

La Differenza Aruba

L'architettura 'mobile edge' di Aruba fornisce caratteristiche e benefici superiori a soluzioni cablate e Wireless LAN concorrenti. Con la soluzione 'mobile edge' di Aruba, le aziende possono trasformare la rete in un vantaggio competitivo grazie a una forza lavoro resa altamente mobile e dotata di accesso istantaneo alle informazioni. Allo stesso tempo i ridotti costi di infrastruttura, la sicurezza migliorata e l'accresciuta flessibilità forniscono un significativo vantaggio economico.

Solo Aruba è in grado di fornire:

1. Sicurezza basata sull'identità per proteggere la rete e gli utenti mobili

Il 'mobile edge' è per definizione mobile. Sul 'mobile edge' qualunque utente può comparire in qualsiasi posto e in qualunque momento, perciò la rete deve riconoscere l'utente o il dispositivo in base alla sua identità. La sicurezza basata sull'identità risolve i problemi di sicurezza applicando regole alle persone piuttosto che alle porte della rete, permettendo soltanto l'accesso appropriato al ruolo di business dell'utente.

2. Integrazione non invasiva nelle reti esistenti

Il 'mobile edge' deve essere caratterizzato da un costo conveniente per poter godere di un'adozione estensiva. Le implementazioni del 'mobile edge' non devono forzare aggiornamenti della rete su larga scala o cambiamenti all'infrastruttura esistente, tanto meno devono obbligare a momenti di fermo della rete. Il 'mobile edge' deve integrarsi negli strumenti di gestione esistenti, nei sistemi di monitoraggio della sicurezza e nelle procedure di verifica.

3. Convergenza sicura per VoIP mobile e servizi dati

Il 'mobile edge' deve essere multi-servizio. Sul 'mobile edge' la voce è un servizio

fondamentale. Voice over wireless LAN (VoWLAN) fornisce tutti i benefici di mobilità della rete cellulare e i risparmi del VoIP e non richiede costosi upgrade degli armadi di cablaggio. I nuovi apparecchi telefonici dual-mode operano attraverso la Wireless LAN dell'azienda ogniqualvolta sia disponibile e attraverso la rete cellulare pubblica in tutti gli altri casi, fornendo una mobilità-voce realmente conveniente per gli utenti.

4. Gestione radio adattativa per WLAN autoconfiguranti

Il 'mobile edge' richiede un controllo adattativo della copertura radio. La trasmissione in radiofrequenza (RF) è una parte intrinseca del wireless, parte con la quale molti amministratori di rete non hanno familiarità. L'obiettivo di qualsiasi deployment wireless è di fornire la copertura richiesta garantendo al contempo le massime prestazioni. Data la natura pervasiva del wireless nel 'mobile edge', la messa a punto della RF non può essere un'operazione manuale da eseguirsi ad opera dell'amministratore di rete. La gestione RF deve essere interamente automatica, affidabile e adattabile.

5. Attivazione remota di hotspot aziendali istantanei

Il 'mobile edge' si muove con l'utente. Gli utenti si muovono al di fuori delle mura dell'azienda e continuano ad avere bisogno di accedere alle reti voce e dati aziendali. Lasciati soli con i propri dispositivi, gli utenti creeranno la propria versione di 'mobile edge' ovunque ne abbiano bisogno – usando DSL o connessioni via cavo a casa, reti wireless aperte presso hotspot pubblici, collegandosi a jack Ethernet nelle stanze d'Hotel o connettendosi attraverso reti wireless pubbliche come GSM o EVDO. Per evitare i problemi di supporto e di sicurezza causati da quest'approccio, il

'mobile edge' deve estendere on-demand la connettività voce e dati attraverso Internet per creare hotspot personali sicuri ovunque gli utenti debbano lavorare. Questi hotspot si muovono con l'utente, ma il controllo e la configurazione restano appannaggio dell'amministratore di rete.

