HUAWEI USG6650

Primo mese nel mondo reale (L2 mode)

Cosa non sara'…

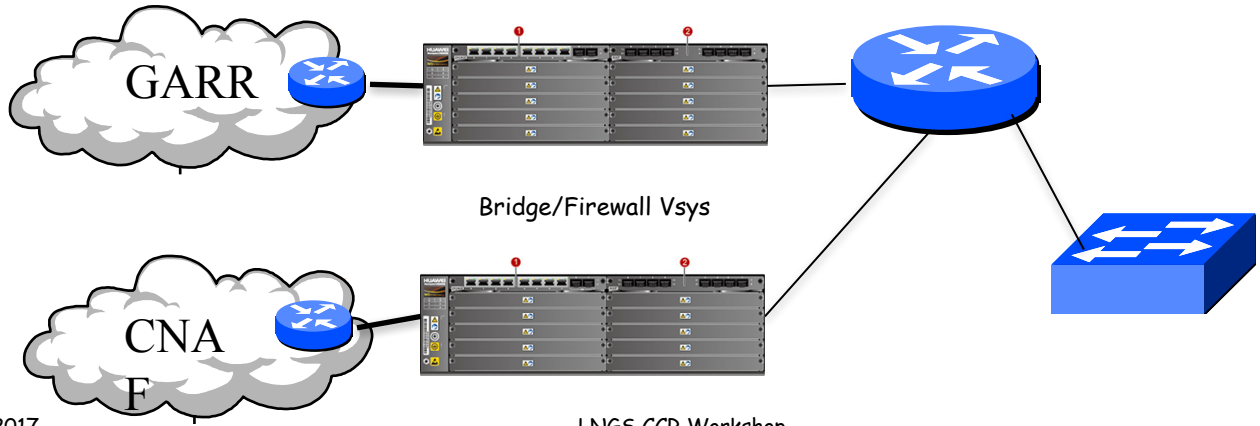
- Misure prestazionali basate su standard
- Confronto con altri device nelle stesse condizioni operative (gli ambienti sono diversi)
- Analisi approfondita delle funzionalita' del prodotto
- Analisi economica dei rapporti costi/benefici

Cosa cercherа' 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 funzionalita'
- 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



Funzionalita' 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

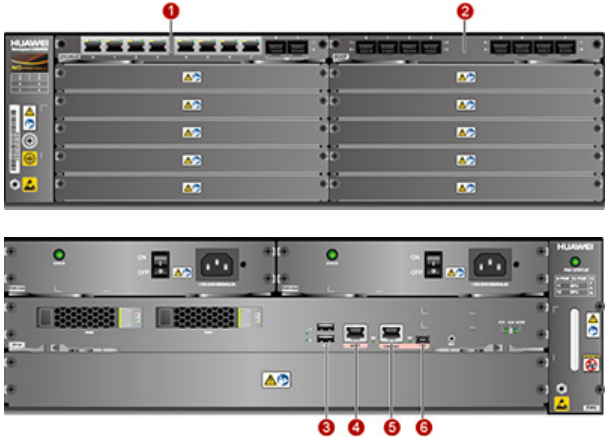


Table 1. Wide Service Interface Cards (WSICs) for USG6600 Series

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)

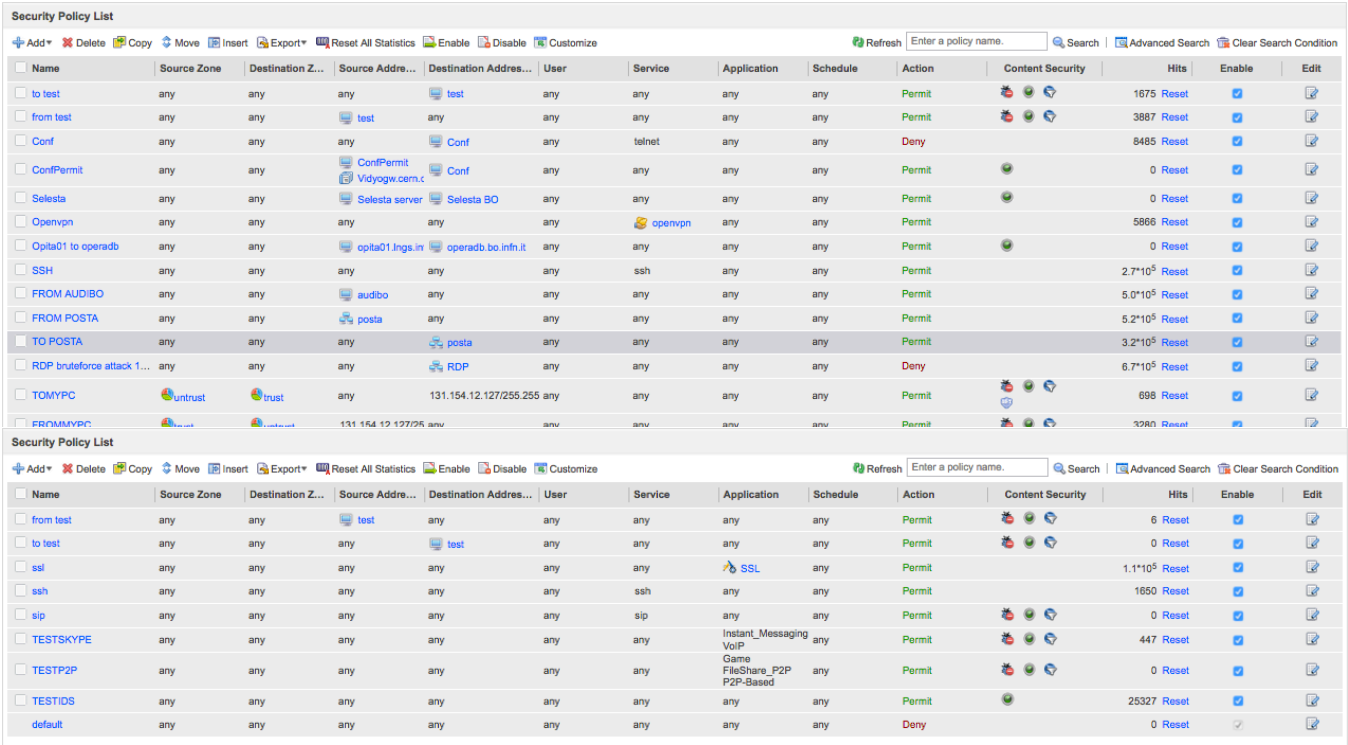
Caratteristiche USG6650

Model	USG6650	USG6660	USG6670	USG6680
IPv4 Firewall Throughput[1] (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[1] (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[2]	15 Gbit/s	18 Gbit/s	19 Gbit/s	20 Gbit/s
FW + SA* Throughput (Realworld)[3]	11 Gbit/s	12 Gbit/s	13 Gbit/s	18 Gbit/s
FW + SA + IPS Throughput[2]	8.8 Gbit/s	8.8 Gbit/s	8.8 Gbit/s	15 Gbit/s
FW + SA + Antivirus Throughput[2]	8 Gbit/s	8 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus + URL Throughput[2]	6 Gbit/s	7 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus Throughput (Realworld)[3]	5 Gbit/s	5.5 Gbit/s	6 Gbit/s	11 Gbit/s
Concurrent Sessions (HTTP1.1)[1]	8,000,000	10,000,000	10,000,000	12,000,000
New Sessions/Second (HTTP1.1)[1]	300,000	350,000	400,000	400,000
IPsec VPN Throughput[1] (AES-128 + SHA1, 1420-byte)	15 Gbit/s	18 Gbit/s	18 Gbit/s	18 Gbit/s

Implementazione

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

Implementazione



Security Policy List

Add | Delete | Copy | Move | Insert | Export | Reset All Statistics | Enable | Disable | Customize | Refresh | Enter a policy name. | Search | Advanced Search | Clear Search Condition

Name	Source Zone	Destination Z...	Source Addre...	Destination Addres...	User	Service	Application	Schedule	Action	Content Security	Hits	Enable	Edit
to test	any	any	any	test	any	any	any	any	Permit		1675 Reset		
from test	any	any	test	any	any	any	any	any	Permit		3887 Reset		
Conf	any	any	any	Conf	any	telnet	any	any	Deny		8485 Reset		
ConfPermit	any	any	ConfPermit Vidyogw.cern.c	Conf	any	any	any	any	Permit		0 Reset		
Selesta	any	any	Selesta server	Selesta BO	any	any	any	any	Permit		0 Reset		
Openvpn	any	any	any	any	any	openvpn	any	any	Permit		5866 Reset		
Opita01 to operadb	any	any	opita01.lngs.in	operadb.bo.infn.it	any	any	any	any	Permit		0 Reset		
SSH	any	any	any	any	any	ssh	any	any	Permit		$2.7*10^5$ Reset		
FROM AUDIBO	any	any	audibo	any	any	any	any	any	Permit		$5.0*10^5$ Reset		
FROM POSTA	any	any	posta	any	any	any	any	any	Permit		$5.2*10^5$ Reset		
TO POSTA	any	any	any	posta	any	any	any	any	Permit		$3.2*10^5$ Reset		
RDP bruteforce attack 1...	any	any	any	RDP	any	any	any	any	Deny		$6.7*10^5$ Reset		
TOMYPC	untrust	trust	any	131.154.12.127/255.255	any	any	any	any	Permit		698 Reset		
FROMMYPC			131.154.12.127/25	any	any	any	any	any	Permit		3280 Reset		

