Confronto tra Cisco Systems Digital Network Architecture e Huawei Agile Campus

DR170921G

Ottobre 2017

Miercom
www.miercom.com

Sommario

1 - Sintesi

Miercom è stata incaricata da Cisco Systems di configurare, far funzionare e quindi valutare in modo indipendente le infrastrutture di rete per campus wireless e cablate di Cisco Systems e Huawei Technologies. I prodotti di ciascun fornitore sono stati configurati e implementati rigorosamente secondo i progetti consigliati dai fornitori e utilizzando il loro rispettivo software per la gestione, il controllo, la configurazione e il monitoraggio della rete in tutto il campus.

Sono stati condotti test in due aree principali:

1. **Modalità wireless:** valutazione di densità dei client, throughput, gestione del collegamento radio e delle interferenze, visibilità e supporto applicativo, definizione dei profili dei dispositivi, alta disponibilità e sicurezza.
2. **Modalità cablata:** valutazione della capacità degli switch di eseguire analisi avanzate del traffico e rilevamento delle minacce criptate, sicurezza e ottimizzazione delle risorse hardware, power stacking e alta disponibilità per l'aumento di dispositivi IoT abilitati da PoE, programmabilità.

Risultati e osservazioni principali:

- **Migliore gestione del collegamento radio**. Nel servire la stessa rete di test wireless con 180 client, gli AP Huawei (AP7050DE) hanno regolato la potenza di trasmissione che era decisamente impegnativa per un'implementazione ad alta densità, a una potenza quasi doppia, in media, rispetto agli AP Cisco (2802i); i segnali troppo forti hanno causato interferenze e problemi di connettività client. Inoltre, la connettività per client era distribuita in modo più uniforme tra gli AP Cisco rispetto agli AP Huawei. In più, gli AP Cisco passavano automaticamente il loro segnale radio da 2,4 GHz a 5 GHz, migliorando l'ottimizzazione della copertura client: una capacità impressionante non supportata dagli AP Huawei.

- **Maggiore throughput wireless e più sessioni video di qualità**. Configurati nella stessa modalità dual-mode a 2,4/5 GHz, gli AP Cisco hanno permesso ai client di ottenere fino al 22% in più di throughput del traffico TCP bidirezionale rispetto agli AP Huawei. Inoltre, Huawei ha mostrato occasionale perdita di pacchetti con mancata trasmissione ad alcuni client, cosa che non è accaduta agli AP Cisco, anche con tutti i 180 client attivi. Abbiamo osservato inoltre che, a parità di traffico, gli AP Cisco supportano più sessioni video client di qualità rispetto a quelli Huawei.

- **Migliore identificazione di traffico, dispositivi client e fonti di interferenza.** L'infrastruttura Cisco è riuscita a identificare molti tipi di traffico simultanei non individuati da quella Huawei, tra cui Instagram, Dropbox e WebEx. L'infrastruttura Cisco è riuscita anche a identificare correttamente tutte le fonti di interferenza che sono state applicate, mentre quella Huawei è riuscita a identificarne parzialmente solo una.

- **Maggiore disponibilità, failover più veloce**. Nelle configurazioni con tolleranza ai guasti, l'ambiente Cisco è riuscito a ripristinare un collegamento interrotto e un controller wireless molto più velocemente dell'ambiente Huawei. Le app temporizzate come i video non hanno subito interruzioni con la soluzione Cisco, mentre con la soluzione Huawei le sessioni sono scadute. Inoltre, l'infrastruttura cablata e wireless Cisco supporta varie opzioni di alimentazione, tra cui alimentatori in pool e condivisi, Perpetual e Fast Power-over-Ethernet, che fanno in modo che i dispositivi di rete alimentati subiscano minime interruzioni dell'alimentazione o addirittura nessuna.
- **Sicurezza senza perdita di prestazioni**. Molti processi di sicurezza, tra cui la crittografia DTLS, sono implementati nell'hardware nell'ambiente Cisco, mentre nell'ambiente Huawei gli stessi processi vengono eseguiti nel software, il che sottrae capacità di elaborazione alla gestione del traffico.
- **Encrypted Traffic Analytics**. Dalla visibilità di base alla sicurezza elevata, Cisco fornisce efficaci strumenti innovativi con cui le aziende possono identificare i flussi applicativi e offrire sicurezza e conformità solide alla loro infrastruttura di rete, anche per le minacce derivanti da malware, botnet, ecc. nascoste all'interno del traffico criptato, senza compromettere la privacy. Le soluzioni Huawei non hanno lo stesso livello di visibilità e sicurezza necessario per le applicazioni e le minacce moderne.
- **Risorse hardware protette e ottimizzate**. Gli switch Catalyst hanno supportato le modifiche (aggiunta/eliminazione) di policy ad alta velocità, con allocazione efficiente delle risorse per scalabilità e implementazione sicura. Grazie a funzioni come "ACL Label-Sharing" e "Hitless ACL updates", gli switch hanno supportato la programmazione della policy sulla rete senza compromissioni. Abbiamo osservato che gli switch Huawei possono subire perdite di dati che dovrebbero essere bloccate, mentre le modifiche dell'ACL vengono propagate e applicate a ogni interfaccia di switch.
- **Alta disponibilità per i dispositivi PoE**. Cisco StackPower offre vantaggi esclusivi rispetto a Huawei, mettendo in pool gli alimentatori delle singole fonti per ottenere la resilienza. Cisco Fast PoE e Perpetual PoE offre alta disponibilità a tutti i dispositivi connessi con PoE quando il dispositivo viene riavviato, intenzionalmente o involontariamente.
- **Programmabilità del software.** La programmabilità di Cisco IOS-XE supporta tecnologie che semplificano l'automazione e il provisioning e rendono più efficienti le attività di gestione della rete. IOS-XE ha la capacità di ospitare applicazioni basate su Linux tramite la funzionalità Guest Shell e questo rende possibili molti utili scenari d'uso per l'infrastruttura di rete.
- **Affidabilità.** Gli affidabili sistemi Cisco costituiscono la base per una rete dall'architettura sicura. Cisco protegge la rete utilizzando la firma delle immagini, l'avvio sicuro, il modulo Trust Anchor, difese di run-time e la sicurezza del piano di controllo.

Sulla base dei risultati di questi test comparativi delle architetture di rete cablata e wireless per campus e dei prodotti di Cisco e Huawei Technologies, abbiamo riscontrato molte funzionalità vantaggiose per le aziende che rendono la soluzione Cisco preferibile. Siamo lieti di conferire la ***Miercom Performance Verified Certification*** ai progetti di rete Cisco per infrastrutture campus e ai relativi pacchetti per il monitoraggio, la gestione e il controllo.

Robert Smithers
CEO
Miercom

2 – La nostra metodologia

Per questo test sono state assemblate l'una accanto all'altra due reti per infrastruttura campus: una di Cisco Systems e una di Huawei Technologies. I dettagli dei principali componenti di ognuna delle reti sono riportati di seguito. I tecnici Miercom si sono assicurati che le topologie, tutti i prodotti e le relative configurazioni di Cisco e Huawei corrispondessero alle più recenti e appropriate soluzioni comparabili dei due fornitori. I test wireless trattati in questo report sono stati eseguiti in una sede configurata e utilizzata esclusivamente per testare apparecchiature wireless.

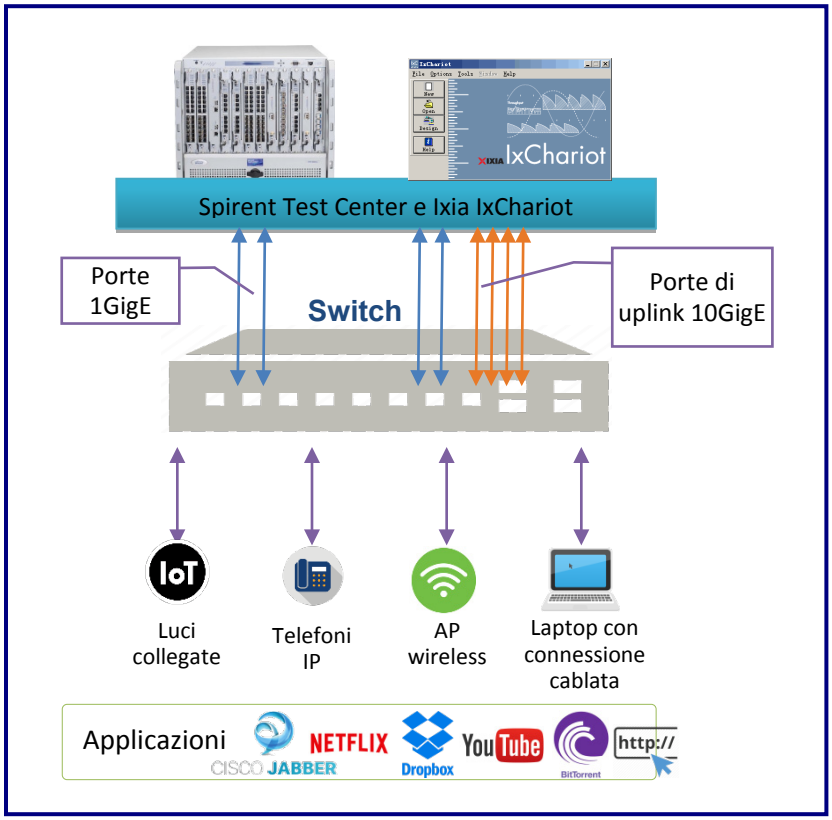
Prodotti testati

	Cisco Systems		**Huawei Technologies**	
Dispositivo	**Modello**		**Modello**	
Access point	2802i 	Prezzo di listino: $ 1.295 Radio: 4x4:3 MU-MIMO Ampiezza canale: 160 MHz Ethernet: 2xGbE	AP7050DE 	Prezzo di listino: $ 1.295 Radio: 4x4:4 MU-MIMO Ampiezza canale: 160 MHz (2x2) Ethernet: 2xGbE
	Modello	**Software**	Modello	**Software**
Controller wireless	5520	V8.3 MR3	AC6605	V200R700C20SPC200
Switch	Catalyst 3850	V16.6.1	S5720 HI	V2R11
Switch	Catalyst 9300	V16.6.1	S5720 HI	V2R11
Switch	Catalyst 2960XR	V15.2.6	S5720 SI	V2R11

Strumenti di test

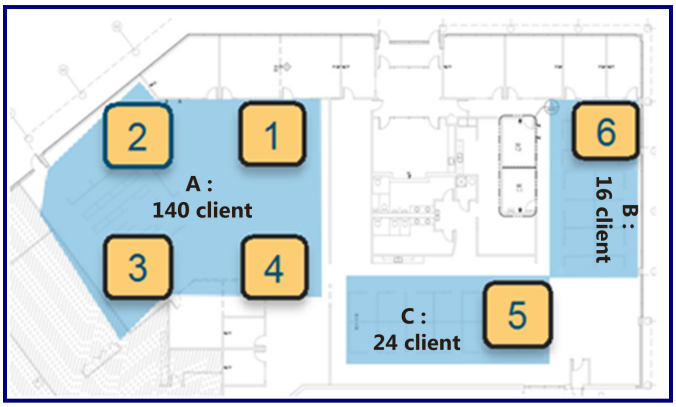
Strumento di test	**Versione**
Ixia IxChariot	V7.3
Spirent Test Center	V4.6.7

Configurazione di test n. 1: switching



Fonte: Cisco

Configurazione di test n. 2: wireless



Fonte: Miercom

Per i test della densità dei client, della potenza del segnale e delle prestazioni di throughput, sono stati implementati sei AP di ciascun fornitore, numerati come mostrato nel diagramma seguente. Sono stati configurati un totale di 180 client sui tavoli delle tre aree celesti. L'area A era un grande ambiente open space con 140 client sui tavoli. Le aree B e C, con 16 e 24 client rispettivamente, erano sale suddivise in tanti uffici mediante pareti divisorie, con 1 o 2 client per postazione.

