White Paper La sicurezza negli ambienti Thin Client **Citrix**

Come indicato nel titolo ci occuperemo in questa white paper della sicurezza negli ambienti informatici virtuali con particolare riferimento a quelli realizzati con tecnologia **Citrix**.

Per rispondere alle problematiche relative alla sicurezza informatica di un ambiente virtuale è indispensabile ricorrere a conoscenze specifiche e diverse da quelle necessarie a risolvere lo stesso problema in un ambiente tradizionale. Questo perché all'interno di un ambiente virtualizzato lo scambio dei dati non è eseguito con la stessa modalità di quello effettuato in un ambiente tradizionale.

Ad una primissima analisi risultano infatti immediatamente diversi sia il protocollo trasmissivo che la modalità gerarchica di scambio dati per cui è evidente che la risposta alla domanda di sicurezza dovrà essere profondamente differente.

Ma procediamo con ordine.

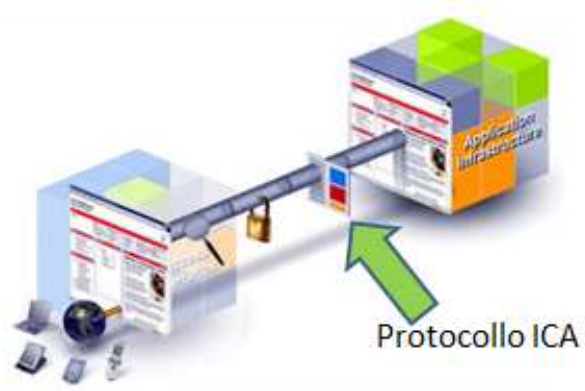
Intanto chi è Citrix

Citrix Systems Inc. è una società multinazionale fondata nel 1989, che fornisce tecnologie per la virtualizzazione desktop e server, networking, Software-as-a-Service (**SaaS**) e Cloud Computing, inclusi i prodotti Xen Open Source. Citrix fornisce le sue soluzioni a più di 230.000 aziende di tutto il mondo e ha sede a Fort Lauderdale, nell'area metropolitana della Florida meridionale, ha filiali in California e Massachusetts e possiede altri centri di sviluppo in Australia, India e Regno Unito. In seguito all'acquisizione di Xen Source, avvenuta nell'ottobre 2007, Citrix dirige il progetto inerente "all'hypervisor open source Xen".

Le soluzioni "**Presentation Server"** di Citrix Systems realizzano il concetto di "**On-Demand Enterprise**", consentendo a tutti gli utenti di accedere ad ogni tipo di applicazione, con qualsiasi device e attraverso qualsiasi connessione, dedicata, Wireless o Web. L'approccio di Citrix, è basato sulle più avanzate tecnologie disponibili sul mercato, come il protocollo di trasmissione **ICA** (Independent Computing Architecture) e la piattaforma operativa **MetaFrame** che consentono ai team IT di gestire le eterogeneità e le complessità tipiche di ogni realtà aziendale.

Lo scambio dei dati

Innanzi tutto bisogna chiarire che in un ambiente Citrix tutte le applicazioni sono poste sul server che comunica con i thin client trasferendo solo i dati (protocollo ICA) che sono il prodotto dell'intera elaborazione realizzata in modo centralizzato sul server. Il risultato di un'elaborazione così concepita è un traffico dati tra client e server ridottissimo.

