DELL Security

# SWARM Report

Dell SonicWALL Application Risk Management Report

**Prepared for:**
sonicwall

**Report on Firewall:**
C0EAE481ED96

**Firewall Type:**
NSA 6600

**SonicOS Version:**
6.2.4.3-31n--demo-5n--

**Report Date:**
Tue, 24 May 2016 09:59:33 PDT

# Table of Contents

# Executive Briefing

Dell SonicWALL network security appliances detect and block sophisticated attacks that legacy stateful inspection firewalls simply cannot. Our next-generation firewalls integrate a patented Reassembly-Free Deep Packet Inspection (RFDPI) firewall engine with a comprehensive array of automated and dynamic security features. These features include advanced anti-evasion intrusion prevention, cloud-updated gateway anti-malware, SSL decryption and inspection (DPI-SSL), application control, content filtering and much more. All of this is delivered on a single high-performance platform that is easy to license, deploy, manage and maintain.

In addition, SonicWALL bundles together a set of powerful security and management tools on a single physical device with an easy-to-understand licensing structure.

For your auditing needs, personal logs are kept by your SonicWALL device. In providing a high-level overview of your network, this report will:

- ✔ Identify vulnerabilities detected and blocked
- ✔ Vulnerability descriptions
- ✔ In-use application description
- ✔ Present traffic distribution statistics by geographic location, URL category, and traffic type
- ✔ Highlight top high-bandwidth applications found
- ✔ Risk definitions
- ✔ Application List
- ✔ List high-risk applications and protocols

# SWARM Summary

The SonicWALL Application Risk Management (SWARM) Report is a snapshot in time of the different threats that have been identified and blocked by your Dell SonicWALL next-generation firewall appliance. This report also provides application and user based data that includes top application traffic, top users, top URL categories and session counts to give insight into the traffic mix on your network.

## Threat Index

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Low | Elevated | High | Severe |

## Threat Protection

| | |
|---|---|
| 0 | Botnet Events |
| 0 | Virus Events |
| 0 | Spyware Events |
| 25208 | IPS Events |

## Endpoint

| | |
|---|---|
| # | Events (based on top X) |

## Highest Traffic by Country

1. United States
2. Germany
3. Russian Federation

| | | |
|---|---|---|
| Company Name<br>sonicwall | SonicWALL Device<br>NSA 6600 | SonicOS Version<br>6.2.4.3-31n--demo-5n-- |
| Subscription Services<br>App Control, GAV, SPY, IPS, CFS, GeoIP, Botnet | Report Date<br>Tue, 24 May 2016 09:59:33 PDT | |

# App Intelligence, Control & Visualization

Dell SonicWALL firewalls put network control back into the hands of your IT administrators. While some applications are business critical and may use more bandwidth, other applications are non-productive and may require policies to block or bandwidth limit usage on your network. Next-Generation Dell SonicWALL firewalls make the job easier with a robust application identification scheme, granular policy control options and detailed visualization tools.

## Application Intelligence

Scanning all network traffic, Dell SonicWALL firewalls identify applications regardless of port and protocol.

- Deep packet inspection of all traffic including SSL-encrypted traffic
- Integrated data leakage prevention
- Applications and URL filtering

## Application Control

Policies that can block or bandwidth manage are placed at the administrator's fingertips. Pre-defined application categories are available along with application and user management.

- Dynamically updated database containing thousands of application signatures
- Dynamically updated cloud database that includes millions of URLs and IP addresses, categorized in 56 different categories
- Predefined actions, including block, bandwidth manage or Bypass DPI

## Application Visualization

Flow Monitor provides visuals for application traffic, ingress and egress bandwidth, web traffic, and general user activity, supplying administrators with the crucial information necessary for maintaining a productive network under rapidly changing conditions.

- Real-time data on everything from potential network threats to URLs visited
- Customizable filter views for repeat access
- Widget creation, such as pie chart view