Per riflettere l'evoluzione del Wi-Fi dall'uso della banda a 2,4 GHz alla banda a 5 GHz, la maggioranza dei client, ovvero 140 ossia il 78%, funzionava a 5 GHz e i rimanenti 40 client (pari al 22%) funzionavano sulla banda a 2,4 GHz.

Il Wi-Fi di ciascun client supportava una combinazione di vari standard: IEEE 802.11n (20), IEEE 802.11ac (120) e IEEE 802.11ac Wave 2 (40). I client e le loro diverse capacità, tra cui client che supportano 802.11ac Wave 2 con MIMO multiutente, sono stati scelti per emulare ambienti reali.

Cliente	Supporto del Wi-Fi, numero di spatial stream, supporto MIMO	N. di client
MacBook Pro	11ac, 3SS, SU-MIMO	50
MacBook Air	11ac, 2SS, SU-MIMO	20
Dell E6430 con Broadcom43460	11ac, 3SS, SU-MIMO	10
Dell E6430 con Intel 7260	11ac, 2SS, SU-MIMO	30
Acer Aspire	11ac, 1SS, MU-MIMO	30
Dell E5450	11ac, 2SS, MU-MIMO	10
MacBook Pro	11n, 3SS, SU-MIMO	10
iPad Air	11n, 2SS, SU-MIMO	10
Apple iPhone 6	11ac, 1SS, SU-MIMO	10

3 – Infrastruttura wireless

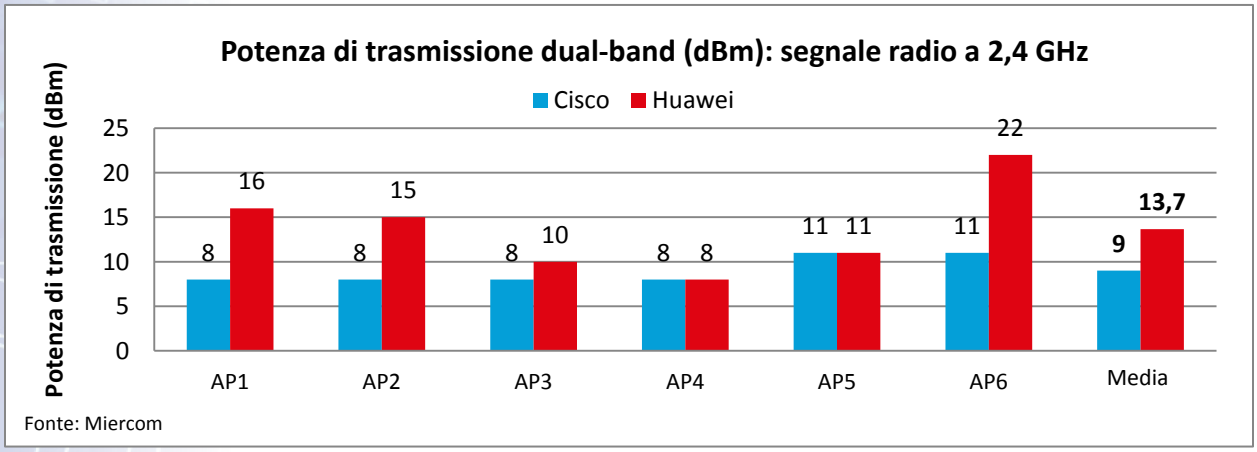
Potenza di trasmissione degli AP

Sono stati testati tre diversi ambienti di AP:

1. Huawei "dual-band", dove ciascuno dei sei AP usava un collegamento radio da 2,4 GHz e uno da 5 GHz;
2. Cisco "dual-band", dove ciascuno dei sei AP usava un collegamento radio da 2,4 GHz e uno da 5 GHz, e
3. Cisco "dual 5 GHz". Questo utilizza una funzionalità esclusiva di Cisco che consente a un AP di adattare il suo collegamento radio da 2,4 GHz e usare 5 GHz, in caso di sovrapposizioni nella banda a 2,4 GHz. In questo terzo scenario due dei sei AP Cisco (numeri 1 e 4 sulla piantina) hanno adattato i loro collegamenti radio da 2,4 GHz a 5 GHz, facendoli funzionare entrambi a 5 GHz.

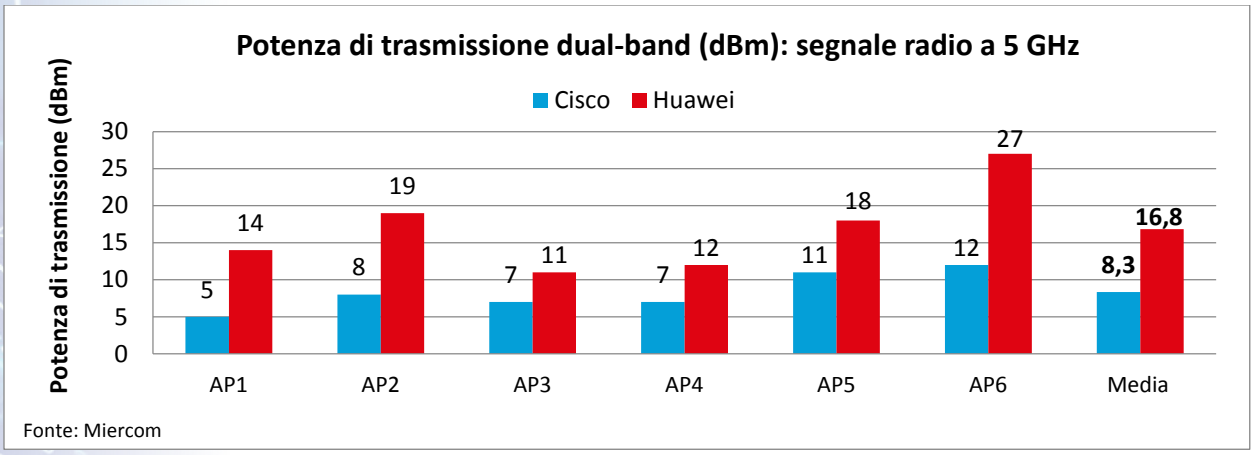
I grafici seguenti mostrano la potenza di trasmissione per canale per questi ambienti.

Segnale radio dual-band a 2,4 e 5 GHz: confronto tra Cisco e Huawei



Fonte: Miercom

Il valore operativo minimo di Cisco è stato 8 dBm. La sua potenza di trasmissione media è stata inferiore di 4,7 dBm rispetto a Huawei.

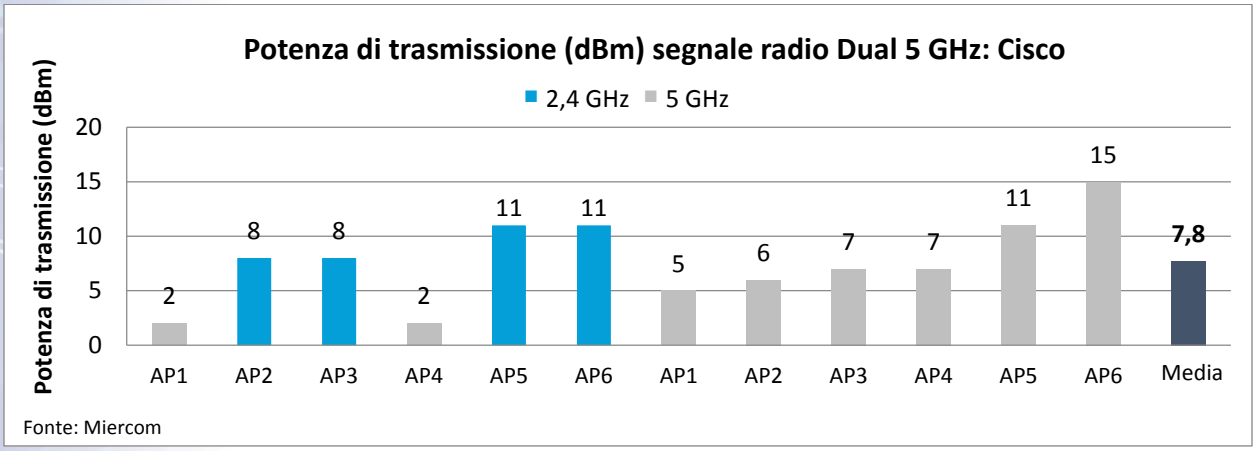


Fonte: Miercom

Il valore operativo minimo di Cisco è stato 8,3 dBm. La sua potenza di trasmissione media è stata inferiore di 8,5 dBm rispetto a Huawei.

I livelli di trasmissione media di Huawei per dual-band sono stati di 15,25 dBm (decibel riferiti a un milliwatt). Un solo AP Huawei operava alla piena potenza di trasmissione (27 dBm). In confronto, gli AP dual-band Cisco hanno registrato una media di solo 8,67 dBm per canale di trasmissione, circa la metà della potenza di trasmissione media di Huawei.

Segnale radio dual-band a 5 GHz: Cisco



Fonte: Miercom

Abbiamo rilevato il valore più basso della potenza di trasmissione degli AP nell'ambiente Cisco Dual 5 GHz, dove la media era di appena 7,8 dBm.

