

## HUAWEI USG6650



Primo mese nel mondo reale ( L2 mode )

## Cosa non sara'...

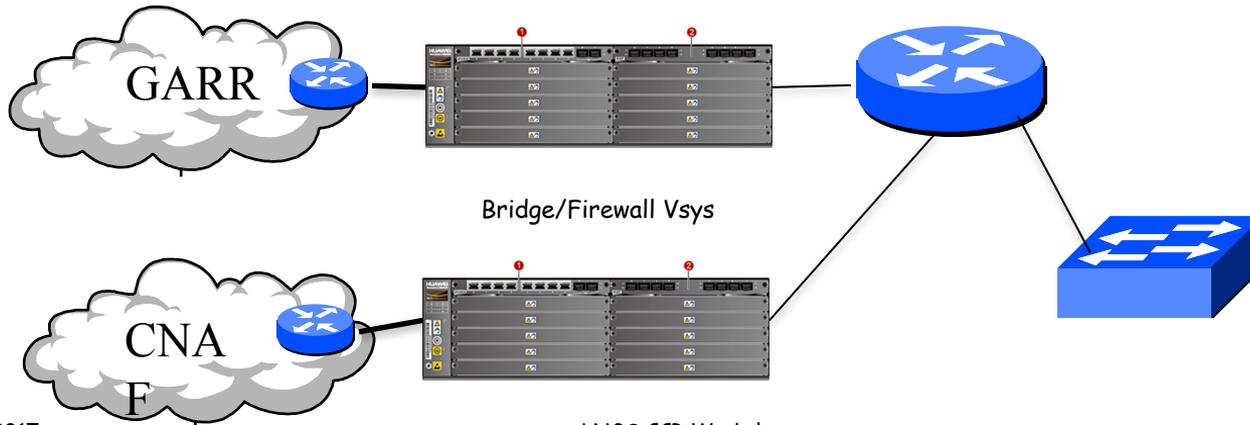
- Misure prestazionali basate su standard
- Confronto con altri device nelle stesse condizioni operative (gli ambienti sono diversi)
- Analisi approfondita delle funzionalita' del prodotto
- Analisi economica dei rapporti costi/benefici

## Cosa cercherà di essere...

- Prove funzionali indirizzate alla sostituzione in produzione del FW/ROUTER esistente JuniperISG2000 (fuori manutenzione)
- Replicazione di ACL e IDS
- Sperimentazione di AV e Application Control
- Analisi di altre funzionalità
- Confronto con Fortinet 1500D seguendo la traccia della presentazione di Massimo a La Biodola (gli ho copiato anche le slide )  
😊

## Layout

- Partizionabile in 10 Vsys (con la licenza base)
- Installabile in configurazione HA



## Funzionalità richieste

- Stateful ACL basate su source:port destination:port
- IDS basato su Anomaly Detection e Application signature behaviour
- AV basato su signature
- Content Filtering preventivo basato su white/black list
- Stateful Policy basate su Application control
- Log real-time e remote syslog

# Caratteristiche USG6650



Table 1. Wide Service Interface Cards (WSICs) for USG6600 Series

Feature	2XG8GE	8GE
		
Technical Specification		
Integrated Ports	2 x 10GE (SFP+), 8 x GE (RJ45)	8 x GE (RJ45)

Feature	8GEF	4GE-BYPASS
		
Technical Specification		
Integrated Ports	8 x GE (SFP)	4 x GE (RJ45) BYPASS

1. 8 x GE (RJ45) and 2 x 10 GE (SFP+) Ports
2. 8 x GE (SFP) Ports
3. 2 x USB Ports
4. 1 x GE (RJ45) Management Port
5. Console Port (RJ45)
6. Console Port (Mini-USB)

## Caratteristiche USG6650

Model	USG6650	USG6660	USG6670	USG6680
IPv4 Firewall Throughput <sup>1</sup> (1518/512/64-byte, UDP)	20/20/8 Gbit/s	25/25/8 Gbit/s	35/35/8 Gbit/s	40/35/8 Gbit/s
IPv6 Firewall Throughput <sup>1</sup> (1518/512/84-byte, UDP)	20/20/8 Gbit/s	25/25/8 Gbit/s	35/35/8 Gbit/s	40/35/8 Gbit/s
Firewall Throughput (Packets Per Second)	12 Mpps	12 Mpps	12 Mpps	12 Mpps
Firewall Latency (64-byte, UDP)	16 μs	16 μs	16 μs	16 μs
FW + SA* Throughput <sup>2</sup>	15 Gbit/s	18 Gbit/s	19 Gbit/s	20 Gbit/s
FW + SA* Throughput (Realworld) <sup>3</sup>	11 Gbit/s	12 Gbit/s	13 Gbit/s	18 Gbit/s
FW + SA + IPS Throughput <sup>2</sup>	8.8 Gbit/s	8.8 Gbit/s	8.8 Gbit/s	15 Gbit/s
FW + SA + Antivirus Throughput <sup>2</sup>	8 Gbit/s	8 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus + URL Throughput <sup>2</sup>	6 Gbit/s	7 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus Throughput (Realworld) <sup>3</sup>	5 Gbit/s	5.5 Gbit/s	6 Gbit/s	11 Gbit/s
Concurrent Sessions (HTTP1.1) <sup>1</sup>	8,000,000	10,000,000	10,000,000	12,000,000
New Sessions/Second (HTTP1.1) <sup>1</sup>	300,000	350,000	400,000	400,000
IPsec VPN Throughput <sup>1</sup> (AES-128 + SHA1, 1420-byte)	15 Gbit/s	18 Gbit/s	18 Gbit/s	18 Gbit/s

## Implementazione

- Filtri abilitati in ingresso ( $Garr \rightarrow BO$ ) ( $CNAF \rightarrow BO$ ):
  - Application Control
  - Intrusion Prevention System
  - Antivirus
- Filtri abilitati in uscita ( $Garr \leftarrow BO$ ) ( $Garr \leftarrow BO$ ) :
  - Application Control
  - Intrusion Prevention System
  - Antivirus
  - Web filtering (solo su alcuni HOST)
  - APT (solo sul mio PC)

# Implementazione

Security Policy List														
Name	Source Zone	Destination Z...	Source Addr...	Destination Addr...	User	Service	Application	Schedule	Action	Content Security	Hits	Enable	Edit	
to test	any	any	test	test	any	any	any	any	Permit		1675	Reset	<input checked="" type="checkbox"/>	
from test	any	any	test	any	any	any	any	any	Permit		3887	Reset	<input checked="" type="checkbox"/>	
Conf	any	any	any	Conf	any	telnet	any	any	Deny		8485	Reset	<input checked="" type="checkbox"/>	
ConfPermit	any	any	ConfPermit	Conf	any	any	any	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
Selesta	any	any	Selesta server	Selesta BO	any	any	any	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
Openvpn	any	any	any	any	any	openvpn	any	any	Permit		5866	Reset	<input checked="" type="checkbox"/>	
Opita01 to operadb	any	any	opita01.Ings.in	operadb.bo.infn.it	any	any	any	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
SSH	any	any	any	any	any	ssh	any	any	Permit		2.7*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
FROM AUDIBO	any	any	audibo	any	any	any	any	any	Permit		5.0*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
FROM POSTA	any	any	posta	any	any	any	any	any	Permit		5.2*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
TO POSTA	any	any	posta	any	any	any	any	any	Permit		3.2*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
RDP bruteforce attack 1...	any	any	any	RDP	any	any	any	any	Deny		6.7*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
TOMYPC	untrust	trust	any	131.154.12.127/255.255	any	any	any	any	Permit		698	Reset	<input checked="" type="checkbox"/>	
FRANMYPC	untrust	trust	131.154.12.127/25	any	any	any	any	any	Permit		3280	Reset	<input checked="" type="checkbox"/>	