6. Scalabilità, affidabilità e performance di livello Enterprise

Il 'mobile edge' deve essere affidabile. Per realizzare in pieno i benefici del 'mobile edge', esso deve fornire performance prevedibili e consistenti, nonché un'elevata affidabilità. Il sistema deve riprendersi da qualunque guasto ai suoi componenti senza che nessuna interruzione del network sia percepibile da parte degli utenti. Le prestazioni devono incontrare tutti i requisiti delle applicazioni mobili e devono restare uniformi anche negli ambienti RF più difficili. Infine, il 'mobile edge' deve crescere di pari passo con l'impresa senza richiedere l'aggiunta di persone dedicate alla sua gestione.

7. Piattaforma di mobilità aperta per lo sviluppo e per l'integrazione

Il 'mobile edge' è una tecnologia abilitante per il business. Nuove applicazioni mobili possono creare nuove opportunità e migliorare le attuali, creando vantaggi competitivi per gli utilizzatori della tecnologia. Applicazioni come la voce, la localizzazione e il rintracciamento, le reti di sensori sono le prime applicazioni puramente mobili e altre sono in fase di sviluppo nel momento in cui le reti mobili diventano più pervasive. In aggiunta alle applicazioni mobili, nuovi servizi continuano ad essere sviluppati per la sicurezza – come il bloccaggio dello spyware basato sulla rete – e per la convergenza – come il trasferimento tra fisso e mobile e la localizzazione delle chiamate di emergenza.

ARUBA™
The Mobile Edge Company



**La Linea di Prodotti
Aruba Mobile Edge**

Distribuito in Italia da:

ARUBA™
The Mobile Edge Company

1322 Crossman Ave.
Sunnyvale, CA 94089-1113
Phone: 408-227-4500
Fax: 408-227-4550
Web: www.arubanetworks.com



Via del Commercio, 69
44100 Ferrara
Phone: +39-0532-783411
Fax: +39-0532-783499
Web: www.icos.it

I Prodotti

Il sistema 'mobile edge' di Aruba consiste di tre componenti:

1. Il software di sistema ArubaOS che fornisce tutta l'intelligenza per il 'mobile edge'
2. I Mobility controller che sono piattaforme centralizzate per la fornitura di servizi nel contesto del 'mobile edge'.
3. Gli Access point (AP) controllati che convogliano il traffico cablato e wireless degli utenti verso i mobility controller attraverso la LAN, la WAN e Internet

Software di sistema ArubaOS

Robusta e sofisticata suite software, ArubaOS coordina tutte le operazioni del 'mobile edge' grazie a capacità avanzate che includono: mobilità senza interruzioni, sicurezza basata sull'identità, integrazione non invasiva nelle reti esistenti, capacità VoIP mobili, gestione adattativa della rete radio, API aperte, qualità del servizio end-to-end e gestione centralizzata. ArubaOS è un software completamente modulare che viene eseguito su tutti i mobility controller e access point controllati di Aruba, consentendo loro di operare senza interruzioni nel fornire servizi agli utenti del 'mobile edge'. Le funzionalità di base di ArubaOS sono incluse in ogni mobility controller e comprendono autenticazione e crittografia avanzate, mobilità senza interruzioni con roaming veloce, gestione della radiofrequenza e strumenti di analisi, configurazione centralizzata, localizzazione degli utenti e altro ancora. ArubaOS fornisce agli amministratori un singolo punto di controllo da cui localizzare e disattivare eventuali AP non autorizzati, identificare e bloccare attacchi alla rete o accessi indesiderati, bilanciare il traffico, individuare "buchi" ed interferenze nella copertura radio e creare

policy di sicurezza che seguono l'individuo nel momento in cui esso si muove attraverso il 'mobile edge'. Dal momento che tutti i mobility controller Aruba utilizzano la stessa architettura hardware, Aruba OS è completamente portabile attraverso l'intera gamma, offrendo le stesse funzionalità con prezzi e prestazioni differenti a seconda dei mobility controller implementati. ArubaOS è completamente modulare, con una particolare enfasi sulle caratteristiche di affidabilità come il riavvio automatico dei processi per minimizzare l'impatto dei guasti software e una piena ridondanza VRRP che include processori e chassis per minimizzare l'impatto di guasti hardware.

