

UN CASO DI SUCCESSO: INTERCONNETTERE LE SEDI DI MY COMPANY SPA

Il presente documento ha lo scopo di sintetizzare una soluzione scalabile per l'interconnessione delle sedi geografiche di "My company Spa". mettendo a confronto soluzioni definite "classiche" con una soluzione rivoluzionaria prodotta dall'azienda americana Meraki Inc. basata su componenti della famiglia "MX Cloud-Managed Routers" di cui Alya S.r.l. è promotore. Per aggiungere valore alla proposta si presenterà la soluzione mediante la formulazione di un business case creato ad-hoc per la realtà "My company Spa", sulla base delle informazioni contenute e desunte dallo scambio di mail intercorso sull'argomento "connettività geografica".

Presentazione Meraki (www.meraki.com)

Meraki Inc. è un'azienda produttrice di soluzioni di networking enterprise-class per aziende di qualsiasi dimensione. Grazie all'approccio completamente basato su controller cloud Meraki consente la gestione centralizzata dell'intera architettura di rete attraverso un'interfaccia web intuitiva, eliminando gli alti costi e le complessità associati ai tradizionali sistemi di networking. Ogni giorno, oltre 18.000 organizzazioni in più di 140 paesi affidano a Meraki le loro esigenze di rete.

Meraki Inc. è nata nel 2007 ed ha sede a San Francisco (California - USA) ed è una società privata sostenuta in parte da Google e Sequoia Capital. Nel marzo del 2011 Meraki è stata posizionata da Gartner Inc. nel Magic Quadrant dei Visionaries per le infrastrutture Wireless LAN. Secondo Gartner, i vendor posizionati nel quadrante Visionaries forniscono un approccio differente e fortemente caratterizzante rispetto alle soluzioni di mercato, producendo innovazione tecnologica e nuovi approcci metodologici:

"Un vendor posizionato nel quadrante Visionaries dimostra la capacità di aumentare le funzionalità della sua offerta per fornire un approccio unico e differenziato verso il mercato. Per essere considerato tale, un visionario dovrà aver contribuito tramite innovazioni in uno o più dei settori chiave delle tecnologie WLAN (ad esempio, convergenza, sicurezza, gestione o di efficienza operativa).

Gartner "Magic Quadrant for Wireless LAN Infrastructure (Global), 2011" - Michael King e Timothy Zimmerman, 3 marzo 2011."

Il nome "Meraki" (may-rah-kee) deriva da una parola greca che significa fare qualcosa con l'anima, con la creatività o con l'amore. Ovvero, quando si mette qualcosa di te stesso in quello che stai facendo.

Obiettivi e requisiti di progetto

Interconnettere in modalità semplice ed ottimale le sedi di "My Company Spa." garantendo che le attuali infrastrutture subiscano il minor impatto possibile in termini di intrusività della soluzione e che l'implementazione della soluzione richieda il minimo effort operativo ed organizzativo.

La soluzione di interconnessione individuata dovrà, inoltre, essere sufficientemente scalabile da poter consentire una rapida espansione del network geografico anche su altre sedi remote (branch offices), fissando i costi fissi di progetto e consentendo una programmabilità degli investimenti in infrastruttura che valorizzino l'azienda e massimizzino contemporaneamente la durabilità dell'investimento (capex) e minimizzino i costi di mantenimento (opex).



Le tecnologie di interconnessione da mettere a confronto con la soluzione proposta saranno i due modelli di rete basati su tecnologia MPLS e VPN.

Il sizing delle interconnessioni per il traffico site-to-site dovrà avere una velocità di trasferimento simmetrico pari almeno ad 1 Mbps.

Esplicitazione dei costi di soluzione necessari alla formulazione del business case

I costi indicati nella seguente scheda comprendono i canoni di noleggio di CPE Cisco Systems della famiglia 18** necessari al routing locale particolare della sede (per ogni sede, almeno un router). In caso di necessità di doppio CPE, per esigenze di alta disponibilità, i costi andranno aumentati di un fattore pari al 10-15%.

Condizione	Costo mensile	Costo attivazione
Linea internet su territorio italiano (HDSL FLAT 2Mbps – BMG 1Mbps)	200€	300€
Linea MPLS su territorio italiano (HDSL FLAT 2Mbps – BMG 1Mbps)	400€	500€
Linea internet su territorio extra italiano (HDSL FLAT 2Mbps – BMG 1Mbps)	200€	300€
Linea MPLS su territorio extra italiano (HDSL FLAT 2Mbps – BMG 1Mbps)	600€	1000€

I costi indicati nella seguente tabella rappresentano i costi di acquisto della componentistica di rete suddivisi per apparato e servizio.

