

Endian UTM Mercury

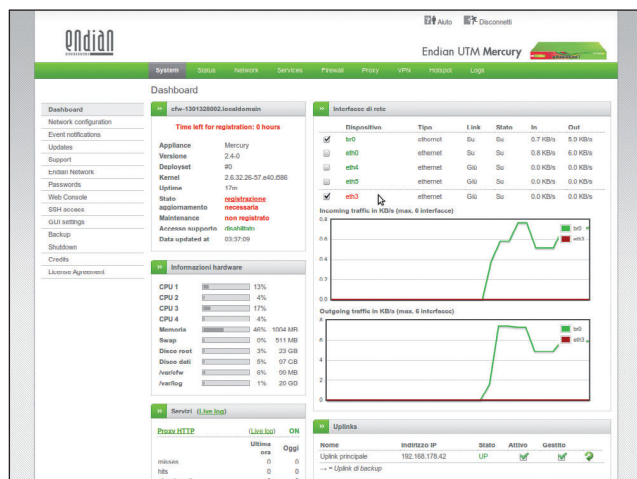
La sicurezza per le reti piccole e medie è targata Open Source

Una rete aziendale deve fornire svariati tipi di servizi garantendo al contempo un alto livello di sicurezza per i suoi utenti. Per ottenere questi risultati e facilitare il lavoro dei sysadmin sono stati sviluppati dei dispositivi detti **UTM** (Unified Threat Management) che unificano in un'unica soluzione diverse funzioni: proxy Web, filtro antispam, antivirus, firewall e gestione delle VPN. Inoltre esistono prodotti UTM di diverse prestazioni e prezzo in base alla tipologia di rete che si vuole proteggere. Questo mese abbiamo provato un prodotto, l'Endian UTM Mercury pensato per le reti di aziende medio/piccole, da 10 a 100 utenti e basato su Linux e su diversi software Open Source.

Setup guidato

Il dispositivo di Endian ha caratteristiche hardware di tutto rispetto (le trovate nel box Specifiche hardware) come la CPU dual-core che garantisce ottime prestazioni e le 6 porte di rete Gigabit che offrono una grande versatilità per quel che riguarda l'impostazione di varie zone (DMZ, rete interna, sottoreti, WAN failover, ecc.). Non è presente un'interfaccia Wi-Fi, quindi bisogna ricorrere ad altri apparati wireless; visto l'alto prezzo del prodotto, ci saremmo aspettati anche questo

tipo di funzionalità. Le porte USB servono per collegare unità a dischi esterne o chiavi USB (per il backup, come vedrete più avanti) oppure una chiave 3G. Endian ha abbondato anche con lo spazio su disco, con due hard disk tradizionali da 160 GB configurati in modalità RAID 1: abilitando molte funzioni di log e con un sistema in attività per qualche anno si potrebbe arrivare a collezionare diversi GB di log. Alla prima accensione è ovviamente necessario configurare il dispositivo collegando un cavo di rete alla prima porta Ethernet (che risponde all'IP 192.168.0.15) e accedendo a un comodo wizard tramite il browser. Anche i successivi interventi di gestione e manutenzione dell'Endian UTM Mercury si svolgono tramite una completa e articolata interfaccia Web ma, essendo un sistema Linux, si può accedere alla shell via SSH, anche se si consiglia di farlo solo per compiere operazioni avanzate di debug o altre cose che vanno oltre la normale configurazione. Tornando alla procedura guidata di configurazione, essa si divide in otto fasi (10 schermate in totale) durante le quali si possono definire le varie zone (green, red, orange e blue) associando a ognuna le porte di rete che interessano. Si può anche importare



La prima pagina dell'interfaccia Web offre un'accurata panoramica dello stato del dispositivo e fornisce l'accesso ai numerosi menu di configurazione

un'eventuale configurazione salvata su chiave USB, definire le password per l'accesso Web e SSH e la lingua dell'interfaccia. Infine ci si può registrare presso Endian per attivare il supporto. Una conoscenza di base sulle reti e un po' di esperienza sono sufficienti per superare questa fase senza intoppi.