Canale Cisco e configurazione della potenza per collegamento radio

AP	Canale	Radio	Potenza (dBm)
AP1	36+	5 GHz	2
	100+	5 GHz	5
AP2	1	2,4 GHz	8
	64-	5GHz	6
AP3	11	2,4 GHz	8
	149+	5 GHz	7
AP4	128-	5 GHz	2
	44+	5 GHz	7
AP5	6	2,4 GHz	11
	161-	5 GHz	11
AP6	11	2,4 GHz	11
	108+	5 GHz	15

Quando si hanno alti livelli di potenza di trasmissione degli AP si possono verificare interferenze da canale condiviso e il problema degli "sticky client": ovvero i client non eseguono il roaming perché il segnale AP è troppo forte, mentre il segnale del client è troppo debole per raggiungere in modo affidabile l'AP.

Distribuzione dei client

Gli AP di entrambi i fornitori erano posizionati allo stesso modo e i client non sono mai stati spostati durante il test. Anche così, la distribuzione dei client connessi ai sei AP era notevolmente diversa, nonostante l'uso di tecniche di bilanciamento del carico client del fornitore.

La distribuzione dei client favorisce la loro prossimità all'AP più vicino, ma ci aspettavamo una distribuzione più uniforme. Uno scenario comune con troppi client su un solo AP rallenta il throughput mentre altri AP vicini sono sottoutilizzati. La tabella mostra il numero dei client a 5 GHz che si sono connessi automaticamente ai sei AP dei fornitori.

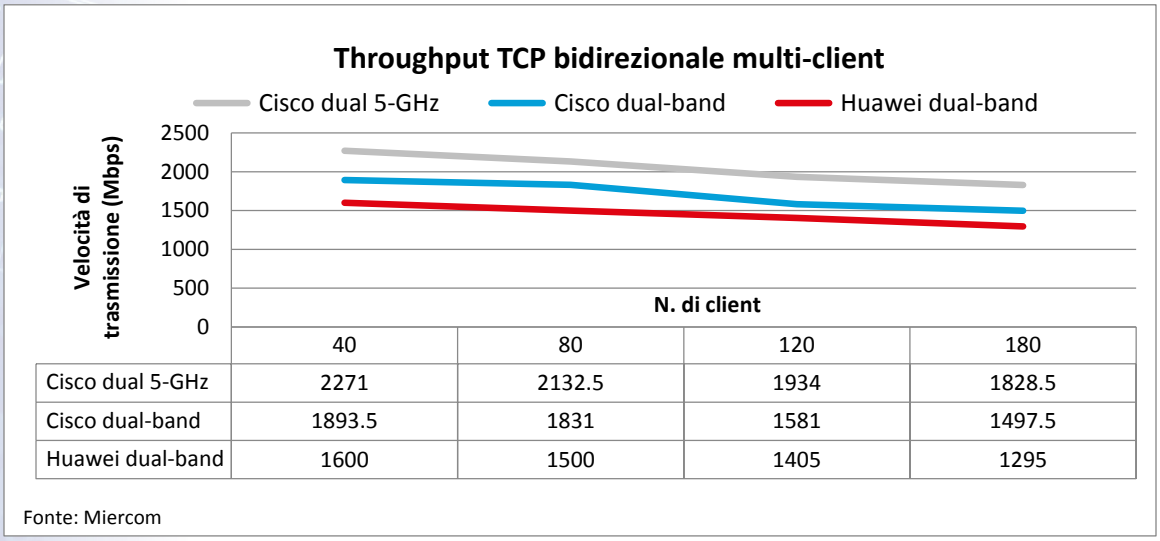
Distribuzione dei client per AP a 5 GHz (140 client in totale)

Numero di AP	Huawei dual-band	Cisco dual-band	Cisco dual 5-GHz
1	30	36	20
2	46	20	43
3	27	29	33
4	3	12	11
5	14	21	21
6	20	22	12

Il numero dei client AP Huawei attivi variava da 3 client su un solo AP fino a un notevole carico di 46. Con una configurazione dual-band Cisco comparabile, il numero di client AP variava da un minimo di 12 client su un solo AP fino a 36 per il carico più pesante: una distribuzione molto più ragionevole.

Prestazioni di throughput

Utilizzando lo strumento di test Ixia IxChariot, sono stati eseguiti test di throughput per misurare quanto throughput aggregato si poteva raggiungere attraverso le infrastrutture di ciascun fornitore da e verso gli stessi client wireless. Per rappresentare il traffico utenti tipico di oggi è stato applicato traffico TCP bidirezionale orientato alla connessione. Sono stati eseguiti test con 40, 80, 120 e tutti i 180 client, utilizzando la stessa combinazione di client a 5 GHz e 2,4 GHz. È stata vincolata la funzionalità FRA (Flexible Radio Assignment) degli AP Cisco per mantenere tutti gli AP Cisco in funzione a 5 e 2,4 GHz (dual-mode). Quando era abilitata e in funzione, la funzionalità FRA adattava automaticamente il collegamento radio di due AP Cisco da 2,4 GHz a 5 GHz, in modo che operassero a 5 GHz. Questo scenario "Cisco dual 5 GHz" ha dato le migliori prestazioni di throughput.



	40	80	120	180
Cisco dual 5-GHz	2271	2132.5	1934	1828.5
Cisco dual-band	1893.5	1831	1581	1497.5
Huawei dual-band	1600	1500	1405	1295

Fonte: Miercom

La configurazione Cisco dual 5-GHz ha raggiunto il 41,8% in più di throughput bidirezionale aggregato rispetto all'infrastruttura Huawei con 40 client attivi. Con 180 client, Cisco ha ottenuto un throughput più alto del 41%. Con il vincolo al funzionamento dual-band, il vantaggio di Cisco si è ridotto, ma era ancora significativo, con il 22% di throughput in più per 80 client attivi e il 15,6% in più per il pieno carico di 180 client.

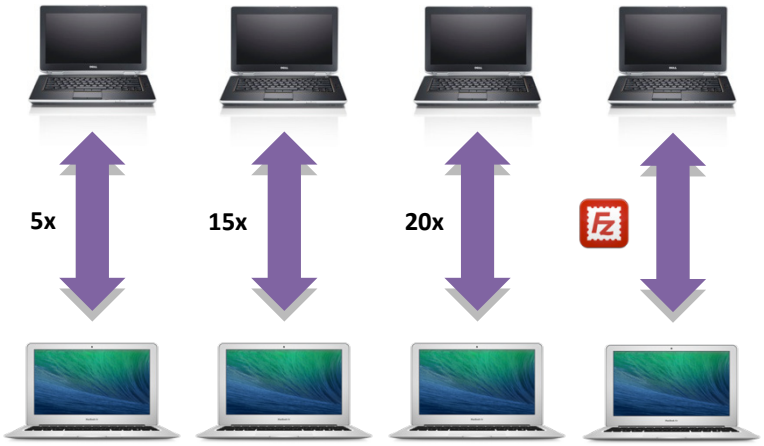
Perdita di pacchetti con Huawei

Abbiamo osservato un'altra differenza tra gli ambienti Cisco e Huawei. Gli stessi test di throughput bidirezionale hanno mostrato perdita di pacchetti, ovvero mancata trasmissione/ricezione di traffico da parte di alcuni client, ma solo con l'infrastruttura Huawei. La perdita di pacchetti non è stata notevole, anche se aumentava con il numero di client attivi. In qualsiasi misura, la perdita di pacchetti causa problemi di prestazioni, perché i pacchetti persi devono essere identificati e inviati di nuovo. Il fatto che non ci fosse alcuna perdita di pacchetti corrispondente con nessuna delle configurazioni Cisco rende questa osservazione importante.

Supporto QoS per le videochiamate

Abbiamo eseguito test per accertare la capacità delle infrastrutture wireless di assegnare priorità al traffico. Questi test hanno coinvolto i 24 client wireless nelle postazioni servite esclusivamente dal quinto AP. In ognuna di esse c'erano un Apple MacBook e un iPhone.

La QoS è stata abilitata nell'infrastruttura wireless per dare priorità ai flussi video secondo le best practice dei fornitori. Quindi è stata inviata una ripetizione continua di un file da 10 GB tramite FTP ai client wireless, per applicare il carico di background. Poi sono state avviate videochiamate Jabber fra i PC e i Mac, con un pattern frattale in continuo movimento sullo sfondo dei video. I tester si muovevano e valutavano la qualità del segnale video di ogni videochiamata. In alcuni dei video c'erano piccoli errori, ma il fattore determinante per l'esecuzione corretta delle videochiamate era che nessuna chiamata venisse interrotta.

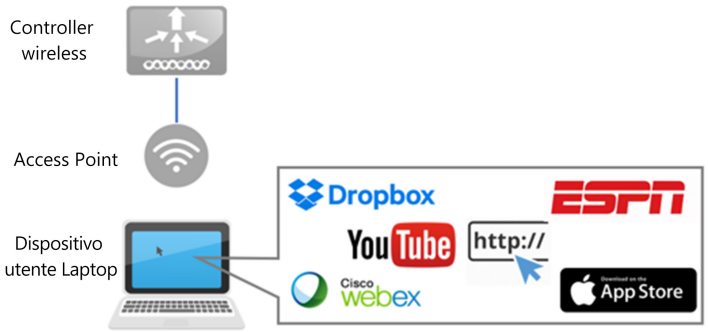


Fonte: Cisco

I test sono iniziati con sessioni video di Jabber con cinque client, che si sono svolte senza problemi con Huawei e Cisco. Poi abbiamo eseguito di nuovo il test con 10, 15 e infine 20 client, osservando quando le videochiamate erano inguardabili o le connessioni del feed video si interrompevano. L'AP Huawei è riuscito a sostenere un massimo di 11 videochiamate Jabber simultanee completamente riuscite. L'AP Cisco, invece, è riuscito a sostenere 18 chiamate simultanee di Jabber senza problemi.

Application Visibility & Control

Le infrastrutture Cisco e Huawei sottoposte ai test presentavano entrambe la capacità di analizzare il traffico, un primo passo necessario per identificare i thread di traffico che potrebbero costituire una minaccia. Huawei, nella sua documentazione, sostiene di riuscire a identificare il traffico proveniente da molte applicazioni. In fase di test, però, abbiamo rilevato che il riconoscimento del traffico di Huawei in molti casi si ferma a un alto livello (ad esempio l'identificazione del traffico come http/https, che è la base per quasi tutto il Web browsing). Di conseguenza, senza identificare ulteriori specifiche del traffico, la visibilità e il conseguente controllo dei flussi di traffico sono limitati.



Fonte: Cisco

La tabella seguente mostra i risultati di alcuni flussi di traffico che abbiamo cercato di identificare nei test. Dove è stato possibile identificare l'origine del traffico specifica è riportato un "Sì". In alcuni casi per Huawei è riportato un "No": il messaggio era visibile ma l'infrastruttura Huawei non è riuscita a distinguere la particolare origine per la mancanza di Deep Packet Inspection.

