

Cyberoam Next Generation Security

ProtektNet

Our Products



Cyberoam
Network Security Appliances - UTM, NGFW
(Hardware & Virtual)



Cyberoam Introduction

- ▶ **Technology Powerhouse**
- ▶ **550+ Employees**
- ▶ **Sales, Distribution Channel and Customers across 125+ Countries**
- ▶ **Amongst the top 3 global players for network security features**
- ▶ **Patent-pending Identity-based Management**

One stop shop: Cyberoam's Holistic Security Solutions



Network Security



Centralized security
Management



Network Monitoring &
Analysis



Securing Home users





Network Security Appliances – UTM, NGFW
(Hardware & Virtual)

Cyberoam Layer 8 User-ID Technology



Powerful Hardware

- Multicore Gigahertz processors for Nano second security processing
- Gigabit Ports to integrate with Gigabit network

Intelligent Firmware

- Tight integration with Hardware
- Network & Crypto Acceleration

Cyberoam®os

The Magic of Parallel Task Execution

Multi-core Technology

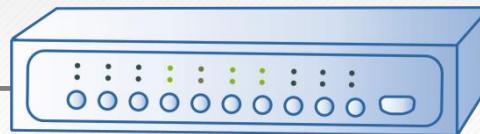


One Task = 3 ms

Parallel Execution

Ten Tasks = 15 ms

Purpose built Technology

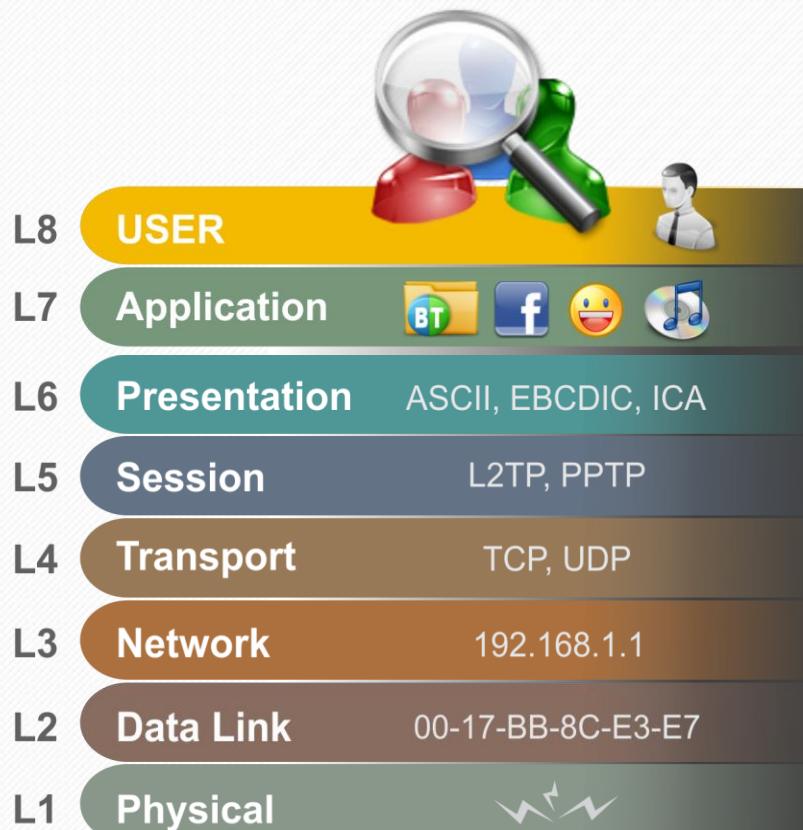


One Task = 2 ms

Serial Execution

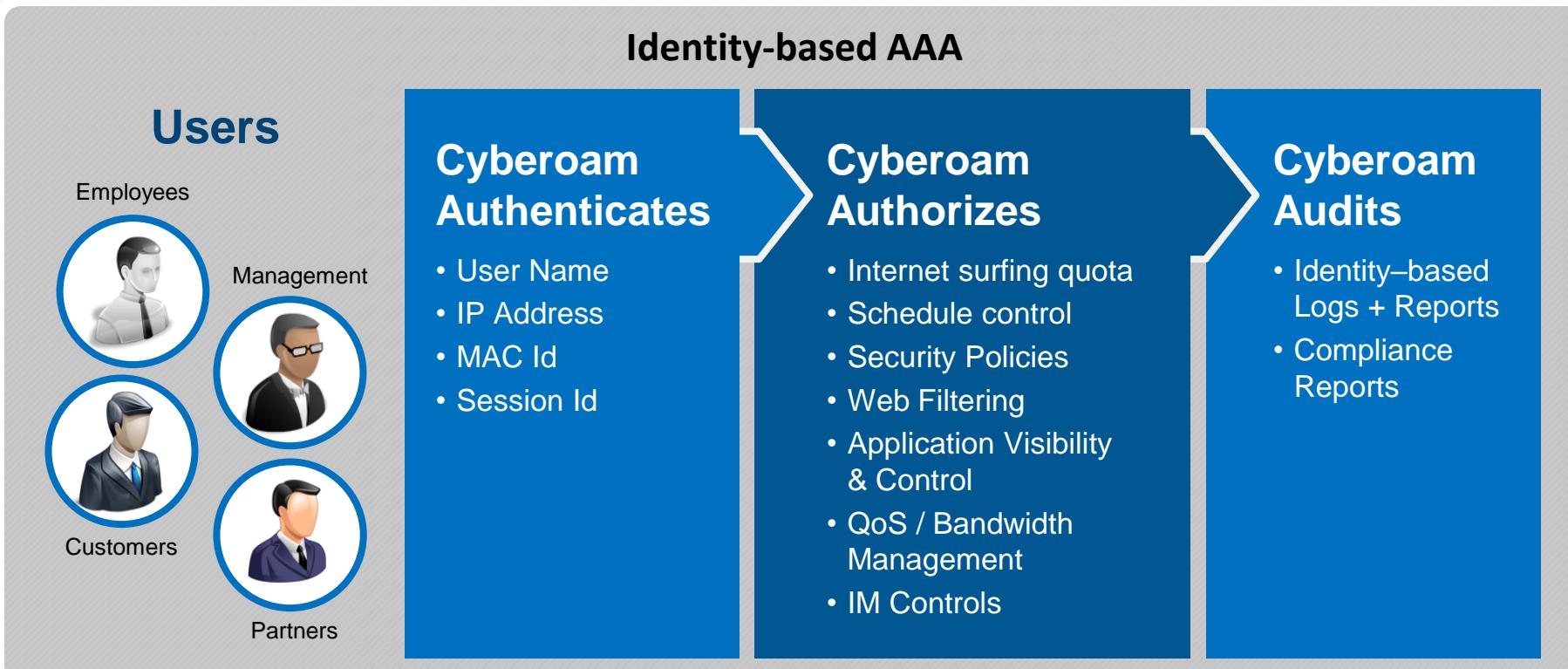
Ten Tasks = 20 ms

This is strictly a conceptual representation of the actual process, not to be taken literally.



**Cyberoam's Layer 8 Technology
treats "User Identity" as the
8th Layer in the protocol stack**

Cyberoam network security appliances offer security across Layer 2-Layer 8 using Identity-based policies



