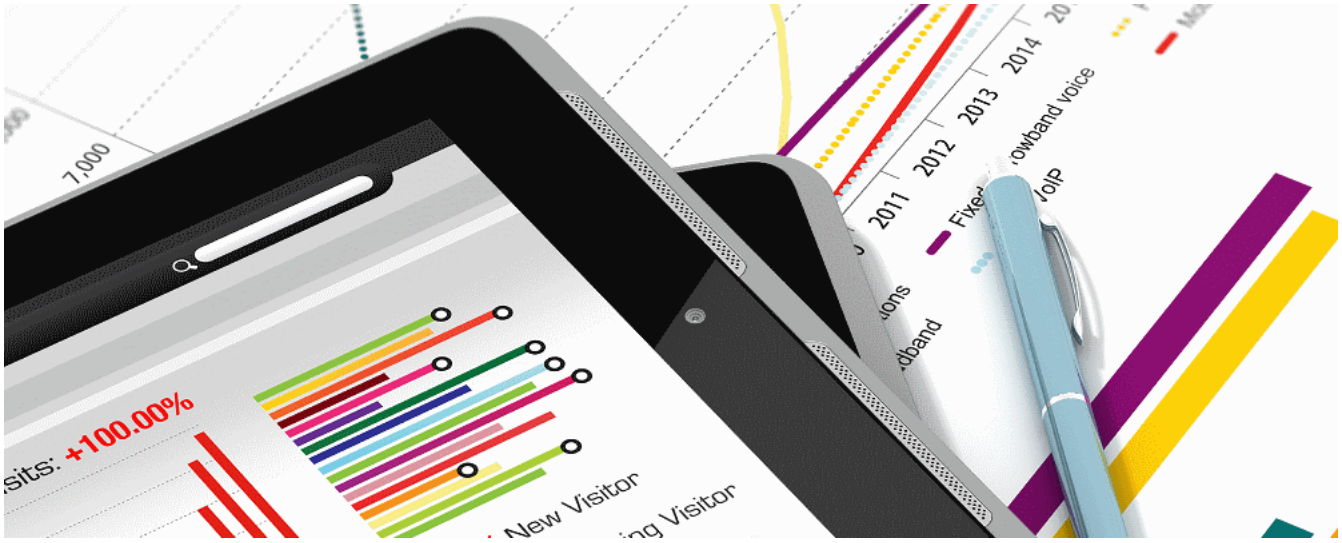
Executive Summary Report

Report generated 2017-11-13 08:22:43 (Europe/Berlin)

Complete Visibility into network traffic and security events boosts efficiency, productivity, and profitability. The summary report provides the business intelligence that you need to support key goals:

- *Ensure productive use of corporate assets and time throughout the organization.*
- *Audit compliance against acceptable usage policies for Internet usage.*
- *Monitor protection against spyware, malware, and viruses.*



Device(s):	WatchGuard-XTM (10.30.1.1) FVE402717F124
From:	2017-10-21 00:00:00 (Europe/Berlin)
To:	2017-11-13 00:00:00 (Europe/Berlin)

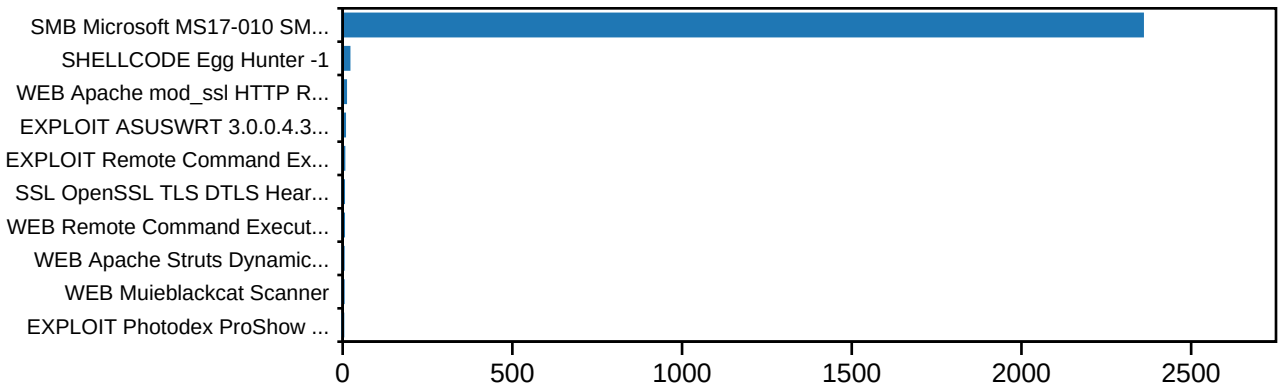
Available Reports

Top Blocked Attacks

The Intrusion Prevention Service (IPS) provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows. Skillful hackers can exploit these vulnerabilities to gain control of computer systems in the network. For example with buffer overflows, the hacker can send input that overflows the allocated memory, enabling them to gain access to the portion of memory where code is executed. Once code is installed, it can be used for theft of company financial data, or botnets could be used to extract company confidential information.

