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 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



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





IXIA TrafficR«WIND

7

#### 

## VOLUME, PROTOCOL, FLOW

CONTROL CENTER TEST	MANAGERS HELP.					
S Live Profile >> jinr_traffic_profile_part1						Browse ?
Traffic View						
Start Time           Thu Oct 29 2020 00:00:00 GMT+0300 (Moscow S           End Time           Fri Oct 30 2020 00:00:00 GMT+0300 (Moscow State           Duration	tandard Time) Indard Time)	Max Throughpu 28852.4 Mbps Max Sessions p 419 Max concurrent	t er second sessions			
1 day, 0 hour, 0 min		25166				
00.00 20067 22222 17778 13333 8889 4444 Thu 29 01:00 02:00 03:00 04:00 Thu 29 01:00 02:00 03:00 04:00	195-00 06:00 07:00 08:00 09:00 10:00	11:00 12:00 13:00	14:00 15:00 15:		19200 20:00 21:3	
Associated Super Flows						
Application Name	Superflow Name	Protocol	Flows	Bytes	% Flows	% Bytes
unknown-tcp	BreakingPoint Bandwidth Raw - TCP	TCP	16,826,699		80.64	97.27
unknown-udp	BreakingPoint Bandwidth Raw - UDP	UDP	3,661,057		17.54	0.01
smpp	BreakingPoint SMPP Transmit	TCP	106,154		0.51	1.51
unknown-ssl	unknown-ssl	TCP	51,230		0.25	1.09
bbciplayer	BBC iPlayer	TCP	16		0.00	0.00
pandora	Pandora Sandvine Bandwidth	TCP	1,004		0.00	0.05
pandora-tis	Pandora	TCP	527		0.00	0.04
рор3	BreakingPoint Bandwidth POP3 Full Session	TCP	162		0.00	0.00
cern.ch	cern.ch	TCP	212,034		1.02	0.03
dcerpc	BreakingPoint DCERPC MAPI Session	TCP	558		0.00	0.00
http	BreakingPoint Bandwidth HTTP	TCP	7,675		0.04	0.00
jincru.	jincru	TCP	304		0.00	0.00

\*

### Layout preparation

	CONTROL CENTER TEST MANAGERS	HELP			11 🔼
6	Test Workspace >> New Test >> Components >> LiveAppSim_	1			Browse 😭 ?
		_			
-	Live AppSim Information	Include in Report	Current Live Profile M Breaki	ngPoint Default	00:30:00 Live Profile
	Component Name:	State:	Parameters		Save As Template Load A Template
	LiveAppSim_1	Active	Filter by Parameter Name		Clear
	Description:				
			App Configuration Ø		
5=			Remove all DNS actions:		•
			Skip 'Unclassified TCP/UDP' superflow;		
	Component Tags	0	Okin Utralagaified COL superflow		
	Filter By Tag Name Clien	nt Tags	Skip Unclassified SSL superilow.		
	evt default	1_default	Replace Streams at Runtime:		
	i1_default		T 🥅 Data Rate 🛛		
	i2_default				-
	i3_default		Data Rate Automatic:		
	i4_default		Data Data Scane:	Limit Aggregate Throughout	
	i5_default		Data Rate Scope.	Limit Aggregate Throughput	
	i6_default		Data Rate Unit.	Megabits / Second	*
	i7_default		Data Rate Type:	Constant	*
	i8_default		Minimum Data Rate	10000	
	I9_default	er Tags		10000	
	i11 default	2 default	Maximum Data Rate:	1	
	i12 default				
	i13 default		PV4 Configuration		
	i14_default		TTI · *	32	
	i15_default >>			52	
	i16_default		TOS/DSCP: *	0	
	i17_default				
	i18_default		Pv6 Configuration		
	i19_default		Han Limit	64	
	i20_default		Hop Limit.	04	
					Return to Test Workspace