ArubaOS include i seguenti moduli software opzionali:

Wireless Intrusion Protection

fornisce una tecnologia di classificazione brevettata che identifica e protegge contro attacchi come 'denial of service', da vulnerabilità come AP non autorizzati, impersonificazione di client e AP, e attacchi 'man-in-the-middle'.

Policy Enforcement Firewall

applica a utenti e gruppi policy di sicurezza attraverso un firewall stateful integrato, certificato ICSA. Le policy possono essere definite centralmente ed applicate per utente o per gruppo, seguendo gli utenti nel momento in cui essi si muovono. Le policy sono applicate dinamicamente, tenendo in considerazione una

varietà di metriche come la localizzazione dell'utente, l'ora del giorno, il tipo di dispositivo, il metodo di autenticazione e altro.

VPN Server supporta l'integrazione con una varietà di implementazioni 'virtual private network', eliminando la necessità di concentratori VPN esterni. L'accelerazione hardware fornisce connettività VPN alla velocità della LAN. I

protocolli VPN supportati includono L2TP/IPsec, IPsec/XAUTH e PPTP. Sono supportate sia le VPN da sito a sito che la terminazione sui client.

Client Integrity fornisce integrazione, attraverso rete cablata e wireless, con strumenti per assicurare l'integrità dei client e proteggere la rete contro l'infezione da virus e worm che possono attaccare i dispositivi mobili. Il modulo Client Integrity si integra con il software di sicurezza di Sygate Technologies.

Remote AP consente ai gestori della rete di estendere in modo sicuro le funzionalità wireless dell'azienda a qualsiasi locazione che disponga di un collegamento ad Internet. Gli AP remoti garantiscono agli utenti casalinghi, agli uffici remoti o ai lavoratori che accedano da qualunque luogo, una connettività WLAN uguale a quella ottenibile in sede.

External Services Interface

consente a qualunque mobility controller Aruba di comunicare con dispositivi di servizio esterni. Il modulo ESI ridirige il traffico di rete in modo selettivo, in base a policy, verso dispositivi che forniscono servizi di rete in linea, come anti-virus, intrusion detection, content filtering, trasformazione dei contenuti e monitoraggio dell'utilizzo. Sono pienamente supportati load balancing e verifica di funzionalità (health checking).

Advanced AAA estende le caratteristiche di autenticazione e autorizzazione fornite in ArubaOS. Le funzionalità fornite includono selezione di authentication server in funzione del dominio, e autenticazione ed autorizzazione virtuali utilizzando RFC 3576 e API XML per costruire portali e sistemi esterni di autenticazione.

xSec fornisce la terminazione per sessioni client altamente sicure di tipo xSec, offrendo crittografia a 256-bit AES-CBC sul link con completo oscuramento dell'header per ambienti fortemente sensibili alla sicurezza. Il modulo xSec abilita inoltre la crittografia delle porte trunk tra mobility controller Aruba, utilizzando lo stesso standard crittografico altamente sicuro.



Mobility Controller

I mobility controller sono piattaforme di networking ad alte prestazioni costruite specificamente per eseguire funzioni centralizzate di ArubaOS, come la gestione dell'accesso degli access point controllati, la gestione del protocollo 802.11, autenticazione e crittografia 802.11x, VPN con encryption Ipsec/3DES, firewall, protezione dalle intrusioni L1-L7, verifica dell'integrità dei client, roaming senza interruzione degli utenti tra diversi access point e tra mobility controller. Tutti i mobility controller condividono la stessa architettura hardware che include un processore di controllo dedicato, un'unità di processo dei dati di rete programmabile ad alte prestazioni ed un motore crittografico programmabile per encryption di livello 2 e 3. Essi aggregano il traffico proveniente dal 'mobile edge', lo ispezionano e lo forniscono alla rete 'core' dell'azienda. I mobility controller sono tipicamente posizionati nei data center, per godere di un ambiente controllato e di un accesso ad alta velocità alla rete principale, dal momento che gestiscono il traffico proveniente da centinaia di AP e migliaia di utenti. La linea di mobility controller Aruba include diversi modelli, di configurazione e prezzo variabili per rispondere alle esigenze di reti mobili di diverse dimensioni.



