Modeling network data traffic for vulnerability scan using the TrafficREWIND test bench infrastructure of TIER1 data centers at JINR

Andrey Baginyan
Laboratory of information technologies
Joint Institute for Nuclear Research
Dubna, Russia
bag@jinr.ru

Andrey Dolbilov
Laboratory of information technologies
Joint Institute for Nuclear Research
Dubna, Russia
dolbilov@jinr.ru

Anton Balandin
Laboratory of information technologies
Joint Institute for Nuclear Research
Dubna, Russia
golter@jinr.ru

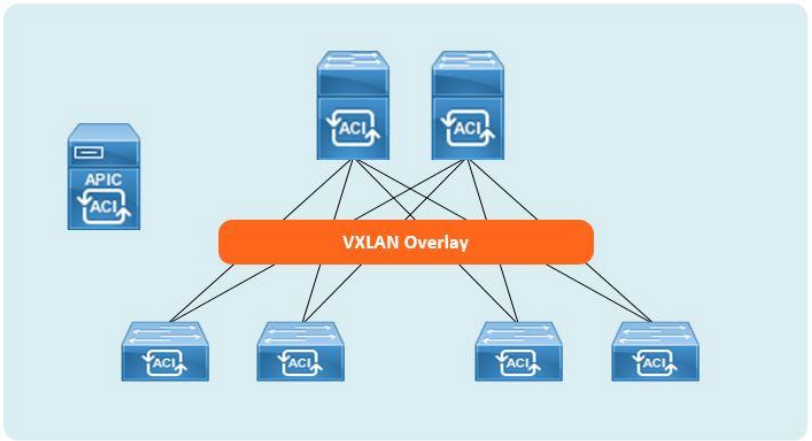
Ivan Kashunin
Laboratory of information technologies
Joint Institute for Nuclear Research
Dubna, Russia
miramir@jinr.ru

Vladimir Korenkov
Laboratory of information technologies
Joint Institute for Nuclear Research
Dubna, Russia
korenkov@jinr.ru

