Application and Risk Analysis

Report Date: November 3, 2014 05:17

Data Range: 2014-10-27 00:00 2014-11-02 23:59 PST (FAZ local)

FORTINET

Table of Contents

Application Control and Assessing Risks 3
Application Visibility is Critical 3
Complete Content Protection 3
Backed by FortiGuard 4

Top Application Users By Bandwidth 5
Top Users By Bandwidth 5

Top Application Users By Sessions 6
Top User Sources By Sessions 6

Client Reputation 7
Top Users By Reputation Scores 7
Top Devices By Reputation Scores 7

Application Usage By Category 8
Top 10 Application Categories By Bandwidth Usage 8
Application Categories By Bandwidth Usage 8

Applications Detected by Risk Behavior 9
Number of Applications by Risk Behavior 9
High Risk Applications 10

Key Applications Crossing The Network 11
Key Applications Crossing The Network 11

Applications Running Over HTTP 12
Top Applications Running Over HTTP 12

Top Web Categories Visited By Network Users 13
Top Web Categories By Sessions 13
Top Web Categories By Sessions/Bandwidth 13

Top Web Sites Visited By Network Users 14
Top Web Domains By Visits 14

Top Destination Countries By Browsing Time 15
Top Destination Countries By Browsing Time 15

Top Web Sites By Browsing Time 16
Top Web Sites By Browsing Time 16

Top Threats Crossing The Network 17
Top Threats Crossing The Network 17
Top Critical Threats Crossing The Network 17
Top High Threats Crossing The Network 17
Top Medium Threats Crossing The Network 17
Top Low Threats Crossing The Network 17
Top Info Threats Crossing The Network 17

Top 20 Viruses Crossing The Network 18

Top Viruses By Name 18

Top Virus Victims 19

Top Virus Victims 19

Malwares Discovered 19

Application Vulnerabilities Discovered 19

Data Loss Prevention Events 20

Top Data Loss Prevention Events 20

Notes 20

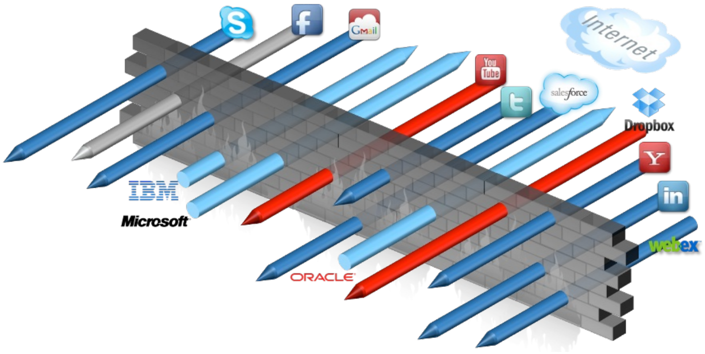
Appendix A 21

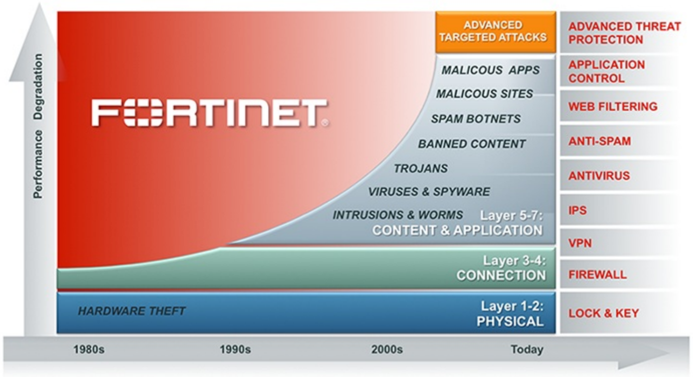
Devices 21

Application Control and Assessing Risks

Application Visibility is Critical

Application control provides granular policy enforcement of application traffic, even with the multitude of traffic using HTTP, which traditional firewalls and security gateways cannot distinguish. It includes the ability to identify more applications than any other vendor in the market, and to selectively block application behavior to minimize the risk of data loss or network compromise.



