

hakin9

Come difendersi

Hard Core IT Security Magazine N° 2/2007 (13) Febbraio prezzo: 7,50 € ISSN: 1733-2095 Mensile

Analisi remota di un host

LIVE TRAINING CENTER
avvia
allenati
impara
27 tutorial

+

Rainbow Tables Password Cracking
ARP poisoning: attacco alle reti locali
LDAP everywhere!
Network Admission Control

PRINCIPIANTE

La privacy del nostro cellulare

NEI CD:

CCNA di Cisco – corso di certificazione – parte 2

VERSIONE COMPLETA:

Eltima Powered Keylogger - versione semestrale,
Uniblue System Tweaker,
10-strike LANState 1.2,
VIP Privacy
+ NetIntercept 3.2 Software Demo



Test di consumatori

Firewall



Aziende Italia S.r.l.

Via San Gondonzo, 109
00189 Roma
Italia
<http://www.webperte.com>

Federico d'Ormea
Responsabile sicurezza servizi
hosting e server dedicati

Il nome del firewall e il suo produttore:

Fortinet Fortigate 100A.

Pensi che è stata una buona scelta?

Assolutamente è soddisfacente.

A mio avviso resta una scelta ottima per tutte quelle realtà dove si ha bisogno di una soluzione di sicurezza perimetrale completa con servizi supplementari al firewalling classico.

Con il fortigate, in particolare con l'ultima release del firmware, si ha a disposizione non solo un ottimo appliance dedicato alla sicurezza, ma anche un potente strumento di networking in generale e questo senza dover sopportare costi allucinanti.

Il suo prezzo è adeguato alle funzioni?

Se considerassimo il costo separato di un firewall, di un sistema IDS/IPS, di un antivirus, di un antispam (sempre perimetrale), di un prodotto di web content filtering e di un concentratore VPN over SSL, sicuramente dovremmo considerare una spesa maggiore rispetto al prodotto di cui scriviamo.

È in accordo con le vostre aspettative?

Direi proprio di sì. La nostra azienda fornisce soluzioni di hosting, server dedicati e server virtuali quindi siamo quotidianamente soggetti ai più svariati attacchi, dai più semplici a quelli più complessi.

Inoltre l'idea di racchiudere in un unico apparato anche un supporto di web content filtering unitamente a servizi antispam e antivirus rende questo prodotto estremamente flessibile. Per queste ragioni non possiamo che esserne soddisfatti.

Le sue qualità?

È un apparato con diverse funzionalità quali Firewalling - IDS - Antivirus - Antispam - Web Content Filtering e, cosa estremamente interessante, con la nuova versione del firmware è in grado anche di offrire la possibilità di VPN over SSL.

L'apparecchio dispone di un sistema operativo proprietario che si chiama FortiOS. Molto apprezzabile l'interfaccia grafica che consente di operare a 360 gradi.

Immane l'interfaccia testuale in SSH ma va detto che dalla GUI è possibile fare il 90% delle operazioni.

Può operare in due modalità: TRASPARENTE e NAT/ROUTE. A livello di connettività offre 4 porte switch, 2 porte DMZ e 2 Porte wan.

Complessivamente quindi è in grado di offrire la gestione di 2 DMZ separate ad esempio per separare server e servizi Web e Email e 2 connettività separate.

Dispone di 2 connettività separate, opzione particolarmente utile in tutti quei casi in cui si vogliono creare strutture ridondate o di Load Balancing del traffico.

L'apparato offre anche tutta una serie di opzioni legate al logging del traffico.

Nel caso di una rete in cui il firewall è attivo subito *dietro* la connettività, tramite le funzioni di gestione dei log è possibile fare delle verifiche accuratissime distinguendo servizi e tipologie di traffico passante.

Inoltre, con i modelli più grandi si possono affrontare discorsi HA dei firewall o di stack e usufruire di collegamenti anche in fibra ottica.

I suoi difetti?

Personalmente al Fortinet riscontro un solo difetto e cioè quello di non avere delle performance eccezionali in modalità Trasparente.

Se però consideriamo che è insito nella natura dei firewall lavorare diciamo a livello 3 più che a livello 2 possiamo capire che si tratta di un difetto *relativo*.

