TEST CENTER

Una barriera per la rete

L'appliance Vital Security NG-5100 di Finjan Software permette di controllare le varie minacce che operano a diversi livelli della pila OSI per attaccare la rete aziendale.

APPLIANCE

Vital Security NG-5100 offre funzioni di rilevamento dei malware anche nei cosiddetti 'zero day attack'

È stata la diffusione di Java l'elemento che ha portato alla nascita di Finjan Software: l'idea era che Java avrebbe portato a una rivoluzione su Internet con l'aggiunta, a pagine statiche e in buona parte prettamente testuali, di un codice che non aveva bisogno di essere compilato. Se questo ha migliorato l'esperienza di Internet, ha d'altro canto creato anche dei nuovi paradigmi per la sicurezza: i rischi per la sicurezza non sono stati più integrati solo con la posta elettronica ma anche con altri protocolli che agiscono trasversalmente ai sette livelli canonici della pila OSI.

Dal punto di vista tecnico Finjan ha quindi sviluppato diversi sistemi software basati anche su una serie di algoritmi proprietari. Da qualche tempo l'azienda ha deciso di lanciare sul mercato anche appliance, basati su Linux. E' uno di questi che abbiamo provato: il Vital Security NG-5100 dedicato alla fascia midrange dell'utenza, da 250 a ben ventimila utenti. Il prodotto ci è stato fornito dal suo distributore, Alias.

IL PRIMO IMPATTO

L'appliance è esteticamente analogo a tutti i modelli di questo tipo di prodotti: di dimensioni contenute (è alto 1U) può essere installato in rack mediante le staffe che possiamo trovare nella confezione, oppure - in casi più rari - utilizzato in stile desktop. La macchina è però tutt'altro che silenziosa (monta tre ventole, il che elimina problemi di surriscaldamento ma non aiuta la quiete) e i decibel che sono normali in un wiring closet non saranno apprezzati dai compagni di ufficio dell'IT manager.

Il modello che abbiamo provato dispone sul frontale di sei porte di rete, due Gigabit e quattro Fast Ethernet. La porta Fast più a sinistra marchiata FE5 va connessa, in fase di configurazione, direttamente a un pc usando un cavo crossover oppure a uno switch o hub attraverso cui raggiungere l'appliance Finjan. Sul frontale della macchina troviamo anche la porta seriale di gestione e un mini-pannello di controllo a cristalli liquidi che mostra informazioni sulla versione del sistema operativo (la 8.2.05, nel nostro caso) e sul carico della CPU e, inoltre, permette di comandare il reset dell'indirizzo della porta FE5 e lo shutdown della macchina. Sul lato posteriore troviamo invece una porta video e due USB, oltre ovviamente all'interruttore dell'alimentazione.

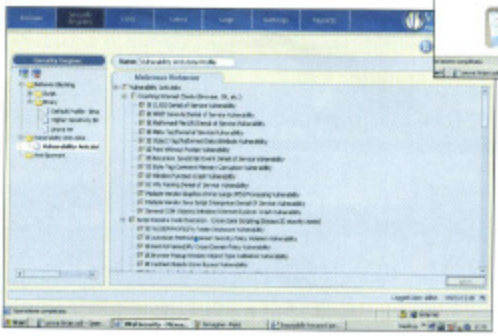
Una volta installata e accesa la macchina, si passa alla configurazione. Avviene, come ormai è tipico, attraverso un'interfaccia Web detta Setup Console e divisa in due parti: il setup iniziale e le configurazioni avanzate. L'accesso al Web server interno della macchina avviene via HTTPS e con scambio di certificati digitali, per una maggiore sicurezza. Un solo dettaglio: gli IT manager che vengono frequentemente distratti nel loro lavoro tengano conto che la connessione alla console di gestione 'scade' dopo otto minuti di inattività del client.

IL WIZARD TI DÀ UNA MANO

Il setup iniziale viene guidato da un vero e proprio wizard passo per passo. Il primo step è definire che compito deve svolgere in rete l'appliance che si sta installando: Policy Server, Scanning Server o entrambi. Non esiste una configurazione consigliata in questo senso, ossia non è a priori possibile dire se sia più conveniente avere una macchina 'tuttofare' o averne due separate per compito. In generale una

configurazione 'dual' garantisce una certa ridondanza e un utilizzo mirato. Ovviamente i costi di acquisto sono superiori, in questo caso.

