COTONIFICIO ALBINI

OFFERTA TECNICA

Milano

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

INDICE

1 Obiettivi

Questo documento costituisce la proposta tecnica di Hackingteam e descrive le soluzioni proposte per le seguenti tre tematiche:

- **Difesa perimetrale**
- **Protezione server critici**
- **Log management e allarmistica**

2 Difesa perimetrale

Per la difesa permetrale Hackingteam propone due soluzioni Firewall/VPN di nuova generazione, entrambe con caratteristiche di Unified Treath Management (UTM), ovvero con funzionalità di sicurezza tipicamente distribuite su più sistemi:

- **ANTIVIRUS:** possibilità di controllare la presenza di virus sul traffico legato a protocolli quali SMTP, HTTP, POP, FTP…
- **INTRUSION PREVENTION:** possibilità di bloccare/segnalare attività illecite tipiche di un'intrusione: port scanning, worm, exploit.
- **ANTI SPAM:** possibilità di bloccare il traffico di posta dovuto a SPAM
- **WEB FILTERING:** possibilià di controllare e limitare l'utilizzo aziendale del web sulla base di politiche di sicurezza.

Le due soluzioni proposte sono:

- **SOLUZIONE A – ISS MX3006**
- **SOLUZIONE B – JUNIPER SSG140**

Nella tabella seguente sono elencate per categoria le caratteristiche principali delle due soluzioni. Per ognuna delle categorie è stato espresso una valutazione da parte di Hackingteam; questo allo scopo di fornire un ulteriore parametro di giudizio delle qualità funzionali fornite nella specifica categoria.

	ISS - MX3006	JUNIPER -SSG140
FIREWALL		
Numero Interfaccie	6x 10/100 Mbps	8x 10/100 + 2x 10/100/1000
Interfacce opzionali	NO	SI (2xT1, 2xE1, 1xISDN BRI S/T, 2xSerial)
FW performance	200 Mbps	350 Mbps
VPN performance (3DES)	65 Mbps	100 Mbps
VPN compatibile XP/2000	SI	SI
Client VPN proprietario	NO	SI
HA con recovery sessioni	NO	SI
HD integrato	SI	DISKLESS
Traffic Shaping	NO	SI
Giudizio HT	Discreto	Ottimo
IPS/IDS		
Numero signature	2500+	Non disponibile
Proprietario	SI	SI
Opzionale	NO	SI
Giudizio HT	Ottimo	Buono
WEB FILTERING		
Numero URL	60 Million URLs	Non disponibile
Proprietario	SI	SI
Integrabile con soluzioni esterne	NO	NO
Opzionale	NO	SI
Giudizio HT	Ottimo	Buono
AV		
Numero signature	Non disponibile	100000+
Proprietario	NO	NO
Protocolli	HTTP, FTP, SMTP, POP3	POP3, SMTP, HTTP, IMAP, FTP
Opzionale	SI	SI
Giudizio HT	Buono	Buono
ANTI-SPAM		
Numero signature	200,000+	Non disponibile
Protocolli	SMTP and POP3	SMTP and POP3
Proprietario	SI	SI
Opzionale	NO	SI

Giudizio HT	Ottimo	Buono
MANAGEMENT		
HTTPS	SI	SI
Console centrale (gratuita)	SI	NO (licenziamento a parte)
Host IDS amministrabili con la stessa console	SI	Non disponibili
Facilità di gestione FW	Discreta	Buona
Facilità di gestione FW	Buona	Discreta
Necessita syslog esterno per store dei LOG	NO	SI

2.1 SOLUZIONE A - ISS MX3006

La soluzione A è basata sulla tecnologia ISS, leader nel settore delle soluzioni di Intrusion Detection/Prevention. Il punto di forza di questa soluzione risiede proprio nelle funzionalità applicative di sicurezza quali IPS/IDS, Antispam e Webfiltering, per le quali ISS ha una tecnologia proprietaria ad eccezione del motore AV. ISS ha un team appositamente dedicato alla ricerca delle vulnerabilità di sicurezza (X-Force team), che assicura agli strumenti di IDS e IPS un continuo aggiornamento e una protezione nei confronti degli exploit 0-day.

PRO: ottima soluzione UTM per la protezione IPS, Antispam, AV e Webfiltering. La licenza base integra la protezione IPS, Antispam e Webfiltering. Solo l'AV e' opzionale. Possibilita' di gestire tutti i prodotti ISS con un server centralizzato (SITE PROTECTOR).

CONTRO: soluzione firewall dalle prestazioni non eccelenti, non e' presente il recovery delle sessioni in configurazione HA, non esiste un client VPN proprietario.

2.2 SOLUZIONE B – JUNIPER SSG140

La soluzione B è basata su tecnologia Juniper, leader nel settore delle soluzioni Firewall/VPN. Il punto di forza di questa soluzione risiede proprio nel firewall dalle elevate prestazioni e dalla possibilità di estendere le funzionalità di sicurezza applicativa con un licenziamento a parte. Juniper fornisce soluzioni IDP dalle quali sono derivate le signature incluse nel motore di Deep inspection, attivabili puntualmente sulle politiche del firewall.

PRO: firewall dalle prestazioni elevate con funzionalità di traffic shaping.

CONTRO: necessità di un server esterno per la conservazione dei log e maggiore complessità della gestione della soluzione di IDP. Poca flessibilità delle configurazioni Antispam e Webfiltering.

2.3 CONCLUSIONI

- La soluzione A privilegia gli aspetti di sicurezza applicativa ed è particolarmente adatta per rispondere ad esigenze di questo tipo.
- La soluzione B privilegia gli aspetti di firewall/VPN e rappresenta una scelta ottimale solo se non ci sono particolari esigenze in termini di sicurezza applicativa.

3 Protezione server critici – ISS Server Sensor

Per la protezione dei server critici si è scelta la soluzione di Host Intrusion Detection di ISS (Proventia Server Sensor). Questa soluzione consente di controllare e proteggere i sistemi critici aziendali attraverso diverse funzionalità:

- **Audit degli eventi di sistema**: logon fallite e riuscite, cambio delle politiche di sicurezza…
- **Protezione IDS**: le stesse signature di attacchi presenti nella famiglia di IPS ISS sono implementate nella soluzion HOST allo scopo di prevenire exploit, escalation di privilegi e DOS.
- **File di log specifici**: possibilità di controllare file di log specifici e segnalare eventi personalizzati.
- **Azioni**: possibilità di bloccare l'attacco, eseguire script.

La soluzione si basa su una componete software, disponibile per sistemi operativi Microsoft, IBM AIX, Linux e Solaris. Gli agenti sono controllati centralmente attraverso il server di management SITE PROTECTOR che gestisce:

- Politiche di sicurezza
- Log e reportistica
- Aggiornamenti

In caso si opti per la SOLUZIONE A per la difesa perimetrale, la console di management sarà la stessa anche per il firewall.

4 Log management e allarmistica – Network Intelligence

La soluzione proposta si basa sulla tecnologia Network Intelligence serie EX, un appliance in grado di centralizzare i log provenienti dai diversi sistemi informativi aziendali. Le funzionalità offerte da questo appliance includono:

- Reportistica centralizzata predefinita e possibilità di personalizzazione della reportistica.
- Correlazione e allarmistica: possibilità di attivare regole predefinite o costruirne di proprie

- Retention dei log: conservazione a scopi legali dei log aziendali
- Enterprise dashborad: cruscotto per la presentazione grafica degli allarmi generati.