# Top Applications by Category

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Google Mail (Gmail) | WEBMAIL | 1 Low | 1.93 MB | 5 |
| Yahoo! Mail | WEBMAIL | 1 Low | 196.34 KB | 21 |
| Microsoft Internet Explorer | WEB-BROWSER | 2 Elevated | 354.67 MB | 32,624 |
| HTTP User-Agent | WEB-BROWSER | 2 Elevated | 80.21 MB | 13,343 |
| Twitter | SOCIAL-NETWORKING | 2 Elevated | 1.20 MB | 172 |
| Facebook | SOCIAL-NETWORKING | 1 Low | 2.12 MB | 90 |
| TeamViewer | REMOTE-ACCESS | 1 Low | 337.69 KB | 33 |
| LogMeIn | REMOTE-ACCESS | 1 Low | 13.86 KB | 2 |
| Encrypted Key Exchange | PROXY-ACCESS | 3 High | 41.76 MB | 37,507 |
| WebSocket | PROTOCOLS | 1 Low | 8.68 MB | 303 |
| IMAP | PROTOCOLS | 1 Low | 1.06 MB | 133 |
| STUN | PROTOCOLS | 1 Low | 5.25 KB | 12 |
| SSL | PROTOCOLS | 1 Low | 203.85 MB | 16,279 |
| ICMP | PROTOCOLS | 1 Low | 68.51 MB | 24,419 |
| HTTP Protocol | PROTOCOLS | 1 Low | 49.86 MB | 2,613 |
| DNS Protocol | PROTOCOLS | 1 Low | 77.20 KB | 838 |
| BitTorrent Protocol | P2P | 1 Low | 65.38 MB | 132,483 |
| YouTube | MULTIMEDIA | 1 Low | 25.04 KB | 2 |
| Shockwave Flash (SWF) | MULTIMEDIA | 1 Low | 266.47 MB | 2,804 |
| Quicktime | MULTIMEDIA | 1 Low | 272.55 KB | 3 |

= sorted by

# Top Applications by Category (continued)

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Amazon.com | MISC-APPS | 1 Low | 12.38 KB | 2 |
| Microsoft CryptoAPI | MISC-APPS | 1 Low | 2.08 MB | 930 |
| The Weather Channel | MISC-APPS | 1 Low | 507.53 KB | 410 |
| WeatherBug | MISC-APPS | 1 Low | 25.32 KB | 2 |
| Bing | MISC-APPS | 1 Low | 10.51 KB | 8 |
| WidgiToolbar | MISC-APPS | 1 Low | 2.90 KB | 2 |
| Fastly CDN | INFRASTRUCTURE | 1 Low | 546.25 KB | 46 |
| Akamai CDN | INFRASTRUCTURE | 1 Low | 445.55 KB | 64 |
| Amazon CloudFront | INFRASTRUCTURE | 1 Low | 163.56 MB | 411 |
| OCSP | INFRASTRUCTURE | 1 Low | 248.20 KB | 79 |
| Skype | IM | 2 Elevated | 611.39 KB | 46 |
| Yahoo! Messenger | IM | 2 Elevated | 401.33 KB | 14 |
| AIM | IM | 2 Elevated | 81.54 KB | 1 |
| General HTTPS MGMT | General | 2 Elevated | 2.44 GB | 403,146 |
| General UDP | General | 2 Elevated | 61.79 MB | 954,397 |
| General HTTP | General | 2 Elevated | 57.36 MB | 123,850 |
| General TCP | General | 2 Elevated | 47.73 MB | 653,197 |
| General HTTPS | General | 2 Elevated | 29.19 MB | 122,806 |
| General HTTP MGMT | General | 2 Elevated | 24.91 MB | 1,669 |
| Service RPC Services (IANA) | General | 2 Elevated | 21.51 MB | 322,482 |

= sorted by

# Top Applications by Category (continued)

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Service RPC Services | General | 2 Elevated | 1.69 MB | 26,521 |
| Service Echo | General | 2 Elevated | 1.29 MB | 1,890 |
| General LDAP | General | 2 Elevated | 1.08 MB | 661 |
| Service iMesh | General | 2 Elevated | 933.92 KB | 8,761 |
| Service SSO Agent 1 | General | 2 Elevated | 788.63 KB | 1,188 |
| Service Edonkey TCP | General | 2 Elevated | 598.24 KB | 4,292 |
| General IKE | General | 2 Elevated | 521.57 KB | 1,311 |
| General DNS | General | 2 Elevated | 378.27 KB | 958 |
| Service NetBios SSN TCP | General | 2 Elevated | 350.96 KB | 1,332 |
| Service NetFlow / IPFIX | General | 2 Elevated | 126.23 KB | 2,382 |
| Service Yahoo Messenger TCP | General | 2 Elevated | 114.61 KB | 2 |
| General NETBIOS | General | 2 Elevated | 108.54 KB | 1,425 |
| Service NT Domain Login Port 1025 | General | 2 Elevated | 106.69 KB | 1,287 |
| Service NTP | General | 2 Elevated | 21.61 KB | 46 |
| General SIP control | General | 2 Elevated | 20.80 KB | 69 |
| Service SSH | General | 2 Elevated | 11.09 KB | 225 |
| Service ZebTelnet | General | 2 Elevated | 9.95 KB | 157 |
| Service Tivo TCP Data | General | 2 Elevated | 9.15 KB | 67 |
| Service Kazaa / FastTrack | General | 2 Elevated | 7.65 KB | 81 |
| General Telnet | General | 2 Elevated | 6.46 KB | 114 |