Il NG-5100 opera tra l'altro come sistema antivirus e di URL filtering. La sua peculiarità in questi casi sta nel fatto che può utilizzare contemporaneamente i database e i file di definizione di provider diversi: Sophos e McAfee nel caso degli antivirus, SurfControl e Secure Computing per la parte di URL filtering. Quali utilizzare va definito nella parte di setup, insieme alle funzioni di casa Finjan (Application Level Behavior Blocking, Vulnerability Anti.dote e Anti-Spyware) da attivare. La parte successiva del setup riguarda alcuni parametri tecnici di connessione (porte di gestione, gateway, DNS, router) e il cambio della password di amministratore per il dopo-setup. Tutti i parametri richiesti non dovrebbero creare problemi all'IT manager e, dopo questa fase, la macchina è funzionante.



Una piccola pecca in questa fase è che l'appliance non è molto 'loquace' una volta cliccato sul link "Apply" che forza appunto la nuova configurazione. Dato che il processo di attivazione della nuova configurazione richiede qualche minuto, si resta davanti al browser senza esattamente sapere a che punto si è. Si tenga anche presente che a questo punto la porta Ethernet usata viene 'chiusa' e bisogna riconnettersi su quella definita nel setup, che ha un indirizzo IP differente.

L'appliance di Finjan Software ha il suo punto di forza nella versatilità, ma richiede mani piuttosto esperte

Tutti i parametri richiesti dal Setup Wizard sono in realtà configurabili allo stesso modo dalla sezione di configurazione avanzata (Advanced Settings). Essa si divide in nove sottosezioni (Appliance Roles, Time Settings, Access Control List, Licensing, Network Settings, Restart Role, Custom Commands, Change Password, Reboot/Shutdown Appliance) che sono tutte abbastanza autoesplicative. Nella parte di Network Settings si segnala la sezione dedicata alla risoluzione dei problemi, che mette a disposizione dell'IT manager alcuni strumenti di uso comune (ping, traceroute, dumping del traffico TCP su una porta...) direttamente dal 'cuore' Linux della macchina.

INTERFACCIA COMPLETA

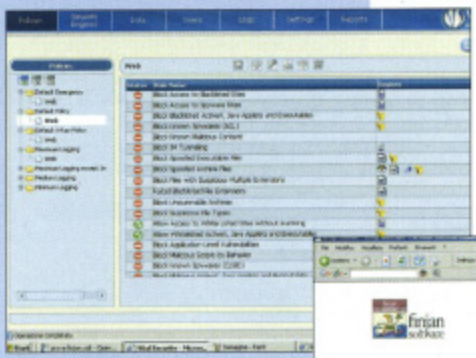
Fatta la configurazione, si passa alla gestione. L'interfaccia è diversa, sempre HTML (si tratta di una applet Java) ma più complessa e dall'aspetto decisamente professionale, simile a quello di vere e proprie piattaforme di network management. Dalla console si accede a sette sottosezioni (Policies, Security Engines, Lists, Users, Logs, Settings, Reports) anche in questo

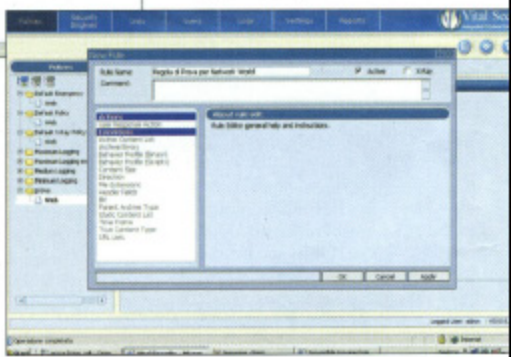
Due schermate importanti per un CSO: qui sopra la console di setup, a fianco la sezione Security Engines del modulo di gestione