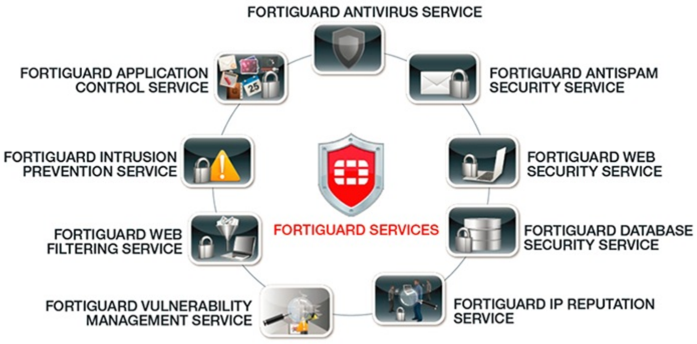


Complete Content Protection

Assessing network risks requires complete content protection, which is more than simply identifying applications and allowing or denying traffic. It is application control coupled with identity-based policy enforcement of all content. It enables organizations to utilize all the security and networking technologies included in the FortiGate platforms, such as access control, traffic shaping, IPS, DLP, and antivirus/antispyware. Complete content protection continuously protects networks against malicious content hidden within applications and data, even from trusted applications from trusted sources.

Backed by FortiGuard

Fortinet has been giving its customers the ability to deploy application-based security since FortiOS 3.0, enabling them to detect and manage applications independent of port or protocol. FortiGuard is the culmination of years worth of security research. New applications and potential threats are identified daily to keep your network up to speed.


FORTIGUARD ANTIVIRUS SERVICE
FORTIGUARD APPLICATION CONTROL SERVICE
FORTIGUARD ANTISPAM SECURITY SERVICE
FORTIGUARD INTRUSION PREVENTION SERVICE
FORTIGUARD WEB SECURITY SERVICE
FORTIGUARD SERVICES
FORTIGUARD WEB FILTERING SERVICE
FORTIGUARD DATABASE SECURITY SERVICE
FORTIGUARD VULNERABILITY MANAGEMENT SERVICE
FORTIGUARD IP REPUTATION SERVICE

Top Application Users By Bandwidth

This chart provides information about the users who are creating the most network traffic in terms of bandwidth usage. It helps the network manager to identify users that are potentially abusing network usage or creating traffic that does not comply with internal security policies. The following chart displays the top 20 users by bandwidth usage.

Top Users By Bandwidth

#	User (or IP)	Source IP	Bandwidth 🟦Traffic Out 🟨Traffic In
1	lrobertson	192.168.10.63	8.49 GB
2	bmatsubara	192.168.10.64	8.45 GB
3	ssalazar	192.168.10.253	8.44 GB
4	rcapobianco	192.168.10.145	8.43 GB
5	smetcalf	192.168.10.121	8.42 GB
6	jgroom	192.168.10.6	8.42 GB
7	cosullivan	192.168.10.228	8.41 GB
8	tramos	192.168.10.151	8.41 GB
9	awinters	192.168.10.125	8.41 GB
10	smagee	192.168.10.211	8.39 GB
11	eking	192.168.10.34	8.39 GB
12	hshaw	192.168.10.93	8.39 GB
13	pmadison	192.168.10.240	8.39 GB
14	vrodriguez	192.168.10.27	8.38 GB
15	bjordan	192.168.10.91	8.38 GB
16	cloomis	192.168.10.12	8.38 GB
17	kmcallister	192.168.10.216	8.37 GB
18	pharris	192.168.10.231	8.36 GB
19	chall	192.168.10.204	8.36 GB
20	szane	192.168.10.48	8.36 GB

Top Application Users By Sessions

The Top Users In Terms of Sessions section illustrates the quantity of network users who are opening the highest number of connections. This is a critical value because some users could open much more sessions than they are suppose to. Statistics on the amount of sessions a user has opened and the memory space used by these sessions is recorded in the FortiGate. The following chart displays the top 20 users by the number of sessions.