This report details the top intrusion attacks that were blocked at the firewall over the reporting period. More details about each intrusion attack are available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/ThreatDB.aspx)

Hits



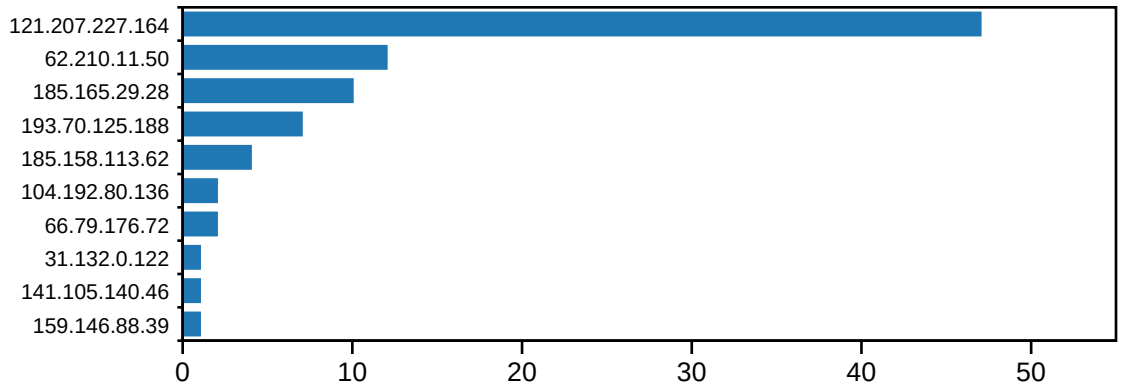
Name	Hits
SMB Microsoft MS17-010 SMB Remote Code Execution -3	2357
SHELLCODE Egg Hunter -1	19
WEB Apache mod_ssl HTTP Request DoS (CVE-2004-0113)	9
EXPLOIT ASUSWRT 3.0.0.4.376_1071 LAN Backdoor Command Execution	6
EXPLOIT Remote Command Execution via Shell Script -2	4
SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -5 (CVE-2	3
WEB Remote Command Execution via Shell Script -1.a	3
WEB Apache Struts Dynamic Method Invocation Remote Code Executi	2
WEB Muieblackcat Scanner	2

Name	Hits
EXPLOIT Photodex ProShow Producer 5.0.3256 load File Handling B	1
Total: 10	2406

Top Blocked Botnet Sites

Detection of Botnet activity is another layer of defense provided by the firewall. Endpoints that become infected with malware via drive by downloads or phishing attacks may contact command-and-control servers to receive instructions, or they may send stolen data to bot servers. The firewall examines traffic for internet IP addresses that belong to known botnets command servers. This report indicates there are nodes on your network that have attempted to contact or were targeted by botnet sites listed here.

