Secure SD-WAN Assessment Report

Prepared For
Informata College

Prepared By
John Smith
Fortinet

Report Date
Aug 28, 2019

Executive Summary

We aggregated key findings from our Secure SD-WAN 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 as well for actionable steps your organization can take to optimize your network for Direct Internet Access, protect your organization from external/branch office threats, and ultimately save money.

Applications

143
External (Potential DIA) Applications

22.8%
Percentage of Cloud IT Traffic

5.8%
Percentage of VoIP/Audio/Video Traffic

Application usage should have a strong influence on your network architecture. Understanding which types of applications are used and specifically business application performance can improve user experience and productivity.

Security

11,126
Application Vulnerability Attacks Detected

13
Malware and/or Botnets Discovered

17
High Risk Applications Detected

Maintaining a full security stack at the WAN edge is critical in any SD-WAN deployment where public Internet circuits are leveraged. 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).

Utilization

40.5GB
Total Bandwidth Used

23.5%
Percentage of Non-Business Traffic

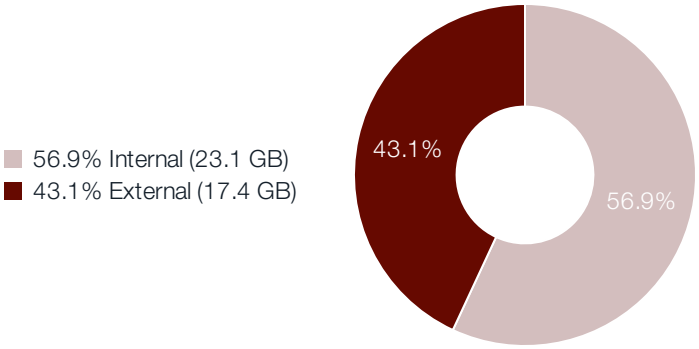
58.0%
Percentage of SSL Encrypted Traffic

In addition to individual applications, understanding overall utilization can help with capacity planning, circuit selection, and streamlining network traffic over time. This awareness can also help reduce operational costs associated with backhauling traffic over more expensive WAN links (such as MPLS).

Applications

Quick Stats

- **143** external (potential DIA) applications
- **43.1%** percentage of external traffic
- **22.8%** percentage of Cloud IT traffic
- **5.8%** percentage of VoIP/Audio/Video traffic
- **SSL** is the most used external application
- **Network.Service** is the top application category

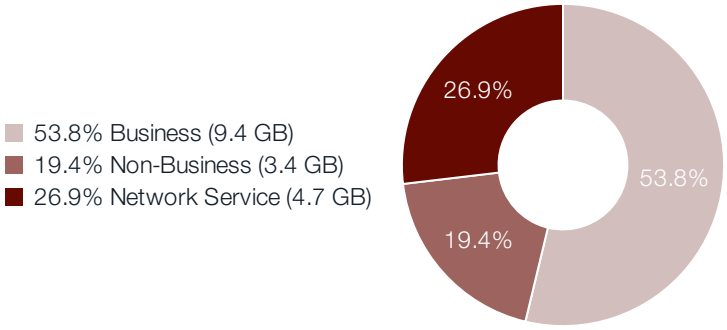


Internal vs. External Traffic

Before setting up an SD-WAN architecture, it's useful to understand high-level traffic flows. By examining applications that are communicating externally, you can begin to calculate costs associated with WAN links (such as typically more costly MPLS lines). Network traffic with either a source or destination address to an external IP address can generally be considered external traffic which is how we've calculated the chart to the left. External traffic can benefit greatly from utilizing broadband circuits for Direct Internet Access.

