Publication: PC Professionale
Date: March 11

PC PROFESSIONALE

FIRST LOOKS
HARDWARE
NETWORKING

Anteprima di Simone Zanardi

Cyberoam CR25wi

Tutta la sicurezza *di cui avete bisogno*

L'azienda indiana propone un sistema di protezione Utm in grado di salvaguardare la rete Soho da tutte le minacce provenienti dal Web.

Approcciare il mercato dello *Small Office Home Office* con un'appliance Utm (*Unified Threat Management*) è impresa non semplice: la percezione dei rischi reali che si affrontano navigando in Internet non è così definita in ambienti consumer quanto lo è a livello aziendale. Per questo molti utenti non comprendono il valore aggiunto di un sistema che ha un costo di ingresso certamente superiore a quello dei classici router domestici. L'indiana Cyberoam (divisione di Elitecore Technologies) tenta di far breccia in questo complicato settore con il nuovo sistema CR25wi, l'ultimo arrivato della famiglia di appliance dedicate alla sicurezza a tutto tondo per piccoli e medi ambienti.

Dal punto di vista hardware, il CR25wi non si discosta da dispositivi di categoria analoga: il telaio in metallo presenta tutte le connessioni sul lato posteriore; sono implementate quattro porte di rete con standard Gigabit Ethernet, ciascuna delle quali può essere configurata separatamente per creare sottoreti, zone demilitarizzate, reti locali virtuali o accessi multipli verso l'esterno. Le impostazioni di default prevedono una porta per la rete locale, una per la Wan, una Dmz e una interfaccia di uso opzionale. È prevista una quinta Rj-45 utile ai collegamenti seriali per l'amministrazione da console, mentre la singola porta Usb può essere utilizzata per collegare dei modem 3G e realizzare così una connessione a Internet tramite rete cellulare. Per massimizzare l'affidabilità del sistema, il CR25wi è inoltre dotato di una doppia flash per il caricamento di due firmware; questa architettura consente di gestire i guasti a uno dei due moduli garantendo continuità di servizio, oltre all'eventuale downgrade di versione in caso di necessità. Per massimizzare le prestazione dell'appliance, il firmware è sempre ottimizzato sull'hardware in uso. L'access point integrato nell'appliance è conforme alle specifiche IEEE 802.11n e può quindi fornire connessioni senza fili a velocità massime teoriche di 300 Mbps; le tre antenne esterne fornite con il CR25wi sono sostituibili grazie agli agganci standard. Il sistema è in grado di gestire sino a otto access point virtuali, ciascuno dotato di proprio identificativo di rete, protocollo di protezione e policy di accesso.

Il CR25wi può essere installato in una rete preesistente in modalità gateway o bridge: nel primo caso opera come vero e proprio router e firewall ai bordi del sistema, nel secondo si integra a una struttura preesistente riducendo al minimo l'impatto sul parco macchine installato. Il sistema proxy integrato (basato tra l'altro sulla piattaforma *Squid*) permette poi di filtrare il traffico a livello Sock e può essere configurato in modalità esplicita o trasparente. A bordo dell'appliance Cyberoam la sicurezza è gestita a tutti i livelli disponibili della pila Iso/Osi, sino al cosiddetto layer 8. Questo significa che le politiche di protezione possono essere applicate non solo a livello di rete e di trasporto (Tcp/IP), ma anche in base alle applicazioni e agli utenti coinvolti. L'autenticazione

Colpo d'occhio L'interfaccia di amministrazione è vasta, ma ben organizzata per mettere a suo agio sin dai primi clic l'amministratore di sistema.

Iso/Osi

Open System Interconnection. Modello teorico per la descrizione dell'architettura di una rete informatica. Si basa su più livelli protocollari distribuiti a *strati*, dove lo strato più basso è quello fisico e quello più elevato è il livello applicativo, passando per la gestione dei collegamenti, della rete, del trasporto dati e delle sessioni di comunicazione.

Porte aperte
Le quattro interfacce di rete a bordo del CR25wi possono essere liberamente configurate per creare reti separate, Dmz o accessi Wan multipli.

degli utenti può essere effettuata sfruttando il client Cyberoam, disponibile per sistemi Windows e Linux, e appoggiandosi quindi a un database interno all'appliance, o demandata a piattaforme di gestione utenti preesistenti. Cyberoam supporta tra l'altro i domini Active Directory, i server Ldap/Radius e la piattaforma Windows Single Sign On. L'interfaccia di amministrazione è ben organizzata e abbastanza intuitiva, chiaramente in relazione alla complessità del sistema. La piattaforma di configurazione si basa su un sistema a oggetti, che consente di creare policy complesse a partire da indirizzi IP e Mac, porte, calendari, utenti, applicazioni e tipi di file. In questo modo è garantita la massima versatilità senza appesantire eccessivamente le procedure. Le policy sono utilizzate non solo per la gestione della sicurezza, ma anche per impostare meccanismi di *Quality Of Service* che distribuiscono le risorse di banda tra le varie componenti del network.

