



# Cyber Threat Assessment Report

Date: March 30, 2015

Created for: ABC Corporation

# Vital Statistics

This document provides the findings of a recent analysis of your infrastructure. The document represents a summary of these findings and presents a set of recommendations for addressing the detected events. The analysis is based on data collected using the characteristics below:

## Company Details

**Company Name:** ABC Corporation

**Location:** Santa Clara, CA

**Industry:** Technology

**Company Size:** 5,500 Employees

## Test Details

**Test Start Date:** 3/20/2015

**Test Duration:** 7 Days

**FortiGate Model:** FortiGate-300D

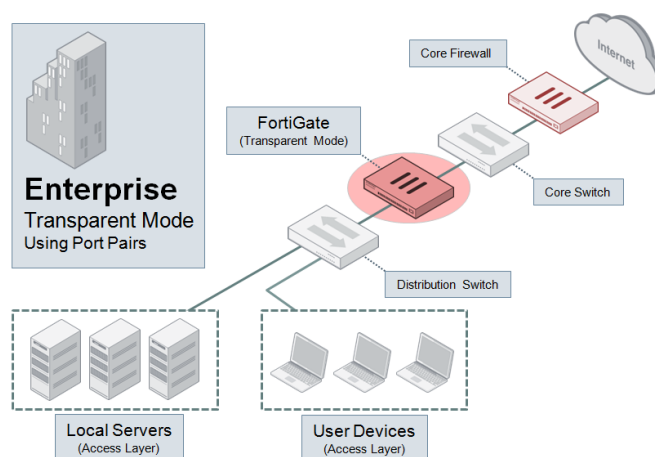
**FortiOS Firmware:** 5.2.2

**Network Analyzed:** Internal LAN

**Functions Enabled:** IPS / AV / Web / App Ctrl

## Deployment and Methodology

The internal network was monitored with a FortiGate-300D (transparent mode using port pairs). This is a non-invasive way to intercept traffic as it moves over your network. The diagram below demonstrates the assessment topology used.



During this assessment, traffic was monitored as it moved over the wire and logs were recorded. These logs are typically categorized by their log type. While traffic logs record much of the session information flowing across your network, Fortinet can also monitor more in-depth security logging, such as IPS, anti-virus, web and application control. This assessment was created based on telemetry from all log types and is meant to provide a big picture view of your network's activity. Used in conjunction with FortiAnalyzer, FortiGates can provide additional functions such as event management (e.g. alerts when malicious activity is detected), FortiView analytics and filtering (e.g. investigating specific user activity) and advanced reporting (e.g. detailed reports on security, user and even wireless activity).

# Executive Summary

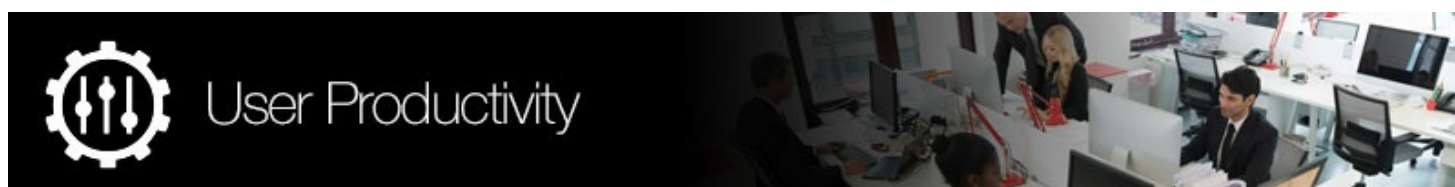


**IPS attacks detected:** 1,592

**Malware & botnet events detected:** 73

**High risk applications detected:** 296

Last year, over 780 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at \$3.5 million USD and is rising at 15% year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to your most sensitive files and database information. FortiGuard Labs mitigates these risks by providing award-winning content security and is consistently rated among industry leaders by objective third parties such as NSS Labs, VB 100 and AV Comparatives.