External Traffic Breakout

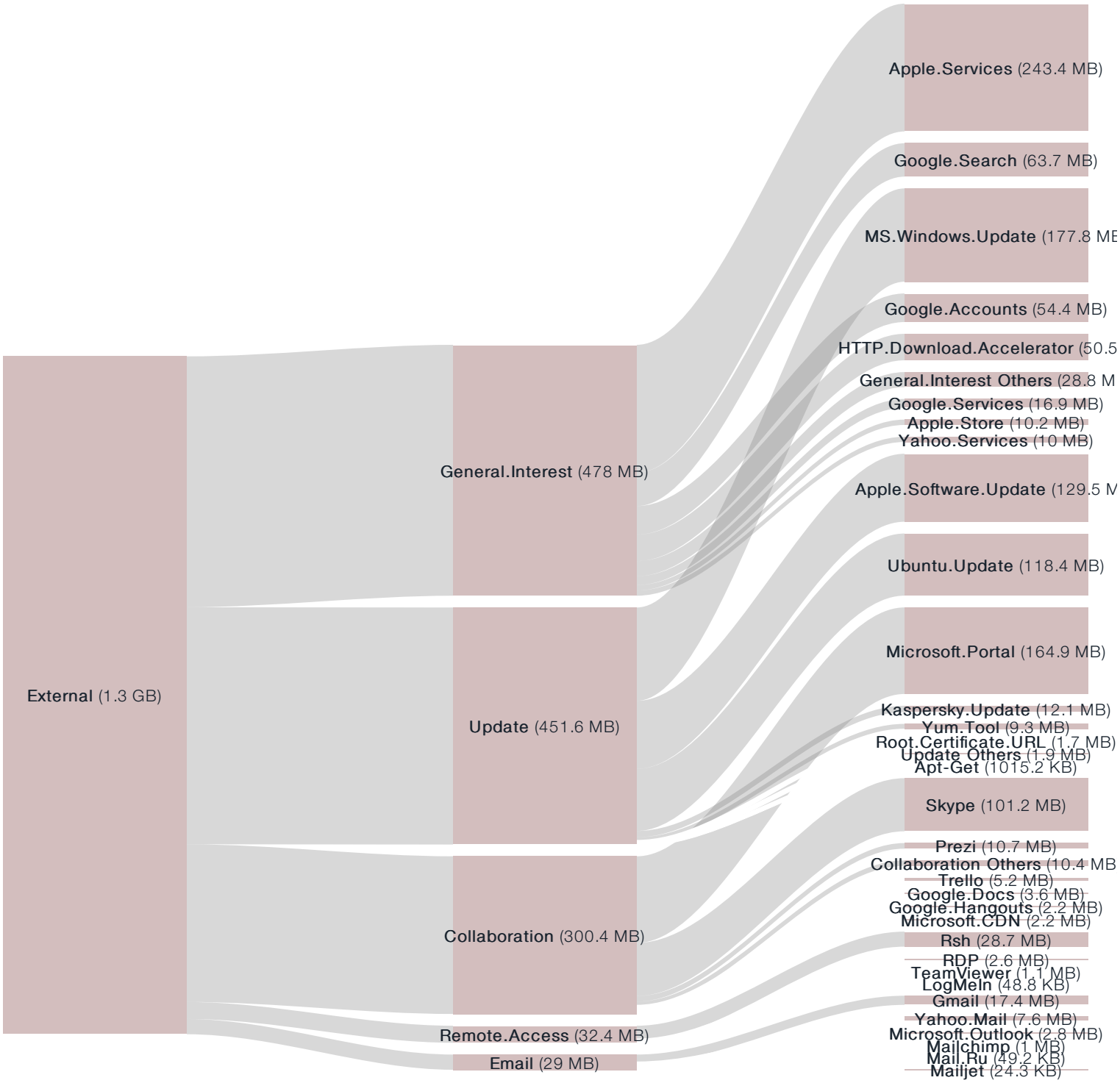
By categorizing internal hosts communicating with external servers, you can get a general sense for bandwidth requirements and how you may want to prioritize Direct Internet Access (DIA) applications within an SD-WAN deployment. Business applications that communicate directly with the Internet could be routed through a broadband circuit instead of backhauling to the datacenter through a dedicated link such as MPLS. This can result in significant savings not to mention increased throughput and lower latency. Non-business and network applications communicating externally can similarly be prioritized and routed.



