



The Future of Network Security

Our Products



Unified Threat Management

Cyberoam – Endpoint Data Protection

- Data Protection & Encryption
- Application Control
- Device Management
- Asset Management



Intelligent Logging & Reporting



Cyberoam Central Console (CC)



SSL VPN

www.cyberoam.com

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.



Comprehensive Network Security

Agenda of Presentation

- **Current Security Challenges**
- **Future Security Trends**
- **Desired Elements in Security Architecture**

www.cyberoam.com

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.

CURRENT SECURITY CHALLENGES

Limitations of Existing Security Architecture



Identity (Lack of User Recognition)

- Who do you give access to: An IP Address or a User?
- Whom do you wish to assign security policies:
Username or IP Addresses?
- In case of an insider attempted breach, whom do you wish to see: User Name or IP Address?
- How do you create network address based policies in a DHCP and a Wi-Fi network?
- How do you create network address based policies for shared desktops?

Limitations of Existing Security Architecture



www.cyberoam.com

- **Scalability**

- To provide IPS, QoS, Centralized logging, etc. normally achieved with multi-core architecture.

- **Lack of Redundancy**

Single point of failure a major business concern in form of redundant device or Multi-Link management.

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.

FUTURE SECURITY TRENDS



Extensible Architecture

www.cyberoam.com

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.



Comprehensive Network Security

Trend: Scalable and Extensible Architecture



- **Scalable Architecture:** Incorporating new threats, and security features within the existing architecture.
- **Extensible Architecture:**
 - Prolongs the life and performance of legacy UTM appliance
 - Automatic security upgrades without end user or Admin intervention
 - Zero hour protection in case of new threats.
 - Ensures continuous business availability.



www.cyberoam.com

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.



Comprehensive Network Security

Trend: Application Layer Control



- **Security Solutions** should recognize and prioritize applications not merely using network ports and protocols for e.g. increase bandwidth for ERP, Accounting, VOIP, and reducing the bandwidth for unproductive applications like P2P, Entertainment.
- **Why?**
 - Enterprises are shifting business critical applications to external Cloud/virtualized platforms
 - Greater tussle for users, applications and bandwidth



www.cyberoam.com

© Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.

Cyberoam Comprehensive Network Security

Trend: Application Layer Control

Internet

Web mail

Medium Quality

High Quality

Low Quality

www.cyberoam.com © Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.

Cyberoam Comprehensive Network Security

Trend: Application Layer Control

Internet

Web mail

Medium Quality

High Quality

Low Quality

Major Benefits

- Visibility and Control over Application Layer i.e. Who is doing what, and consuming how much bandwidth?
- More effective controls over applications such as BitTorrent, SIP, file transfer in Instant Messaging(IMs)
- Ensure Guaranteed & Prioritized access to important applications such as SAP, ERP, CRM, VOIP etc.

www.cyberoam.com © Copyright 2010 Elitecore Technologies Ltd. All Rights Reserved.

Trend: IPv6 as Network Security Layer



- **IPv6 Compliance** is becoming increasingly mandatory for security solutions
 - **Why?**
 - IPv4 addresses are running out
 - Examples:
 - IPv4 - 192.0.2.235
 - IPv6 – 0000:0000:0000:0000:0000:0000



Trend: SSL Inspection



- **SSL Inspection** is an emerging trend in security which Allows filtering of HTTPS traffic same as HTTP traffic.
 - **Why?** To increase security and policy control among Encrypted traffic streams.
 - **Major Benefits:**
 - Admin can control user access to websites via encrypted traffic streams



Trend: Social Networking Protection



Social Networking Growing need to protect social media from malware/financial fraud

- **Why?**
 - Extremely lucrative medium for cyber-criminals
 - Personal info up for grabs
 - User ignorance in using Facebook apps.

Trend: Social Networking Protection



VC's automated Twitter feed spreads malware

by Elinor Mills

[Font size](#) [Print](#) [E-mail](#) [Share](#) [16 comments](#)
[3 retweet](#) [Share](#) [12](#)

Updated June 25 at 9:00 a.m. PDT with Trend Micro saying the Trojan is harmful to Macs and PCs.

Venture capitalist Guy Kawasaki got more than he bargained for from an automated feed he set up on his Twitter account.

Some of Kawasaki's more than 139,000 Twitter followers noticed something strange when they saw a particular non-VC-related tweet sent from his account on Tuesday.