Tutto sotto controllo

Terminata la configurazione si può accedere finalmente all'interfaccia Web di gestione. La prima schermata fornisce un riepilogo della situazione e subito a prima vista se ne può intuire la doverosa complessità, visti i tanti menu presenti. Per gestire il tutto, infatti, è necessario un utente che sappia muoversi tra le varie opzioni e configurazioni, anche se tutto è strutturato in modo ottimale. In alto si trovano ben nove menu (System, Status, Network, Services, Firewall, Proxy, VPN, Hotspot e Logs), in pratica le nove "categorie" di funzionalità dell'UTM, e ognuna di queste voci, una volta selezionata, fa apparire due sottomenu diversi, uno sulla sinistra e uno subito sotto il menu principale. Vediamo lo scopo dei menu principali. La voce System offre, tra le altre cose, l'opzione per la configurazione della rete,

la console Web, il controllo dell'accesso via SSH e il backup. Da quest'ultima voce si può definire di cosa fare il backup (impostazioni, log, ecc.) e schedarne l'esecuzione. Le possibilità sono diverse, ad esempio lasciando una chiave USB in una delle porte USB ogni notte verrà effettuato automaticamente un backup completo, di questi solo gli ultimi tre (quindi gli ultimi tre giorni) rimarranno sul dispositivo. Si può decidere anche di ricevere via mail delle notifiche quando accadono determinati eventi, anzi con le funzionalità Hotspot+Smart Connect attive è possibile anche acquistare degli SMS anche per le notifiche degli eventi di sistema. Gli SMS verranno comunque veicolati tramite Endian Network che a sua volta inoltra a servizi online di gateway SMS. Il menu Status, come si può intuire dal nome, fornisce tutti i dettagli sul funzionamento della macchina e dei servizi, indicando quali sono attivi e quali no. Le informazioni vengono mostrate in forma tabellare e tramite diversi grafici. Ma è con Services che si inizia a entrare nel cuore dell'UTM. Da qui si controllano il DHCP, l'accesso a un eventuale servizio di DNS dinamico (sono supportati 14 servizi diversi), ma soprattutto si

Specifiche hardware

- **Case Rack:** Rack 19" 1 U
- **Alimentatore:** interno 300 Watt
- **CPU:** Dual-Core
- **Memoria:** 1 GB (DDR2 667 MHz)
- **Ethernet:** 6 x GigE (10/100/1000)
- **Hard disk:** 2 x 160 GB (RAID 1)
- **Raffreddamento:** ventola
- **Dimensioni:** 44x425x240 mm
- **Peso:** 3,4 kg
- **Display LCD**
- **Garanzia hardware:** 12 mesi
- **Certificazioni:** FCC/CE/ROHS

Prestazioni

- **Utenti consigliati:** 10-100
 - **Firewall Throughput:** 500 Mbps
 - **Connessioni simultanee:** 500.000
 - **VPN Throughput:** 55 Mbps
 - **IPS Throughput:** 55 Mbps
 - **UTM Throughput:** 50 Mbps
 - **E-mail per giorno:** 340.000*
- * Con antivirus e antispam abilitati.

Endian UTM Mercury Test



Un ottimo UTM se cercate alte prestazioni, ma occhio al prezzo

incontrano le voci di configurazione di alcuni dei software Open Source di qualità integrati, come ClamAV (antivirus), Ntop (monitoraggio del traffico) e Snort (IDS). Per cui da Services si gestisce la frequenza degli aggiornamenti del database dei virus (direttamente dal sito di ClamAV), l'attivazione dello spam training, si attiva l'IDS, si controlla fin nei minimi particolari il traffico che passa dall'UTM e si attiva anche la funzione di High Availability. Per Snort il sistema usa le regole open basate sulla community www.emergingthreats.net, aggiornabili a intervalli di tempo pianificati. Queste regole possono essere modificate grazie a un editor integrato nell'interfaccia, e si possono anche inserire nuove regole personalizzate. Qualche dettaglio anche sull'alta affidabilità (utilizzabile avendo due dispositivi uguali o configurati con lo stesso numero di porte): la HA è di tipo hot-standby/scorta a caldo, non si effettua bilanciamento del carico se non per il DHCP e per configurare l'HA si imposta il master, anche con una configurazione basilare, mentre lo slave può essere configurato anche in modalità gateway (una sola scheda di rete come se fosse un normale server/

host) con un IP interno alla LAN del master. A questo punto si configura il servizio HA su entrambi i sistemi (IP, password, e-mail e poco altro). Una volta attivato il servizio lo slave perderà tutte le configurazioni ereditando quelle del master. Lo slave avrà i servizi attivi ma le interfacce di rete tutte disattivate eccetto quella dove effettua il *keepalive*; ogni modifica del master verrà sincronizzata anche sullo slave. Infine, sempre da Services, si può gestire la QoS (Quality of Service) e l'utilizzo della banda in modo molto accurato.