= sorted by

# Top Applications by Category (continued)

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Service MS SQL | General | 2 Elevated | 3.98 KB | 75 |
| General RADIUS | General | 2 Elevated | 3.59 KB | 52 |
| General RAS control | General | 2 Elevated | 3.57 KB | 26 |
| Service MMS TCP | General | 2 Elevated | 2.23 KB | 15 |
| Service Enhanced TV | General | 2 Elevated | 1.74 KB | 15 |
| Service MMS UDP | General | 2 Elevated | 1.55 KB | 11 |
| Service Terminal Services TCP | General | 2 Elevated | 1.35 KB | 28 |
| Service PC Anywhere UDP | General | 2 Elevated | 1.10 KB | 20 |
| General Oracle data | General | 2 Elevated | 936.00 Bytes | 15 |
| Service SonicWALL Console Proxy | General | 2 Elevated | 870.00 Bytes | 9 |
| Service Quake | General | 2 Elevated | 870.00 Bytes | 6 |
| General PPTP control | General | 2 Elevated | 631.00 Bytes | 11 |
| Service WinMX TCP 7729-7735 | General | 2 Elevated | 608.00 Bytes | 12 |
| Service ShoreTel Call Control | General | 2 Elevated | 576.00 Bytes | 4 |
| Service SIP | General | 2 Elevated | 563.00 Bytes | 10 |
| Service Timbuktu TCP 1417-1420 | General | 2 Elevated | 456.00 Bytes | 9 |
| Service MSN TCP | General | 2 Elevated | 456.00 Bytes | 3 |
| General SNMP | General | 2 Elevated | 448.00 Bytes | 6 |
| Service MSN UDP | General | 2 Elevated | 432.00 Bytes | 3 |
| General SMTP | General | 2 Elevated | 328.00 Bytes | 7 |

= sorted by

# Top Applications by Category (continued)

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Service SMB | General | 2 Elevated | 250.00 Bytes | 5 |
| Service Redirect | General | 2 Elevated | 224.00 Bytes | 4 |
| General FTP control | General | 2 Elevated | 198.00 Bytes | 4 |
| Service T120 (Whiteboard+A43) | General | 2 Elevated | 152.00 Bytes | 1 |
| Service Apple Bonjour | General | 2 Elevated | 149.00 Bytes | 2 |
| General Tftp | General | 2 Elevated | 138.00 Bytes | 3 |
| Service Squid | General | 2 Elevated | 138.00 Bytes | 3 |
| Service ShoreTel RTP | General | 2 Elevated | 131.00 Bytes | 1 |
| Service IRC (Chat) 6666-6670 | General | 2 Elevated | 92.00 Bytes | 2 |
| Service DCE EndPoint | General | 2 Elevated | 46.00 Bytes | 1 |
| Service RTSP TCP | General | 2 Elevated | 46.00 Bytes | 1 |
| Electronic Arts | GAMING | 1 Low | 1.76 MB | 1,609 |
| Steam Software | GAMING | 1 Low | 81.40 MB | 67 |
| Executable | FILETYPE-DETECTION | 3 High | 675.86 MB | 26 |
| Archive | FILETYPE-DETECTION | 3 High | 50.10 KB | 2 |
| Audio Video Stream | FILETYPE-DETECTION | 2 Elevated | 9.40 MB | 148 |
| Image | FILETYPE-DETECTION | 1 Low | 134.17 MB | 24,575 |
| IDM | DOWNLOAD-APPS | 1 Low | 2.10 KB | 1 |
| Google Analytics | BROWSING-PRIVACY | 1 Low | 1.90 MB | 887 |
| AppNexus | BROWSING-PRIVACY | 1 Low | 1.35 MB | 218 |