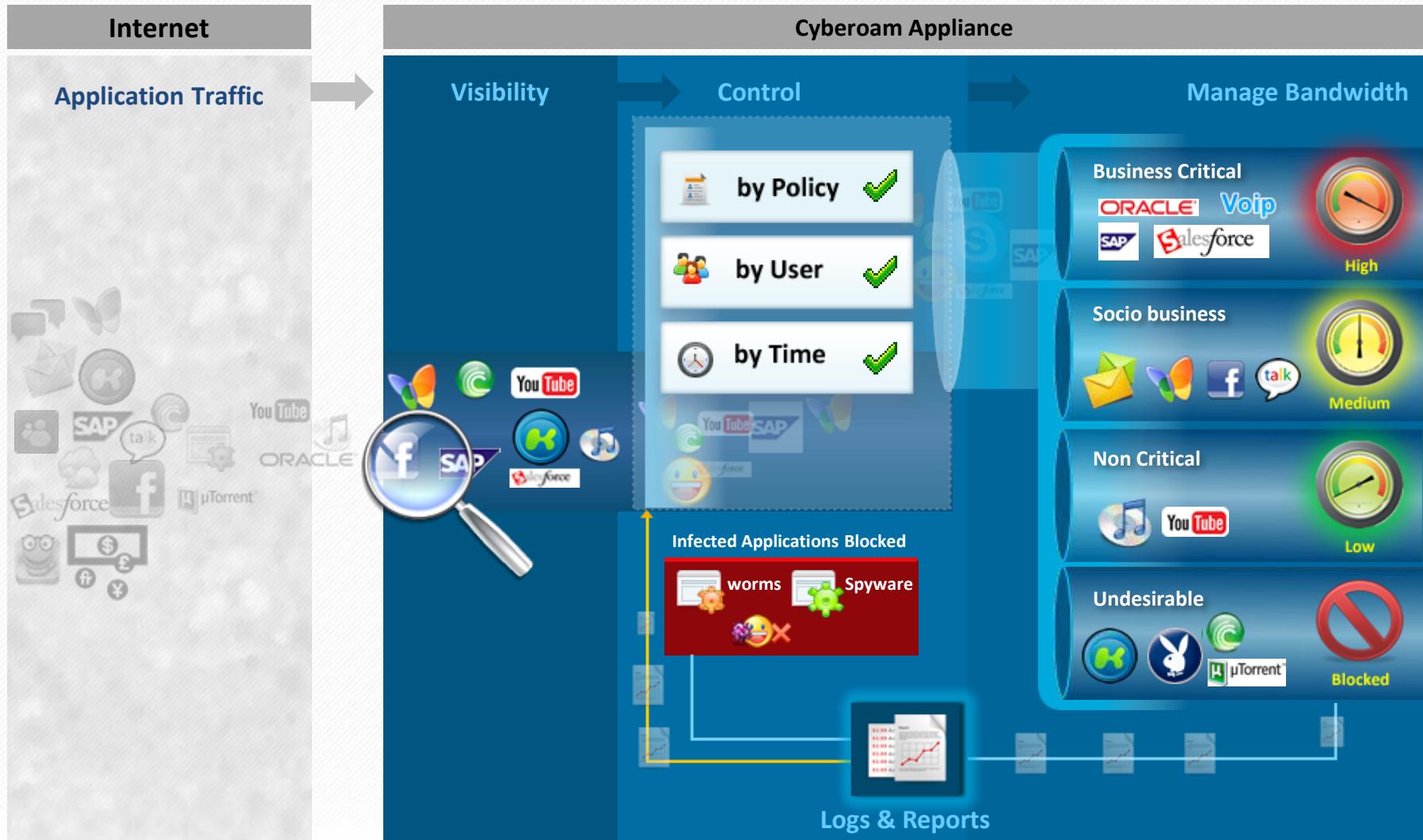
Control user network activities

- Who can connect to the network
- Who can access what
- What have they accessed

Ability to track the user activities; identify attackers /victims

Take quick network security decisions

Prioritize applications with Layer 7 and Layer 8 controls



Controls over applications based on User Identity, Time, Application and Bandwidth

Granular classification of applications

Policy	Category	Risk Level	Characteristics	Technology
Application Filter Criteria <div style="border: 2px solid red; padding: 5px;"> Category <input checked="" type="checkbox"/> Select All <input checked="" type="checkbox"/> File Transfer (29) <input checked="" type="checkbox"/> Gaming (20) <input checked="" type="checkbox"/> General Internet (49) </div> <div style="border: 2px solid blue; padding: 5px;"> Risk <input type="checkbox"/> Select All <input type="checkbox"/> 1 - Very Low (353) <input type="checkbox"/> 2 - Low (126) <input type="checkbox"/> 3 - Medium (271) </div> <div style="border: 2px solid green; padding: 5px;"> Characteristics <input type="checkbox"/> Select All <input type="checkbox"/> Excessive Bandwidth (355) <input type="checkbox"/> Prone to misuse (187) <input type="checkbox"/> Transfer files (262) </div> <div style="border: 2px solid yellow; padding: 5px;"> Technology <input type="checkbox"/> Select All <input type="checkbox"/> Browser Based (313) <input type="checkbox"/> Client Server (315) <input type="checkbox"/> Network Protocol (354) </div>	File Transfer	Very Low (1)	Excessive Bandwidth	Browser Based
	Gaming	Low (2)	Prone to misuse	Client Server
	General Internet	Medium (3)	Transfer files	Network Protocol
	Instant Messenger	High (4)	Tunnel other apps	P2P
	Infrastructure	Very High (5)	Widely used	Network Protocol
	Network Services		Loss of Productivity	Client Server
	P2P		Can bypass firewall policy	Browser Based
	Proxy and Tunnel			
	Remote Access			
	Streaming Media			
	VoIP			
	Mobile Applications			
	Social Networking			
	Web Mail			
	And more...			

- **Real time visibility into user and network activities**
- **Traffic Discovery**
 - Real-time visibility into bandwidth utilization by user, protocol, application



Layer-8 User-based Reports

Cyberoam

DASHBOARDS Main Dashboard Custom Dashboard SEARCH REPORTS TREND REPORTS COMPLIANCE REPORTS

Start Date: 2013-01-01 End Date: 2013-02-08 Go

Application Show 5 records per page User: joseph@cyberoam.local X From: 2013-01-01 00:00:00 To: 2013-02-08 23:59:59

Top Application Categories

Category	Bytes
Streaming Media	4.12GB
Infrastructure	3.49GB
General Internet	1.98GB
P2P	1.44GB
Conferencing	501.49MB

Top Applications

Application/Proto/Port	Bytes
Youtube Video Streaming	3.49GB
POP3	2.24GB
HTTP	1.85GB
Secure Socket Layer Protocol	1.07GB
TCP:80	667.66MB

Top Technologies

Technology	Bytes
Browser Based	6.24GB
Network Protocol	3.48GB
P2P	1.44GB
Client Server	846.29MB

Top Users

User	Bytes
joseph@cyberoam.local	12.03GB
joseph@cyberoam.local	640372
joseph@cyberoam.local	12.03 GB

Home Help Logout

Risk 2.04

The screenshot shows a Cyberoam user-based reporting interface. On the left, a sidebar lists navigation options: DASHBOARDS, Main Dashboard (selected), Custom Dashboard, SEARCH, REPORTS (selected), TREND REPORTS, and COMPLIANCE REPORTS. The main area displays four reports: Top Application Categories, Top Applications, Top Technologies, and Top Users. The Top Applications report includes a risk rating scale from 1 to 5. A green circle highlights the search bar in the Application report and the risk rating in the Applications report. The Top Users report shows a single user entry for 'joseph@cyberoam.local' with a large blue bar indicating 12.03GB usage.