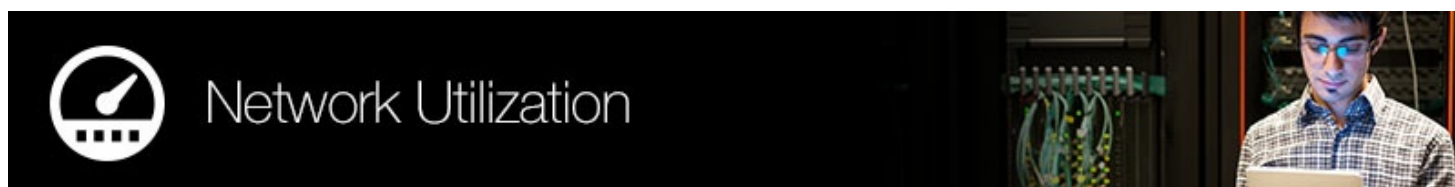


**Application Categories:** Network.Service / Video/Audio / Web.Others

**Top 3 Web Categories:** Shopping and Auction / Streaming Media and Download / Web-based Email

**Top 3 Web Domains:** mail.google.com / stream.pandora.com / en.wikipedia.org

User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that businesses must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity. All of which expose the company to undue liability and potential damages. With over 5,800 application control rules and 250 million categorized websites, FortiGuard Labs provides telemetry that FortiOS uses to keep your business running effectively.



**Top Hosts/Clients by Bandwidth:** 8.1.0.215 / 10.1.82.175 / 8.1.0.222

**Average Throughput:** 28 Mbps

**Unique Hosts Detected:** 664

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetics indicates that 77% of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year. FortiGates leverage FortiASICs to accelerate CPU intensive functions such as packet forwarding and pattern matching. This offloading typically results in a 5-10X performance increase when measured against competitive solutions.

# Recommended Actions

## Botnet Infections ( 0 )

Bots can be used for launching denial-of-service (DoS) attacks, distributing spam, spyware and adware, propagating malicious code, and harvesting confidential information which can lead to serious financial and legal consequences. Botnet infections need to be taken seriously and immediate action is required. Identify botnet infected computers and clean-up the computers using AntiVirus software. Fortinet AntiVirus product FortiClient can be used to scan the infected computers and remote botnets from the computer.

## Evasive Applications ( 42 )

Proxy applications are often used to conceal their activity and bypass the security control. This represents both business and security risks to your organization. Implement the application policies to dictate the use of these applications.

## P2P and Filesharing Applications ( 10 )

These applications can be used to bypass existing content controls and lead to unauthorized data transfer and data policy violations. Policies on appropriate use of these applications need to be implemented.

## Bandwidth Consuming Applications ( 61 )

Applying application policies to regain control in the use of these applications. One of the options would be a traffic shaping rule to limit consumption.

## Deploy a Fortinet Next Generation Firewall to Ensure Application Visibility and Control

Fortinet next-generation firewalls enable organizations to gain visibility on all application traffic and deliver scalable and secure application control for enterprises. Deploying a Fortinet firewall in your organization and creating secure application policies to ensure that your network is being used according to the organization's priorities.

# Security and Threat Prevention

## 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.

### High Risk Applications Crossing the Network

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	4	RDP	Remote.Access	Client-Server	80	23.53 MB	5,830
2	4	Meraki.Cloud.Controller	Cloud.IT	Client-Server	641	10.12 MB	2,501
3	4	Rlogin	Remote.Access	Client-Server	4	2.52 KB	99
4	4	VNC	Remote.Access	Client-Server	1	798 B	25
5	4	Synergy	Remote.Access	Client-Server	1	4.05 KB	25
6	4	Dameware.Remote	Remote.Access	Client-Server	1	7.07 KB	1

Figure 1: Highest risk applications sorted by risk and sessions

## Application Vulnerability Exploits

An application vulnerability could be exploited to compromise the security of the network. The FortiGuard research team analyses application traffic patterns and application vulnerabilities and then develops signatures to prevent the vulnerability exploits. The FortiGuard Intrusion Prevention Service (IPS) provides Fortinet customers with the latest defenses against stealthy network-level threats. It uses a customizable database of more than 5,800 known threats to stop attacks that evade traditional firewall systems. For Application Vulnerability and IPS see: <http://www.fortiguard.com/static/intrusionprevention.html>.