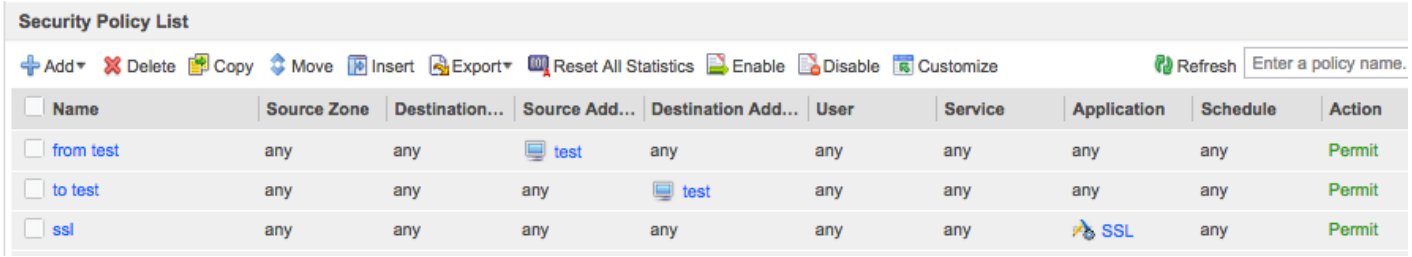
Security Policy List

Add | Delete | Copy | Move | Insert | Export | Reset All Statistics | Enable | Disable | Customize | Refresh | Enter a policy name. | Search | Advanced Search | Clear Search Condition

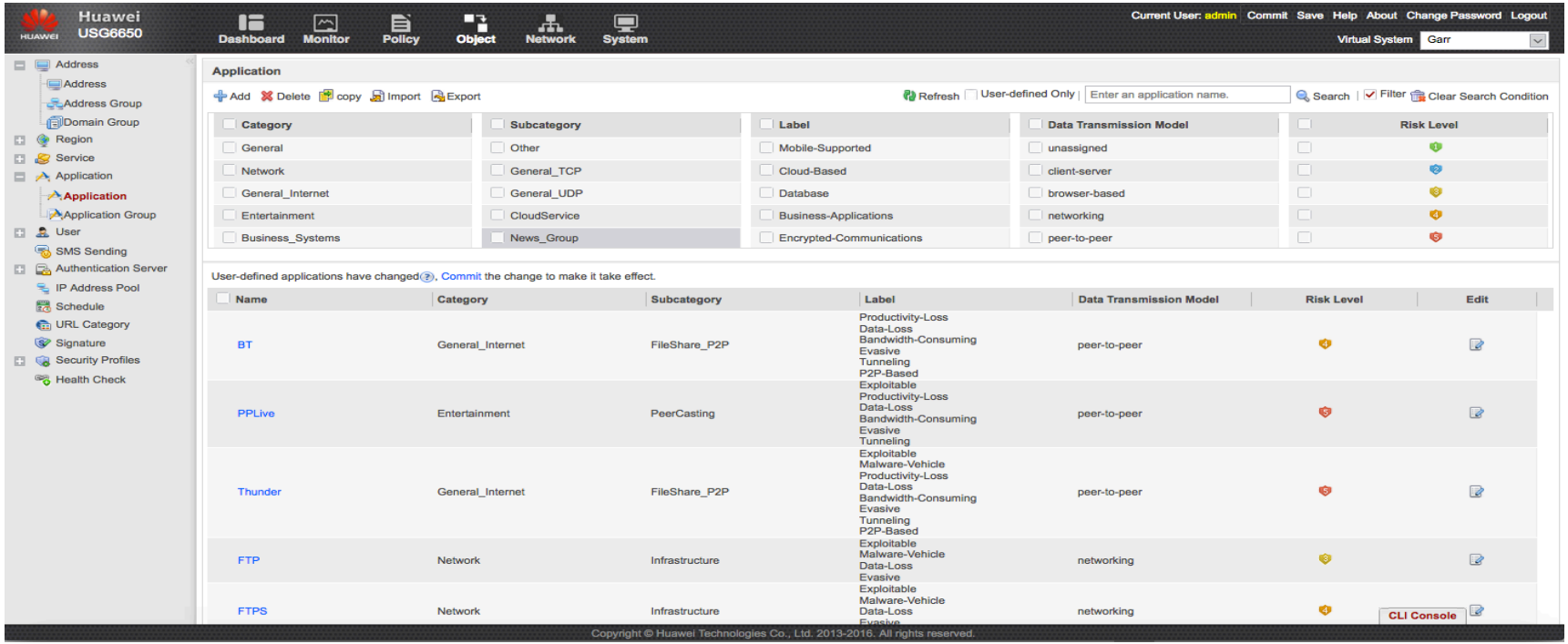
Name	Source Zone	Destination Z...	Source Addre...	Destination Addres...	User	Service	Application	Schedule	Action	Content Security	Hits	Enable	Edit
from test	any	any	test	any	any	any	any	any	Permit		6 Reset		
to test	any	any	any	test	any	any	any	any	Permit		0 Reset		
ssl	any	any	any	any	any	any	SSL	any	Permit		$1.1*10^5$ Reset		
ssh	any	any	any	any	any	ssh	any	any	Permit		1650 Reset		
sip	any	any	any	any	any	sip	any	any	Permit		0 Reset		
TESTSKYPE	any	any	any	any	any	any	Instant_Messaging VoIP	any	Permit		447 Reset		
TESTP2P	any	any	any	any	any	any	Game FileShare_P2P P2P-Based	any	Permit		0 Reset		
TESTIDS	any	any	any	any	any	any	any	any	Permit		25327 Reset		
default	any	any	any	any	any	any	any	any	Deny		0 Reset		