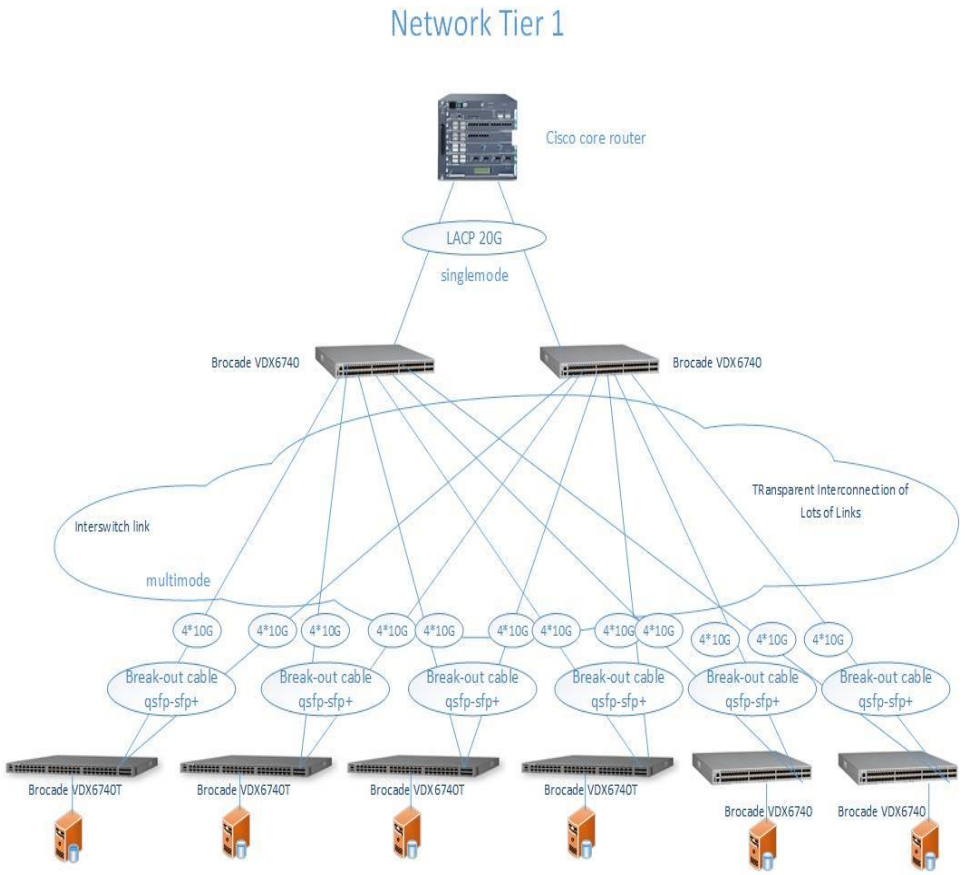
GRID’2021

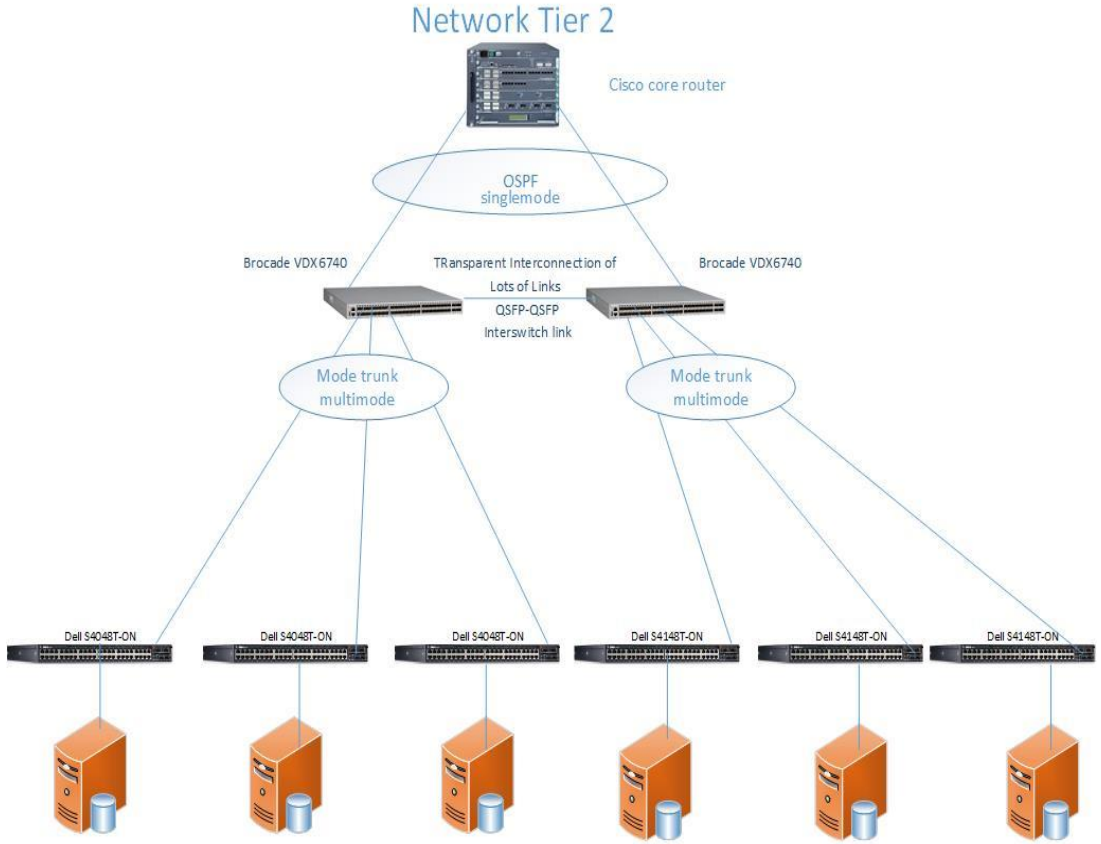
JINR Network infrastructure consists of three main parts:

1) JINR Local Area Network (Backbone),
2) MICC (Multifunctional Information and Computing Complex) Network,
3) external channels - JINR Telecommunication Channels.



The EOS distributed file system,
the HybriLIT heterogeneous platform,
the Govorun supercomputer,
WEB services,
Tier-2, Tier-1,
Cloud computing networks
are connected to the ACI factory.





Provide interaction between 160 disk servers, 25 blade servers, 100 infrastructure servers, and a tape robot.
The first module contains 80 disk storage servers (with 160 10G-ports in bonding mode), 15 blade servers
(30 of 10G-ports in bonding mode), 60 servers infrastructure (with 40 10G-ports and 40 1G-ports in bonding mode).
The data center network segment provides 230 10G-ports and 40 1G-ports.

Coloring data

It can be implemented with the help of

variable length subnet masks

Deep Packet Inspection (DPI)

additional fields in the transmitted frame “quality of service” (QoS)

One of the newest ways is the method of mirroring visualizing the network at the application level (OSI model level 7)

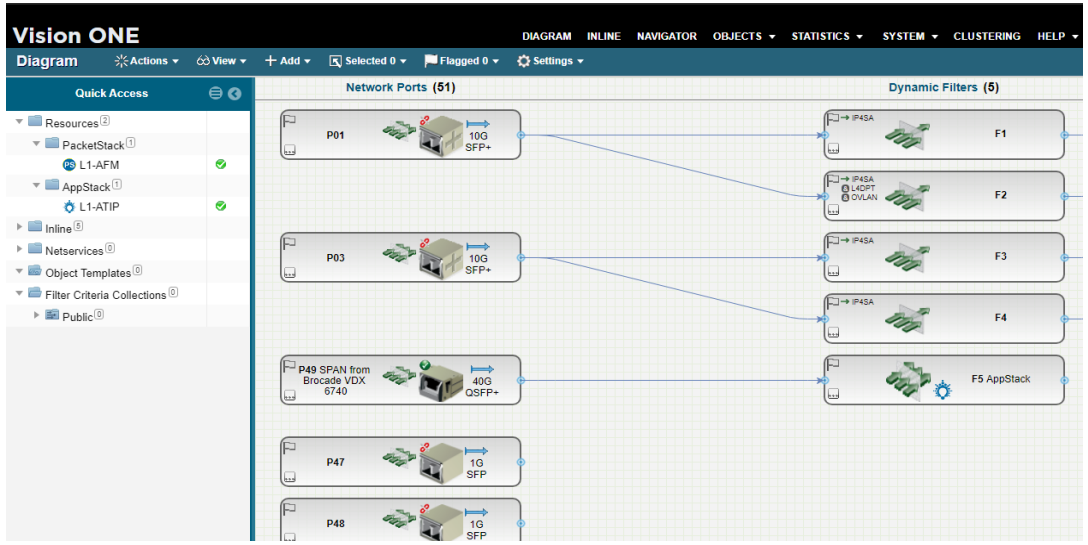
Construction of modern networks for intercepting and distributing traffic in order to increase the efficiency of monitoring systems, security systems and data control

