NGFW Assessment Report

Prepared For
Informata College

Prepared By
John Smith
Fortinet

Report Date
May 5, 2021

Executive Summary

We aggregated key findings from our NGFW assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report for actionable steps your organization can take to mitigate inbound threats, implement corporate use policies, and avert capacity planning issues.

Security

11,126
Application Vulnerability Attacks Detected

13
Malware and/or Botnets Discovered

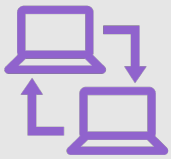
17
High Risk Applications Detected

Note that any threats observed within this report have effectively bypassed your existing network security gateway, so they should be considered active and may lead to increased risk (such as a data breach).

Productivity

330
Total Applications Detected

5
Total Proxy Applications Detected



5
Total Peer to Peer Applications

Application usage should have a strong influence on your network architecture. Understanding which types of applications are being used can affect corporate use policies, controls on segmented networks, and utilization of cloud-based service platforms.

Utilization

40.5GB
Total Bandwidth Used

12.5
Average Log Rate per Second

58.0%
Percentage of SSL Encrypted Traffic

In addition to individual applications, understanding overall utilization can help with capacity planning and streamlining network traffic over time.

Security

Quick Stats

- **11,126** application vulnerability attacks detected
- **1** known botnet detected
- **125** malicious websites detected
- **17** high risk applications detected
- **1** phishing websites detected
- **13** known malware detected
- **8,190** files analyzed by sandbox
- **36** suspicious files detected by sandbox

Top Application Vulnerability Exploits Detected

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develops signatures to detect them. FortiGuard currently leverages a database of more than 5,800 known application threats to detect attacks that evade traditional firewall systems. For more information on application vulnerabilities, please refer to FortiGuard at: http://www.fortiguard.com/intrusion.

#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	Adobe.Flash.Player.Authplay.DLL.SWF.Handling.Code.Execution		1	1	2,035
2	5	IBM.Rational.ClearQuest.Username.Parameter.SQL.Injection	SQL Injection	30	1	195
3	5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	8	3	15
4	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	3	2	10
5	5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	1	1	2
6	5	McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution	Code Injection	1	1	1
7	4	LaVague.PrintBar.PHP.File.Inclusion	Code Injection	30	1	183
8	4	IISadmin.ISM.DLL.Access	Information Disclosure	29	1	169
9	4	GameSiteScript.Index.PHP.SQL.Injection	SQL Injection	30	1	169
10	4	OTE.Header.PHP.File.Inclusion	Code Injection	30	1	163

Top Malware, Botnets and Spyware/Adware Detected

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, Fortinet identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

#	Malware Name	Type	Application	Victims	Sources	Count
1	EICAR_TEST_FILE	Virus	FTP	1	1	824
2	EICAR_TEST_FILE	Virus	HTTP	1	1	792
3	Asprox.Botnet	Botnet C&C	Asprox.Botnet	55	1	600
4	Adware/TEST_FILE	Adware	HTTP	1	1	411
5	ETDB_TEST_FILE	Virus	FTP	1	1	406
6	W32/NGVCK	Virus	HTTP	1	1	405
7	W32/ForeignRansom.583D!tr	Virus	HTTP	1	1	400
8	W32/ForeignRansom.583D!tr	Virus	FTP	1	1	395
9	W32/NGVCK	Virus	FTP	1	1	384
10	Adware/TEST_FILE	Adware	FTP	1	1	379

Security

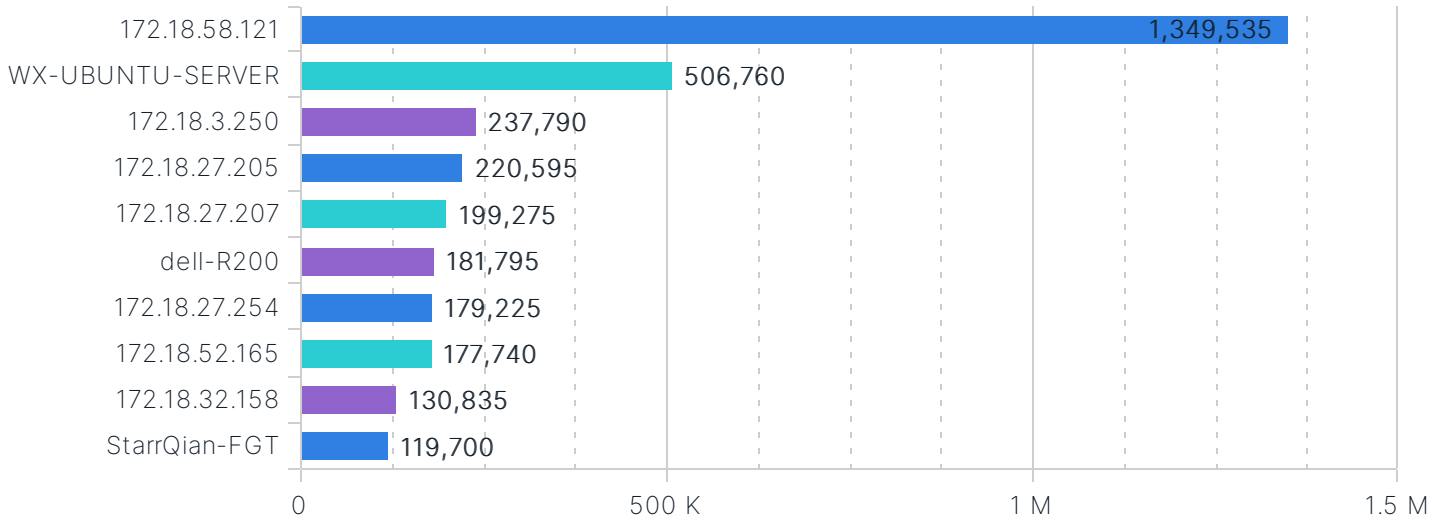
High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38

