TEST DEL NEXT GENERATION FIREWALL FORTIGATE 1500D

Massimo Pistoni

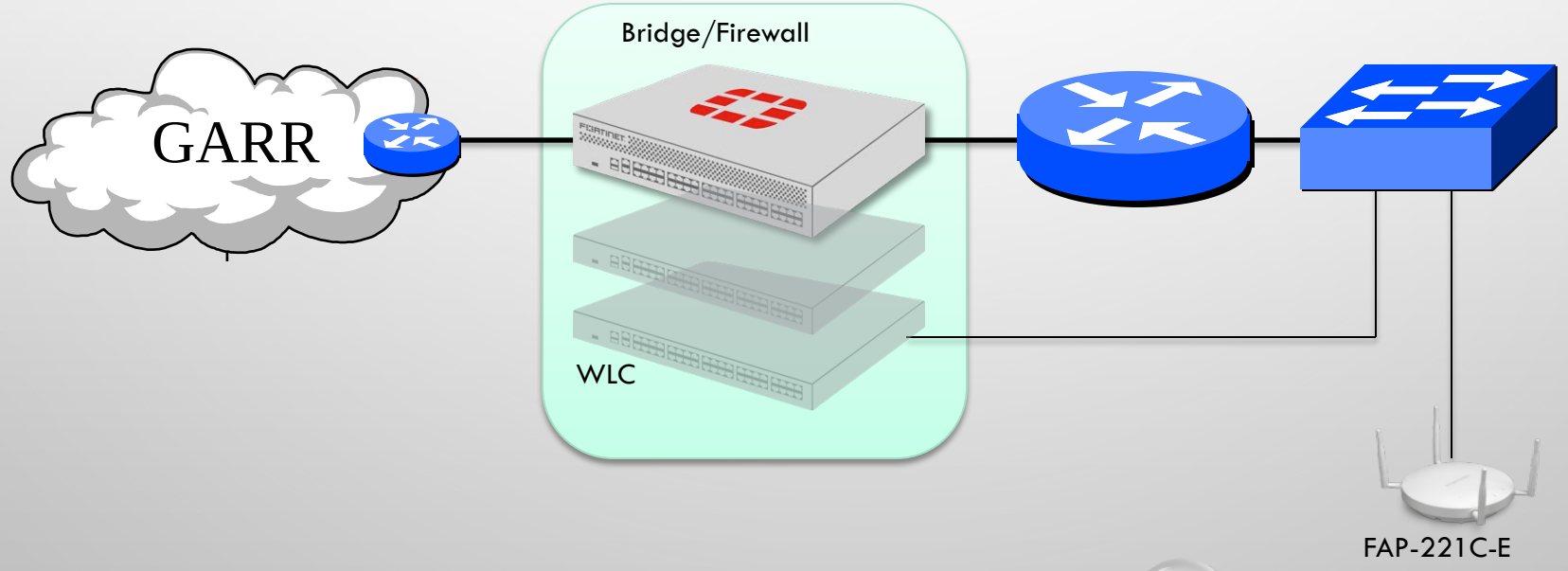
SPECIFICHE TECNICHE

Hardware specifications, Performances	
porte 10Gb/s SFP+	8
16 porte 1Gb/s SFP	16
16 porte 1Gb/s RJ45	16
IP F/W Throughput (1512,512,64 Byte)	80/80/55 Gbps
IPS Throughput	13 Gbps
NGFW Throughput	5,5 Gbps

NGFW / WLC

- PARTIZIONABILE IN 10 DOMINI
- INSTALLABILE IN CONFIGURAZIONE HA

CONFIGURAZIONE LNF



NGFW

- FILTRI ABILITATI IN INGRESSO (GARR→LNF):
  - APPLICATION CONTROL
  - INTRUSION PREVENTION SYSTEM
  - ANTIVIRUS
- FILTRI ABILITATI IN USCITA (GARR←LNF):
  - APPLICATION CONTROL
  - INTRUSION PREVENTION SYSTEM
  - ANTIVIRUS
  - WEB FILTERING

FortiGate - FG1K5D3I1580

https://fortigate.lnf.infn.it/ng/firewall/policy/policy/standard?vdom=Transparent

Apps | Bookmarks | Imported From Firefo | DB | Banca | Calcolo | jcalc | Sport | Maps | https://fortigate.lnf.i | Calendar | starpix | maxpix | Terracan - Removal | Other Bookmarks

FortiGate 1500D FG1K5D3I15803664 — admin

- Transparent
- FortiView
- Network
- System
- Policy & Objects
  - IPv4 Policy
  - IPv4 Access Control List
  - IPv4 DoS Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Traffic Shapers
  - Traffic Shaping Policy
- Security Profiles
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

Create New | Edit | Delete | Search | Interface Pair View | By Sequence

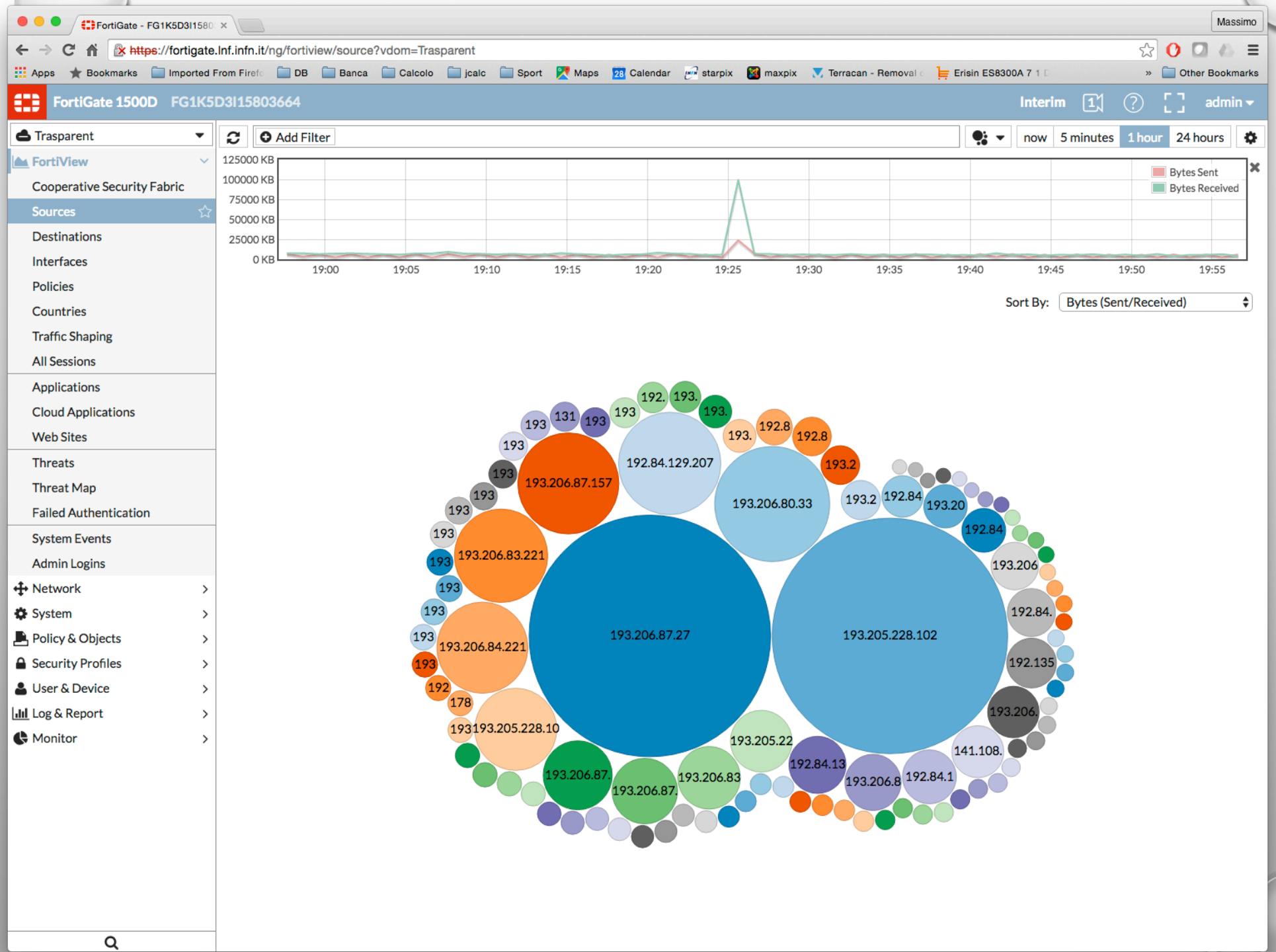
Seq.#	Name	Source	Destination	Schedule	Service	Action	Security Profiles	Log	Bytes
port34_926 (port34) - port35_926 (port35) (1 - 3)									
1	LicenseServer-IN-926	all	LicenseServer	always	ALL	Accept		All	1.17 MB
2	Fortiguard-access-IN	all	fortigate-mgmt	always	ALL	Accept		All	6.28 kB
3	GARR-IN-926	all	all	always	ALL	Accept	AV APP IPS PRX	All	53.81 GB
port34_927 (port34) - port35_927 (port35) (4 - 4)									
4	GARR-IN-927	all	all	always	ALL	Accept	AV APP IPS PRX	All	19.34 MB
port34_928 (port34) - port35_928 (port35) (5 - 5)									
5	GARR-IN-928	all	all	always	ALL	Accept		All	265.38 MB
port35_926 (port35) - port34_926 (port34) (6 - 8)									
6	LicenseServer-OUT-926	LicenseServer	all	always	ALL	Accept		All	2.03 MB
7	Fortiguard-access-OUT	fortigate-mgmt	all	always	ALL	Accept		All	36.52 MB
8	GARR-OUT-926	all	all	always	ALL	Accept	AV WEB APP IPS PRX	All	141.40 GB
port35_927 (port35) - port34_927 (port34) (9 - 9)									
9	GARR-OUT-927	all	all	always	ALL	Accept	AV WEB APP IPS PRX	All	947.34 MB
port35_928 (port35) - port34_928 (port34) (10 - 10)									
10	GARR-OUT-928	all	all	always	ALL	Accept		All	322.27 MB
Implicit (11 - 11)									
11	Implicit Deny	all	all	always	ALL	Deny		Disabled	0 B

