sysnet TELEMATICA

NEL FUTURO DELLE TELECOMUNICAZIONI

Application Usage

and

Risk Report

Top Geo Locations

Knowing where network traffic is originating from or going to, is vital information for increasing overall network security. For example, you may want to exclude any traffic that originates from Country X, if you are not doing business there (unless there is valid VPN traffic from a remote worker). The Barracuda NextGen Firewall F-Series helps administrators to monitor and enforce such policies, based on the geographical locations.

The following chart provides a list of the top 10 Geo Destinations for traffic:

#	GEO DESTINATIONS	TRAFFIC	SESSIONS
2	Non-routable or Private IP	0 B	35

The following chart provides a list of the top 10 Geo Sources from where a session was established into your network:

#	GEO SOURCES	TRAFFIC	SESSIONS
2	Non-routable or Private IP	106 MB	240
3	China	24 MB	26
4	Netherlands	2 MB	12
5	Russian Federation	11 MB	2
6	United States	306 KB	1

Key Findings and Observations:

The countries from where the most sessions are initiated are China (6 sessions), Netherlands (2 sessions), and Russian Federation (2 sessions). Internal Traffic (from Non-routable or Private IP Addresses) was 68.6% of the sessions. These findings should be considered by when refining the firewall policies.

Top High-Risk Traffic traversing the Network

The following chart provides a breakdown of the top risk applications identified on the network. These applications may represent vectors for delivering malware to the network, reduce performance or significantly decrease employee productivity. They should be addressed in the corporate application usage policy.

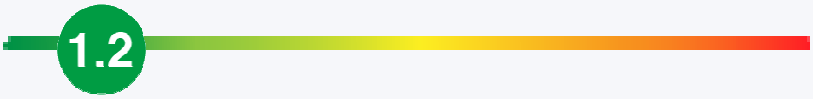
#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	TeamViewer file transfer	3	61.2 MB	13
2	Yahoo Messenger General		900.2 KB	30
3	Zoom	3	80.4 KB	7
4	Skype Chat		3.0 KB	10
5	Skype General	3	1.7 KB	8

Top Application Traffic traversing the Network

The Barracuda NextGen Firewall F-Series provides powerful and extremely reliable detection and classification of applications and sub-applications by combining Deep Packet Inspection (DPI) and behavioral traffic analysis - no matter if the protocols are using advanced obfuscation, port hopping techniques or encryption. The Barracuda NextGen Firewall F-Series comes with real-time and historical application visibility that shows application traffic on the corporate network. This provides a basis for deciding which connections should be given bandwidth prioritization, which is crucial for QoS optimization of business-critical applications. Furthermore, it allows for adjusting and refining the corporate application use policy.

Barracuda Networks provides a risk rating for any identified application and protocol crossing the network. Based in the conducted traffic analysis the overall risk rating is as follows:

Risk Rating



The following chart provides an overview of the top applications based on bandwidth consumption that are traversing the network:

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	Microsoft Update and Microsoft Activation	1	1.3 GB	2168
2	Web browsing		308.5 MB	1515
3	OneDrive	2	108.5 MB	25
4	TeamViewer General		90.2 MB	31437
5	TeamViewer file transfer	3	61.2 MB	13
6	Akamai CDN		30.7 MB	83
7	Microsoft Services Base	1	29.2 MB	2665
8	Windows 10 Privacy Data Collection		13.0 MB	2184
9	Bing Search	1	11.5 MB	256
10	Microsoft Push Notification Service		10.7 MB	35
11	Microsoft Account	1	4.7 MB	187
12	Microsoft Windows Store		4.4 MB	356
13	Xbox Live	2	1.0 MB	8
14	Yahoo Messenger General		900.2 KB	30
15	Oracle Java Update	1	188.4 KB	8
16	Microsoft Teams		172.4 KB	47
17	Microsoft Office 365 Base	2	158.9 KB	3
18	Google Services Base		145.4 KB	32
19	Microsoft Office 365 OneNote	2	124.5 KB	12
20	Zoom		80.4 KB	7

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
21	Yahoo! Services Base	2	72.0 KB	15
22	Microsoft Azure Storage		67.3 KB	5
23	Google Analytics	2	24.3 KB	1
24	Microsoft Azure Base		22.8 KB	2
25	Skype Chat	3	3.0 KB	10
26	Skype General		1.7 KB	8

Key Findings and Observations:

The Top 3 applications (based on consumed bandwidth) are Microsoft Update and Microsoft Activation, Web browsing and OneDrive. The findings of the traffic analysis can help to define or refine firewall policies in order to minimize threat vectors by blocking unwanted traffic.

