SOPHOS

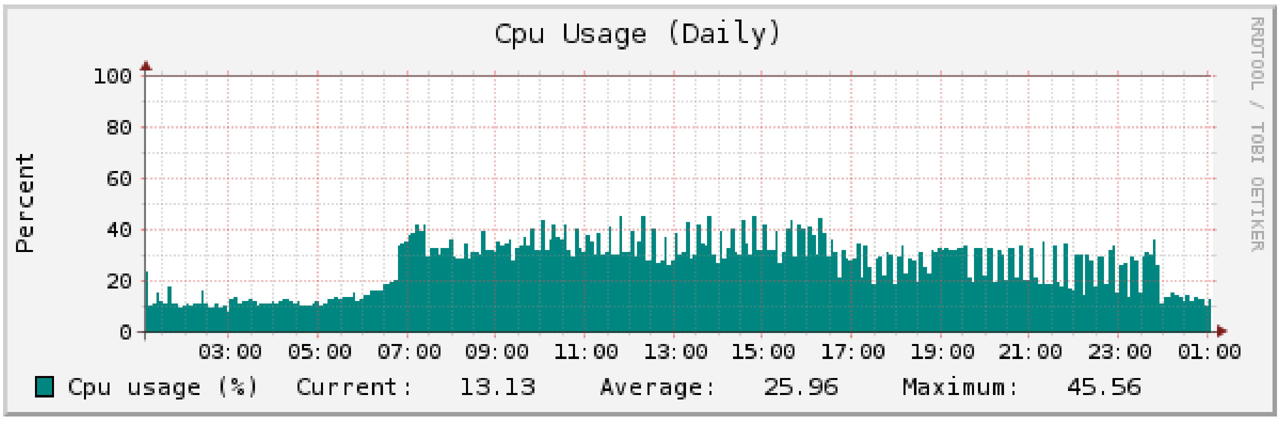
Executive Report

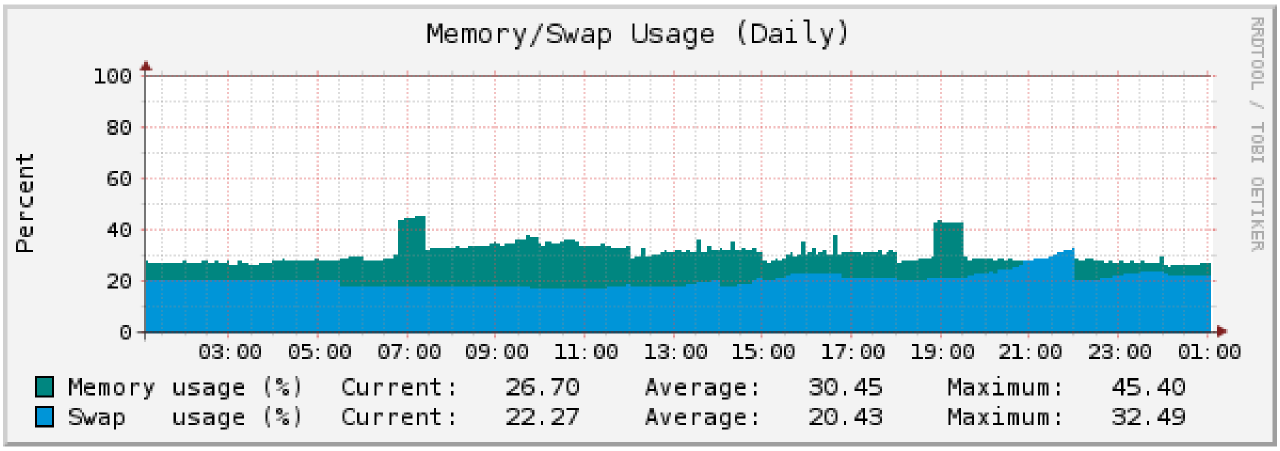
Date	2025/06/24
Type	daily

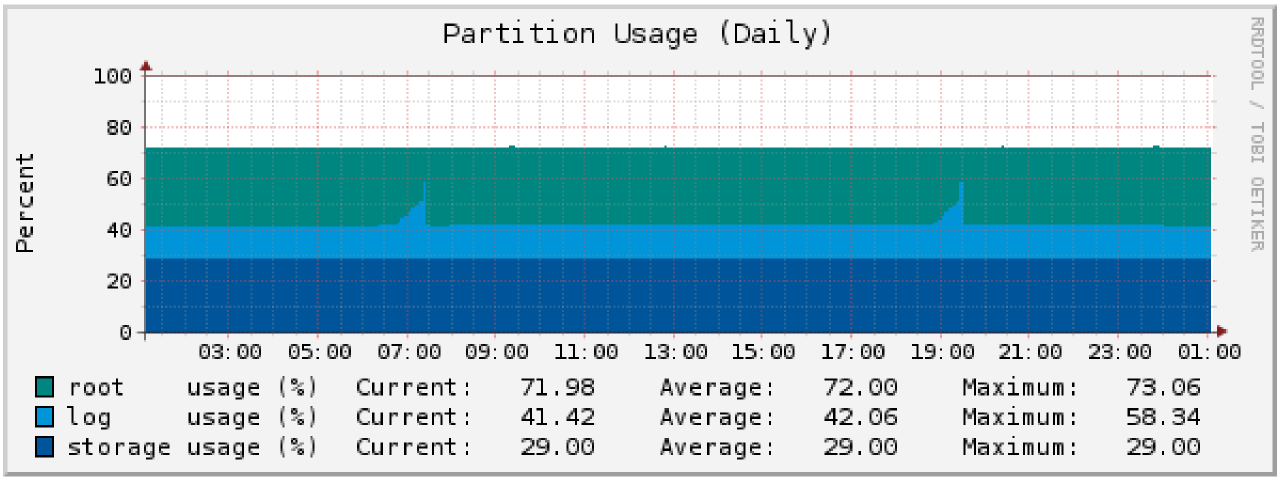
Device	
Organization	Benh Vien Hung Vuong
Country	VN
City	HCM
Serial	S320D46YJ9T3703
License ID	1792722
Hostname	118.69.68.214
Firmware Version	9.720-5
Uptime	66 days 2 hours 9 minutes

Summary			
Network Usage		WebAdmin Logins	
Traffic processed	2.3 TB	Successful	4
Connections Handled	26 318 561	Failed	2
Network Protection		Console Logins	
Packets blocked by Firewall	777 657	Successful	16
Packets blocked by IPS	0	Failed	123
Web Filtering		Up2Date	
Total Website Requests	7948	Requests successful	96
URLs blocked	0	Requests failed	0
HTTP/S viruses blocked	0	Firmware updates installed	0
HTTP/S malware blocked	0	Pattern updates installed	20
Mail Filtering		System	
Mails processed	0	System Restarts	0
Spam Mails blocked	0	Uplink fail-overs	1
Virus Mails blocked	0	HA/Cluster failovers	0
VPN			
VPN connections	1		
VPN traffic	not accounted		

Resource Usage







Network Usage

TOP10 Clients

Total Packets: 2 774 787 658

Total Traffic: 2.3 TB

	IP	Hostname	Packets	Traffic	%
lan	10.17.3.15	veeam	227 704 446	171.0 GB	7.37