Inoltre, per esigenze diverse, il Fortinet dispone anche di sistemi proprietari di management e di gestione dei log.

Il voto 1–5 (1– pessimo, 5– ottimo)

★★★★



DiNets s.r.l.

Francesco Aruzzoli
Sede: ss 16 Adriatica 28/i -
60027 Osimo (AN) ITALY
Telefono: +39 071 7211234
Fax: +39 071 7213365
E-Mail: info@dinets.it
Web: www.dinets.it

Il nome del firewall e il suo produttore:

Netscreen Firewall, Juniper

Pensi che è stata una buona scelta?

Sì, come installatori, gestori e utilizzatori di queste soluzioni abbiamo riscontrato maggiori prestazioni, funzionalità, facilità d'uso, integrazione e personalizzazione rispetto alla concorrenza; il prodotto si presenta come un'appliance di dimensioni sempre molto contenute anche nelle versioni di fascia alta, pronto da installare e configurare.

Il suo prezzo è adeguato alle sue funzioni?

Sì, grazie ad un'ottima segmentazione del mercato dispone di vari modelli di prodotti con le funzionalità necessarie per ogni fascia di utenza (dalla piccola azienda a quella enterprise).

È in accordo con le vostre aspettative?

Sì, nel complesso il prodotto è ottimo dal punto di vista funzionale e buono dal punto di vista del supporto tecnico. Tutti i prodotti si presentano ben imballati, corredati di manuali cartacei sintetici ma efficaci, documentazione elettronica soddisfacente e con tutti gli accessori necessari per l'installazione.

Le sue qualità?

La nuova generazione dei firewall juniper grazie ai nuovi processori ASIC Gigascreen permette maggiori prestazioni e maggiore flessibilità, nelle versioni di fascia medio alta risulta essere la prima piattaforma integrata per il supporto di funzionalità Firewall, VPN e IDS/IDP (firewalling a livello 7); funzionalità complete, facile da gestire anche in architetture complesse, ottima modularità. Per il management centralizzato di più apparati dispone di un software (da acquistare separatamente) facile e potente da utilizzare che permette la gestione e la distribuzione (programmate e/o per gruppi) di policy e configurazioni, aggiornamenti remoti di firmware e gestione con correlazione di log e report dettagliati.

I suoi difetti?

Nessun difetto di rilievo, potrebbe però migliorare le politiche sulle licenze di base degli utenti e del maintenance

(una scelta meno ristrettiva nelle licenze sul numero degli utenti e prezzi leggermente più bassi sul maintenance potrebbe fargli guadagnare più fette di mercato).

Il voto 1-5 (1-pessimo, 5-ottimo):

★★★★★



Pierpaolo Palazzoli

SnortAttack

Il nome del firewall e il suo produttore:

Netscreen modelli 25 e 5GT

Pensi che è stata una buona scelta?

Ottima, I firewall netscreen permettono di gestire tutte le funzionalità con frontend web, da linea di comando e NMS. L'approccio alle VPN è ben strutturato e particolareggiato, di modo da ottenere il massimo dalla crittografia IPSEC. La architettura del firewall è basata su HW ASIC permette di avere le massime prestazioni HW/SW. La parte di routing è in forte sviluppo data la fusione con Juniper, di pregevole interesse sono: l'opzione Dual Untrusted che permette la gestione di linee di backup, il source routing, VPN policy based e QOS su VPN.

È in accordo con le vostre aspettative?

Assolutamente sì, a parere mio il firewall deve essere un oggetto che dopo l'installazione deve essere *dimenticato* l'unica attività deve essere l'aggiornamento delle policy. Il firewall non dovrebbe essere mai riavviato. Il netscreen queste qualità le implementa molto bene.

Il suo prezzo è adeguato alle sue funzioni?

Nei modelli ad alte prestazioni (ISG100...) sì. Nei modelli base non sono accessibili a tutte le aziende ma di sicuro di superiore qualità alla media.

Le sue qualità?

Performance, configurabilità, continuità di servizio, velocità grazie ad una architettura ASIC.

I suoi difetti?

Il parser dell'interfaccia web non è impeccabile, alcune funzionalità dell'interfaccia web funziona solo con explorer.