At-Risk Devices and Hosts

Based on the types of activity exhibited by an individual host, we can approximate the trustworthiness of each individual client. This client reputation is based on key factors such as websites browsed, applications used and inbound/outbound destinations utilized. Ultimately, we can create an overall threat score by looking at the aggregated activity used by each individual host.



Security

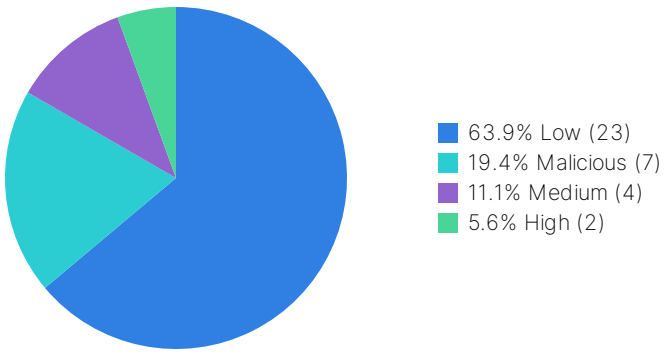
Unknown Malware

Today's increasingly sophisticated threats can mask their maliciousness and bypass traditional antimalware security. Conventional antimalware engines are, in the time afforded and to the certainty required, often unable to classify certain payloads as either good or bad; in fact, their intent is unknown. Sandboxing helps solve this problem – it entices unknown files to execute in a protected environment, observes its resultant behavior and classifies its risk based on that behavior. With this functionality enabled for your assessment, we have taken a closer look at files traversing your network.

#	Filename	Service	Risk	Suspicious Behaviors	Count
1	1D26B266.vXE	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess	1
2	1D28E4E7.vsc	HTTP	Malicious	Threat_Intelligence	1
3	1D43634F.vsc	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess Executable deleted itself after execution Executable dropped a copy of itself This file checked registry for anti-virtualization or anti-debug	1
4	1D45FCB7.vsc	HTTP	Malicious	Threat_Intelligence	1
5	1D46A1FA.vsc	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess	1
6	1D46A601.vXE	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess Executable deleted itself after execution Executable dropped a copy of itself This file checked registry for anti-virtualization or anti-debug	1
7	1D46EE5B.vsc	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess Executable deleted itself after execution Executable dropped a copy of itself This file checked registry for anti-virtualization or anti-debug	1

Malicious and Suspicious Files

The results of behavioral analysis are usually categorized in one of three ways: clean, suspicious, or malicious. A designation of clean means that no abnormal behaviors were observed and the file can be considered safe. Suspicious activities are potentially dangerous and may warrant further attention – for instance, a high suspicion file may try to replicate itself whereas a low suspicion file may only create abnormal registry settings. A malicious designation should be considered a legitimate threat to your network and requires immediate attention. The chart rendered here shows malicious and suspicious files (e.g. it does not include files designated as clean).