lan	10.17.47.51	10.17.47.51	36 772 017	36.7 GB	1.58
lan	172.16.49.211	172.16.49.211	21 213 629	19.6 GB	0.85
lan	10.17.9.41	10.17.9.41	19 563 269	18.3 GB	0.79
lan	10.17.23.97	10.17.23.97	16 650 442	14.7 GB	0.64
lan	10.17.34.166	10.17.34.166	14 797 263	14.3 GB	0.61
lan	10.17.104.78	10.17.104.78	13 568 792	14.0 GB	0.60
vn	210.2.89.195	210.2.89.195	18 431 155	13.9 GB	0.60
lan	172.16.47.201	172.16.47.201	16 283 578	13.2 GB	0.57
lan	10.17.45.84	10.17.45.84	16 143 008	12.4 GB	0.54

TOP10 Servers

Total Packets: 2 774 789 506

Total Traffic: 2.3 TB

	IP	Hostname	Packets	Traffic	%
vn	124.158.9.155	124.158.9.155	227 687 432	171.0 GB	7.37
vn	113.171.65.17	static.vnpt.vn	142 810 578	148.4 GB	6.40
vn	113.171.65.81	static.vnpt.vn	58 499 972	60.4 GB	2.61
vn	113.171.105.17	static.vnpt.vn	58 331 713	60.3 GB	2.60
vn	113.171.64.81	static.vnpt.vn	56 736 072	58.7 GB	2.53
hk	157.240.211.13	xx-fbcdn-shv-02-hkg4.fbcdn.net	51 259 248	52.1 GB	2.25
vn	14.238.118.255	static.vnpt.vn	42 045 789	43.4 GB	1.87
vn	58.186.151.147	58.186.151.147	36 683 029	38.2 GB	1.65
hk	163.70.159.13	xx-fbcdn-shv-02-hkg1.fbcdn.net	35 672 950	36.4 GB	1.57
hk	157.240.199.15	xx-fbcdn-shv-01-hkg4.fbcdn.net	34 712 196	35.4 GB	1.52

