ACI Global

Progetto di IPS e anomaly detection

Allegato tecnico relativo alla soluzione di IPS e anomaly detection

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
0.1	29 Maggio 2008	Emissione
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	29 Maggio 2008	
Versione	0.1	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	7	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Roberto Banfi	
Approvato da		

INDICE

1 Obiettivo

Lo scopo del presente documento consiste nel descrivere la soluzione IPS e anomaly detection nella infrastruttura di rete di Aci Global. La delivery di questa soluzione permetterà al cliente di avere sotto controllo il traffico di rete in termini di variazioni ed evoluzioni ed avere una protezione da attacchi verso i server in DMZ protetti da una sonda IPS.

2 Analisi dei requisiti

Obiettivi del monitoraggio:

- Protezione dei server attestati sulla rete DMZ.
- Monitoraggio in tempo reale delle reti specificate.
- Mappatura del traffico della rete e gestione di eventi in funzione di anomalie.
- Gestione centralizzata degli eventi sia delle sonde sia dell'apparato IPS.

3 Ambiente di riferimento

Le reti e il relativo volume di traffico generato dagli host indicati è riassunto nella seguente tabella:

Sistema IT	N° host
Rete DMZ throughput 45 Mb/s	25
Rete EXT throughput 10 Mb/s	19
Rete Server throughput 100 Mb/s	75
Network throughput 10 Mb/s	30

4 La soluzione proposta

4.1 La tecnologia

La soluzione di Anomaly Detection & IPS proposta è basata sul software Sourcefire. Questo sistema volto alla prevenzione delle intrusioni, prevede un'architettura suddivisa logicamente in 3 sistemi con funzioni specifiche:

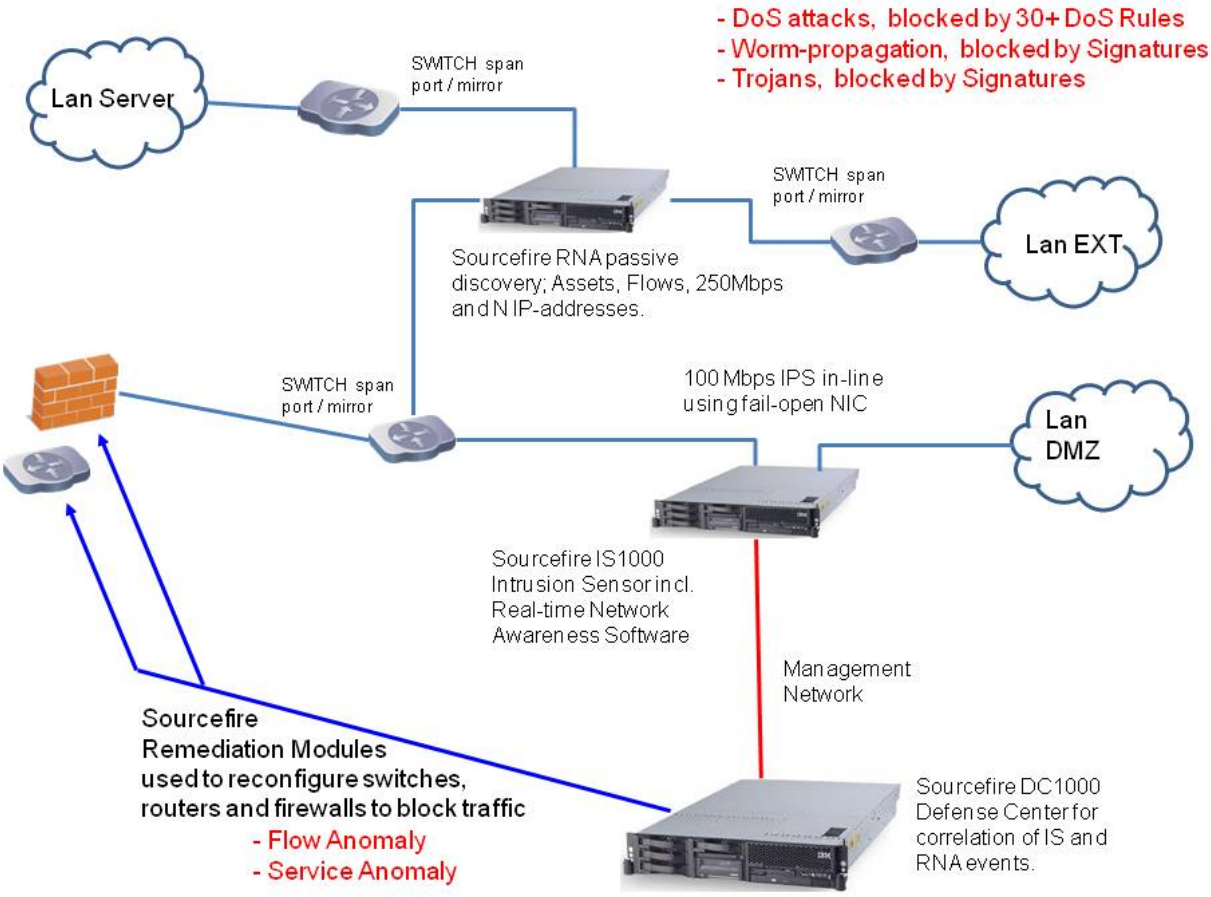
1. **IPS:** Intrusion Prevention System permette di analizzare il traffico "*in-line*" e bloccare tutte le attività malevole e tentativi di denial of services
2. **Real Network Awarness (RNA):** permette di "*capire*" come si comporta la rete e i server e fotografare il comportamento normale in modo tale da generare eventi in caso ci si discosti dalla "normalità".
3. **Defence Center:** sistema di gestione centralizzata con le seguenti caratteristiche principali
   - **Reporting system:** sistema di reportistica
   - **Active Vulnerability Audit System:** sistema per la generazione di scansioni attive sulla rete da correlare con le informazioni ottenute in modo passivo.
   - **Correlation System:** sistema di correlazione dei dati ottenuti dalle sonde e dalle scansioni effettuate
   - **Remediation System:** sistema per l'integrazione con apparati perimetrali, pilotabili in funzione di eventi critici rilevati
   - **Policy System:** sistema per la gestione delle politiche di rilevamento anomalie e blocco.