#### Interface status



10

### Test criteria, test components

CONTROL CENTER TEST	MANAGERS HELP				
5 Test Workspace >> New Test					Browse 😭 ?
Network Neighborhood	SHARED COMPONENT	SETTINGS			SUMMARY INFORMATION
BreakingPoint Switching	Maximum Flow Creation Rate				Test Name:
					Description
Iest Components 🔍 🗹 ADD NEW 🕂	100,000 flows/sec	100,000 flows/sec	100 %		Description.
Application Simulator	Total Bandwidth				
▼ Live AppSim (1)	Current	Original	Percent Change		
● LiveAppSim_1 <u> </u>	0 mogabite/sec	0 megabite/cos	100 %	Set	
Client Simulation	megabits/sec	megabits/sec		(1836)	Total Unique Superflows
Session Sender					0
Routing Robot	100.000	100,000	100 st		Total Unique Strikes
Advanced Routing Robot	flows	flows			0
Bit Blaster					Total MAC Addresses
Security					2
Malwara	0 attacks	0 attacks	100 %		Total Subnets
Desert	Total Addresses				2
Recreate	Current	Original	Percent Change		Populard MTU
Stack Scrambler	131,068	131,068	100 %	set	
	ip addresses	ip addresses		(1996)	·
	The period between data samples	Original	Porcent Change		Seed Override:
	1			set	
	seconds	seconds	100 %	reset	Lock lest to This User
Test Criteria					
No Custom Criteria Defined					
Device Under Test					
BreakingPoint Default					
Test Status Export Import Rev	ert				Save Save As Save and Run

#### Tests browser

	EST MANAGERS	HELP						
5 Test Browser >> Browse Tests								9
Select Test								
<enter criteria="" search=""></enter>							Clear	Search
Test Type: All								
							Ad	vanced 💌
		Displaving 2	5 of 438   Get more results					
Name	Test Type	Interfaces Created By	Last Run By	Pass/Fail	Bandwidth (Mbps)	Created	Last Changed	
0VM_RESTART_CS_DC		1			0	NA	NA	合
0VM_RESTART_CS_VDS		1			0	NA	NA	合
All MultiVariant Strikes - Random 100		2			0	NA	NA	合
All MultiVariant Strikes - Subset 1,2,4-6	,10	2			0	NA	NA	合
Andariel-2017 Campaign Scenario - 1		2			0	NA	NA	音
Andariel-2019 Infection Procedure - 1		2			0	NA	NA	音
Andariel-2019 Infection Procedure - 2		2			0	NA	NA	音
AppSim		2			400	NA	NA	
AppSimQuicktest		2			400	NA	NA	音
APT-29 July 2020 SoreFang Campaign		2			0	NA	NA	合
AZORult Neutrino September 2018 Cam	ipaign	2			0	NA	NA	音
Bandwidth HTTP over SCTP		2			2000	NA	NA	雷
BitBlaster		2			10000	NA	NA	合
BitBlaster_1000		2			1000	NA	NA	音
BitBlasterComplete		2			0	NA	NA	雷
BlackEnergy Botnet Command and Con	trol Co	2			10	NA	NA	音
Blog Post 2010-08-20 HTTP DDoS Floor	t	2			2000	NA	NA	雷
Blog Post 2010-08-20 HTTP DDoS Floor	d with A	2			4000	NA	NA	音
BreakingPoint 100K UE SGW-PGW Conf	ìrmed Ki	2			2000	NA	NA	雷
BreakingPoint Angler EK		2			20000	NA	NA	雷
BreakingPoint AppSim IPv4 SNAT		2			2000	NA	NA	氜
BreakingPoint Asymmetric Test		2			0	NA	NA	f
BreakingPoint Conditional DNS		2			30000	NA	NA	雷
BreakingPoint DDoS ICMP Echo Reply F	lood	2			500	NA	NA	音