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



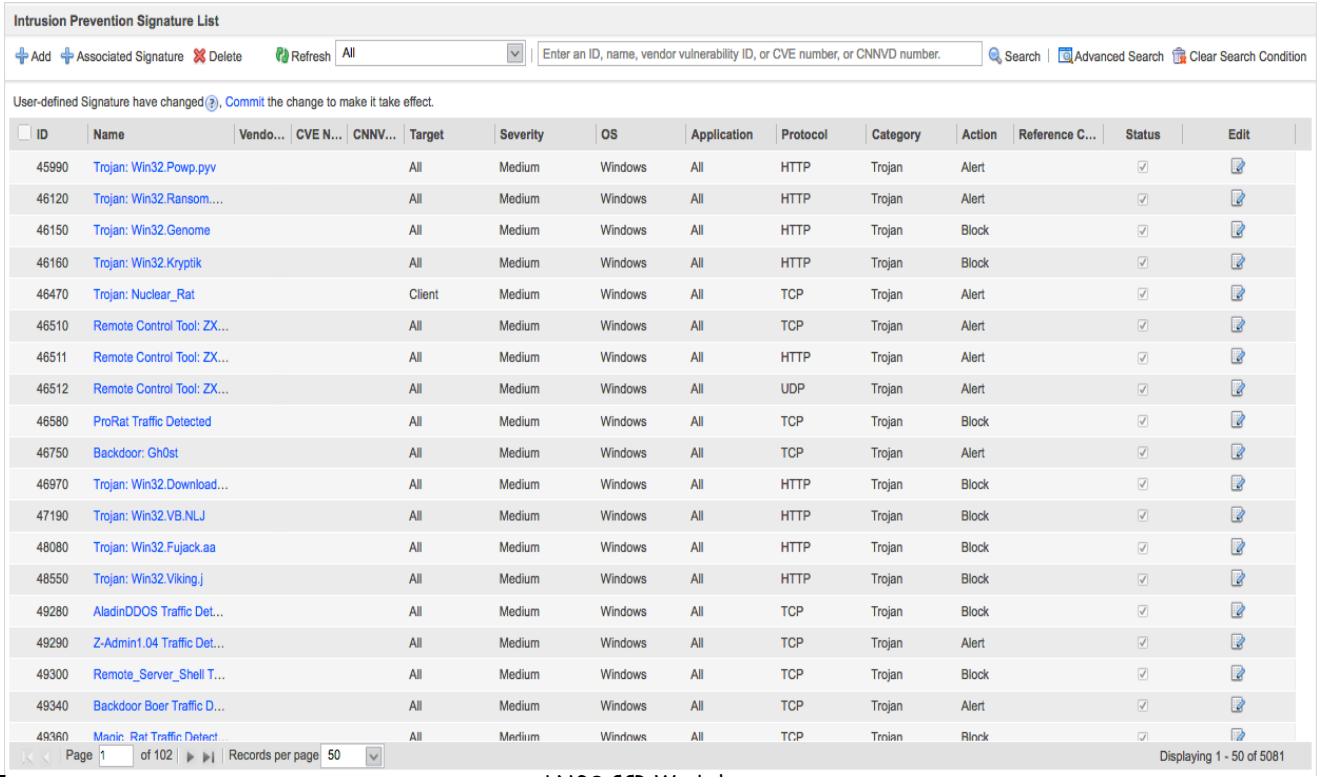
Application Control



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

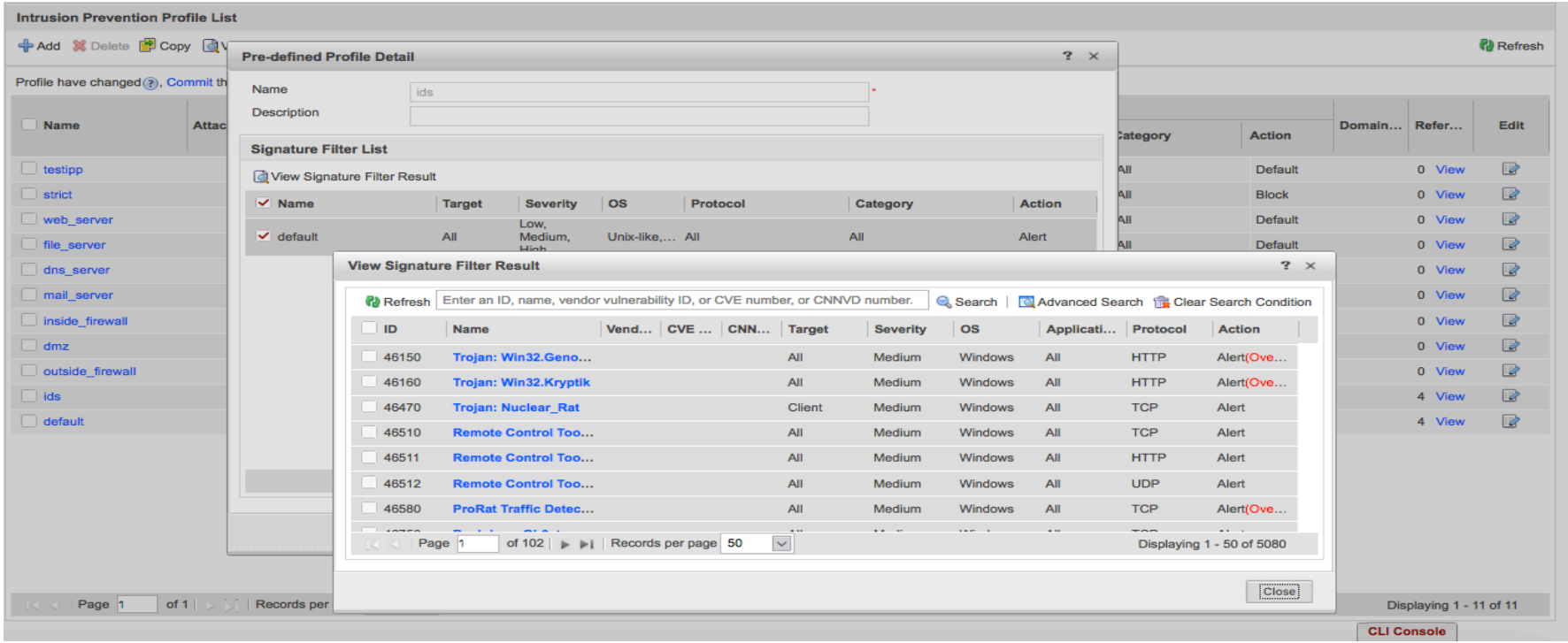
Add | Associated Signature | Delete | Refresh | All | Enter an ID, name, vendor vulnerability ID, or CVE number, or CNNVD number. | Search | Advanced Search | Clear Search Condition

User-defined Signature have changed, Commit the change to make it take effect.