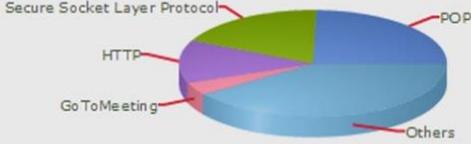
Dual Dashboard – Traffic & Security Dashboard

Traffic Dashboard

Traffic Dashboard Security Dashboard    From: 2012-11-01 00:00:00
To: 2012-11-23 23:59:59

Show 5 records per page

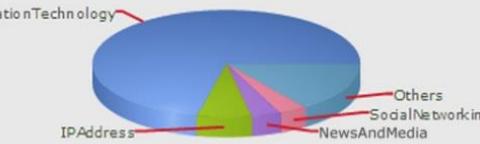
Top Applications



Application/Proto:Port	Bytes	Percent
POP3	17.8 GB	24.6 %
Secure Socket Layer Protocol	13.32 GB	18.41 %
HTTP	9.2 GB	12.71 %
GoToMeeting	2.81 GB	3.88 %
Others	29.23 GB	40.4 %

[View All](#)

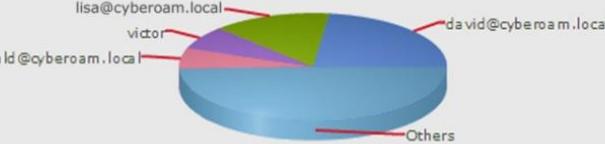
Top Categories



Category	Hits	Percent
InformationTechnology	1652646	71.39 %
IPAddress	154844	6.69 %
NewsAndMedia	83453	3.6 %
SocialNetworking	78151	3.38 %
Others	345957	14.94 %

[View All](#)

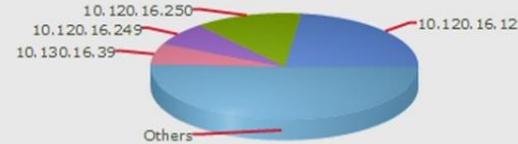
Top Users



User	Bytes	Percent
david@cyberoam.local	16.63 GB	22.98 %
lisa@cyberoam.local	10.5 GB	14.51 %
victor	5.07 GB	7.01 %
donald@cyberoam.local	4.42 GB	6.11 %
Others	35.74 GB	49.39 %

[View All](#)

Top Hosts



Host	Bytes	Percent
10.120.16.127	16.61 GB	22.96 %
10.120.16.250	9.55 GB	13.2 %
10.120.16.249	5.07 GB	7.01 %
10.130.16.39	4.43 GB	6.12 %
Others	36.69 GB	50.71 %

[View All](#)

©

Top Source Countries

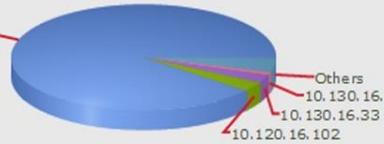
Top Destination Countries

Security Dashboard

Traffic Dashboard **Security Dashboard**

Show 5 records per page

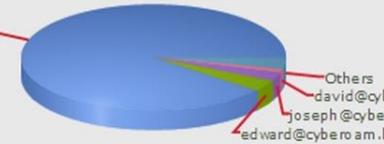
Top Denied Hosts



Host	Hits	Percent
10.130.16.43	118450	89.28 %
10.120.16.102	3835	2.89 %
10.130.16.33	3257	2.45 %
10.130.16.36	1242	0.94 %
Others	5889	4.44 %

[View All](#)

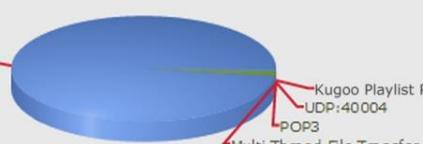
Top Denied Users



User	Hits	Percent
bunny@cyberoam.local	118538	89.35 %
edward@cyberoam.local	4650	3.5 %
joseph@cyberoam.local	3380	2.55 %
david@cyberoam.local	1460	1.1 %
Others	4645	3.5 %

[View All](#)

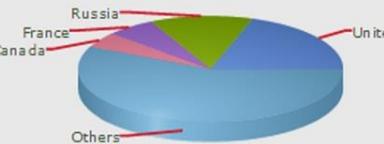
Top Denied Applications



Application/Proto:Port	Hits	Percent
Torrent Clients P2P	130085	98.05 %
Multi Thread File Transfer	1159	0.87 %
POP3	118	0.09 %
UDP:40004	110	0.08 %
Kugoo Playlist P2P	1201	0.91 %

[View All](#)

Top Denied Destination Countries



Country	Hits	Percent
United States	26162	19.72 %
Russia	17031	12.84 %
France	8088	6.1 %
Canada	6012	4.53 %
Others	75380	56.82 %

[View All](#)

From: 2012-11-01 00:00:00 To: 2012-11-23 23:59:59

Application Reports

REPORTS

- Application
 - Top Application Categories
 - Top Applications
 - Top Technologies
 - Top Risks
 - Top Users
 - Top Hosts
 - Country Map
 - Top Source Countries
 - Top Destination Countries
 - Top Rule ID
- Web Usage
- WAF
- Mail Usage
- IM Usage
- FTP Usage
- VPN
- SSL VPN
- Internet Usage
- Blocked Applications
- Blocked Web Attempts
- Blocked IM Attempts
- Denied SSL VPN Attempts
- Attacks
- Spam
- Virus
- Event
- Search Engine

Start Date: 2013-05-01 End Date: 2013-05-10

Application > Top Applications Show: 10 records per page

Application/Proto:Port	Category	Bytes
POP3	Protocol	2.39GB
Secure Socket Layer Protocol	Protocol	4.5GB
HTTP	Protocol	3.73GB
Skype Services	Protocol	2.79GB
NetBIOS	Protocol	4.66GB
Windows Live Website	Protocol	
Skype	Protocol	
DNS	Protocol	
Facebook Website	Social Networking	
Multi Thread File Transfer	File Transfer	