### Top Application Vulnerability Exploits Detected

#	Severity	Threat Name	Type	Victim	Source	Count
1	5	HTTP.URI.Overflow		9	9	8,891
2	5	HTTP.Chunk.Overflow	Numeric Errors	3	4	4,562
3	5	IBM.Domino.iNotes.Buffer.Overflow	Buffer Errors	3	3	2,675
4	5	Minishare.HTTP.Server.Buffer.Overflow	Buffer Errors	1	1	2,278
5	5	MS.Windows.Message.Queuing.Remote.Buffer.Overflow	Buffer Errors	2	2	2,277
6	5	MS.SMB.DCERPC.WKSSVC.NetrJoinDomain2.Buffer.Overflow	Buffer Errors	2	2	2,226
7	5	MS.Windows.IGMP.Integer.Overflow	Numeric Errors	1	1	1,823
8	5	MS.Windows.RPC.DNS.Service.Buffer.Overflow	Buffer Errors	2	2	1,811
9	5	Sun.Solaris.rpc.yppupdated.Remote.Command.Execution	Code Injection	1	1	1,574
10	5	MS.Windows.PnP.Buffer.Overflow	Buffer Errors	1	1	1,173

Figure 2: Top vulnerabilities identified, sorted by severity and count

## Malware 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-related events which indicate malicious file downloads or connections to malware-infested sites.

### Top Viruses, Spyware and Adware Detected

#	Malware Name	Type	Application	Victim	Source	Count
1	<a href="#">W32/FakeAV.OY!tr</a>	Virus	Wikipedia	33	30	33
2	<a href="#">W32/Zbot.ANM!tr</a>	Virus	YouTube.Video.Embedded	31	26	31
3	<a href="#">W32/Jorik.EF78!tr</a>	Virus	Youtube	30	28	30
4	<a href="#">W32/Agent.RNI!tr</a>	Virus	Wikipedia	30	25	30
5	<a href="#">W32/Agent.RNI!tr</a>	Virus	YouTube.Video.Embedded	30	27	30
6	<a href="#">W32/Agent.RNI!tr</a>	Virus	Youtube	29	22	29
7	<a href="#">W32/Simda.B!tr</a>	Virus	Youtube	29	26	29
8	<a href="#">W32/Zbot.ANM!tr</a>	Virus	HTTP.BROWSER	28	23	28
9	<a href="#">W32/FakeAV.OY!tr</a>	Virus	HTTP.BROWSER	27	25	27
10	<a href="#">W32/Simda.B!tr</a>	Virus	HTTP.BROWSER	27	21	27

Figure 3: Common Viruses, Spyware and Adware detected

## Botnets Detected

A bot is malicious software that invades your computer. Bots allow criminals to remotely control computer systems and execute illegal activities without user's awareness. These activities can include: stealing data, spreading spam, distributing malware, participating in Denial of Service attacks and more. Bots are often used as tools in targeted attacks known as Advanced Persistent Threats (APTs). A botnet is a collection of such compromised computer systems.

### Top Command and Control Botnets Detected

#	Malware Name	Type	Application	Victim	Source	Count
1	<a href="#">W32/FakeAV.OY!tr</a>	Virus	Wikipedia	33	30	33
2	<a href="#">W32/Zbot.ANM!tr</a>	Virus	YouTube.Video.Embedded	31	26	31
3	<a href="#">W32/Jorik.EF78!tr</a>	Virus	Youtube	30	28	30
4	<a href="#">W32/Agent.RNI!tr</a>	Virus	Wikipedia	30	25	30
5	<a href="#">W32/Agent.RNI!tr</a>	Virus	YouTube.Video.Embedded	30	27	30
6	<a href="#">W32/Agent.RNI!tr</a>	Virus	Youtube	29	22	29
7	<a href="#">W32/Simda.B!tr</a>	Virus	Youtube	29	26	29
8	<a href="#">W32/Zbot.ANM!tr</a>	Virus	HTTP.BROWSER	28	23	28
9	<a href="#">W32/FakeAV.OY!tr</a>	Virus	HTTP.BROWSER	27	25	27
10	<a href="#">W32/Simda.B!tr</a>	Virus	HTTP.BROWSER	27	21	27