Top User Sources By Sessions

#	User (or IP)	Source IP	Sessions
1	10.88.41.10	10.88.41.10	164,986
2	dsimpson	192.168.10.49	86,743
3	tramos	192.168.10.151	86,684
4	cosullivan	192.168.10.228	86,595
5	rcrawford	192.168.10.229	86,504
6	lrobertson	192.168.10.63	86,503
7	ydalton	192.168.10.9	86,467
8	jtorres	192.168.10.186	86,460
9	smetcalf	192.168.10.121	86,437
10	esmith	192.168.10.246	86,434
11	sanderson	192.168.10.202	86,399
12	fzoller	192.168.10.79	86,390
13	ychen	192.168.10.79	86,380
14	pdavis	192.168.10.57	86,374
15	rramirez	192.168.10.152	86,359
16	ajohnson	192.168.10.204	86,339
17	psmith	192.168.10.206	86,306
18	handerson	192.168.10.242	86,287
19	hstiglitz	192.168.10.7	86,286
20	bjordan	192.168.10.91	86,276

Client Reputation

The Security scan types available on FortiGate units are varied and tailored to detect specific attacks. However, sometimes user/client behavior can increase the risk of attack or infection. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect the client, or a discussion with the user about this issue may be worthwhile. Before you can decide on a course of action, you need to know the problem is occurring. Client reputation can provide this information by tracking client behavior and reporting on activities that you determine are risky or otherwise noteworthy.

Top Users By Reputation Scores

#	User (or IP)	Scores
1	tramos	390,981
2	handerson	390,232
3	dsimpson	389,831
4	ydalton	389,427
5	smetcalf	389,298
6	gmcclung	389,247
7	echavez	389,075
8	rcrawford	389,044
9	jtorres	389,034
10	lrobertson	388,952

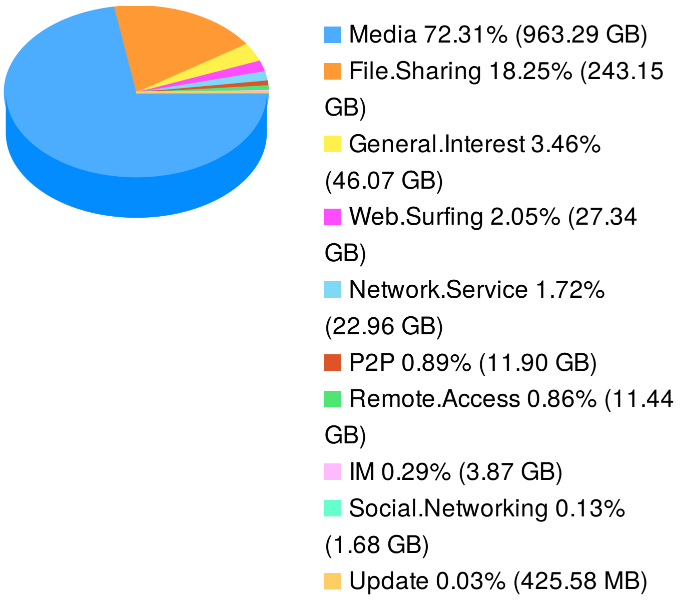
Top Devices By Reputation Scores

#	Device	Scores
1	3a:a8:a6:c9:3c:81	390,981
2	72:a0:2a:b2:8b:2d	390,232
3	72:1c:e6:24:c6:da	389,831
4	ca:1b:23:ed:2c:e5	389,427
5	a2:a9:92:63:3e:b0	389,298
6	Windows Tablet c9:09:c6:69:02:8b	389,247
7	f5:67:da:3f:d4:71	389,075
8	43:01:7a:27:57:16	389,044
9	b5:49:a1:8e:3b:90	389,034
10	18:90:dc:9c:04:46	388,952

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Top 10 Application Categories By Bandwidth Usage



Application Categories By Bandwidth Usage

#	Application Category	Bandwidth
1	Media	963.29 GB
2	File.Sharing	243.15 GB
3	General.Interest	46.07 GB
4	Web.Surfing	27.34 GB
5	Network.Service	22.96 GB
6	P2P	11.90 GB
7	Remote.Access	11.44 GB
8	IM	3.87 GB
9	Social.Networking	1.68 GB
10	Update	425.58 MB
11	eMail	354.66 MB
12	Web.Others	169.11 MB
13	Storage.Backup	53.08 MB
14	VoIP	11.70 MB
15	Collaboration	8.74 MB
16	Proxy	5.61 MB
17	Botnet	596.59 KB

Applications Detected by Risk Behavior

Modern security organizations need increasingly complex security processes in place to handle the myriad applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.