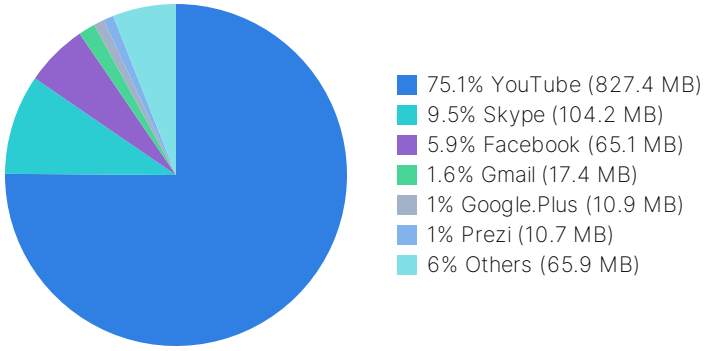
Productivity

Quick Stats

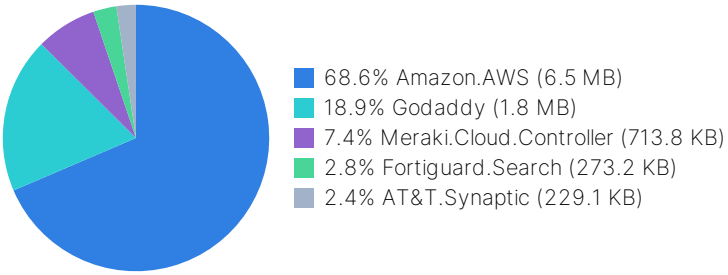
- **330** total applications detected
- **5** total proxy applications detected
- **5** peer to peer applications detected
- **5** remote access applications detected
- **SSL** is the top used application
- **Network.Service** is the most used application category
- **567** total websites visited
- **ca.archive.ubuntu.com** is the most visited website

Cloud Usage (SaaS)

IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.



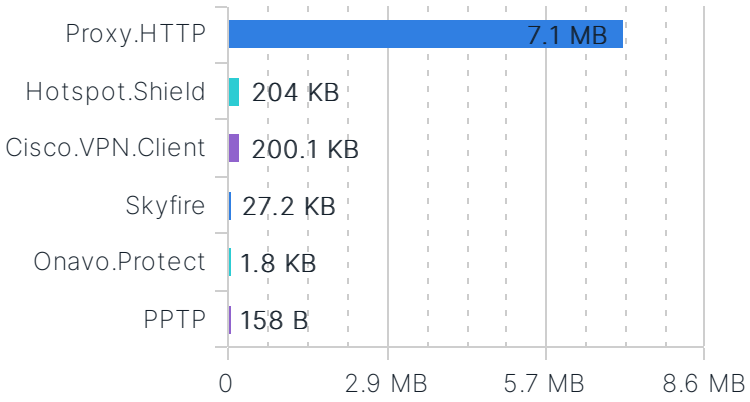
Cloud Usage (IaaS)



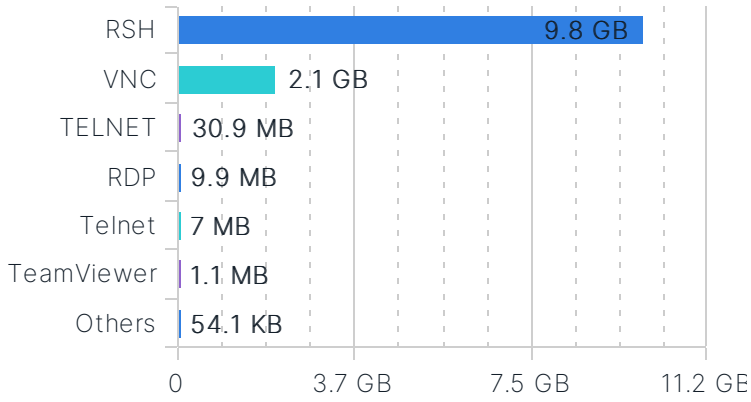
The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