Hits

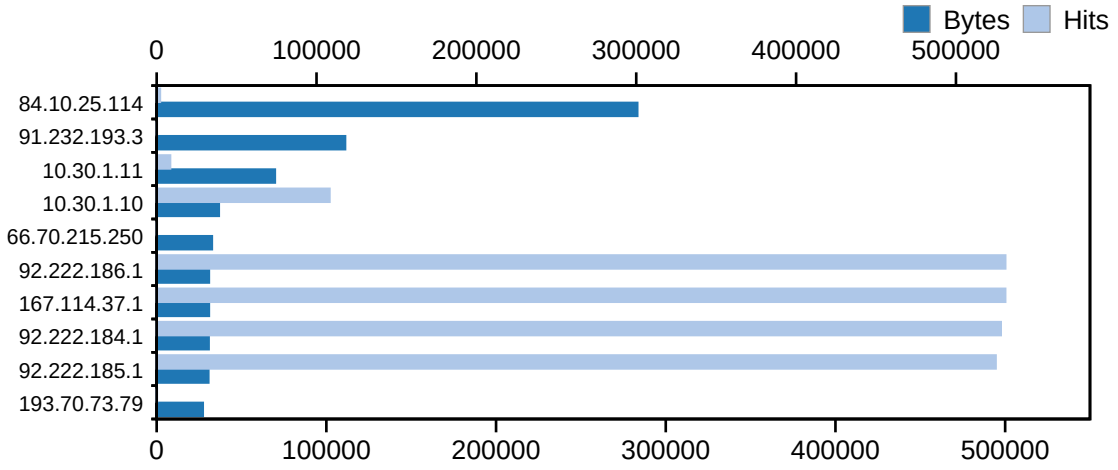


Name	Hits
121.207.227.164	47
62.210.11.50	12
185.165.29.28	10
193.70.125.188	7
185.158.113.62	4
104.192.80.136	2
66.79.176.72	2
31.132.0.122	1
141.105.140.46	1
159.146.88.39	1
Total: 10	87

Top Clients

This report shows the most active endpoints on the network, i.e. the ones that generated the most traffic. When Single Sign-on is implemented at the firewall, the report shows the name of the user associated with the IP address.

Bytes Transferred, Hits

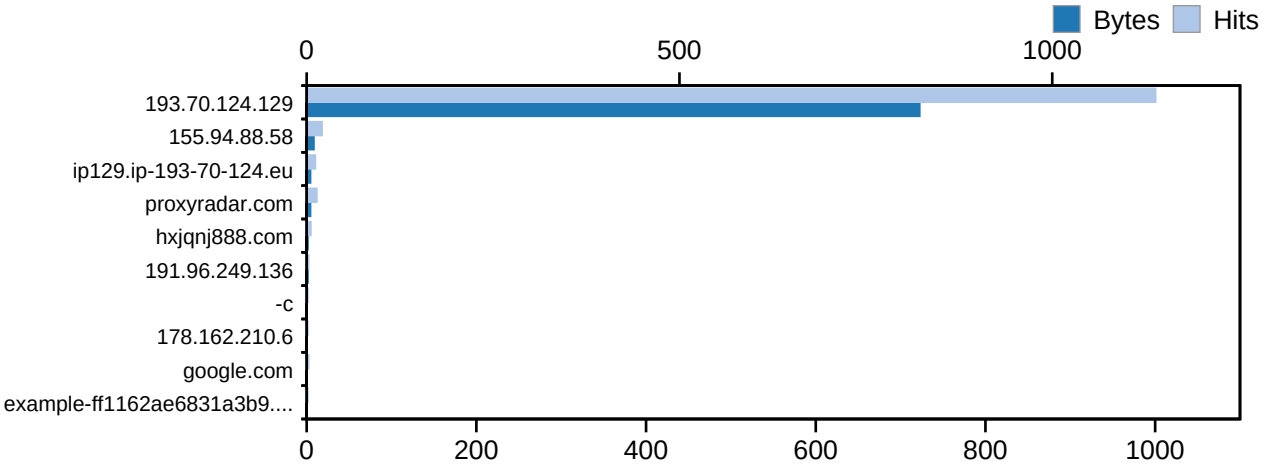


Name	Bytes	Hits
84.10.25.114	277 MB	1989
91.232.193.3	108 MB	75
10.30.1.11	68 MB	8349
10.30.1.10	36 MB	108043
66.70.215.250	32 MB	62
92.222.186.1	30 MB	530772
167.114.37.1	30 MB	530754
92.222.184.1	30 MB	527961
92.222.185.1	30 MB	524748
193.70.73.79	26 MB	108
Total: 10	666 MB	2232861

Top Domains

Internet access is an essential requirement for most employees to perform their job functions, but unlimited Internet access can sap productivity and also open the door to inappropriate adult content and sexually explicit images that could put your organization at risk. This report shows the top web domains that were visited over the reporting period.