From: 2013-05-01 00:00:00 To: 2013-05-10 23:59:59

Risk: 1.95

Compliance Reports



DASHBOARDS

SEARCH

REPORTS

TREND REPORTS

COMPLIANCE REPORTS

HIPAA

GLBA

SOX

PCI

- Top Viruses

- Top Attacks

- Top Attackers

- Admin Events

- Authentication Events

FISMA

Start Date 2013-01-29

End Date 2013-02-04



COMPLIANCE REPORTS

► HIPAA

► GLBA

► SOX

► PCI

.. Top Viruses

.. Top Attacks

.. Top Attackers

.. Admin Events

.. Authentication Events

► FISMA

GnuTLS TLS Record Application

WEB-MISC SSLv2 Client_Hello

HTTPS/SSL Renegotiation DoS

SNMP request udp

SNMP public access udp

GnuTLS TLS Record Application Ge

NETBIOS SMB-DS repeated logon fa

WEB-MISC PCT Client_Hello overlow

MS-SQL probe response overflow attempt

WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt

HTTP DoS Attack - Slowloris

POP3 Login Brute Force Attack

Page 1 of 3

Go to page :

Go

[Hide Graph]

[Hide Table]



From: 2013-01-29 00:00:00
To: 2013-02-04 23:59:59

4.45K

3.39K

3.39K

2K

3K

4K

5K

Hits

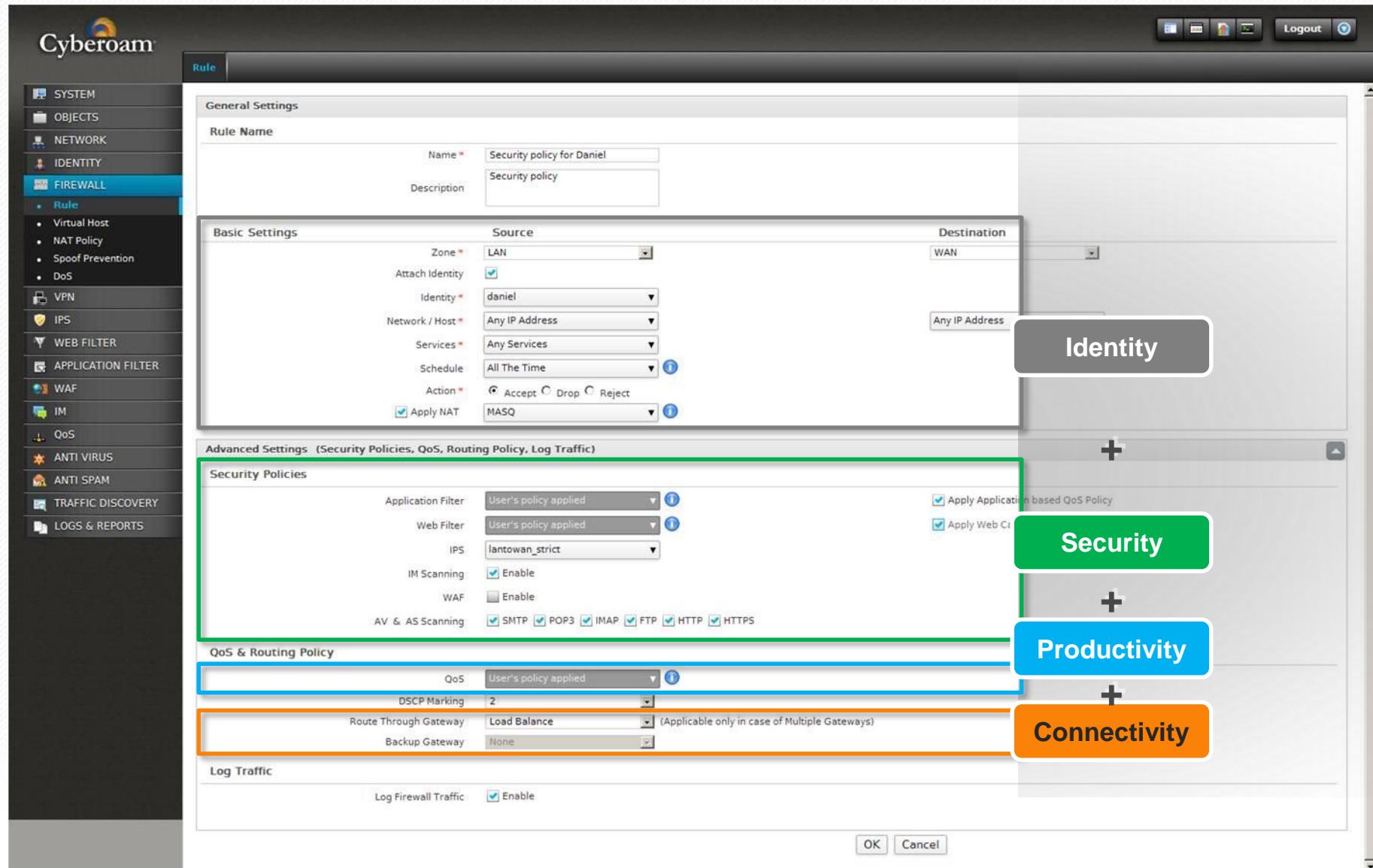
Hits

Interactive World Traffic Map



Interactive World Traffic Map for Source and Destination traffic

Configure rules for all features from Firewall page



The screenshot shows the Cyberoam Firewall configuration interface. The left sidebar contains navigation links for SYSTEM, OBJECTS, NETWORK, IDENTITY, FIREWALL, Rule, Virtual Host, NAT Policy, Spoof Prevention, DoS, VPN, IPS, WEB FILTER, APPLICATION FILTER, WAF, IM, QoS, ANTI VIRUS, ANTI SPAM, TRAFFIC DISCOVERY, LOGS & REPORTS, and Firewall Rules.