Figure 4: Top Botnets attempting to communicate with Command and Control hosts

## 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.

### Most At-Risk Devices and Hosts











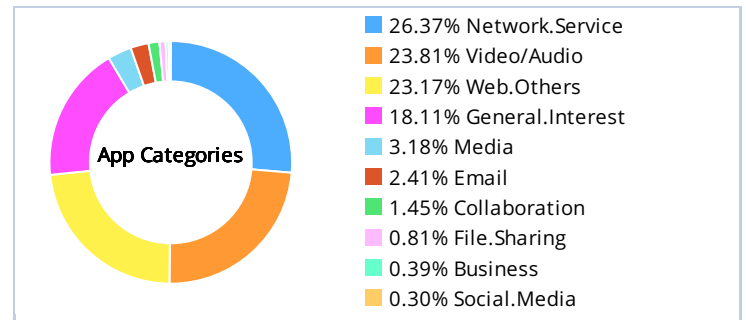
#	Device	Scores
1	 192.168.1.110	41,500
2	 8.1.0.218	39,840
3	 8.1.0.215	28,215
4	 8.1.0.222	12,770
5	 a4:5d:36:58:bb:8e	11,760
6	 10.1.82.175	7,870
7	 28:80:23:d5:e3:03	7,810
8	 8.1.0.230	7,130
9	 a4:5d:36:58:aa:63	6,750
10	 00:24:81:8d:b8:61	6,560

Figure 5: These devices should be audited for malware and IPS susceptibility

# User Productivity

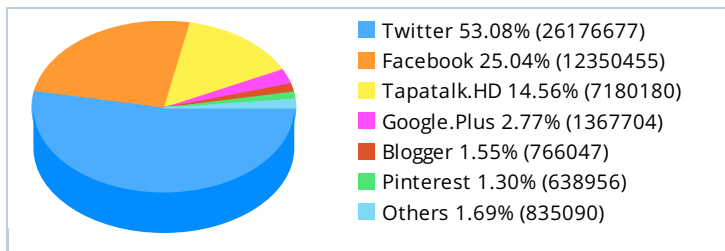
## Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: <http://www.fortiguard.com/encyclopedia/applications>

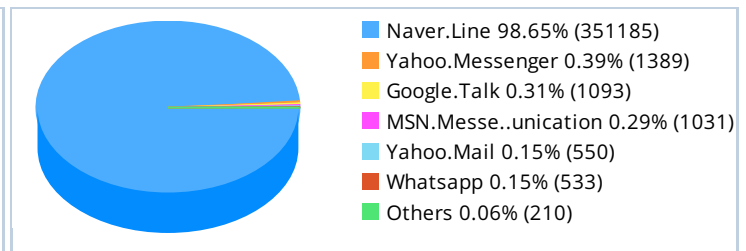


Understanding application subcategories can give invaluable insights into how efficiently your corporate network is operating. Certain application types (such as P2P or gaming applications) are not necessarily conducive to corporate environments and can be blocked or limited in their scope. Other applications may have dual purpose uses (such as instant messenger or social media apps) and can be managed accordingly. These charts illustrate application categories sorted by the amount of bandwidth they used during the discovery period.