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

Page 1 of 102 | Records per page 50 | Displaying 1 - 50 of 5081

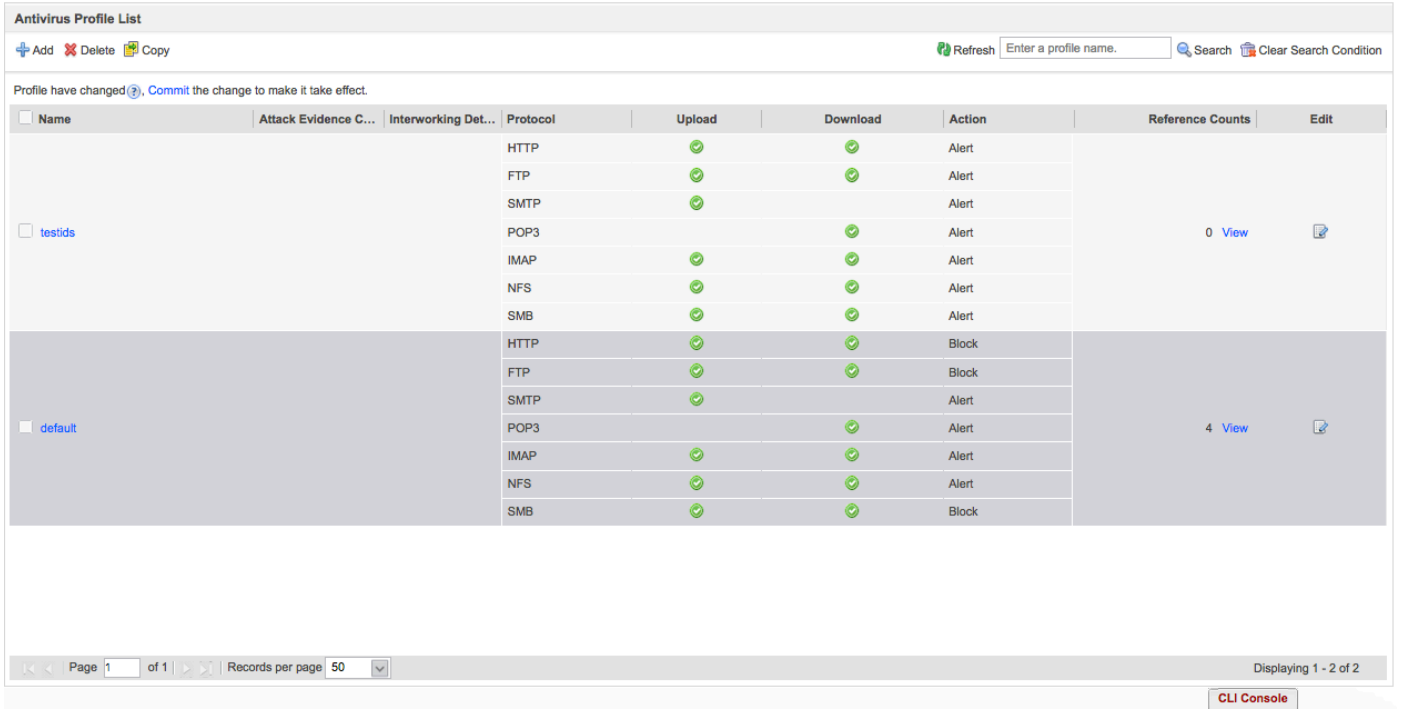
Intrusion Prevention



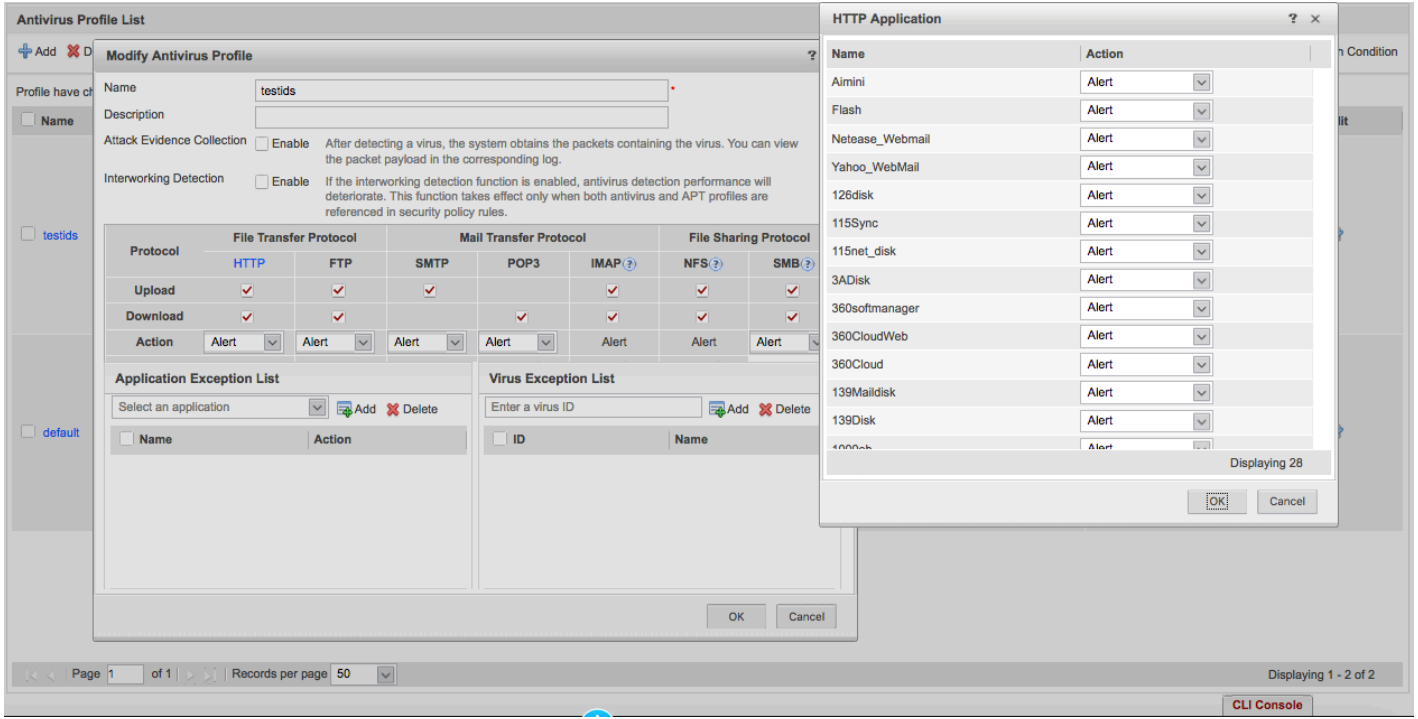
AntiVirus

- 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
Delete
Copy
Refresh
Enter a profile name.
Search
Clear Search Condition
Profile have changed, Commit the change to make it take effect.
Name
Attack Evidence C...
Interworking Det...
Protocol
Upload
Download
Action
Reference Counts
Edit
HTTP Alert
FTP Alert
SMTP Alert
testids POP3 Alert 0 View
IMAP Alert
NFS Alert
SMB Alert
HTTP Block
FTP Block
SMTP Alert
default POP3 Alert 4 View
IMAP Alert
NFS Alert
SMB Block
Page 1 of 1
Records per page 50
Displaying 1 - 2 of 2
CLI Console

AntiVirus


Antivirus Profile List
Add
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
Download
Action
Alert
Application Exception List
Select an application
Add
Delete
Name
Action
Virus Exception List
Enter a virus ID
ID
OK
Cancel
HTTP Application
Name
Action
Aimini
Flash
Netease_Webmail
Yahoo_WebMail
126disk
115Sync
115net_disk
3ADisk
360softmanager
360CloudWeb
360Cloud
139Maildisk
139Disk
Displaying 28
Page
of 1
Records per page
50
Displaying 1 - 2 of 2
CLI Console

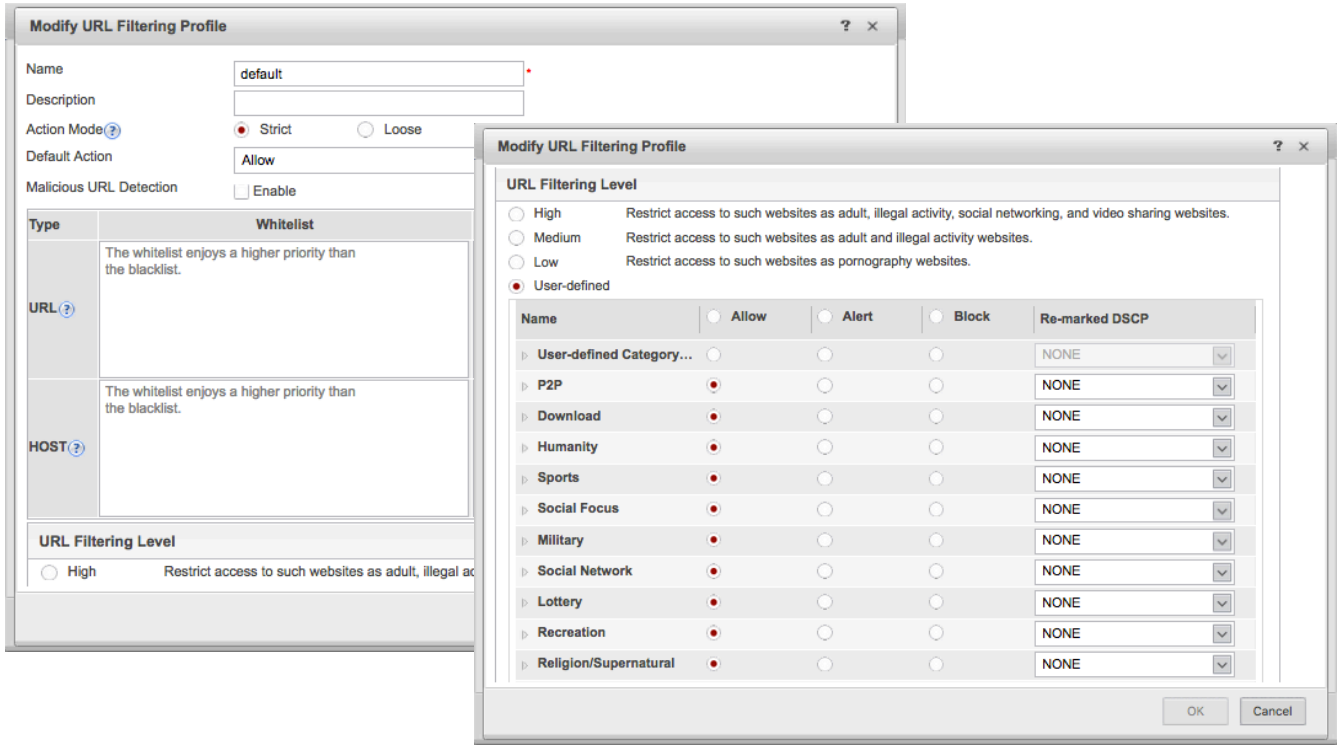
URL Filtering

- 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 pericolosita'
- 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