General Settings:

- Rule Name: Security policy for Daniel
- Description: Security policy

Basic Settings:

Source		Destination
Zone:	LAN	WAN
Attach Identity:	<input checked="" type="checkbox"/>	
Identity:	daniel	
Network / Host:	Any IP Address	Any IP Address
Services:	Any Services	
Schedule:	All The Time	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Drop <input type="radio"/> Reject	
Apply NAT:	MASQ	

Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic):

Security Policies:

- Application Filter: User's policy applied
- Web Filter: User's policy applied
- IPS: lanwan_strict
- IM Scanning: Enable
- WAF: Enable
- AV & AS Scanning: SMTP POP3 IMAP FTP HTTP HTTPS

QoS & Routing Policy:

- QoS: User's policy applied
- DSCP Marking: 2
- Route Through Gateway: Load Balance (Applicable only in case of Multiple Gateways)
- Backup Gateway: None

Log Traffic:

- Log Firewall Traffic: Enable

Identity (highlighted in grey box over Basic Settings)

Security (highlighted in green box over Advanced Settings)

Productivity (highlighted in blue box over Log Traffic)

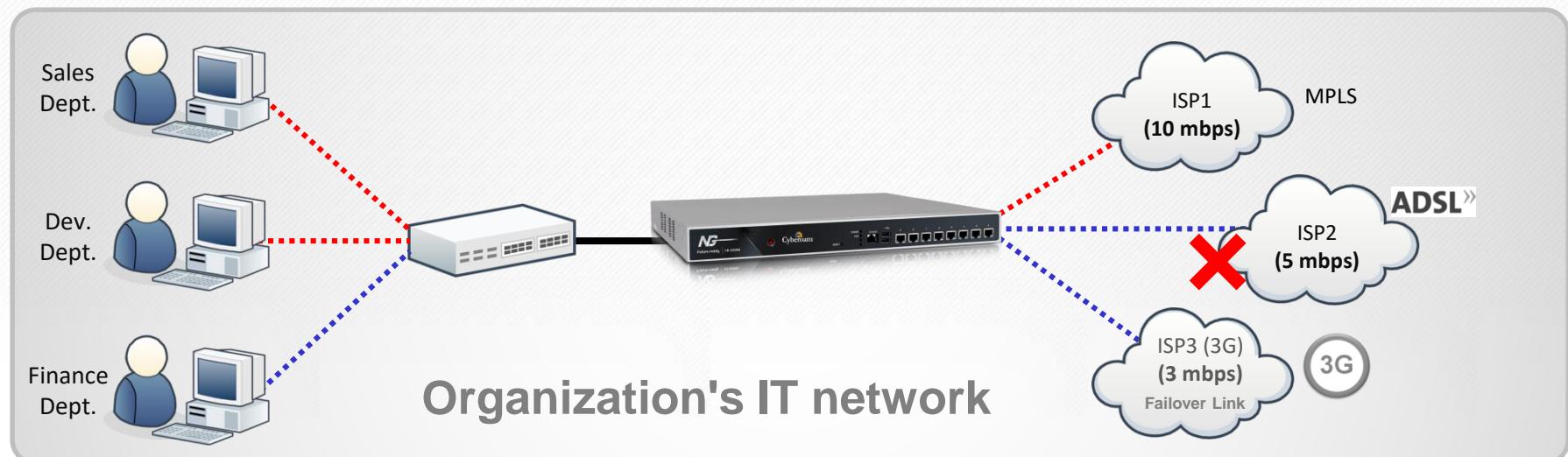
Connectivity (highlighted in orange box over Log Traffic)