Number of Applications by Risk Behavior

#	Risk	Number of Applications	Percentage
1	Botnet	1,812	0.01%
2	Evasive	1,370,300	10.05%
3	Excessive-Bandwidth	5,437,122	39.88%
4	Other Applications	6,825,002	50.06%

High Risk Applications

#	Risk	Application Name	Category	Technology	Bandwidth	Sessions
1	Botnet	Zeroaccess.Botnet	Botnet	Client-Server	596.59 KB	1,812
2	Evasive	Skype	P2P	Peer-to-Peer	169.68 MB	531,489
3	Evasive	WebEx	Collaboration	Browser-Based|Client-Server	1.18 GB	531,137
4	Evasive	Skype_Communication	P2P	Peer-to-Peer	17.10 MB	53,579
5	Evasive	Google.Desktop	General.Interest	Client-Server	38.87 GB	53,089
6	Evasive	EBay.Toolbar	General.Interest	Browser-Based	8.41 MB	26,273
7	Evasive	Evernote	General.Interest	Browser-Based	5.04 MB	15,773
8	Evasive	SOCKS5	Proxy	Network-Protocol	5.03 MB	15,684
9	Evasive	RDP	Remote.Access	Client-Server	11.43 GB	15,549
10	Evasive	Stumbleupon.Toolbar	General.Interest	Browser-Based	3.43 MB	10,719
11	Evasive	Paypal	Business	Browser-Based	3.34 MB	10,414
12	Evasive	Yahoo.Toolbar	General.Interest	Browser-Based	3.28 MB	10,267
13	Evasive	Rss	Network.Service	Browser-Based	2.96 MB	9,238
14	Evasive	SOAP	Network.Service	Network-Protocol	2.89 MB	9,018
15	Evasive	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	2.33 MB	7,291
16	Evasive	Google.Earth	General.Interest	Client-Server	3.94 GB	5,390
17	Evasive	Facebook_Like.Button	Social.Media	Browser-Based	1.73 MB	5,385
18	Evasive	Facebook_Plugins	Social.Media	Browser-Based	1.72 MB	5,382
19	Evasive	Yahoo.Mail_Messenger	Collaboration	Browser-Based	1.70 MB	5,339
20	Evasive	QQLive	P2P	Peer-to-Peer	3.87 GB	5,314

Key Applications Crossing The Network

This part of the PoC Security Report offers a summary of the key applications crossing the network based on the amount of bandwidth they are using and then sorted into different application types. It provides a high level view of the types of application that are used most commonly across the network.

Key Applications Crossing The Network

#	Application	Category	Sessions	Bandwidth
1	Youtube	Media	1,124,317	807.97 GB
2	Dropbox	File.Sharing	321,172	231.27 GB
3	Vimeo	Media	184,277	134.95 GB
4	Google.Desktop	General.Interest	53,089	38.87 GB
5	HTTP.Video	Web.Surfing	108,055	26.45 GB
6	FTP	Network.Service	67,993	19.21 GB
7	Hulu	Media	26,121	15.31 GB
8	RDP	Remote.Access	15,549	11.43 GB
9	Akamai	File.Sharing	381,906	7.84 GB
10	Skydrive	File.Sharing	5,456	4.03 GB
11	QVoD	P2P	5,491	4.00 GB
12	Google.Earth	General.Interest	5,390	3.94 GB
13	QQLive	P2P	5,314	3.87 GB
14	Naver.Line	IM	5,273	3.87 GB
15	QQ.Download	P2P	5,220	3.83 GB
16	SSL	Network.Service	62,315	3.46 GB
17	YouTube.Video.Embedded	Media	945,464	2.10 GB
18	Silverlight	Media	9,081	1.34 GB
19	Sharepoint	General.Interest	1,768	1.30 GB
20	Pandora	Media	531,607	1.18 GB
21	WebEx	General.Interest	531,137	1.18 GB
22	Facebook	Social.Networking	479,409	1.07 GB
23	HTTP.BROWSER	Web.Surfing	1,088,350	347.73 MB
24	Wikipedia	General.Interest	1,050,660	335.66 MB
25	HTTP.Flash	Web.Surfing	145,094	329.94 MB
26	Craigslist	Social.Networking	793,957	253.64 MB
27	Last.FM	Media	107,006	243.18 MB
28	McAfee.Update	Update	106,646	242.75 MB
29	Gmail	eMail	531,878	169.95 MB
30	Skype	P2P	531,489	169.68 MB