L'offerta in breve

La gamma di prodotti Finjan Software è suddivisa in tre fasce di apparati. La prima (dai 25 ai 250 utenti) include le famiglie 1Box e Vital Security NG-1000 (che sfrutta tutte le tecnologie Finjan). La gamma midrange (dai 250 a 20 mila utenti) include i sistemi Vital Security NG-5000 oggetto della prova mentre in fascia alta (fino a 250 mila utenti) si posiziona la serie modulare NG-8000 (basata su IBM BladeCenter). "I prodotti su cui puntiamo per il mercato italiano, considerate le dimensioni delle imprese, sono quelli della prima e seconda fascia anche se in ogni caso non escludiamo a priori opportunità anche per i sistemi più grandi", commenta Stefano Cucit, responsabile business development di Alias, distributore per l'Italia di Finjan Software.

caso denominate in modo abbastanza autoesplicativo. Semplici da comprendere non significa però limitate nelle funzionalità: l'IT manager a questo punto può definire policy sui contenuti e sul traffico di rete praticamente di tutti i generi e in base a un numero di parametri (direzione del traffico, uso di IM, estensioni dei file, dimensioni dei file, contenuto binario, intervalli di tempo, header...) molto elevato. Lo stesso dicasi per la parte dei Security Engines di Finjan: il controllo sui contenuti e sul loro comportamento può tenere conto di un grande numero di variabili, ad esempio se una applet Java cambia i registri di sistema o se un controllo ActiveX è programmato per cercare di accedere alla rete.





Altre tre schermate del software dell'appliance. Si nota in particolare, a destra e qui in alto, la parte di definizione delle policy

Il ragionamento vale, infine, anche per la parte di gestione delle liste di tutto ciò che in rete è ammesso o proibito: URL, contenuti, estensioni dei file, dimensioni degli attach, intervalli di tempo sono tutti parametri che possono essere usati nelle operazioni di controllo.

Tra le varie sottosezioni della console di gestione, quella dei Settings è particolarmente importante, perché rappresenta una sorta di ponte di comando dal quale si gestiscono diversi parametri importanti delle macchine Finjan e soprattutto la parte degli aggiornamenti software. Questi sono essenziali perché il funzionamento corretto di alcune delle feature della macchina dipende proprio dalla frequenza degli update dei suoi database. In questa sezione si trovano anche i pannelli per la configurazione dei valori di default di alcuni protocolli usati dal NG-5100 (HTTP, ICAP, autenticazione...).

Anche in questo caso si evidenzia come il NG-5100 richieda, se si vuole andare oltre le impostazioni di default, una competenza da IT manager di media azienda, che è poi il target del prodotto in sé. Chiude la serie la parte Report, che contiene una settantina di report predefiniti visualizzabili via Web.

VALUTAZIONI CONCLUSIVE

L'appliance Finjan ha nella versatilità il suo punto di forza: dalla console di gestione è possibile fare sostanzialmente di tutto, sfruttando pienamente le funzioni della macchina. Il dispositivo è ampiamente scalabile in quanto a numero di utenti gestibili e la possibilità di avere configurazioni ridondanti o in cluster ne amplia gli scenari di utilizzo sino a comprendere, crediamo, le esigenze di gran parte delle imprese italiane.

Non è un appliance per gli IT manager poco esperti, però. Chi non riuscisse ad andare oltre i wizard, che pure sono presenti e completi, avrebbe un sistema funzionante ma ben al di sotto delle sue potenzialità. Queste diventano evidenti quando l'IT manager usa il software di gestione per creare policy su misura per la sua rete, 'cucendosi adosso' - per così dire - l'apparato. **nw_lab**

in breve

Finjan Vital Security NG-5100

Appliance per la protezione della rete che offre 'tutela' a vari livelli della pila ISO-OSI, esaminando i contenuti in transito sulla rete indipendentemente dal loro protocollo.

PRODUTTORE
Finjan Software

PREZZO
3.930 euro IVA esclusa

PRO
Completezza delle funzioni, elasticità di configurazione, adattabile alle proprie esigenze in fase di definizione delle policy

CONTRO
Richiede un IT manager esperto