Applications

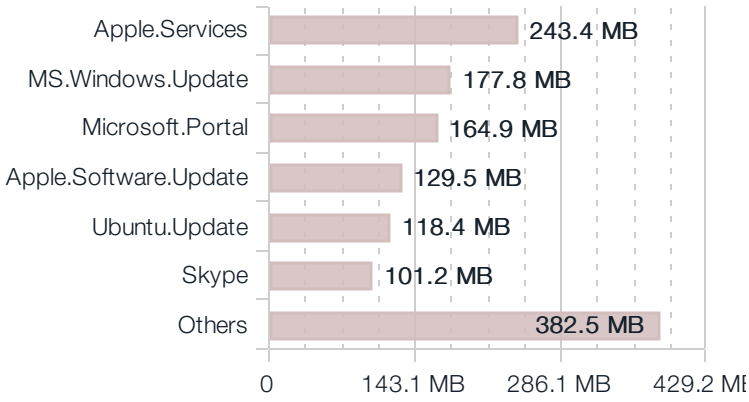
Potentially DIA Business Applications

This chart illustrates a breakout of important business applications specific to your network as ranked by bandwidth and grouped by the top five application categories. It does not include non-business (such as YouTube, Spotify, etc.) or Network Service (such as DNS, NTP, etc.) applications which could impact overall bandwidth. Instead, these are applications which can be prioritized by leveraging SD-WAN application steering strategies and Service Level Agreements (SLAs) in order to engineer their optimal path to the Internet.