Aruba 6000 è il solo mobility controller modulare sul mercato. Il suo chassis modulare a quattro slot supporta fino a 8 Gbps di throughput in chiaro (7.2 Gbps crittografato), fino a 72 porte 10/100 Mbps, 8000 utenti simultanei e da 4 a 512 AP. Gli slot per schede rimovibili a caldo supportano opzioni di connettività multiple tra cui una scheda 24 porte Fast Ethernet + 2 porte Gigabit Ethernet e una scheda 2 porte Gigabit Ethernet.



Aruba 2400 è un mobility controller impilabile a 24 porte che supporta 48 AP. Progettato per sedi regionali o installazioni in edifici ad alta densità di utenti, Aruba 2400 supporta fino a 512 utilizzatori simultanei e fornisce fino a 400 Mbps di throughput crittografato.



Aruba 800 è un mobility controller a configurazione fissa progettato per piccole applicazioni o per filiali remote. Aruba 800 fornisce otto porte utente 10/100 Mbps e un uplink gigabit in rame o fibra. La crittografia hardware programmabile supporta fino a 200 Mbps di traffico full-duplex crittografato.

Access Point controllati

Controllati centralmente dal software ArubaOS, gli Access Point cablati o wireless di Aruba fungono da raccoglitori distribuiti di traffico, convogliandolo ai mobility controller attraverso la rete IP. Gli AP wireless forniscono copertura radio e servizi di connettività end-user fungendo al contempo da dispositivi di sorveglianza che controllano costantemente l'area coperta alla ricerca di minacce alla sicurezza basate sulla radiofrequenza. Inoltre eseguono funzioni di protezione dalle intrusioni quando le minacce wireless siano individuate. Gli AP wireless eseguono anche le funzioni distribuite di ArubaOS come la gestione adattativa della copertura radio, l'encryption distribuita per il forwarding locale di traffico Wireless LAN, l'individuazione e protezione da intrusioni wireless, l'individuazione di AP non autorizzati e altro. Gli AP cablati fungono semplicemente da collettori di traffico allo scopo di convogliarlo attraverso la LAN o la WAN verso un mobility controller Aruba. Aruba offre un'ampia gamma di AP controllati, tra cui access point indoor e outdoor 802.11a/b/g a singola radio, access point 802.11a/b/g a doppia radio,

access point cablati 802.3 e access point ibridi cablati/wireless. Gli AP WLAN sono equipaggiati con un'antenna integrata o possono opzionalmente essere collegati ad una varietà di antenne esterne. Tutti gli AP controllati lavorano con tutti i mobility controller Aruba per fornire un 'mobile edge' sicuro e ad alte prestazioni. Connessi ad una rete IP esistente, gli AP scopriranno automaticamente un Aruba mobility controller, si autoconfigureranno e cominceranno ad operare. Il mobility controller è responsabile per il downloading delle immagini software, la configurazione e il coordinamento di tutti gli AP controllati. Gli AP sono alimentati attraverso il Power over Ethernet (PoE) 802.3af, eliminando la necessità di ulteriori cablaggi. Sono anche equipaggiati con jack in corrente continua che funzionano con alimentatori AC se PoE non è disponibile. Tutti gli AP possono fornire simultaneamente servizi wireless e monitoraggio dell'area radio coperta. Essi scansionano continuamente l'ambiente RF, localizzando e tenendo traccia di tutti i client wireless in modo da fornire avviso di intrusione o interferenza. Questa doppia funzionalità elimina il bisogno di uno strato separato di sensori RF per individuare guasti e ottimizzare l'ambiente wireless. Gli AP controllati di Aruba sono disponibili in una varietà di forme e capacità.

