Premessa

In generale i servizi di un Full Service Provider sono più o meno paragonabili. Qui di seguito viene descritto il servizio di Firewalling specifico di un fornitore ma di contenuto assolutamente generico, quindi valido per chiunque voglia offrire o acquistare sul mercato Italiano tale servizio.

1 INTRODUZIONE

I servizi di Firewalling (Firewalling Services) di un Full Service Provider consistono nell' insieme dei sistemi di protezione fisica e logica contro l'accesso indesiderato alle infrastrutture hw/sw del Cliente ospitate nel Data Center del Service Provider o presso la sede stessa del Cliente. Il Full Service Provider deve adottare le migliori tecnologie a disposizione sul mercato per garantire i massimi livelli di sicurezza e deve essere in grado di offrire un servizio comprendente tutte le fasi di implementazione di un sistema di Firewall, dal disegno della soluzione, alla fornitura, configurazione e gestione degli apparati.

2 DESCRIZIONE DEI SERVIZI

L'offerta di Firewalling di un Full Service Provider si articola in due tipologie:

- Firewall dedicati (Data Center o sede Cliente)
- Firewall condiviso

La scelta tra le due formule dovrà essere fatta in base a:

- Complessità di filtraggio
- banda utilizzata (>2Mbps = Dedicato)
- numero di host (verifica break-even con soluzione dedicata).

L'impostazione modulare rende il servizio scalabile; il Cliente può costruire la propria soluzione utilizzando i seguenti moduli:

- Consulenza per il disegno dell'architettura e lo studio delle policy appropriate a garantire i servizi del Cliente nel rispetto delle norme di security
- Servizio di fornitura, configurazione e attivazione del sistema e delle policies definite - Monitoraggio della disponibilità e dello stato del Firewall 24h x 7gg - Servizio di manutenzione del sistema di Firewall
- Servizio di reporting
- Servizio di modifica delle policies di filtraggio
- Servizio di gestione delle emergenze

Il Full Service Provider implementa in genere un primo livello di protezione sui router di connessione ad Internet, avente il solo scopo di filtrare tutti i servizi non rilasciati (ad es. SNMP, RMON, ecc.), e sul quale in genere non possono essere implementate le regole di filtraggio specifiche per ciascun Cliente.

2.1 CONSULENZA

2.1.1 Disegno dell'architettura

Tale attività mira ad utilizzare le competenze tecniche del personale del Full Service Provider per suggerire la migliore soluzione HW/SW, in relazione alle specifiche esigenze del Cliente. Il disegno dell'architettura HW si basa principalmente sulla valutazione di elementi quali:

- Sicurezza: vengono identificati i sottosistemi logici che devono essere isolati o controllati al fine di segmentare la struttura poiché in questi punti verranno attuati i controlli. (es. Front-end, applications, DBs, Staging, test, etc)
- Performance: in funzione di requisiti quali n. utenti, banda utilizzata, n. di connessioni contemporanee, impiego di VPN, complessità delle policies di filtraggio adottate si definiscono le caratteristiche della struttura, dell'apparato e delle regole da applicare
- Disponibilità: sulla base delle caratteristiche del servizio erogato dal Cliente vengono proposte soluzioni di ridondanza quali configurazione in singola macchina, Fail Over, High Availability, Load Sharing

L'analisi delle esigenze del Cliente permette di identificare, la configurazione hw/sw necessaria.

2.1.2 Definizione delle Policies

Esistono due tipologie di policies: generali e specifiche del Cliente. Le prime sono associate a comportamenti intrinsecamente errati e che vengono implementate indipendentemente dai servizi erogati dal Cliente (anti spoofing). Le seconde sono disegnate sulle esigenze del Cliente e hanno come obiettivo la comprensione del servizio offerto al fine di rendere solo questo accessibile dall'esterno. Queste policies di filtraggio o autorizzazione al passaggio del traffico dati tra una sorgente esterna ed una fonte interna (o viceversa) vengono definite in base a:

- indirizzo sorgente
- indirizzo di destinatazione
- protocollo di rete
- protocollo di servizio

Mediante la realizzazione di un'infrastruttura dedicata è in genere anche possibile richiedere di configurare soluzioni di maggiore complessità alfine di soddisfare particolari esigenze quali:

- autenticazioni aggiuntive (login+pwd)
- logging del traffico
- protezione da attacchi specifici quali Syn Attack, Spoofing,...