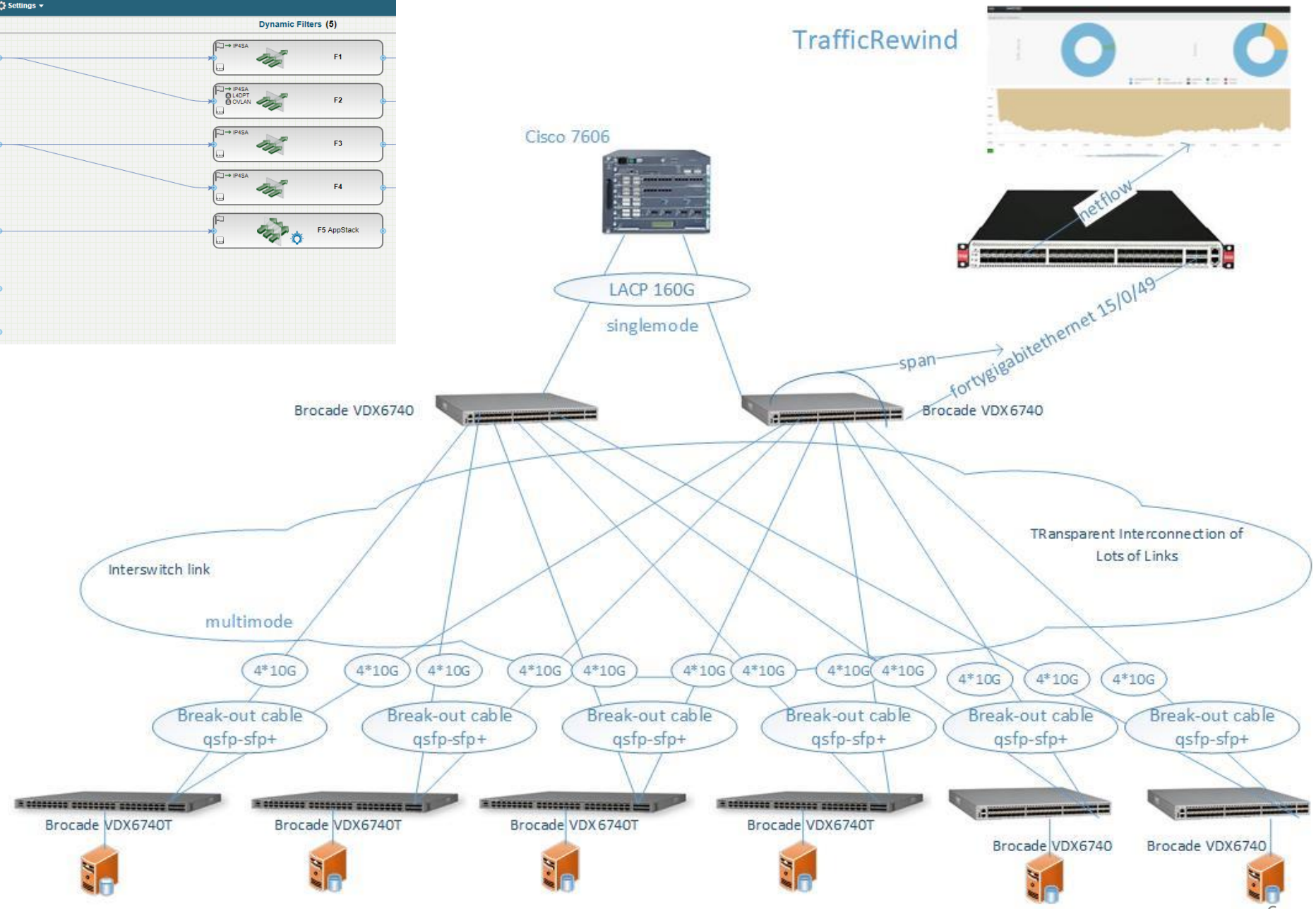
Load testing is an effective tool for the implementation, operation and development of networks and services

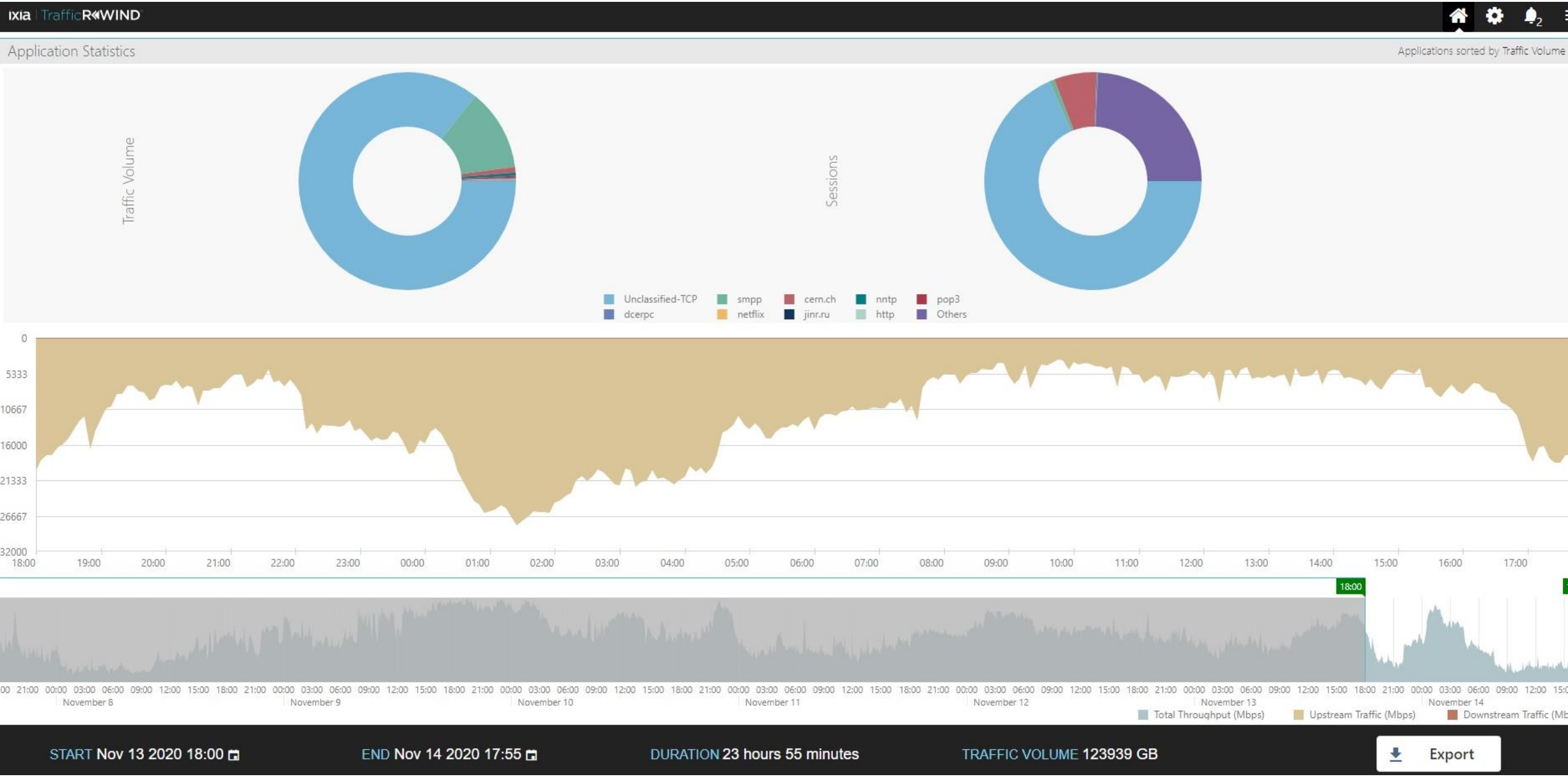
Testing the effectiveness of information security systems under load