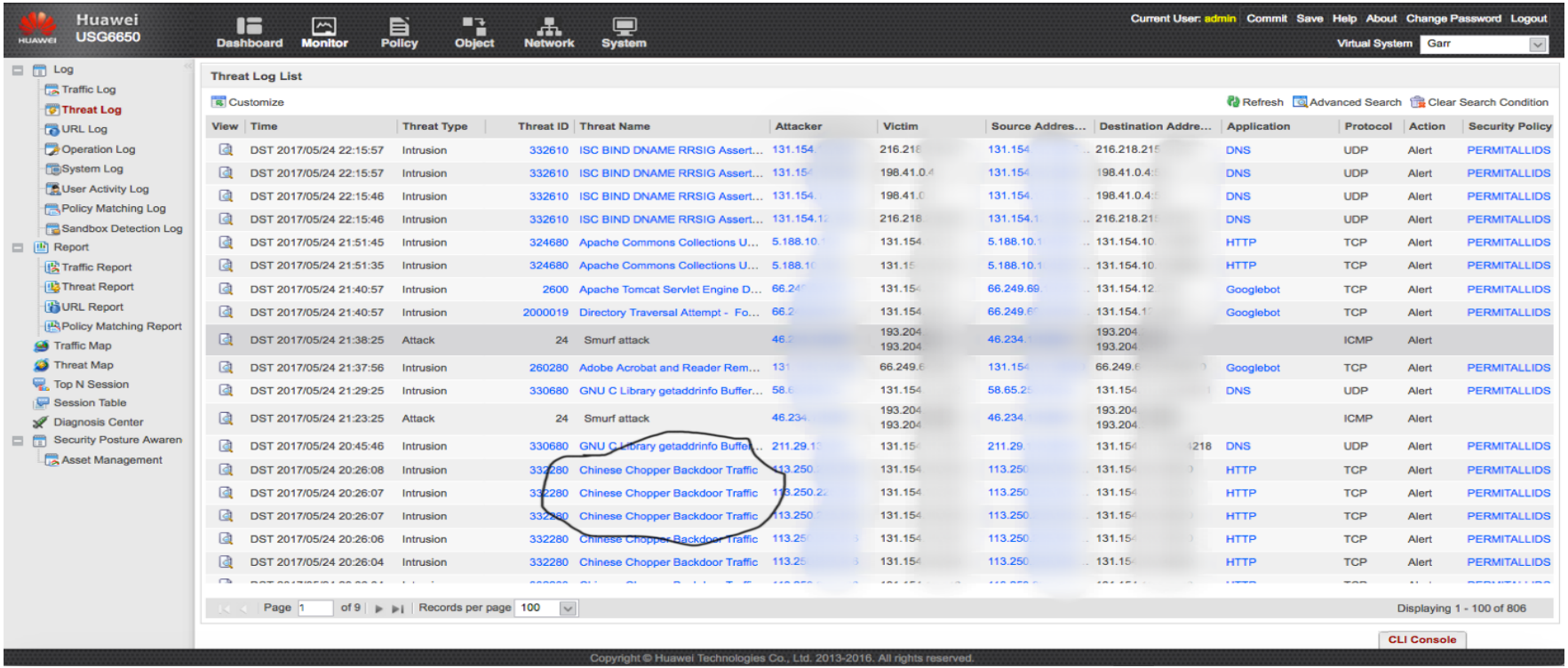
Syslog

- 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 gia' realizzati per Splunk e Q-radar (altri chissa') ma non abbiamo avuto il tempo di testarli