I moduli di sicurezza configurabili sull'appliance includono innanzitutto un sistema di filtro delle applicazioni e dell'accesso Web. Questa opzione permette in primo luogo di inibire l'utilizzo di particolari servizi basati sulla connessione online e che possono minare la produttività aziendale o comunque non rispettano le policy imposte dall'amministratore; un esempio in questo senso sono le applicazioni per il download e la condivisione di file su reti peer-to-peer, o i software di instant messaging. Il sistema supporta nativamente Msn Live e Yahoo! Messenger, sui quali si possono definire filtri specifici sui contatti o sulla modalità di comunicazione (solo chat o invio file).

Il motore di Web Filtering è invece mirato a bloccare l'accesso a determinati siti, elencati in un database dinamico e suddivisi in categorie costantemente aggiornate dalla stessa Cyberoam. In questo modo si possono impostare policy che impediscono di navigare su siti pornografici, o su portali dedicati alle news sportive. L'apparato prevede anche un meccanismo di *safe search* che gestisce i filtri a livello di risultati sui principali motori di ricerca (Google, Bing). Il sistema di filtraggio dinamico è affiancato da un modulo che consente di inserire manualmente una lista di indirizzi Url precisi. L'accesso al Web è inoltre regolato sulla base del tempo di connessione, della mole di dati trasferiti su Internet o di un pratico sistema di quote utente.

Oltre al modulo di filtraggio delle applicazioni e delle connessioni Web, il CR25wi integra poi una serie di servizi che Cyberoam fornisce in partnership con alcuni tra i più noti attori del settore. L'*Intrusion Prevention e Detection System* è così basato sul motore *Snort*, mentre il gateway antivirus sfrutta *Kaspersky*. Allo stesso modo, *Commtouch* è uno dei filtri impostati per il controllo antispam della posta elettronica in ingresso e in uscita. Un modulo speciale è poi dedicato all'assistenza post-vendita: sono disponibili il pacchetto base che garantisce supporto 8 ore al giorno nei 5 giorni lavorativi della settimana o l'opzione evoluta per un servizio 24x7. L'assistenza è assicurata tramite ticket elettronici gestiti via e-mail, telefono o chat (in lingua inglese), oltre che dal distributore italiano Horus Informatica. Per quanto concerne la manutenzione del sistema, il CR25wi offre un dettagliato set di log per la collezione e l'analisi statistica dei dati di traffico; i log sono esportabili in formato syslog e visualizzabili attraverso una serie di software appositi, tra cui *iView* della stessa Cyberoam, mentre il sistema di notifica Smtp permette di inviare e-mail di allerta o report all'amministratore. In conclusione, il CR25wi è un ottimo esempio di come anche le piccole realtà produttive e gli uffici possano dotarsi di un sistema di protezione della rete completo a cifre ragionevoli; certo, si tratta di un appliance complessa da gestire, ma il sistema a oggetti e l'interfaccia di management riescono in parte a semplificare la configurazione di regole anche complesse sulla rete. •

Cyberoam CR25wi

a partire da **768,00** Iva incl.

VOTO **8,0**

Pro

- Protezione a tutto tondo
- Interfaccia di amministrazione ben strutturata

Contro

- (Naturale) complessità nella gestione di alcune funzioni avanzate.

Produttore: Cyberoam, www.cyberoam.com.

Caratteristiche tecniche

Utenti gestiti: illimitati
Throughput Firewall: 450 Mbps (Udp), 225 Mbps (Tcp)
Throughput Utm: 50 Mbps
Throughput Antivirus: 65 Mbps
Throughput Ips: 70 Mbps
Connessioni gestite: 130.000
Interfacce Ethernet: 4
Interfacce Usb: 1
Terminazione Vpn: IPsec/Ssl
Throughput Vpn: 30Mbps (3Des), 75 Mbps (Aes)
Wireless: 802.11n
Sicurezza wireless: Wep, Wpa, Wpa2, 802.1x