⇅ = sorted by

# Top Applications by Category (continued)

The Top Applications section provides information on top applications, categories, risk level, traffic volume and session count. This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

| Application | Category | Risk | Traffic | Sessions |
|---|---|---|---|---|
| Media Innovation Group | BROWSING-PRIVACY | 1 Low | 488.91 KB | 177 |
| Serving-Sys | BROWSING-PRIVACY | 1 Low | 445.42 KB | 176 |
| Chart Beat | BROWSING-PRIVACY | 1 Low | 434.74 KB | 41 |
| Betr Ad | BROWSING-PRIVACY | 1 Low | 196.33 KB | 164 |
| MediaMath | BROWSING-PRIVACY | 1 Low | 178.82 KB | 80 |
| Quantcast | BROWSING-PRIVACY | 1 Low | 103.93 KB | 83 |
| Double Verify | BROWSING-PRIVACY | 1 Low | 54.83 KB | 10 |
| DoubleClick | BROWSING-PRIVACY | 1 Low | 26.80 KB | 11 |
| AOL Advertising | BROWSING-PRIVACY | 1 Low | 23.46 KB | 2 |
| eXelate Media | BROWSING-PRIVACY | 1 Low | 7.79 KB | 3 |
| Dropbox | BACKUP-APPS | 2 Elevated | 6.37 MB | 327 |
| Box | BACKUP-APPS | 2 Elevated | 1.48 MB | 253 |
| Evernote | BACKUP-APPS | 1 Low | 287.34 KB | 55 |
| Syncplicity | BACKUP-APPS | 1 Low | 5.60 MB | 796 |
| Apple Updates | APP-UPDATE | 1 Low | 1.87 MB | 6 |
| Microsoft Windows Updates | APP-UPDATE | 1 Low | 2.63 MB | 16 |
| Google Picasa | APP-UPDATE | 1 Low | 112.01 KB | 56 |

= sorted by

# Top Applications by Risk Level

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. Dell SonicWALL firewalls identify, log and rank traffic flowing through your network to protect against such attacks.

The applications listed below represent the most vulnerable applications seen on your network.

| Application | Risk | Traffic | Sessions |
|---|---|---|---|
| Executable | 3 High | 675.86 MB | 26 |
| Encrypted Key Exchange | 3 High | 41.76 MB | 37,507 |
| Archive | 3 High | 50.10 KB | 2 |
| General HTTPS MGMT | 2 Elevated | 2.44 GB | 403,146 |
| Microsoft Internet Explorer | 2 Elevated | 354.67 MB | 32,624 |
| HTTP User-Agent | 2 Elevated | 80.21 MB | 13,343 |
| General UDP | 2 Elevated | 61.79 MB | 954,397 |
| General HTTP | 2 Elevated | 57.36 MB | 123,850 |
| General TCP | 2 Elevated | 47.73 MB | 653,197 |
| General HTTPS | 2 Elevated | 29.19 MB | 122,806 |
| General HTTP MGMT | 2 Elevated | 24.91 MB | 1,669 |
| Service RPC Services (IANA) | 2 Elevated | 21.51 MB | 322,482 |
| Audio Video Stream | 2 Elevated | 9.40 MB | 148 |
| Dropbox | 2 Elevated | 6.37 MB | 327 |
| General Multicast | 2 Elevated | 2.52 MB | 34,044 |
| Service RPC Services | 2 Elevated | 1.69 MB | 26,521 |
| Box | 2 Elevated | 1.48 MB | 253 |
| Service Echo | 2 Elevated | 1.29 MB | 1,890 |
| Twitter | 2 Elevated | 1.20 MB | 172 |
| General LDAP | 2 Elevated | 1.08 MB | 661 |

= sorted by

# Top Applications by Bandwidth

Excessive demand, often the result of large downloads or streaming video, can place an unacceptable strain on your network infrastructure.

These applications represent the biggest consumers of bandwidth on your network.

| Application | Risk | Traffic | Sessions |
|---|---|---|---|
| General HTTPS MGMT | 2 Elevated | 2.44 GB | 403,146 |
| Executable | 3 High | 675.86 MB | 26 |
| Microsoft Internet Explorer | 2 Elevated | 354.67 MB | 32,624 |
| Shockwave Flash (SWF) | 1 Low | 266.47 MB | 2,804 |
| SSL | 1 Low | 203.85 MB | 16,279 |
| Amazon CloudFront | 1 Low | 163.56 MB | 411 |
| Image | 1 Low | 134.17 MB | 24,575 |
| Steam Software | 1 Low | 81.40 MB | 67 |
| HTTP User-Agent | 2 Elevated | 80.21 MB | 13,343 |
| ICMP | 1 Low | 68.51 MB | 24,419 |
| BitTorrent Protocol | 1 Low | 65.38 MB | 132,483 |
| General UDP | 2 Elevated | 61.79 MB | 954,397 |
| General HTTP | 2 Elevated | 57.36 MB | 123,850 |
| HTTP Protocol | 1 Low | 49.86 MB | 2,613 |
| General TCP | 2 Elevated | 47.73 MB | 653,197 |