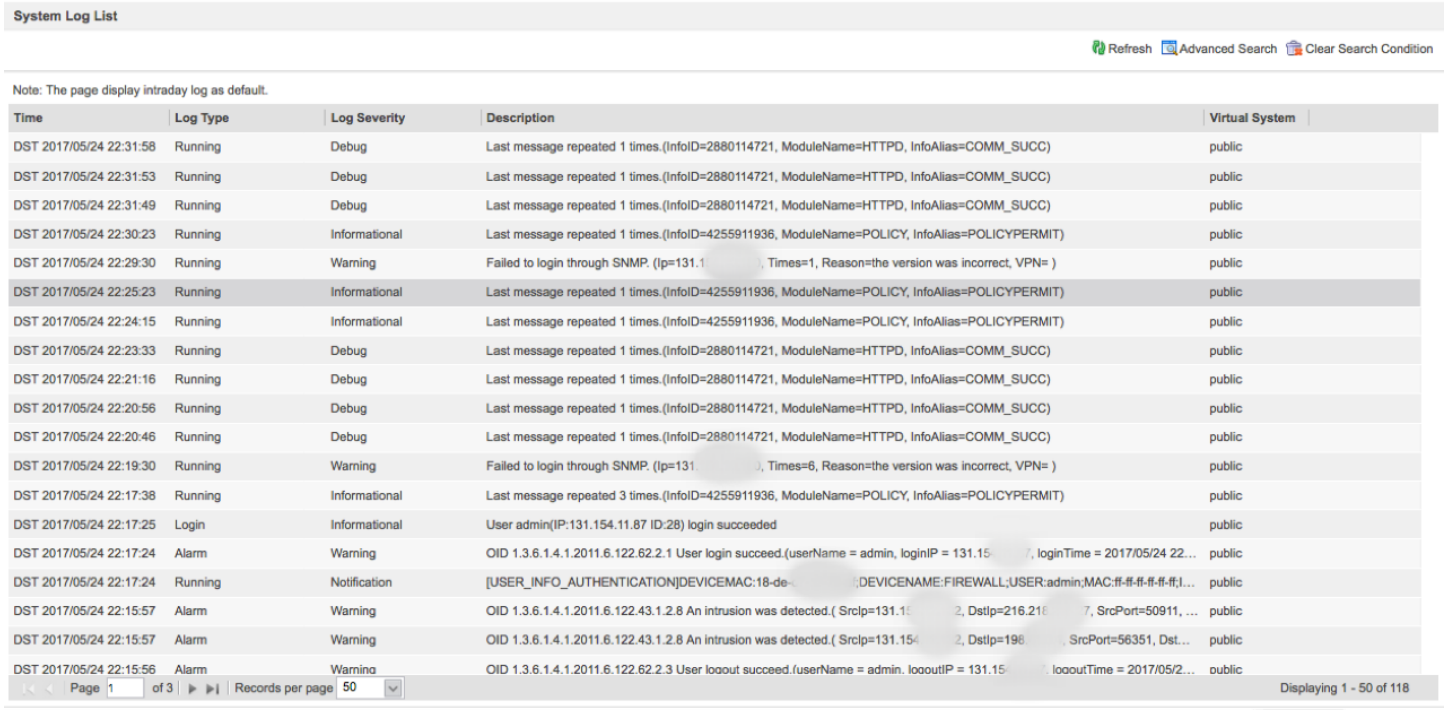
Real Time Monitor

- 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



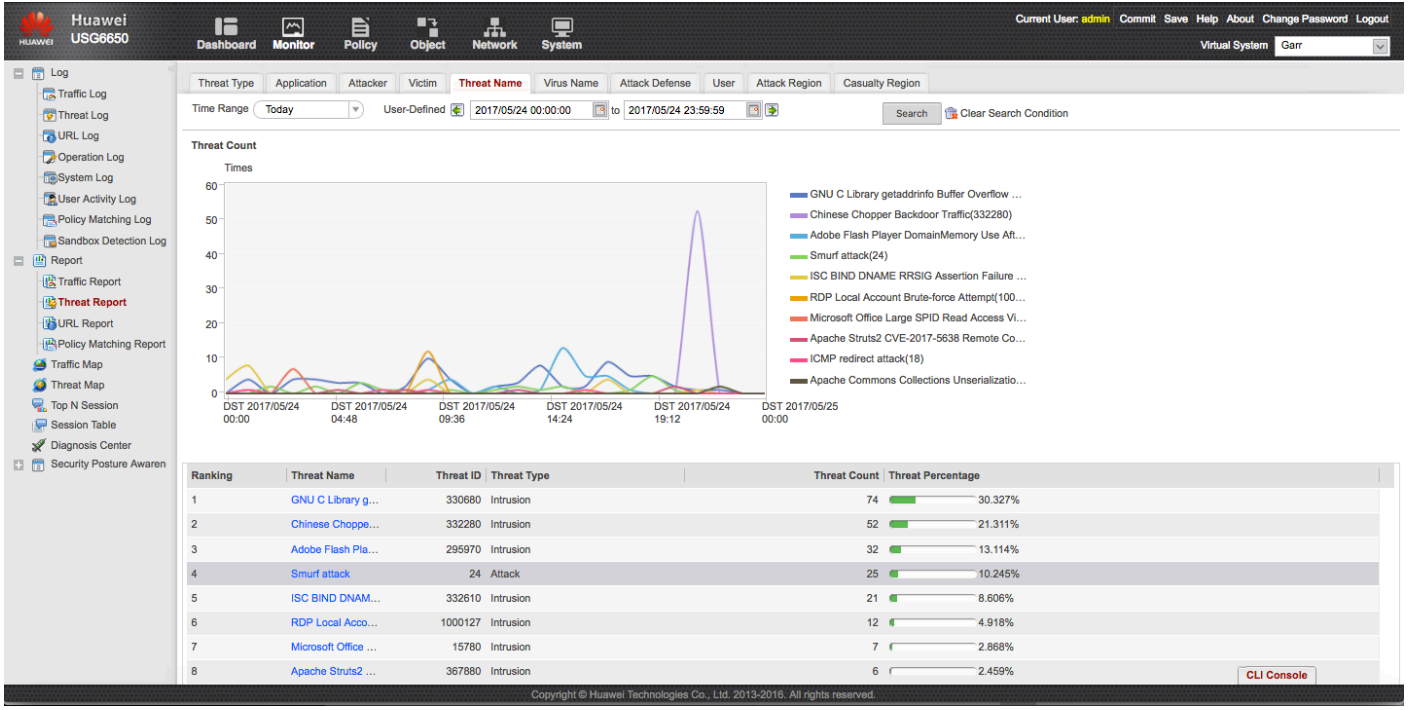
Monitor integrato



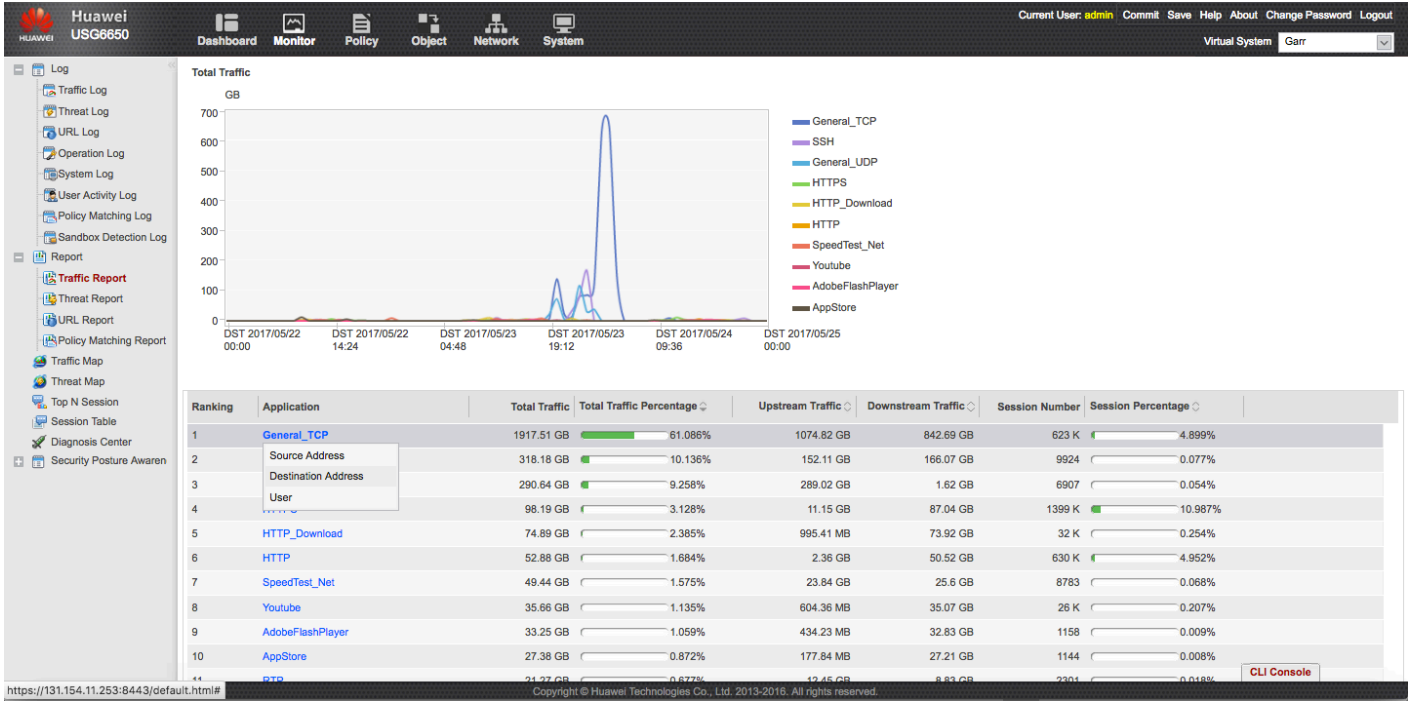
Report

- 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 probabilemente piu' utile sia per le operation che per la remediation
- Ne i monitor integrati ne i report sono strumenti adeguati x la Forensic