The update advertised a sexy video of "Gossip Girl" star Leighton Meester and had a link leading to a site where, if the visitor clicked to view the video (and ostensibly download a necessary codec), a Trojan called **OSX/Jahlov-C** for the **Mac OS** would be installed instead, Graham Cluley [wrote on his blog](#) on Wednesday for antivirus vendor Sophos.



Guy Kawasaki's Twitter page
(Credit: Twitter)

Late
[Sex-Crazed Tech CEOs Should Be Seen and Not Hurd](#)

hosted by Google, where they are told they need a new version of Adobe's Flash player and are urged to download an executable file to watch the video.

Trend: Avoiding Single Point of Failure



Organizations will have greater need to prevent single Point of failure in their information systems.

Example

- Single point of failure blamed for network Outage for Verizon's Broadband customers.

Trend: Avoiding Single Point of Failure



Single point of failure blamed for Verizon FiOS, DSL outage

By Scott M. Fulton, III | Published October 5, 2009, 11:15 AM

Print Article E-mail Article 5 Comments

A single stalled router is being blamed by Verizon officials for a service outage that impacted customers of its high-speed Internet service, including fiber optic FiOS, in New York and Massachusetts.

The outage occurred at approximately 3:15 pm EDT, according to a message Friday afternoon from the company's chief PR executive, Eric Rabe. He acknowledged that routers typically fail over to adjacent ones, but in this instance, this one didn't.

Wholesale iPhones \$149



Compass/WiFi/TV

Free Shipping

Digitalis.com Ads by Google

"The router went into a hung state and did not appear to the rest of the network as though it was having problems," Rabe wrote, being careful not to name the manufacturer.

According to reporting from Telephony Online's Ed Gubbins, Verizon's principal hardware provider for FiOS is Juniper Networks. In fact, Gubbins reports, Verizon contributes 13% of Juniper's total revenue, and may be the sole reason why that company found black ink again last year.

Juniper's E-series routers service Verizon's broadband network. Last October, Juniper announced a major upgrade to its routers' operating system, adding features that included the capability for service providers to deploy deep packet inspection -- the ability to analyze Internet traffic based on its contents. The company marketed this feature as part of its "Intelligent Services Edge" portfolio, which it described as



Trend: Avoiding Single Point of Failure

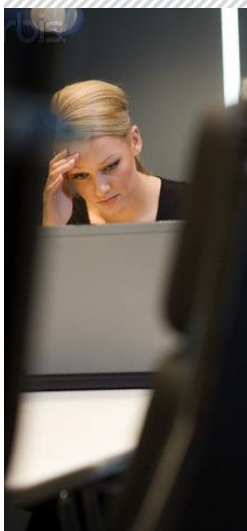


Current Methods

- Multiple Link Management with more than 1 ISP Link Failover
- High Availability
- 3G/4G Connectivity



Trend: Securing Wireless Networks



- **Organizations** must afford the same degree of security to wireless networks as wired networks

Why?

- Guest user access to goes untraced.
- Cyber-terrorism.

How to Ensure WLAN Security?

- Gain Visibility over User activities in the Network through identity-based controls

Trend: Growing demand for NAC



- **Network Access Control** systems integrate endpoint security technologies with user or system authentication.
 - **Why?** Unified Policies for Network Access prevents insider threats and data leakage.



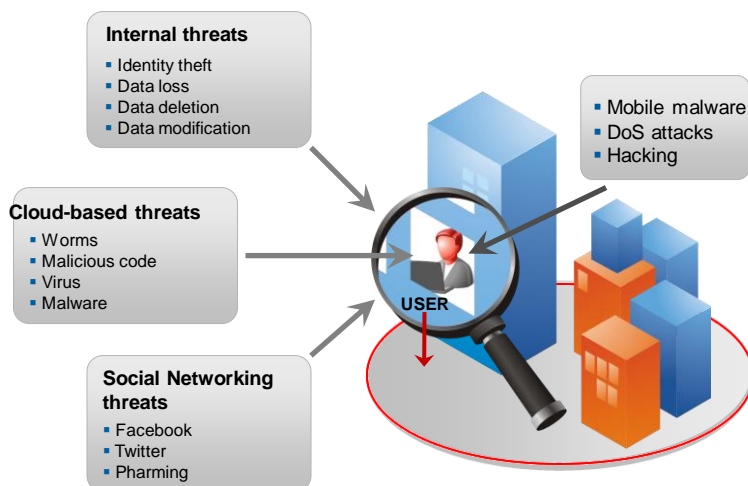
DESIRED ELEMENTS IN SECURITY ARCHITECTURE