Categoria	Applicazione/origine	Huawei	Cisco
Web	ESPN	Sì	Sì
	BBC	Sì	Sì
	Fox News	No	Sì
	YouTube	Sì	Sì
	Instagram	No	Sì
	Test di velocità	No	Sì
Riunione	WebEx	No	Sì
	Condivisione dello schermo WebEx	No	Sì
Condivisione di file	Dropbox	No	Sì
Aggiornamento iOS	Download di app iOS	No	Sì

Abbiamo osservato che Cisco esamina il traffico in modo più approfondito ed è in grado di fornire più dettagli sulle origini di traffico sospette attraverso la Deep Packet Inspection (DPI). Cisco è anche più abile nella definizione dei profili e nel riconoscimento dei flussi di pacchetti criptati.

Definizione dei profili client

Oggi, la sicurezza della rete richiede la capacità di identificare facilmente le origini di traffico che potrebbero costituire una minaccia. Abbiamo richiesto al controller Cisco di definire il tipo di dispositivi wireless collegati agli AP nel nostro banco di prova. Il dashboard Cisco ha mostrato le seguenti identità dei dispositivi:

Identità segnalata	Tipologia effettiva di dispositivo wireless
OS_X-Workstation	MacBook
Microsoft-Workstation	PC (MS Windows 10)
Apple-iPhone	Apple iPhone
Android-Google	Smartphone Android Nexus 5X

Huawei non supporta questa capacità di definizione dei profili client.

Rilevamento e identificazione delle interferenze

Le infrastrutture wireless di Cisco e di Huawei, secondo quanto dichiarano i fornitori, includono applicazioni e strumenti per l'identificazione delle fonti di interferenza wireless. In questo test abbiamo introdotto vari dispositivi comuni, noti per interferire con il funzionamento e le frequenze wireless. Fra questi c'erano un altoparlante wireless Bluetooth, un forno a microonde, una videocamera e un Jammer, dispositivo realizzato appositamente per interferire con le reti wireless. Quindi, utilizzando le funzionalità disponibili per l'infrastruttura wireless di ciascun fornitore, abbiamo verificato in quale misura i prodotti riuscivano a identificare le fonti di interferenza. I risultati sono mostrati di seguito.

Dispositivo effettivo che genera interferenza	Cisco: rilevato e riconosciuto?	Come l'ha identificato e segnalato?	Huawei: rilevato e riconosciuto?	Come l'ha identificato e segnalato?
Altoparlante Bluetooth	Sì	"BT Link"	No	N/D
Forno a microonde	Sì	"MW Oven"	No	N/D
Videocamera	Sì	"Video Camera"	Parzialmente*	Dispositivo "unknown fixed frequency"
Jammer	Sì	"Jammer"	No	N/D

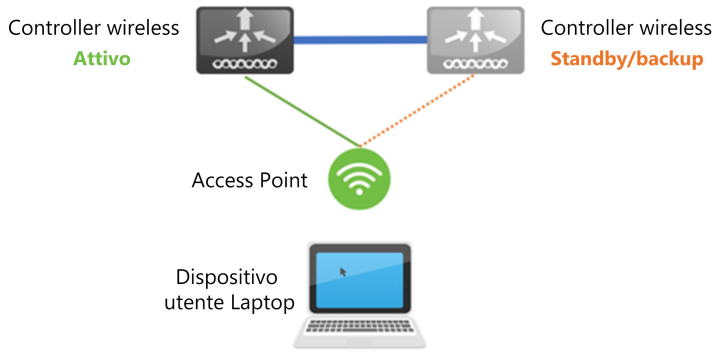
*Huawei non ha rilevato alcun dispositivo generatore di interferenza a una distanza di almeno 9 metri dall'AP. La videocamera è stata rilevata come dispositivo "unknown fixed frequency" (sconosciuto a frequenza fissa) quando era in funzione a circa 120 cm dall'AP.

Alta disponibilità

Entrambi i fornitori offrono cosiddette soluzioni ad alta disponibilità (HA), per minimizzare l'effetto dell'errore di un singolo collegamento o dispositivo. Abbiamo condotto test per accertare l'efficacia relativa di queste soluzioni per mantenere l'operatività dei client wireless.

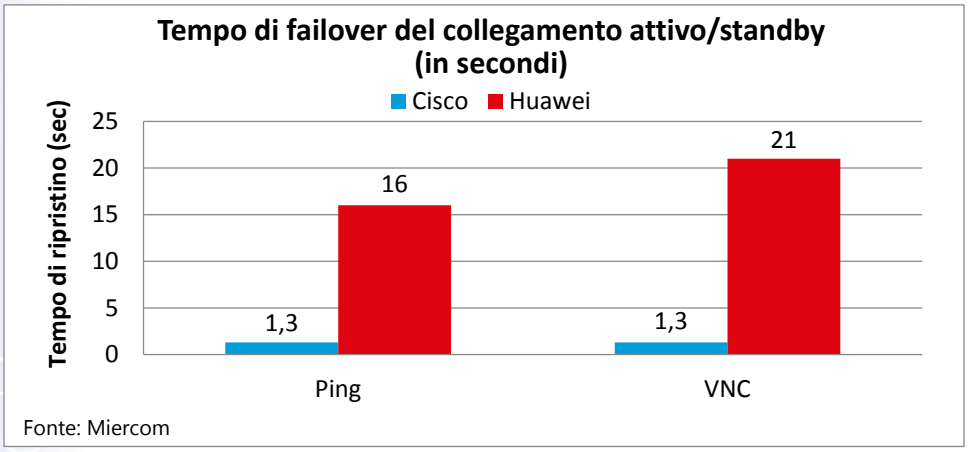
Nell'ambito della sua offerta HSB (Hot Standby), Huawei consente di configurare due controller di accesso (AC) wireless in modalità standby/attiva, con dual-home degli AP a questi mediante uno switch di accesso. Per accelerare il failover, viene eseguito il backup delle informazioni utente nel controller di accesso di standby. Quando il controller di accesso attivo viene ripristinato, le operazioni e i servizi vengono riattivati con un'interruzione minima.

Cisco, analogamente, consente di implementare due dei suoi Wireless LAN Controller (WLC) per la ridondanza. Inoltre, abbiamo notato che Cisco offre altri miglioramenti dell'affidabilità, come il riavvio veloce del sistema, la connettività ridondante a 1 gigabit o a 10 gigabit, l'archiviazione a stato solido senza parti mobili e gli alimentatori opzionali, ridondanti e sostituibili a caldo.



Fonte: Cisco

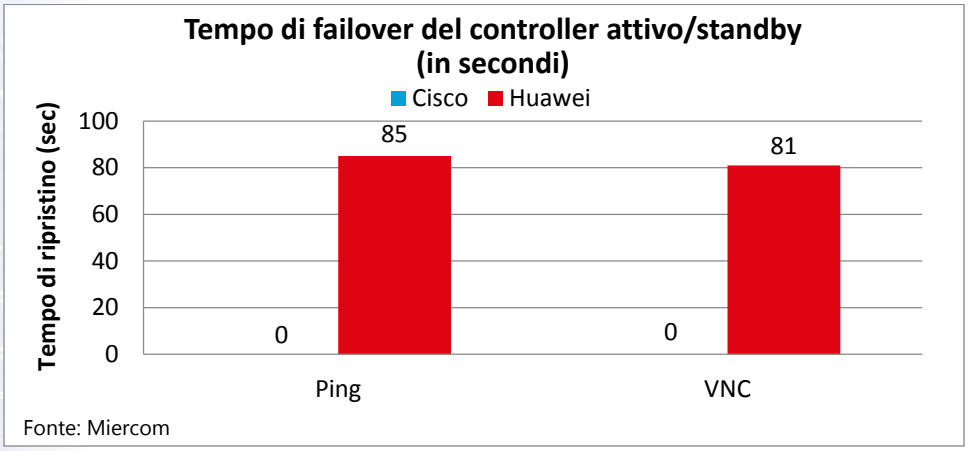
Abbiamo innanzitutto testato la perdita del collegamento attivo tra i controller (errore di switch/porta), che implica il passaggio al collegamento ridondante. Questo è stato fatto mentre erano in funzione due applicazioni tra i dispositivi collegati tramite il collegamento disconnesso, per vedere quanto tempo impiegavano le applicazioni per ripristinare la connessione. Le applicazioni erano un ping continuo veloce a 0,1 secondi e un flusso video VNC. Il grafico sottostante mostra il tempo necessario, in secondi, per ristabilire la connessione dell'applicazione.



Fonte: Miercom

Cisco ha dimostrato tempi di recupero molto inferiori. Cisco è stato più veloce di 14,7 secondi nel recuperare la connessione dell'applicazione per un ping rispetto a Huawei. Il tempo di failover per il flusso video VNC è stato di 19,7 secondi più veloce per Cisco che per Huawei.

In un secondo test abbiamo tolto l'alimentazione al controller attivo, causando un failover allo standby, mentre venivano eseguite le stesse applicazioni di ping e video VNC.



Fonte: Miercom

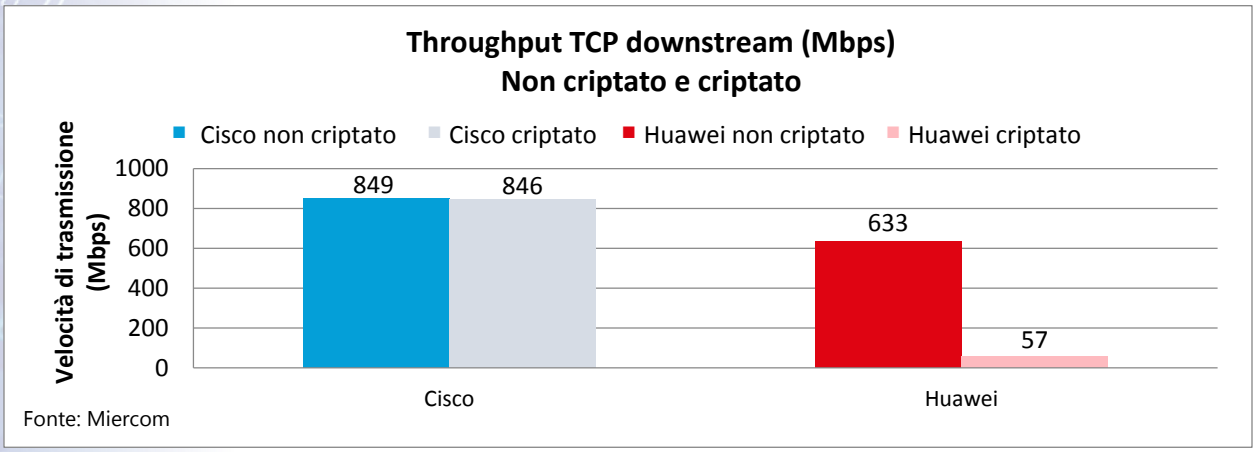
Cisco non ha registrato nessuna interruzione di queste applicazioni durante il failover. Huawei ha avuto bisogno di ben 85 secondi di tempo per il ripristino.