TOP10 Services

Total Packets: 2 773 384 636

Total Traffic: 2.3 TB

Service Name	Protocol	Service Port	Packets	Traffic	%
HTTPS	UDP	443	1 216 187 712	1.1 TB	48.96
HTTPS	TCP	443	897 477 344	744.4 GB	32.11
MICROSOFT-DS	TCP	445	249 409 924	171.4 GB	7.39
HTTP	TCP	80	67 852 675	61.3 GB	2.65
4200	UDP	4200	60 921 794	23.3 GB	1.00
16002	TCP	16002	18 460 227	13.9 GB	0.60
NAT-STUN-PORT	UDP	3478	17 259 453	12.0 GB	0.52
IRDMI	TCP	8000	13 270 505	8.1 GB	0.35
9502	TCP	9502	5 680 410	5.5 GB	0.24
9132	TCP	9132	5 022 586	3.8 GB	0.17

TOP10 Applications

Total Packets: 2 773 959 879

Total Traffic: 2.3 TB

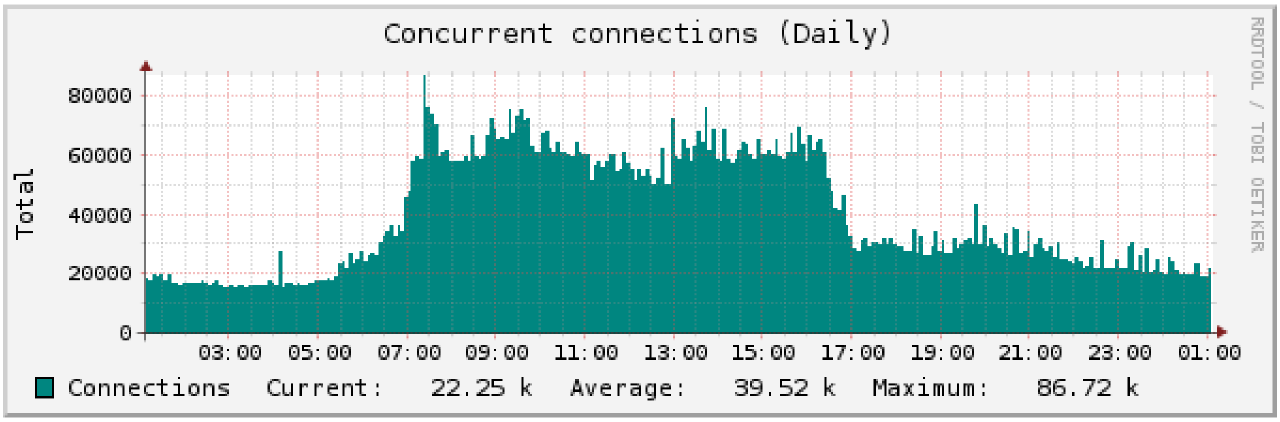
Application	Packets	Traffic	%
Facebook	659 361 085	639.5 GB	27.58
TikTok	285 111 839	271.4 GB	11.70
SSL	303 199 156	265.1 GB	11.43
QUIC IETF	242 082 884	195.2 GB	8.42
CIFS	237 799 834	171.5 GB	7.39
YouTube	159 524 135	142.6 GB	6.15
Unclassified	241 512 537	129.2 GB	5.57
HTTP/2	87 307 493	76.2 GB	3.28
Hotspot Shield	68 190 814	66.4 GB	2.86
iTunes	57 598 999	49.8 GB	2.15