■ High Availability

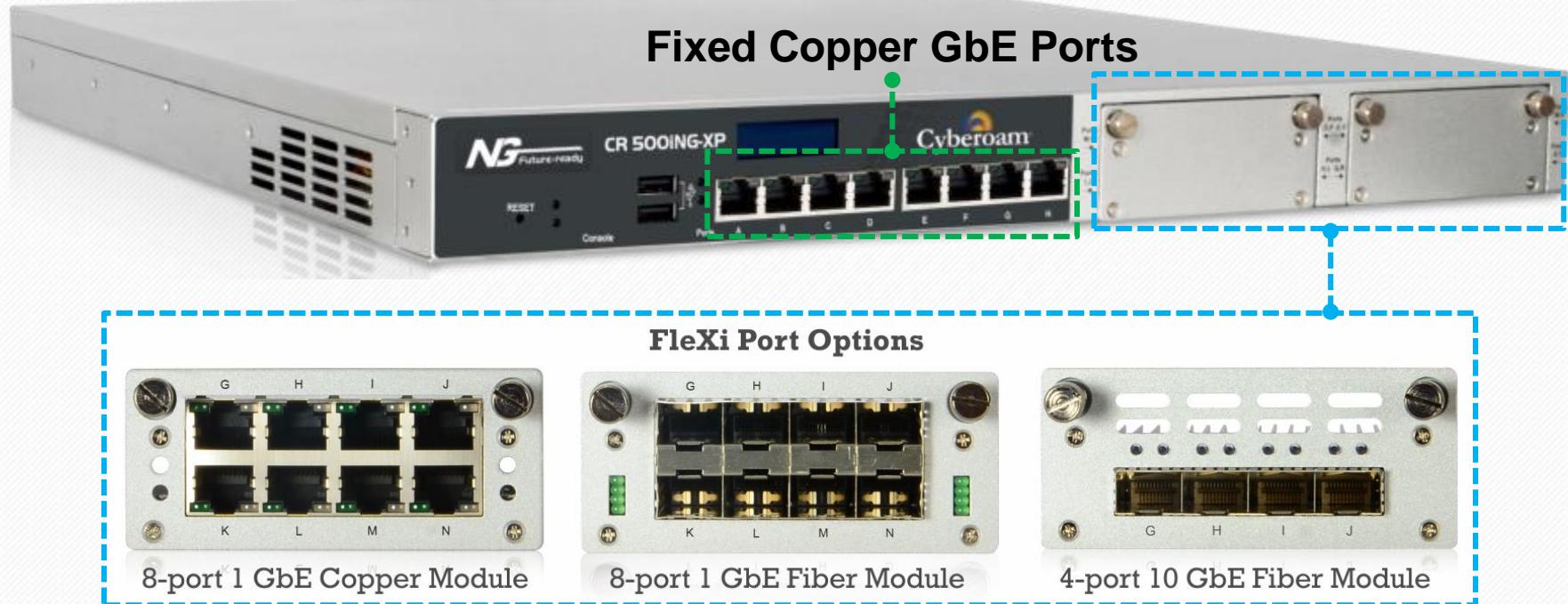
- Active-Active & Active-Passive
- Reduces single-point-of-failure
- Maximizes network uptime
- Ensures continuous network security

■ Multiple Link Management with Automated Load Balancing

- Multiple WAN and WWAN (3G/4G, WiMax) link management with multiple failover conditions
 - Active-Active and Active-Passive Auto Link Failover
 - Gateway failover over VPN