Abbiamo rilevato che il tempo di ripristino si deve all'architettura Stateful Switch Over (SSO) di Cisco, che salva gli stati delle porte nell'hardware quando il controller smette di funzionare. Il tempo effettivo impiegato da Cisco per il passaggio è inferiore a un secondo, perciò il tempo di failover dell'applicazione diventa impercettibile agli utenti finali.

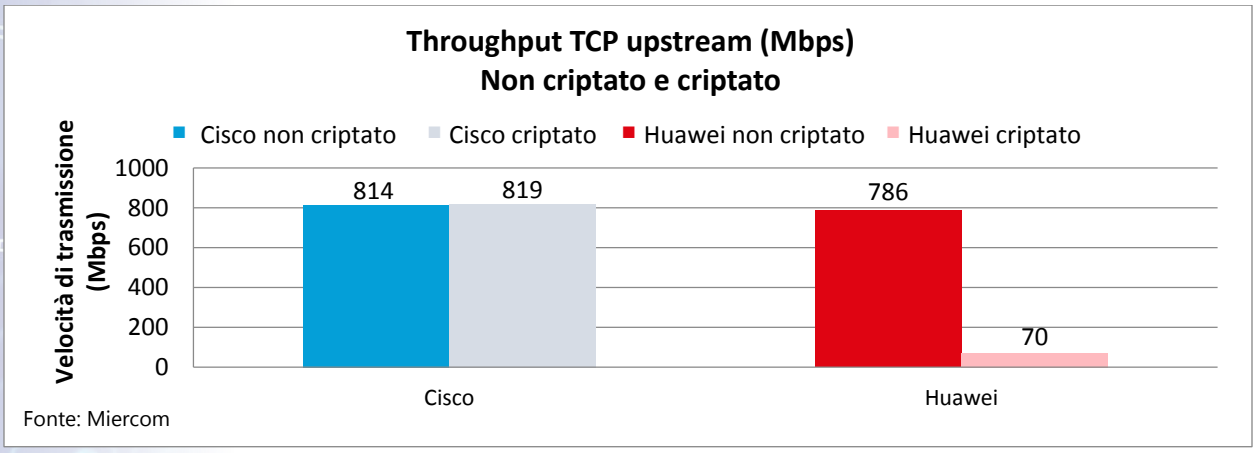
Crittografia DTLS

Il protocollo Datagram Transport Layer Security (DTLS), progettato per impedire intercettazioni, manomissioni e falsificazioni dei messaggi, è sempre più usato per proteggere le trasmissioni wireless. Insieme ad altri meccanismi di sicurezza, DTLS comprende anche la crittografia del payload del messaggio. In genere questa viene eseguita dall'AP per i messaggi wireless in uscita.

Sono stati eseguiti test di misurazione del throughput dell'AP per il traffico TCP. Prima abbiamo inviato traffico non criptato ai client wireless, mostrato nel grafico di seguito come "TCP Down" con "DTLS Off". Inoltre abbiamo misurato il throughput "TCP Up" per il traffico di ritorno all'AP dai client wireless. Poi abbiamo ripetuto il test, questa volta dopo aver attivato la crittografia DTLS. Come mostrato, il throughput di Huawei è sceso vertiginosamente intorno al 10% circa del throughput senza crittografia.



Fonte: Miercom



Fonte: Miercom

Il throughput con crittografia di Cisco ha avuto solo una lieve flessione, grazie all'hardware di crittografia specializzato. Gli AP Huawei, invece, eseguono l'elaborazione di crittografia utilizzando il software, il che applica un carico pesante, riducendo il throughput di oltre il 90%.

4 - Infrastruttura cablata

Encrypted Traffic Analytics

Oggi è indispensabile conoscere il traffico o i dati utilizzati dalle applicazioni all'interno della rete. Le applicazioni, gli utenti, il tempo di utilizzo e soprattutto la sicurezza e la conformità sono informazioni vitali per le policy aziendali.

Nelle reti moderne ci sono molte applicazioni diverse:

Porte note	Porte casuali	Flussi criptati (SSL)
Esempi: HTTP (80), FTP (21), Telnet (23).	Esempi: Skype, Bit Torrent, applicazioni voce/video	Esempi: Malware, botnet
Difficoltà di rilevamento: bassa	Difficoltà di rilevamento: media	Difficoltà di rilevamento: alta

Fonte: Cisco

Con l'evolversi di applicazioni, utenti e dispositivi oltre l'utilizzo di flussi e porte standard, i fornitori di infrastrutture devono rendere i loro prodotti e servizi più intelligenti nel rilevare, identificare e controllare ogni pacchetto che scorre sulla rete. Ci sono varie procedure e protocolli standardizzati per la raccolta di pacchetti e flussi di dati specifici che arrivano sulle interfacce di rete. Cisco AVC (Application Visibility & Control) utilizza DPI (Deep Packet Inspection) e l'analisi euristica per identificare flussi di applicazioni granulari e flussi secondari attraverso le sue piattaforme di routing wireless e cablate. Analogamente a Cisco AVC, Huawei offre SAC (Smart Application Control) per il wireless ma non è disponibile nei suoi switch.

Aggregando le informazioni dei flussi delle applicazioni dai dispositivi dell'infrastruttura mediante NetFlow in Cisco StealthWatch, un amministratore di rete può identificare l'origine e la destinazione del traffico, la classe del servizio e aspetti simili del traffico di rete. Huawei supporta anche l'aggregazione di flussi tramite NetStream.

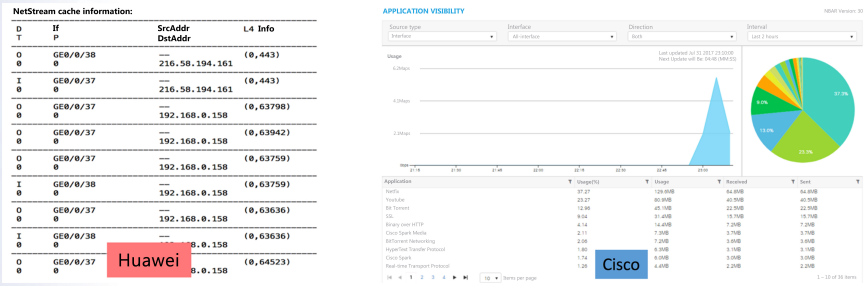
Ultimamente il numero di applicazioni criptate cresce in modo esponenziale. Queste applicazioni sono difficili da identificare perché i dispositivi di rete non sono in grado di esaminare l'interno del traffico criptato, per questioni tecniche o relative alla privacy. Gli utenti malintenzionati approfittano di questa opportunità per nascondere malware, botnet o trojan all'interno del traffico criptato e inviare pacchetti dannosi su tutte le reti, lasciando così completamente al buio gli amministratori di rete sulle potenziali minacce nascoste all'interno dei flussi criptati. Cisco può identificare le minacce all'interno del traffico criptato con la sua nuova tecnologia ETA (Encrypted Threat Analytics). Cisco StealthWatch con Cognitive Threat Analysis utilizza un algoritmo di machine learning multi-livello e varie altre tecniche, come la temporizzazione dei pacchetti, la sequenza dei pacchetti e l'etichettatura dei pacchetti iniziali, per identificare le minacce all'interno del traffico criptato senza violare la privacy dei dati.

Nella nostra analisi comparativa abbiamo rilevato che Cisco implementa AVC e NetFlow in un ASIC (Application Specific Integrated Circuit) hardware, perciò le acquisizioni di NetFlow non sottraggono potenza ai processori dello switch principale.
Abbiamo confrontato le tecnologie Cisco e Huawei in tre scenari di test principali di analisi del traffico:

1. Identificazione del traffico in base alle porte
2. Visibilità a livello dell'applicazione
3. Rilevamento delle minacce nel traffico criptato

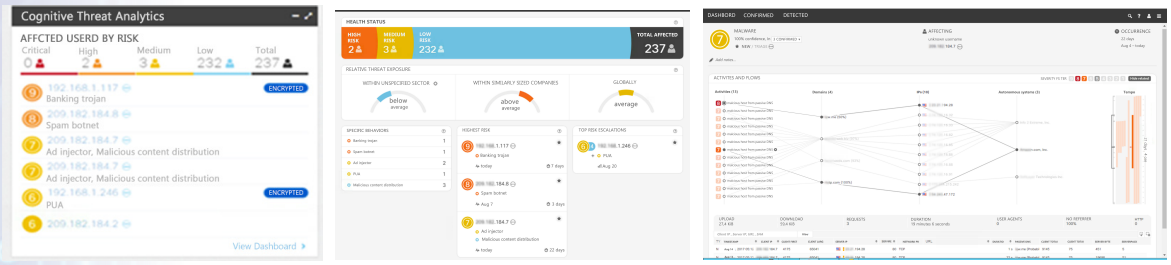
Risultati

Nei primi due scenari di test, Huawei ha identificato le applicazioni solo sulla base dei numeri di porta standard, ad esempio HTTPS (443). Huawei non ha fornito informazioni approfondite su applicazioni come WebEx, YouTube, BitTorrent, Netflix, Spark e Skype. Inoltre, Huawei non offriva alcuna interfaccia Web per monitorare questo traffico. Cisco, invece, offriva un intuitivo dashboard Web (e CLI) per identificare le applicazioni in base al numero di porta e ai nomi (YouTube, BitTorrent, Netflix, Spark Media).



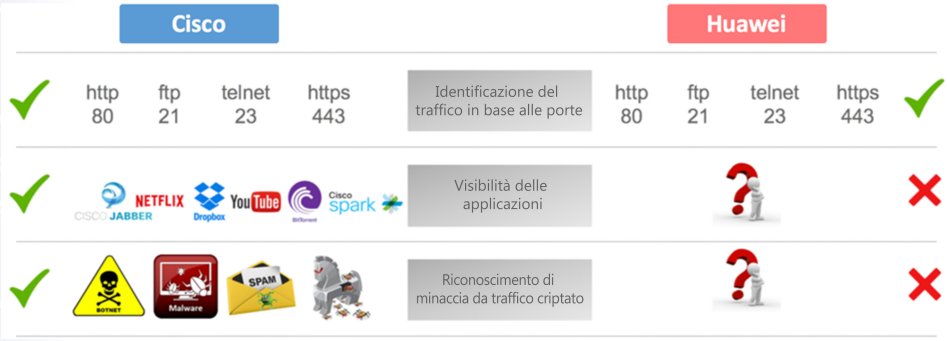
Fonte: Cisco

Nel terzo scenario di test, Huawei non è riuscita a offrire alcun tipo di visibilità sulle minacce all'interno del traffico criptato. In Huawei tutto il traffico è stato identificato come traffico SSL/TLS, senza nessuna informazione sulle botnet e il malware nascosti all'interno del traffico criptato. Cisco ha identificato con precisione le minacce nascoste all'interno del traffico criptato e ha attivato le misure necessarie per mitigarle.