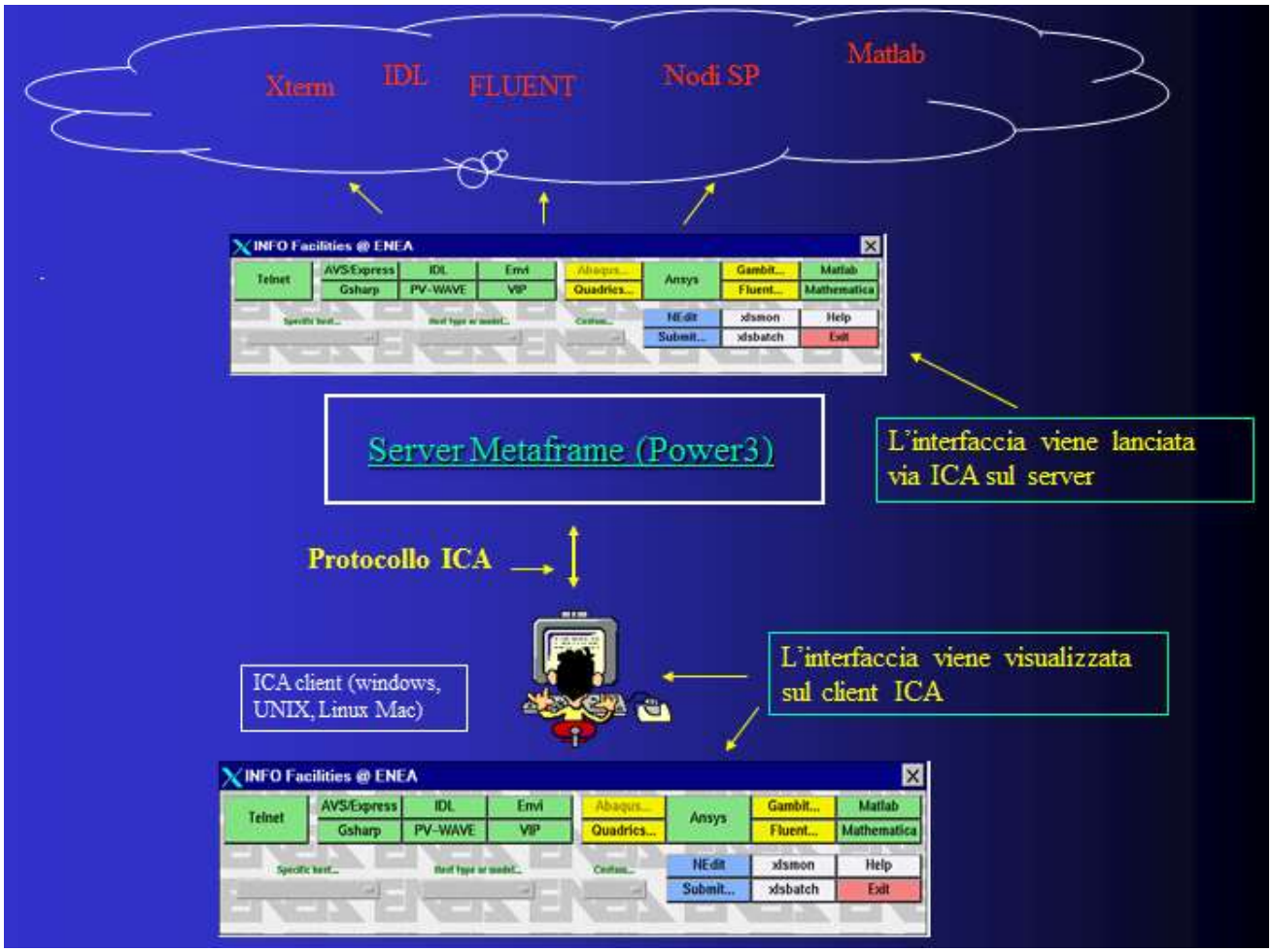


Il protocollo ICA

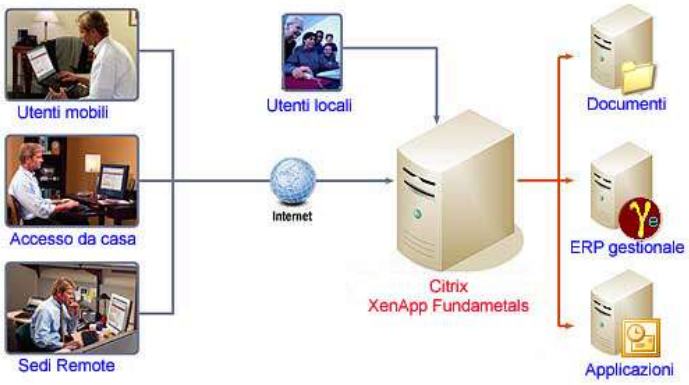
Qual è l'elemento centrale della tecnologia Citrix? **Il protocollo ICA.** Esso consente di eseguire le applicazioni sulla server farm, mentre i client visualizzano solo le schermate Windows