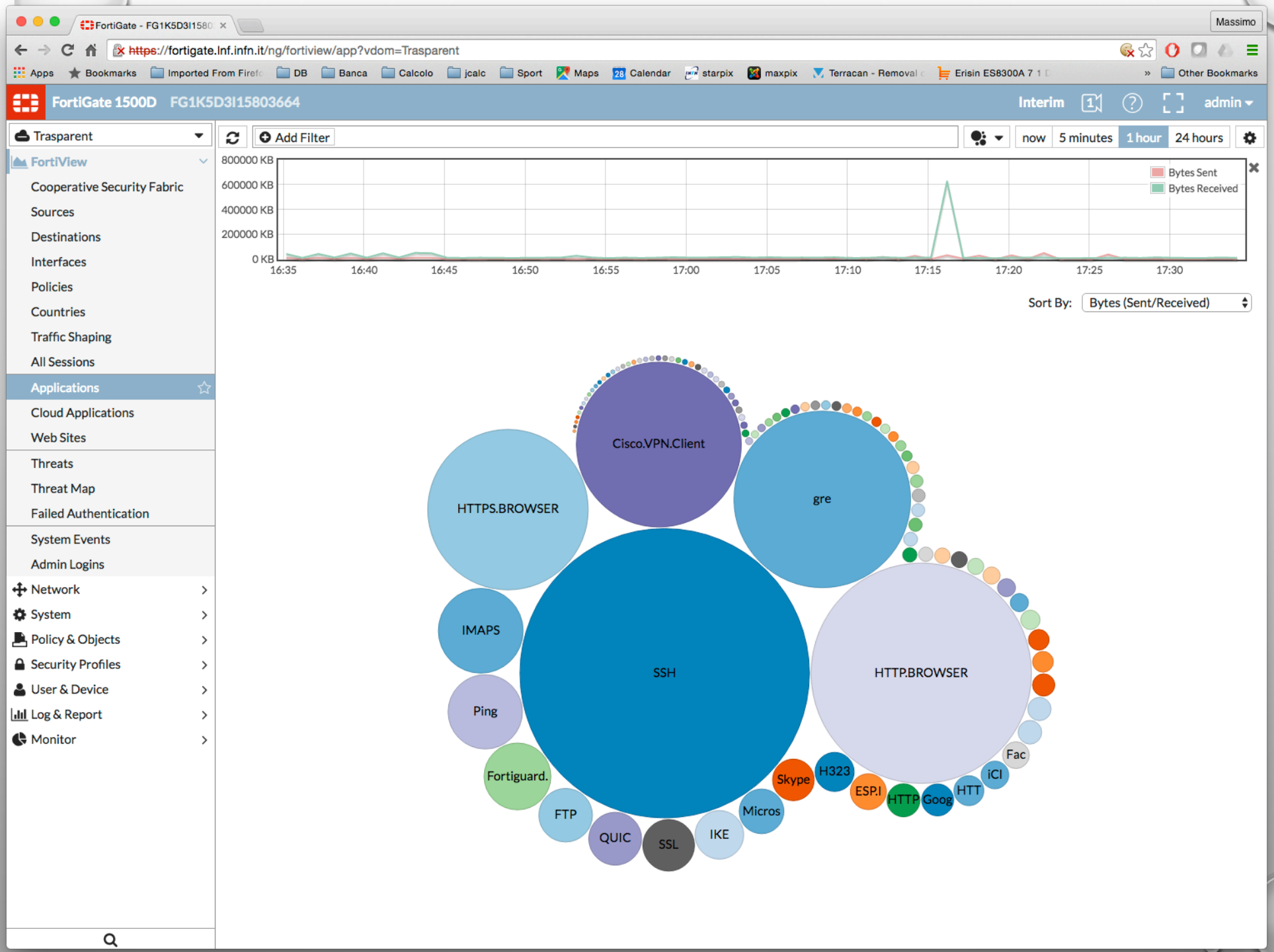
WEB FILTER (SOLO OUT)

- SITI GIA' CATEGORIZZATI SECONDO RISCHIO E/O CONTENUTO, MA SELEZIONABILI ANCHE SINGOLARMENTE (O CON USO DI WILDCHAR)
- BLOCK DELLA CATEGORIA "SECURITY RISK"
  - CON ECCEZIONE PER DYNAMIC DNS
- ABILITATE TUTTE LE ALTRE CATEGORIE
- BLOCK DI SITI SPECIFICI PUNTATI NEI MAIL DI PHISHING RICEVUTI DAGLI UTENTI LNF

MONITOR

- FUNZIONALITA' DI MONITORING ATTRAVERSO LA VOCE **FORTIVIEW**
  - NOW, 5 MINUTES, 1 HOUR, 24 HOURS
- FILTRI DI RICERCA E DI SELEZIONE ANCHE IN COMBINAZIONE (AND)
  - SOURCES, DESTINATIONS, INTERFACES, POLICIES, COUNTRIES, SESSIONS, APPLICATIONS, CLOUD APPLICATIONS, WEB SITES, THREATS, ETC.
- RAPPRESENTAZIONE IN TABELLA O IN BOLLE


FortiGate - FG1K5D3I1580
https://fortigate.lnf.infn.it/ng/fortiview/source?vdom=Trasparent
Massimo
Apps
Bookmarks
Imported From Firefo
DB
Banca
Calcolo
jcalc
Sport
Maps
Calendar
starpix
maxpix
Terracan - Removal
Erisin ES8300A 7 1
Other Bookmarks
FortiGate 1500D
FG1K5D3I15803664
Interim
admin
Trasparent
FortiView
Cooperative Security Fabric
Sources
Destinations
Interfaces
Policies
Countries
Traffic Shaping
All Sessions
Applications
Cloud Applications
Web Sites
Threats
Threat Map
Failed Authentication
System Events
Admin Logins
Network
System
Policy & Objects
Security Profiles
User & Device
Log & Report
Monitor
Add Filter
now
5 minutes
1 hour
24 hours
125000 KB
100000 KB
75000 KB
50000 KB
25000 KB
0 KB
19:00
19:05
19:10
19:15
19:20
19:25
19:30
19:35
19:40
19:45
19:50
19:55
Bytes Sent
Bytes Received
Sort By:
Bytes (Sent/Received)
193.206.87.27
193.205.228.102
193.206.80.33
192.84.129.207
193.206.87.157
193.206.83.221
193.206.84.221
193.205.228.10
193.205.22
193.206.83
193.206.87.
193.206.87.
192.84.13
193.206.8
192.84.1
141.108.
193.206.
192.135
192.84.
193.206
192.84
193.20
193.2
192.8
192.8
193.
193.
193.
192.
193
193
131
193
193
193
193
193
193
193
193
193
193
193
193
193
193
192
178
193
193.205.228.10


FortiGate - FG1K5D3I1580
https://fortigate.lnf.infn.it/ng/fortiview/app?vdom=Trasparent
Massimo
Apps
Bookmarks
Imported From Firefo
DB
Banca
Calcolo
jcalc
Sport
Maps
Calendar
starpix
maxpix
Terracan - Removal
Erisin ES8300A 7
Other Bookmarks
FortiGate 1500D
FG1K5D3I15803664
Interim
admin
Trasparent
FortiView
Cooperative Security Fabric
Sources
Destinations
Interfaces
Policies
Countries
Traffic Shaping
All Sessions
Applications
Cloud Applications
Web Sites
Threats
Threat Map
Failed Authentication
System Events
Admin Logins
Network
System
Policy & Objects
Security Profiles
User & Device
Log & Report
Monitor
Add Filter
now
5 minutes
1 hour
24 hours
800000 KB
600000 KB
400000 KB
200000 KB
0 KB
16:35
16:40
16:45
16:50
16:55
17:00
17:05
17:10
17:15
17:20
17:25
17:30
Bytes Sent
Bytes Received
Sort By:
Bytes (Sent/Received)
Cisco.VPN.Client
gre
HTTPS.BROWSER
IMAPS
SSH
HTTP.BROWSER
Ping
Fac
iCl
HTT
Goog
HTTP
ESP.I
H323
Skype
Micros
IKE
SSL
QUIC
FTP
Fortiguard.

FortiGate - FG1K5D3I1580

https://fortigate.lnf.infn.it/ng/fortiview/web/category/26?vdom=Trasparent

FortiGate 1500D FG1K5D3I15803664

Interim admin

Trasparent

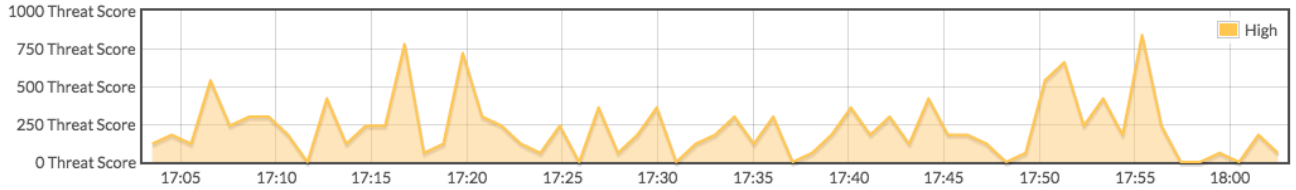
FortiView
- Cooperative Security Fabric
- Sources
- Destinations
- Interfaces
- Policies
- Countries
- Traffic Shaping
- All Sessions
- Applications
- Cloud Applications
- Web Sites
- Threats
- Threat Map
- Failed Authentication
- System Events
- Admin Logins

Network
System
Policy & Objects
Security Profiles
User & Device
Log & Report
Monitor

Category: Malicious Websites | Add Filter | Categories | 5 minutes | 1 hour | 24 hours

Summary of Malicious Websites

Sessions : 220
Time Period : Last Hour



Sources | Destinations | Countries | Threats | Domains | Sessions

Threat	Category	Threat Level	Threat Score (Blocked/Allowed)	Sessions (Blocked/Allowed)
pr.ohmyad.co	Malicious Websites	High	3720	62
ad.adriver.ru	Malicious Websites	High	1080	18
counter.yadro.ru	Malicious Websites	High	1080	18
tr.affiliate.hu	Malicious Websites	High	780	13
xa.ghokswa.com	Malicious Websites	High	780	13
hostingtv.org	Malicious Websites	High	420	7
cdnrep.reimage.com	Malicious Websites	High	360	6
i.mgicinjs.info	Malicious Websites	High	360	6
i.mgicinsrc.org	Malicious Websites	High	360	6
tag.clrstm.com	Malicious Websites	High	360	6
update.picexa.com	Malicious Websites	High	360	6
ads.heias.com	Malicious Websites	High	300	5
xa.xingcloud.com	Malicious Websites	High	300	5
a.company-target.com	Malicious Websites	High	240	4
adblock.qihuweb.com	Malicious Websites	High	240	4
sync.malwareprotectionlive.com	Malicious Websites	High	240	4
cdn.optimizely.com	Malicious Websites	High	180	3
beacon.securestudies.com	Malicious Websites	High	120	2
cdncache-a.akamaihd.net	Malicious Websites	High	120	2
dp.g.doubleclick.net	Malicious Websites	High	120	2
t.dtscdn.com	Malicious Websites	High	120	2
thecloudservices.net	Malicious Websites	High	120	2
track.eyeviewads.com	Malicious Websites	High	120	2