Bytes Transferred, Hits



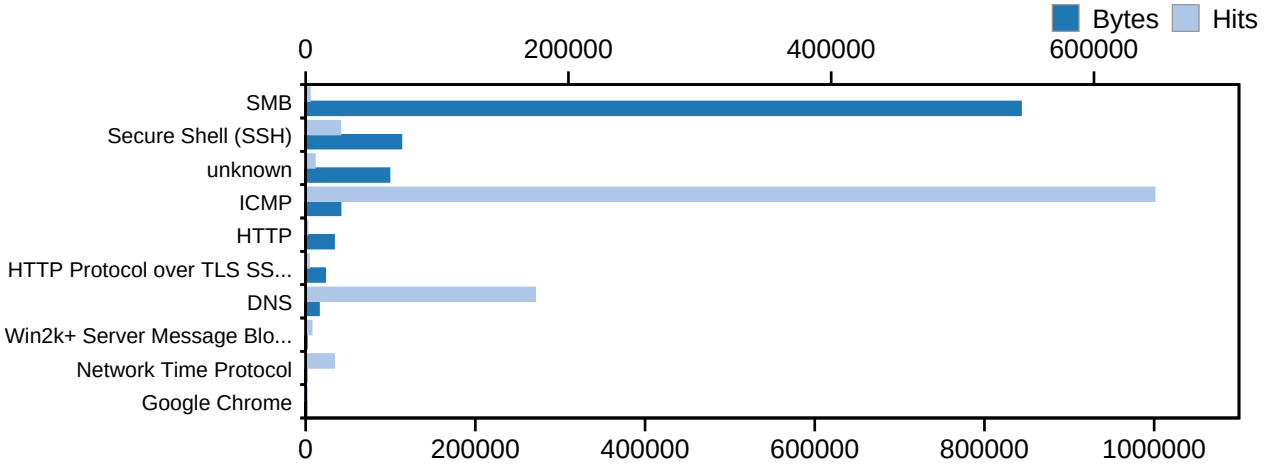
Name	Bytes	Hits
193.70.124.129	722 KB	1138
155.94.88.58	8 KB	20
ip129.ip-193-70-124.eu	5 KB	11
proxyradar.com	5 KB	13
hxjqnj888.com	2 KB	5
191.96.249.136	1 KB	2
-c	946	1
178.162.210.6	782	1
google.com	725	2
example-ff1162ae6831a3b9.com	430	1
Total: 10	745 KB	1194

Top Applications

The firewall inspects all traffic and it identifies the applications in use. Applications can range from business-centric cloud applications like Salesforce.com, to social networking sites like Facebook.com. This report highlights the top applications that are identified on the network. Note that when web browsing is not detected as any specific application, it is recorded as use by the browser application.

More specific information about each application is available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/AppDB.aspx).

Bytes Transferred, Hits

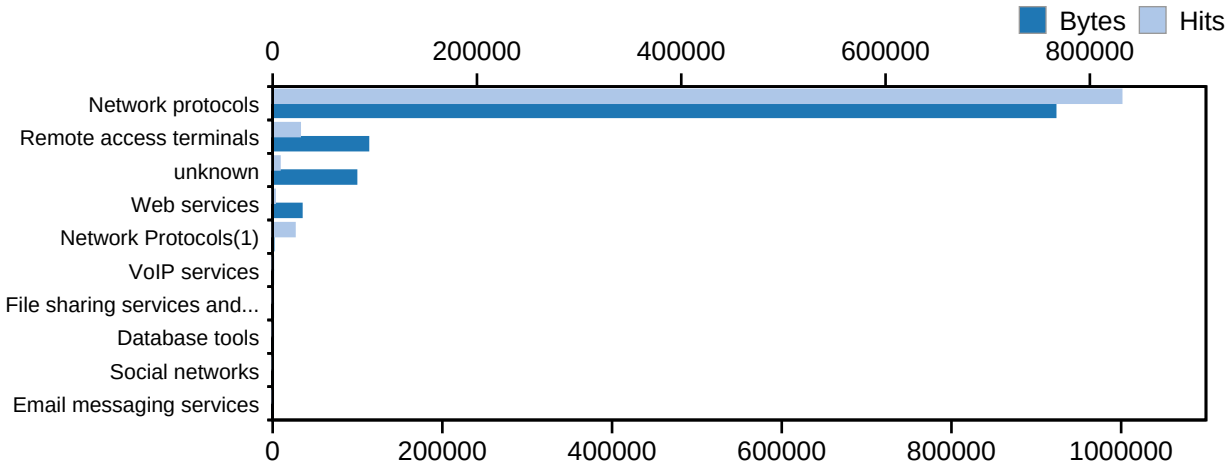


Name	Bytes	Hits
SMB	823 MB	2896
Secure Shell (SSH)	110 MB	26055
unknown	96 MB	6633
ICMP	40 MB	645793
HTTP	32 MB	1118
HTTP Protocol over TLS SSL	22 MB	2169
DNS	15 MB	174344
Win2k+ Server Message Block	938 KB	4224
Network Time Protocol	619 KB	21302
Google Chrome	566 KB	664
Total: 10	1 GB	885198

Top Application Categories

Unlimited use and download of web-based applications can open the company to IT failures, cyber-attack, and IP theft. Best practices mandate the ability to compare between business and personal app usage, and to drill-down to app usage by user. A broad array of applications are routinely delivered via http and https, the standard Internet protocols. Traffic is classified into 16 high level application categories. This report shows the top categories for application traffic. The traffic is sorted by the categories that get the most hits, but it also shows the bandwidth used by each application category.