Aruba 41 è un AP a singola radio di basso costo progettato per i telelavoratori o per l'home office. Dotato di una singola antenna integrata e Power over Ethernet 802.3af, Aruba 41 è un AP ideale per situazioni dove diversità d'antenna e installazione a controsoffitto non sono fattori critici.



Aruba 60 e 61 sono AP a singola radio, 802.11a o b/g progettati per essere messi in opera in implementazioni wireless molto 'dense' presso gli uffici aziendali. Certificati per l'installazione nelle controsoffittature ('plenum rated') e alimentati da Power over Ethernet 802.3af o attraverso un adattatore AC esterno opzionale, i modelli Aruba 60 e 61

La Sfida

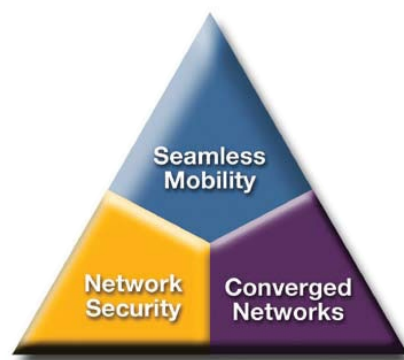
I network manager devono fronteggiare tre principali tendenze dell'IT: mobilità, sicurezza e convergenza. La mobilità è fortemente richiesta dagli utenti attraverso tecnologie come Wireless LAN, telefoni cellulari e VPN, per portare avanti le funzioni di business in ufficio, in viaggio e a casa. La sicurezza di rete, la protezione delle informazioni contro pubblicazioni non autorizzate, alterazioni o distruzione è diventata sempre più importante nell'era degli internet worm, dei virus e degli spyware. La sicurezza ha inoltre assunto crescente importanza negli Stati Uniti, nell'Unione Europea, nella regione Asia-Pacifico ed altre zone, a causa dell'introduzione di nuove legislazioni correlate alla privacy, alla confidenzialità e all'integrità dei dati finanziari. Infine, le reti convergenti che supportano sia dati che voce offrono significativi benefici finanziari e supportano una più ricca comunicazione d'impresa grazie all'integrazione della multimedialità.

Tutti questi trend si intersecano al limite

più esterno della rete (in inglese 'edge') – il punto in cui gli utenti si collegano ai servizi dell'azienda. L'estremità delle attuali reti aziendali, costruita sulla tecnologia degli ultimi dieci anni, è oggi un confine 'fisso'. È stato progettato per periodi in cui utenti e dispositivi non erano mobili ed il wireless era un prodotto puntuale utilizzato esclusivamente nei magazzini e nelle fabbriche. L'edge delle reti di oggi è altamente affidabile ed estremamente semplice. Quando gli utenti si connettono a una porta, la rete provvede a fornire loro un accesso ad alta velocità. Ma questa semplicità non coincide con la sicurezza – la rete non fa distinzioni tra utenti autorizzati e non autorizzati, e non può prendere decisioni su quale accesso garantire a determinati utenti. Il network attuale è stato costruito con lo scopo di fornire dati nel modo più efficiente possibile. È stato costruito prima che esistesse l'alimentazione elettrica attraverso Ethernet (Power over Ethernet, PoE) e prima che fossero necessarie policy di Quality of Service per assicurare

un'alta qualità alle comunicazioni in voce attraverso la rete dati.

La rete di oggi può essere aggiornata per indirizzare la mobilità, la sicurezza e la convergenza. L'upgrade può essere sostanziale, includendo ogni armadio switch, ogni router di filiale, ogni core router e addirittura l'impianto di cablaggio stesso. La sfida per il network manager è di supportare i tre trend in modo gestibile ed affidabile – senza l'invasività e i costi impliciti in un upgrade massivo della rete.