Generalmente ai fini della tariffazione viene definita "regola" una riga di configurazione sul firewall.

2.2 FORNITURA E ATTIVAZIONE SISTEMA

Stabilite configurazione e policies si passa all'implementazione del servizio, la quale viene normalmente effettuata nelle tempistiche concordate con il Cliente e si conclude con il collaudo per la verifica delle funzionalità.

2.3 MONITORAGGIO

Il Full Service Provider attiva quindi un servizio di monitoraggio dei firewall condivisi e dedicati, finalizzato ad ottenere dati sulla disponibilità del dispositivo (up-time) e sulle condizioni di utilizzo (RAM, CPU ed utilizzo delle interfacce).

2.4 MANUTENZIONE

Le attività previste nell'ambito della gestione e manutenzione sono relative agli strati hw e sw del sistema scelto:

- Manutenzione software; consiste nell'installazione e configurazione di patch, fix, aggiornamenti di release, e in generale di tutte le attività di manutenzione ordinaria/straordinaria del Sistema operativo, applicativo o firmware installati. Le eventuali patch o nuove release sw sono di norma comprese nel canone di servizio.
- Manutenzione hardware; consiste nel servizio di intervento on-site (Cesano Maderno o sede Cliente) in modalità 8x5 con intervento entro il giorno lavorativo successivo oppure 24x7 entro 5h (1h per il tempo di reazione Un Full Service Provider + 4h per il manutentore) dalla chiamata. Il servizio comprende anche la sostituzione dell'HW guasto e la riconfigurazione del sistema.

Gli aspetti di gestione e manutenzione degli apparati di rete concorrono normalmente al calcolo degli SLA (Service Level Agreement) concordati con il Cliente secondo le specifiche del servizio acquistato.

2.5 REPORTING

Il Full Service Provider rende di solito disponibili al Cliente i seguenti servizi di reportistica:

Tipo report	Oggetto	Cadenza	Tipo Servizio di Firewalling
Rep1	Modifiche configurazione e relativo stato	mensile	Condiviso e dedicato
Rep2	Dati relativi al monitoraggio	settimanale	dedicato
Rep3	Invio del file di log dell'apparato	a richiesta	dedicato

Il servizio di Reporting non comprende attività diagnostiche inerenti eventuali eventi anomali che potrebbero emergere dall'analisi dei Log. Il servizio di reporting può essere reso disponibile su web, nell'area Cliente, protetta mediante sistemi di accesso basati su "strong authentication".

2.6 MODIFICA DELLE POLICIES

Alfine di soddisfare le esigenze del Cliente, oltre a rendersi disponibile ad implementare tutte le modifiche alle politiche di Firewall richieste, il Full Service Provider effettua un'attività di "validation" con lo scopo di verificare la congruenza con gli obiettivi di security richiesti dal Cliente. Data la delicatezza dell'operazione di cambiamento delle policies di sicurezza, in genere la comunicazione delle richieste deve essere effettuata dal Cliente in via formale e ben documentata, su moduli

predisposti via fax e firmata da una persona autorizzata (il cui specimen di firma sia stato depositato precedentemente presso il Full Service Provider).
Il Full Service Provider successivamente analizza le modifiche richieste e controlla se:

- il fax contiene tutte le informazioni necessarie
- da un punto di vista security la richiesta è priva di rischi e quindi è considerabile accettabile. Nel caso in cui il Provider rilevasse problemi di sicurezza relativamente alle modifiche richieste, informerà il Cliente via e-mail dei problemi riscontrati e, quando possibile, propone delle alternative
- prima di effettuare le modifiche comunque il Provider contatta il Cliente ad un numero di telefono concordato precedentemente per la conferma finale.