Il voto 1-5 (1-pessimo, 5-ottimo):

★★★★★



Technomind S.p.A.

via G.Galilei,
20124 Milano
Italia
www.technomind.it

Stefano Maccaglia
CSO e Responsabile del Technomind Security Center
viale Città d'Europa, 681
00144 Roma
Italia

Il nome del firewall e il suo produttore:

Cisco PIX 515E della Cisco e Netscreen 204 della Juniper Networks

Pensi che è stata una buona scelta?

Sì, indubbiamente, entrambi sono stati un'ottima scelta.

Il suo prezzo è adeguato alle sue funzioni?

Sì. Garantisce un'ottimo rapporto/prezzo prestazioni sia il PIX che i Netscreen.

Il PIX offre un buon compromesso tra costi e caratteristiche, non ha alcune feature avanzate presenti in alcuni altri firewall commerciali, come ad esempio Check Point, ma per me un firewall è un firewall... se Cisco dovesse tentare di integrare feature aggiuntive senza un vero beta testing e un reale controllo (come capita per ISS o Check Point) è possibile che il firewall stesso non funzioni più così bene...

Stesso discorso per il Netscreen, non a caso li ho scelti io...

È in accordo con le vostre aspettative?

Sì. Anche in questo caso entrambi sono facili da installare (per chi ha esperienza) e facili da gestire. Non si possono mettere nelle mani di uno poco esperto.

Le sue qualità?

Per il PIX: Performance, facilità di installazione, e gestione. Il NETSCREEN è più ampio nella customizzazione, abbastanza semplice da gestire ed ha un'interfaccia meglio organizzata sia web che CLI.

Un altro firewall che mi piace molto è ASTARO Security Linux, ma è fuori mercato per il costo troppo alto (secondo me).

Ultimamente mi piacciono anche i prodotti della Stonesoft (Stonegate), ma ancora li sto testando e non posso darne un parere approfondito.

I suoi difetti?

Per il PIX: Un po' confusionario nella gestione delle ACL. Per il NETSCREEN: in modalità Trasparent ha volte mi ha dato qualche grattacapo.

Ho molti anni di configurazioni alle spalle e so che non sono semplici da impostare per chi è alle prime armi, ma se hai esperienza non hai molto altro da scegliere (nell'ambito commerciale).

La carenza maggiore sia nei PIX che nei NETSCREEN è dovuta alla mancanza di scalabilità della soluzione di management. Mi spiego meglio... fin quando hai un paio di PIX o di Netscreen in azienda non ci sono molti problemi nel gestirli.

Ti connetti via SSH e con la CLI li configuri... se però devi metterli in mano a persone meno esperte che chiedono la solita interfaccia grafica questi due prodotti sono un po' *avari* di features. In aggiunta se devi controllarne molti contemporaneamente allora diventa difficile gestirli in maniera umana, se non ricorrendo a software terze parti come SOLSoft che però costano molto.

Il PIX ha il difetto che per filosofia si configura come un router (non a caso il suo software è stato sviluppato integrando quello dei Router), ovvero con le Access-list che però a volte diventano troppe e confusionarie...

Il Netscreen ha invece qualche problema quando, lavorando in transparent mode, si trova a scontrarsi con il forwarding di multicast o di altri protocolli *anomali*...

Per il resto sia l'uno che l'altro sono molto affidabili.

Il voto 1-5 (1-pessimo, 5-ottimo):

(da notare che non ho ancora trovato il firewall perfetto e quindi il 5 non l'avrei dato a nessuno).

PIX: ★★★★★,
NETSCREEN ★★★★★

RE@LITY NET – System Solutions S.n.c.

La Consulenza nel Mondo dell'Informatica
via Assarotti 4/1
16122 Genova
www.realitynet.it

Il nome del firewall e il suo produttore?

Il firewall prodotto dalla 3COM. Il nome del prodotto è 3ComR OfficeConnectR ADSL Wireless 54 Mbps 11g Firewall Router. Il codice del prodotto è 3CRWDR101A-75.

Pensi che è stata una buona scelta?

È stata una buona scelta. Questo prodotto è assolutamente adeguato per un utilizzo in una realtà SOHO. Infatti integra diverse funzionalità, tra cui: connettività ADSL con supporto per ADSL 2+, connettività Wireless con supporto di WPA e WEP Encryption, Switch da 4 porte, Firewall.