Top Business-related Application Traffic

The Barracuda NextGen Firewall F-Series can provide deeper insights regarding what benefit an application can provide to the business. The following chart provides a breakdown of the top applications that can help drive business, time to market and productivity. These applications should be prioritized, by means of Quality of Service and Dynamic Path selection, above all other applications in use on the corporate network.

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	Microsoft Teams	1	172.4 KB	47
2	Microsoft Office 365 Base		158.9 KB	3
3	Microsoft Office 365 OneNote	2	124.5 KB	12
4	Microsoft Azure Storage		67.3 KB	5
5	Google Analytics	2	24.3 KB	1
6	Microsoft Azure Base		22.8 KB	2

Key Findings and Observations:

Business applications such as Microsoft Teams (172.4 KB) and Microsoft Office 365 Base (158.9 KB) were identified on the network. The Barracuda NextGen Firewall F-Series can help to ensure that these applications are prioritized and will receive the bandwidth they deserve, in order to not harm the business continuity.

Top Application Traffic related to Software Updates

Software updates improve usability and performance of an application while providing security enhancements. However, software updates can reduce corporate bandwidth and slow down business applications, especially when many clients are updating during peak business hours (e.g. their iOS devices). By providing the possibility to assign QoS policies to single Applications, Application Groups and Application Categories, the Barracuda NextGen Firewall F-Series can help to mitigate these issues.

The following chart provides an overview of identified software update traffic on the network of:

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	Microsoft Update and Microsoft Activation	1	1.3 GB	2168
2	Oracle Java Update		188.4 KB	8

Key Findings and Observations:

Applications such as Microsoft Update and Microsoft Activation and Oracle Java Update perform software updates. In total 1.349 GB of traffic was related to Software Updates.

Application Usage by Category

As part of application identification, the Barracuda NextGen Firewall F-Series categorizes application traffic traversing the corporate network into various categories. The following chart provides an overview of the top application categories, based on consumed bandwidth and number of sessions:

#	CATEGORIES	TRAFFIC	SESSIONS
1	Software Update	1.3 GB	2176
2	Web Browsing	355.6 MB	2073
3	Remote Access	151.4 MB	31450
4	File Storage and Backup	108.5 MB	25
5	Standard Network	46.7 MB	5463
6	Mobile	10.7 MB	35
7	Games	1.0 MB	8
8	Instant Messaging	903.2 KB	40
9	Business	570.2 KB	70
10	Conferencing	80.4 KB	7
11	Social Networking	72.0 KB	15
12	VOIP	1.7 KB	8

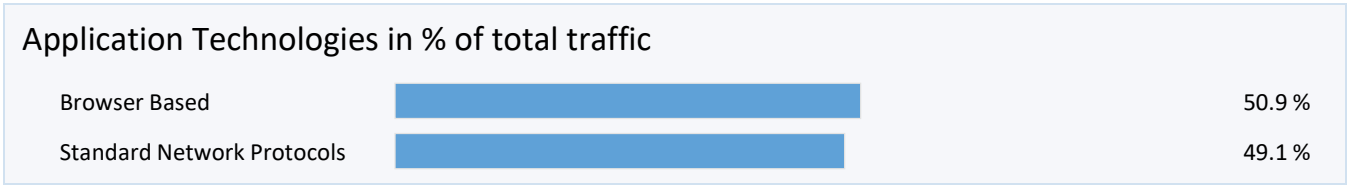
Key Findings and Observations:

The application categories consuming the highest amount of bandwidth are Software Update, Web Browsing, and Remote Access. This information should be considered by when defining or refining the corporate application usage policy.

Application Usage by Technology

The Barracuda NextGen Firewall F-Series can provide deep visibility into what is traversing the network of by categorizing the network traffic into various underlying technologies.

The following chart provides a complete summary of the findings:



Key Findings and Observations:

The traffic analysis shows that 50.9% of the traffic is consumed by Browser Based Applications such as Microsoft Update and Microsoft Activation, Web browsing, and OneDrive

Standard Network Protocols

Besides application traffic, many standard network protocols are in use on the network.