I Provider più evoluti possono rendere disponibile tale funzionalità di modifica, anche via web attraverso il proprio sito dedicato ai Clienti. Tale funzionalità, permetteno al Cliente di:

- inserire le richieste di modifiche direttamente attraverso il web
- tracciare lo stato avanzamento della modifica e lo storico delle modifiche richieste.

L'accesso al sito sarà protetto mediante "strong authentication". In genere i Provider si riservano il diritto di non implementare una policy richiesta dal Cliente se, ad insindacabile giudizio dei propri tecnici, risulti essere in conflitto con le proprie politiche di sicurezza.

2.7 GESTIONE EMERGENZE

Il Full Service Provider mette in genere a disposizione dei propri Clienti un servizio di intervento dei propri tecnici entro 30 minuti dalla richiesta. Sono da considerarsi in modalità di *emergenza* tutti gli interventi finalizzati a coprire esigenze fuori dal contesto delle normali attività di gestione e manutenzione. Tale servizio può essere messo a disposizione in 2 diverse modalità:

- 10x5: prevede l'intervento durante l'orario lavorativo (giorni feriali dalle ore 8.30 alle ore 18.30)
- 24x7: prevede l'intervento 24 ore su 24.

Nel caso in cui l'intervento sia off-site (es. presso la sede del Cliente) ai 30 minuti vanno sommati i tempi tecnici per raggiungere il luogo dove l'intervento è stato richiesto.

3 FIREWALL DEDICATO

3.1 DESCRIZIONE

Le soluzioni di Firewall Dedicato di un Full Service Provider permettono di soddisfare le esigenze dei Clienti che necessitano di sistemi in grado di garantire oltre ad alta affidabilità, anche massima autonomia di gestione (installazione patch, nuove release sw, ecc.), configurazione (implementazione di particolari regole di filtraggio) e scelta dell'opportuno dimensionamento, coerente con le condizioni di *lavoro* previste (volume di traffico gestito, tipologia di filtraggio, ecc.). Una ulteriore opportunità è rappresentata dalla possibilità di implementare configurazioni in modalità Dual Bastion, che prevede l'utilizzo contemporaneo di due diverse tecnologie (ad es. Cisco + Nokia/CheckPoint) allo scopo di rendere ancora più sicura l'infrastruttura di protezione.

3.2 SERVIZIO DI HW/SW PROVISIONING PER LA FORNITURA DEL FIREWALL

Il Full Service Provider può offrire il servizio di fornitura hw/sw di Firewall in modalità *renting* nell'ambito di contratti della durata di 24 o 36 mesi. Su base progetto è possibile ottenere sistemi e configurazioni diversi da quelle rese disponibili nell'offerta standard, e sui quali verrà effettuata una attività di validazione. Sono attualmente disponibili soluzioni base con 3 interfacce (Internet, BE, FE) in configurazione standard o Fail Over. In genere sono anche disponibili moduli per l'upgrade delle subnet. Il servizio comprende il monitoraggio H24 e la manutenzione hw e sw del firewall.

3.3 FIREWALL LATO CLIENTE

Normalmente il Full Service Provider offre ai propri Clienti anche un servizio di fornitura e gestione del Firewall a protezione della rete aziendale presso la stessa sede Cliente. Il servizio trova la sua applicazione nei casi di connessione della LAN interna ad Internet. Tipologie di apparato e modalità di fornitura sono le medesime previste per il servizio a protezione dei server ospitati nel Data Center del Provider.