Productivity

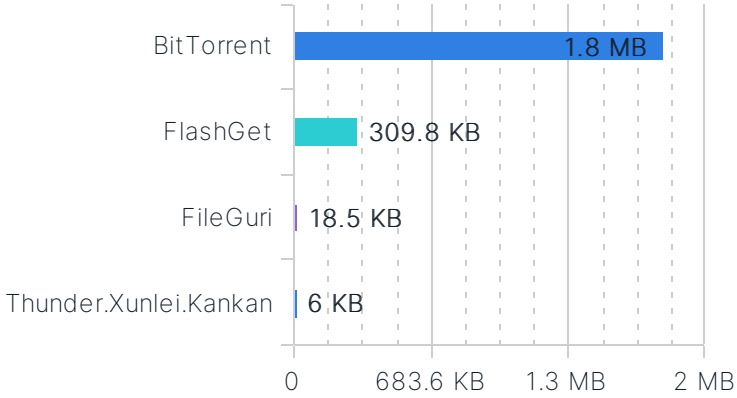
Proxy Applications



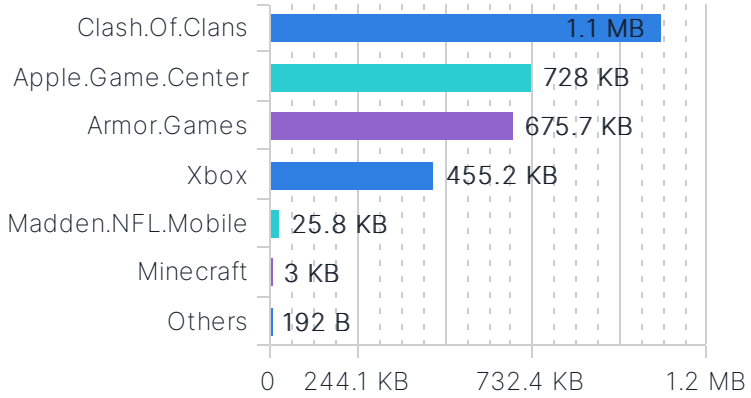
Remote Access Applications



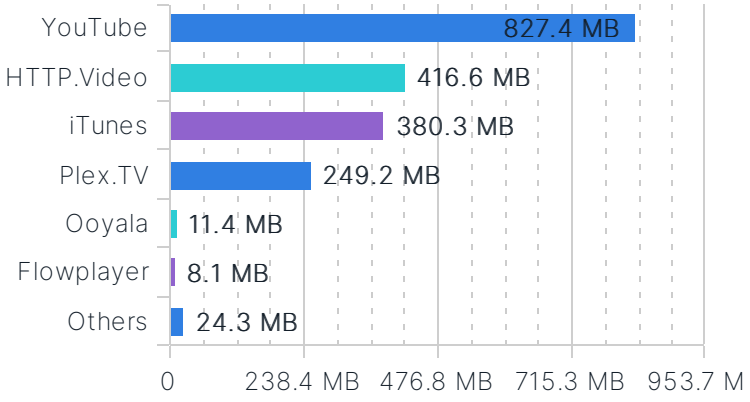
Top Peer to Peer Applications



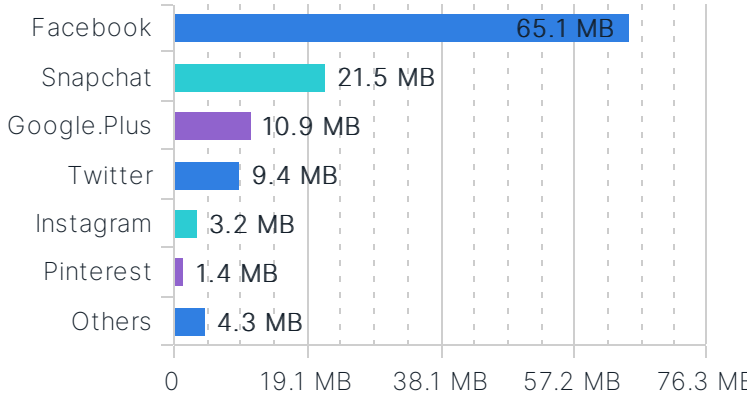
Top Gaming Applications



Top Video/Audio Streaming Applications



Top Social Media Applications



Productivity

Top Web Applications

In today's network environments, many applications leverage HTTP for communications – even some you wouldn't normally expect. The primary benefit of HTTP is that communication is ubiquitous, universally accepted and (generally) open on most firewalls. For most business-related and whitelisted applications this typically augments communication, but some non-business applications also use HTTP in either unproductive or potentially nefarious ways.

#	Application	Sessions	Bandwidth
1	SSL	129,754	6.28 GB
2	HTTP.BROWSER	223,132	4.41 GB
3	HTTPS	110,074	2.99 GB
4	HTTP	48,555	853.75 MB
5	YouTube	4,139	806.89 MB
6	HTTP.Audio	532	507.46 MB
7	HTTP.Video	298	415.62 MB
8	iTunes	180	380.32 MB
9	HTTPS.BROWSER	7,338	372.21 MB
10	Apple.Services	25	241.61 MB

Top Websites by Browsing Time

Estimated browsing times for individual websites can be useful when trying to get an accurate picture of popular websites. Typically, these represent internal web resources such as intranets, but they can occasionally be indicative of excessive behavior. Browse times can be employed to justify the implementation of web caching technologies or help shape organizational corporate use policies.

#	Domain	Category	Browsing Time (hh:mm:ss)
1	ssw.live.com	Search Engines and Portals	00:26:46
2	blu407-m.hotmail.com	Web-based Email	00:17:32
3	crl.microsoft.com	Information Technology, Web Hosting	00:16:22
4	www.microsoft.com	Information Technology	00:12:13
5	173.194.33.86	Search Engines and Portals	00:11:15
6	23.209.27.138	Unrated	00:10:35
7	64.37.102.54	Business	00:10:25
8	ca.archive.ubuntu.com	Reference	00:10:24
9	17.154.66.47	Unrated	00:09:53
10	109.200.4.26	Unrated	00:09:48

Productivity

Top Web Categories

Web browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines.

#	URL Category	Users	Count	Bandwidth
1	Unrated	3	1,359	2.06 MB
2	Information Technology	5	1,106	56.71 MB
3	Search Engines and Portals	5	757	40.05 MB
4	Advertising	4	558	4.82 MB
5	Web Hosting	3	447	2.68 MB
6	Instant Messaging	3	285	1.75 MB
7	File Sharing and Storage	3	257	1,018.61 KB
8	Business	4	245	3.97 MB
9	News and Media	3	212	7.78 MB
10	Content Servers	4	205	7.94 MB

Most Visited Web Domains

Websites browsed are strong indicators of how employees utilizing corporate resources and how applications communicate with specific websites. Analyzing domains accessed can lead to changes in corporate infrastructure such as website blocking, deep application inspection of cloud-based apps and implementation of web traffic acceleration technologies.