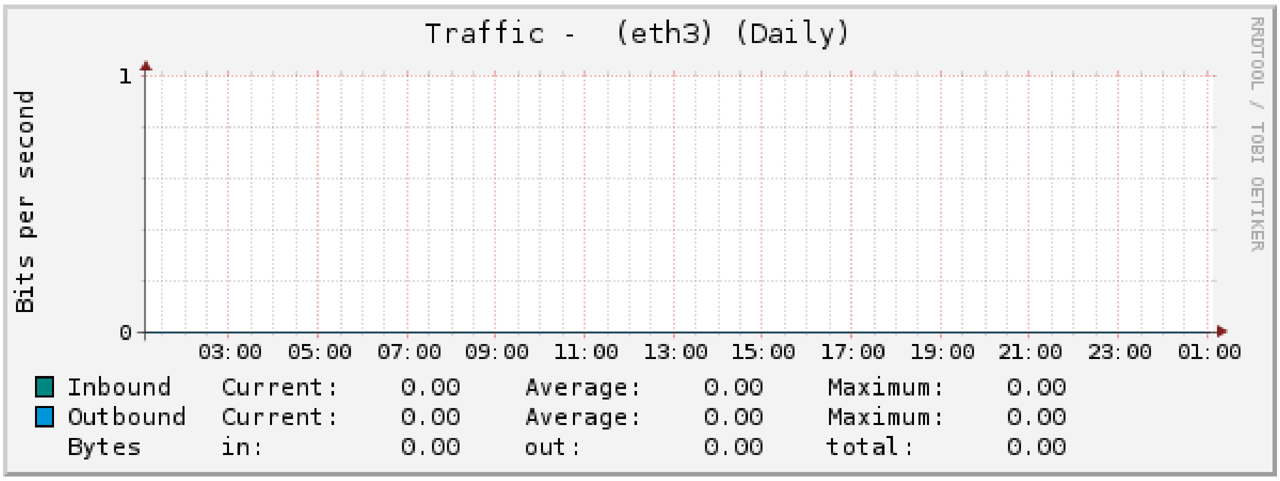
TOP10 Application Categories

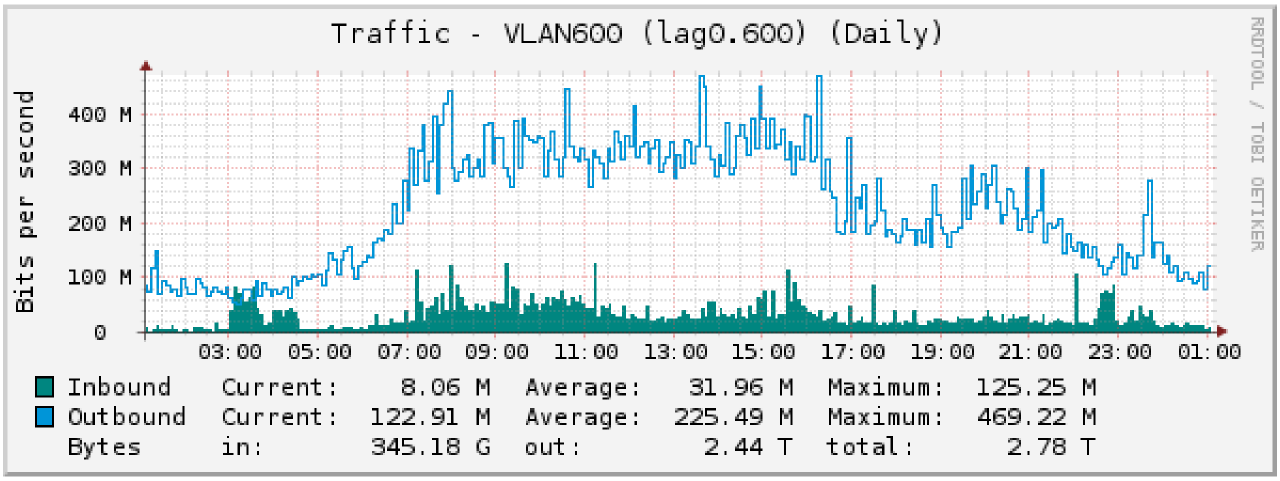
Total Packets: 2 773 963 694

Total Traffic: 2.3 TB

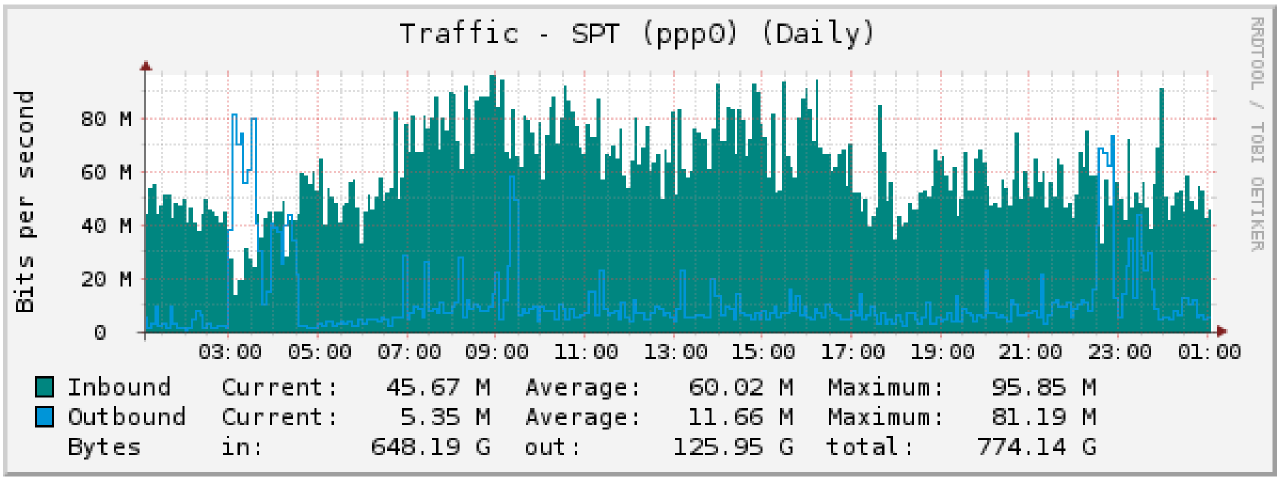
Application Category	Packets	Traffic	%
Social Networking	681 099 992	656.1 GB	28.29
Streaming Media	537 197 725	489.0 GB	21.09
Web Services	523 370 723	438.9 GB	18.93
File Transfer	352 328 216	265.5 GB	11.45
Networking	296 695 474	224.0 GB	9.66
Unclassified	241 512 737	129.2 GB	5.57
VPN and Tunneling	88 553 164	81.4 GB	3.51
Messaging	30 359 600	20.0 GB	0.86
Collaboration	5 159 297	5.3 GB	0.23
Proxy	7 518 037	3.8 GB	0.16