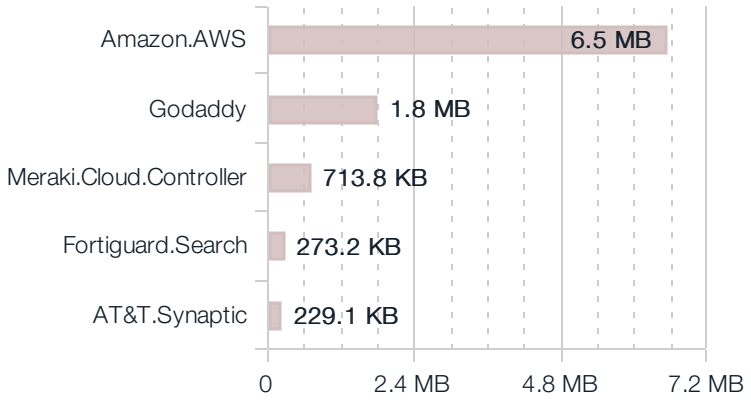


Applications

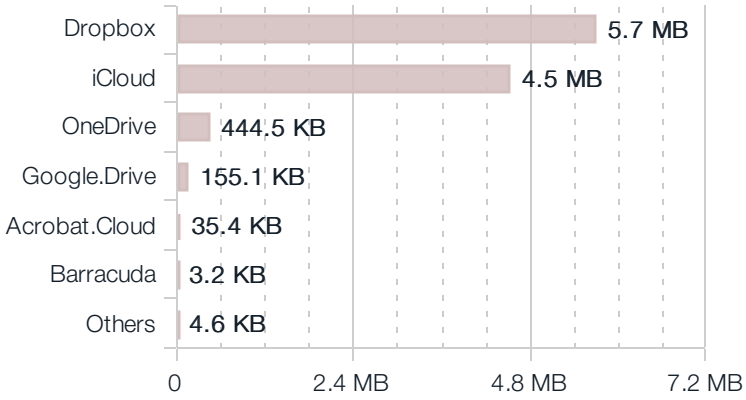
Top Business Applications



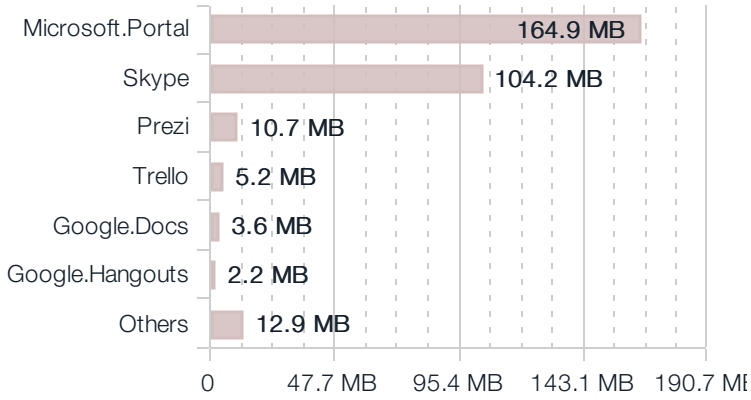
Top Cloud IT Applications



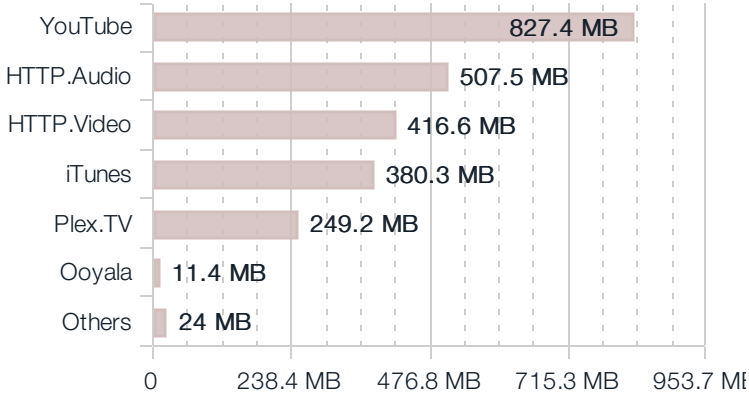
Top Storage Backup Applications



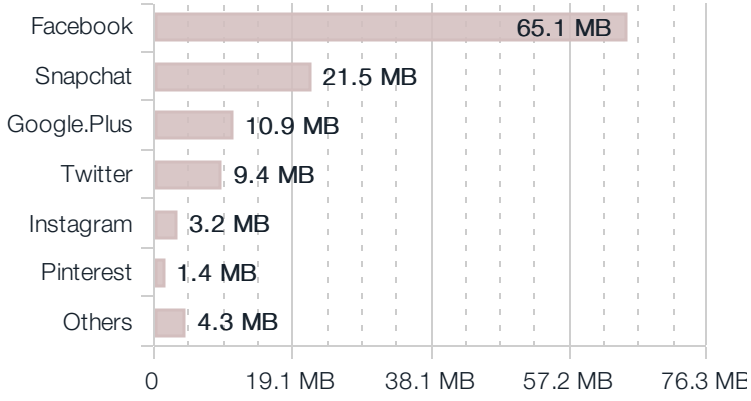
Top Collaboration Applications



Top VoIP/Audio/Video Applications



Top Social Media Applications



Security

Quick Stats

- **50** 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

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	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
4	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
5	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
6	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
7	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
8	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
9	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38
10	4	FlashGet	P2P	Peer-to-Peer	3	309.78 KB	37

Top Application Vulnerability Exploits Detected

The performance gains and cost savings from leveraging public Internet circuits in an SD-WAN deployment need to be protected by a full security stack at the WAN edge. Application vulnerabilities at the branch can be exploited to compromise the security of your entire 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

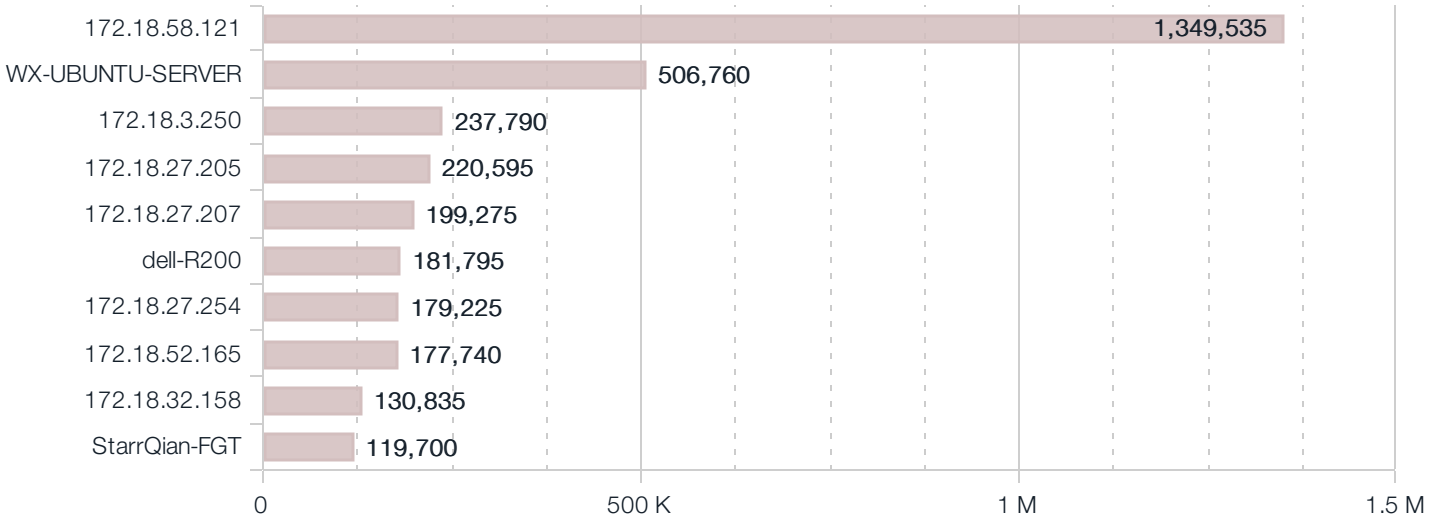
Top Malware, Botnets and Spyware/Adware Detected

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

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.