Security Policy List														
Name	Source Zone	Destination Z...	Source Addr...	Destination Addr...	User	Service	Application	Schedule	Action	Content Security	Hits	Enable	Edit	
from test	any	any	test	any	any	any	any	any	Permit		6	Reset	<input checked="" type="checkbox"/>	
to test	any	any	any	test	any	any	any	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
ssl	any	any	any	any	any	SSL	any	any	Permit		1.1*10 <sup>5</sup>	Reset	<input checked="" type="checkbox"/>	
ssh	any	any	any	any	any	ssh	any	any	Permit		1650	Reset	<input checked="" type="checkbox"/>	
sip	any	any	any	any	any	sip	any	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
TESTSKYPE	any	any	any	any	any	any	Instant_Messaging	any	Permit		447	Reset	<input checked="" type="checkbox"/>	
TESTP2P	any	any	any	any	any	any	Game	any	Permit		0	Reset	<input checked="" type="checkbox"/>	
TESTIDS	any	any	any	any	any	any	FileShare_P2P	any	Permit		25327	Reset	<input checked="" type="checkbox"/>	
default	any	any	any	any	any	any	any	any	Deny		0	Reset	<input type="checkbox"/>	

# Application Control

- Le Applicazioni sono categorizzate ed utilizzabili per la creazione di Policy
- **Abilitate e monitorate tutte le applicazioni**
- **Utilizzata una regola in permit per SSL verso il CNAF (falsi positivi in anomaly detection per traffico di analisi)**
- **Utilizzata una regola in test per la rilevazione di traffico P2P**

Security Policy List										
+ Add ▾ × Delete 📄 Copy ↕ Move 📄 Insert 📄 Export ▾ 📄 Reset All Statistics 📄 Enable 📄 Disable 📄 Customize 🔄 Refresh <input type="text" value="Enter a policy name."/>										
<input type="checkbox"/>	Name	Source Zone	Destination...	Source Add...	Destination Add...	User	Service	Application	Schedule	Action
<input type="checkbox"/>	from test	any	any	📄 test	any	any	any	any	any	Permit
<input type="checkbox"/>	to test	any	any	any	📄 test	any	any	any	any	Permit
<input type="checkbox"/>	ssl	any	any	any	any	any	any	📄 SSL	any	Permit

# Application Control

Huawei USG6650 Current User: admin Commit Save Help About Change Password Logout

Dashboard Monitor Policy Object Network System Virtual System Carr

- Address
- Address Group
- Domain Group
- Region
- Service
- Application
- Application Group
- User
- SMS Sending
- Authentication Server
- IP Address Pool
- Schedule
- URL Category
- Signature
- Security Profiles
- Health Check

### Application

[Add](#) [Delete](#) [copy](#) [Import](#) [Export](#)

[Refresh](#)  User-defined Only | 
[Search](#) |  Filter [Clear Search Condition](#)

Category	Subcategory	Label	Data Transmission Model	Risk Level
<input type="checkbox"/> General	<input type="checkbox"/> Other	<input type="checkbox"/> Mobile-Supported	<input type="checkbox"/> unassigned	<input type="checkbox"/> <span style="color: green;">↑</span>
<input type="checkbox"/> Network	<input type="checkbox"/> General_TCP	<input type="checkbox"/> Cloud-Based	<input type="checkbox"/> client-server	<input type="checkbox"/> <span style="color: blue;">↑</span>
<input type="checkbox"/> General_Internet	<input type="checkbox"/> General_UDP	<input type="checkbox"/> Database	<input type="checkbox"/> browser-based	<input type="checkbox"/> <span style="color: orange;">↑</span>
<input type="checkbox"/> Entertainment	<input type="checkbox"/> CloudService	<input type="checkbox"/> Business-Applications	<input type="checkbox"/> networking	<input type="checkbox"/> <span style="color: orange;">↓</span>
<input type="checkbox"/> Business_Systems	<input type="checkbox"/> News_Group	<input type="checkbox"/> Encrypted-Communications	<input type="checkbox"/> peer-to-peer	<input type="checkbox"/> <span style="color: red;">↓</span>

User-defined applications have changed. [Commit](#) the change to make it take effect.

Name	Category	Subcategory	Label	Data Transmission Model	Risk Level	Edit
BT	General_Internet	FileShare_P2P	Productivity-Loss Data-Loss Bandwidth-Consuming Evasive Tunneling P2P-Based Exploitable	peer-to-peer	<span style="color: orange;">↓</span>	<a href="#">Edit</a>
PPLive	Entertainment	PeerCasting	Productivity-Loss Data-Loss Bandwidth-Consuming Evasive Tunneling Exploitable	peer-to-peer	<span style="color: red;">↓</span>	<a href="#">Edit</a>
Thunder	General_Internet	FileShare_P2P	Malware-Vehicle Productivity-Loss Data-Loss Bandwidth-Consuming Evasive Tunneling P2P-Based Exploitable	peer-to-peer	<span style="color: red;">↓</span>	<a href="#">Edit</a>
FTP	Network	Infrastructure	Malware-Vehicle Data-Loss Evasive Exploitable	networking	<span style="color: orange;">↓</span>	<a href="#">Edit</a>
FTPS	Network	Infrastructure	Malware-Vehicle Data-Loss Evasive Exploitable	networking	<span style="color: orange;">↓</span>	<a href="#">Edit</a>

[CLI Console](#)

Copyright © Huawei Technologies Co., Ltd. 2013-2015. All rights reserved.

## Intrusion Prevention

- Le signature di default (5096) non sono editabili ma e' possibile aggiungerne di personalizzate
- Predefinito comportamento di default Alert o Block per ciascuna signature ma modificabile per ogni policy
- Block per Critical e High severity
- Alert per Medium e Low
- Il block di SIPVicious avviene direttamente come anomaly detection relativa alla scansione (IP Sweep) e non come regola di IPS
- Rilevate durante il mese varie possibili intrusioni

# Intrusion Prevention

**Intrusion Prevention Signature List**

[+](#) [+](#) Associated Signature [✕](#) Delete [🔄](#) Refresh All  [🔍](#) Search [🔍](#) Advanced Search [🗑️](#) Clear Search Condition

User-defined Signature have changed [?](#), [Commit](#) the change to make it take effect.