#### IXIA A Keysight Business

#### 

	RESOURCE GROUPS	+	TRAFFIC (LAST HOUR)		APP DISTRIBUTION (LAST H	OUR)			TOP THREATS (LAST HOUR)		TOP COUNTRIES (LAST HOU	R)		
- Bis/5       - Second/5         - PLICES       - Bis/5       - Second/5         - PLICES       - Second/5         - PLICES       - Second/5         - Second/5       - Second/5         - PLICES       - Second/5         - Second/5	- DEFAULT	DA NE SSL MPLS TCP	In all the (shart free by)		All pipticiperior (Lapris	ook)			Threat Type	Sessions 1	Country	Sessions	Total B	Share 1
Image: Source is a contract of the function of the of the functin of the function of the function of the functin of th			- Bits/s	- Sessions/s	cer	n.ch			exploit	2 122	Russia	1 356 783	7274.6 GB	89%
N P I       Items       Items <th< th=""><th>RESOURCES</th><th></th><th></th><th></th><th>ndl-a3128)</th><th>1</th><th></th><th></th><th>bilacked</th><th>46</th><th>United States</th><th>201.818</th><th>312.9 GB</th><th>496</th></th<>	RESOURCES				ndl-a3128)	1			bilacked	46	United States	201.818	312.9 GB	496
Interest       Image: 1000 mp / 10000 mp / 1000 mp / 100	1 NP #1		17		tonid 4465)				malware	17	Switzerland	204 775	214.4 GB	396
• Lites         • end         end         end         end         en	And a second second				(chind				obishing	0	Private-IP	1 959	154.7 GB	296
<ul> <li>App from DC</li> <li>Coogle</li> <li>App from DC</li> <li>Limit and staff cool</li> <li>Unmatched staffic</li> <li>Unmatch</li></ul>	▼ FILTERS	+ 1£			nicel1095) -				bothet	0	Spain	12.858	68.8 GB	196
2       Coople       1 </th <th>1 App from DC</th> <th></th> <th>1M</th> <th></th> <th>targu5201)</th> <th></th> <th></th> <th></th> <th>outiet</th> <th></th> <th>Germany</th> <th>16,265</th> <th>58.4 GB</th> <th>196</th>	1 App from DC		1M		targu5201)				outiet		Germany	16,265	58.4 GB	196
2       Code       1					SunRPC /						Belgium	12,525	51.5 GB	196
3 Apple       1 </th <th>2 Google</th> <th></th> <th></th> <th></th> <th>steam7020)</th> <th></th> <th>2</th> <th></th> <th></th> <th></th> <th>and United Kingdom</th> <th>28.244</th> <th>17.3 GB</th> <th>0%</th>	2 Google				steam7020)		2				and United Kingdom	28.244	17.3 GB	0%
4       Utymatched traffic       8.15am       8.30am       8.45am       9.00am       Extended traffic       1000000000000000000000000000000000000	3 Apple		1		auror 3123)	/	CMDD				🔅 Republic of Korea	6.854	5.7 GB	096
A DUPLACING DUAL         WORLD (LAST HOUR)         Inters DYNAMIC APPS (LAST HOUR)	A Dimensional surface	S.	8:15am 8:30am	8:45am 9:00am	44101		* SMPP				France	13,901	4.1 GB	096
WORLD       ULXET DV/NAMIC APPS (LAXT HOUR)       Image       Top DEVICES BY OS (LAXT HOUR)       Image       Top DEVICES BY OS (LAXT HOUR)         Andro       Session       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       133.66       12/09/20       139.76       120.97.20 <th>4 Unmatched trainc</th> <th>5</th> <th></th>	4 Unmatched trainc	5												
Abo       Sessions       Total Lo       Norwered 4         Abo       Sessions       Total Lo       Sessions       Total Lo </th <th></th> <th></th> <th>WORLD (LAST HOUR)</th> <th></th> <th>LATEST DYNAMIC APPS (LA</th> <th>ST HOUR)</th> <th></th> <th></th> <th>TOP DEVICES BY OS (LAST HOUR)</th> <th></th> <th>TOP SERVICE PROVIDERS (L</th> <th>AST HOUR)</th> <th></th> <th></th>			WORLD (LAST HOUR)		LATEST DYNAMIC APPS (LA	ST HOUR)			TOP DEVICES BY OS (LAST HOUR)		TOP SERVICE PROVIDERS (L	AST HOUR)		
eman       31.09       13.36       12.09/20       MICHES       1014.82 <t< th=""><th></th><th></th><th></th><th>*****</th><th>Арр</th><th>Sessions</th><th>Total B</th><th>Discovered 🕹</th><th></th><th></th><th>Service Provider</th><th>Sessions</th><th>Total B</th><th>Share 🕹</th></t<>				*****	Арр	Sessions	Total B	Discovered 🕹			Service Provider	Sessions	Total B	Share 🕹
operations grind or g       7,112       181.8 NB       1209.20       NAL-45-termit Vational Acc.       1.60       284         intra       3.490       7114       181.9 NB       1209.20       11.8       1209.20       11.8       1209.20         intra       3.290       3.640       1209.20       11.8       1209.20       11.8       1209.20         intra       3.295       5.5M8       1209.20       11.8       1209.20       11.8       1209.20         intra       3.293       3.11.8       1209.20       11.8       1209.20       11.8       1209.20         intra       1.393.221.13       12.3       11.8       1209.20       11.8       1209.20       11.8       1209.20         intra       1.393.221.13       5       9.945.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       11.8       1209.20       12.8       12.8       12.8       12.8       12.8       12.8       12.8       12.8       12.8       12.8 <t< th=""><th></th><th></th><th>ANITA A</th><th></th><th>cern.ch</th><th>31,079</th><th>13.3 GB</th><th>12/09/20</th><th>All Others</th><th></th><th>JINR-AS JINR/HEPNET, RU (AS</th><th>59,171</th><th>6990.9 GB</th><th>91%</th></t<>			ANITA A		cern.ch	31,079	13.3 GB	12/09/20	All Others		JINR-AS JINR/HEPNET, RU (AS	59,171	6990.9 GB	91%