1 /1 [Total: 43]

LOG & REPORT

- VENGONO RACCOLTI I LOG SU RAM O SU HD
- POSSONO ESSERE INOLTRATI ANCHE:
  - LOG SERVER ESTERNO (SYSLOGD)
  - FORTIANALYZER (APPOSITA VM), CONSIGLIATO!
- I LOG SONO GENERATI IN QUANTITA' ESAGERATA (VARIE CENTINAIA DI RECORD/S)
- IL FORTIGATE E' COMUNQUE IN GRADO DI VISUALIZZARE UN PO' DI LOG (7 GG.)
- GESTIONE DEGLI ALERT VIA E-MAIL

FortiGate - FG1K5D3I1580

https://fortigate.lnf.infn.it/ng/log/view/web?vdom=Trasparent

Apps | Bookmarks | Imported From Firefo | DB | Banca | Calcolo | jcalc | Sport | Maps | Calendar | starpix | maxpix | Terracan - Removal | Erisin ES8300A 7 | Other Bookmarks

FortiGate 1500D FG1K5D3I15803664 — Interim — admin

Trasparent

- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- User & Device
- Log & Report
  - Forward Traffic
  - System Events
  - AntiVirus
  - Web Filter
  - Application Control
  - Intrusion Protection
  - Log Settings
  - Threat Weight
  - Alert E-mail
- Monitor

Add Filter — Log location: Disk — Details

#	Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
1	19:24:57		193.206.	blocked	xa.xingcloud.com/v4/sof-px/WDCXWD3200AAJS-41VWA1_WD-WCARW700128…	Malicious Websites		187 B / 0 B
2	19:24:57		193.206.	blocked	xa.xingcloud.com/v4/sof-px/WDCXWD3200AAJS-41VWA1_WD-WCARW700128…	Malicious Websites		168 B / 0 B
3	19:24:40		193.206.	blocked	cdnrep.reimage.com/protector/system_settings.rei	Malicious Websites		289 B / 0 B
4	19:24:00		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
5	19:22:30		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
6	19:21:49		193.205.	blocked	spb.bid.run/sync/rambler.gif?ssp_uid=000000c9-572b-81f1-6cc4-64…	Malicious Websites		2.77 kB / 0 B
7	19:21:49		193.205.	blocked	spb.bid.run/sync/begun.gif?ssp_uid=000000c9-572b-81f1-6cc4-641f…	Malicious Websites		2.77 kB / 0 B
8	19:21:49		193.205.	blocked	ad.dumedia.ru/uid/sync?sspId=5&id=000000c9-572b-81f1-6cc4-6…	Malicious Websites		2.77 kB / 0 B
9	19:21:49		193.205.	blocked	sync.audtd.com/match/begun?uid=000000c9-572b-81f1-6cc4-641fc7b6…	Malicious Websites		2.77 kB / 0 B
10	19:20:59		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
11	19:20:53		193.206.	blocked	a.company-target.com/bidswitch_match?bidswitch_ssp_id=switchcon…	Malicious Websites		410 B / 0 B
12	19:20:49		193.206.	blocked	www.technologiesaintjoseph.com/addon/script/content_site?integr…	Malicious Websites		721 B / 0 B
13	19:19:45		193.206.	blocked	hostingtv.org/files/FooterGs2.php	Malicious Websites		633 B / 0 B
14	19:19:29		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
15	19:18:09		193.206.	blocked	update.picexa.com/Yacapi/returnExec?version=2.1.57&pid=px&a…	Malicious Websites		243 B / 0 B
16	19:17:59		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
17	19:16:29		193.206.	blocked	www.shtyle.fm/getchatmsg.do?_x=1&lastmsgts=1462404364000	Phishing		586 B / 0 B
18	19:16:27		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		274 B / 0 B
19	19:16:26		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		270 B / 0 B
20	19:16:25		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		263 B / 0 B
21	19:16:25		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		262 B / 0 B
22	19:16:25		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		265 B / 0 B
23	19:16:25		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		270 B / 0 B
24	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		272 B / 0 B
25	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		204 B / 0 B
26	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		270 B / 0 B
27	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		210 B / 0 B
28	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		202 B / 0 B
29	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		223 B / 0 B
30	19:16:24		193.206.	blocked	xa.ghokswa.com/v4/ghokswa/5D125D027841D51B7801F3BDF8F16FC3?acti…	Malicious Websites		211 B / 0 B
31	19:15:36		193.206.	blocked	a.company-target.com/bidswitch_match?bidswitch_ssp_id=switchcon…	Malicious Websites		438 B / 0 B
32	19:15:12		193.206.	blocked	a.company-target.com/bidswitch_match?bidswitch_ssp_id=switchcon…	Malicious Websites		410 B / 0 B
33	19:15:00		193.206.	blocked	storage.stgbssint.com/IEBackgroundContainer/TBUpdaterLogic/4.0.…	Malicious Websites		356 B / 0 B
34	19:14:59		193.206.	blocked	usage.toolbar.tbccint.com/ToolbarUsage.ashx	Malicious Websites		262 B / 0 B
35	19:14:59		193.206.	blocked	usage.toolbar.tbccint.com/ToolbarUsage.ashx	Malicious Websites		262 B / 0 B

1 /379 [Total: 37831]

CONCLUSIONI

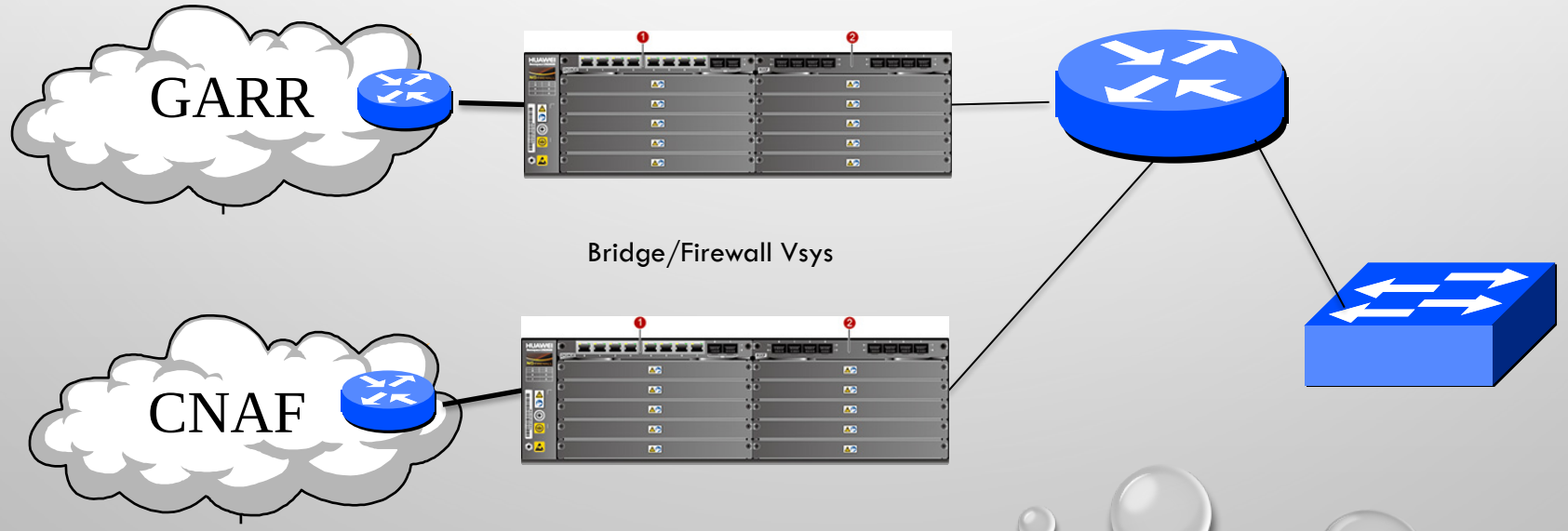
- FATTI SALVI ALCUNI PICCOLI PROBLEMI RISCONTRATI, IN PARTE SANATI DURANTE LA DEMO, IL FORTIGATE SEMBRA UN VALIDO STRUMENTO PER AUMENTARE LA SICUREZZA DEI SISTEMI INFORMATICI CONNESSI SULLA LAN
- ANCHE COME WLC SVOLGE EGREGIAMENTE IL SUO LAVORO
- L'INTERFACCIA DI GESTIONE APPARE SEMPLICE ED ABBASTANZA INTUITIVA

HUAWEI USG6650

PRIMO MESE NEL MONDO REALE (L2 MODE)

LAYOUT

- PARTIZIONABILE IN 10 VSYS (CON LA LICENZA BASE)
- INSTALLABILE IN CONFIGURAZIONE HA



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

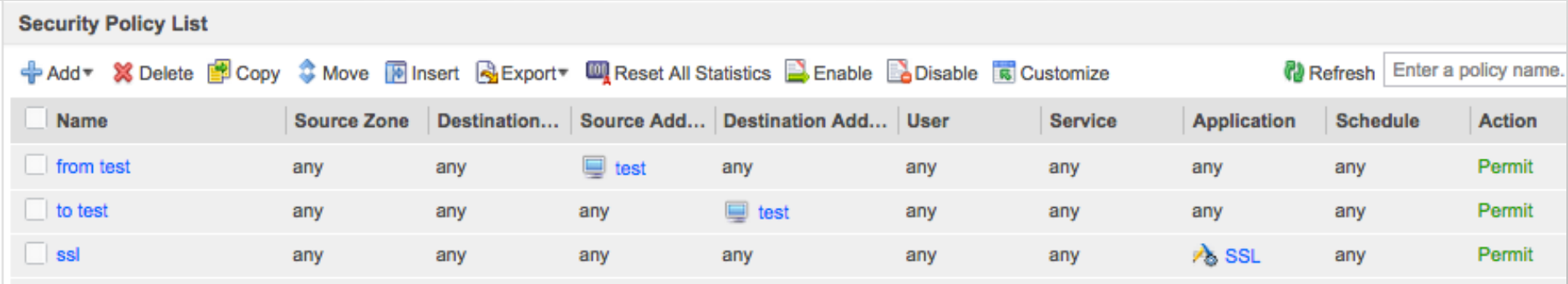
1. 8 x GE (RJ45) and 2 x 10 GE (SFP+) Ports
2. 8 x GE (SFP) Ports
3. 2 x USB Ports
4. 1 x GE (RJ45) Management Port
5. Console Port (RJ45)
6. Console Port (Mini-USB)

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)

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



Name	Source Zone	Destination...	Source Add...	Destination Add...	User	Service	Application	Schedule	Action
from test	any	any	test	any	any	any	any	any	Permit
to test	any	any	any	test	any	any	any	any	Permit
ssl	any	any	any	any	any	any	SSL	any	Permit