Functional testing and analysis of information security tools, testing the security and performance of these systems

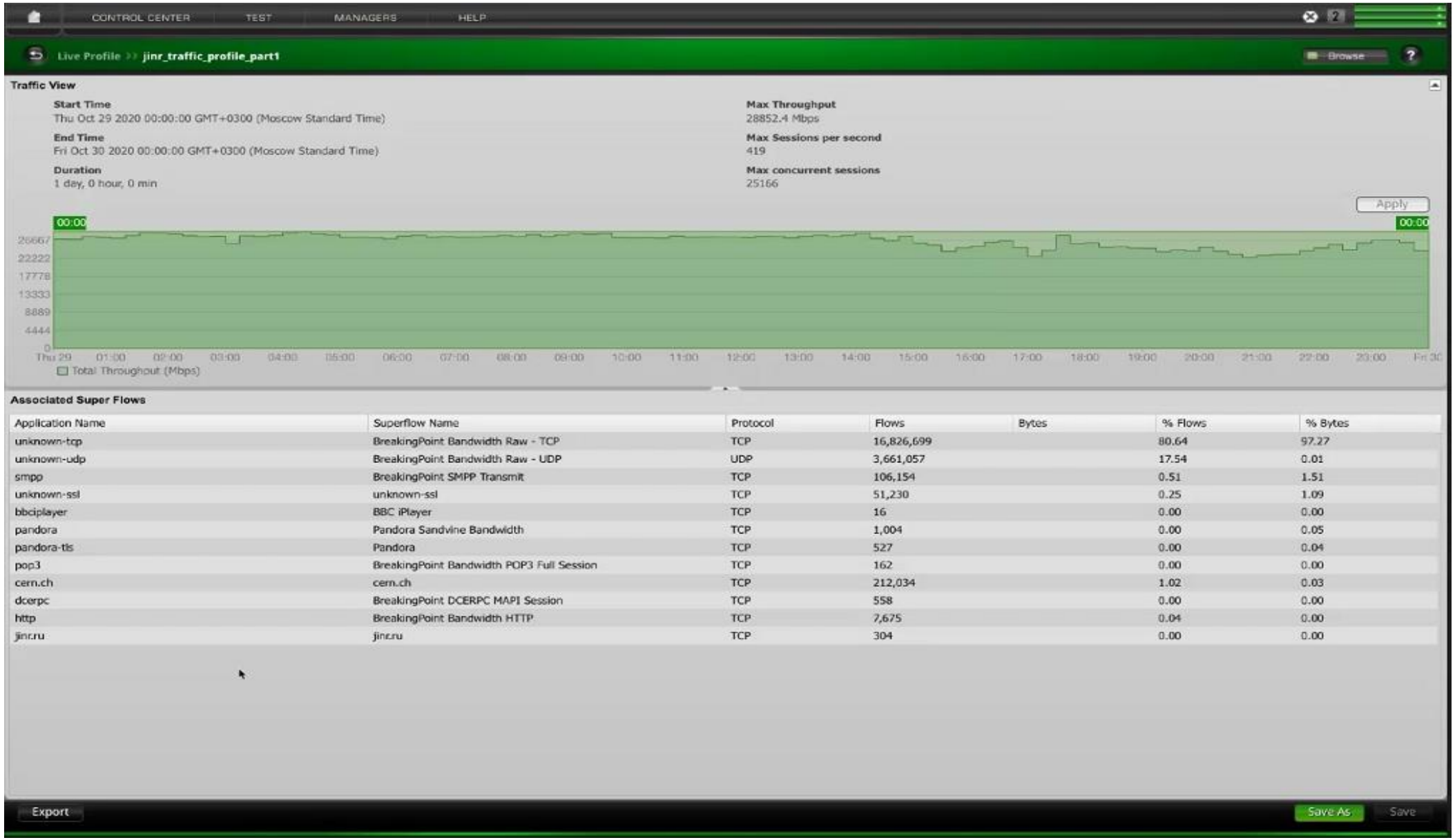
Cybersecurity services


Vision ONE
DIAGRAM INLINE NAVIGATOR OBJECTS STATISTICS SYSTEM CLUSTERING HELP
Diagram
Actions View Add Selected 0 Flagged 0 Settings
Quick Access
Resources
PacketStack
L1-AFM
AppStack
L1-ATIP
Inline
Netservices
Object Templates
Filter Criteria Collections
Public
Network Ports (51)
Dynamic Filters (5)
P01
10G SFP+
P03
10G SFP+
P49 SPAN from Brocade VDX 6740
40G QSFP+
P47
1G SFP
P48
1G SFP
F1
F2
F3
F4
F5 AppStack