#	Domain	Category	Visits
1	ca.archive.ubuntu.com	Reference	1,256
2	ads2.westca.com	Advertising	462
3	security.ubuntu.com	Information Technology	387
4	cdn.speedshiftmedia.com	Advertising	335
5	gs-loc.apple.com	Information Technology	194
6	caextshort.weixin.qq.com	Instant Messaging	157
7	mmsns.qpic.cn	Content Servers	156
8	173.194.33.86	Search Engines and Portals	133
9	23.209.27.138	Unrated	123
10	23.3.105.162	Unrated	122

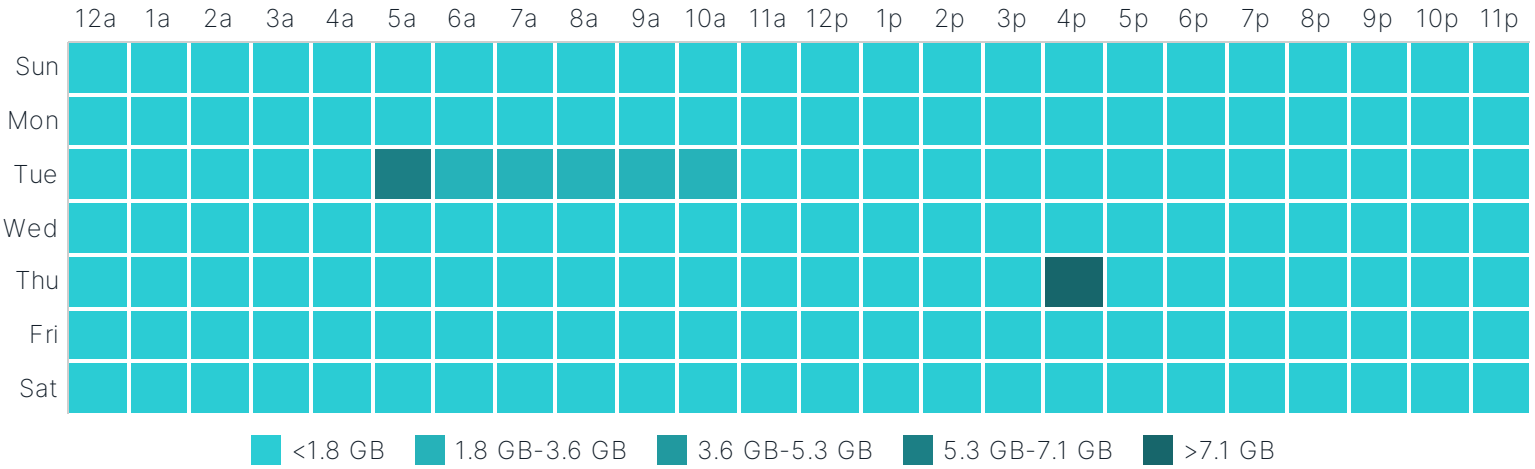
Utilization

Quick Stats

- **40.5 GB** total bandwidth used
- **58.0%** percentage of SSL encrypted traffic
- **4pm - 5pm** is the highest daily peak usage
- **192.168.1.119** is the highest session bandwidth source
- **10.2.60.117** is the highest session count source
- **12.5** average log rate per second
- **2.8%** average FortiGate CPU usage
- **61.7%** average FortiGate memory usage