FleXi Ports for flexible network connectivity



Combination of Fixed Ports
and Flexible Ports

Flexibility to choose Copper,
Fiber 1GbE / 10GbE modules

Modules can be purchased
individually as per need

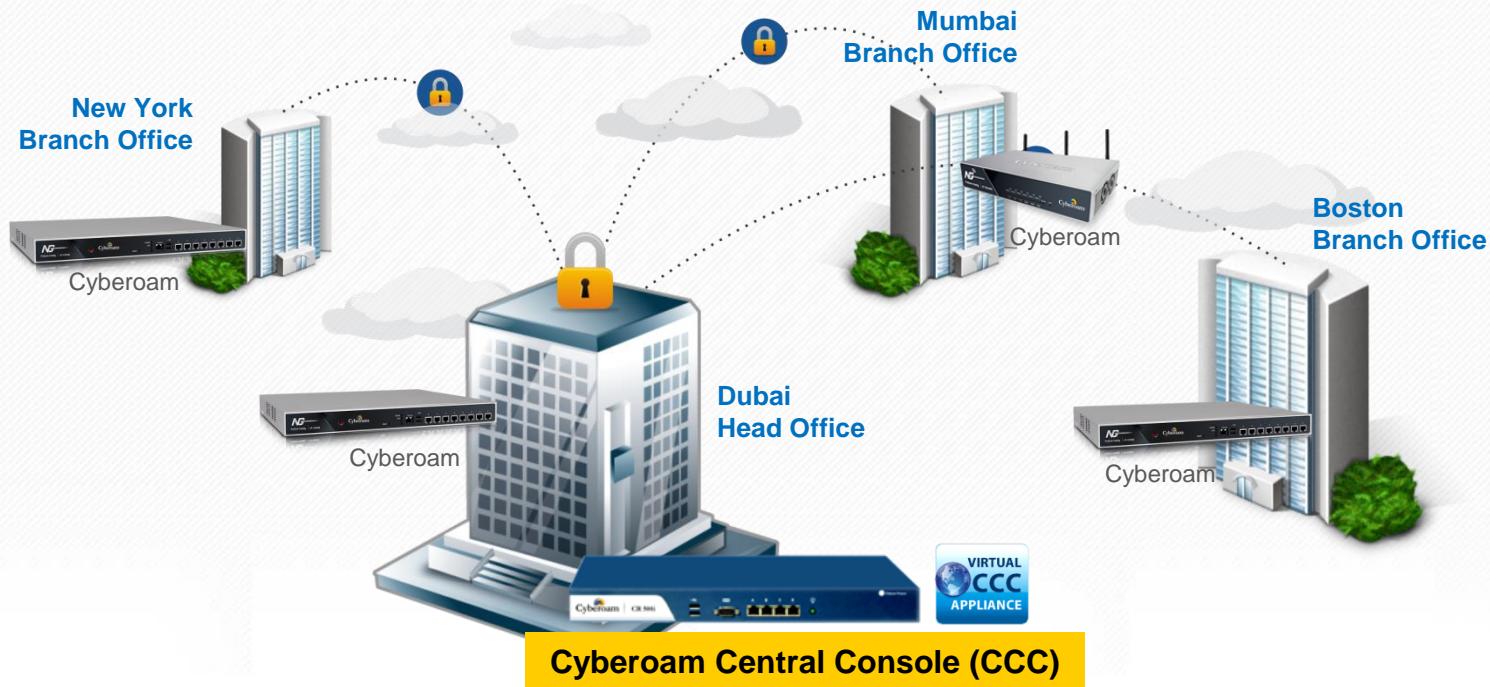


Holistic Security for Connected Critical Infrastructure

Integrated threat protection, situational awareness and security controls for Industrial Control Systems (ICS) including SCADA

Cyberoam Central Console (CCC)

- CCC is for centralized, integrated management and monitoring of Cyberoam network security devices
 - Offers complete control over distributed networks from head office (H.O.) or Security Operations Center (S.O.C.) of MSSPs
- Available as
 - Hardware CCC Appliances, Virtual CCC Appliances



Organizations cannot afford to compromise on any of these.
The right SCP balance is essential!

Security

Network Security

- Firewall
- Intrusion Prevention System
- Web Application Firewall

Content Security

- Anti-Virus/Anti-Spyware
- Anti-Spam (Inbound/Outbound)##
- HTTPS/SSL Content Security

Administrative Security

- Next-Gen UI
- iView- Logging & Reporting



Connectivity

Business Continuity

- Multiple Link Management
- High Availability

Network Availability

- VPN
- 3G/4G/WiMAX Connectivity

Future-ready Connectivity

- "IPv6 Ready" Gold Logo
- FleXi Ports



Productivity

Employee Productivity

- Content Filtering
- Instant Messaging Archiving & Controls

IT Resource Optimization

- Bandwidth Management
- Traffic Discovery
- Application Visibility & Control

Administrator Productivity

- Next-Gen UI



... - WebUI
- UI Next-Gen