Fonte: Cisco

Per riassumere, dalla visibilità di base alla sicurezza elevata, Cisco riesce a fornire strumenti innovativi con cui le aziende possono identificare i flussi applicativi e offrire sicurezza e conformità solide alla loro infrastruttura di rete. Le soluzioni Huawei non hanno lo stesso livello di visibilità e sicurezza necessario per le applicazioni e le minacce moderne.



Risorse di switching ottimizzate e protette

La nascita e l'espansione dei mercati IoT comportano un bisogno crescente di sicurezza e segmentazione. La rete deve identificare correttamente e fornire accesso controllato a utenti e dispositivi. Indipendentemente dal mezzo di comunicazione, oggi è richiesto un accesso dinamico tramite una policy automatizzata. L'infrastruttura di rete deve supportare la programmazione delle sue risorse in modo sia statico che dinamico. I costrutti della policy di rete sono applicati sotto forma di ACL di sicurezza e filtro QoS a porte fisiche e logiche, come VLAN L2 o interfacce di accesso con routing L3.

Miercom ha testato e confrontato le funzionalità hardware degli switch per campus Cisco e Huawei. Lo switch Huawei S5720-HI è stato confrontato con gli switch Cisco Catalyst delle serie 9300 e 3850. Si è trattato di un test ad ampio spettro, svolto per valutare i limiti di scalabilità dei filtri di policy degli switch e la gestione delle risorse. Inoltre, ogni switch è stato testato per determinare la probabilità di subire violazioni della sicurezza di rete durante le modifiche a un filtro di policy esistente.

Le funzionalità di filtro di sicurezza di Cisco e Huawei sono state confrontate in quattro scenari di test:

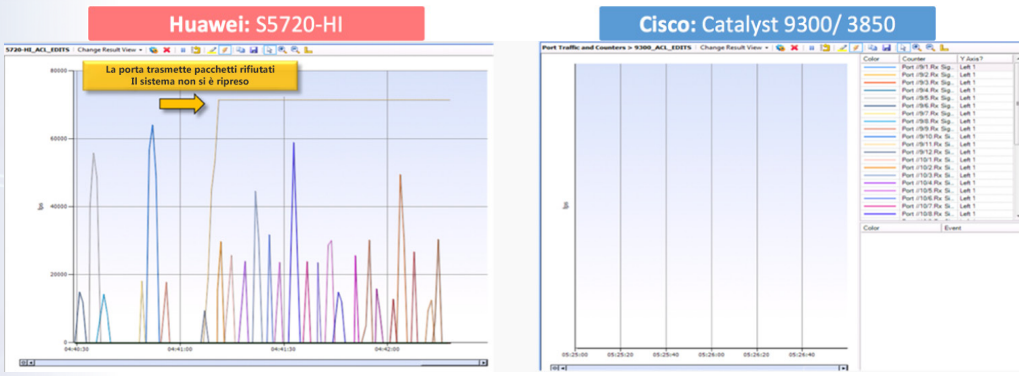
1. Quando si applica lo stesso ACL a più interfacce, l'ACL usa un numero di voci pari a N x TCAM, dove N è il numero di porte a cui è applicato l'ACL?
2. Lo switch supporta le risorse ottimizzate: condivisione dell'ACL?
3. In che modo lo switch gestisce le modifiche all'ACL esistente?
4. Lo switch consente l'inoltro del traffico rifiutato durante la modifica dell'ACL?

Ogni switch è stato configurato con una singola policy ACL con 300 regole. A ciascuna interfaccia L3 sono state applicate policy in ingresso e in uscita. È stato collegato uno Spirent

Test Center a ogni switch per la generazione del traffico, con PC connessi a ogni switch per testare l'accesso a servizi come FTP, ICMP, Telnet e SSH. Gli switch sono stati monitorati per l'utilizzo delle risorse, ad esempio TCAM, utilizzo della CPU, contatori ALC e logging di sistema.

Quando si applica lo stesso ACL a più interfacce, l'ACL usa N x TCAM voci, dove N è il numero di porte a cui è applicato l'ACL. Ad esempio, su Huawei S5720-HI, un ACL in ingresso con 300 regole applicato a tutte le porte (48 interfacce in direzione sud e 4 interfacce uplink) utilizzava 15.600 regole. Quando si è tentato di applicare lo stesso ACL per la direzione in uscita, S5720-HI era limitato solo a un sottoinsieme delle interfacce, in quanto aveva esaurito completamente le risorse hardware dello switch Huawei. L'allocazione delle risorse di Huawei non era ottimizzata e non ha offerto scalabilità per questo caso di test. La documentazione di Huawei consiglia all'utente di unire le regole, cambiare un modello di risorsa hardware o passare a un approccio basato su VLAN.

Quando è stato applicato l'ACL a tutte le 48 porte di S5720-HI, l'interruttore ha impiegato molto tempo (in minuti) per l'attivazione degli ACL. Durante la modifica di un ACL su S5720-HI, il comportamento di implementazione è apparso difettoso e ha esposto la rete a una violazione della sicurezza. A causa dell'architettura delle risorse di switching, lo switch Huawei 5720-HI ha "consentito" che il traffico rifiutato fosse inoltrato durante una modifica dell'ACL. Al termine delle modifiche, la vecchia policy di sicurezza è stata rimossa dalle risorse hardware dello switch. Lo switch ha quindi riprogrammato le risorse con le istruzioni modificate. Non solo questo ha richiesto molto tempo, ma ha lasciato la rete in uno stato vulnerabile.



Fonte: Cisco

Durante le modifiche della policy, il PC è riuscito a scaricare un file dal server FTP che aveva una regola ACL per bloccare il traffico FTP come parte della policy configurata.

Fonte: Cisco

Lo switch S5720-HI ha anche lasciato passare migliaia di pacchetti rifiutati in ogni porta dello switch. Il sistema Spirent ha segnalato che, nel momento in cui la modifica dell'ACL è diventata efficace su tutte le porte dello switch Huawei, sono riusciti a passare attraverso ciascuna porta dello switch 70.000 pacchetti: più di 3,3 milioni di pacchetti che avrebbero dovuto essere bloccati. Questa è una violazione della policy che crea un'opportunità di violazione della sicurezza.

Lo stesso gruppo di test è stato eseguito sugli switch delle serie Catalyst 3K/9K. Gli switch Catalyst hanno supportato le modifiche (aggiunta/eliminazione) di policy ad alta velocità, con allocazione efficiente delle risorse per scalabilità e implementazione sicura. Grazie a funzioni come "ACL Label-Sharing" e "Hitless ACL updates", gli switch hanno supportato la programmazione della policy sulla rete senza compromissioni.

Operazioni di rete: modifiche della policy di sicurezza	Huawei S5720-HI	Cisco Catalyst 3850	Cisco Catalyst 9300
Numero totale di pacchetti (rifiutati) ricevuti per ogni switch	70.000 pacchetti per porta/ 3,3 milioni di pacchetti per switch	Zero	Zero

Fonte: Cisco

L'ACL è uno dei meccanismi più elementari utilizzati per la classificazione del traffico. Può essere usato per multicast, QoS e sicurezza. È fondamentale che la modifica delle voci per un caso d'uso specifico non influenzi altri casi d'uso operativi per i clienti. Mentre Cisco ha superato il test, Huawei non è riuscito a soddisfare questo requisito importante.

Alimentazione dei dispositivi connessi dallo switch

Uno dei motivi principali delle interruzioni dei servizi rete è l'interruzione dell'alimentazione. Assicurare il funzionamento continuo delle apparecchiature dell'infrastruttura di rete e dei dispositivi collegati, in caso di interruzione dell'alimentazione, è uno dei modi principali per mitigare questo problema. Con l'evoluzione dello standard Power over Ethernet (PoE) per offrire un'alimentazione sempre maggiore, da PoE (15,4 W), a PoE+ (30 W), a UPoE (60 W) fino a oltre 100 W (in futuro), sono sempre più numerosi i dispositivi che si connettono alla porta dello switch per l'accesso ai dati e all'alimentazione. Nell'organizzazione tipica vediamo dispositivi PoE tradizionali (telefoni IP, videocamere, wireless access point) e una nuova generazione di dispositivi IoT (sensori, luci LED collegate). Il funzionamento continuo di dispositivi come le luci e le telecamere di sorveglianza è estremamente critico.

Cisco sta facendo grandi sforzi per offrire alta disponibilità e alimentazione continua a questi dispositivi, anche quando lo switch che li alimenta perde alcune delle sue unità di alimentazione (PSU) o sta riavviando o aggiornando il software. Huawei dichiara di offrire alcune funzioni simili a Cisco, come il disaccoppiamento dei circuiti di alimentazione con hardware di switching o una

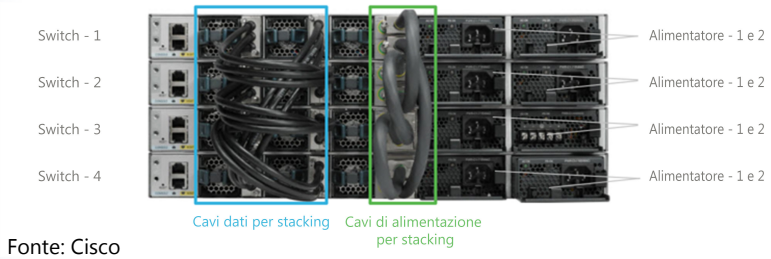
più veloce negoziazione dell'alimentazione, ma la realtà delle implementazioni aziendali non suffraga queste dichiarazioni.

I test eseguiti su processi e tecniche di alimentazione comparativi hanno esaminato due aspetti:

1. Fornire alimentazione ridondante agli stack di switch
2. Alta disponibilità per l'alimentazione (provisioning PoE più veloce e alimentazione senza interruzioni)

Alimentazione in stack

Abbiamo osservato che uno stack di switch di Cisco può condividere tutti gli alimentatori collegati tramite l'uso di speciali cavi di alimentazione di stacking. Grazie all'aiuto della tecnologia Cisco StackPower, la necessità di un apposito alimentatore esterno ridondante viene eliminata, con un conseguente risparmio di tempo e spazio. È possibile assegnare priorità a switch e porte specifiche, come con i dispositivi PoE collegati, per una maggiore disponibilità durante le interruzioni.