<input type="checkbox"/>	ID	Name	Vendo...	CVE N...	CNNV...	Target	Severity	OS	Application	Protocol	Category	Action	Reference C...	Status	Edit
<input type="checkbox"/>	45990	Trojan: Win32.Powp.pyv				All	Medium	Windows	All	HTTP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46120	Trojan: Win32.Ransom...				All	Medium	Windows	All	HTTP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46150	Trojan: Win32.Genome				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46160	Trojan: Win32.Kryptik				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46470	Trojan: Nuclear_Rat				Client	Medium	Windows	All	TCP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46510	Remote Control Tool: ZX...				All	Medium	Windows	All	TCP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46511	Remote Control Tool: ZX...				All	Medium	Windows	All	HTTP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46512	Remote Control Tool: ZX...				All	Medium	Windows	All	UDP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46580	ProRat: Traffic Detected				All	Medium	Windows	All	TCP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46750	Backdoor: Gh0st				All	Medium	Windows	All	TCP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	46970	Trojan: Win32.Download...				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	47190	Trojan: Win32.VB.NLJ				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	48080	Trojan: Win32.Fujack.aa				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	48550	Trojan: Win32.Viking.j				All	Medium	Windows	All	HTTP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	49280	AladinDDOS Traffic Det...				All	Medium	Windows	All	TCP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	49290	Z-Admin1.04 Traffic Det...				All	Medium	Windows	All	TCP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	49300	Remote_Server_Shell T...				All	Medium	Windows	All	TCP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	49340	Backdoor Boer Traffic D...				All	Medium	Windows	All	TCP	Trojan	Alert		<input checked="" type="checkbox"/>	<a href="#">🔗</a>
<input type="checkbox"/>	49360	Mania: Rat Traffic: Dnter...				All	Medium	Windows	All	TCP	Trojan	Block		<input checked="" type="checkbox"/>	<a href="#">🔗</a>

<< Page 1 of 102 >> Records per page 50 Displaying 1 - 50 of 5081

# Intrusion Prevention

Intrusion Prevention Profile List

[Add](#) [Delete](#) [Copy](#) [View](#) [Refresh](#)

Profile have changed (?). [Commit this](#)

Name    [Attach](#)

- testipp
- strict
- web\_server
- file\_server
- dns\_server
- mail\_server
- inside\_firewall
- dmz
- outside\_firewall
- ids
- default

**Pre-defined Profile Detail**    ? x

Name:

Description:

**Signature Filter List**

[View Signature Filter Result](#)

<input checked="" type="checkbox"/> Name	Target	Severity	OS	Protocol	Category	Action
<input checked="" type="checkbox"/> default	All	Low, Medium, High	Unix-like,...	All	All	Alert

**View Signature Filter Result**    ? x

[Refresh](#)    Enter an ID, name, vendor vulnerability ID, or CVE number, or CNNVD number.    [Search](#) | [Advanced Search](#)    [Clear Search Condition](#)

<input type="checkbox"/> ID	Name	Vend...	CVE ...	CNN...	Target	Severity	OS	Applicati...	Protocol	Action
<input type="checkbox"/> 46150	Trojan: Win32.Geno...				All	Medium	Windows	All	HTTP	Alert(Ove...
<input type="checkbox"/> 46160	Trojan: Win32.Kryptik				All	Medium	Windows	All	HTTP	Alert(Ove...
<input type="checkbox"/> 46470	Trojan: Nuclear_Rat				Client	Medium	Windows	All	TCP	Alert
<input type="checkbox"/> 46510	Remote Control Too...				All	Medium	Windows	All	TCP	Alert
<input type="checkbox"/> 46511	Remote Control Too...				All	Medium	Windows	All	HTTP	Alert
<input type="checkbox"/> 46512	Remote Control Too...				All	Medium	Windows	All	UDP	Alert
<input type="checkbox"/> 46580	ProRat Traffic Detec...				All	Medium	Windows	All	TCP	Alert(Ove...

Page 1 of 102    Records per page 50    Displaying 1 - 50 of 5080

[Close](#)

Displaying 1 - 11 of 11

[CLI Console](#)

## AntiVirus

- Signature predefinite
- Detect Virus impostato di default su Deny, nel test impostato su Alert
- Controllo su tutti i protocolli (previsti)
- Non abbiamo rilevato alcun virus escluse le prove di Eicar (Il traffico from/to Mailserver era escluso 😊)

# AntiVirus

**Antivirus Profile List**

[+](#) Add 
 [x](#) Delete 
 [c](#) Copy 
 [r](#) Refresh 
 
[🔍](#) Search 
 [🗑️](#) Clear Search Condition

Profile have changed [?](#), [Commit](#) the change to make it take effect.

<input type="checkbox"/>	Name	Attack Evidence C...	Interworking Det...	Protocol	Upload	Download	Action	Reference Counts	Edit
<input type="checkbox"/>	testids			HTTP	✓	✓	Alert	0 <a href="#">View</a>	<a href="#">📄</a>
				FTP	✓	✓	Alert		
				SMTP	✓		Alert		
				POP3		✓	Alert		
				IMAP	✓	✓	Alert		
				NFS	✓	✓	Alert		
				SMB	✓	✓	Alert		
<input type="checkbox"/>	default			HTTP	✓	✓	Block	4 <a href="#">View</a>	<a href="#">📄</a>
				FTP	✓	✓	Block		
				SMTP	✓		Alert		
				POP3		✓	Alert		
				IMAP	✓	✓	Alert		
				NFS	✓	✓	Alert		
				SMB	✓	✓	Block		

[⏪](#) [⏩](#) Page  of  [⏪](#) [⏩](#) Records per page  [⏴](#) [⏵](#)
Displaying 1 - 2 of 2

[CLI Console](#)

# AntiVirus

### Antivirus Profile List

**Modify Antivirus Profile**

Name: testids

Description:

Attack Evidence Collection  Enable  
After detecting a virus, the system obtains the packets containing the virus. You can view the packet payload in the corresponding log.

Interworking Detection  Enable  
If the interworking detection function is enabled, antivirus detection performance will deteriorate. This function takes effect only when both antivirus and APT profiles are referenced in security policy rules.

Protocol	File Transfer Protocol			Mail Transfer Protocol		File Sharing Protocol	
	HTTP	FTP	SMTP	POP3	IMAP	NFS	SMB
Upload	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Download	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Action	Alert						

**Application Exception List**

Select an application

Name      Action

**Virus Exception List**

Enter a virus ID

ID      Name

### HTTP Application

Name	Action
Aimini	Alert
Flash	Alert
Netease_Webmail	Alert
Yahoo_WebMail	Alert
126disk	Alert
115Sync	Alert
115net_disk	Alert
3ADisk	Alert
360softmanager	Alert
360CloudWeb	Alert
360Cloud	Alert
139Maildisk	Alert
139Disk	Alert
4000-2	Alert

Displaying 28

OK Cancel

Page 1 of 1    Records per page 50    Displaying 1 - 2 of 2

CLI Console

## URL Filtering

- Abilitato solo per alcuni host
- Permette di categorizzare il traffico in funzione delle URL ed un DB che si aggiorna in automatico
- Stabilisce livelli di pericolosità
- Si applica a livello di policy
- In aggiunta alle categorie standard se ne possono creare nuove applicando Whitelist e Blacklist x policy

## IP reputation

- The IP reputation function filters packets based on the IP addresses recorded in the IP reputation database. The current IP reputation database is a set of zombie hosts' IP addresses, and the FW filters out the packets sent by these zombie hosts. The IP reputation database supports automatic update.
- After the IP reputation function is enabled, the FW matches the source IP address of a packet against the IP reputation database. If a match is found, the FW discards the packet. In addition, exception IP addresses can be configured on the FW. If an exception IP address is configured on the FW, the FW does not discard the packets sent from the exception IP address.
- **IL DB BASE NON E' VISIBILE**

# URL Filtering

**Modify URL Filtering Profile** ? x

Name:

Description:

Action Mode:  Strict  Loose

Default Action:

Malicious URL Detection:  Enable

Type	Whitelist
URL ?	The whitelist enjoys a higher priority than the blacklist.
HOST ?	The whitelist enjoys a higher priority than the blacklist.