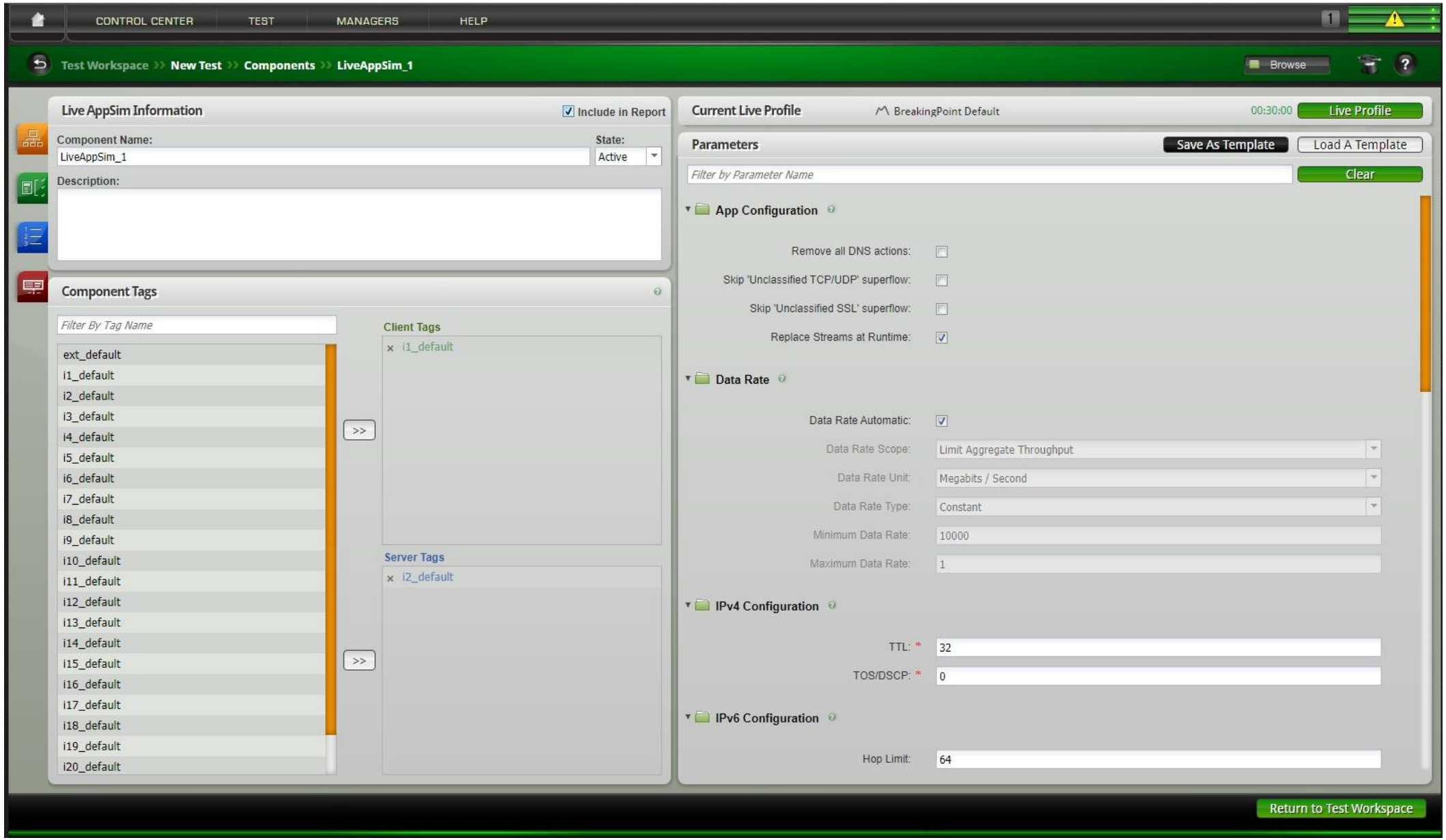

TrafficRewind
Cisco 7606
netflow
LACP 160G
singlemode
span
fortygigabitethernet 15/0/49
Brocade VDX6740
Brocade VDX6740
TRansparent Interconnection of Lots of Links
Interswitch link
multimode
4*10G
Break-out cable qsfp-sfp+
Brocade VDX6740T
Brocade VDX6740T
Brocade VDX6740T
Brocade VDX6740T
Brocade VDX6740
Brocade VDX6740


ixia | TrafficRewind
Application Statistics
Applications sorted by Traffic Volume
Traffic Volume
Sessions
Unclassified-TCP
smpp
cern.ch
nntp
pop3
dcerpc
netflix
jinr.ru
http
Others
0
5333
10667
16000
21333
26667
32000
18:00
19:00
20:00
21:00
22:00
23:00
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
November 8
November 9
November 10
November 11
November 12
November 13
November 14
Total Throughput (Mbps)
Upstream Traffic (Mbps)
Downstream Traffic (Mb
START Nov 13 2020 18:00
END Nov 14 2020 17:55
DURATION 23 hours 55 minutes
TRAFFIC VOLUME 123939 GB
Export