Apparato	Costo acquisto	Costo servizi sicurezza/anno	Costo manutenzione/anno
Firewall enterprise class generico (sede con più di 10/20 utenti)	750€	400€	140€
Firewall enterprise class generico (sede con più di 500 utenti)	1500€	800€	300€
Meraki MX 60 Enterprise Edition (sede con più di 10/20 utenti)	750€	370€	garantito a vita
Meraki MX 70 Enterprise Edition (sede con più di 500 utenti)	1500€	740€	garantito a vita
Meraki MX 60 Enterprise Advanced Security (sede con più di 10/20 utenti)	750€	740€	garantito a vita
Meraki MX 70 Enterprise Advanced Security (sede con più di 500 utenti)	1500€	1470€	garantito a vita

Differenze tra Meraki MX Enterprise Edition ed Enterprise Advanced Security Edition ed un firewall generico con sottoscrizione dei servizi di sicurezza:

Feature	Enterprise Edition	Advanced Edition	Security	Firewall Generico
Stateful Firewall	X	X		X
NAT, DHCP, DMZ	X	X		X
Layer 7 Application QoS	X	X		tipicamente no



Cloud-based Centralized Management	X	X	
Monitoring, Asset Discovery and Alerts	X	X	tipicamente no
WAN link aggregation and failover (MX70)	X	X	X
Site to site (IPsec) VPN		X	da gestire manualmente
Layer 7 Application Firewall		X	estremamente costoso
Content Filtering		X	da gestire manualmente
Anti-Virus and Anti-Phishing		X	da gestire manualmente

Differenze tra apparati Meraki MX 60 e Meraki MX 70:

	MX60	MX70
Suggested Usage	Small branches (10-20 users)	Medium-large branches (up to hundreds of users)
WAN Interfaces with balancing and failover	1 x 1000 Base-T Ethernet	2 x 1000 Base-T Ethernet
LAN Interfaces	4 x 1000 Base-T Ethernet	4 x 1000 Base-T Ethernet
USB Interfaces	1 x USB 2.0	2 x USB 2.0
Stateful firewall throughput	100 Mbps	400 Mbps
Advanced security throughput	20 Mbps	125 Mbps
Maximum site-to-site VPN sessions	20	100
Maximum VLANs	4	32

N.B.: Tutti i costi esplicitati nelle tabelle precedenti sono approssimazioni per eccesso di costi reali effettivi (non listino). Come ISP Telecomunicazioni italiano è stata considerata una media dei costi finali proposti da operatori quali Telecom Italia e Fastweb. Come ISP Telecomunicazioni estero sono stati considerati costi identici per l'attivazione di linee internet ed una maggiorazione del 50% per le linee dedicate di tipo MPLS. Per i costi relativi alle soluzioni firewall, sono stati considerati costi relativi ad apparati di tipo Fortinet e Sonicwall relativi ai segmenti esplicitati.

Business Case - Definizione dell'ambito

Il presente paragrafo sarà articolato partendo dalla presentazione dei tre scenari di soluzione possibili fino a giungere ad una chiara evidenziazione del TCO di ogni soluzione e dei benefici della soluzione proposta mediante l'ausilio di un approccio di SWOT analysis.

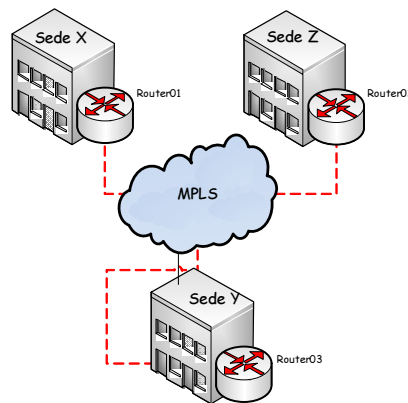
In tutti gli scenari presentati sarà considerata la sede X di My Company Spa, come centro stella della magliatura geografica. Come conseguenza si presuppone che il routing prevederà una tipica regola di default "universo - 0.0.0.0" verso gli apparati della sede X, questa assunzione deriva dal presupposto che i servizi centrali siano ospitati ed erogati dal datacenter della sede X stesso. La rete, inoltre, prevederà la possibilità di avere traffico bidirezionale tra le diverse sedi (es. se necessario e consentito dalla sede di X potrà essere acceduto un servizio ospitato sulla sede di Y o Z e viceversa, il medesimo assetto di servizio sarà considerato per le altre sedi periferiche - Y verso Z e viceversa - X verso Z e viceversa, etc.).