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 Profile List

Add | Delete | Copy | Refresh

Profile have changed, Commit th

Name	Attac	Category	Action	Domain...	Refer...	Edit
testipp		All	Default		0 View	
strict		All	Block		0 View	
web_server		All	Default		0 View	
file_server		All	Default		0 View	
dns_server					0 View	
mail_server					0 View	
inside_firewall					0 View	
dmz					0 View	
outside_firewall					0 View	
ids					4 View	
default					4 View	

Page 1 of 1 | Records per

Displaying 1 - 11 of 11

CLI Console

Pre-defined Profile Detail

Name: ids

Description:

Signature Filter List

View Signature Filter Result

Name	Target	Severity	OS	Protocol	Category	Action
default	All	Low, Medium, High	Unix-like,...	All	All	Alert

View Signature Filter Result

Refresh | Enter an ID, name, vendor vulnerability ID, or CVE number, or CNNVD number. | Search | Advanced Search | Clear Search Condition

ID	Name	Vend...	CVE ...	CNN...	Target	Severity	OS	Applicati...	Protocol	Action
46150	Trojan: Win32.Geno...				All	Medium	Windows	All	HTTP	Alert(Ove...
46160	Trojan: Win32.Kryptik				All	Medium	Windows	All	HTTP	Alert(Ove...
46470	Trojan: Nuclear_Rat				Client	Medium	Windows	All	TCP	Alert
46510	Remote Control Too...				All	Medium	Windows	All	TCP	Alert
46511	Remote Control Too...				All	Medium	Windows	All	HTTP	Alert
46512	Remote Control Too...				All	Medium	Windows	All	UDP	Alert
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

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☺)

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

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

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 Log List

Customize | Refresh | Advanced Search | Clear Search Condition

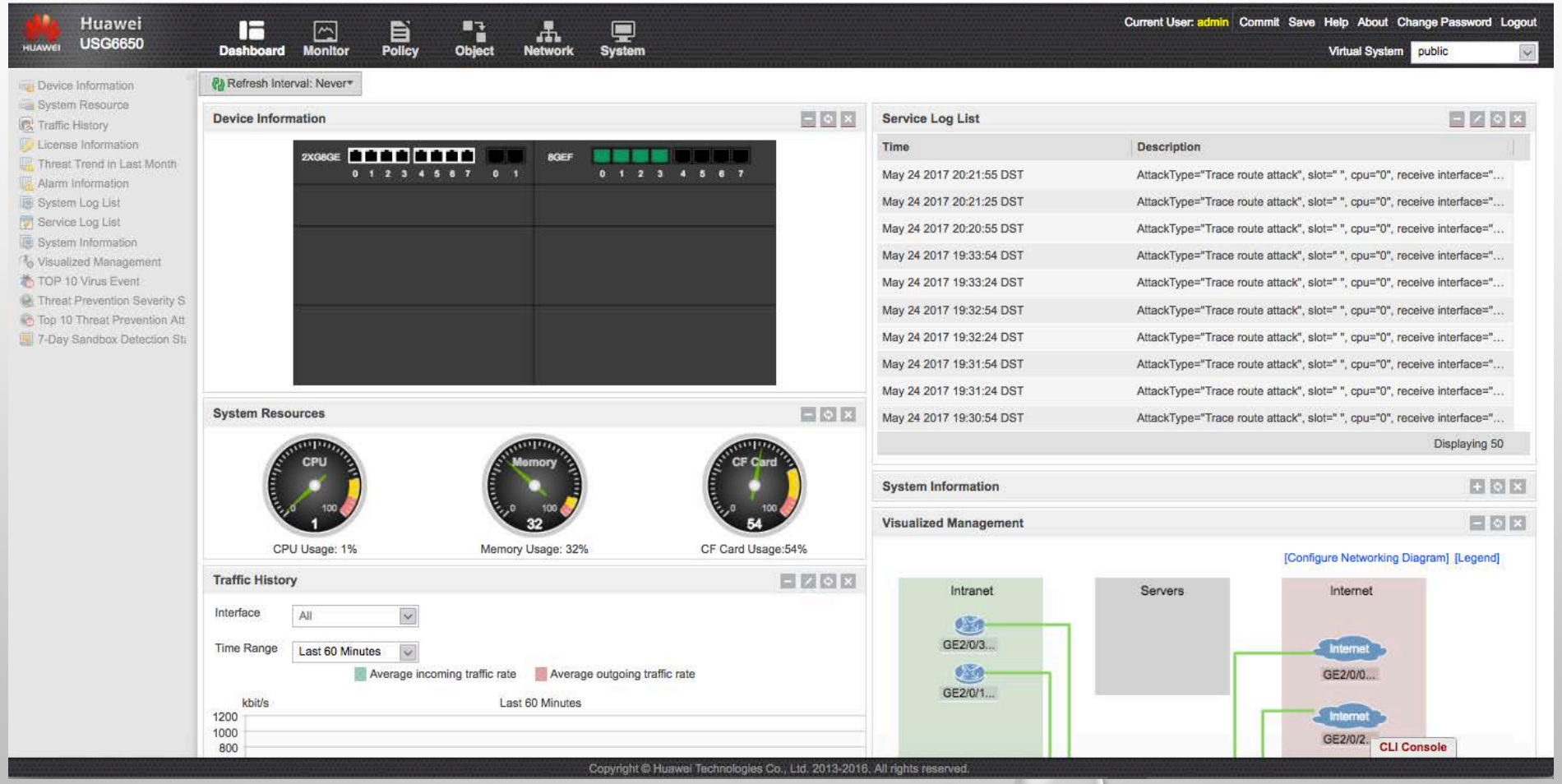
View	Time	Threat Type	Threat ID	Threat Name	Attacker	Victim	Source Addres...	Destination Addre...	Application	Protocol	Action	Security Policy
	DST 2017/05/24 22:15:57	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.154	216.21	131.154	216.218.21	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 22:15:57	Intrusion	332610	ISC BIND DNAME RRSIG Assert...	131.15	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	198.41.	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	216.218.21	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 21:51:45	Intrusion	324680	Apache Commons Collections U...	5.188.10	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...	5.188.1	131.1	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...	66.24	131.154	66.249.69.	131.154.12	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:40:57	Intrusion	2000019	Directory Traversal Attempt - Fo...	66.2	131.154	66.249.6	131.154.1	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:38:25	Attack	24	Smurf attack	46.	193.204 193.204	46.234	193.204 193.204		ICMP	Alert	
	DST 2017/05/24 21:37:56	Intrusion	260280	Adobe Acrobat and Reader Rem...	131	66.249.6	131.154	66.249.6	Googlebot	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 21:29:25	Intrusion	330680	GNU C Library getaddrinfo Buffer...	58.	131.154	58.65.2	131.154	DNS	UDP	Alert	PERMITALLIDS
	DST 2017/05/24 21:23:25	Attack	24	Smurf attack	46.234	193.204 193.204	46.234	193.204 193.204		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 :218	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	113.25	131.154	113.250	131.15	HTTP	TCP	Alert	PERMITALLIDS
	DST 2017/05/24 20:26:04	Intrusion	332280	Chinese Chopper Backdoor Traffic	113.25	131.154	113.250	131.15	HTTP	TCP	Alert	PERMITALLIDS

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

CLI Console

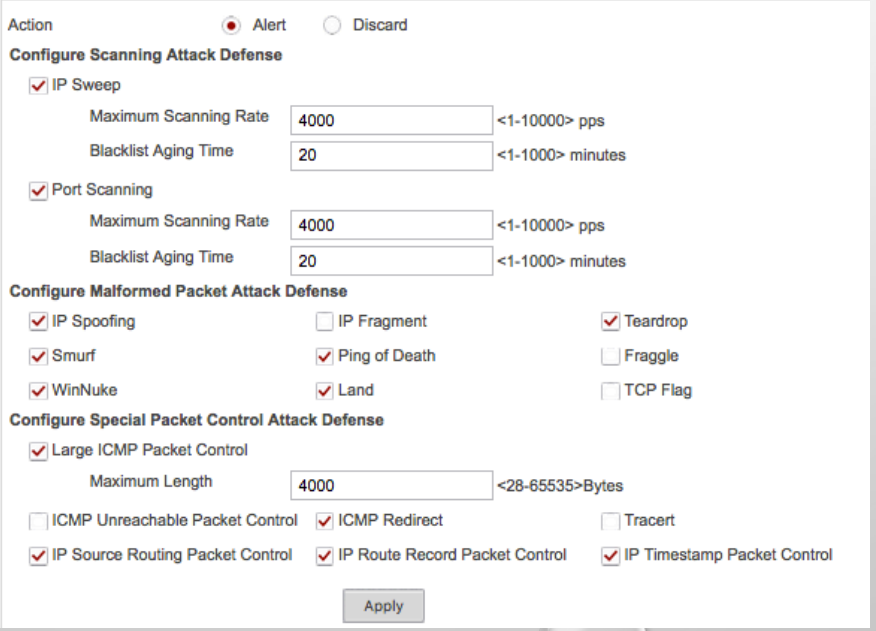
Copyright © Huawei Technologies Co., Ltd. 2013-2016. All rights reserved.

