgersi.

È per tutti questi motivi che, per costruire una rete Wi-Fi performante, affidabile e sicura l'unica scelta vincente è Fortinet-Meru.


C'è
SEMPRE
la tua
Soluzione

FORTINET

MERU®

ALFACOD®
sistemi di identificazione automatica
mobile computing

Il Gruppo Alfacod sviluppa soluzioni di identificazione automatica e tracciabilità dal 1986.
É considerato fra i maggiori esperti nella progettazione e realizzazione di architetture WiFi ad alta velocità, soluzioni di Cybersecurity, sistemi RFid, soluzioni di geolocalizzazione (RTLS e FGS), sistemi di automazione del fine linea, soluzioni di tracciabilità e rintracciabilità e vanta oltre trent'anni di esperienza nel campo della stampa digitale.

GRUPPO ALFACOD

Sede di Bologna
via Cicogna, 83 - 40068 San Lazzaro di Savena (BO)
Tel. 051 4997211 / info-bo@alfacod.it

Sede di Milano
via San Cristoforo, 84 - 20090 Trezzano sul Naviglio (MI)
Tel. 02 90420055 / info-mi@alfacod.it

WWW.ALFACOD.IT