White Paper

Il mondo del networking è profondamente cambiato. Deve sempre di più rispondere ad esigenze che nascono dalla delocalizzazione del business, con conseguente aumento del numero delle sedi che compongono l'organizzazione aziendale e dalla sempre maggior richiesta di lavoro da svolgere in modalità remota. Per questi motivi il settore del mobile, che consente di dare una risposta puntuale alle necessità sopra descritte, ha subito una vera e propria esplosione. Queste nuove modalità operative necessitano, come qualunque altro endpoint, di una connessione ai sistemi informatici aziendali esponendoli nel contempo ad un maggior rischio in termini di sicurezza. Le strutture che prima erano in grado, perché progettate per garantire la sicurezza in un area/campus ben delimitata, di rispondere ai canoni tradizionali della sicurezza, si trovano ora a fare i conti con un' area informatica potenzialmente illimitata (internet) per cui i potenziali attaccanti possono essere dovunque, **ma sono soprattutto gli utenti e i sistemi da proteggere che possono essere ovunque!** Di conseguenza, anche la sicurezza deve essere riposizionata ovunque e in grado di coprire oltre ai CED e ai data center anche gli uffici remoti, i dispositivi mobili, le infrastrutture virtuali e ogni nuovo punto d'accesso che potrebbe essere richiesto alla propria rete. Questa situazione non va affrontata nei termini di un aumento del livello di complessità e di richiesta delle risorse dedicate alla gestione delle problematiche di sicurezza, ma piuttosto ad un ripensamento complessivo dell'intera problematica che va affrontata da un altro punto di vista.

Tutte le aziende, grandi e piccole, devono garantire la costante disponibilità della rete e dei dati sottraendoli nel contempo ad un'ampia gamma di minacce come il fuoco, internet, guasti hardware, furti di identità, tentativi di accesso, ecc. La soluzione **Cyberoam High Availability** fornisce una serie di soluzioni ideali che sono in grado di garantire la continuità del business anche in presenza di anomalie gravi perché riescono a sostituire in tempo reale

Vitalize your IT

quella parte della struttura informatica danneggiata o malfunzionante, consentendo così la disponibilità delle applicazioni e la coerenza dei dati agli utenti connessi.

Per ottenere un risultato del genere è innanzitutto necessario parlare in termini di alta affidabilità. Vediamo in quali campi, della struttura informatica aziendale, possiamo andare a collocare questo concetto partendo ovviamente da quella che è la richiesta fondamentale:

High Availability (alta affidabilità HA) e il suo raggiungimento secondo **Cyberoam.**

- HA a livello hardware.
- HA a livello di applicazione.
- HA a livello di rete.

La necessità di High Availability.

Una delle maggiori sfide affrontate dai manager di rete di oggi è quello di garantire la costante disponibilità della rete e dei dati della propria azienda. I danni a cui si deve far fronte possono essere semplici, come ad esempio quelli provocati da una connessione internet ISP precaria, a quelli dovuti ad un problema del firewall che sottintende alla struttura perimetrale aziendale o peggio ancora alla totale perdita di dati. Diventa perciò un "**must**" proteggere l'infrastruttura IT attraverso un piano di sicurezza che garantisca un' elevata disponibilità della struttura. Tutto ciò si riflette in maniera diretta sulla reputazione dell'azienda ed una garanzia di continuità del proprio business. Ciò detto pare non sia sufficiente per tutte le aziende predisporre di un piano che garantisca l'**HA** perché una grossa parte di loro preferisce nascondersi dietro ad un mare di scuse quali:

"A noi non può succedere!"

Tutte le aziende, grandi e piccole, devono prepararsi ad affrontare ogni sorta di evento in difesa dei dati e dei sistemi che sono alla base dei servizi necessari alla continuità del business.

Bhè, qualcosa può andare storto, ma non è detto che succeda! E' noto che i componenti hardware si possono guastare, ma sono coperti da garanzia. Il software invece non ha parti elettroniche per cui, una volta installato, non dovrebbe mandare in crash i sistemi. Poi abbiamo pianificato periodi di manutenzione specifici nei quali facciamo un controllo dello stato dell'intera struttura. L'esperienza insegna invece che un buon IT Manager non dovrebbe mai essere sicuro che quanto sperato non possa accadere alla sua struttura. E soprattutto, dovrebbe considerare che la rete non è più un' entità statica fine a se stessa, ma che le connessioni ad internet e gli accessi in mobilità cambiano in ogni istante la sua struttura mandando di fatto "**a farsi friggere**" i piani di manutenzione predisposti.