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

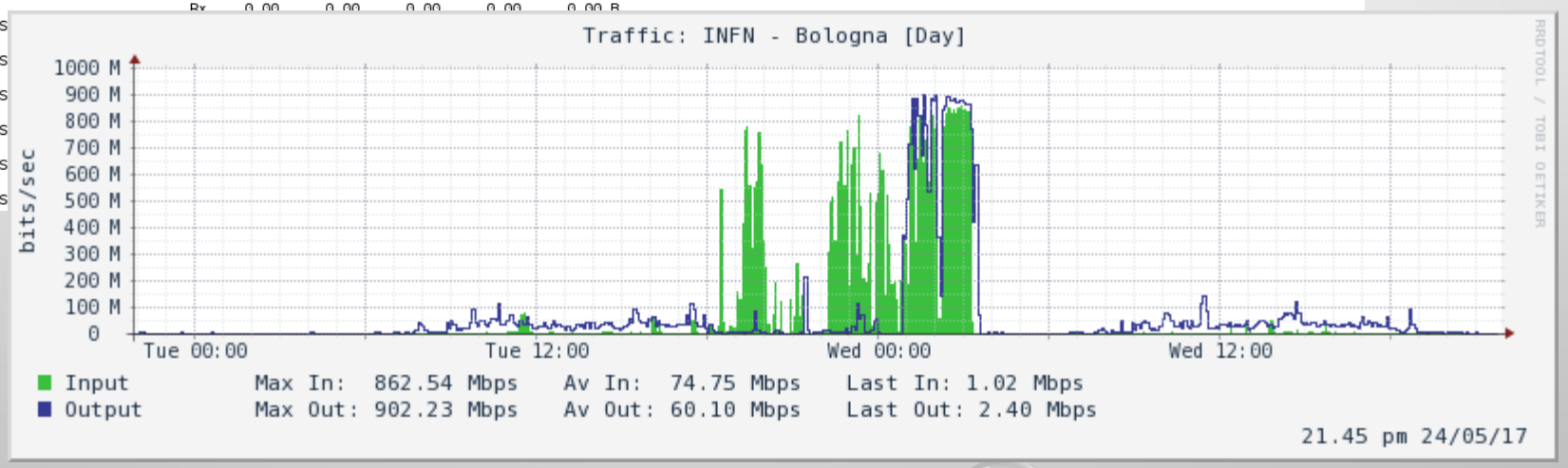


FALSI POSITIVI – NON FALSI

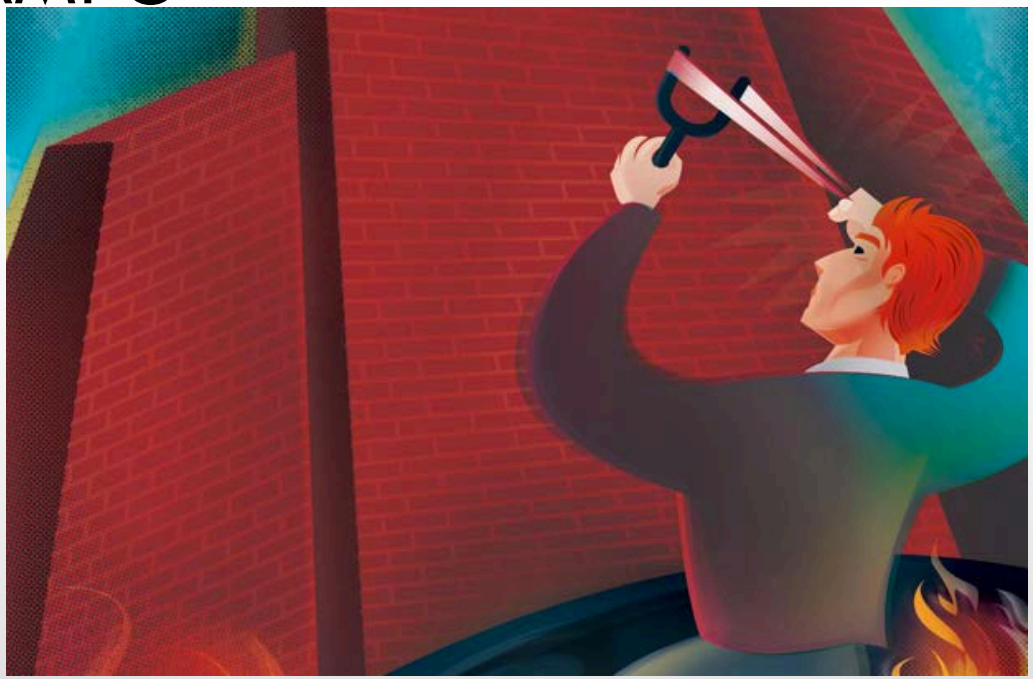
- ABBIAMO DOVUTO CREARE DELLE POLICY DI PERMIT SENZA LOG E SENZA IDS PER GLI HOST AUDIBO !!
- DURANTE UNA SCANSIONE ATTIVATA ON DEMAND HANNO TRIGGERATO MIGLIAIA DI EVENTI DI IDS, ANOMALY ETC.
- ABBIAMO CREATO UNA REGOLA AD-HOC PER IL TRAFFICO SSL BASED VERSO CNAF PERCHE' TRIGGERAVA FALSI POSITIVI SU APPLICATIVI DI ESPERIMENTO (USO PARTICOLARE DI CERTIFICATI X509)

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
RRDTOOL / TOBI OETIKER
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
RRDTOOL / TOBI OETIKER
Input
Max In: 862.54 Mbps
Av In: 74.75 Mbps
Last In: 1.02 Mbps
Output
Max Out: 902.23 Mbps
Av Out: 60.10 Mbps
Last Out: 2.40 Mbps
21.45 pm 24/05/17

NEXT GENERATION FIREWALL CONSIDERAZIONI GENERALI E PROVE SUL CAMPO



Credit: Stephen Sauer

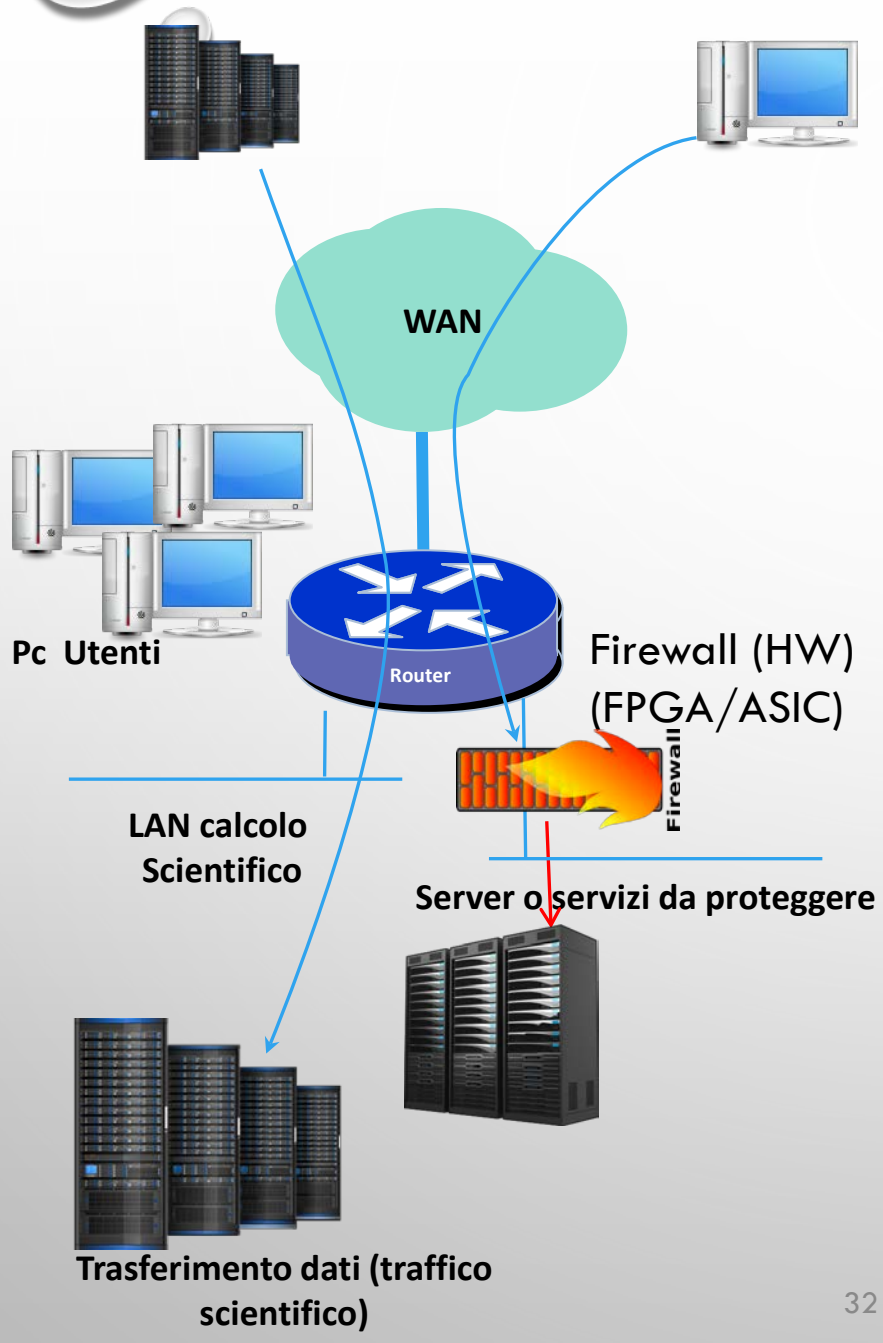
NETGROUP@CCR

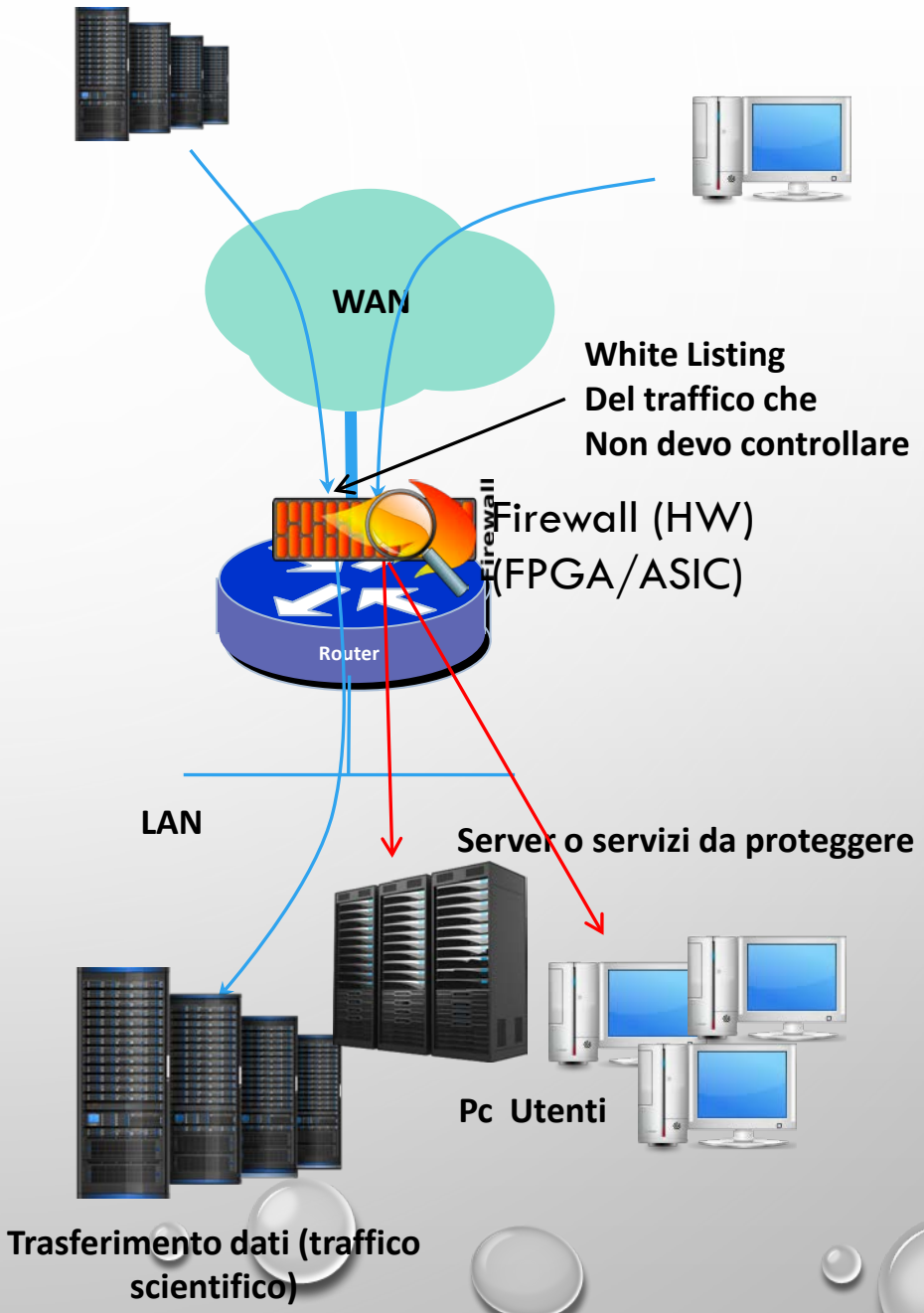
MASSIMO PISTONI (INFN LNF)