Il suo prezzo è adeguato alle sue funzioni?

Il prezzo è molto economico (110 euro IVA inclusa - listino Novembre 2006) direi che è adeguato rispetto alle funzionalità che il prodotto offre. Ne sono soddisfatto.

È in accordo con le vostre aspettative?

Il prodotto offre buone garanzie di protezione da accessi indesiderati.

Svolge adeguatamente il suo ruolo sia per la protezione delle postazioni dedicate alla navigazione sia per un web server cui è collegato.

Le sue qualità?

Ottime funzionalità hackerpattern detection, stateful packet inspection e url filtering.

I suoi difetti?

La principale pecca del prodotto è dovuta al fatto che non supporta le VPN. L'altro difetto è la lentezza dell'accesso alla pagina di configurazione via web.

Il voto 1-5 (1-pessimo, 5-ottimo)?

★★★★

**Ez Konz**

Via Casola 12
80067 Sorrento (NA)
P.Iva 05431661213
Tel & Fax +39 081 532 3696
email: info@ezcons.com
web: www.ezcons.com

Il nome del firewall e il suo produttore:

Netfilter/IpTables 1.3.5, progetto Open Source sviluppato da Netfilter Core Team. È possibile installarlo su sistemi operativi basati sul Kernel Linux 2.4.X e 2.6.X

Pensi che è stata una buona scelta?

Prodotto di punta per la sua flessibilità e configurabilità. Infatti può essere plasmato a proprio piacimento applicando regole di filtraggio in base a:

- Indirizzi sorgente o destinazione,
- Porta sorgente o destinazione,
- Tipo di protocollo (TCP, UDP, ICMP),
- Flag TCP (SYN, ACK, RST, PSH, FYN),
- Interfaccia d'ingresso o d'uscita.

Offre la possibilità del connection-tracking ovvero di abilitare solo alcuni tipi di connessioni (ad esempio quelle ini-

ziate dall'interno) e di utilizzare quei protocolli che come l'FTP necessitano di porte assegnate dinamicamente.

Iptables consente inoltre di registrare molte delle informazioni contenute nei pacchetti, così come è possibile stabilire la frequenza con cui un certo evento debba essere registrato; ad esempio è possibile stabilire che 1 su 10 pacchetti che soddisfino un dato prerequisito siano registrati.

Il software implementa il NAT sia sorgente che destinazione, nonché permette di effettuare elaborazioni sui pacchetti; è possibile modificarne alcuni campi IP come il TOS o il TTL. Permette di gestire i pacchetti in base al loro proprietario; per pacchetti generati dal firewall stesso è per esempio possibile stabilire regole in base all'utente che ha generato quel pacchetto. Mette a disposizione la possibilità di selezionare i pacchetti che verificano una data regola trasferendoli ad un'applicazione in user-space; questo consente di sviluppare codice, per la manipolazione dei pacchetti, in user-space invece che in kernel-space.

Con iptables non è possibile ispezionare il campo dati dei pacchetti ed in questo senso non può essere considerato un application filtering firewall.

Il suo prezzo è adeguato alle sue funzioni?

È un prodotto Open Source sotto licenza GNU GPL, quindi è gratuito, liberamente scaricabile dalla rete (www.netfilter.org).

Per una media grande azienda che ha la figura dell'amministratore di rete è sicuramente il prodotto che deve essere adottato, in quanto non necessita di strabilianti caratteristiche hardware per funzionare (un personal computer di qualche anno fa va più che bene), ma semplicemente di un buon amministratore che possa sfruttare pienamente tutte le sue capacità.

È in accordo con le vostre aspettative?

Non è un prodotto semplice da gestire e da configurare, richiede un minimo di esperienza in ambiente linux, quindi non è adatto sicuramente all'utenza domestica o a piccole aziende con pochi terminali;

È un ottimo prodotto se aggiornato costantemente e configurato correttamente.

Le sue qualità?

È gratuito e molto flessibile. Necessita di poche risorse hardware. Sul sito di riferimento è presente un'ottima guida dettagliata.

I suoi difetti?

Il maggior difetto è che non esiste una versione per windows.

Non esiste neanche un modulo per l'aggiornamento automatico.

Il voto 1-5 (1-pessimo, 5-ottimo)

★★★★★