Bytes Transferred, Hits



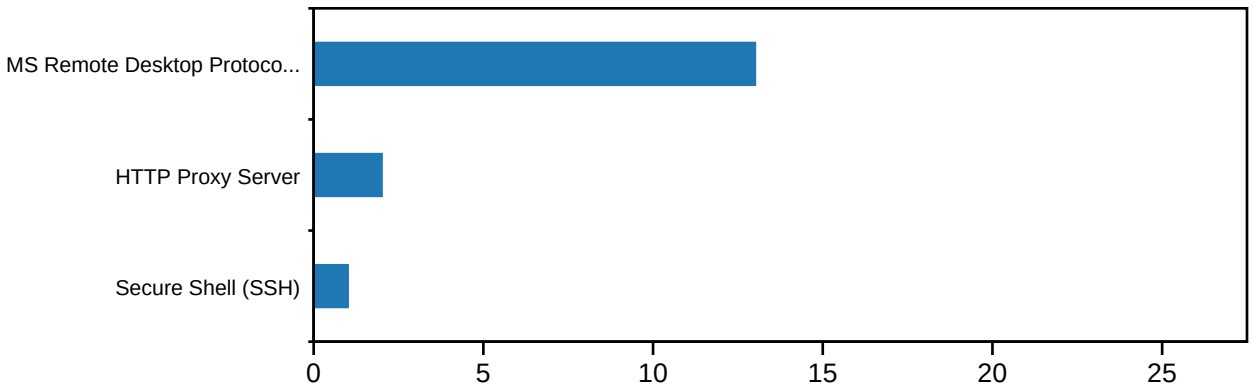
Name	Bytes	Hits
Network protocols	901 MB	830625
Remote access terminals	110 MB	26437
unknown	96 MB	6633
Web services	33 MB	1887
Network Protocols(1)	619 KB	21302
VoIP services	95 KB	225
File sharing services and tools	64 KB	91
Database tools	37 KB	90
Social networks	20 KB	6
Email messaging services	6 KB	68
Total: 10	1 GB	887364

Top Blocked Applications

This report shows more details and highlights the names of the top applications that were blocked.

More specific information about each application is available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/AppDB.aspx)

Hits

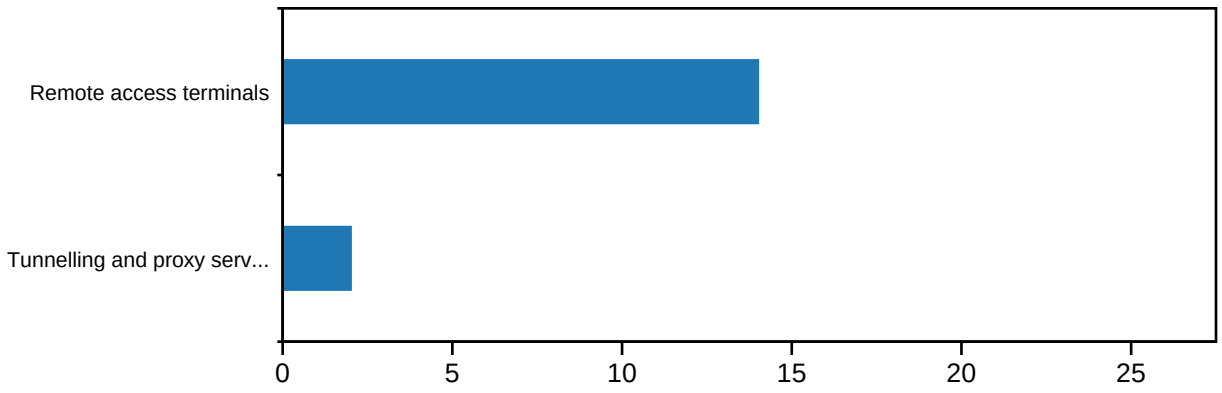


Name	Hits
MS Remote Desktop Protocol (RDP)	13
HTTP Proxy Server	2
Secure Shell (SSH)	1
Total: 3	16

Top Blocked Application Categories

Firewall rules are in place to block application categories that are considered security risks or unproductive use of time. Most businesses choose to block inappropriate application categories like **Games** and **Web Bypass Proxies.** This report shows the top application categories that were blocked over the reporting period.

Hits



Name	Hits
Remote access terminals	14
Tunnelling and proxy services	2
Total: 2	16