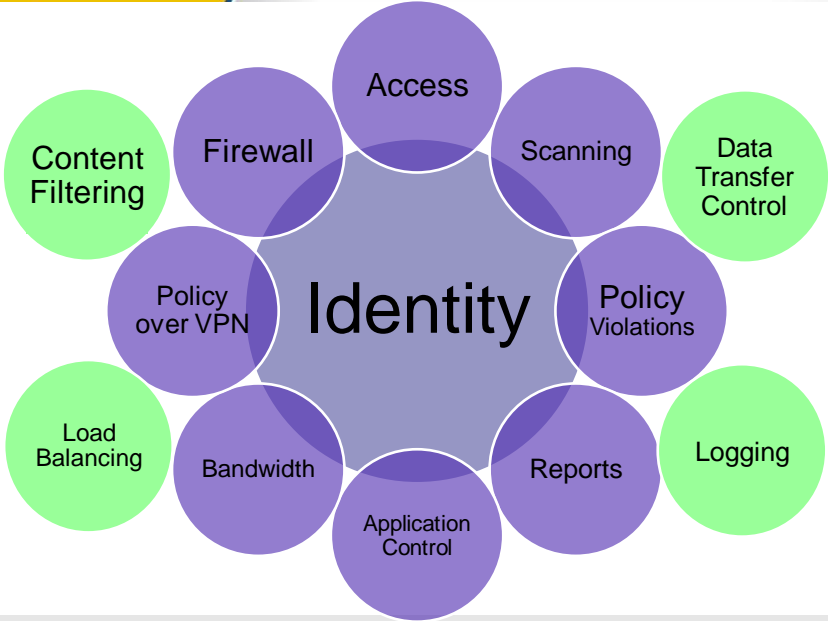
Desired Elements in NSA



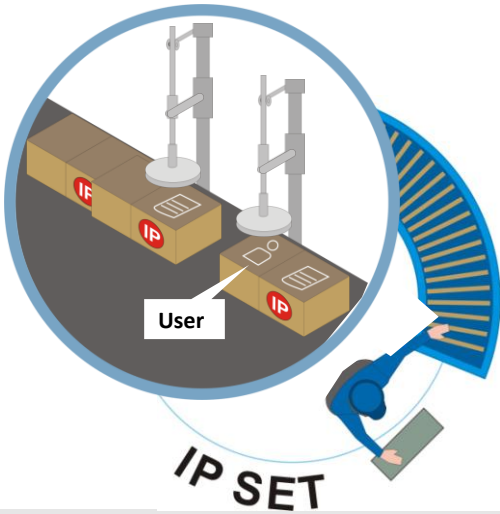
- Identity-based Security
 - *Secure the User – Secure the Organization*
- Hardware and Software Intelligence
 - Adaptability, Reliability, Robustness of systems
- Unified Policy and Configuration Management
- Redundant hardware components to support High Availability
- Scalable Processing Capability
- Connectivity

User: The Missing Link in Security



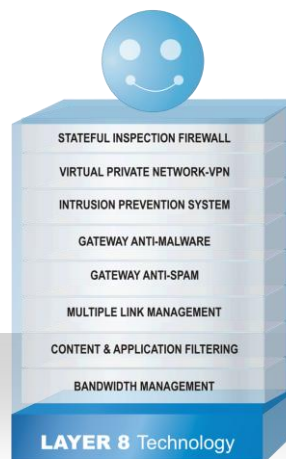


IDENTITY-BASED TECHNOLOGY



Cyberoam UTM- Identity-based Security

- Integrated security over single platform
- Layer 8 penetrates through each security module





About Elitecore



- Established in 1999
- 1000+ Employees
- ISO 9001:2000 certified company
- Sales, Distribution Channel & Customers across 100+ countries
- Communication - Networks – Security
 - Cyberoam - Network to Endpoint Security
 - CRESTEL - Telecommunication OSS BSS
 - EliteAAA - Telecommunication
 - 24online - Bandwidth Management Solution

Cyberoam Comprehensive Network Security

Cyberoam Product Range

Cyberoam – Identity Based UTM



Cyberoam IView – Logging & Reporting (Open Source - Software)



Cyberoam – End Point Data Protection



Cyberoam – SSL VPN



CR SSL Series : CR-SSL-800, CR-SSL-1200, CR-SSL-2400

Cyberoam Comprehensive Network Security

Thank You