URL Filtering Level

High Restrict access to such websites as adult, illegal ac

**Modify URL Filtering Profile** ? x

URL Filtering Level

High Restrict access to such websites as adult, illegal activity, social networking, and video sharing websites.

Medium Restrict access to such websites as adult and illegal activity websites.

Low Restrict access to such websites as pornography websites.

User-defined

Name	<input type="radio"/> Allow	<input type="radio"/> Alert	<input type="radio"/> Block	Re-marked DSCP
▶ User-defined Category...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ P2P	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Download	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Humanity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Sports	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Social Focus	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Military	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Social Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Lottery	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Recreation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
▶ Religion/Supernatural	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE

OK Cancel

## Syslog

- Esistono tre tipologie di remote syslog e vari livelli di informazione
  - SysLog, SessionLog e ServiceLog
- Esiste anche un formato proprietario binario per la piattaforma Huawei
- Dovrebbero esistere plugin già realizzati per Splunk e Q-radar (altri chissà') ma non abbiamo avuto il tempo di testarli

## Real Time Monitor

- Permette di mantenere una certa quantita' di log nella memoria di massa del dispositivo
- Di default ha una FlashCard relativamente piccola
- Puo' essere equipaggiato con una coppia di SSD in Raid di capacita' 600GB
- Quando termina lo spazio (secondo queue a profondita' variabili) sovrascrive i dati piu' antichi
- I log abilitati sul traffico (i piu' verbosi) ad un rate di 100Mb/s hanno una persistenza di pochi minuti

# Monitor integrato

Huawei USG6650

Dashboard Monitor Policy Object Network System

Current User: admin Commit Save Help About Change Password Logout

Virtual System Garr

Log

- Traffic Log
- Threat Log**
- URL Log
- Operation Log
- System Log
- User Activity Log
- Policy Matching Log
- Sandbox Detection Log
- Report
  - Traffic Report
  - Threat Report
  - URL Report
  - Policy Matching Report
- Traffic Map
- Threat Map
- Top N Session
- Session Table
- Diagnosis Center
- Security Posture Awareness
- Asset Management

Threat Log List

Refresh Advanced Search Clear Search Condition

View	Time	Threat Type	Threat ID	Threat Name	Attacker	Victim	Source Address...	Destination Address...	Application	Protocol	Action	Security Policy
	DST 2017/05/24 22:15:57	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.154	216.218	131.154	216.218.215	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 22:15:57	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.154	198.41.0.4	131.154	198.41.0.4	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 22:15:46	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.154	198.41.0	131.154	198.41.0.4	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 22:15:46	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.154.1	216.218	131.154.1	216.218.215	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 21:51:45	Intrusion	324680	Apache Commons Collections U...	5.188.10.1	131.154	5.188.10.1	131.154.10	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:51:35	Intrusion	324680	Apache Commons Collections U...	5.188.10.1	131.154	5.188.10.1	131.154.10	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:40:57	Intrusion	2600	Apache Tomcat Servlet Engine D...	66.249.66	131.154	66.249.66	131.154.12	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:40:57	Intrusion	2000019	Directory Traversal Attempt - Fo...	66.249.66	131.154	66.249.66	131.154.11	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:38:25	Attack	24	Smurf attack	46.234	193.204	46.234	193.204		ICMP	Alert	
	DST 2017/05/24 21:37:56	Intrusion	260280	Adobe Acrobat and Reader Rem...	131.154	66.249.66	131.154	66.249.66	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:29:25	Intrusion	330680	GNU C Library getaddrinfo Buffer...	58.65.2	131.154	58.65.2	131.154	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 21:23:25	Attack	24	Smurf attack	46.234	193.204	46.234	193.204		ICMP	Alert	
	DST 2017/05/24 20:45:46	Intrusion	330680	GNU C Library getaddrinfo Buffer...	211.29.1	131.154	211.29	131.154	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:08	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.250	131.154	113.250	131.154	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:07	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.250.2	131.154	113.250	131.154	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:07	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.250	131.154	113.250	131.154	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:06	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.250	131.154	113.250	131.154	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:04	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.250	131.154	113.250	131.154	HTTP	TCP	Alert	PERMITALLIDS

Page 1 of 9 | Records per page 100 | Displaying 1 - 100 of 806

CLI Console

Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

# Monitor integrato

## System Log List

 Refresh  Advanced Search  Clear Search Condition

Note: The page display intraday log as default.

Time	Log Type	Log Severity	Description	Virtual System
DST 2017/05/24 22:31:58	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:31:53	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:31:49	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:30:23	Running	Informational	Last message repeated 1 times.(InfoID=4255911936, ModuleName=POLICY, InfoAlias=POLICYPERMIT)	public
DST 2017/05/24 22:29:30	Running	Warning	Failed to login through SNMP. (Ip=131.154.11.87, Times=1, Reason=the version was incorrect, VPN= )	public
DST 2017/05/24 22:25:23	Running	Informational	Last message repeated 1 times.(InfoID=4255911936, ModuleName=POLICY, InfoAlias=POLICYPERMIT)	public
DST 2017/05/24 22:24:15	Running	Informational	Last message repeated 1 times.(InfoID=4255911936, ModuleName=POLICY, InfoAlias=POLICYPERMIT)	public
DST 2017/05/24 22:23:33	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:21:16	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:20:56	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:20:46	Running	Debug	Last message repeated 1 times.(InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public
DST 2017/05/24 22:19:30	Running	Warning	Failed to login through SNMP. (Ip=131.154.11.87, Times=6, Reason=the version was incorrect, VPN= )	public
DST 2017/05/24 22:17:38	Running	Informational	Last message repeated 3 times.(InfoID=4255911936, ModuleName=POLICY, InfoAlias=POLICYPERMIT)	public
DST 2017/05/24 22:17:25	Login	Informational	User admin(IP:131.154.11.87 ID:28) login succeeded	public
DST 2017/05/24 22:17:24	Alarm	Warning	OID 1.3.6.1.4.1.2011.6.122.62.2.1 User login succeed.(userName = admin, loginIP = 131.154.11.87, loginTime = 2017/05/24 22:17:24)	public
DST 2017/05/24 22:17:24	Running	Notification	[USER_INFO_AUTHENTICATION]DEVICEMAC:18-de-3d-31-30-30-30,DEVICENAME:FIREWALL,USER:admin,MAC:ff-ff-ff-ff-ff-ff,IP:131.154.11.87	public
DST 2017/05/24 22:15:57	Alarm	Warning	OID 1.3.6.1.4.1.2011.6.122.43.1.2.8 An intrusion was detected.( SrcIp=131.154.11.87, DstIp=216.213.14.1, SrcPort=50911, DstPort=50911)	public
DST 2017/05/24 22:15:57	Alarm	Warning	OID 1.3.6.1.4.1.2011.6.122.43.1.2.8 An intrusion was detected.( SrcIp=131.154.11.87, DstIp=196.16.16.1, SrcPort=56351, DstPort=56351)	public
DST 2017/05/24 22:15:56	Alarm	Warning	OID 1.3.6.1.4.1.2011.6.122.62.2.3 User logout succeed.(userName = admin, logoutIP = 131.154.11.87, logoutTime = 2017/05/24 22:15:56)	public