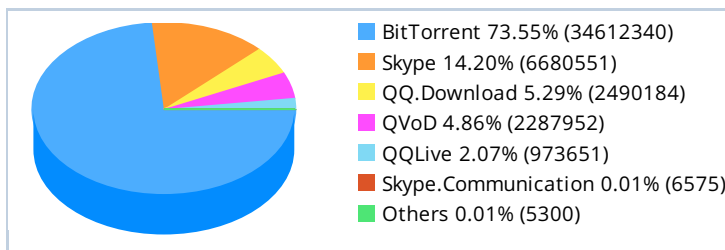
### Top Social Media Applications



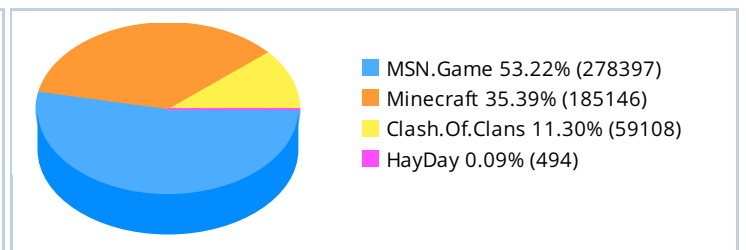
### Top Instant Messaging Applications



### Top Peer to Peer Applications



### Top Gaming Applications





## Web Usage

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.

### Top Web Categories

#	URL Category	User	Count	Bandwidth
1	Shopping and Auction	126	752	244.79 KB
2	Streaming Media and Download	120	674	228.79 MB
3	Web-based Email	115	570	187.19 KB
4	Information Technology	113	554	1.12 MB
5	Social Networking	109	478	861.01 KB
6	File Sharing and Storage	105	460	79.78 MB
7	Internet Radio and TV	109	444	1,009.68 KB
8	Reference	100	390	3.08 MB

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.

### Top Web Applications

#	Application	Sessions	Bandwidth
1	HTTP.BROWSER	298,833	3.52 GB
2	HTTP.Video	5,349	2.00 GB
3	SSL	243,338	1.29 GB
4	YouTube	7,093	1.04 GB
5	Ebay	39,603	861.80 MB
6	Android.Market	16,767	608.01 MB
7	HTTP.Audio	247	582.94 MB
8	Youtube	586	419.58 MB

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.

### Top Web Domains

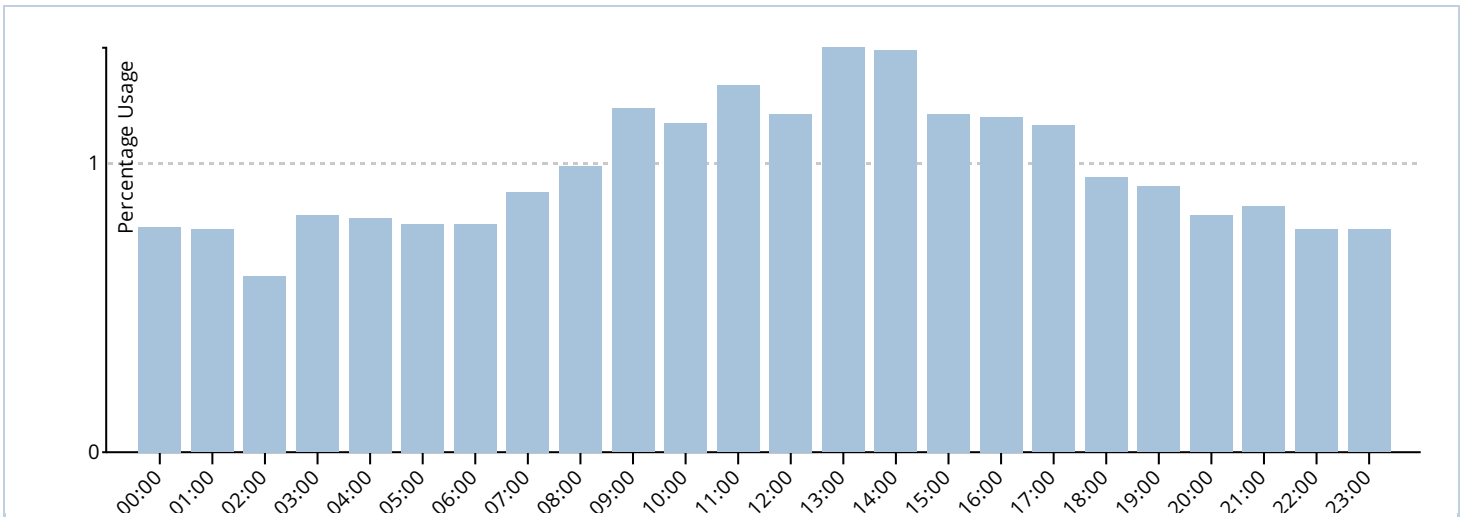
#	Domain	Category	Visits
1	mail.google.com	Web-based Email	416
2	stream.pandora.com	Internet Radio and TV	334
3	en.wikipedia.org	Reference	306
4	youtube.com	Streaming Media and Download	300
5	accounts.google.com	Search Engines and Portals	222
6	craigslist.org	Shopping and Auction	211
7	webex.com	Information Technology	184
8	linkedin.com	Business	183