trasmettendo i soli comandi di mouse e tastiera. Questo modo di trasmettere dati necessita di poche risorse locali e di pochissima banda. In tal modo è possibile accedere alle applicazioni in tempo reale, anche da remoto utilizzando qualunque device, anche un thin client. Il fatto che le applicazioni vengano poi eseguite centralmente permette agli amministratori di sistema di poter installare e aggiornare centralmente i software, con notevoli risparmi sui costi di gestione e una maggior sicurezza dell'intero network.

- **L'ICA software** (Independent Computing Architecture) viene installato sulla macchina client, permettendo agli utenti di connettersi al server Metaframe .
- **L'ICA Client software** è distribuito in modalità free, ed è disponibile per diverse piattaforme (Windows, UNIX , LINUX , MAC).
- **Metaframe** utilizza il protocollo ICA per la connessione tra il client e il server.
- **Il protocollo ICA** invia solo keystrokes, mouse clicks e screen updates tra il client e il server.
- L'applicazione rimane "running" sul server con un carico minimo sul client pur simulando l'intero processo come se il software fosse installato localmente.



In pratica anche al di fuori di un'architettura tradizionale la virtualizzazione client server in ambiente Citrix consente ogni sorta di connessione.



La sicurezza in ambiente CITRIX

Per proteggere adeguatamente una rete Citrix è necessario innanzi tutto dare una risposta ai tre quesiti sotto riportati:

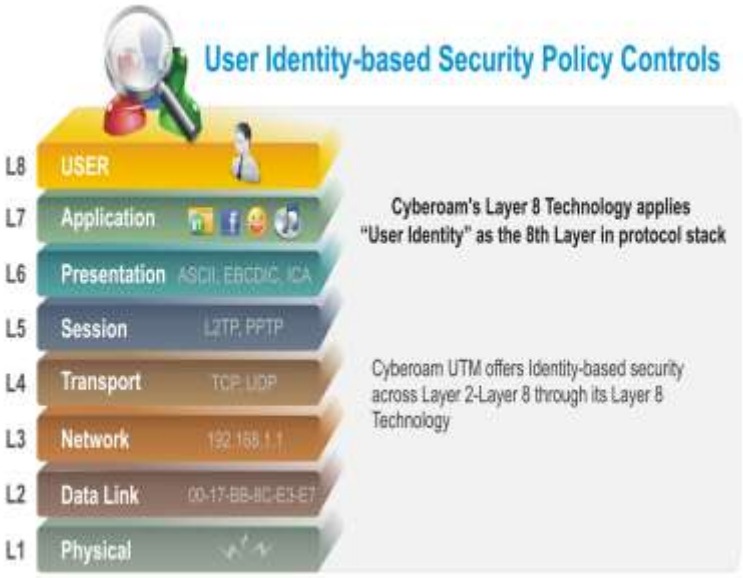
1. Come identificare gli utenti negli ambienti Citrix?
2. Come proteggere le reti dei clienti dalle minacce interne?
3. Come creare policy di accesso a internet per utenti specifici?

La risposta alle necessita di sicurezza espresse dalle domande sopra riportate passa quindi per soluzioni che inevitabilmente debbono entrare nel merito del protocollo ICA.

Le soluzioni di sicurezza di seguito descritte sono realizzate con l'apporto della tecnologia **Cyberoam** che risolve in maniera particolarmente brillante queste problematiche grazie anche all'introduzione di nuovi concetti trasformati dal costruttore in veri e propri brevetti.