Applications Running Over HTTP

This section provides an overview of applications crossing the network that use HTTP. Software updates, error reporting or help guides are used by different business applications as a means of improving the overall user experience. Social networks, streaming video or audio, file sharing are among the most common non-business applications that use HTTP. Assessing the number and type of applications that use HTTP provides a critical part of developing an efficient network security strategy.

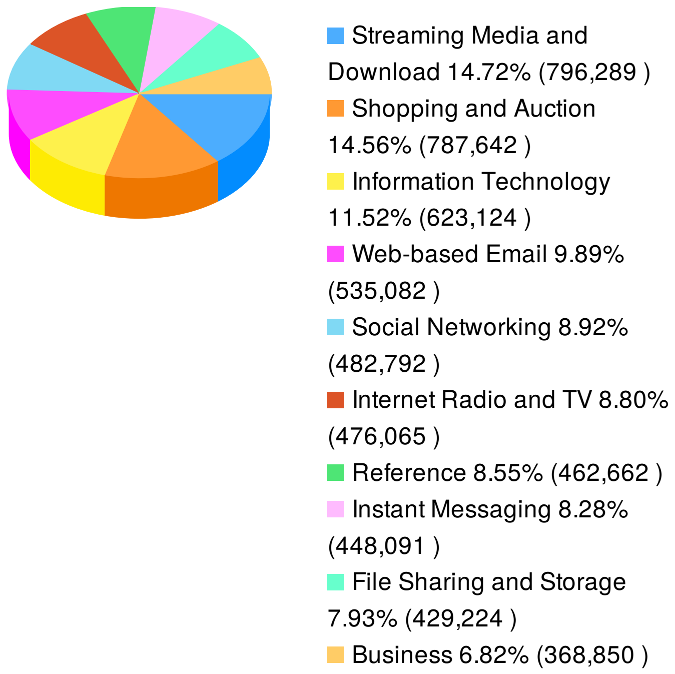
Top Applications Running Over HTTP

#	Application	Sessions	Bandwidth
1	Youtube	1,124,317	807.97 GB
2	Dropbox	315,872	231.27 GB
3	Vimeo	104,861	76.79 GB

Top Web Categories Visited By Network Users

User 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. This chart details web categories by the number of times URLs within those categories were requested and by the number of bandwidth used.

Top Web Categories By Sessions



Top Web Categories By Sessions/Bandwidth

#	Category Description	Sessions	Bandwidth
1	Streaming Media and Download	796,289	282.30 GB
2	Shopping and Auction	787,642	251.55 MB
3	Information Technology	623,124	1.18 GB
4	Web-based Email	535,082	170.91 MB
5	Social Networking	482,792	853.27 MB
6	Internet Radio and TV	476,065	1.05 GB
7	Reference	462,662	3.04 GB
8	Instant Messaging	448,091	5.80 GB
9	File Sharing and Storage	429,224	85.12 GB
10	Business	368,850	117.87 MB
11	Search Engines and Portals	241,557	5.77 GB
12	Finance and Banking	172,713	55.13 MB
13	Personal Websites and Blogs	103,898	33.18 MB
14	Entertainment	102,339	69.38 GB
15	Freeware and Software Downloads	42,936	28.65 GB
16	News and Media	40,125	20.47 MB
17	Web-based Applications	36,190	11.57 MB
18	Newsgroups and Message Boards	36,004	11.51 MB
19	Education	7,573	2.41 MB
20	Arts and Culture	7,548	2.41 MB

Top Web Sites Visited By Network Users

Identifying and managing the top URLs visited by network users provides greater visibility and control, and subsequently, better network security. By leveraging Fortinet threat prevention, application control and URL filter technologies, the volume of web sites by category can be reviewed and strategies put in place to prevent users accessing sites considered to be a risk to overall network security.