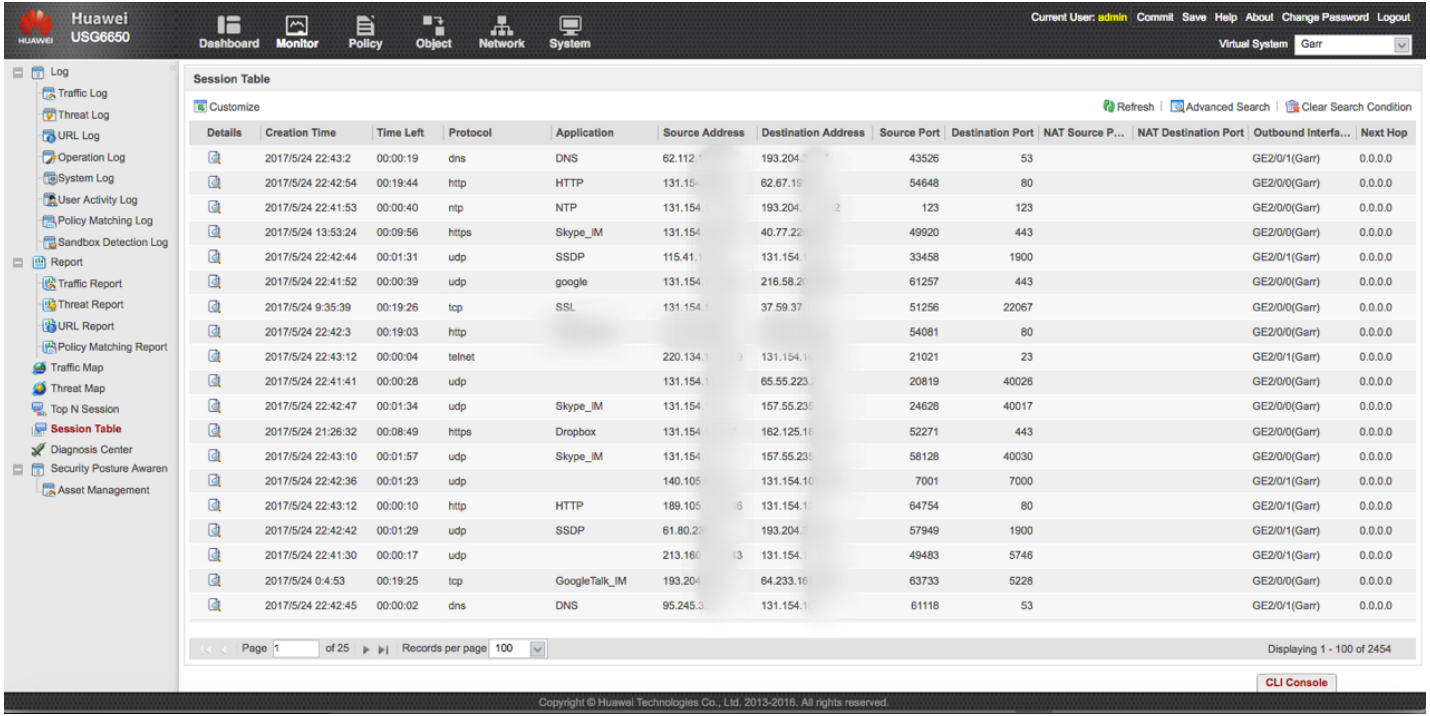
Threat Report



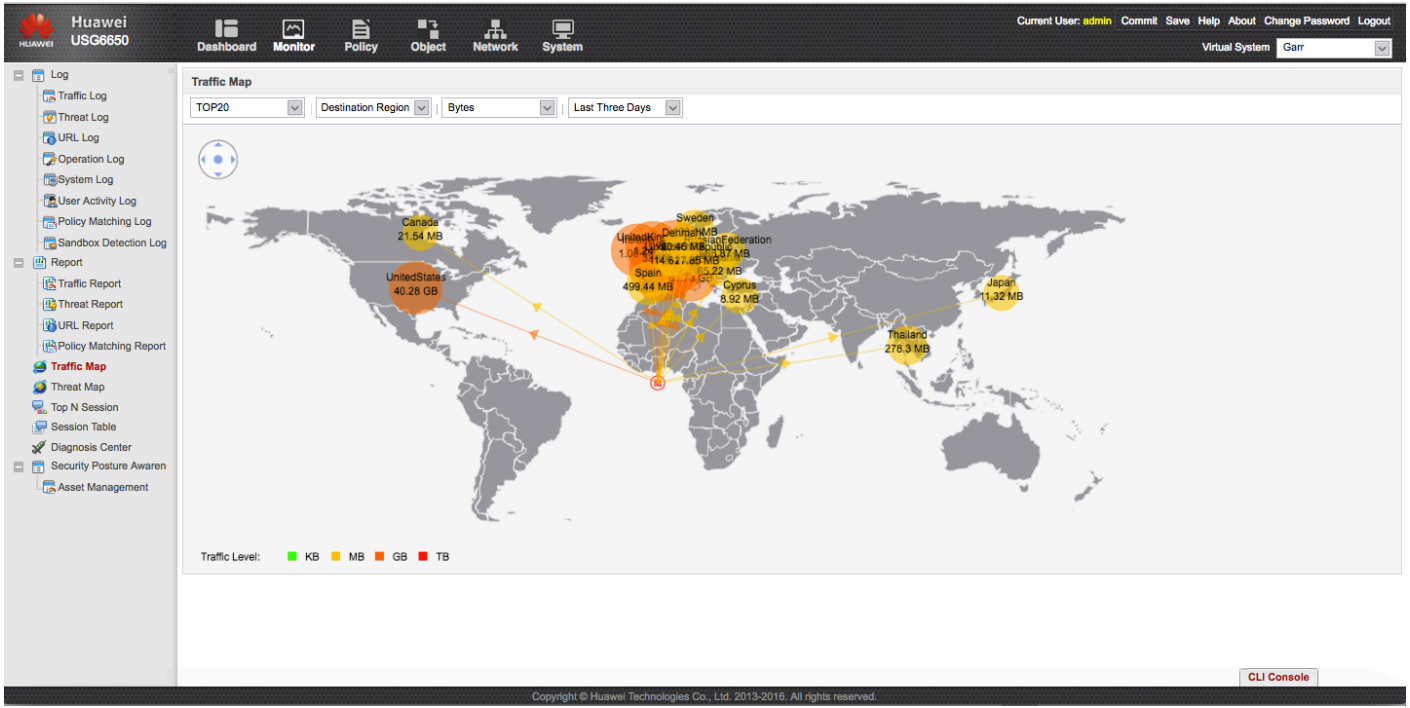
Traffic Report



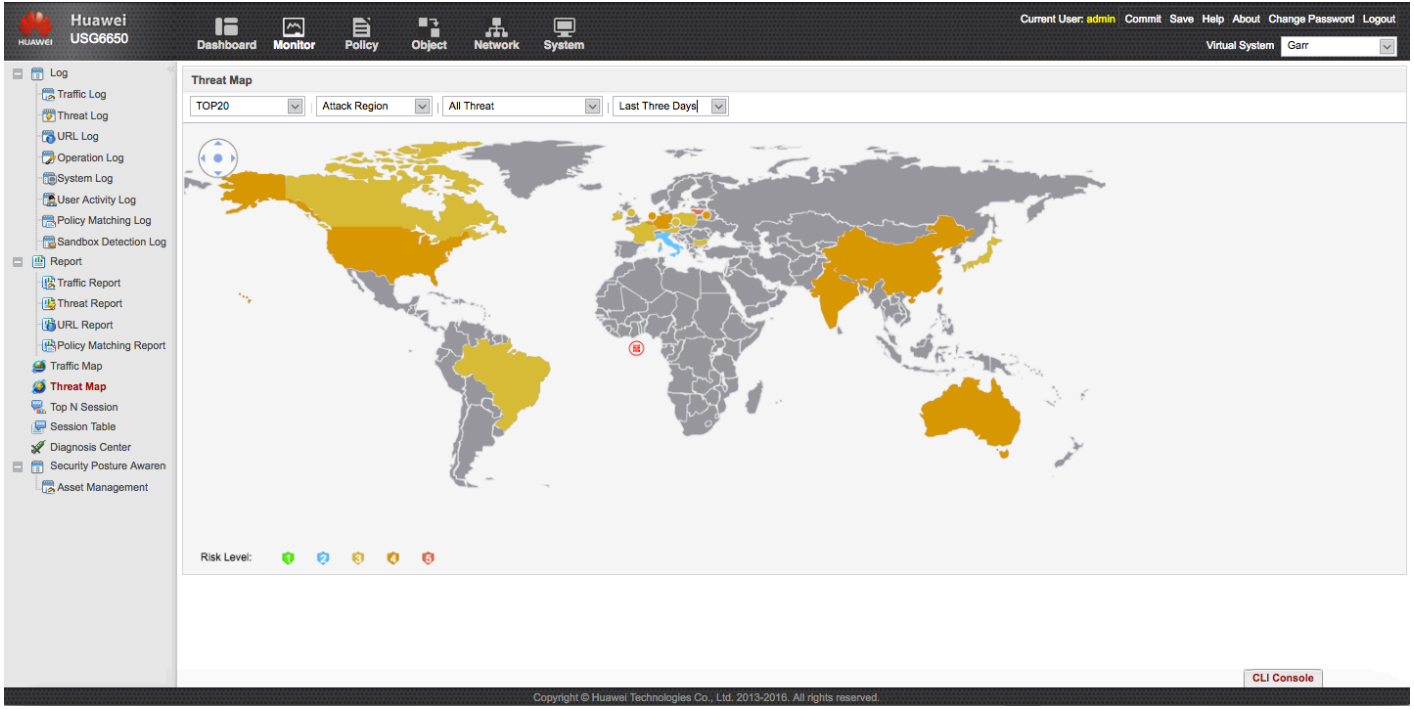
Session Table



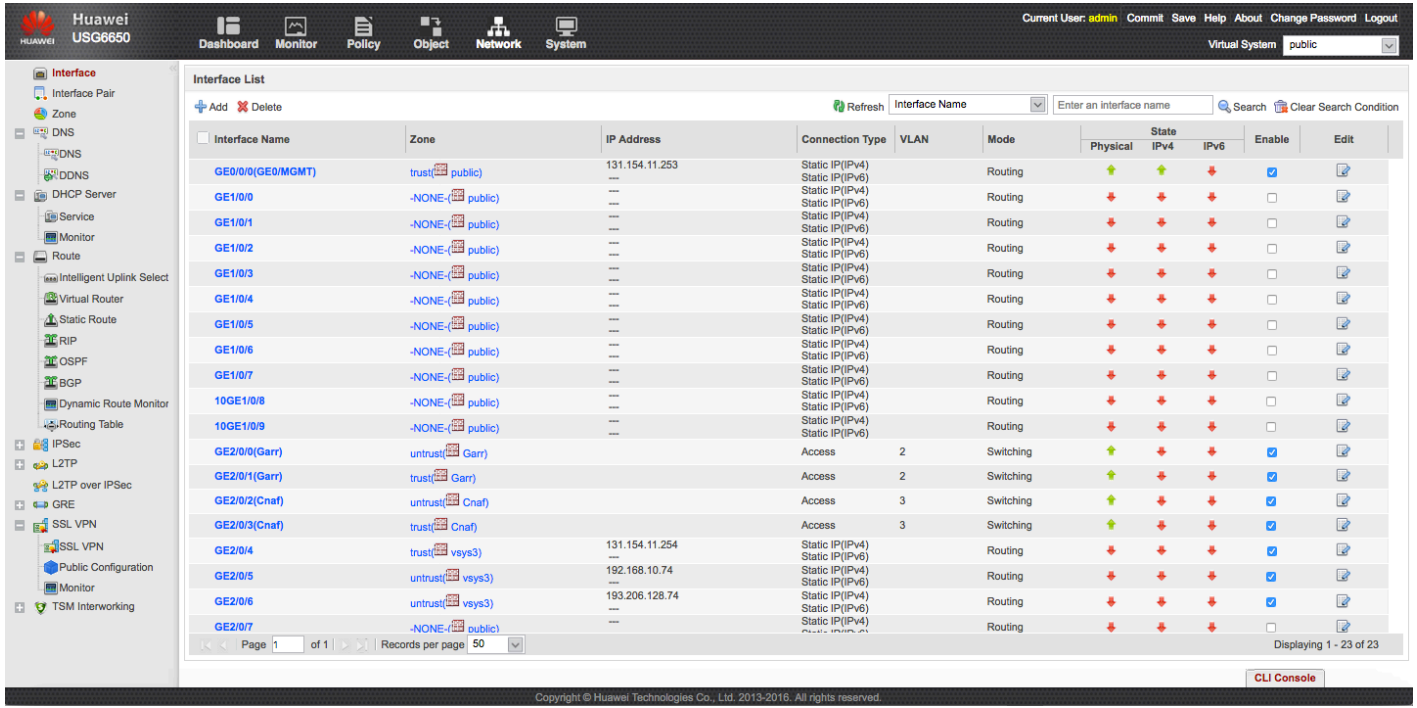
Traffic Map


Huawei
USG6650
Dashboard
Monitor
Policy
Object
Network
System
Current User: admin
Commit
Save
Help
About
Change Password
Logout
Virtual System
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 Awaren
Asset Management
Traffic Map
TOP20
Destination Region
Bytes
Last Three Days
Canada
21.54 MB
UnitedStates
40.28 GB
Sweden
Denmark
Spain
499.44 MB
Cyprus
8.92 MB
Japan
11.32 MB
Thailand
278.3 MB
Traffic Level:
KB
MB
GB
TB
CLI Console
Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