Cyberoam UTM - Total Security

Per poter identificare e controllare le attività degli utenti in un ambiente thin client, **Cyberoam** ha aggiunto ai normali 7 livelli della pila ISO/OSI un **ottavo livello** per identificare in modo univoco l'utente (**livello utente**). Senza questo passaggio, per altro non contemplato da nessun altro, costruttore risulta impossibile identificare gli utenti in ambienti Citrix. L'aggiunta di questo livello consente invece, all'appliance dedicato alla sicurezza, tutti quei controlli comprensivi anche dell' "**identità umana**" (user IP) come parte integrante delle Policy di sicurezza aziendale.



Le appliance UTM Identity-based di **Cyberoam** offrono una protezione completa contro le esistenti ed emergenti minacce Internet, inclusi virus, worm, trojan, spyware, phishing, pharming e altro ancora.
Cyberoam UTM offre in una sola piattaforma la gamma completa di security functionality come:

- Stateful Inspection Firewall;
- VPN;
- gateway antivirus;
- gateway anti-malware;
- gateway anti-spam;
- intrusion prevention system;
- content filtering;
- bandwidth management;
- multiple link management.

Il portafoglio di soluzioni Cyberoam comprende:

- Cyberoam Central Console (**CCC**), una soluzione per la gestione e il controllo centralizzato della sicurezza all'interno di network distribuiti ed estesi;
- Cyberoam iView, soluzione per logging e reporting;
- **Cyberoam** ha la certificazione CheckMark UTM Level 5, ICSA Labs;
- **Cyberoam** è un membro del Virtual Private Network Consortium;
- **Cyberoam** è stata classificata come "Visionary" all'interno del Magic Quadrant per SMB Multi-function Firewalls di Gartner;
- **Cyberoam** è continuamente valutato con 5 stelle da SC Magazine;
- **Cyberoam** ha uffici a Woburn, MA e in India.

Per ulteriori informazioni visitare il sito www.cyberoam.com

Tante funzionalità ma una sola console di controllo

Disegnate per svolgere anche funzioni di gestione della banda (bandwidth management), di filtraggio dei contenuti (content filtering) oltre che di firewall, le appliance UTM della serie CR possono essere amministrate centralmente attraverso il cruscotto unificato Central Console di **Cyberoam**.
Le loro prerogative di difesa dei dati sensibili in transito sui network aziendali comprendono anche funzionalità VPN SSL e IPSec, gateway anti-virus, anti-spam e anti-spyware, Multiple link management e Web Application Firewall (WAF). Quest'ultimo in particolare è il modulo per la protezione delle Applicazioni Web aziendali che offre un livello aggiuntivo di sicurezza contro gli attacchi informatici prima che questi possano raggiungere le applicazioni web cruciali per il business (CRM, ERP, inventory management, online banking, e-commerce), intercettando il traffico in entrata ed in uscita dagli web server.

Grazie a questa ricca gamma di risorse **Cyberoam** è in grado di fronteggiare con successo la continua diffusione di virus, malware e intrusioni indesiderate in ambienti di rete sempre più complessi e si adatta senza problemi all'evoluzione di tecnologie e applicazioni caratterizzate da un ampio consumo di banda come SaaS e Web 2.0.

Appliance UTM virtuali

Con 58 milioni di macchine virtuali nel 2012 (un aumento di 47,2 milioni di macchine virtuali dal 2010) oggi la virtualizzazione è la scelta preferita dalle aziende per i vantaggi economici, la scalabilità e l'abbattimento delle barriere delle infrastrutture di rete fisiche che comporta l'adozione di questo tipo di soluzione. Tuttavia, spesso per queste aziende, la sicurezza delle reti virtuali si rivela un problema difficile da affrontare.

Le appliance UTM virtuali di **Cyberoam** offrono una soluzione di network security adatta ai principali scenari di virtualizzazione:

- proteggono i data center virtuali senza la necessità di implementare soluzioni di sicurezza hardware dedicate;
- offrono sicurezza **Layer-8** e controllo degli accessi basati sull'utente fondamentali in ambienti "Office-in-a-Box" e BYOD;
- supportano diverse piattaforme di virtualizzazione tra cui VMWare e Hyper-V con la possibilità di trasformarle facilmente in configurazioni sicure.