STEFANO ZANI (INFN CNAF)

WORKSHOP CCR

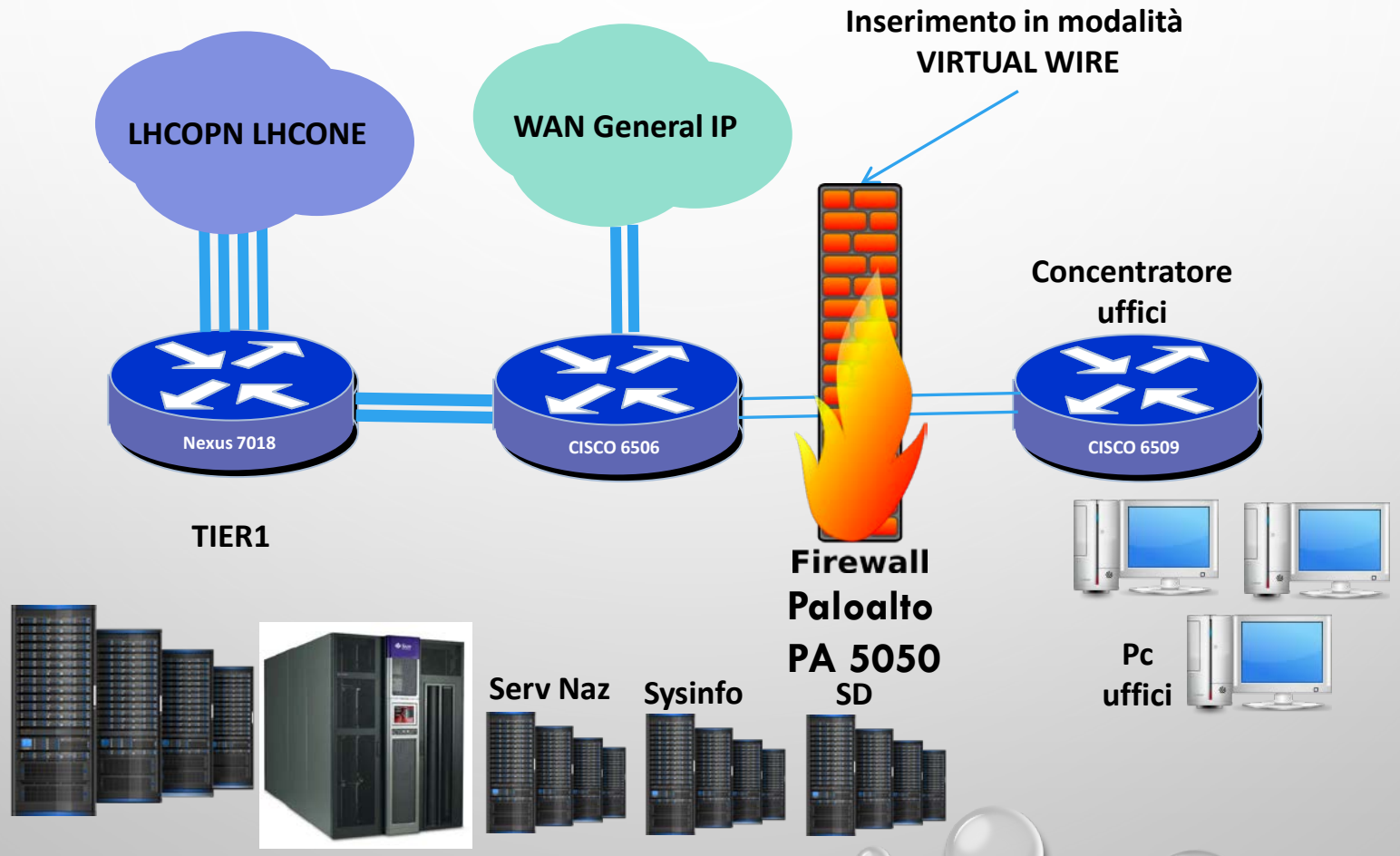
RIOPOLA, 17 MAGGIO 2016


WAN
Pc Utenti
Router
Firewall (HW)
(FPGA/ASIC)
Firewall
LAN calcolo
Scientifico
Server o servizi da proteggere
Trasferimento dati (traffico
scientifico)


WAN
White Listing
Del traffico che
Non devo controllare
Firewall
Firewall (HW)
(FPGA/ASIC)
Router
LAN
Server o servizi da proteggere
Pc Utenti
Trasferimento dati (traffico
scientifico)