Fonte: Cisco

Cisco StackPower è stato testato creando uno stack di switch con un singolo alimentatore ridondante e collegando i seguenti dispositivi: un AP wireless, laptop wireless e cablati, un iPhone e varie luci con collegamento PoE. Venivano inviati continuamente dati ai laptop e all'iPhone e contemporaneamente abbiamo disattivato un alimentatore alla volta per vedere l'effetto sui dispositivi collegati. Abbiamo rilevato che, fino a quando lo stack di switch ha abbastanza capacità di alimentazione, fornisce l'energia rimanente ai dispositivi PoE. Dato che si trattava di un pool di alimentazione condiviso, non era importante quale particolare alimentatore fosse funzionante o meno.

Huawei non è riuscito a offrire questa capacità di pooling dell'alimentazione. L'unica alternativa per Huawei è stata quella di aggiungere un altro alimentatore ridondante per 4-6 switch, opzione che tuttavia richiede un investimento aggiuntivo in conto capitale, in termini di costi di acquisto e spazio richiesto, e ulteriori costi operativi di mantenimento e monitoraggio di sistemi di alimentazione sottoutilizzati.

Alta disponibilità dell'alimentazione PoE

Cisco offre due opzioni di alta disponibilità per i dispositivi connessi e alimentati da switch Cisco: Fast PoE (FPoE) e Perpetual PoE (PPoE).

Con Fast PoE, lo switch ricorda i requisiti di potenza dell'ultima alimentazione prelevata da una determinata porta e può ristabilire rapidamente l'alimentazione PoE dopo che l'alimentazione CA è stata ripristinata, senza attendere che il software dello switch si avvii completamente.

Per testare Fast PoE, è stato configurato uno switch Cisco 9300 per dispositivi PoE, utilizzando tre luci a LED, un wireless access point e un telefono IP. Cisco ha registrato l'energia prelevata da ogni dispositivo PoE nell'hardware per possibili eventi di interruzione dell'alimentazione. Gli switch hanno ripristinato velocemente l'energia non appena è stata riattivata l'alimentazione dello switch, senza aspettare che il sistema operativo dello switch si avviasse. Gli switch non hanno dovuto imparare di nuovo i parametri di ciascun dispositivo, risparmiando tempo prezioso nella riattivazione dei dispositivi PoE. I test eseguiti hanno rilevato che questo si verifica in 15-20 secondi dal ripristino dell'alimentazione.

Lo stesso test è stato poi eseguito con uno switch Huawei configurato in modo simile. Quando si è verificata l'interruzione dell'alimentazione e poi è stata ripristinata, lo switch ha eseguito il ciclo di riavvio completo prima di tornare ad alimentare i dispositivi PoE. Sono stati eseguiti più test e il ripristino dell'alimentazione PoE ha richiesto in media 3 minuti e 8 secondi con Huawei, contro i 15-20 secondi con Cisco: Huawei risulta perciò quasi 12 volte più lento di Cisco. Questo ritardo si è ulteriormente dilatato nel caso di Huawei perché anche i dispositivi PoE hanno richiesto altro tempo per l'avvio e la configurazione della connettività alla rete.

Fast PoE	Cisco	Huawei
Tempo medio di ripristino dell'alimentazione ai dispositivi PoE	17,5 secondi	3 minuti e 8 secondi

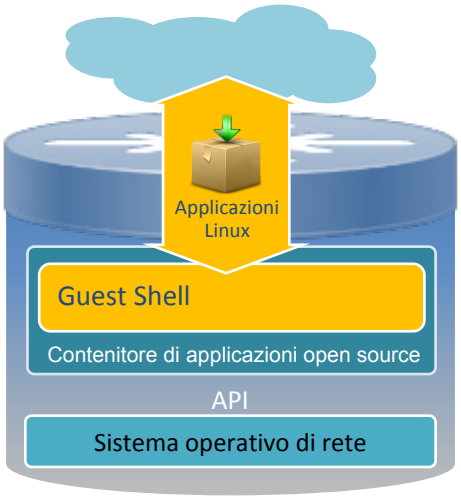
Con Perpetual PoE (PPoE) di Cisco l'alimentazione delle porte specificate è essenzialmente continua e ininterrotta. Per testare PPoE, sono state collegate molte luci con PoE alle porte degli switch Huawei e Cisco designate come PPoE. L'alimentazione degli switch non si è interrotta in quanto ogni switch era riavviato dal software. È stato misurato il tempo di spegnimento delle luci e loro riaccensione. I risultati riportati di seguito mostrano che con PPoE i dispositivi non hanno perso l'alimentazione dopo il riavvio software dello switch Cisco, mentre i dispositivi PoE sullo switch Huawei hanno perso l'alimentazione per una media di 12 secondi. Qualsiasi interruzione dell'alimentazione causa il riavvio del dispositivo PoE connesso, il che aggiunge altro tempo di interruzione dell'operatività, cosa inaccettabile quando allo switch sono collegati dispositivi critici.

Perpetual PoE	Cisco	Huawei
Tempo medio di spegnimento delle luci dopo il riavvio dello switch	0 secondi (le luci non si sono spente)	12 secondi in media (da 8 a 16 secondi)

Per riepilogare, Cisco StackPower offre vantaggi esclusivi rispetto a Huawei mettendo in pool gli alimentatori delle singole fonti per abilitare la resilienza. Cisco Fast PoE e Perpetual PoE offre alta disponibilità a tutti i dispositivi connessi con PoE quando il dispositivo viene riavviato, intenzionalmente o involontariamente.

Miglioramenti e programmabilità del software

Durante i test si è notato che il più recente software di switch Cisco si è evoluto, dal monolitico IOS del passato, in un sistema operativo più moderno e programmabile. Gli switch di Cisco testati possedevano la più recente versione 16.6.1 di IOS XE, che esegue le funzionalità IOS come un'applicazione sopra un kernel Linux. Con il kernel Linux, Cisco è in grado di offrire agli utenti e agli sviluppatori l'accesso completo a una Guest Shell Linux tramite numerose interfacce di programmazione, incluse quelle di hosting delle applicazioni.



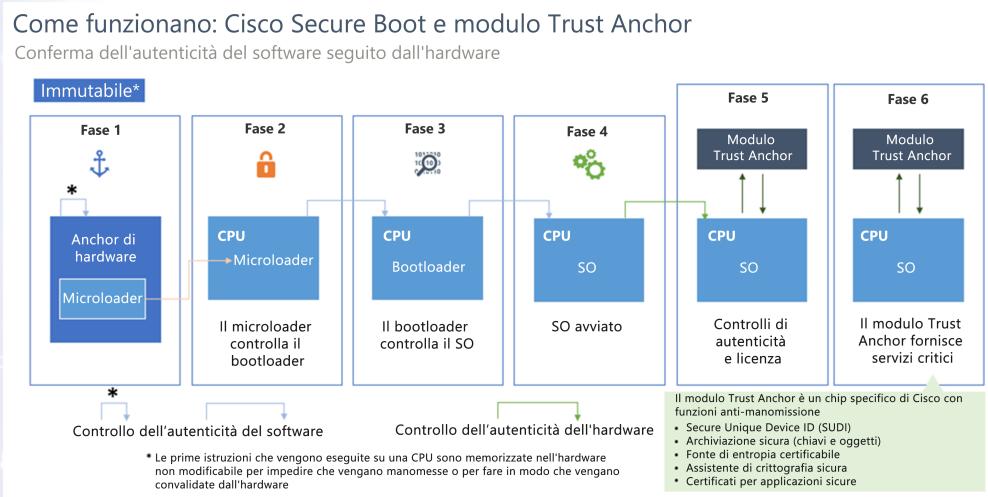
- Cisco IOS-XE ha la capacità di ospitare applicazioni basate su Linux tramite la funzionalità Guest Shell e questo rende possibili molti scenari d'uso per l'infrastruttura di rete. Guest Shell consente ai clienti di utilizzare e installare in modo sicuro applicazioni Linux note e comuni, come YDK (Yang Development Kit), programmazione a oggetti Python, supporto del protocollo per NETCONF (IETF Network Configuration Protocol) e RPC (remote procedure call), codifica JSON (Java Script Object Notation) e XML e molto altro. In questo modo permette di ospitare ed eseguire applicazioni Linux aperte, garantendo al tempo stesso che non danneggino alcuna funzionalità critica dello switch (per esempio riavviando lo switch dalla shell, alterando il kernel o provocando un'interruzione dell'operatività del dispositivo mentre è in modalità di produzione).
- Uno dei vantaggi di una Guest Shell basata su Linux è che consente ai clienti di utilizzare qualsiasi linguaggio di scripting disponibile in Linux per eseguire attività di automazione di base on-box. Uno di questi linguaggi è Python, che è supportato come linguaggio di programmazione integrato in Cisco Polaris Guest Shell.

- Per valutare Guest Shell abbiamo usato uno script di automazione eseguito sullo switch come un "agente" e, per ogni modifica di configurazione rilevata, veniva inviata all'amministratore un'e-mail di notifica delle modifiche rilevate. È stato possibile configurare facilmente il Guest Shell Linux per il ruolo di server di posta, da cui sono state automatizzate le e-mail di notifica tra lo switch e l'amministratore. Quindi è stato eseguito l'agente di script Python in Guest Shell.
- Mentre l'agente era in funzione, abbiamo apportato diverse modifiche alla configurazione dello switch, e le e-mail di notifica sono state inviate immediatamente all'amministratore. Con il codice Python abbiamo potuto impostare l'indirizzo e-mail dell'amministratore. Nei prodotti valutati in questo report, Huawei non ha alcuna funzionalità che sia equivalente alla Guest Shell di Cisco.

5 - Affidabilità: sicurezza della rete

Abbiamo osservato anche diverse funzionalità nuove che rafforzano la sicurezza della rete e del sistema e la capacità dell'utente di monitorare e identificare problemi e minacce. Fra questi gli aspetti più importanti sono:

- **Firma delle immagini**: per la protezione contro l'uso di immagini contraffatte e per garantire che l'immagine non sia stata modificata o manomessa, viene utilizzato il software di firma digitale. La firma del codice utilizza un algoritmo di hash, simile a un checksum; l'hash viene quindi criptato utilizzando una chiave di firma. Il codice firmato viene controllato al run-time e convalidato da un elemento del sistema attendibile per garantire che non è stato modificato. L'elemento attendibile è una parte di codice nota per essere autentica e che non può cambiare (non modificabile).
- **Secure Boot**: assicura che venga avviato solo il software Cisco autentico (attraverso un processore sicuro, la memoria e la ROM di boot) sulla piattaforma Cisco. Questo migliora la firma delle immagini utilizzando un trust anchor hardware, anche questo non modificabile, e impedisce molti attacchi fisici e di sostituzione dei componenti.