La tecnologia Sourcefire ha la possibilità integrare funzionalità di IPS anomaly detection e correlare gli eventi raccolti, conferendo alla soluzione un'architettura scalabile.

Nella soluzione prospettata la sonda IPS per la protezione della DMZ ha a bordo sia le funzioni di anomaly detection che le funzioni di intrusion prevention. I segmenti di rete rimanenti, come specificato nel paragrafo 3, vengono analizzati dalla sonda RNA per la sola rilevazione di anomalie.

Oltre alle precedenti componenti, Sourcefire fornisce strumenti per integrare le informazioni legate alla rete con il repository degli utenti, utilizzare software di visualizzazione grafica della rete e la possibilità di analizzare flussi provenienti da sistemi network dove non è possibile inserire una sonda.

4.2 Schema logico



5 Vantaggi della soluzione proposta

La soluzione proposta permette di implementare una soluzione completa volta ad identificare anomalie nella rete, bloccare gli attacchi riconosciuti ed avvisare gli amministratori in caso di eventi critici.

Sourcefire permette di gestire centralmente l'infrastruttura tramite un'interfaccia web da cui è possibile configurare, gestire ed analizzare tutte le reti monitorate.

Oltre alle funzionalità di blocco fornite dalla sonda IPS è possibile utilizzare le caratteristiche di rilevamento delle anomalie fornite dalla sonda RNA. Questa sonda permette di analizzare il traffico delle reti e costruire un modello di funzionalità ottimale della rete specifica per il cliente. In questo modo è possibile avere sempre sotto controllo cosa avviene e generare degli eventi in funzione di quanto ci si discosta dal comportamento ottimale del traffico. Configurando l'RNA a

bordo della sonda IPS e correlando gli eventi tramite il Defence Center, è possibile automaticamente correggere e applicare policy al verificarsi di un determinato evento.
La soluzione proposta permette ampiamente di monitorare e proteggere oltre alla rete DMZ altri segmenti di rete, sostenendo senza problemi eventuali picchi di traffico. È sempre possibile, in caso di necessità, estendere la soluzione ad altre network posizionando opportunamente altre sonde e agganciarle allo stesso sistema di gestione. Ogni sonda RNA inoltre ha la possibilità di essere eventualmente configurata (con una licenza aggiuntiva) anche in modalità IPS mettendosi inline tra una coppia di segmenti di rete. In questo modo sarebbe possibile integrare le funzionalità di RNA con quelle di un IPS e bloccare in tempo reale eventuali minacce.

6 Considerazioni

La soluzione proposta si basa sul dimensionamento degli apparati in modo tale da avere un spazio di scalabilità e la possibilità di poter aggiungere alle sonde RNA la funzionalità IPS e utilizzare entrambe le caratteristiche correlando gli eventi e organizzando le azioni da intraprendere.
La soluzione IPS è dotata di una scheda di “by pass” che permette di far proseguire il traffico da e verso entrambe le reti senza creare alcun disservizio. È possibile scegliere la scheda in modo tale da bloccare tutto il traffico in caso di fault. La sonda IPS è assolutamente trasparente alla rete e non crea alcun ritardo sensibile durante i flussi di traffico. Le sonde RNA sono assolutamente passive e controllano il traffico che gli apparati di rete gli recapitano tramite una configurazione di una porta detta mirror o span.