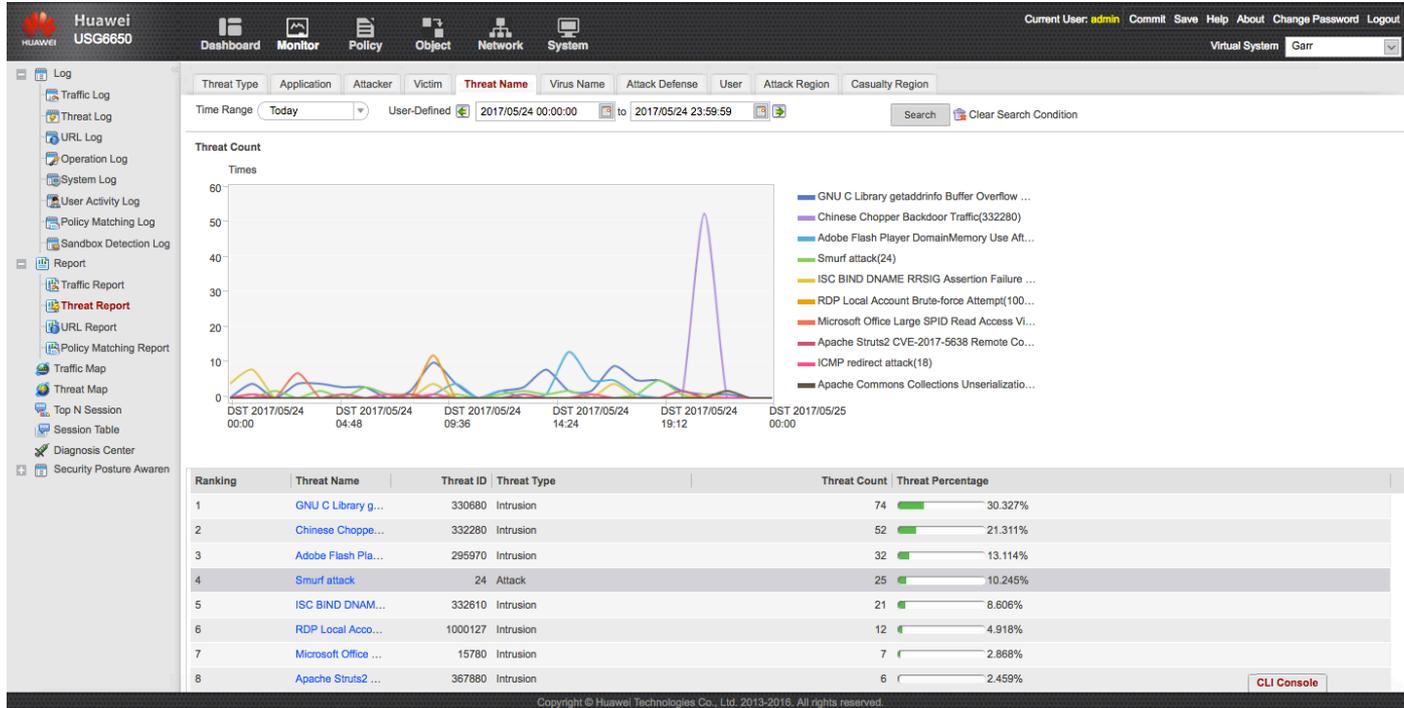
Page 1 of 3 Records per page 50

Displaying 1 - 50 of 118

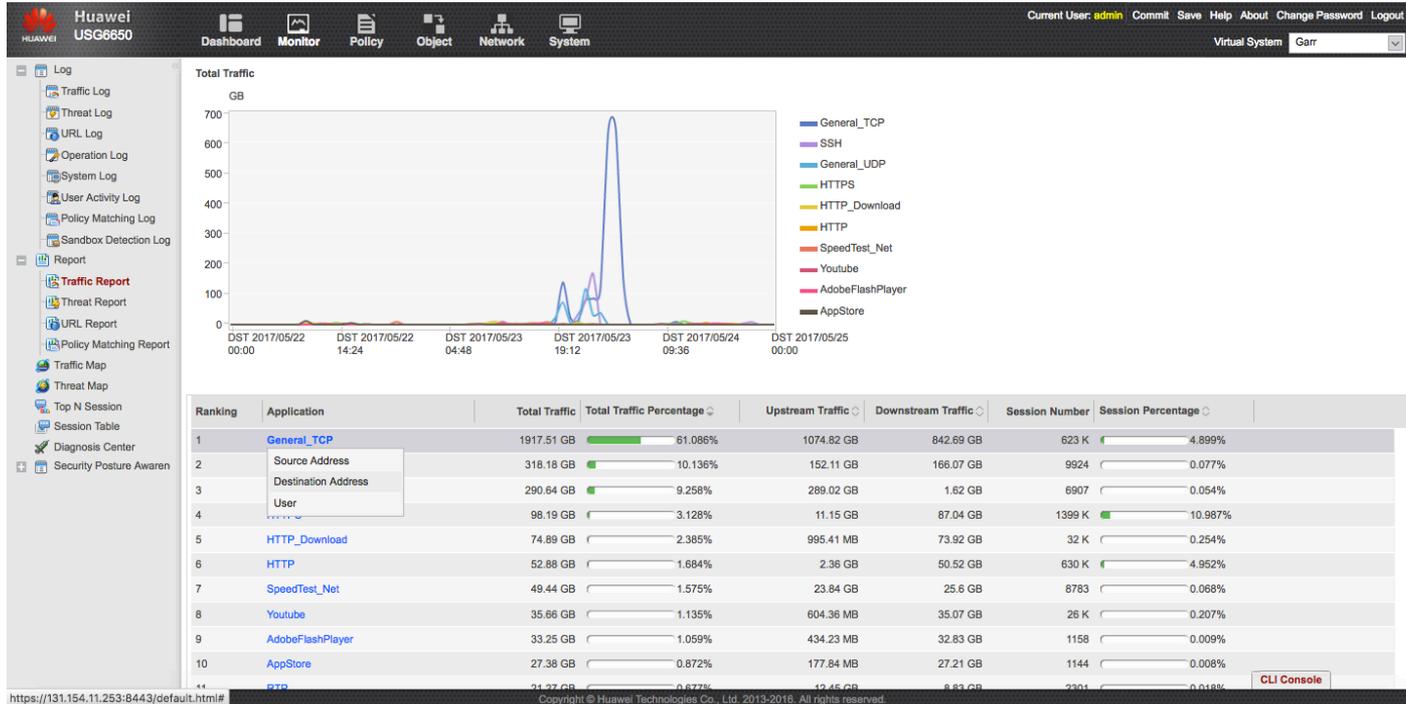
## Report

- I report sono raccolte statistiche delle informazioni raggruppate per tipologia
- Hanno una persistenza piu' alta e sono visibili a step di 1 giorno 3 giorni o un mese
- Sono preimpostati per Traffic, Threat, URL e Policy matching
- Sono lo strumento probabilmente piu' utile sia per le operation che per la remediation
- Ne i monitor integrati ne i report sono strumenti adeguati x la Forensic