"Siamo troppo piccoli per costituire un interesse per un attacco"

Se la continuità del business dipende dalla disponibilità dei dati, nessuna azienda è troppo piccola per avere un piano di **HA**. L'eventualità che la rete si fermi rappresenta un disastro in quanto viene a mancare il mezzo fisico che rende possibile il

vostro business.
Affidare alle procedure di "**Backup and Recovery**" la sicurezza della rete, è come chiamare i pompieri dopo che è scoppiato l'incendio sperando che arrivino in tempo per salvare quanto è possibile. Ricordatevi che anche l'acqua gettata sul fuoco procura danni. **E se ritardassero?**

Il **Down-time** è il termine che si usa per definire il periodo di inattività di una rete informatica. Identifica il periodo di indisponibilità dell'intero sistema quasi sempre dovuto ad un fail.

Esistono anche down-time pianificati e solitamente sono il risultato dell'esperienza dell'IT Manager, il quale, in base alla conoscenza della sua architettura, decide quei fermi di rete per permettere gli interventi di manutenzione H/W necessari, l'applicazione di patch S/W, riconfigurazioni o modifiche che hanno comunque l'effetto di consentire l'accesso ai dati solo dopo un "**system reboot**".

Secondo Gartner, il costo medio orario dovuto all'inattività di una rete di computer è di 42.000$ per ora. Se poi l'attività dell'azienda è a carattere negoziale via internet, e-commerce, transazioni finanziarie, etc. i rischi di un down-time possono costare milioni di dollari all'ora. Anche un down-time medio di 87 ore all'anno, che rappresenta il 99% di tempo di disponibilità annua di una rete di una media azienda ammonta a 3,6 milioni di dollari.

Availability %	Downtime per year
55.5555555% ("nine fives")	162.22 days
90% ("one nine")	36.5 days
95%	18.25 days
97%	10.96 days
98%	7.30 days
99% ("two nines")	3.65 days
99.5%	1.83 days
99.8%	17.52 hours
99.9% ("three nines")	8.76 hours
99.95%	4.38 hours
99.99% ("four nines")	52.56 minutes
99.999% ("five nines")	5.26 minutes
99.9999% ("six nines")	31.5 seconds

Le reti progettate in "**High Availability**" hanno molte meno probabilità di soccombere ad un qualsiasi degli eventi sopra descritti. I sistemi ad alta disponibilità devono essere progettati

dedicando le risorse necessarie suggerite dall'analisi degli scenari di inattività provocati dagli eventi scatenanti l'inattività stessa, in modo che in presenza dell'evento la struttura reagisca evitando il fermo rete e la perdita dei dati. Meglio ancora se si riesce a mettere la struttura nelle condizioni di prevenire l'effetto scatenante. **Non è più necessario chiamare i pompieri semplicemente perché si previene l'incendio.** Il costo della progettazione e della pianificazione di una tale struttura è infinitamente inferiore ai costi dovuti al down-time.
La procedura di analisi "**Risk analisys**" calcola il maggior rischio sopportabile da parte dell'azienda in caso di fermo dell'attività. Più questo rischio è basso più i costi di progettazione e realizzazione sono alti. Il giusto equilibrio è funzione di decisioni aziendali che debbono essere prese ai più alti livelli e che coinvolgono non solo la natura del business ma anche la reputazione dell'azienda nei confronti del mercato e della clientela.