La Soluzione

Il sistema 'mobile edge' di Aruba abilita una nuova tipologia di 'edge' per la rete delle aziende: l'estremità mobile. Il 'mobile edge' consente ad utenti e dispositivi di connettersi senza fili e a qualsiasi rete, per ottenere accesso sicuro alle risorse dell'impresa. Si tratta di un nuovo 'strato' del network che si posiziona logicamente al di sopra della rete fissa e soddisfa i requisiti di sicurezza, mobilità e convergenza senza richiedere aggiornamenti sostanziali alla rete esistente. Il 'mobile edge' è progettato per lavorare in modo sicuro al di sopra delle infrastrutture della rete IP e

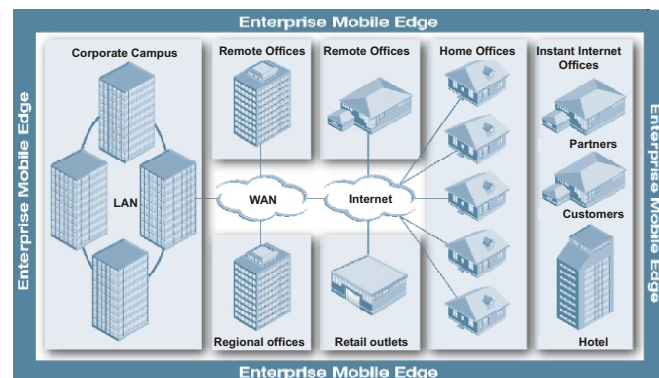
si estende attraverso sia le reti private che attraverso Internet.

Il 'mobile edge' per definizione supporta una reale mobilità, per cui gli utenti possono spostarsi senza interruzioni e in modo sicuro attraverso locazioni multiple. Inoltre fornisce la convergenza delle comunicazioni in voce attraverso dispositivi multimediali e apparecchi telefonici di tipo 'Voice over Wireless LAN' (VoWLAN), con alta qualità ed affidabilità. Questo elimina la spesa non indifferente di aggiungere porte VoIP alla rete fissa. Inoltre, il 'mobile edge' è costruito con il concetto di sicurezza basata sull'identità.

che questa identità sia riconosciuta, policy di sicurezza personalizzate possono essere applicate in modo che venga fornito solo il tipo di accesso appropriato alle esigenze di business dell'utente o del dispositivo che lo richiede. Tutto ciò migliora drasticamente la sicurezza, eliminando privilegi in eccesso e fornendo un controllo basato sull'identità.

Il 'mobile edge' non risolve soltanto le sfide della mobilità, sicurezza e convergenza, ma fornisce allo stesso tempo un percorso per ridurre i costi complessivi dell'infrastruttura di rete. Nel lungo periodo, la naturale evoluzione del limite estremo della rete aziendale è prevalentemente verso la mobilità. Quando questo accade, si realizza una radicale trasformazione delle dinamiche economiche relative alla rete, dal momento che si possono eliminare i costi di cablaggio e i costi relativi a operazioni di spostamento, aggiunta o cambiamento di apparati.

Utenti e dispositivi mobili, per definizione, non si connettono alla rete attraverso una porta fissa. Per questa ragione, la rete deve identificare ogni utente che si collega. Una volta



forniscono capacità, performance e copertura superiori. Aruba 61 presenta un'antenna integrata omnidirezionale 802.11a/b/g, mentre Aruba 60 è fornito di doppio connettore per antenne esterne. Aruba 60 e 61 sono i perfetti AP per ambienti 'Wireless Grid' ad alta densità.



Aruba 65 è un AP a doppia radio 802.11a/b/g AP progettato per il lavoratore mobile o per quello costantemente in viaggio. Dotato di antenne diversity integrate, Power over

Ethernet 802.3af, un alimentatore esterno e un design compatto, Aruba 65 sta facilmente in una valigetta e si connette ovunque l'utente mobile si sposti.