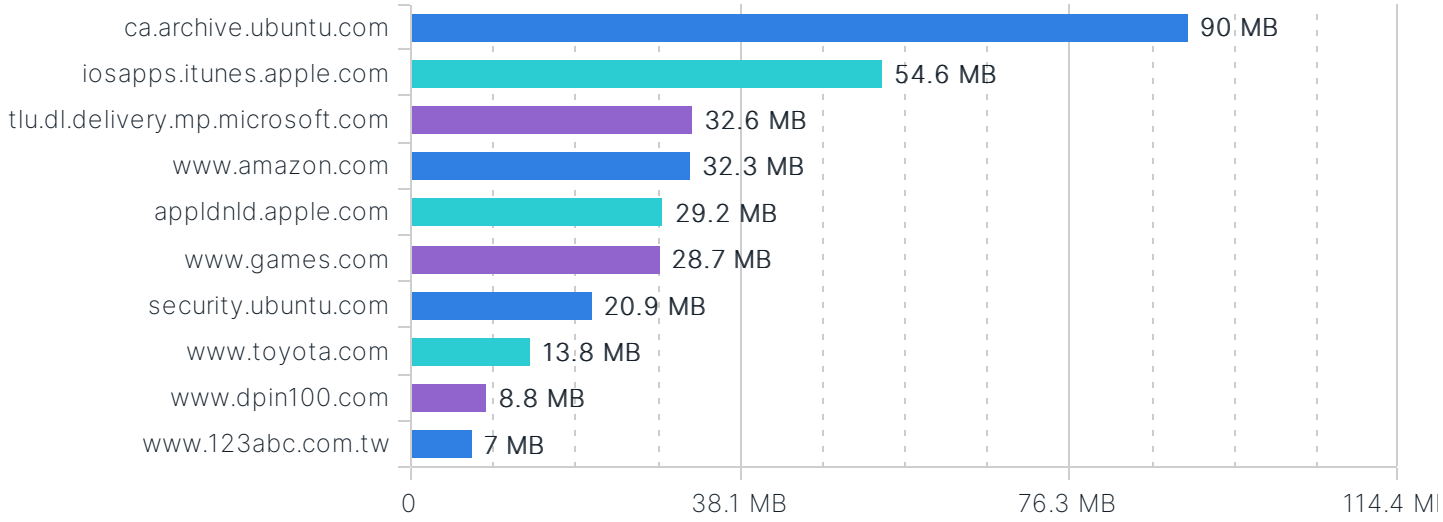
Average Bandwidth by Hour

By looking at bandwidth usage when distributed over an average day, administrators can better understand their organizational ISP connection and interface speed requirements. Bandwidth can also be optimized on an application basis (using throttling), specific users can be prioritized during peak traffic times, and updates can be rescheduled outside of working hours.



Top Bandwidth Consuming Sources/Destinations

One of the most telling ways to analyze bandwidth is by looking at destinations and sources generating the most traffic. Common destination sites (e.g. external websites), such as those for OS/firmware updates, can be throttled to allow prioritized, business critical traffic. Internally, high traffic hosts can be optimized through traffic shaping or corporate use policies.



Utilization

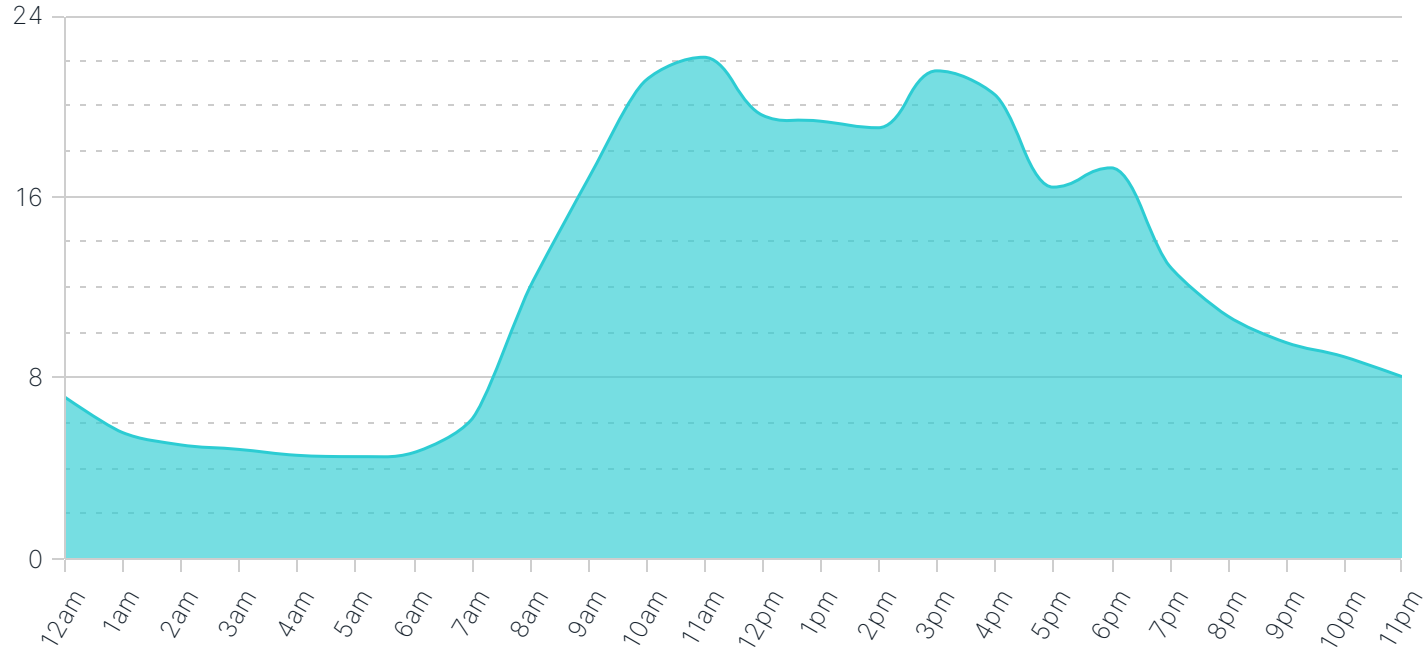
Top Source Countries

By looking at IP source traffic, we can determine the originating country of any particular request. Certain botnets, command and control functions, and even remote access can be session heavy and indicative of targeted attacks or persistent threats from nation-states. This chart is representative of country-based traffic - activity from specific originating nations may be anomalous and warrant further investigation.