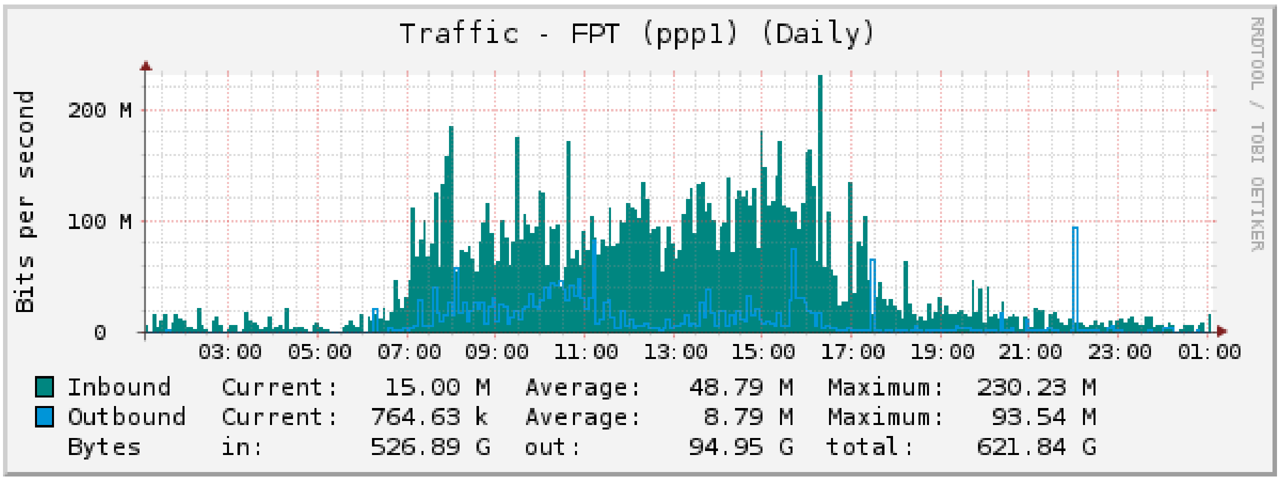




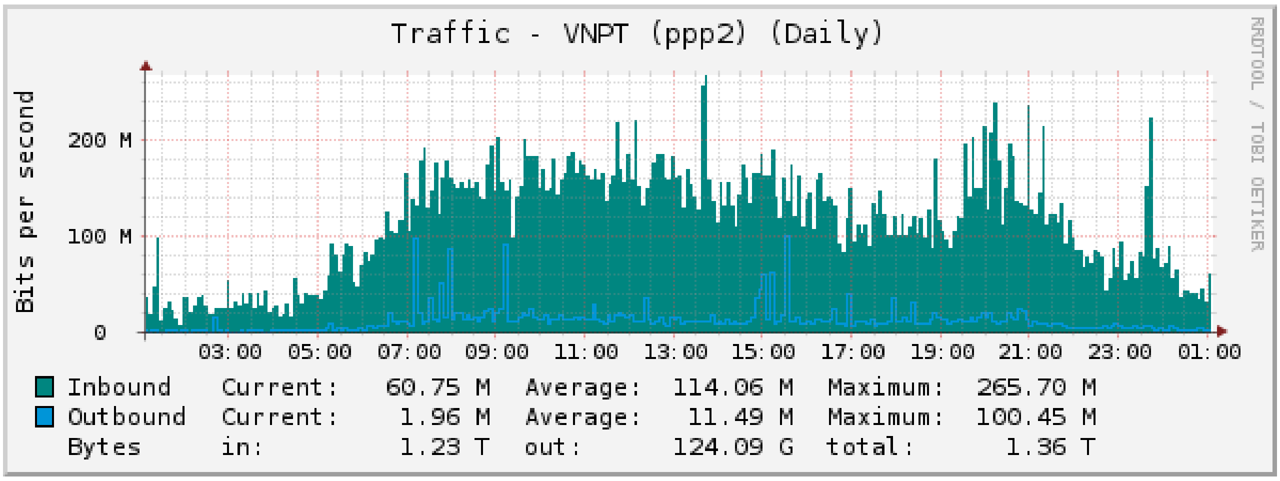
```
🟩 Inbound   Current:    8.06 M  Average:   31.96 M  Maximum:  125.25 M
🟦 Outbound  Current:  122.91 M  Average:  225.49 M  Maximum:  469.22 M
   Bytes     in:       345.18 G  out:        2.44 T  total:      2.78 T
```



```
🟩 Inbound   Current:   45.67 M  Average:   60.02 M  Maximum:   95.85 M
🟦 Outbound  Current:    5.35 M  Average:   11.66 M  Maximum:   81.19 M
   Bytes     in:       648.19 G  out:      125.95 G  total:    774.14 G