H.A. secondo Cyberoam

High Availability (**HA**) è definita come l'attuazione di un sistema posto a garanzia della continuità di servizio di una rete. La progettazione deve garantire il livello prestabilito di prestazioni operative su un determinato periodo di tempo. Le prestazioni operative richieste dipendono dall' hardware e dal software impiegato, dalle configurazioni adottate, dalle applicazioni, dalla connettività impiegata e da tutti gli altri elementi che debbono fornire i servizi al business, ai dipendenti e ai clienti. Anche la capacità del sistema di minimizzare il down-time al minor numero possibile di servizi erogati o al minor numero possibile di dipendenti o clienti distingue un buon progetto da uno meno buono. Molto spesso la qualità del progetto, a parità di H/W e S/W impiegato, determina automaticamente un bassissimo livello di rischio rispetto ad uno sostanzialmente più alto. Cyberoam affronta il problema partendo da tre differenti considerazioni:

Hardware Level	Application Level	Network Level
- Appliance Clustering - Redundant Power Supply - Hardware Bypass	- Load Balancing	- Multilink Management - 3G and Wimax WAN - VPN Failover

H.A. a livello Hardware

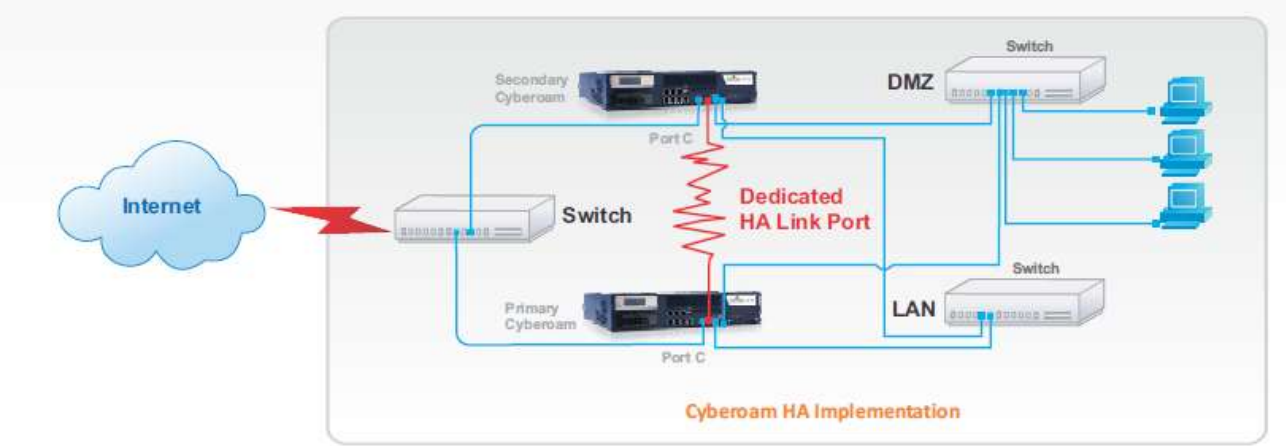
Clustering appliance: Cyberoam realizza questa configurazione utilizzando due apparati configurati per funzionare come se fossero uno solo. Gli apparati sono logicamente definiti primario e secondario, sono fisicamente connessi tramite una porta dedicata "**HA link**" e condividono un medesimo indirizzo IP "**Virtual MAC**".

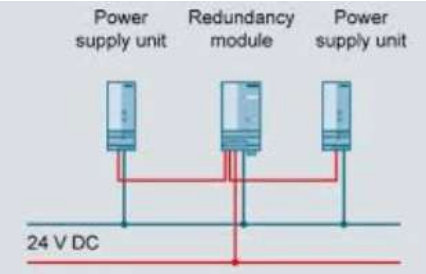
Cyberoam può realizzare la configurazione HA in due modalità definite:

- Modalità Attivo-Attivo
- Modalità Attivo-Passivo

Attivo-Attivo: in questo modo il traffico dei dati viene processato da entrambi gli apparati che compongono il cluster, primario e secondario. Quando il traffico entra nella rete viene inoltrato all'apparato primario, che ha il controllo dell'indirizzo MAC virtuale. Da qui il traffico viene automaticamente bilanciato e diviso con l'apparecchio secondario. In caso di fault del primario, l'apparato secondario processa l'intero carico e prende le funzionalità di primario arrogando a sè il MAC virtuale. Qualora il fault interessi l'unità secondaria sarà il primario a prendersi carico dell'intero traffico della rete. Ovviamente, in presenza di fault di uno qualsiasi dei componenti del cluster verranno inviati all'amministratore di rete gli alert necessari. In questa modalità è possibile scegliere apparati in grado di supportare il 50% dell'intero traffico di rete in quanto eseguono il bilanciamento del traffico. In caso di fault di uno dei due apparati ci si accolla il rischio di un potenziale dimezzamento del traffico di rete.