I moduli di licenza permettono di assegnare il numero di vCPU per l'appliance Cyberoam UTM virtuale in base all'esigenza dell'azienda. Tale flessibilità, unitamente alla compatibilità con diverse piattaforme virtuali e alla possibilità di facili aggiornamenti garantisce alle aziende pieno controllo delle infrastrutture di rete.
Grazie alla scansione del traffico e alle funzionalità di sicurezza, integrata su un'unica appliance, Cyberoam virtual UTM protegge le reti da attacchi su console di gestione quali hypervisor, hypervisor & Guest OS, applicazioni web virtualizzate e server, permettendo alle aziende di proteggere le reti Zero Trust Networks.
In pratica **Cyberoam** offre una soluzione di sicurezza completamente virtualizzata.

Le necessità del mercato

Le aziende moderne si trovano ad affrontare le problematiche legate alla sicurezza delle loro infrastrutture lottando su 2 fronti. Da una parte le minacce esterne sono in continua evoluzione, dall'altra, e quasi in egual misura, è necessario adottare strumenti di protezione dai pericoli provenienti dall'interno della propria rete. Inoltre, in un contesto in cui ogni azienda ha uffici dislocati in diverse sedi ed infrastrutture IT composte da dispositivi di vario tipo, sorge l'esigenza di una protezione globale che garantisca la visibilità completa di tutte le attività svolte sulla rete sia che queste avvengano nelle sedi centrali che in quelle remote.

Cyberoam iView. La soluzione per Logging & Reporting

Cyberoam iView è una soluzione per il logging e il reporting che aiuta le aziende a monitorare le loro reti attraverso dispositivi multipli in modo da poter garantire un elevato livello 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 o modificare le policy di sicurezza da una sola postazione centrale. L'interfaccia grafica di iView è molto semplice e fornisce diversi tipi di report tutti accorpati in una singola pagina così da offrire costantemente la visione integrata di tutti i parametri della rete. **Cyberoam iView** permette alle aziende di individuare l'anello debole del sistema grazie a report identity-based su vari tipi di anomalie. Offre ad esempio la visuale degli attacchi principali, delle applicazioni maggiormente usate per gli attacchi stessi, dei principali destinatari di mail spam, dei virus più diffusi ed altro ancora. In questo modo è possibile individuare velocemente i problemi e risolverli. Informazioni legate all'identità, come quelle relative agli utenti che occupano maggiormente la banda per upload e download o sulle principali applicazioni usate, aiutano le aziende a gestire le risorse ed a pianificare le necessità future.

Caratteristiche principali

Cyberoam garantisce la personalizzazione delle white e blacklist e un controllo granulare sul trasferimento dei dati, basato sul profilo degli utenti, dei gruppi, degli orari di accesso, sulla tipologia e la dimensione dei documenti trattati e sulla creazione di copie fantasma.

Le operazioni di criptazione e decriptazione su file e dispositivi USB sono in grado di evitare la perdita delle informazioni critiche sia in caso di smarrimento dei device sia in caso di azioni malevole.

Log Management

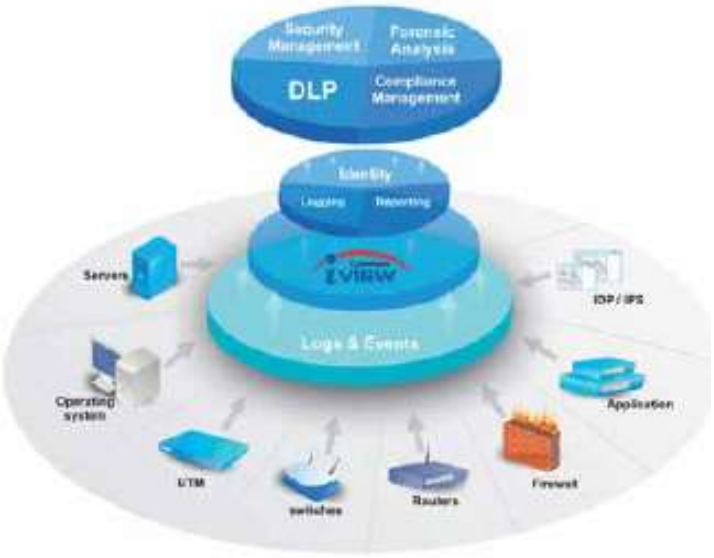
Cyberoam iView raccoglie, filtra, normalizza, archivia e centralizza i log provenienti dall'infrastruttura in tutte le sue componenti su standard "**Syslog**" rendendo disponibili funzionalità di ricerca e reporting evoluto riducendo in modo significativo il costo e la complessità delle attività di analisi.