```



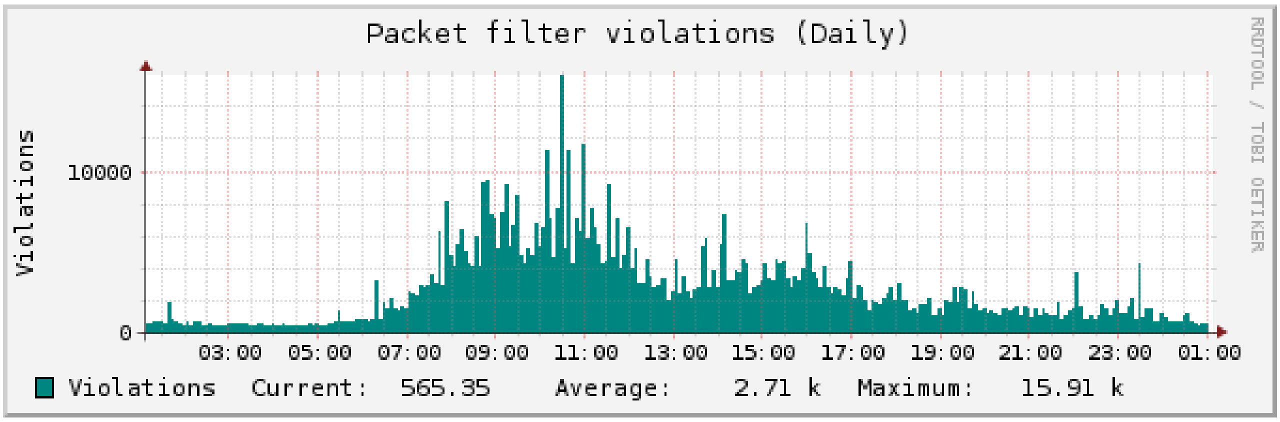
```
🟩 Inbound   Current:   15.00 M  Average:   48.79 M  Maximum:  230.23 M
🟦 Outbound  Current:  764.63 k  Average:    8.79 M  Maximum:   93.54 M
   Bytes     in:       526.89 G  out:       94.95 G  total:    621.84 G
```



```
🟩 Inbound   Current:   60.75 M  Average:  114.06 M  Maximum:  265.70 M
🟦 Outbound  Current:    1.96 M  Average:   11.49 M  Maximum:  100.45 M
   Bytes     in:         1.23 T  out:      124.09 G  total:      1.36 T
```