#	Country	Bandwidth
1	United States	213.31 MB
2	Anonymous Proxy	7.73 MB
3	United Kingdom	4.13 MB
4	Belgium	1.51 MB
5	Netherlands	603.07 KB
6	Ireland	389.32 KB
7	Romania	47.75 KB
8	Russian Federation	37.82 KB
9	France	26.88 KB
10	China	4.12 KB

Average Log Rate by Hour

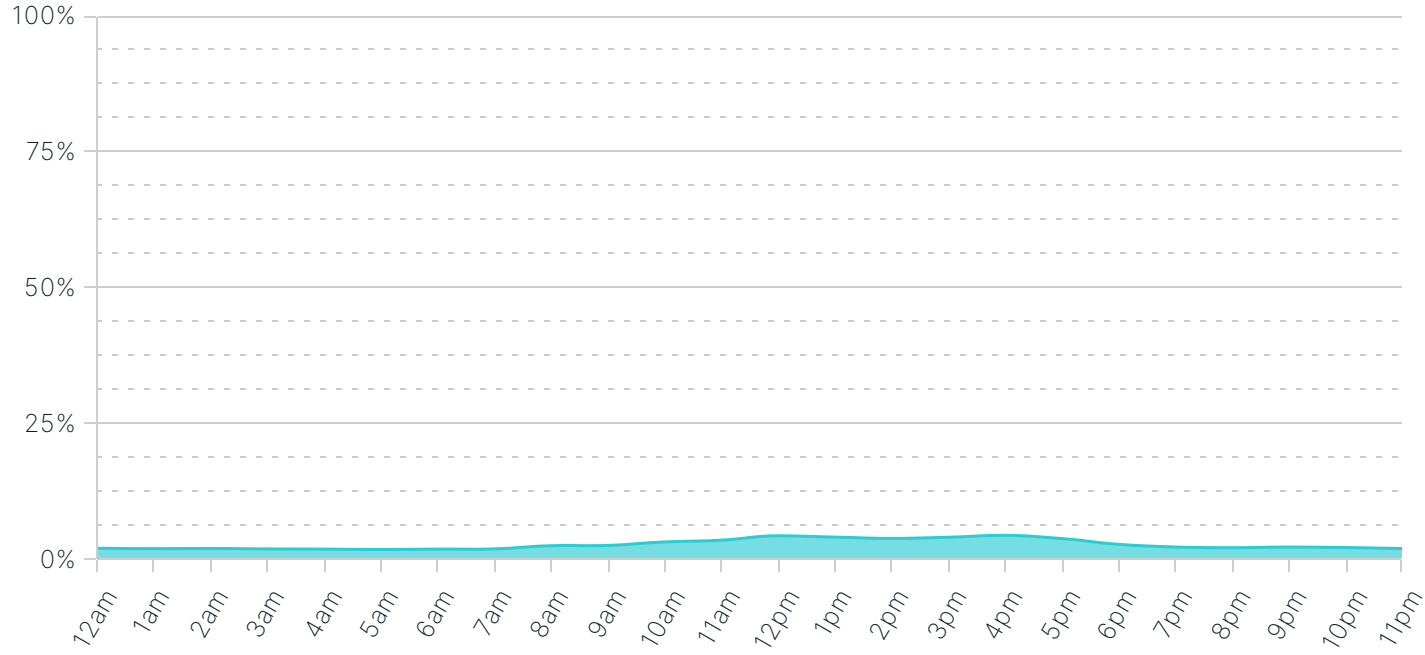
Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream logging/analytics devices such as FortiAnalyzer. Keep in mind, the log rates presented here are with the full logging capabilities of the FortiGate enabled and will include all log types (traffic, anti-virus, application, IPS, web and system events).