Negli scenari trattati, ogni sede sarà interconnessa alla sede principale con un link da almeno 1Mbps di BMG, la sede centrale X, dovendo funzionare da collettore, dovrà essere opportunamente dimensionata in termini di banda per raccogliere il traffico proveniente/generato dalle sedi periferiche (es. 2Mbps di BMG).



Soluzione A – MPLS:

Assunzioni: singolo router per ogni sede, doppia connettività per unbounding fisico di linea sul centrostella della sede X, utilizzo di interconnessioni MPLS verso le sedi periferiche, sicurezza e controllo del traffico di linea, possibilità di magliatura full mesh;



Strenghts:

1. Singolo apparato di routing nella sede centrale ed in ogni sede periferia (possibilità di aggiungere un secondo router in ogni sede per ottenere la fault tolerance);
2. Interfaccia organizzativa con singolo operatore internazionale (se presente);
3. Routing su magliatura any-to-any (es. una sede può raggiungere l'altra mediante un link diretto);
4. Possibilità di definizione di politiche di QoS integrate (se consentito/permesso dall'operatore);

Weaknesses:

1. Assenza di servizi di sicurezza integrati (la sicurezza è tipicamente demandata all'implementazione di ulteriori apparati o soluzioni (eg. firewall, application performance, etc.) con conseguente aggravio ed aumento dei costi);
2. Assenza di una piattaforma di monitoraggio delle bande integrata a livello worldwide;
3. Assenza di controllo e flessibilità (i device di routing sono tipicamente gestiti dall'operatore);

Opportunities:

1. Rete completamente integrata con logiche di routing demandate alla rete stessa;
2. Definizione di SLA e di eventuali penali su KPI concordati con l'operatore di rete MPLS;

Threaths:

1. Accordi labili tra operatori Telco e difficoltà di gestione degli incident / problem;
2. Bassa possibilità di controllo del fornitore (negli interventi pianificati e non pianificati);
3. Costi estremamente variabili (es. cambio euro/dollaro, cambio dei listini, controllo di gestione, etc.);
4. E'possibile che l'operatore Telco non abbia possibilità di coprire un particolare paese (soluzione poco scalabile);
5. Tempi di attivazione incerti (tipicamente 90/120 gg a seconda del paese);

Costi associati alla soluzione:

Voce di costo	Costo una tantum (capex)	Costo mensile (opex)
Costo di attivazione MPLS per la sede X	500€	-



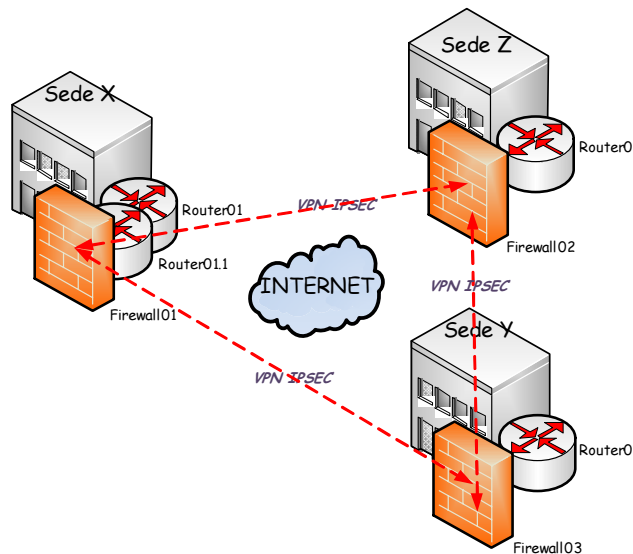
Costo di attivazione MPLS per la sede di Y	1000€	-
Costo di attivazione MPLS per la sede di Z	1000€	-
Costo mensile della sede principale per 2 Mbps di banda	-	2 x 400€
Costo mensile della sede di Y per 1 Mbps di banda	-	600€
Costo mensile della sede di Z per 1 Mbps di banda	-	600€
Costo dei servizi di sicurezza (es. firewall su ogni sede?)	?	?
Totale investimento e costi di gestione/mantenimento	2500€ +	2000€ +

Costo annuale per la gestione dell'interconnessione di 2 sedi periferiche: 24.000€/anno;

Conclusion: la soluzione è poco scalabile su realtà enterprise con necessità di interconnessione di sedi periferiche europee ed extra europee e, oltre ad essere lacunosa sotto il punto di vista della sicurezza, produce dei costi non facilmente predicibili oltre a delle forti complessità organizzative.