Sicurezza di rete

Accedendo ai menu Firewall e Proxy si controllano tutte le altre voci relative alla sicurezza della rete. Firewall offre un controllo con una ottima granularità in base a servizi, porte e protocolli. Per attivare filtri a livello 7 (il livello applicativo) – ad esempio se si vuole bloccare l'invio di file dai client di IM – si deve ricorrere a servizi di proxy e Intrusion Prevention System. Il firewall gestisce port forwarding/Nat, si possono stabilire regole per il traffico in uscita o quello inter-zona e anche per il traffico su VPN. Il menu Proxy offre l'accesso al potente Dansguardian per quel



Il dispositivo di Endian ha tutte le porte di rete che vi possono servire e anche funzionalità che non sempre si trovano (come il captive portal), manca però in Wi-Fi integrato

che riguarda il filtraggio dei contenuti, oltre a usare il sistema di blacklist del progetto <http://urlblacklist.com>. Inoltre si può impostare il proxy HTTP/FTP in modo trasparente o non trasparente, attivare il controllo antivirus e altro ancora. L'autenticazione degli utenti che possono uscire su Internet con le modalità specificate avviene tramite autenticazione locale o appoggiandosi a Windows Active Directory, LDAP o RADIUS. È anche possibile attivare delle restrizioni di tempo, ad esempio. Il proxy agisce anche su SMTP e POP3 con antivirus, antispyware e greylisting. C'è anche il proxy DNS con funzionalità anti-spyware. Insomma, ci sembra che le possibilità di controllo siano pressoché complete, e il tutto si gestisce in modo abbastanza semplice dall'interfaccia Web, anche se attivando più controlli la complessità aumenta. Gli ultimi tre menu a disposizione sono VPN, Hotspot e Logs. Il primo consente di attivare una o più VPN (fino a un centinaio secondo Endian, ovviamente in base alla banda disponibile) usando OpenVPN, IPSEC e diversi tipi di cifratura e autenticazione; esistono client nativi per tutti i maggiori sistemi operativi scaricabili dalla Endian Network. Le funzionalità Hotspot attivano in pratica un captive portal con supporto wired/wireless e include un gran numero di funzioni, integrando un server RADIUS, il log delle connessioni e la gestione di ticket gratuiti o a pagamento. Anche in questo caso è necessaria un po' di esperienza per la configurazione, ma l'interfaccia appare comunque chiara. Infine il menu dei log consente di visualizzare

e impostare i vari livelli di log per tutti i servizi del dispositivo. Qualche difetto dell'UTM? Nulla di grave, a nostro parere: mancanza del Wi-Fi; a volte l'interfaccia passa dall'italiano all'inglese quando si va da un menu a un sottomenu; alcune funzionalità, come l'antivirus, si appoggiano solo sui servizi d'origine e non sulla rete Endian, anche se sono previsti miglioramenti da questo punto di vista in futuro; l'interfaccia, a volte, è piuttosto complessa (ma non potrebbe essere altrimenti per uno strumento simile) e alcuni strumenti mantengono la propria GUI invece di integrarsi in quella principale. I pregi invece sono numerosissimi e quanto detto in questa recensione dovrebbe farvi capire le potenzialità e la versatilità del dispositivo. Il costo, a dir la verità, appare abbastanza alto: 2.125 €, più il canone annuale di maintenance e supporto, il cui prezzo base è di 470 €, ma è comunque giustificato dal livello qualitativo dei tanti software Open presenti. **LXP**



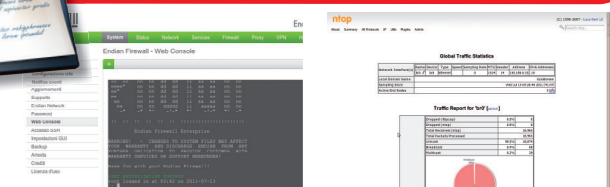
In evidenza

Web console

Gli amministratori che preferiscono gestire le configurazioni dalla shell trovano una console integrata nell'interfaccia Web.

Ntop

L'UTM di Endian integra i migliori software Open Source per svolgere i suoi compiti, come Ntop, Squid e ClamAV.



Giudizio

Endian UTM Mercury

Produttore: Endian
Web: www.endian.com/it/
Prezzo: 2.125 € + canone assistenza base di 470 €/anno

Caratteristiche	8
Prestazioni	9
Facilità d'uso	7.5
Qualità/prezzo	6.5

» Un UTM dalle ottime prestazioni e ricco di funzionalità; i contro sono il prezzo e la mancanza del Wi-Fi.

Il voto di Linux Pro

8