Attivo-Passivo: se configurato in questo modo, il cluster affida l'intero controllo del traffico all'unità primaria. L'apparato secondario rimane in ascolto tramite l'HA Link, che connette i due apparati e che di fatto realizza il cluster, in attesa di tutte le comunicazioni che l'apparato primario deve inviargli entro le tempistiche predefinite. In mancanza di comunicazioni l'apparato secondario considererà guasto il primario e lo sostituirà automaticamente in tutte le sue funzioni divenendo lui stesso primario. Qualora la situazione si ristabilisse, sempre attraverso una comunicazione del link HA, il dispositivo primario si riavvierà riportando la configurazione del cluster allo stato iniziale. Durante questa modalità di funzionamento non viene attivata la funzionalità di bilanciamento del traffico, ed entrambe le macchine devono essere dimensionate per supportare entrambe l'intero traffico della rete.





Alimentatore di rete ridondato: per gli apparati di fascia alta **Cyberoam** rende disponibile l'alimentazione ridondata. In questo caso gli apparati includono due alimentatori all'interno di ogni unità, ciascuno dei quali è in grado di alimentare l'intero sistema. Se per qualche motivo, uno degli alimentatori non fosse in grado di erogare l'energia necessaria, l'altro alimentatore prenderebbe immediatamente e senza causare interruzioni di sorta, l'intero carico. Normalmente i due alimentatori si distribuiscono il carico in modo da mantenere più basse le temperature interne insieme al livello di stress elettrico della componentistica elettronica.

Hardware Bypass: in questa modalità l'apparato **Cyberoam** risulta connesso in trasparente, "**transparent mode**" in modo da garantire la disponibilità dell'hardware che lo compone per tamponare l'hardware dell'altro apparato che si è guastato oppure in caso di un malfunzionamento del software. In modalità bypass hardware, le interfacce dell'apparato si connettono in bridge con le interfacce guaste e permettono il transito dei flussi dati dall'interfaccia guasta a quella replicata senza nessuna interruzione.

H.A. a livello applicativo

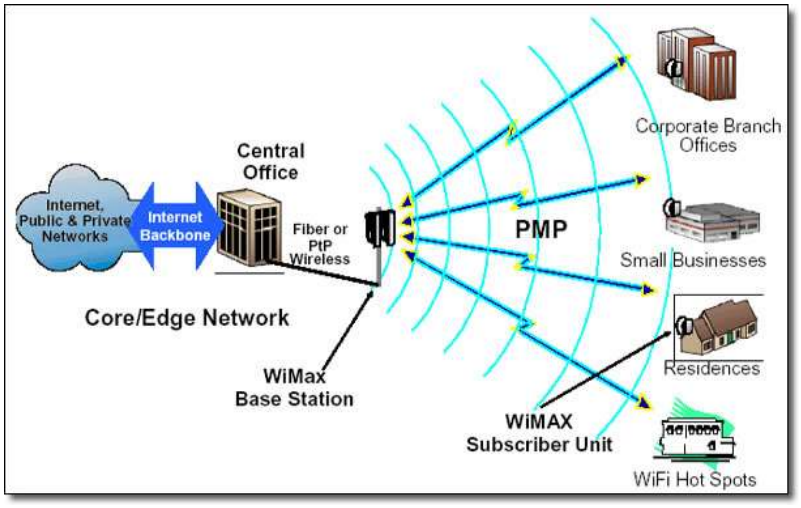
Load balancing: se configurato in un cluster "**attivo-attivo HA**", sia l'apparato primario che il secondario elaborano il traffico ed effettuano il delivery dei dati secondo le regole impostate. Il dispositivo primario si incarica anche di bilanciare il traffico della rete tra le due unità. Ciò consente prestazioni fortemente migliorate, una maggiore disponibilità delle risorse e una migliore scalabilità dell'intero sistema informatico. Inoltre, in cluster attivo-attivo, **Cyberoam** permette il "**failover**" del dispositivo e il "**failover**" della singola sessione.