4 FIREWALL CONDIVISO

4.1 DESCRIZIONE

Il servizio condiviso è in genere offerto dal Full Service Provider per soddisfare i Clienti con limitate necessità di configurazione, personalizzazione e che generano volumi di traffico contenuti (connettività internet <=2Mbps). La soluzione consente al Cliente di ricavare un sistema di firewall virtualmente dedicato a partire da un'infrastruttura condivisa, costituita da firewall ridondati, abbinata alle features disponibili nel sistema di switching della rete Un Full Service Provider. In particolare la creazione di Super VLAN rende possibile la condivisione *fisica* della stessa subnet preservando le caratteristiche di segregazione, garantendo quindi le infrastrutture del Cliente da attacchi sferrati per il tramite di altro host residente sulla medesima subnet. La struttura condivisa viene costantemente monitorata allo scopo di rilevare le condizioni di funzionamento (utilizzo RAM, CPU, ecc.) alfine di consentire un tempestivo intervento in presenza di eventuali anomalie. Sul Firewall condiviso in genere il Provider provve ad impostare policies di filtraggio standard che non possono essere modificate in quanto parte integrante delle politiche di sicurezza definite dal Provider sulle infrastrutture condivise:

- traffico consentito in ingresso soltanto http, https, ftp, smtp, pop3, dns, soap
- blocco di telnet, ssh, terminal server e servizi analoghi
- Antispoofing
- traffico in uscita non consentito (navigazione internet)

Fatto salvo quanto sopra esposto, il Provider si rende in genere disponibile ad implementare le regole di filtraggio richieste dal Cliente, tranne nei casi in cui, ad insindacabile giudizio dei propri specialisti, queste risultino non conformi con le politiche di sicurezza previste sulle infrastrutture condivise. Nel caso in cui questa soluzione si riveli non adatta alle specifiche esigenze del Cliente, questi dovrà orientarsi verso le altre più flessibili soluzioni di Firewalling.

Il servizio base è composto dai seguenti elementi:

- Configurazione soluzione e attivazione delle policies definite nell'ambito di quelle consentite
- Monitoraggio h24 finalizzato alla verifica della disponibilità e dello stato del Firewall
- Manutenzione del sistema di Firewall

Opzioni:

- Reporting di tipo Rep1
- Modifica delle policies di filtraggio nell'ambito di quelle consentire
- Servizio di gestione delle emergenze
-

5 CUSTOMER CARE

Il Cliente potrà usufruire di un servizio di Customer Care con accesso mediante username/pwd attivo nei giorni previsti dagli SLA. Opzionalmente il Cliente potrà richiedere la possibilità di ricevere un supporto di Help Desk attivo 24x7. Supporto per modifica policies 10x5. Supporto di emergenza 24x7

6 SERVICE LEVEL AGREEMENT

Il Full Service Provider si dovrebbe impegnare a garantire l'up-time del servizio di Firewalling su sistemi condivisi a valori non inferiori al 99.90% su base mensile. Vanno esclusi da tale valorizzazione eventuali interruzioni del servizio dovuti a interventi di manutenzione (che verranno concordati dal Full Service Provider con il Cliente con almeno una settimana di preavviso salvo emergenze) o ad operazioni "non-convenzionali" effettuate dal Cliente sulla propria rete/server sia presso il Data Center, sia presso le infrastrutture del Cliente stesso. Per i Firewall dedicati al Cliente, la percentuale di disponibilità è fortemente dipendente da un insieme di fattori (hardware e software scelto, carico elaborativo, configurazione di HA, qualità degli ambienti in cui il sistema è installato, se presso la sede del Cliente) che non sono prevedibili a priori; per questa ragione, la percentuale di disponibilità sarà concordata di volta in volta come requirement di progettazione architetturale. Normalmente nel caso in cui il servizio erogato richieda di installare apparati hw e/o sw off-site (i.e. presso la sede del Cliente), il Provider è disponibile all 'estensione di SLA (il cui valore di disponibilità dovrà essere formulato a progetto) nel caso in cui vengano rispettate le seguenti condizioni:

- il Cliente non ha "accesso logico" ai sistemi e quindi tutta la gestione e configurazione viene effettuata esclusivamente dal Provider
- il Cliente è responsabile della protezione fisica dei sistemi: condizioni ambientali (temperatura, umidità,...) di funzionamento come da scheda prodotto, alimentazione elettrica, protezione da furti e danneggiamenti