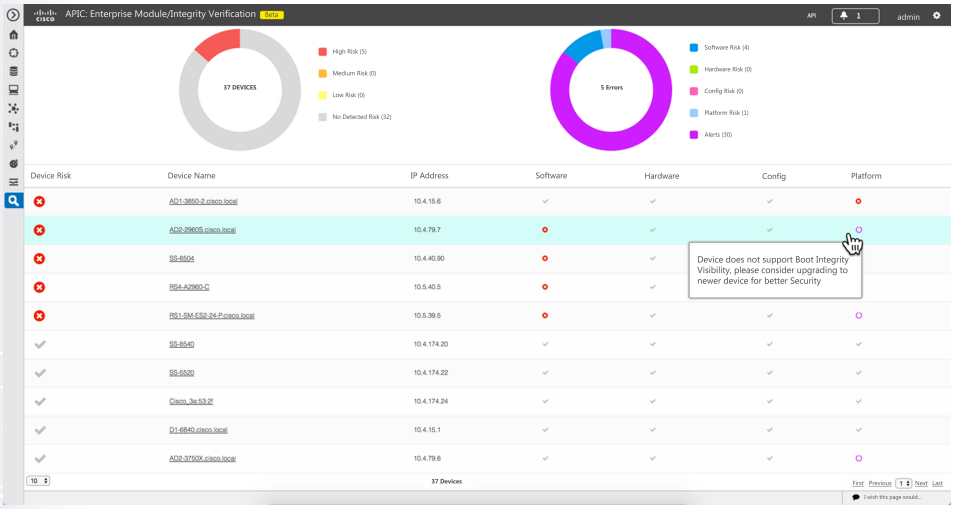
Fonte: Cisco

- **Modulo Trust Anchor (TAm)**: è uno speciale chip anti-furto e anti-manomissione progettato con funzioni di crittografia integrate che fornisce la protezione sia dell'utente finale sia della filiera di approvvigionamento. La protezione degli utenti finali include l'archiviazione estremamente sicura delle credenziali dell'utente, delle password ecc., mentre la protezione della filiera di approvvigionamento prevede l'inserimento del Secure Unique Device Identifier (SUDI) durante la produzione per convalidare l'autenticità dell'hardware, ovvero per garantire che si tratti di un prodotto Cisco originale. A differenza di soluzioni generalizzate come Trusted Platform Module (TPM),

che sono l'ideale per dispositivi di elaborazione per scopi generici come server e PC, Cisco TAm è l'ideale per i dispositivi di elaborazione integrati come router e access point Wi-Fi, per garantire protezione in combinazione con Secure Boot dagli attacchi di manomissione del firmware nella filiera di approvvigionamento e firmware basati sul possesso fisico.

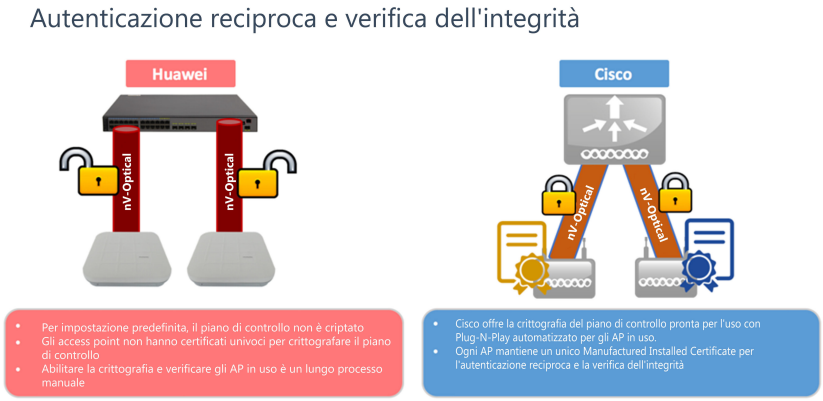
- **Difese di run-time**: garantiscono la protezione contro i continui attacchi da remoto di overflow del buffer e Return-Oriented Programming (ROP), diffondendo le best practice di sviluppo di software e hardware. Le prassi Cisco utilizzano librerie sicure e tecniche come Address Space Layout Randomization (ASLR), X-Space e altre che rendono estremamente difficile per gli hacker capire quale punto della memoria violare, offrendo così resilienza e riduzione del rischio dagli attacchi ROP

Le reti Cisco per campus possono anche utilizzare APIC-EM: Application Policy Infrastructure Controller - Enterprise Module. Si tratta di un unico punto per la gestione automatizzata dell'intero fabric di infrastruttura: risorse sia fisiche che virtuali. Il "Trustworthy Dashboard" di APIC-EM fa parte del suo modulo "Integrity Verification", come illustrato di seguito, che monitora tutti i livelli dell'infrastruttura.



Fonte: Cisco

- **Protezione del piano di controllo**: il canale di comunicazione tra gli access point e il controller per lo scambio sicuro delle configurazioni e delle informazioni sui client wireless. Per impostazione predefinita, Cisco protegge il canale del piano di controllo sfruttando gli esclusivi Manufactured Installed Certificate (MIC) per la mutua autenticazione e la crittografia, mentre Huawei sceglie di mantenere il canale di controllo non criptato pronto per l'uso. Un canale non protetto rende Huawei passibile di attacchi remote replay packet e man-in-the-middle che possono compromettere l'identità dell'utente wireless. L'approccio di Huawei per la protezione del piano di controllo è un processo manuale impegnativo e difficile, poiché si basa sull'utilizzo privato di una chiave privata segreta (PSK) per ogni access point.



Fonte: Cisco

6 - Riepilogo

Dalla valutazione è emerso che, nonostante Cisco e Huawei offrano entrambi componenti paragonabili per la realizzazione di un'infrastruttura di rete wireless e cablata per campus, per ogni test il pacchetto Cisco ha dimostrato di offrire più vantaggi rispetto a Huawei. Cisco ha mostrato prestazioni superiori rispetto alla soluzione wireless Huawei, con una piattaforma di sicurezza, hardware, software e gestione delle risorse estremamente evoluta per fornire il sistema più ottimizzato e affidabile a ogni cliente.

Potenza ed efficienza del segnale radio. Entrando nel merito del funzionamento e delle prestazioni wireless, è stato rilevato che Cisco emette livelli di segnale più bassi ed efficienti rispetto a Huawei per la stessa esatta configurazione e implementazione a 180 client. La connettività per client sulle reti per campus a sei AP è risultata distribuita in modo più uniforme nell'infrastruttura Cisco. Più degna di nota è la capacità degli AP Cisco di adattare automaticamente il segnale radio da 2,4 GHz a 5 GHz per una copertura ottimale dei client.

Prestazioni elevate. I test delle prestazioni hanno dimostrato che gli AP Cisco sono in grado di raggiungere il 15-22% in più di throughput aggregato nella modalità dual-band. Quando due dei sei AP Cisco sono passati automaticamente alla modalità dual 5 GHz, le prestazioni sono aumentate del 40%.

QoS delle videochiamate e rilevamento delle interferenze. Durante lo streaming di video attivo, Cisco ha sostenuto più sessioni di Huawei utilizzando lo stesso traffico e ambiente client. La capacità di Cisco di rilevare correttamente e identificare le sorgenti di interferenze Wi-Fi è stata molto superiore a quella di Huawei.

Gestione del failover impressionante. I test di alta disponibilità hanno dimostrato che Cisco offre prestazioni di failover e tempi di attività wireless migliori per utenti e applicazioni.

Encrypted Traffic Analytics. Cisco offre alcuni strumenti innovativi con cui le imprese possono identificare le applicazioni e proteggere la rete da minacce avanzate nascoste all'interno del traffico criptato, senza compromettere la privacy.

Risorse hardware protette e ottimizzate. Gli switch Cisco Catalyst hanno dimostrato di supportare la programmazione della policy della rete senza subire compromissioni. Abbiamo osservato invece che gli switch Huawei hanno lasciato passare dati che dovevano essere bloccati durante le modifiche dell'ACL.

Alta disponibilità per i dispositivi PoE. Cisco StackPower offre vantaggi esclusivi rispetto a Huawei. Cisco Fast PoE e Perpetual PoE offrono alta disponibilità a tutti i dispositivi connessi con PoE quando il dispositivo viene intenzionalmente o involontariamente riavviato

Programmabilità del software. La programmabilità di Cisco IOS-XE supporta tecnologie che semplificano l'automazione e il provisioning e rendono più efficienti le attività di gestione della rete.

Affidabilità. Gli affidabili sistemi Cisco costituiscono la base per una rete dall'architettura sicura.

7 - Informazioni sui test "Performance Verified" di Miercom

Questo report è stato sponsorizzato da Cisco Systems, Inc. Tutti i dati sono stati ottenuti in modo indipendente da tecnici e personale addetto ai test di laboratorio di Miercom come parte della nostra valutazione "Performance Verified". I test come questi si basano su una metodologia sviluppata insieme al fornitore che sponsorizza l'iniziativa. Gli scenari di test sono progettati in modo da verificare specifiche dichiarazioni del fornitore che sponsorizza l'iniziativa, con lo scopo di confermare o smentire tali dichiarazioni. I risultati sono presentati in un report come questo, pubblicato in modo indipendente da Miercom.

8 - Informazioni su Miercom

Miercom ha pubblicato centinaia di analisi comparative di prodotti di rete sui principali periodici del settore e altre pubblicazioni di rilievo. La fama di Miercom come azienda leader indipendente nel campo dei test di prodotti è indiscussa.

Tra i servizi privati offerti figurano analisi di prodotti della concorrenza, nonché valutazioni di singoli prodotti. Miercom vanta programmi completi di certificazione e di testing, tra cui Certified Interoperable, Certified Reliable, Certified Secure e Certified Green. È inoltre possibile che i prodotti vengano valutati nell'ambito del programma Performance Verified, lo strumento più approfondito e affidabile del settore per determinarne l'usabilità e le prestazioni.

9 - Utilizzo di questo report

Nonostante siano stati adottati tutti i provvedimenti del caso per garantire l'accuratezza dei dati presenti in questo report, è possibile che siano stati commessi errori e/o vi siano state sviste. Le informazioni fornite sono basate su vari strumenti di testing, sulla cui precisione non è possibile offrire garanzie. Inoltre, il documento attinge a determinate dichiarazioni da parte dei fornitori che, sebbene verificate in misura ragionevole da Miercom, non è stato possibile controllare in termini di certezza assoluta.

Miercom mette quindi a disposizione il presente documento "così com'è", non rilasciando alcuna garanzia o dichiarazione, non assumendosi alcun impegno (esplicito o implicito) e declinando ogni responsabilità legale (diretta o indiretta) in merito all'accuratezza, alla completezza, all'utilità o all'idoneità delle informazioni contenute al suo interno.