Test sul campo

Posizionamento del firewall sulla rete di produzione del CNAF durante la prova

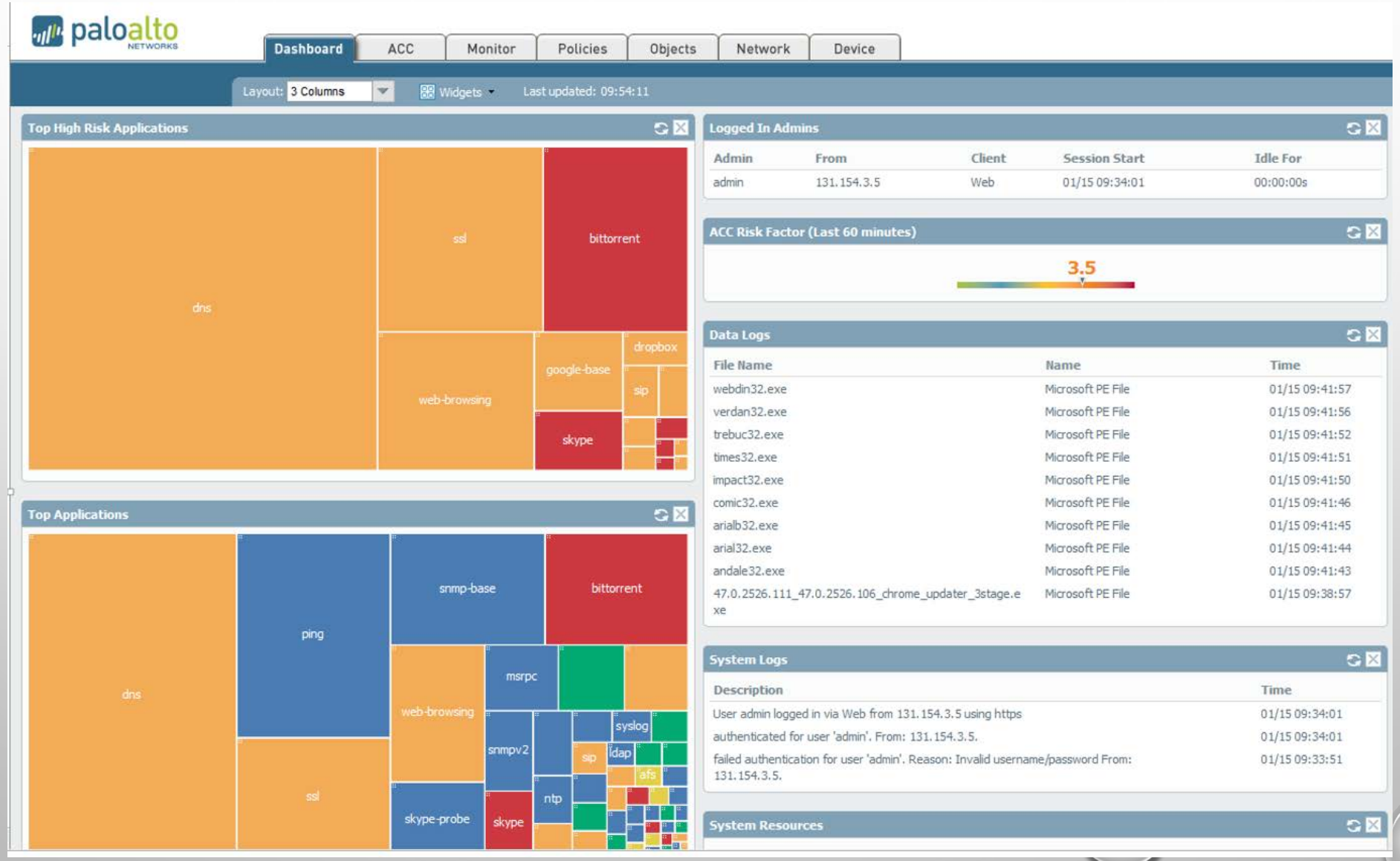


Test sul campo

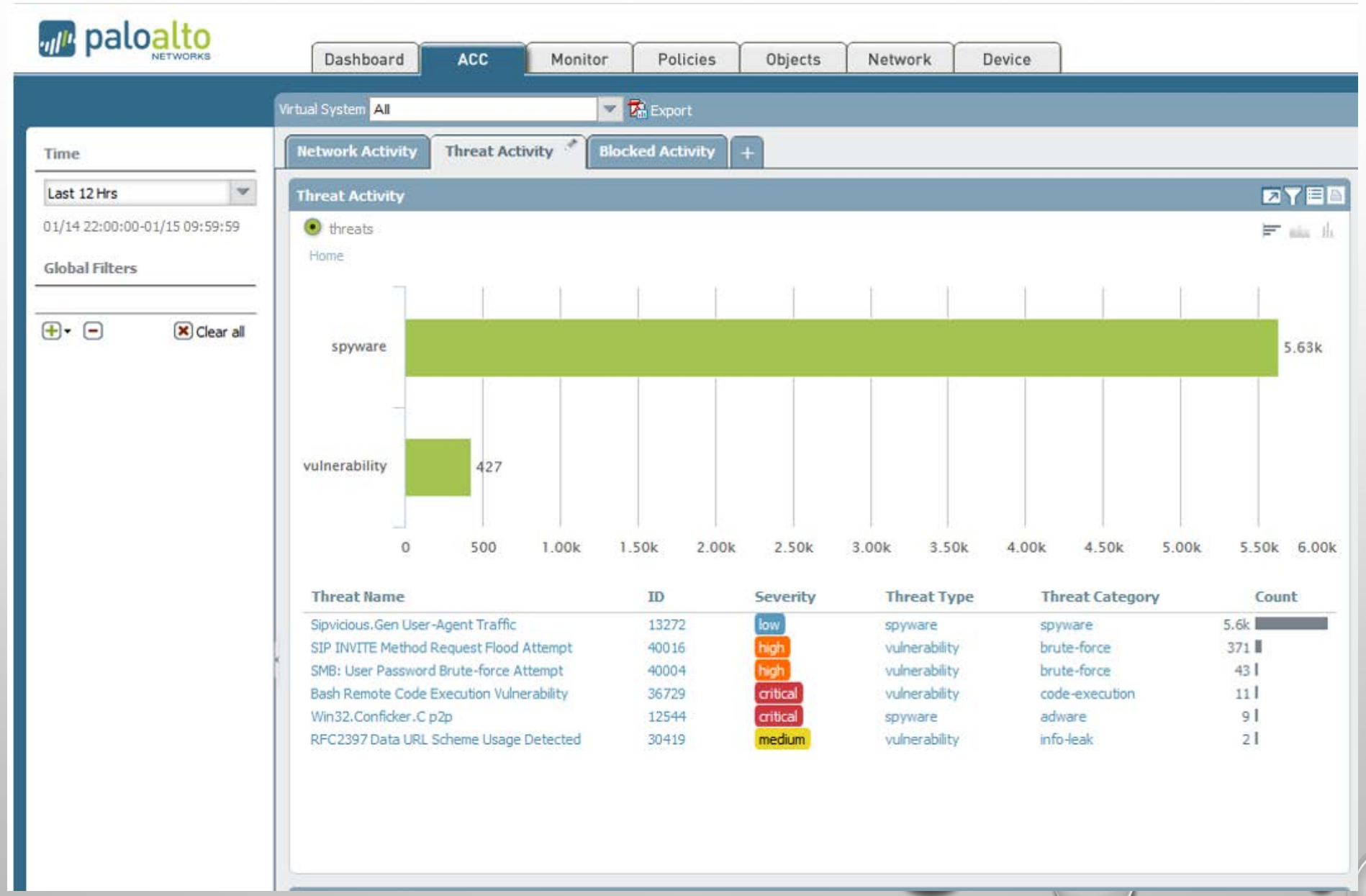
(Prime impressioni)

- Il firewall collegato in virtual wire a protezione degli uffici. E' stato configurato all'inizio in modalità "permit all" ma con tutte le funzioni di Threat prevention attive, in modo da definire le regole di "Blocking" Successivamente a mano.
- Nel giro di pochissimi minuti ha fornito un quadro della distribuzione del traffico che lo attraversava ed ha classificato secondo le sue regole di default i vari flussi a seconda della "Pericolosità".

Le dashboard danno l'idea a "Colpo d'occhio"di cosa stia avvenendo sulla rete

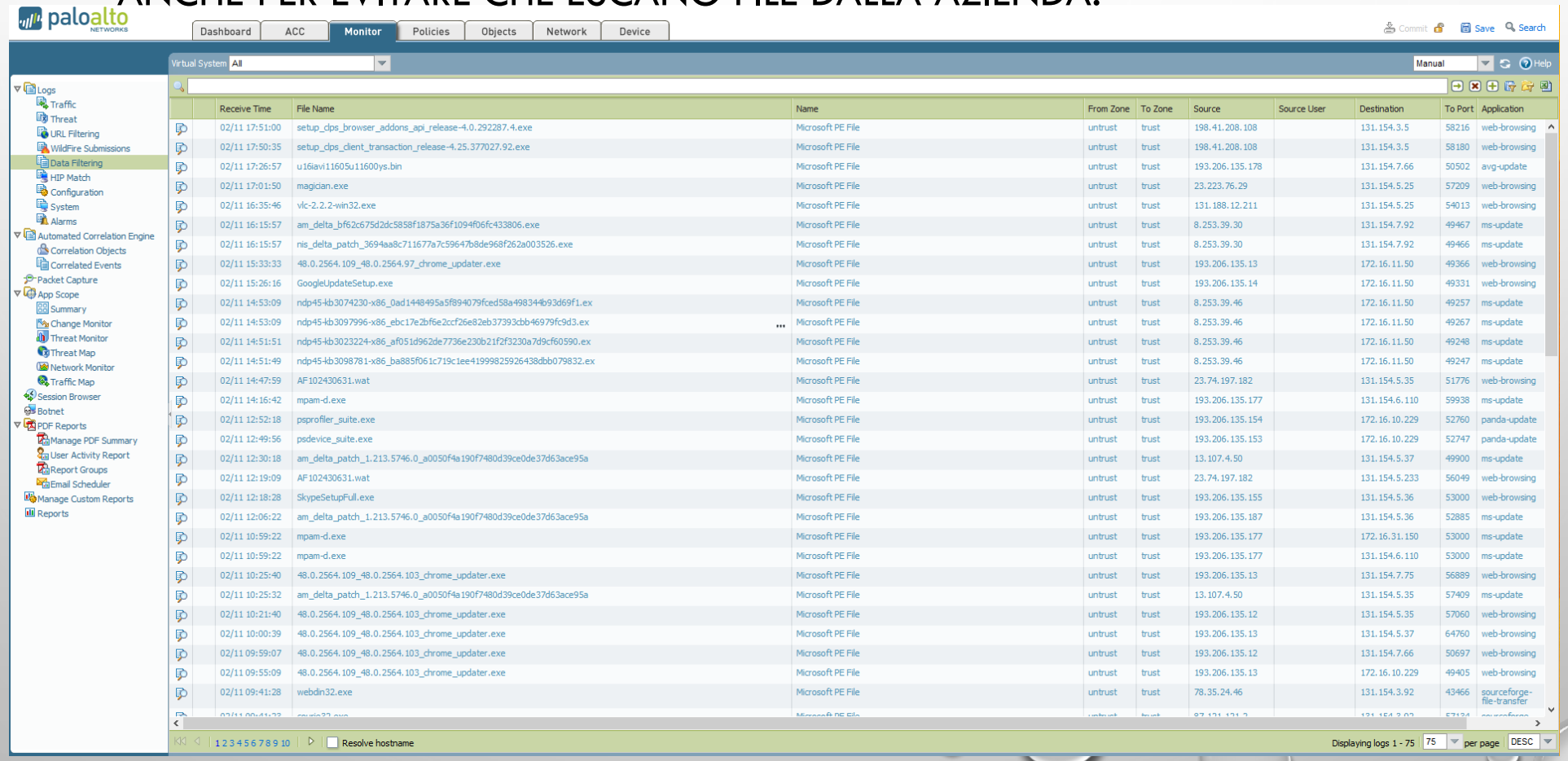


Individuazione e classificazione dei “threat” efficace



DATA FILTERING (FILE BLOCKING) ANTIVIRUS ONLINE

- SI PUÒ IMPOSTARE IL FIREWALL PER BLOCCARE IN AUTOMATICO I FILE ENTRANTI RITENUTI PERICOLOSI (FRA GLI ESEGUIBILI O POTENZIALMENTE ESEGUIBILI). PER ALTRE REALTÀ QUESTO SISTEMA PUÒ ESSERE UTILIZZATO ANCHE PER EVITARE CHE ESCANO FILE DALLA AZIENDA.



Receive Time	File Name	Name	From Zone	To Zone	Source	Source User	Destination	To Port	Application
02/11 17:51:00	setup_clps_browser_addons_api_release-4.0.292287.4.exe	Microsoft PE File	untrust	trust	198.41.208.108		131.154.3.5	58216	web-browsing
02/11 17:50:35	setup_clps_client_transaction_release-4.25.377027.92.exe	Microsoft PE File	untrust	trust	198.41.208.108		131.154.3.5	58180	web-browsing
02/11 17:26:57	u16iavi11605u11600ys.bin	Microsoft PE File	untrust	trust	193.206.135.178		131.154.7.66	50502	avg-update
02/11 17:01:50	magician.exe	Microsoft PE File	untrust	trust	23.223.76.29		131.154.5.25	57209	web-browsing
02/11 16:35:46	vlc-2.2.2-win32.exe	Microsoft PE File	untrust	trust	131.188.12.211		131.154.5.25	54013	web-browsing
02/11 16:15:57	am_delta_bf62c675d2dc5858f1875a36f1094f06fc433806.exe	Microsoft PE File	untrust	trust	8.253.39.30		131.154.7.92	49467	ms-update
02/11 16:15:57	nis_delta_patch_3694aa8c711677a7c59647b8de968f262a003526.exe	Microsoft PE File	untrust	trust	8.253.39.30		131.154.7.92	49466	ms-update
02/11 15:33:33	48.0.2564.109_48.0.2564.97_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.13		172.16.11.50	49366	web-browsing
02/11 15:26:16	GoogleUpdateSetup.exe	Microsoft PE File	untrust	trust	193.206.135.14		172.16.11.50	49331	web-browsing
02/11 14:53:09	ndp45-kb3074230-x86_0ad1448495a5f894079fced58a498344b93d69f1.ex	Microsoft PE File	untrust	trust	8.253.39.46		172.16.11.50	49257	ms-update
02/11 14:53:09	ndp45-kb3097996-x86_ebc17e2bf6e2ccf26e82eb37393cbb46979fc9d3.ex	Microsoft PE File	untrust	trust	8.253.39.46		172.16.11.50	49267	ms-update
02/11 14:51:51	ndp45-kb3023224-x86_af051d962de7736e230b21f2f3230a7d9cf60590.ex	Microsoft PE File	untrust	trust	8.253.39.46		172.16.11.50	49248	ms-update
02/11 14:51:49	ndp45-kb3098781-x86_ba885f061c719c1ee419998259264 38dbb079832.ex	Microsoft PE File	untrust	trust	8.253.39.46		172.16.11.50	49247	ms-update
02/11 14:47:59	AF102430631.wat	Microsoft PE File	untrust	trust	23.74.197.182		131.154.5.35	51776	web-browsing
02/11 14:16:42	mpam-d.exe	Microsoft PE File	untrust	trust	193.206.135.177		131.154.6.110	59938	ms-update
02/11 12:52:18	psprofiler_suite.exe	Microsoft PE File	untrust	trust	193.206.135.154		172.16.10.229	52760	panda-update
02/11 12:49:56	psdevice_suite.exe	Microsoft PE File	untrust	trust	193.206.135.153		172.16.10.229	52747	panda-update
02/11 12:30:18	am_delta_patch_1.213.5746.0_a0050f4a190f7480d39ce0de37d63ace95a	Microsoft PE File	untrust	trust	13.107.4.50		131.154.5.37	49900	ms-update
02/11 12:19:09	AF102430631.wat	Microsoft PE File	untrust	trust	23.74.197.182		131.154.5.233	56049	web-browsing
02/11 12:18:28	SkypeSetupFull.exe	Microsoft PE File	untrust	trust	193.206.135.155		131.154.5.36	53000	web-browsing
02/11 12:06:22	am_delta_patch_1.213.5746.0_a0050f4a190f7480d39ce0de37d63ace95a	Microsoft PE File	untrust	trust	193.206.135.187		131.154.5.36	52885	ms-update
02/11 10:59:22	mpam-d.exe	Microsoft PE File	untrust	trust	193.206.135.177		172.16.31.150	53000	ms-update
02/11 10:59:22	mpam-d.exe	Microsoft PE File	untrust	trust	193.206.135.177		131.154.6.110	53000	ms-update
02/11 10:25:40	48.0.2564.109_48.0.2564.103_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.13		131.154.7.75	56889	web-browsing
02/11 10:25:32	am_delta_patch_1.213.5746.0_a0050f4a190f7480d39ce0de37d63ace95a	Microsoft PE File	untrust	trust	13.107.4.50		131.154.5.35	57409	ms-update
02/11 10:21:40	48.0.2564.109_48.0.2564.103_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.12		131.154.5.35	57060	web-browsing
02/11 10:00:39	48.0.2564.109_48.0.2564.103_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.13		131.154.5.37	64760	web-browsing
02/11 09:59:07	48.0.2564.109_48.0.2564.103_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.12		131.154.7.66	50697	web-browsing
02/11 09:55:09	48.0.2564.109_48.0.2564.103_chrome_updater.exe	Microsoft PE File	untrust	trust	193.206.135.13		172.16.10.229	49405	web-browsing
02/11 09:41:28	webdin32.exe	Microsoft PE File	untrust	trust	78.35.24.46		131.154.3.92	43466	sourceforge-file-transfer