- Virtualization Ready



... - FleXi Ports
- Network Availability
- Future-ready Connectivity



... - UI Next-Gen
- Virtualization Ready



Product Certifications



Cyberoam achieves
Common Criteria
EAL4+ Certification

Checkmark



UTM Level 5:

Cyberoam holds a unique & complete UTM certification

westcoast labs
Checkmark
www.check-mark.com

westcoast labs
Checkmark
www.check-mark.com

westcoast labs
Checkmark
www.check-mark.com

westcoast labs
Checkmark
www.check-mark.com

Firewall VPN Anti-Virus Anti-Spyware

Premium
Checkmark
www.check-mark.com

Premium
Checkmark
www.check-mark.com

Premium
Checkmark
www.check-mark.com

Anti-Spam URL Filtering IPS/IDP



ICSA Certified Firewall



ICSA Certified
High-Availability

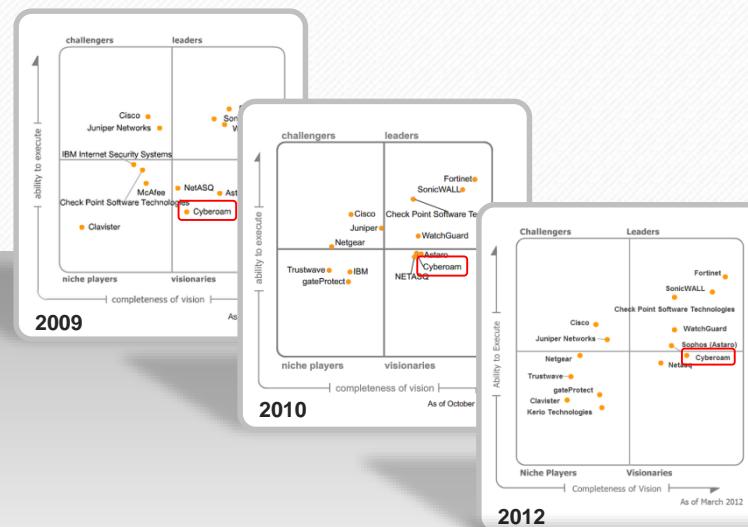


VPNC Certified for Basic
VPN & AES Interoperability

Recognized as 'Visionary' in the Gartner UTM MQ

2013

Magic Quadrant for Unified Threat Management



Clientele Worldwide

BFSI



Manufacturing



Government



Education



Pharma & Healthcare



Telecom & ISP



Clientele Worldwide

Hotels



Retail & Services



IT/BPO & Media



Others



Cyberoam Live Demo



Link:
<http://demo.cyberoam.com>

Credentials:
guest /guest

Get a 30 day FREE Evaluation of
Cyberoam Virtual appliance

Username:

Password:

Language: English

Log on to: Web Admin Console

Username:

Password:

Training & Certification



PROTEKTNET



Developing competencies with
Cyberoam Next Generation security appliances

CYBEROAM CERTIFIED NETWORK & SECURITY PROFESSIONAL (CCNSP)

CYBEROAM CERTIFIED NETWORK & SECURITY EXPERT (CCNSE)

CYBEROAM CERTIFIED TRAINER (CCT)