Soluzione B – Firewall:

Assunzioni: singolo router internet per ogni sede periferica, singolo firewall per ogni sede, doppia connettività per unbounding fisico di linea sulla sede principale di My company Spa, utilizzo di interconnessioni internet economiche, sicurezza e controllo del traffico di linea, possibilità di magliatura full mesh;



Strengths:

1. Interfaccia verso operatore internazionale unificabile o comunque gestibile/demandabile a livello locale (es. facilità nel reperire operatori internet locali ove non disponibile l'operatore internazionale);
2. Gestione granulare della sicurezza a livello di singola sede mediante l'apparato firewall locale;

Weaknesses:

1. Impossibilità di gestione dei servizi di sicurezza in assetto unificato (es. assenza di un controller centrale di gestione, etc.);
2. Assenza di una piattaforma di monitoraggio delle bande integrata a livello worldwide;
3. Assenza di una piattaforma di gestione del change management sugli apparati (es. database delle password dei dispositivi, tracking delle configurazioni, aggiornamenti OS e firmware degli apparati, etc.);



4. Difficoltà di implementazione e mantenimento della soluzione (es. occorrono interventi di setup locale alle singole sedi o comunque interventi complessi, etc.);
5. Difficoltà nella configurazione di una rete any-to-any full mesh con conseguente aumento della complessità (es. ogni singola sede deve essere interconnessa alle altre mediante una VPN IPSEC creata ad-hoc, ogni sede deve essere dotata di indirizzo IP pubblico, etc.);
6. Il routing della rete non è integrato nella soluzione di interconnessione e va definito volta per volta (es. la rete non converge centralmente se non mediante configurazione dei singoli apparati, etc.);

Opportunities:

1. Definizione di SLA e di eventuali penali su KPI concordati con l'operatore di connettività Internet;
2. Riduzione dei costi dipendente dalla scelta di connettività meno pregiate (es. connettività internet a basso costo, etc.);
3. Tempi di adozione della soluzione abbastanza bassi (es. relativi alla fornitura della connettività internet locale, etc.);

Threats:

1. Difficoltà di gestione degli incident / problem sui device periferici;
2. Bassa possibilità di controllo dell'operatore internet (negli interventi pianificati e non pianificati);
3. Occorre formare il personale della sede centrale per la gestione della soluzione globale e della sede locale per la gestione della soluzione di prossimità (non sempre possibile);
4. Aggravio dei costi di gestione della soluzione di interconnessione e di sicurezza (es. ogni device deve essere dotato di un pacchetto di sicurezza specifico oltre che della sottoscrizione di un servizio di maintenance, etc.);
5. La soluzione non è durevole e non crea valore aggiunto all'azienda (es. andranno gestiti i cespiti, andrà gestita l'obsolescenza degli apparati, etc.);

Costi associati alla soluzione:

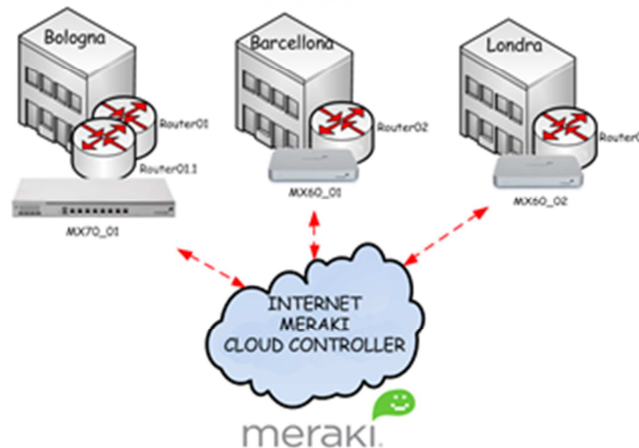
Voce di costo	Costo una tantum (capex)	Costo mensile (opex)
Costo di attivazione linea internet per la sede X	300€	-
Costo di attivazione linea internet per la sede di Y	300€	-
Costo di attivazione linea internet per la sede di Z	300€	-
Costo mensile della sede principale per 2 Mbps di banda	-	2 x 200€
Costo mensile della sede di Y per 1 Mbps di banda	-	200€
Costo mensile della sede di Z per 1 Mbps di banda	-	200€
Costo del firewall e dei servizi di sicurezza per la sede di X	1500€	(800€ + 300€ / 12 mesi)
Costo del firewall e dei servizi di sicurezza per la sede di Y	750€	(400€ + 150€ / 12 mesi)
Costo del firewall e dei servizi di sicurezza per la sede di Z	750€	(400€ + 150€ / 12 mesi)
Costi nascosti (es. trasferta, formazione, downtime, etc.)	?	?
Totale investimento e costi di gestione/mantenimento	3900€ +	984€ +