#	PROTOCOLS	RISK	TRAFFIC	SESSIONS
1	HTTP direct	1	1.6 GB	33139
2	SSL	1	379.6 MB	7208
3	SOAP	2	1.5 MB	514
4	OCSP	1	223.0 KB	165

Key Findings and Observations:

The protocols consuming the highest amount of bandwidth are HTTP direct (1.566 GB), SSL (379.6 MB), and SOAP (1.493 MB). This information should be considered by when defining or refining Firewall Rules and Quality of Service policies.

SSL encrypted Applications

Many applications are using SSL encryption in order to enable safe data transfer and data protection. At the same time, these applications can expose to business and security risks, as malicious content may be hidden in the encrypted traffic stream or conceal user activity. The Barracuda NextGen Firewall F-Series can provide full visibility into SSL encrypted data streams thus removing network blind spots.

The following table, based on consumed bandwidth, lists all applications traversing the network that use SSL encryption*:

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	OneDrive	2	108.5 MB	25
2	Web browsing		80.7 MB	1138
3	TeamViewer General	2	54.6 MB	14
4	Akamai CDN		30.7 MB	83
5	Microsoft Update and Microsoft Activation	1	30.2 MB	435
6	Microsoft Services Base		28.1 MB	2616
7	Windows 10 Privacy Data Collection	1	13.0 MB	2184
8	Bing Search		11.5 MB	256
9	Microsoft Push Notification Service	2	10.7 MB	35
10	Microsoft Account		4.7 MB	187
11	Microsoft Windows Store	2	3.9 MB	111
12	Xbox Live		1.0 MB	4
13	Yahoo Messenger General	3	896.3 KB	15
14	Oracle Java Update		188.4 KB	8
15	Microsoft Teams	1	163.8 KB	20
16	Microsoft Office 365 Base		158.9 KB	3
17	Google Services Base	2	145.4 KB	32
18	Microsoft Office 365 OneNote		124.5 KB	12
19	Zoom	3	80.4 KB	7
20	Yahoo! Services Base		72.0 KB	15
21	Microsoft Azure Storage	1	67.3 KB	5
22	Google Analytics		24.3 KB	1
23	Microsoft Azure Base	1	22.8 KB	2

Key Findings and Observations:

The analysis shows that 9.39% of 's traffic is SSL encrypted. SSL-encrypted applications which are consuming the highest amount of bandwidth are OneDrive (108.5 MB), Web browsing (80.72 MB), and TeamViewer General (54.6 MB).

SaaS / IaaS related Applications

The modern network includes a combination of local and cloud-hosted applications such as Office 365, Salesforce, and public cloud platforms like Amazon Web Services (AWS) and Microsoft Azure. With the increasing adoption of Software-as-a-Service (SaaS), virtualization, and public cloud applications, the role of the firewall has evolved from a security device to a solution that also improves network performance and availability. Besides safely enabling SaaS applications, Barracuda's NextGen Firewalls ensure a high Quality-of-Service for cloud applications such as Office 365, Salesforce, and other productivity SaaS applications. By link-balancing traffic, administrators can ensure that business-critical data has priority over non-essential data. Granular visibility into user activity helps administrators create traffic-shaping policies that are appropriate for their organization.

The following table, based on consumed bandwidth, lists all applications traversing the network*:

#	APPLICATIONS	RISK	TRAFFIC	SESSIONS
1	OneDrive	2	108.5 MB	25
2	TeamViewer General		55.4 MB	31437
3	TeamViewer File transfer	3	15.4 MB	13
4	Microsoft Teams		172.4 KB	47
5	Microsoft Office 365 Base	2	158.9 KB	3
6	Microsoft Office 365 OneNote		124.5 KB	12
7	Zoom	3	80.4 KB	7
8	Microsoft Azure Storage		67.3 KB	5
9	Google Analytics	2	24.3 KB	1
10	Microsoft Azure Base		12.5 KB	2
11	Skype Chat	3	3.0 KB	10
12	Skype General		1.7 KB	8

Key Findings and Observations:

The analysis shows that 4.45% of 's traffic is SaaS-related. SaaS applications which are consuming the highest amount of bandwidth are OneDrive (108.5 MB), TeamViewer General (55.43 MB), and TeamViewer file transfer (15.43 MB).