Network Protection

Packet Filter / Firewall



TOP10 dropped source hosts

Total dropped packets: 777 657

	Source IP	Hostname	Packets	%
vn	112.197.233.246	112.197.233.246	17 483	2.25
vn	14.191.220.206	static.vnpt.vn	14 952	1.92
vn	42.112.134.127	42.112.134.127	13 379	1.72
vn	116.106.2.139	dynamic-ip-adsl.viettel.vn	12 605	1.62
lan	10.17.12.254	10.17.12.254	11 650	1.50
vn	42.119.81.227	42.119.81.227	8 449	1.09
vn	42.119.229.185	42.119.229.185	7 865	1.01
vn	118.68.85.70	118.68.85.70	7 787	1.00
vn	1.52.1.63	1.52.1.63	7 676	0.99
vn	1.54.153.216	1.54.153.216	7 242	0.93

TOP10 dropped destination hosts

Total dropped packets: 777 657

	Destination IP	Hostname	Packets	%
vn	14.224.128.41	VNPT (Address)	474 877	61.07
vn	116.118.112.238	SPT (Address)	154 862	19.91
vn	118.69.68.214	FPT (Address)	114 265	14.69
lan	172.16.0.184	172.16.0.184	12 695	1.63
lan	224.0.0.1	all-systems.mcast.net	6 253	0.80
lan	10.17.47.56	10.17.47.56	2 944	0.38
lan	10.17.4.41	4.41	1 650	0.21
lan	172.16.0.40	172.16.0.40	1 453	0.19
lan	172.16.232.56	172.16.232.56	1 082	0.14
lan	10.17.13.3	NHI	899	0.12

TOP10 dropped services

Total dropped packets: 777 657

Service Name	Protocol	Service	Packets	%
	TCP	34340	115 322	14.83
	UDP	34340	36 406	4.68
	UDP	63221	19 828	2.55
SNAPENETIO	TCP	22000	17 131	2.20
SNAPENETIO	UDP	22000	15 759	2.03
T3C10	ICMP	t3c10	11 052	1.42
	UDP	8567	11 050	1.42
	TCP	7680	9 195	1.18
	UDP	16403	8 384	1.08
HTTPS	UDP	443	7 968	1.02

Advanced Threat Protection (ATP)