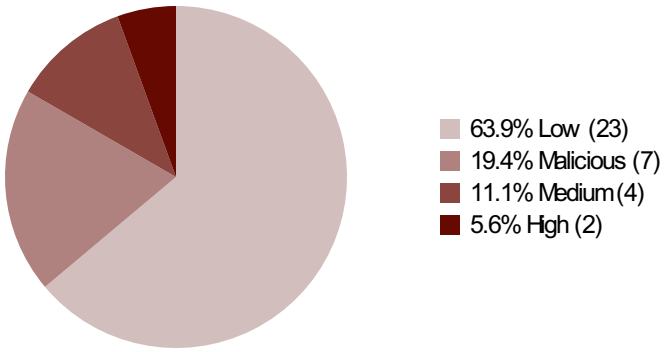
Unknown Malware

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	1
2	1D28E4E7.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	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 This file checked devices for anti-virtualization or anti-debug	1
4	1D45FCB7.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	1
5	1D46A1FA.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
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	1
7	1D46EE5B.vsc	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess Executable deleted itself after execution	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).



Utilization

Quick Stats

- **40.5 GB** total bandwidth used
- **23.5%** percentage of non-business traffic
- **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
- **11.8** average log rate per second
- **2.8%** average FortiGate CPU usage
- **61.7%** average FortiGate memory usage