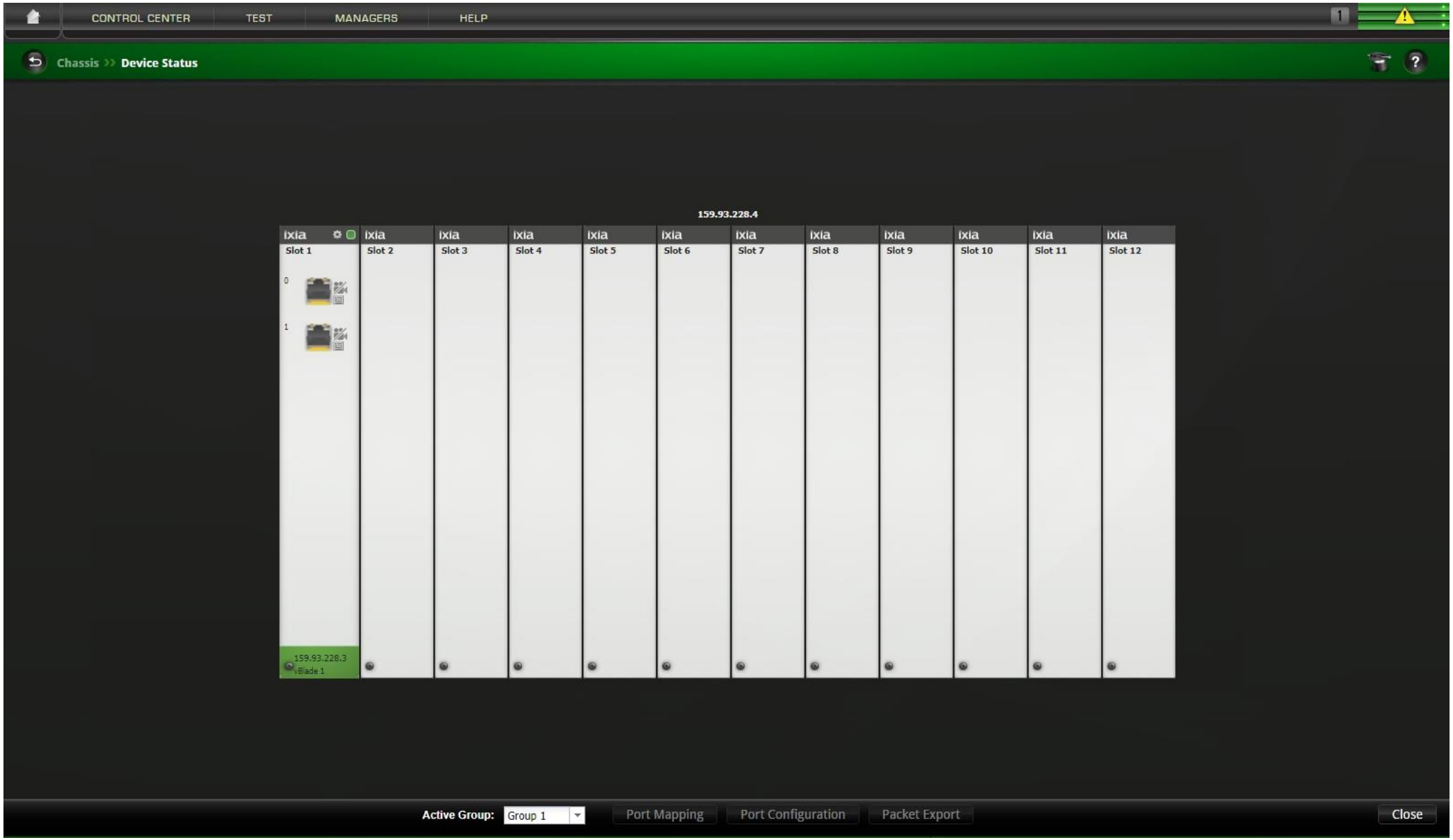
VOLUME, PROTOCOL, FLOW



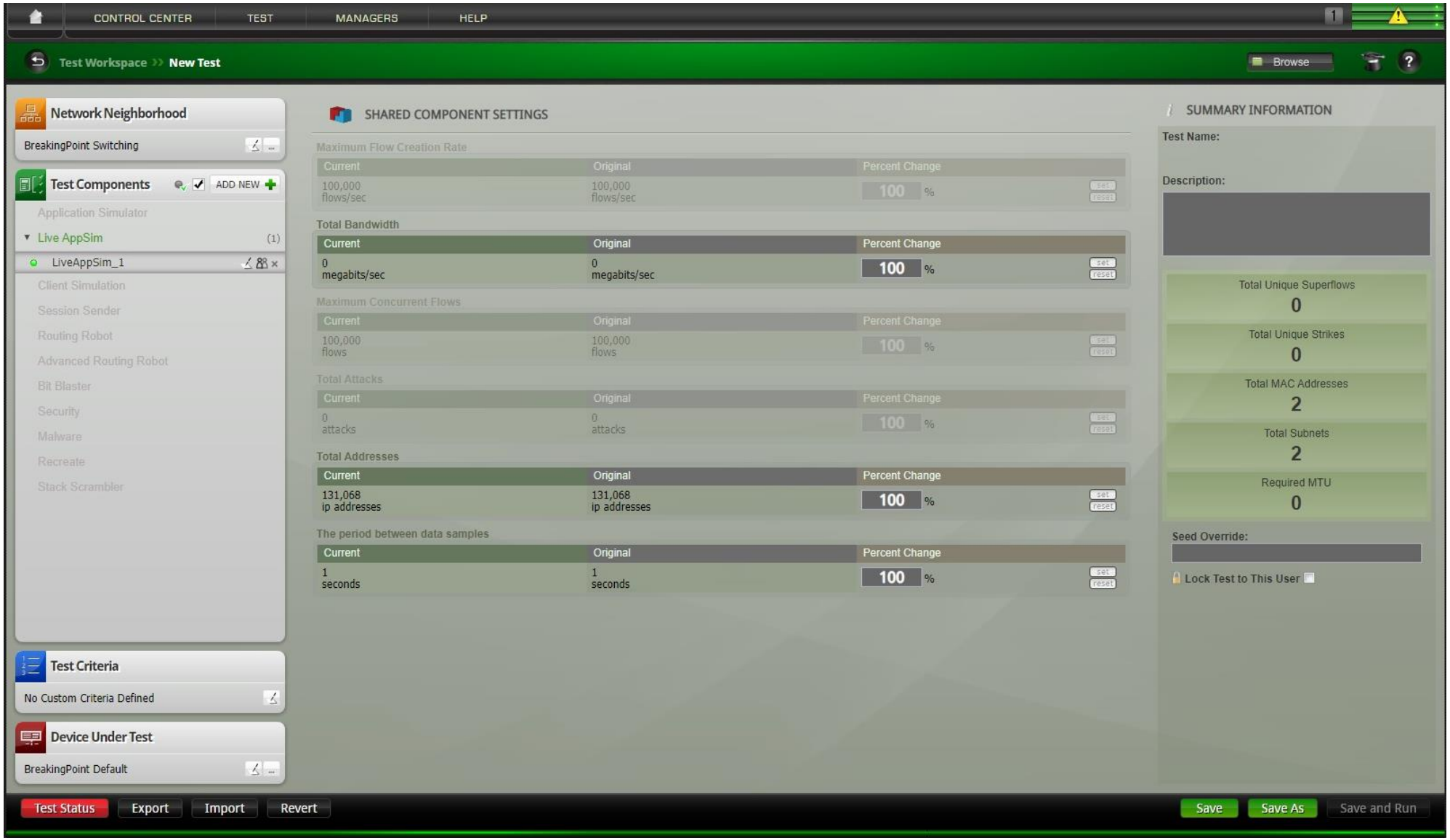
Layout preparation



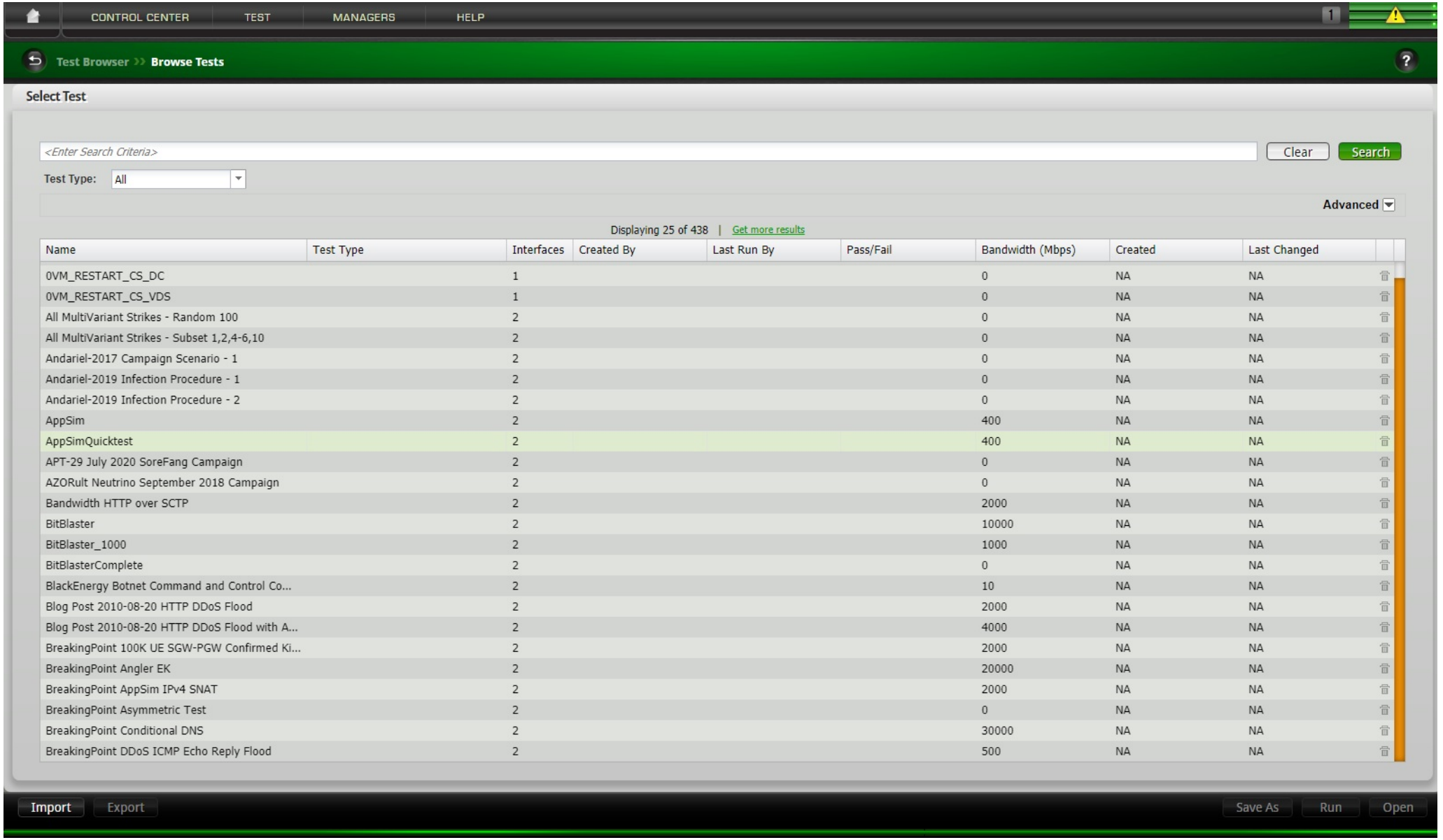
Interface status

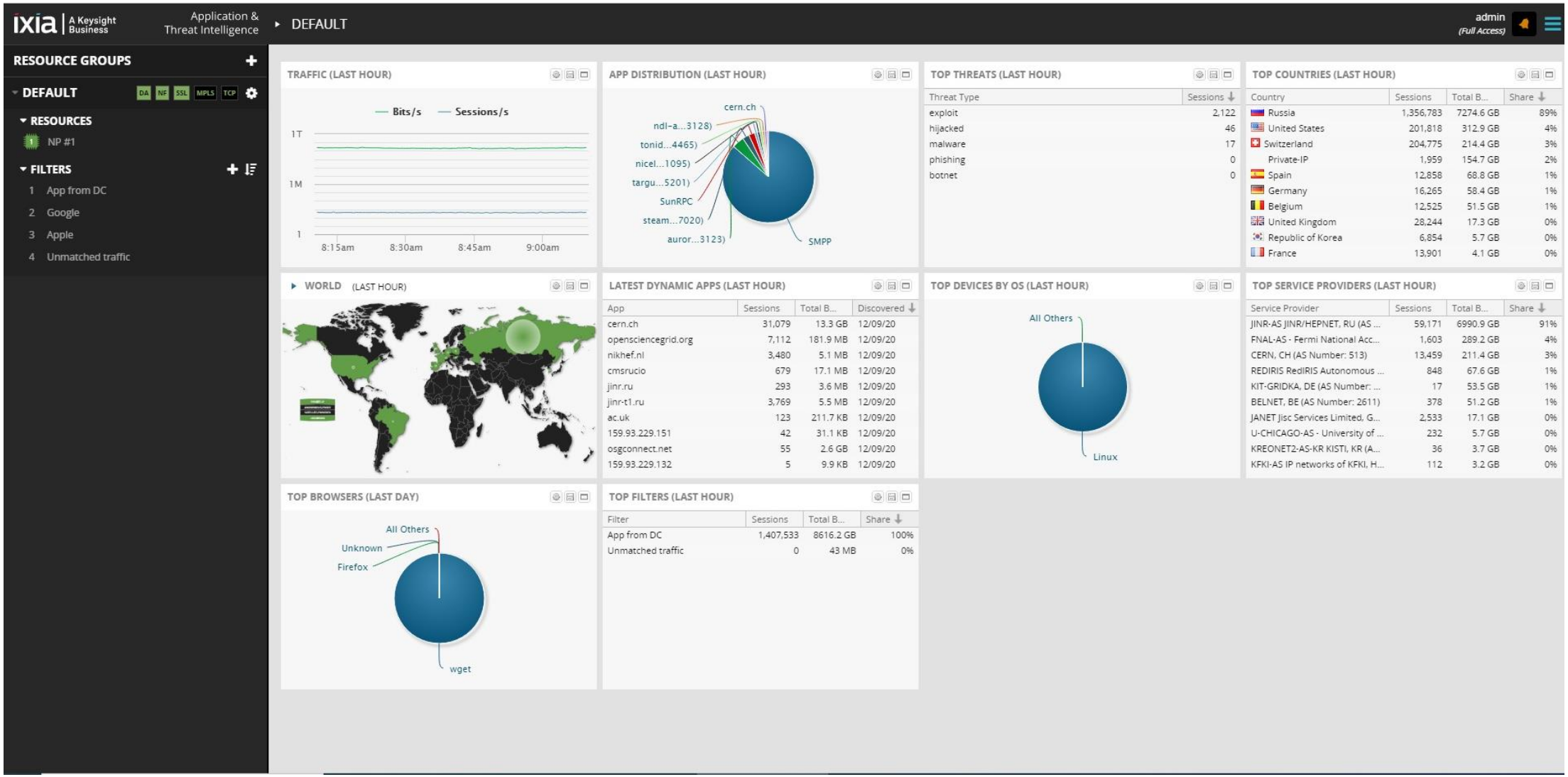


Test criteria, test components



Tests browser




ixia | A Keysight Business
Application & Threat Intelligence
DEFAULT
admin
(Full Access)
RESOURCE GROUPS
DEFAULT
DA NF SSL MPLS TCP
RESOURCES
NP #1
FILTERS
1 App from DC
2 Google
3 Apple
4 Unmatched traffic
TRAFFIC (LAST HOUR)
Bits/s
Sessions/s
1T
1M
1
8:15am
8:30am
8:45am
9:00am
APP DISTRIBUTION (LAST HOUR)
cern.ch
ndl-a...3128)
tonid...4465)
nicel...1095)
targu...5201)
SunRPC
steam...7020)
auror...3123)
SMPP
TOP THREATS (LAST HOUR)
Threat Type
Sessions
exploit 2,122
hijacked 46
malware 17