Top Web Domains By Visits

#	Domain	Category	Visits
1	youtube.com	Streaming Media and Download	633,772
2	craigslist.org	Shopping and Auction	413,171
3	mail.google.com	Web-based Email	394,188
4	stream.pandora.com	Internet Radio and TV	392,997
5	en.wikipedia.org	Reference	359,999
6	skype.com	Instant Messaging	351,590
7	webex.com	Information Technology	350,938
8	facebook.com	Social Networking	320,224
9	linkedin.com	Business	316,534
10	akamai.com	File Sharing and Storage	248,851
11	amazon.com	Shopping and Auction	248,849
12	accounts.google.com	Search Engines and Portals	200,940
13	finance.google.com	Finance and Banking	117,927
14	dropbox.com	File Sharing and Storage	100,453
15	vimeo.com	Entertainment	84,911
16	hotmail.com	Web-based Email	73,605
17	maps.google.com	Reference	72,498
18	last.fm	Internet Radio and TV	70,914
19	ud.mcafee.com	Information Technology	70,557
20	m.facebook.com	Social Networking	70,410

Top Destination Countries By Browsing Time

The following chart shows the distribution of web traffic according to the destination country. This chart offers the possibility to the network administrator to analyze which countries web sites are visited for longer time. The administrator can then decide to create security policy based on Geo-location.

Top Destination Countries By Browsing Time

#	Destination Country	Browsing Time(hh:mm:ss)	Bandwidth 🟦Traffic Sent 🟨Traffic Received
1		45388:05:09	1.30 TB
2	United States	28:44:48	1.82 GB
3	Canada	08:27:30	120.28 MB
4	Taiwan	00:48:52	308.42 KB
5	Netherlands	00:00:01	18.02 KB

Top Web Sites By Browsing Time

The following chart shows the web sites that users visit for longer time. The administrator can then decide to create security policy to mitigate or block web sites access, accordingly to internal corporate policy.

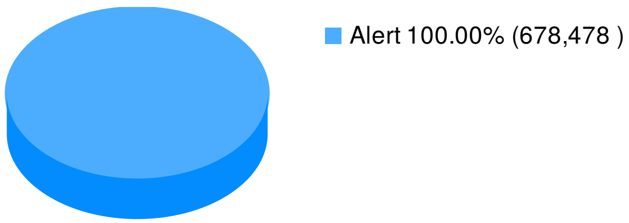
Top Web Sites By Browsing Time

#	Website	Browsing Time(hh:mm:ss)	Bandwidth ■Traffic Sent ■Traffic Received
1	youtube.com	6042:41:15	810.07 GB
2	craigslist.org	3332:27:55	253.64 MB
3	en.wikipedia.org	3060:33:58	335.66 MB
4	skype.com	2682:10:48	169.68 MB
5	stream.pandora.com	2678:54:21	1.18 GB
6	mail.google.com	2676:38:36	169.95 MB
7	webex.com	2676:35:11	1.18 GB
8	facebook.com	2440:45:32	1.07 GB
9	linkedin.com	2411:57:11	152.57 MB
10	amazon.com	1903:58:31	121.78 MB
11	akamai.com	1903:02:19	7.84 GB
12	accounts.google.com	1372:37:52	87.35 MB
13	dropbox.com	947:43:52	231.27 GB
14	finance.google.com	805:01:36	50.98 MB
15	vimeo.com	708:56:39	134.95 GB

Top Threats Crossing The Network

By individually reviewing both the applications and traffic flows crossing the network, threat vector identification and prevention becomes easier. Threat prevention technologies filter the total number of applications and traffic crossing the network down to those applications or packets that pose a potential risk, picking up threat vectors such as spyware, application vulnerabilities or viruses. The result is improved overall network performance and lower network latency.

Top Threats Crossing The Network



Top Critical Threats Crossing The Network

No matching log data for this report

Top High Threats Crossing The Network

No matching log data for this report

Top Medium Threats Crossing The Network

No matching log data for this report

Top Low Threats Crossing The Network

No matching log data for this report

Top Info Threats Crossing The Network

No matching log data for this report

Top 20 Viruses Crossing The Network

As the FortiGate scans the network, it provides information about the viruses that are crossing the network. The Fortigate is able to apply different strategies in order to detect malware: - Signatures: Fortinet's Compact Pattern Recognition Language (CPRL) - Heuristics: These are applied to: * file structure; * API call. The FortiGate's antivirus engine provides two main capabilities: Decompression allows embedded files to be extracted; Emulation allows the hidden layers of malicious file of be extracted.