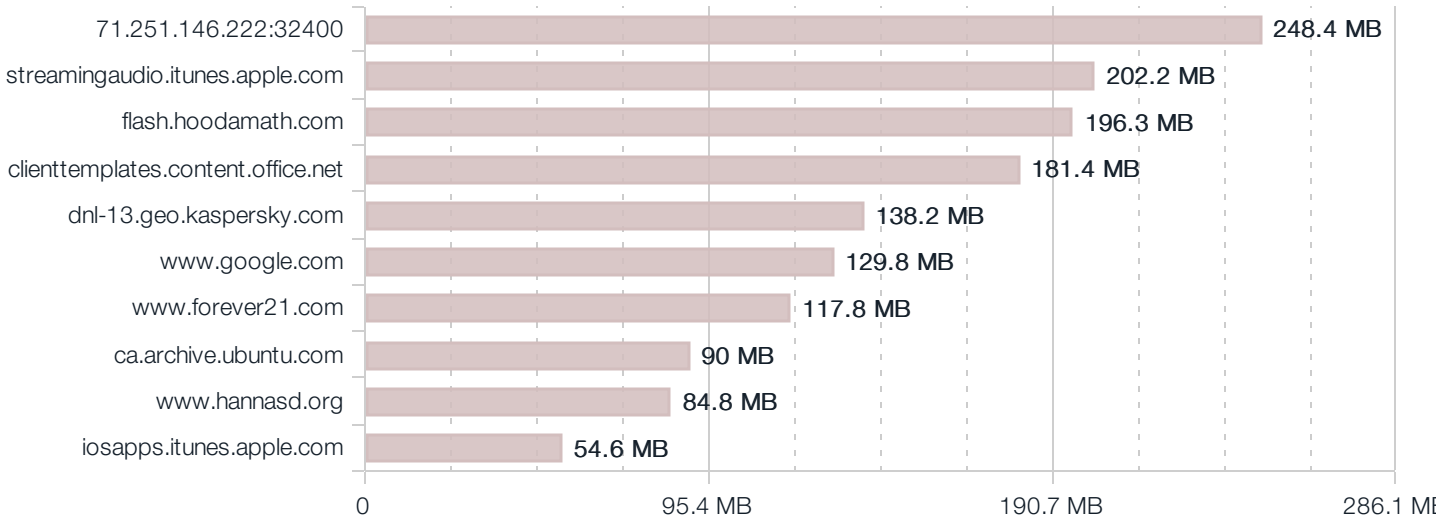
Top Source Locations

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

Top Bandwidth Consuming Sources/Destinations

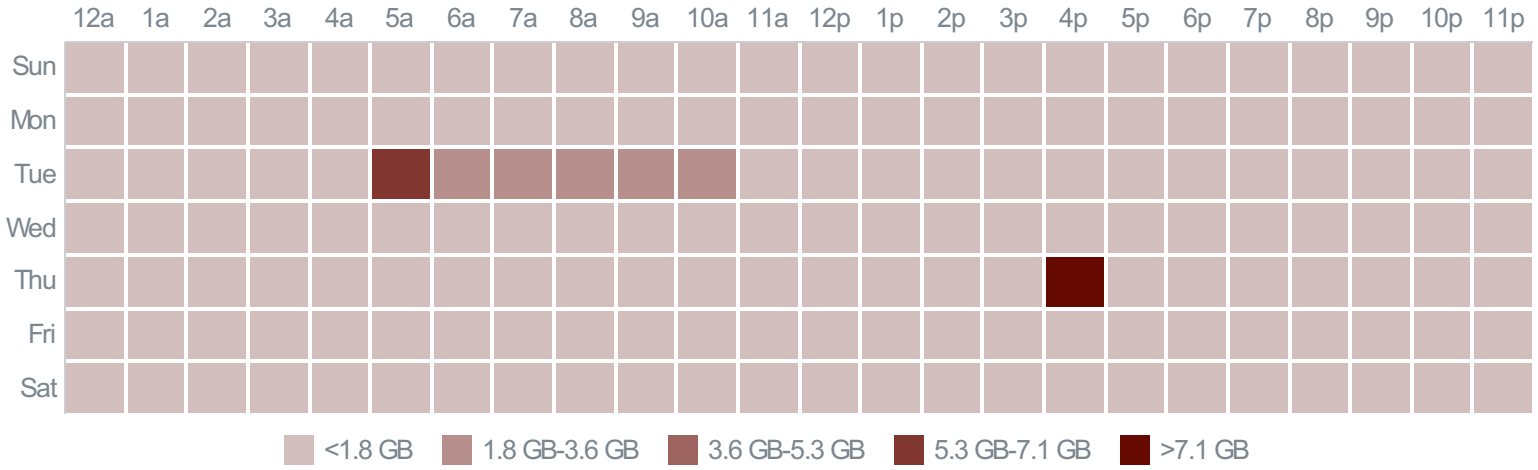
One of the most telling ways to analyze bandwidth is by looking at destinations and sources generating the most traffic. Common destination sites (e.g. external websites), such as those for OS/firmware updates, can be throttled to allow prioritized, business critical traffic. Internally, high traffic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