# Threat Report



# Traffic Report



# Session Table

Huawei USG6650 Current User: admin Commit Save Help About Change Password Logout

Dashboard Monitor Policy Object Network System Virtual System Garr

Log

- Traffic Log
- Threat Log
- URL Log
- Operation Log
- System Log
- User Activity Log
- Policy Matching Log
- Sandbox Detection Log

Report

- Traffic Report
- Threat Report
- URL Report
- Policy Matching Report
- Traffic Map
- Threat Map
- Top N Session
- Session Table**
- Diagnosis Center
- Security Posture Awareness
- Asset Management

**Session Table**

Refresh Advanced Search Clear Search Condition

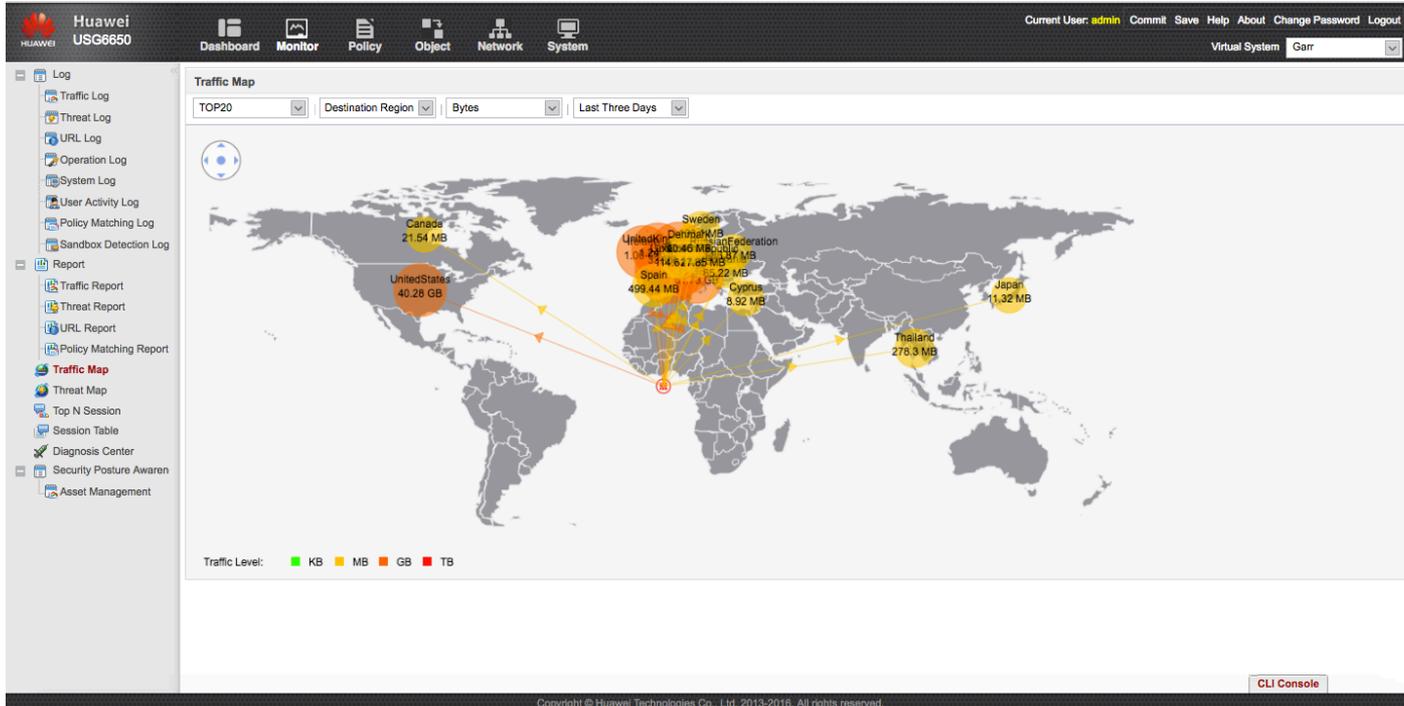
Details	Creation Time	Time Left	Protocol	Application	Source Address	Destination Address	Source Port	Destination Port	NAT Source P...	NAT Destination Port	Outbound Interfa...	Next Hop
	2017/5/24 22:43:2	00:00:19	dns	DNS	62.112.1	193.204.1	43526	53			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:42:54	00:19:44	http	HTTP	131.154.1	62.67.16	54648	80			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:41:53	00:00:40	ntp	NTP	131.154.1	193.204.2	123	123			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 13:53:24	00:09:56	https	Skype_IM	131.154.1	40.77.22	49920	443			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:42:44	00:01:31	udp	SSDP	115.41.1	131.154.1	33458	1900			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:41:52	00:00:39	udp	google	131.154.1	216.58.2	61257	443			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 9:35:39	00:19:26	tcp	SSL	131.154.1	37.59.37	51256	22067			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:42:3	00:19:03	http				54081	80			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:43:12	00:00:04	telnet		220.134.1	131.154.1	21021	23			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:41:41	00:00:28	udp		131.154.1	65.55.223	20819	40026			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:42:47	00:01:34	udp	Skype_IM	131.154.1	157.55.23	24628	40017			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 21:26:32	00:08:49	https	Dropbox	131.154.1	162.125.1	52271	443			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:43:10	00:01:57	udp	Skype_IM	131.154.1	157.55.23	58128	40030			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:42:36	00:01:23	udp		140.105.1	131.154.10	7001	7000			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:43:12	00:00:10	http	HTTP	189.105.1	131.154.1	64754	80			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:42:42	00:01:29	udp	SSDP	61.80.2	193.204.1	57949	1900			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 22:41:30	00:00:17	udp		213.160.1	131.154.1	49483	5746			GE2/0/1(Garr)	0.0.0.0
	2017/5/24 0:4:53	00:19:25	tcp	GoogleTalk_IM	193.204.1	64.233.1	63733	5228			GE2/0/0(Garr)	0.0.0.0
	2017/5/24 22:42:45	00:00:02	dns	DNS	95.245.3	131.154.1	61118	53			GE2/0/1(Garr)	0.0.0.0