H.A. a livello di network

Multilink Management: con la crescente popolarità del cloud computing e l'aumento della sua disponibilità unita ad una riduzione sostanziale dei costi, un sempre maggior numero di aziende canalizzano il proprio business attraverso internet. Per questo aumenta l'importanza di disporre di collegamenti veloci, stabili e ridondanti. Un solo collegamento a internet, espone l'azienda ad un livello di vulnerabilità francamente insopportabile in quanto in caso di fault della linea i tempi di inattività farebbero lievitare in modo abnorme le perdite dovute all'improduttività.
"**Cyberoam Multilink Management**" fornisce il bilanciamento automatico dell'intero traffico di rete e il failover automatico quando uno o più collegamenti Internet risultano guasti o scarsamente performanti. **Cyberoam** rileva automaticamente il carico su ogni link e dinamicamente lo bilancia utilizzando il metodo "**round robin ponderato**". La **politica di scheduling Round Robin** (RR) è quella in cui tutti i processi attivi in un sistema ricevono il controllo della CPU secondo un turno, assegnato in maniera circolare. Questo è quello che accade alle CPU delle macchine poste in HA che provvedono insieme al delivery del traffico secondo delle regole aziendali (policy) precedentemente ponderate.
Insieme al bilanciamento del carico tra due o più link ISP, che è utile avere per un aumento delle prestazioni e della sicurezza, il "**failover**" automatico di **Cyberoam** rileva automaticamente i fault dei gateway di destinazione e reindirizza il traffico verso un altro gateway in modo da impedire il down-time della rete. **Cyberoam** controlla continuamente lo

stato di ciascun gateway e rileva i guasti o le situazione potenzialmente pericolose in tempo reale. L'allocazione dinamica del traffico rende sicura, se dovesse verificarsi una situazione di "**failover**", la disponibilità della rete e della connettività in particolare deviando o bilanciando il traffico attraverso percorsi e Gateway diversificati.

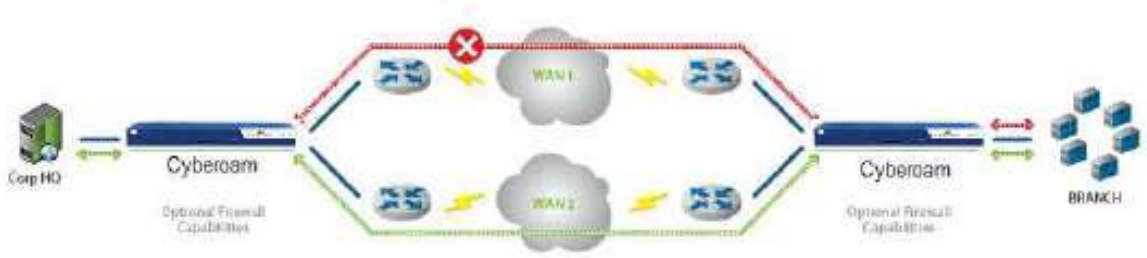
3G e WiMAX WAN: Cyberoam supporta le connessioni wireless WAN "**3G e WiMAX**", per garantire la connettività anche in quelle località che non sono raggiunte dalla connettività cablata. Le connessioni wireless WAN vengono gestiti dal modulo "**Multilink**" esattamente come se fossero link cablati con tutte le stesse funzionalità. Ciò permette alle aziende di usare ad esempio il **3G** solo in caso di fault del link principale (Active-Passive) oppure come canale di trabocco qualora il traffico richiesto superasse il limite stabilito per il link principale.



VPN Failover: Cyberoam è di fatto un'unità server VPN certificato "**VPNC**" e quindi compatibile con la maggior parte dei server/apparati VPN di terze parti. Offre un elevato numero di VPN all'interno dello steso apparato. Supporta la modalità "**VPN failover**" il che consente in caso di down la possibilità dell'instaurazione immediata di rotte sostitutive sempre in modalità protetta VPN.
Quando esistono uno o più link configurati in WAN un tunnel VPN può essere configurato, come link di back-up oppure reso disponibile in modalità failover, ad una connessione WAN che fornisce la connessione principale a internet. In questo modo il link VPN realizzerà la doppia funzione di Backup e di failover in caso di down del link principale.