Utilization

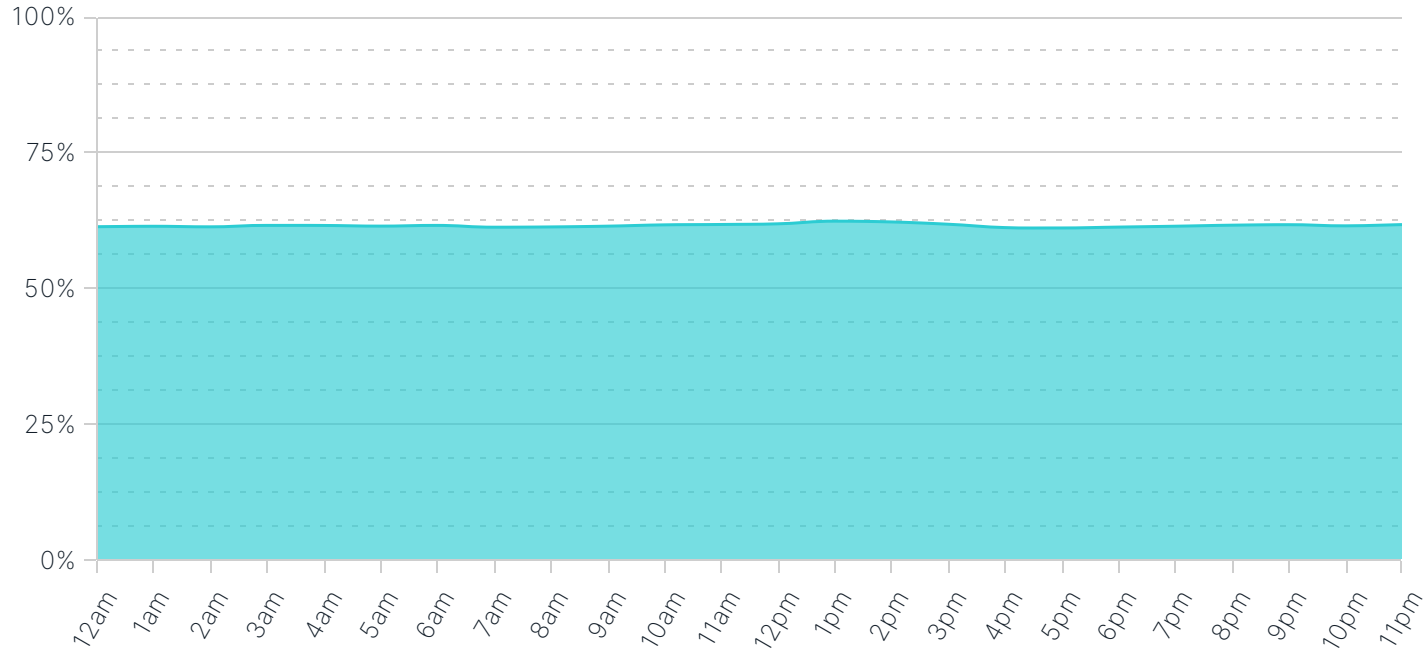
Average FortiGate CPU Usage by Hour

CPU usage of a FortiGate is often used to size a final solution properly. By looking at an hourly breakdown of CPU utlilization statistics, it's easy to get a good idea about how FortiGates will perform in the target network. Typically, with higher throughput, more logs are generated. If 75% or more utilization is sustained over a long period of time, either a more powerful model or revised architecture may be required for final implementation.



Average FortiGate Memory Usage by Hour

Similarly, memory usage over time is an indicator of the FortiGate's sustainability in the target network environment. Memory usage may remain high even when throughput is relatively low due to logging activity (or queued logging activity) over time.



Recommendations

1. Quarantine Botnet Hosts

Botnet activity was detected on at least one host within your network. You should immediate quarantine any botnet hosts (e.g. remove them from the network) and investigate any associated breach activity.

2. Augment Your Email Security to Protect Against Known Malware

Known malware is currently bypassing your existing security gateway. We recommend that you verify the malware signatures on your existing security gateway are up to date. If those signatures are already current, consider augmenting your security with a secondary firewall or replacing your existing gateway solution.

3. Add Sandboxing Technology to Detect Unknown Malware

Files exhibiting suspicious behaviors (potentially unknown malware) were detected. Consider implementing sandboxing technology to supplement your gateway security solution.

4. Improve Malicious URL Detection and Training

Websites containing known malicious URLs are being accessed from your organization and may be circumventing web filtering controls. We suggest two courses of action: 1) ensure your existing web filtering controls are using up to date blacklists 2) train your email users to never click on unknown URLs.

5. Educate and Protect Users from Phishing Attempts

We detected visited URLs which were an attempt to extract sensitive information from your internal users. Ensure that you have: 1) trained your email users how to determine legitimate senders 2) implemented an email gateway which can detect and mitigate modern phishing attacks.

6. Audit High Risk Hosts for Attack Susceptibility

Some hosts on your network are exhibiting a high degree of suspicious behavior (which could include originating lateral attacks, potential malware installation, or botnet activity detected). Review the hosts most at risk, and quarantine those devices until you can determine the root cause of the suspicious behavior.

7. Enforce Corporate Use Policies on Peer to Peer Applications

Peer to peer applications were detected on your network. Some organizations allow P2P applications, but many are surprised to learn their network is engaged in unwarranted file sharing. Assuming your organization disallows P2P use, identify the originating hosts and use this opportunity to train your users on proper corporate use of organizational resources.