Page 1 of 25 Records per page 100 Displaying 1 - 100 of 2454

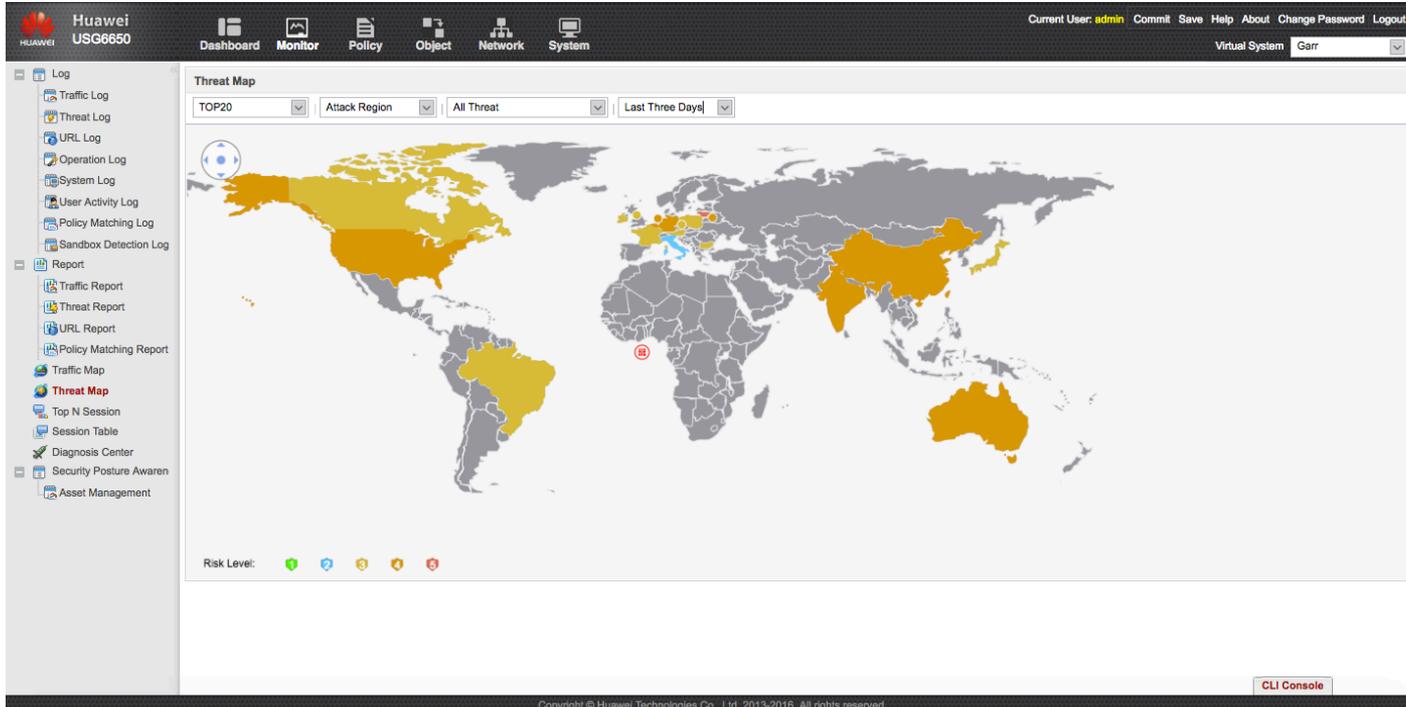
CLI Console

Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

# Traffic Map



# Threat Map



# Network configuration

Huawei USG6650

Current User: admin Commit Save Help About Change Password Logout

Virtual System public

Interface List

Refresh Interface Name Enter an interface name Search Clear Search Condition

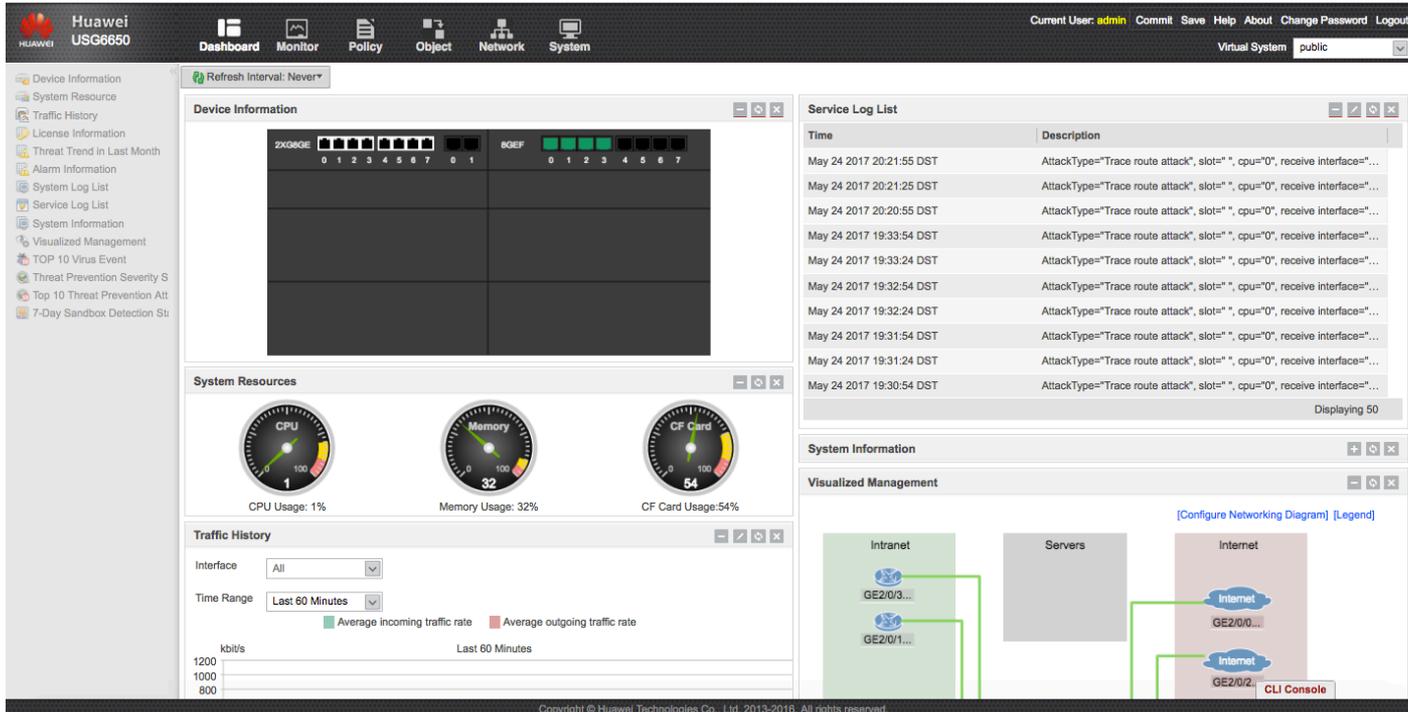
Interface Name	Zone	IP Address	Connection Type	VLAN	Mode	State			Enable	Edit
						Physical	IPv4	IPv6		
GE0/0/0(GE0/MGMT)	trust(public)	131.154.11.253	Static IP(IPv4) Static IP(IPv6)		Routing	↑	↑	↓	<input checked="" type="checkbox"/>	⚙
GE1/0/0	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/1	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/2	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/3	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/4	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/5	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/6	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE1/0/7	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
10GE1/0/8	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
10GE1/0/9	-NONE-(public)	---	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙
GE2/0/0(Garr)	untrust(Garr)		Access	2	Switching	↓	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/1(Garr)	trust(Garr)		Access	2	Switching	↑	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/2(Cnaf)	untrust(Cnaf)		Access	3	Switching	↑	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/3(Cnaf)	trust(Cnaf)		Access	3	Switching	↑	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/4	trust(vsys3)	131.154.11.254	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/5	untrust(vsys3)	192.168.10.74	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/6	untrust(vsys3)	193.206.128.74	Static IP(IPv4) Static IP(IPv6)		Routing	↓	↓	↓	<input checked="" type="checkbox"/>	⚙
GE2/0/7	-NONE-(public)	---	Static IP(IPv4)		Routing	↓	↓	↓	<input type="checkbox"/>	⚙

Page 1 of 1 Records per page 50 Displaying 1 - 23 of 23

CLI Console

Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

# Dashboard del contesto



The screenshot displays the Huawei USG6650 management interface. At the top, it shows the user 'admin' and system status 'Virtual System public'. The main dashboard is divided into several sections:

- Device Information:** Shows two rows of status indicators for '2XGEOE' and 'BOEF', each with 8 slots.
- System Resources:** Three gauges showing CPU Usage (1%), Memory Usage (32%), and CF Card Usage (54%).
- Service Log List:** A table of logs showing 'Trace route attack' events. The table has columns for 'Time' and 'Description'.
 