Utilization

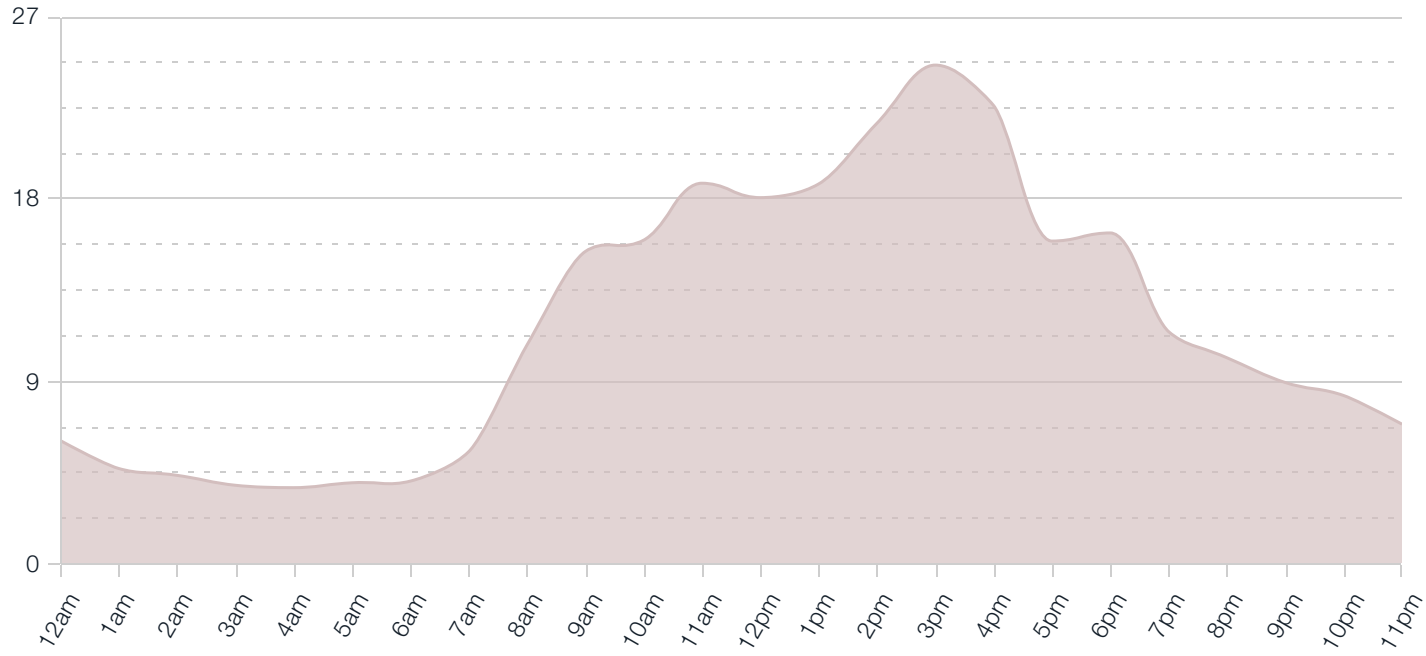
Average Bandwidth by Hour

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.



Average Log Rate by Hour

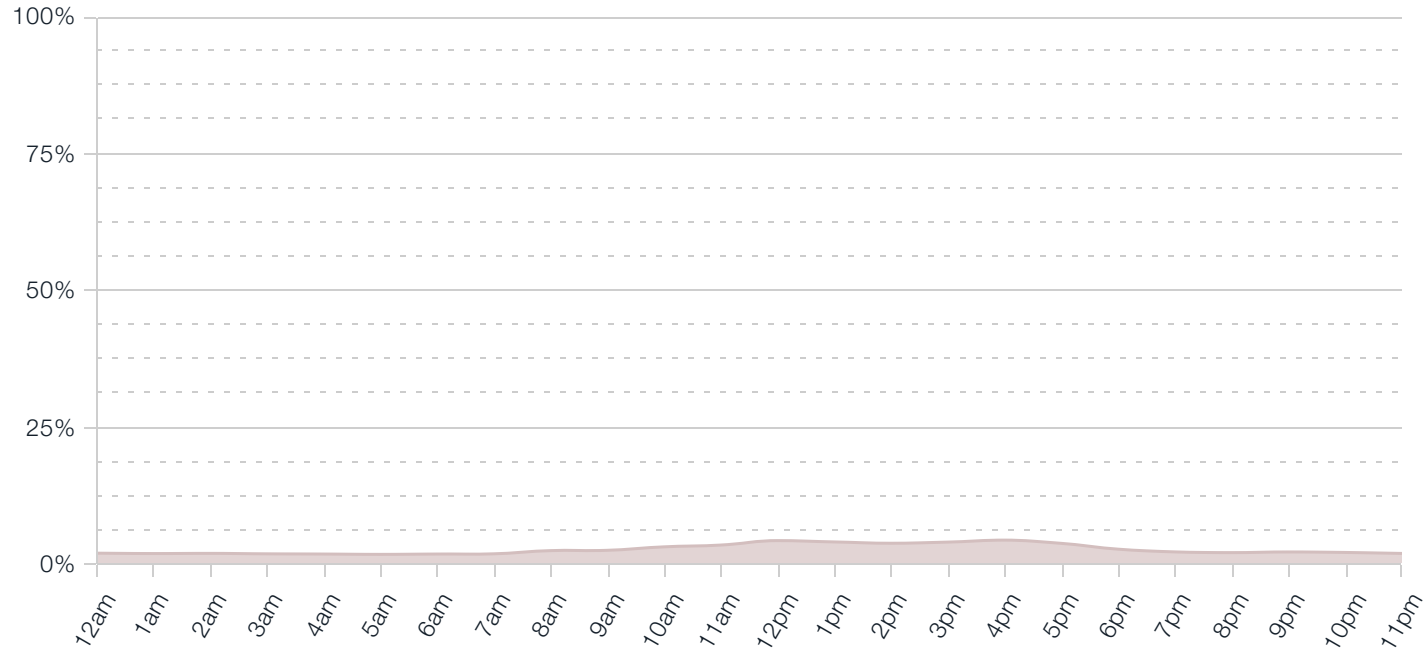
Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream 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