Costo annuale per la gestione dell'interconnessione di 2 sedi periferiche: 11.800€/anno;

Conclusion: la soluzione basata su firewall è decisamente più granulare e scalabile di una soluzione MPLS in ambito geografico (europeo o extra europeo), tuttavia, benchè sia apparentemente più economica in termini di costi di mantenimento, è fortemente carente dal punto di vista dell'impatto organizzativo introducendo delle forti componenti di complessità e organizzativa che tecnica, fortemente dipendenti dalla tipologia di apparati scelti come dotazione.

Soluzione C – Meraki MX Cloud-Managed Routers:

Assunzioni: singolo router internet per ogni sede periferica, singolo device MX per ogni sede, doppia connettività per unbounding fisico di linea sulla sede principale di My Company Spa, utilizzo di interconnessioni internet economiche, sicurezza e controllo del traffico di linea, possibilità di magliatura full mesh;



Strengths:

1. Indipendenza dal provider di connettività internet e virtualizzazione della rete geografica con interfaccia organizzativa con singolo operatore internazionale (se dispinibile);
2. Gestione granulare di ogni aspetto di “intelligenza della rete” effettuato mediante l’unica interfaccia web del Meraki cloud controller (es. politiche di sicurezza, change management, configurazioni, monitoraggio delle bande, logging degli accessi alla rete centralizzato, etc.);
3. Interconnessione full meshed (routing any-to-any) – out of the box – di tutte le sedi periferiche con possibilità di definizione delle politiche granulari (es. visibilità di una certa seda da un’altra, etc.);
4. Funzionalità avanzate con possibilità di implementare politiche di QoS integrate, a costi fissi ed estremamente contenuti;

Weaknesses:

1. L’attuale release degli apparati non permette la configurazione in alta disponibilità / fault tolerance dell’apparato (es. due apparati MX 60 o MX 70 non possono essere messi in stack / ha) - si sopperisce al problema avendo a disposizione un device di “cold stand by” nella sede periferica, pronto per essere sostituito in caso di rottura, in attesa dell’apparato nuovo proveniente dal call to repair Meraki (con tempi di consegna worldwide estremamente contenuti);

Opportunities:

1. Definizione di SLA e di eventuali penali su KPI concordati con l’operatore di connettività Internet;
2. Rete completamente integrata con logiche di routing demandate alla rete stessa;
3. Indipendenza dalla tecnologia (es. eliminazione delle complessità di gestione di una piattaforma vendor specific, etc.);
4. Riduzione dei costi dipendente dalla scelta di connettività meno pregiate (es. connettività internet a basso costo, etc.);
5. Tempi di adozione della soluzione estremamente bassi (es. relativi alla fornitura della connettività internet locale, etc.);



6. Semplicità di gestione degli incident / problem sui device periferici (es. semplicità di setup dei dispositivi – plug and play, etc.) – un device MX si configura e si rilascia in produzione in meno di 15 minuti;
7. Modalità di gestione della rete unificata, semplice ed estremamente intuitiva (es. unico punto di accesso webbased strutturato in maniera ottimale);
8. Reporting unificato della rete su scala globale (es. utilizzo della banda internet per applicazione, per utente, per sede, tutto disponibile da una singola interfaccia web con invio di report schedulati di default, etc.);
9. Pacchetto di sicurezza avanzato (es. application 7 firewall, etc.) disponibile by design;
10. Ottica di gestione a servizio - cloud based - con rilascio nuove funzionalità senza necessità di upgrade degli apparati e senza costi aggiuntivi;