Una soluzione di sicurezza con **Cyberoam**, configurato in VPN failover, può far fronte a due condizioni di fail completamente diverse:

1. Il collegamento internet è down. **Cyberoam** rileva automaticamente attraverso il suo Multilink Manager che il link della connessione WAN è down per cui ristabilisce la connessione tramite un altro link WAN disponibile.
2. Quando l'endpoint VPN non è disponibile. Per cui CYberoam segnala la situazione di indisponibilità.



VPN Failover

E' possibile però chiedere a **Cyberoam** di configurarsi in modo tale per cui se il collegamento principale fallisse la connessione VPN provvederà a prendere il suo posto, almeno per quella tipologia di traffico considerato critico per l'azienda.

In altre parole: la disponibilità della rete informatica e delle sue risorse è fondamentale per il business. Il down della rete o la discontinuità dei servizi provoca all'azienda un aumento dei costi dovuti all'improduttività forzata, un calo di credibilità e la perdita di opportunità. Le soluzioni di **Cyberoam** "**High Availability**" mitigano gli effetti dei fault dovuti ad un hardware difettoso o ad un software non proprio performante, riducendo drasticamente il tempo di inattività percepito dagli utenti e dal mercato.

UTM "Unified Threat Management" di Cyberoam

Le soluzioni di gestione unificata degli attacchi UTM, ovvero "**Unified Threat Management**" sono pensate per rispondere alle necessità delle aziende di dotarsi di piattaforme unificate, facili da gestire e in grado di assicurare prestazioni ottimali a fronte degli investimenti in sicurezza. La flessibilità e la vasta gamma delle appliance **Cyberoam** le rende inoltre adatte sia alle strategie delle piccole e medie aziende sia a quelle delle organizzazioni di maggiori dimensioni. Grazie all'approccio UTM alla gestione unificata degli attacchi, le appliance **Cyberoam** riuniscono in una sola piattaforma numerose funzionalità di protezione come Firewall, VPN, gateway antivirus, anti-malware, anti-spam, intrusion prevention system, filtraggio dei contenuti e gestione della disponibilità della banda e dei multiple link.
Ovviamente non è sufficiente proteggere, ma è di fondamentale importanza poter verificare in real time cosa succede all'interno della propria rete attraverso un sistema di reportistica centralizzata che informi costantemente gli IT manager sullo stato di salute della struttura informatica e sull'identità degli utenti e i loro accessi ai servizi che debbono essere in linea con quanto pianificato. La frequenza dei reports evita agli IT manager fermi rete dovute ad operazioni di manutenzione H/W e S/W e la sicurezza della rispondenza ai dettami legislativi.

iView
Monitoraggio della propria architettura informatica

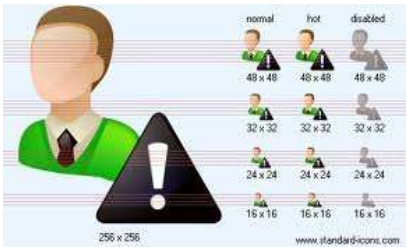
Cyberoam iView è una soluzione che consente il monitoraggio delle reti aziendali e dei dispositivi ad esse collegati garantendo elevati livelli di sicurezza e riservatezza dei dati nella totale conformità alle normative vigenti. Una singola interfaccia centrale restituisce il quadro globale della sicurezza aziendale su tutti i dispositivi geograficamente

dislocati. In questo modo le aziende sono in grado di applicare security policy o modificarle da una sola postazione centrale. L'interfaccia grafica di **iView** è molto semplice e fornisce diversi tipi di report in una singola pagina così da offrire costantemente una visuale completa di tutti i parametri della rete.

Cyberoam iView permette alle aziende di individuare **l'anello debole del sistema** grazie a report identity-based sui vari tipi di anomalie. Offre ad esempio la visuale degli attacchi principali, delle applicazioni maggiormente usate per gli attacchi, dei principali destinatari di mail spam, dei virus più diffusi ed altro. In questo modo è possibile individuare velocemente i problemi e risolverli in conformità alle normative vigenti. Informazioni legate all'identità come quelle sugli utenti che occupano maggiormente la banda per upload e download o sulle principali applicazioni usate aiutano le aziende a gestire le loro risorse ed a pianificare le necessità future oltre a migliorare i livelli di sicurezza.