# Network Utilization

## Bandwidth and Sessions

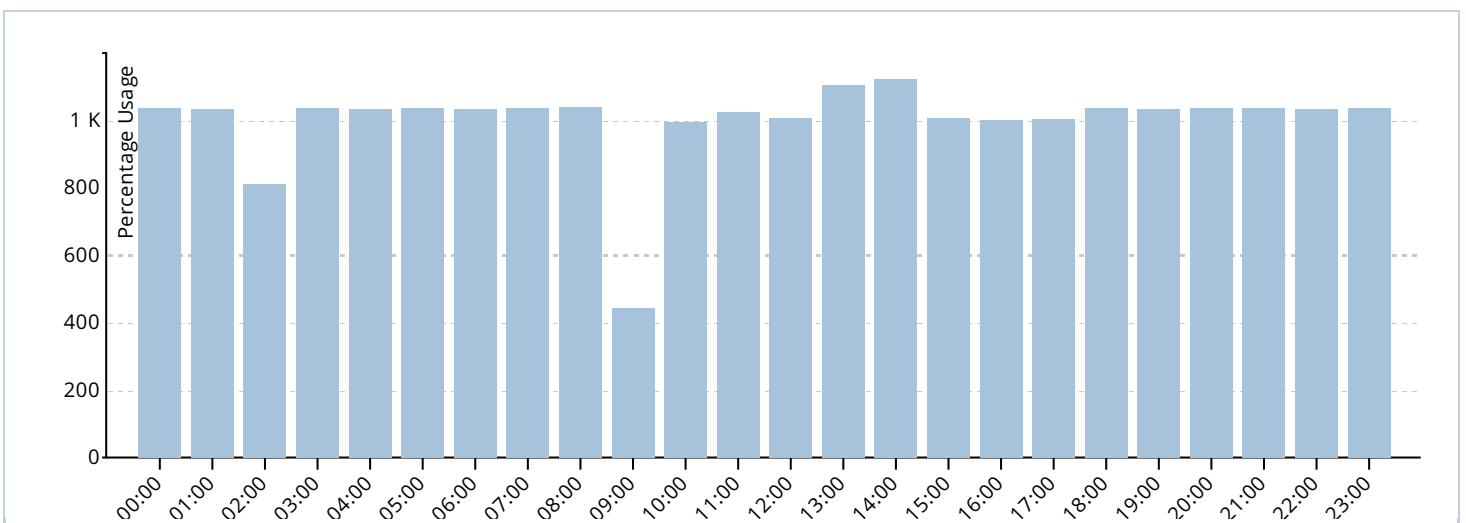
Bandwidth usage is the primary indicator for throughput and capacity planning. FortiGates can analyze bandwidth by application usage or by host. In addition, looking at daily usage trends can assist with peak capacity planning.

### Average Bandwidth Usage by Hour



Session averages on a daily basis are useful for calculating throughput and proper sizing. It can help when determining peak planning as a typical enterprise will see more sessions being generated in the morning when the network is at its most active.