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 le azioni correttive più opportune da qualsiasi luogo ci si trovi.

Compliance Reporting

Cyberoam iView fornisce una reportistica chiara ed esaustiva rispondente alle normative vigenti. Grazie al facile accesso ai report ed alla verifica dei log si riducono notevolmente i costi necessari a mantenere il sistema conforme. Gli amministratori vengono subito informati dei comportamenti anomali che si discostano dalle pratiche di sicurezza consentite con una conseguente riduzione dei tempi di risposta in caso di incidenti.



Complete UTM Security Coverage

Cyberoam utilizza la tecnologia di autenticazione utente (**CATC** in maniera trasparente). Nel caso di più appliance contemporanei non c'è la necessità di dispositivi aggiunti di gestione.

Consolidamento interfaccia di sicurezza

La tecnologia dell' **8° livello** permea ogni struttura degli appliance Cyberoam. Tutte le funzioni di sicurezza possono essere configurate e gestite da una singola pagina di istruzioni inserita nel Firewall. Il livello 8 lega tutte le policy di sicurezza creandone una sola monolitica in modo da consentire all'amministratore di seguire le attività dell'utente in ambiente thin client adattandole solo all'evenienza.

L'utente è protetto come in un guscio di noce.

Aumento della produttività

Attraverso l'applicazione di un filtro appositamente creato è possibile limitare la navigazione internet sulla base della durata dei siti visitati correlandola all'utente o ad un gruppo di utenti. **Cyberoam** permette di creare filtri si fatti scegliendo tra 82 categorie pre impostate. L'UTM Cyberoam consente di settare ogni singolo utente in modo che non possa rimanere connesso oltre un tempo definito oppure non possa avere un consumo di banda superiore a quanto fissato. Ciò consente di limitare la navigazione Internet ed i Download improduttivi.
Il Controllo degli Instant Messaging permette agli amministratori di abilitare le chat da chi e verso chi tramite un controllo diretto sul testo della chat. Stesso discorso avviene per le webcam ed il trasferimento di file. Le aziende possono controllare le applicazioni che utilizzano le porte standard 80, 443, le porte non standard, la porta hopping o il traffico criptato SSL garantendo così la sicurezza delle applicazioni. Possono essere sottoposte a filtro utente o di gruppo anche le applicazioni come i social network (Facebook, Twitter), applicazione di carattere più generale quali YouTube, iTunes, gaming, BitTorrent, applicazioni P2P, applicazioni IM e Skype.

Anche queste ultime possono essere settate in base al tempo di navigazione o alla larghezza di banda consentita. Tutto ciò con l'aggiunta del parametro fondamentale definito dal Layer 8 Principi Identity-based. (**Layer 8 Identity-based policies)**.

Contrasto delle minacce e dei malware

Cyberoam fornisce S/W anti-virus e anti-spyware in ambiente thin client. Oltre a questo protegge il traffico in entrata e in uscita eseguendo controlli su più protocolli quali HTTP, HTTPS, FTP, IM, P2P, SMTP, POP3, IMAP, tunnel VPN.