Image: Note of all states of the state of the states of					opensciencegrid.org	7,112	181.9 MB	12/09/20			FNAL-AS - Fermi National Acc	1,603	289.2 GB	496
Image: construction of the second of the				Antonio and	nikhef.nl	3,480	5.1 MB	12/09/20			CERN, CH (AS Number: 513)	13,459	211.4 GB	3%
Importung       233       3.5 MB       1209/20       MT-GIDKA, DE 45 Number:       17       33         acuk       123       211.7 KB       1209/20       123       211.7 KB       1209/20       MT-GIDKA, DE 45 Number:       17       33         gatomatical kines       123       211.7 KB       1209/20       MT-GIDKA, DE 45 Number:       17       33       85       123       211.7 KB       1209/20       MT-GIDKA, DE 45 Number:       17       33       81       123       23       5       123       11.7 KB       1209/20       MT-GIDKA, DE 45 Number:       17       33       81       123       23       5       129       129       10       10       123       23       5       129       129       129       10       112       33       111       112       33       111       12       33       111       120       120       111       120       120       111       112       33       111       120       120       111       111       111       112       33       111       112       33       111       112       111       112       111       111       111       111       111       111       111       111 <t< th=""><th></th><th></th><th></th><th>- PLC - 1</th><th>cmsrucio</th><th>679</th><th>17.1 MB</th><th>12/09/20</th><th></th><th></th><th>REDIRIS RedIRIS Autonomous</th><th>848</th><th>67.6 GB</th><th>196</th></t<>				- PLC - 1	cmsrucio	679	17.1 MB	12/09/20			REDIRIS RedIRIS Autonomous	848	67.6 GB	196
Image: Section Since with the section					jinr.ru	293	3.6 MB	12/09/20			KIT-GRIDKA, DE (AS Number:	17	53.5 GB	1%
ac.uk       123       211.7 KB       1209/20         159.93.229.151       42       31.1 KB       1209/20         uc.uk       159.93.229.132       5       9.9 KB       1209/20         TOP BROWSERS (LAST DAY)       Image: All others       Image: A					jinr-t1.ru	3,769	5.5 MB	12/09/20			BELNET, BE (AS Number: 2611)	378	51.2 GB	196
1593229151       42       31.1 KB       12/09/20       Unux       UCHICAGO-A5-University of 232       5         TOP BROWSERS (LAST DAY)       Image: Comparison of KRK, Hall (Last HOUR)       Image: Comparison of KRK, Hall (Last HOU					ac.uk	123	211.7 KB	12/09/20			JANET Jisc Services Limited, G	2,533	17.1 GB	0%
orgeonnetc.net       55       2.6 GB 1/2/09/20       Linux       KREONET2A5/KR KISTL KR (A					159.93.229.151	42	31.1 KB	12/09/20			U-CHICAGO-AS - University of	232	5.7 GB	0%
19.93.229.132       5       9.9 KB       12/09/20       KFKI-AS IP networks of KFKI, H       112       3         TOP BROWSERS (LAST DAY)       Image: Comparison of the compariso					osgconnect.net	55	2.6 GB	12/09/20	Linux		KREONET2-AS-KR KISTI, KR (A	36	3.7 GB	0%
TOP BROWSERS (LAST DAY)       Image: Top Filters (LAST HOUR)         All Others       Filter       Sessions       Total B         Sessions       Total B       Share       App from DC       1,407,533       8616.2 GB       100%         Unknown       Filter       Sessions       Total B       Share       App from DC       1,407,533       8616.2 GB       100%         Unmatched traffic       0       43 MB       0%       0%       0%       0%       0%			€~		159.93.229.132	5	9.9 KB	12/09/20	Entry		KFKI-AS IP networks of KFKI, H	112	3.2 GB	096
All Others       Filter       Sessions       Total B       Share         App from DC       1,407,533       8616.2 GB       100%         Unmatched traffic       0       43 MB       0%			TOP BROWSERS (LAST DAY)		TOP FILTERS (LAST HOUR)									
All Others Unknown Firefox wget					Filter	Sessions	Total B	Share 1						
Unknown Firefox wget			All Others	)	App from DC	1,407,533	8616.2 GE	100%						
Firefox wget			Unknown		Unmatched traffic	C	) 43 MB	0%						
			Firefox	wget										

# Thank you