Top Viruses By Name

#	Virus Name	Occurrences
1	W32/Simda.B!tr	373,989
2	W32/Agent.RNI!tr	373,475
3	W32/Jorik.EF78!tr	372,944
4	JS/Redirector.M!exploit	372,877
5	W32/Zbot.DHN!tr	372,747
6	W32/Zbot.ANM!tr	372,369
7	W32/FakeAV.OY!tr	372,366

Top Virus Victims

This counter provides information about which network users are more prone to infection from viruses. This enables direct identification of the host(s) that are creating sources of malicious traffic on the network. The following chart displays the counter of the number of viruses per end user.

Top Virus Victims

#	Virus Victims	Occurrences
1	dsimpson	20,340
2	lrobertson	20,299
3	rcapobianco	20,255
4	rcrawford	20,206
5	paltidore	20,198
6	tzhang	20,173
7	bchao	20,162
8	tramos	20,159
9	zgeary	20,143
10	ajohnson	20,118
11	jkirovski	20,114
12	tchang	20,108
13	lcorrales	20,106
14	xgibbs	20,085
15	qbalboa	20,083
16	ydalton	20,081
17	bolsen	20,072
18	pmadison	20,056
19	tlee	20,056
20	jgroom	20,049

Malwares Discovered

#	Day	Malware
1	2014-11-02	386,187
2	2014-11-01	370,953
3	2014-10-29	370,917
4	2014-10-28	370,811
5	2014-10-27	370,728
6	2014-10-30	370,705
7	2014-10-31	370,466

Application Vulnerabilities Discovered

No matching log data for this report

Data Loss Prevention Events

Fortinet Data Loss Prevention solution uses sophisticated pattern matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. Fortinet DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching and data archiving. Let's remember that data loss events continue to increase every year, resulting in fines, penalties and loss of revenue for companies worldwide. Many data loss events are caused by trusted employees who frequently send sensitive data into untrusted zones, either intentionally or by accident.

Top Data Loss Prevention Events

#	DLP Type	Number
1	dlp	1,969

Notes

Traffic sessions that are not scanned by the Application Control engine are excluded from application category related charts in this report. Please enable Application Control to allow application traffic to be properly identified/secured on your network.

Appendix A

Devices

FGT60C3G12031337
FGT60C3G12031338
FGT60C3G12031339
FGT60C3G12031340
FGT60C3G12031341
FGT60C3G12031342
FGT60C3G12031343
FGT60C3G12031344
FGT60C3G12031345
FGT60C3G12031346
FGT60C3G12031347
FGT60C3G12031348
FGT60C3G12031349
FGT60C3G12031350
FGT60C3G12031351
FGT60C3G12031352
FGT60C3G12031353
FGT60C3G12031354
FGT60C3G12031355
FGT60C3G12031356
FGT60C3G12031357
FGT60C3G12031358
FGT60C3G12031359
FGT60C3G12031360
FGT60C3G12031361
FGT60C3G12031362
FGT60C3G12031363
FGT60C3G12031364
FGT60C3G12031365
FGT60C3G12031366
FGT60C3G12031367
FGT60C3G12031368
FGT60C3G12031369

FGT60C3G12031370
FGT60C3G12031371
FGT60C3G12031372
FGT60C3G12031373
FGT60C3G12031374
FGT60C3G12031375
FGT60C3G12031376
FGT60C3G12031377
FGT60C3G12031378
FGT60C3G12031379
FGT60C3G12031380
FGT60C3G12031381
FGT60C3G12031382
FGT60C3G12031383
FGT60C3G12031384
FGT60C3G12031385
FGT60C3G12031386
FGVM080000022885[L2_VDOM1]
FGVM080000022885[L2_VDOM2]
FGVM080000022885[L3_VDOM]
FGVM080000022885[root]
FortiGate-Demo-140D