Threats:

1. Bassa possibilità di controllo dell'operatore internet (negli interventi pianificati e non pianificati);
2. Occorre formare il personale della sede centrale per la gestione della soluzione globale (anche se molto semplice ed intuitiva);

Costi associati alla soluzione:

Voce di costo	Costo una tantum (capex)	Costo mensile (opex)
Costo di attivazione linea internet per la sede di X	300€	-
Costo di attivazione linea internet per la sede di Y	300€	-
Costo di attivazione linea internet per la sede di Z	300€	-
Costo mensile della sede principale per 2 Mbps di banda	-	2 x 200€
Costo mensile della sede di Y per 1 Mbps di banda	-	200€
Costo mensile della sede di Z per 1 Mbps di banda	-	200€
Costo MX 70 Enterprise Advanced Security Edition per la sede di X	1500€	(1470€ / 12 mesi)
Costo MX 60 Enterprise Advanced Security Edition per la sede di Y	750€	(740€ / 12 mesi)
Costo MX 60 Enterprise Advanced Security Edition per la sede di Z	750€	(740€ / 12 mesi)
Costi nascosti (es. trasferta, formazione, downtime, etc.)	estremamente bassi	estremamente bassi
Totale investimento e costi di gestione/mantenimento	3900€	1046€

Costo annuale per la gestione dell'interconnessione di 2 sedi periferiche: 12.512€/anno – i costi si riducono notevolmente su contratti triennali e quinquennali;

Conclusion: la soluzione basata su tecnologia Meraki è decisamente più granulare e scalabile rispetto ad una soluzione classica basata su MPLS o Firewalling. In ambito geografico (europeo o extra europeo) permette l'attivazione di una sede periferica in modo tempestivo a prescindere dall'operatore scelto (un device si configura e si rende disponibile in meno di 15 minuti, senza partire da una configurazione di backup, basta una connessione ad internet anche non dotata di indirizzamento pubblico!) offrendo vantaggi sotto qualsiasi punto di vista, sia in termini di riduzione dei costi, sia in termini di facilità di gestione e prestazioni del network (QoS e firewall a livello 7). Tutti gli apparati Meraki hanno garanzia a vita e, in caso di rottura, sono sempre sostituiti gratuitamente dal produttore. In termini di economie, adottando la soluzione Meraki, si costificano in maniera fissa i costi dovuti alla tecnologia di networking (es. una nuova sede di dimensione piccola, si attiva con poco più di 750€ di investimento e 750€ di servizio, una sede di grandi dimensioni si attiva con poco più di 1500€ di investimento e 1500€ di servizio, senza alcun costo aggiuntivo) necessaria all'interconnessione di una sede periferica, in sostanza basta attivare una qualsiasi connettività internet ad agganciarla ad un device Meraki, qualche semplicissimo step di configurazione tramite interfaccia web based et voilà!

N.B.: Nel contesto applicativo "reale", nella sede X dovrà essere conservata l'attuale infrastruttura di firewalling di frontend e, nelle sedi periferiche, soprattutto in vista del fatto che non si ha una piena autonomia organizzativa/di



controllo, potrà essere fatto altrettanto (ovvero, su ogni sede, sarà sufficiente connettere l'apparato Meraki stabilito e gestire il routing inter- sede – non è indispensabile pensare agli apparato Meraki come oggetti da collocare in sostituzione agli apparati L3 o firewall locali, anche se ovviamente possibile).

Matrice comparativa delle soluzioni presentate

La seguente tabella mette a confronto ulteriormente le soluzioni presentate e offre ulteriori spunti di riflessione:

Soluzione	Costi una tantum (capex)	Costi mensili (opex)	Semplicità di gestione	Qualità dei servizi	Indipendenza Operatore	Scalabilità della soluzione nel contesto geografico
Soluzione A – MPLS	2500€	2000€	Alta	Bassa	Bassa	Bassa / Costosa
Soluzione B – Firewall	3900€	984€	Bassa	Bassa	Media	Bassa / Complicata
Soluzione C – Meraki MX Cloud-Managed Routers	3900€	1046€	Alta	Alta	Alta	Alta

Ci rendiamo disponibili ad approfondire ulteriormente le argomentazioni sostenute avvalorandone ulteriormente i contenuti ove si rendesse necessario in seguito a Vs gradita richiesta.