Report conformi

IView di **Cyberoam** fornisce logging e reporting sulla base della tecnologia "**Layer 8 Identity"** che aiuta ad individuare all'interno dell'intera attività di rete le tracce e l'azione di ogni singolo utente. L'interfaccia utente "**cruscotto**" mostra gli eventuali attacchi evidenziandoli su un unico schermo. Da qui è possibile scendere attraverso 3 differenti livelli (modalità drill-down con un massimo di 1000+ aggiornamenti) per indagare sulla tipologia degli attacchi e degli utenti che stanno dietro ognuno di loro. Nonostante la granularità di cui è dotato questa modalità di ricerca permette comunque alle aziende di rispettare la conformità alla privacy relativa alle normative quali HIPAA, CIPA, PCI-DSS, GLBA, ecc. Infine il modulo di reporting chiamato "**4-Eye Authentication**" garantisce che gli amministratori o gli utenti con un elevato livello di privilegi non possano di proposito o accidentalmente accedere autonomamente a dati o documenti ritenuti critici per la sicurezza aziendale normalmente residenti in archivio senza il consenso di una seconda persona precedentemente designata.

Click sull'immagine per aprire il collegamento

Analisi legali

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

Multiple Devices Support

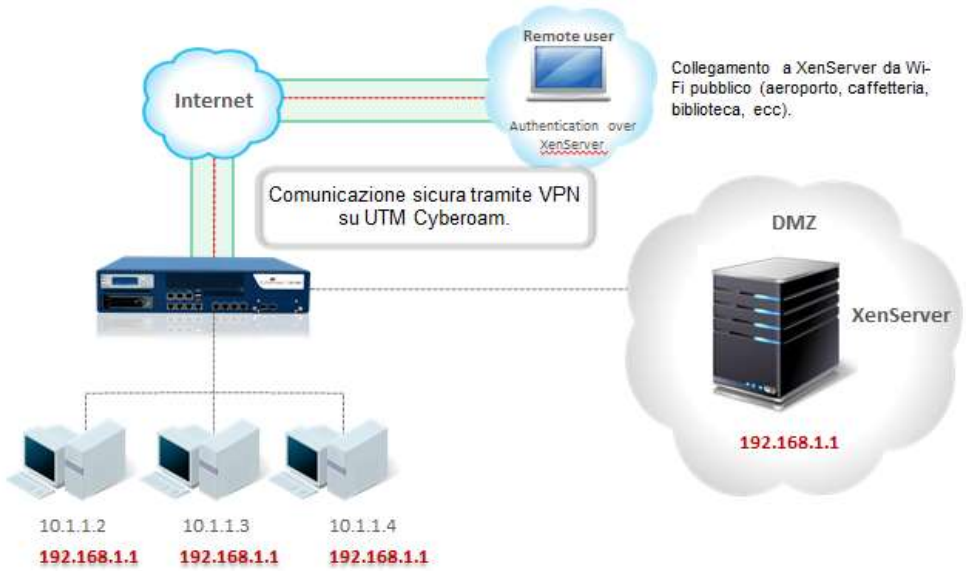
Le appliance Cyberoam iView garantiscono logging e reporting intelligente su diversi dispositivi di rete compresi firewall UTM, Linux IP Tables/Net Filter firewall, Squid ed altri. Le aziende sono così dotate di report sui log attraverso una singola **GUI** molto semplice da utilizzare.

Spazio Terabyte per lo Storage

Cyberoam iView offre Terabyte di spazio disponibile per le esigenze di archiviazione di tutta la reportistica.

Ridondanza dei dati

Le appliance Cyberoam iView utilizzano tecnologia RAID per garantire la ridondanza ed elevati livelli di affidabilità di storage dei dati in modo da salvaguardare l'appliance anche in caso di guasto dell'hard disk. Ecco perché un apparato **Cyberoam** inserito a protezione di una rete virtualizzata Citrix è il massimo che la tecnologia oggi possa offrire.



Ricordate che per poter controllare un gruppo di persone che parlano o scambiano dati tra di loro (ICA protocol) la prima cosa da fare è capirli. Quindi parlare la loro stessa lingua.

Cyberoam GOLD PARTNER

Cliccare sotto per scaricare la presentazione tecnica

"**La sicurezza in ambiente Citrix**"

Il Tuo EterNet Team