Aruba 70 è il primo AP a doppia radio 'ibrido', che fornisce contemporaneamente servizi 802.11a e 802.11b/g, così come accesso cablato attraverso una porta Ethernet aggiuntiva. Aruba 70 è un dispositivo multi-purpose che può funzionare sia come access point che come monitor RF – in modo indipendente o concorrente – attraverso bande di 2.4 GHz e 5 GHz. Adatto ad installazioni nella controsoffittatura o nello



Le Applicazioni

Il 'mobile edge' è una tecnologia abilitante per nuove applicazioni che possono fornire maggiore produttività, costi inferiori miglioramenti alla sicurezza e un più veloce accesso alle informazioni. Il 'mobile edge' abilita diverse applicazioni nelle aree della mobilità, della sicurezza e della convergenza.

Mobilità

Accesso degli ospiti – Fornisce un accesso controllato a Internet, sia cablato che wireless, ai visitatori autorizzati, mantenendo sicura la rete interna.

Hotspot WLAN interni – Accesso Wireless LAN per dipendenti e visitatori in zone strategiche come sale riunioni, ingressi, mense e auditorium.

WLAN di impresa – Accesso wireless LAN pervasivo, altamente disponibile e altamente performante attraverso l'intero edificio dell'azienda, campus, o impresa estesa.

Accesso delle filiali remote – Estensione sicura del 'mobile edge' agli uffici e alle filiali remote usando Internet o la WAN aziendale.

Accesso SOHO e dei lavoratori in viaggio – Estende il 'mobile edge'

ovunque si trovi un utente attraverso AP remoti personali portatili.

Mobilità sicura per WLAN di vecchia generazione – Estende la vita delle WLAN esistenti attraverso una migliore sicurezza, roaming e gestione.

Tracking dei dispositivi – Utilizza la WLAN per fornire una precisa localizzazione di qualsiasi dispositivo Wi-Fi nell'area coperta.

Sicurezza

Sicurezza basata sull'identità – Migliora la sicurezza identificando il ruolo dell'utente e consentendogli solo l'accesso alla rete appropriato per quel ruolo.

WLAN Intrusion Prevention – Previene violazioni alla sicurezza attraverso la rete radio, identificando minacce al network da attaccanti e dispositivi wireless non controllati.

Integrità degli 'endpoint' – Assicura un livello predefinito di sicurezza del client, come ad esempio il controllo che un anti-virus, anti-spyware, o firewall personale siano presenti prima di garantire accesso alla rete.

Servizi di sicurezza esterni – Integra

spazio di lavoro, Aruba 70 può essere montato a muro, a soffitto, o sulla scrivania.

Aruba 80 è il primo AP controllato per esterni. Con il supporto di 802.11a, 802.11b/g e del wireless bridging, Aruba 80 gestisce tutte le applicazioni wireless in ambienti outdoor. Aruba 80 è certificato per ambienti esterni estremi, con una temperatura operativa da -30 a 55 gradi celsius. Dispone inoltre di una protezione da scariche elettriche e una messa a terra integrata.



le migliori appliance di sicurezza – anti-virus, content filtering e IDS o altro – come servizi di rete interni indipendenti dal client.

Sicurezza L2 per le LAN cablate – Fornisce alle LAN cablate le soluzioni del 'mobile edge', come crittografia, mobilità e sicurezza basata sull'identità.

Convergenza

Soluzioni di telefonia – Fornisce i vantaggi finanziari del Voice over IP con i benefici di mobilità delle comunicazioni cellulari.

Instant Messaging Vocale – Consente comunicazione in voce a mani libere attraverso una classe innovativa di dispositivi 'voice instant messaging'.

Dispositivi mobili convergenti – Fornisce qualità del servizio e controllo di accesso ai dispositivi di comunicazione e messaggistica convergenti, che integrano servizi multimediali come voce, dati, email e fax.

Convergenza fisso-mobile – Unifica le reti voce pubbliche e private fornendo un trasferimento senza interruzioni tra reti differenti nel caso di utilizzo di telefoni a doppia modalità cellulare/Wi-Fi.