Time	Description
May 24 2017 20:21:55 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 20:21:25 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 20:20:55 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:33:54 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:33:24 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:32:54 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:32:24 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:31:54 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:31:24 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
May 24 2017 19:30:54 DST	AttackType="Trace route attack", slot=" ", cpu="0", receive interface="..."
- Traffic History:** A graph showing traffic rates over the last 60 minutes. The y-axis is labeled 'kbit/s' with values 800, 1000, and 1200. The x-axis is 'Last 60 Minutes'. It includes a legend for 'Average incoming traffic rate' and 'Average outgoing traffic rate'.
- Visualized Management:** A network diagram showing connections between 'Intranet', 'Servers', and 'Internet' blocks. Specific interfaces like GE2/0/3, GE2/0/1, GE2/0/0, and GE2/0/2 are labeled. A 'CLI Console' button is visible at the bottom right.

## Falsi positivi (forse) in IDS

- Abbiamo disabilitato alcune anomaly detection che Huawei chiama Single packet attack perche' troppo rumorose. Occorrera' verificare l'eventualita' di falsi positivi

Action  Alert  Discard

Configure Scanning Attack Defense

IP Sweep

Maximum Scanning Rate  <1-10000> pps

Blacklist Aging Time  <1-1000> minutes

Port Scanning

Maximum Scanning Rate  <1-10000> pps

Blacklist Aging Time  <1-1000> minutes

Configure Malformed Packet Attack Defense

IP Spoofing  IP Fragment  Teardrop

Smurf  Ping of Death  Fraggle

WinNuke  Land  TCP Flag

Configure Special Packet Control Attack Defense

Large ICMP Packet Control

Maximum Length  <28-65535> Bytes

ICMP Unreachable Packet Control  ICMP Redirect  Tracert

IP Source Routing Packet Control  IP Route Record Packet Control  IP Timestamp Packet Control

Apply

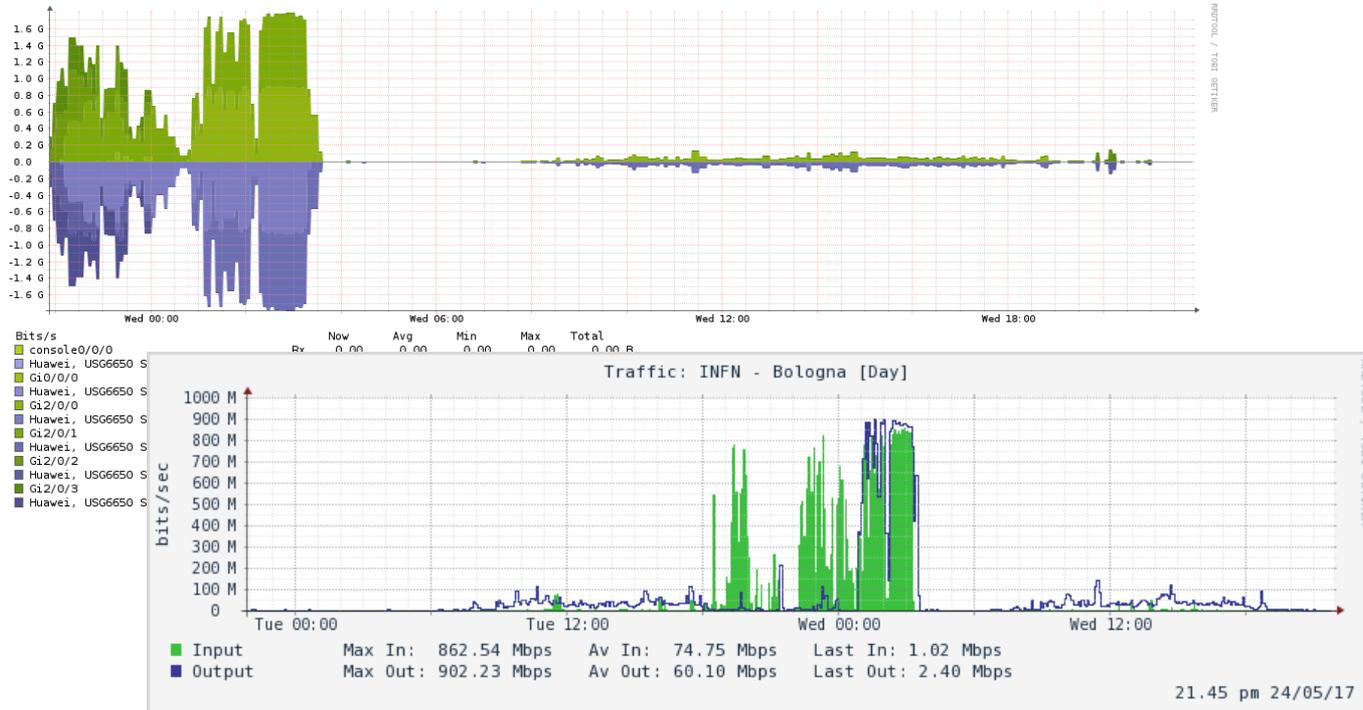
## Falsi positivi - non falsi

- Abbiamo dovuto creare delle policy di permit senza log e senza IDS per gli host audibo !!
- Durante una scansione attivata on demand hanno triggerato migliaia di eventi di IDS, anomaly etc.
- Abbiamo creato una regola ad-hoc per il traffico SSL based verso CNAF perche' triggerava falsi positivi su applicativi di esperimento (uso particolare di certificati X509)

## Casi reali

- Abbiamo rilevato un attacco brute force su alcuni RDP aperti in perimetro mitigato tramite blacklist e rimediato suggerendo agli amministratori la soluzione
- Abbiamo rilevato e inviato in blacklist varie scansioni dirette a SIP e web server
- Abbiamo in lista ancora parecchi threat da analizzare
- Il SOC diventa un lavoro full time anche per noi ?!

# Test banda



## Problemi riscontrati

- Nessuno, ma... troppo rumore (maledizione di Tutankhamon ?! Della concorrenza ?!) occorre altra statistica
- Nell'ultimo mese abbiamo avuto almeno 6 blocchi totali e parziali di rete, un rate mai accaduto !
  - Probabile problema a switch da tavolo che iniettava flood di mac address
  - Probabile problema di memory leak ai due core switch delle due sedi (Extreme x450) con reboot e 10min di down
  - Il firewall/router Juniper ha fatto reboot due volte durante la generazione del certificato https
  - Un probabile loop parziale non mitigato da STP ha provocato vari rallentamenti
  - Per terminare abbiamo bloccato venerdì' (!@?) con una policy invertita il traffico uscente ( User Experience ??? )

## Test ancora da effettuare

- Provare il contesto L3 che sostituisce la configurazione attuale
- Implementare in maniera "profonda" gli Application Control e AV
- Inserire tutte le regole di FIREWALL ACL esistenti
- Abilitare la funzione ANTISPAM per qualche prova
- VPN ??
- SIEM e Analisi dei LOG per difesa in profondita'

## Discussione e Q&A