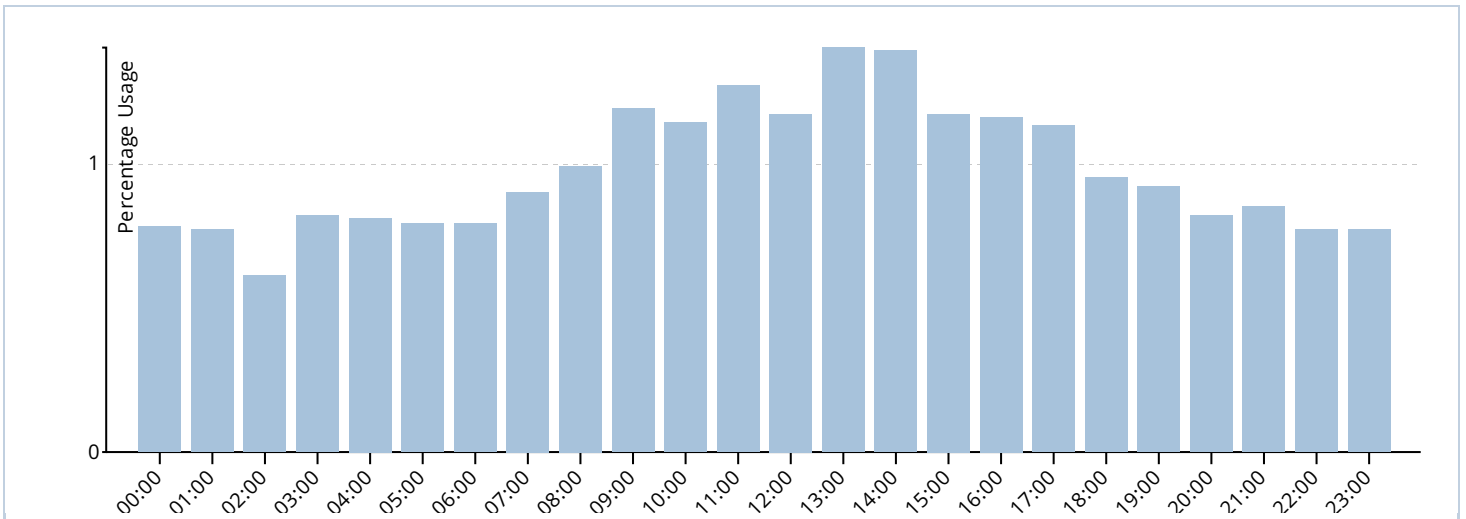
### Average Session Usage by Hour



## Firewall Statistics

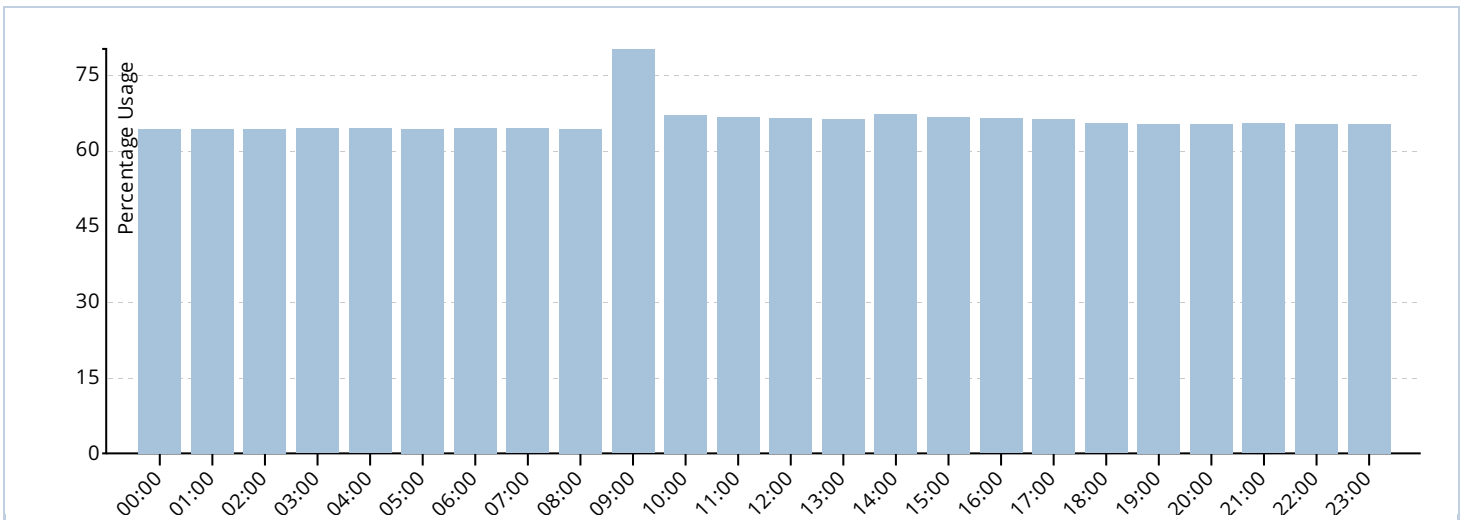
CPU usage of a FortiGate is often used to size a final solution properly. By looking at an hourly breakdown of CPU utilization statistics, it's easy to get a good idea about how FortiGates will perform in the target network. Typically, with higher throughput, more logs are generated. If 90% or more utilization is sustained over a long period of time, either a new model or revised architecture may be required for final implementation.

### Average CPU 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.

### Average Memory Usage by Hour



## Appendix A: About FortiGuard Key Services

Fortinet next-generation firewalls provide the visibility to detect advanced threats within legitimate content, even from trusted sources and authorized applications. This protection safely enables new applications into your network, but automatically block any malicious content or behavior. FortiGuard delivers rapid product/service updates and detailed security knowledge, providing protection from new and emerging threats.

### AntiVirus

The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to enable FortiGate, FortiMail, and FortiWiFi appliances, and FortiClient end point security agents, to prevent both new and evolving threats from gaining access to your network and its valuable content and applications.

### AntiSpam

The FortiGuard AntiSpam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages.

### Application Control

Application Control protects managed desktops and servers by allowing or denying network application usage based on policies established by the network administrator. Enterprise applications, databases, web mail, social networking applications, IM/P2P, and file transfer protocols can all be identified accurately by sophisticated detection signatures. Application Control signature updates are provided via the global FortiGuard distribution network.