Caratteristiche principali

Il pacchetto di **Cyberoam** garantisce la personalizzazione delle **white e blacklist** e un controllo granulare sul trasferimento dei dati, fondato sul profilo degli utenti, dei gruppi e degli orari di accesso; sulla tipologia e la dimensione dei documenti trattati; sulla creazione di copie fantasma. Le operazioni di cifratura e de-cifratura su file e dispositivi Usb permettono di evitare la perdita delle informazioni critiche sia in caso di smarrimento dei device sia in caso di azioni dannose.



Log Management: Cyberoam iView raccoglie, filtra, normalizza, archivia e centralizza i log provenienti dall'infrastruttura in tutte le sue componenti su standard syslog rendendo disponibili funzionalità di ricerca e reporting evoluto riducendo in modo significativo il costo e la complessità delle attività di analisi.

Security Management: Cyberoam iView offre una visuale completa dello stato di sicurezza dell'azienda attraverso una singola interfaccia. Le aziende possono individuare immediatamente attacchi di rete, la loro origine e la destinazione attraverso un rapido sguardo al pannello principale e possono subito intraprendere azioni sulla rete in qualsiasi luogo del mondo.

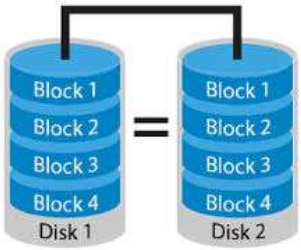
Compliance reporting: Cyberoam iView fornisce report che rispondono alle normative vigenti. Grazie al facile accesso ai report ed alla verifica dei log si riducono notevolmente i costi

per mantenere il sistema conforme alle normative. Gli amministratori sono subito informati di comportamenti che si scostano dalle pratiche di sicurezza con una conseguente riduzione dei tempi di risposta agli incidenti.

Analisi legali: Cyberoam iView, attraverso i suoi log e i suoi report, aiuta le aziende a ricostruire la sequenza degli eventi che si sono verificati nel momento di una determinata violazione della sicurezza. Consente alle aziende di estrarre lo storico degli eventi relativi alla rete, riducendo i costi necessari a indagare sull'accaduto e ridurre il down time della rete.

Multiple Devices Support: le appliance **Cyberoam iView** garantiscono logging e reporting intelligente su diversi dispositivi di rete compresi firewall UTM, Linux IP Tables/Net Filter firewall, Squid ed altri. Le aziende sono così dotate di report sui log attraverso una singola GUI molto semplice da utilizzare.

Spazio Terabyte per lo Storage: Cyberoam iView offre TB di spazio disponibile per le esigenze di archiviazione di tutta la reportistica.



Ridondanza dei dati. le appliance **Cyberoam iView** utilizzano tecnologia RAID per garantire ridondanza ed elevati livelli di affidabilità di storage in modo da salvaguardare i dati anche in caso di guasto dell'hard disk.

La **Central Console** di **Cyberoam** (**CCC**), disponibile sia in versione hardware che come appliance virtuale, consente la gestione centralizzata degli aggiornamenti e delle security policies in real-time sia ad aziende con uffici remoti che agli MSSP che hanno l'esigenza di gestire migliaia di appliance, con una notevole riduzione dei tempi di risposta. Grazie alle policy **Layer 8 identity-based** della **CCC,** è possibile impostare per gli utenti accessi basati su ruoli offrendo controlli granulari, ma flessibili. La **CCC** consente il back-up sia automatico che manuale della configurazione **Cyberoam** UTM, incluse policy ed altre impostazioni.

Cyberoam Central Console

Clik per scaricare la presentazione della Central Console

Cyberoam GOLD PARTNER

Non si è mai abbastanza piccoli da poter pensare di non essere interessanti per nessuno e tralasciare la sicurezza!!

Il Tuo EterNet Team

EterNet Vitalize your IT