phishing 0
botnet 0
TOP COUNTRIES (LAST HOUR)
Country
Sessions
Total B...
Share
Russia 1,356,783 7274.6 GB 89%
United States 201,818 312.9 GB 4%
Switzerland 204,775 214.4 GB 3%
Private-IP 1,959 154.7 GB 2%
Spain 12,858 68.8 GB 1%
Germany 16,265 58.4 GB 1%
Belgium 12,525 51.5 GB 1%
United Kingdom 28,244 17.3 GB 0%
Republic of Korea 6,854 5.7 GB 0%
France 13,901 4.1 GB 0%
WORLD (LAST HOUR)
LATEST DYNAMIC APPS (LAST HOUR)
App
Sessions
Total B...
Discovered
cern.ch 31,079 13.3 GB 12/09/20
opensciencegrid.org 7,112 181.9 MB 12/09/20
nikhef.nl 3,480 5.1 MB 12/09/20
cmsrucio 679 17.1 MB 12/09/20
jinr.ru 293 3.6 MB 12/09/20
jinr-t1.ru 3,769 5.5 MB 12/09/20
ac.uk 123 211.7 KB 12/09/20
159.93.229.151 42 31.1 KB 12/09/20
osgconnect.net 55 2.6 GB 12/09/20
159.93.229.132 5 9.9 KB 12/09/20
TOP DEVICES BY OS (LAST HOUR)
All Others
Linux
TOP SERVICE PROVIDERS (LAST HOUR)
Service Provider
Sessions
Total B...
Share
JINR-AS JINR/HEPNET, RU (AS ... 59,171 6990.9 GB 91%
FNAL-AS - Fermi National Acc... 1,603 289.2 GB 4%
CERN, CH (AS Number: 513) 13,459 211.4 GB 3%
REDIRIS RedIRIS Autonomous ... 848 67.6 GB 1%
KIT-GRIDKA, DE (AS Number: ... 17 53.5 GB 1%
BELNET, BE (AS Number: 2611) 378 51.2 GB 1%
JANET Jisc Services Limited, G... 2,533 17.1 GB 0%
U-CHICAGO-AS - University of ... 232 5.7 GB 0%
KREONET2-AS-KR KISTI, KR (A... 36 3.7 GB 0%
KFKI-AS IP networks of KFKI, H... 112 3.2 GB 0%
TOP BROWSERS (LAST DAY)
All Others
Unknown
Firefox
wget
TOP FILTERS (LAST HOUR)
Filter
Sessions
Total B...
Share
App from DC 1,407,533 8616.2 GB 100%
Unmatched traffic 0 43 MB 0%

Thank you