### Intrusion Prevention

The FortiGuard Intrusion Prevention Service provides Fortinet customers with the latest defenses against stealthy network-level threats. It uses a customizable database of more than 5,100 known threats to enable FortiGate and FortiWiFi appliances to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats for which no signature has yet been developed. The combination of known and unknown threat prevention enables FortiGate systems to stop the most damaging attacks at the network border regardless of whether the network is wired or wireless, or whether it is at corporate headquarters or a branch office.

### IP Reputation

The FortiGuard IP Reputation Service aggregates data from locations and sources around the world that collaborate to provide up to date information about threatening sources. With breaking intelligence from distributed network gateways combined with world class research done from FortiGuard Labs, organizations can stay up to date and proactively block attacks.

### Web Filtering

Web Filtering Service provides URL filtering to block access to harmful, inappropriate, and dangerous websites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose organizations to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on more than 75 web content categories, and more than 47 million rated websites - all continuously updated via the FortiGuard Network.

### Vulnerability Management Service

The FortiGuard Vulnerability Management Service enables organizations to minimize the risk of vulnerabilities by quickly discovering vulnerabilities, measuring the potential risk, and then providing the information necessary to mitigate those risks. Additionally, a compliance reporting function provides organizations with actionable reports that can identify areas for remediation. These policies are continuously updated to ensure OS regulatory compliance requirements are met and releases are delivered via the FortiGuard global distribution network.