TOP10 ATP Contaminated

Total events: 8 509

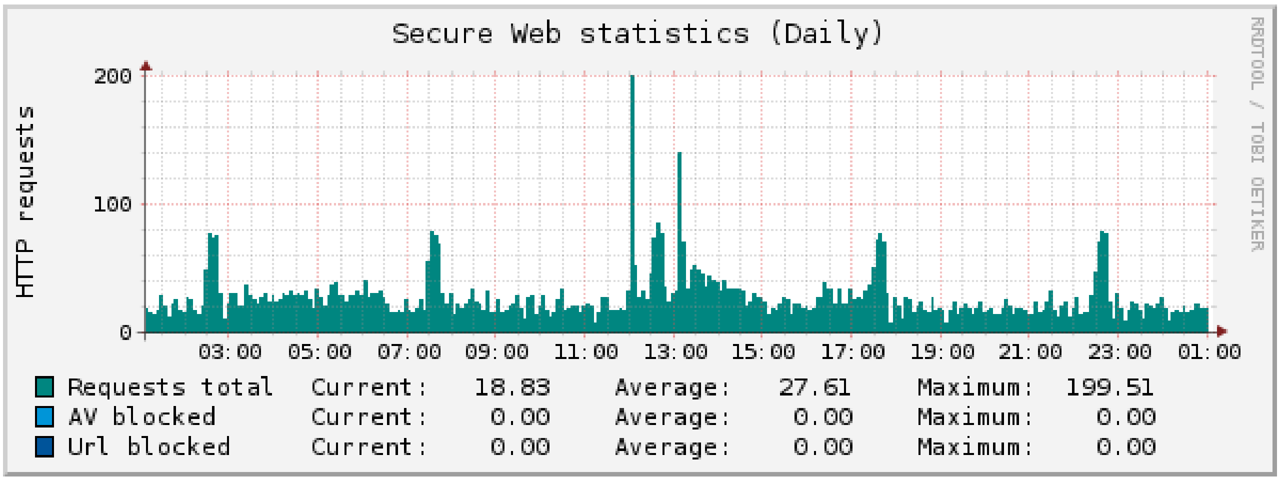
Source IP	Threat Name	Destination IP	Events	Origin
10.17.12.180	C2/Generic-A	jdyqyjooh.org	521	AFCd
10.17.41.50	C2/Generic-A	jdyqyjooh.org	512	AFCd
10.17.12.180	C2/Generic-A	tbfmfkhopjn.info	496	AFCd
10.17.12.180	C2/Generic-A	lwqvlgnbez.info	485	AFCd
10.17.41.50	C2/Generic-A	tbfmfkhopjn.info	473	AFCd
10.17.41.50	C2/Generic-A	lwqvlgnbez.info	465	AFCd
10.17.4.11	C2/Generic-A	tbfmfkhopjn.info	269	AFCd
10.17.4.11	C2/Generic-A	lwqvlgnbez.info	250	AFCd
10.17.18.63	C2/Generic-A	jdyqyjooh.org	211	AFCd
10.17.47.86	C2/Generic-A	lwqvlgnbez.info	203	AFCd

TOP10 ATP Recent Events

Total events: 8 509

Source IP	Threat Name	Destination IP	Events	Origin
10.17.18.55	C2/Generic-A	t.zz3r0.com	1	AFCd
172.16.0.184	C2/Generic-A	78.129.184.4	1	Iptables
172.16.0.184	C2/Generic-A	85.10.204.140	1	Iptables
10.17.4.12	C2/Generic-A	cdn.chatcdn.net	1	AFCd
172.16.0.184	C2/Generic-A	85.10.198.196	2	Iptables
10.17.4.12	C2/Generic-A	jdyqyjooh.org	4	AFCd
172.16.0.184	C2/Generic-A	173.212.224.110	1	Iptables
10.17.4.12	C2/Generic-A	t.zz3r0.com	1	AFCd
10.17.47.56	C2/Generic-A	146.71.79.49	1	Iptables
172.16.0.184	C2/Generic-A	178.63.238.181	1	Iptables

Web Protection



Web Usage

TOP10 Users by time

Total time: 25:12:00

User	Duration	%
172.16.0.40	25:12:00	100.0

TOP10 Users by traffic

Total Traffic: 596.7 MB

User	Traffic	%
172.16.0.40	596.7 MB	100.0

TOP10 Domains by time

Total time: 76:16:45

Domain	Duration	%
googleapis.com	19:46:46	25.9
launchdarkly.com	11:51:18	15.5
meraki.com	10:09:22	13.3
nr-data.net	07:27:48	9.8
zalo.me	03:42:23	4.9
microsoft.com	03:10:47	4.2
mozilla.com	02:48:56	3.7
216.157.133.167	02:03:01	2.7
gvt2.com	01:52:09	2.5
gvt1.com	01:29:37	2.0

TOP10 Domains by size

Total Traffic: 596.7 MB

Domain	Traffic	%
googleapis.com	187.1 MB	31.4
meraki.com	161.3 MB	27.0
microsoft.com	155.9 MB	26.1
216.157.133.167	33.2 MB	5.6
nr-data.net	16.8 MB	2.8
intercom.io	10.0 MB	1.7
launchdarkly.com	7.6 MB	1.3
symantecliveupdate.com	4.8 MB	0.8
35.174.127.31	3.4 MB	0.6
zalo.me	3.3 MB	0.6

VPN

TOP10 VPN Clients by duration

TOP10 VPN Clients by duration

Total duration: 09:34:25

Number of users: 1

User	Service	Traffic	Duration	%	# of connections
khoa.ids	SSL VPN	not accounted	09:34:25	100.00	1