Principali caratteristiche della piattaforma Paloalto in prova (PA 5050)

- Piattaforma bi alimentata e con totale **separazione hardware del control plane dal data plane** (Sempre gestibile anche sotto attacco ed a full rate)
- 12x 1Gb SFP ports + 4X 10Gb SFP+ ports
  - Max Throughput 10Gb/s (5Gb/s Full threat prevention)
- Possibilità di dividere il firewall in **sistemi virtuali** indipendenti (fino a 125).
- Routing (RIP,OSPF, BGP) – **Può funzionare come ROUTER**
- VPN (Lan to Lan o funzionalità di VPN concentrator)
- Possibilità di funzionare in modalità **Virtual Wire, L2 ed L3 (Routing) contemporaneamente** senza dovere partizionare il FW in differenti contesti virtuali.
- Supporto di IPv6
- Implementazione di QoS sul traffico che lo attraversa(Traffic shaping)
- Utilizzo di FPGA (Quindi HW Riprogrammabile): Con gli aggiornamenti si può cambiare anche il comportamento dell'HW.
- Possibilità di funzionare in HA (clustering)

Principali caratteristiche della piattaforma Paloalto in prova (PA 5050)

- **Application Matching** Classificazione delle applicazioni indipendentemente dalle porte utilizzate in hardware (utilizzo delle applicazioni come criterio di matching).
- Possibilità di creazione della "signature" di una applicazione custom sconosciuta al sistema (cattura del traffico e profilazione)
- **IDS ed IPS integrato.**
  - Riconoscimento dei "Threat" dovuti ad attacchi automatici, virus, worm, malware, spyware con aggiornamento automatico delle signature (dei comportamenti sospetti sulla rete).
- **FILE BLOCKING** <u>anche su determinate applicazioni specifiche</u>.
- URL Filtering (allo scopo di bloccare le connessioni verso siti pericolosi attraverso un servizio di DB dei siti considerati fonte di malware o "threats" In generale)
  - **Si può uitilizzare anche una URL category come criterio di matching** (Posso per esempio applicare regole di antivirus solo per URL relative a determinate categorie di sito).
- Meccanismi di **protezione dai DoS** (Denial of Service) in modo da mantenere utilizzabile un servizio sotto attacco, riconoscendo e fermando solo i flussi di traffico "Malevolo" o comunque mitigando l'effetto del DoS.
- Sistema di logging e reportistica avanzata integrati (senza bisogno di ricorrere a componenti aggiuntivi)
- Tool automatico per la conversione delle ACL CISCO in regole da applicare sul Paloalto (anche se ovviamente consigliano di riscriverle comunque da zero vista la enorme differenza di filosofia della piattaforma)

CONCLUSIONI

IN GENERALE L'ADOZIONE DI UN NEXT GENERATION FIREWALL È CERTAMENTE DI GRANDE AIUTO NELLA GESTIONE DELLA SICUREZZA.

LA DEFINIZIONE DI ACL COMPLESSE HA ORMAI RAGGIUNTO IL LIMITE HARDWARE DEL ROUTER DI FRONTIERA DEL CNAF (E MI DICONO CHE ANCHE LNF STA SOFFRENDO SU QUESTO PUNTO)

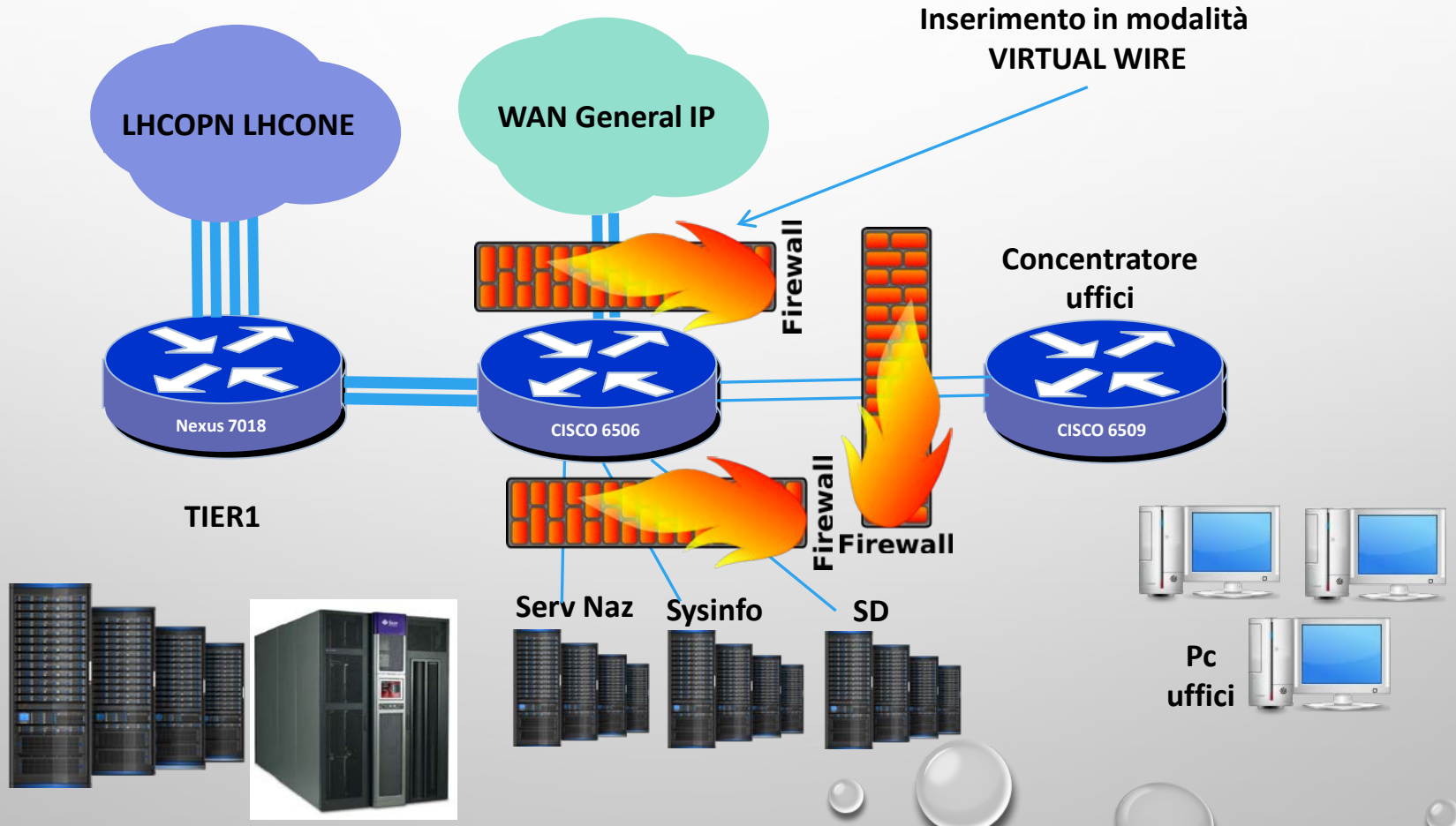
LE "FEATURE" PRINCIPALMENTE LEGATE ALLA CAPACITÀ DI RILEVARE ATTACCHI DALLA **ANALISI DEL COMPORTAMENTO** DELLE APPLICAZIONI SULLA RETE RENDONO QUESTO STRUMENTO ENORMEMENTE PIÙ POTENTE RISPETTO AI FIREWALL DI VECCHIA GENERAZIONE.

IL SISTEMA DI BLOCCO AUTOMATICO DEI TENTATIVI DI INTRUSIONE OLTRE A COSTITUIRE UN OTTIMO SISTEMA DI INTRUSION DETECTION, DA IL TEMPO EVENTUALMENTE DI METTERE IN SICUREZZA I SISTEMI VULNERABILI MANTENENDO IN SICUREZZA IL CENTRO.

PER QUANTO RIGUARDA LA PIATTAFORMA PALOALTO NELLO SPECIFICO IL SISTEMA DI RIFERIMENTO PER IL CNAF SAREBBE IL PA 5060.

CONCLUSIONI

PER QUANTO RIGUARDA IL CNAF NELLO SPECIFICO, L'IDEALE È INSTALLARLO FRA IL ROUTER DI FRONTIERA ED IL ROUTER DEL GARR IN MODO DA PROTEGGERE ANCHE IL ROUTER STESSO, TUTTI I SERVIZI NAZIONALI, IL SISTEMA INFORMATIVO ED I PC DEI DIPENDENTI (ESCLUDENDO IL TRAFFICO RELATIVO AL TRASFERIMENTO DATI SCIENTIFICI)



41

GRAZIE

UN RINGRAZIAMENTO A STEFANO ZANI E MASSIMO PISTONI PER LA COLLABORAZIONE E LA CONCESSIONE DELLE SLIDE

Q&A