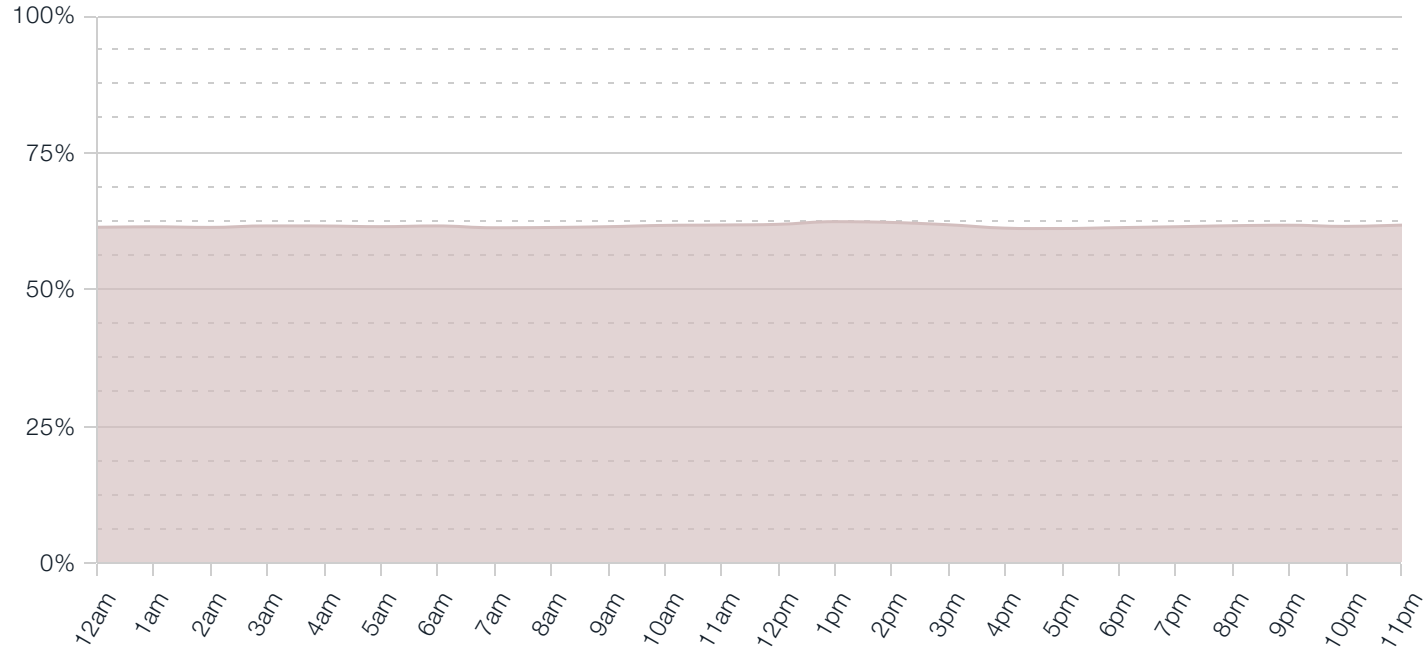
Average FortiGate CPU Usage by Hour

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. Leverage Direct Internet Access for External Traffic

Approximately 43.1% of all organizational traffic was classified as external. If you haven't done so already, weigh routing external traffic remotely versus backhauling through a centralized gateway. This will optimize traffic flows and reduce overall operational costs.

2. Create Service Level Agreements (SLAs) for Key Applications

A significant number of applications were detected which are communicating with external (e.g. cloud-based) servers. When architecting an SD-WAN rollout, ensure that these applications are selecting WAN links that meet performance (latency, jitter, and packet loss) criteria.

3. Route High Bandwidth Applications Through Broadband Circuits

We detected a large amount of high bandwidth applications (typically Audio/Video streaming, P2P, etc.) which are consuming your available bandwidth. If that traffic is originating from your branch offices, we suggest that you consider Direct Internet Access for those applications when setting up your SD-WAN.

4. Augment Your Security to Protect Against Known Malware

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

5. 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.

6. Inspect Encrypted Traffic

A significant amount of your organizational network traffic is encrypted. Contemplate implementing SSL inspection to ensure full application visibility and traffic inspection.