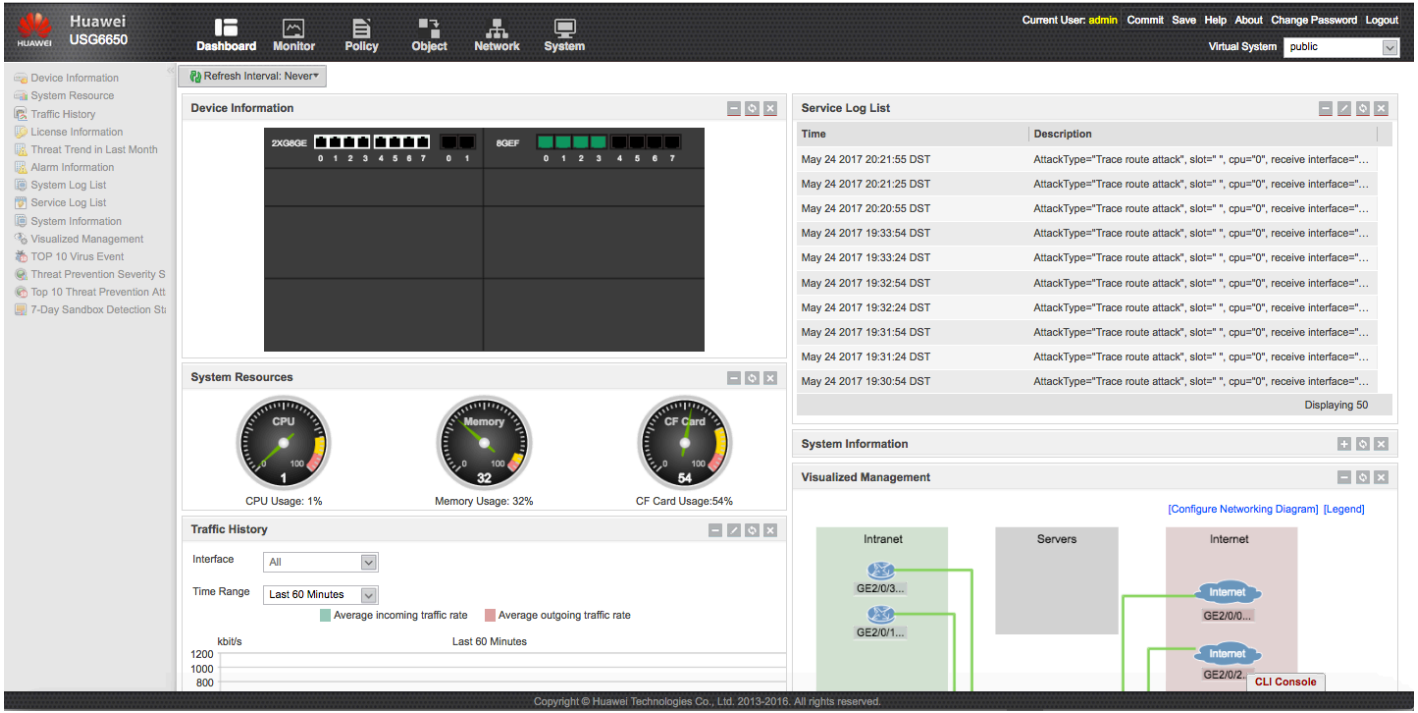
Threat Map


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 Awaren
Asset Management
Threat Map
TOP20
Attack Region
All Threat
Last Three Days
Risk Level:
CLI Console
Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

Network configuration

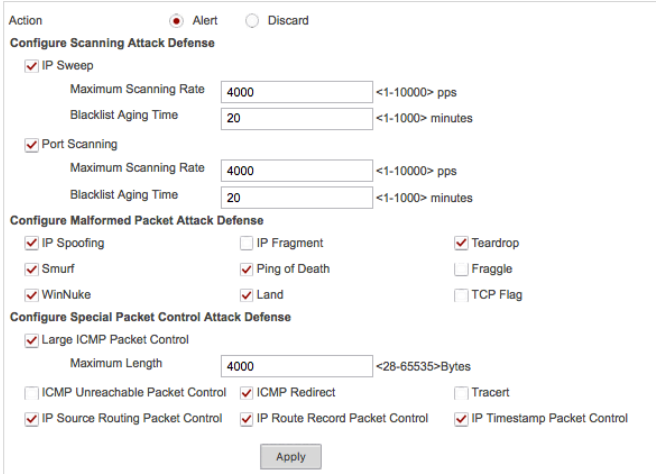


Dashboard del contesto



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



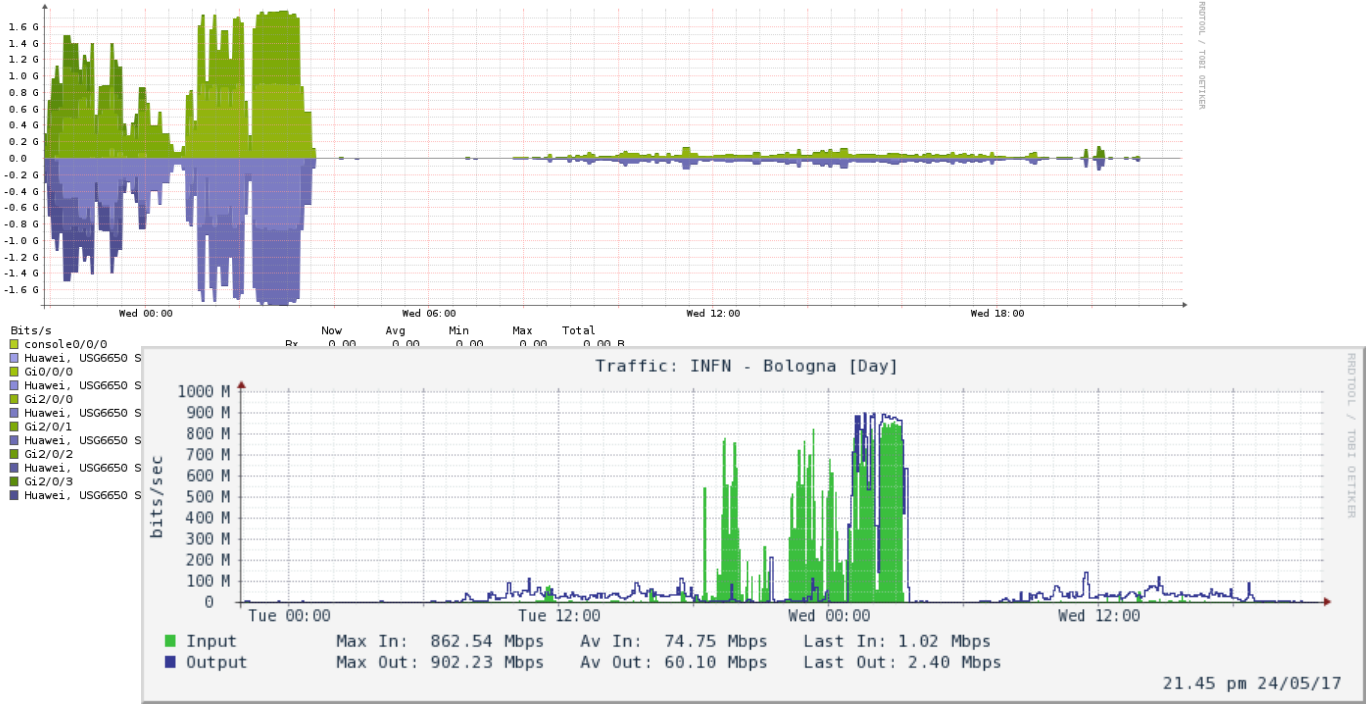
Falsi positivi – non falsi

- 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


1.6 G
1.4 G
1.2 G
1.0 G
0.8 G
0.6 G
0.4 G
0.2 G
0.0
-0.2 G
-0.4 G
-0.6 G
-0.8 G
-1.0 G
-1.2 G
-1.4 G
-1.6 G
Wed 00:00
Wed 06:00
Wed 12:00
Wed 18:00
Bits/s
Now
Avg
Min
Max
Total
console0/0/0
Huawei, USG6650 S
Gi0/0/0
Huawei, USG6650 S
Gi2/0/0
Huawei, USG6650 S
Gi2/0/1
Huawei, USG6650 S
Gi2/0/2
Huawei, USG6650 S
Gi2/0/3
Huawei, USG6650 S
Traffic: INFN - Bologna [Day]
bits/sec
1000 M
900 M
800 M
700 M
600 M
500 M
400 M
300 M
200 M
100 M
0
Tue 00:00
Tue 12:00
Wed 00:00
Wed 12:00
Input
Output
Max In: 862.54 Mbps
Av In: 74.75 Mbps
Last In: 1.02 Mbps
Max Out: 902.23 Mbps
Av Out: 60.10 Mbps
Last Out: 2.40 Mbps
21.45 pm 24/05/17

Problemi riscontrati

- Nessuno, ma… troppo rumore (maledizione di Tutankhamon ?! Della concorrenza ?!) occore 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 venerdi' (!@?) 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