## Next Steps

If you find applications that are non-productive and use most of the bandwidth on your network, it's possible to create policies using Application Control in your Dell SonicWALL firewall to either bandwidth limit or block access to those applications.

= sorted by

# Top Applications by Bandwidth (continued)

Excessive demand, often the result of large downloads or streaming video, can place an unacceptable strain on your network infrastructure.

These applications represent the biggest consumers of bandwidth on your network.

| Application | Risk | Traffic | Sessions |
|---|---|---|---|
| Google | 1 Low | 33.33 MB | 2,009 |
| General HTTPS | 2 Elevated | 29.19 MB | 122,806 |
| General HTTP MGMT | 2 Elevated | 24.91 MB | 1,669 |
| Service RPC Services (IANA) | 2 Elevated | 21.51 MB | 322,482 |

## Next Steps

If you find applications that are non-productive and use most of the bandwidth on your network, it's possible to create policies using Application Control in your Dell SonicWALL firewall to either bandwidth limit or block access to those applications.

= sorted by

# Top Exploitation Attempts

The Top Exploitation Attempts section provides details on the top exploits blocked by your Dell SonicWALL next-generation firewall. The report includes information on the event type, name, and total number of attempts blocked per signature. To learn more about other potential exploits being blocked by your firewall visit the Dell Security SonicAlerts page.

| Event Type | Name | Blocked |
|---|---|---|
| IDP | Destination Unreachable (Port Unreachable) | 24420 |
| IDP | Time-To-Live Exceeded in Transit | 624 |
| IDP | SSLv2.0 Client Hello 2 | 121 |
| IDP | Suspicious XML File -l 01 | 41 |
| IDP | Obfuscated JavaScript Code 13 | 2 |

## Next Steps

Using the information from the Top Exploitation Attempts you can determine whether any system on your network may be open to these types of malware attacks or vulnerabilities. This typically results from a specific exploit in unpatched software or from a vulnerable version of software used on an endpoint.

= sorted by

# Top URL Categories

The Top URL Categories section provides a percentage breakdown of the HTTP/HTTPS URL traffic bandwidth based on Dell SonicWALL Content Filtering Service categories.

| URL Category | Traffic (%) | Session/Count |
|---|---|---|
| Business and Economy | 26 | 1278 |
| Information Technology/Computer | 23 | 1146 |
| Search Engines and Portals | 11 | 566 |
| Not Rated | 9 | 426 |
| Advertisement | 8 | 405 |
| News and Media | 5 | 224 |
| Freeware/Software Downloads | 4 | 208 |
| Reference | 3 | 161 |
| Sports/Recreation | 3 | 156 |
| Arts/Entertainment | 1 | 64 |
| Multimedia | 1 | 63 |
| Web Communications | <1 | 48 |
| Social Networking | <1 | 47 |
| Web Hosting | <1 | 33 |
| Education | <1 | 31 |
| Kid Friendly | <1 | 30 |
| Games | <1 | 17 |
| Chat/Instant Messaging (IM) | <1 | 15 |
| Shopping | <1 | 10 |
| E-Mail | <1 | 6 |
| Personals and Dating | <1 | 2 |

= sorted by

# Top URL Categories (continued)

The Top URL Categories section provides a percentage breakdown of the HTTP/HTTPS URL traffic bandwidth based on Dell SonicWALL Content Filtering Service categories.

| URL Category | Traffic (%) | Session/Count |
|---|---|---|
| Political/Advocacy Groups | <1 | 1 |
| Health | <1 | 1 |
| Malware | <1 | 1 |
| Real Estate | <1 | 1 |
| Hacking/Proxy Avoidance Systems | <1 | 1 |
| Pornography | <1 | 1 |

= sorted by

# Top Application Categories by Bandwidth

The Top Application Categories by Bandwidth section provides a percentage breakdown of the top application traffic bandwidth based on the Dell SonicWALL Application Control categories.

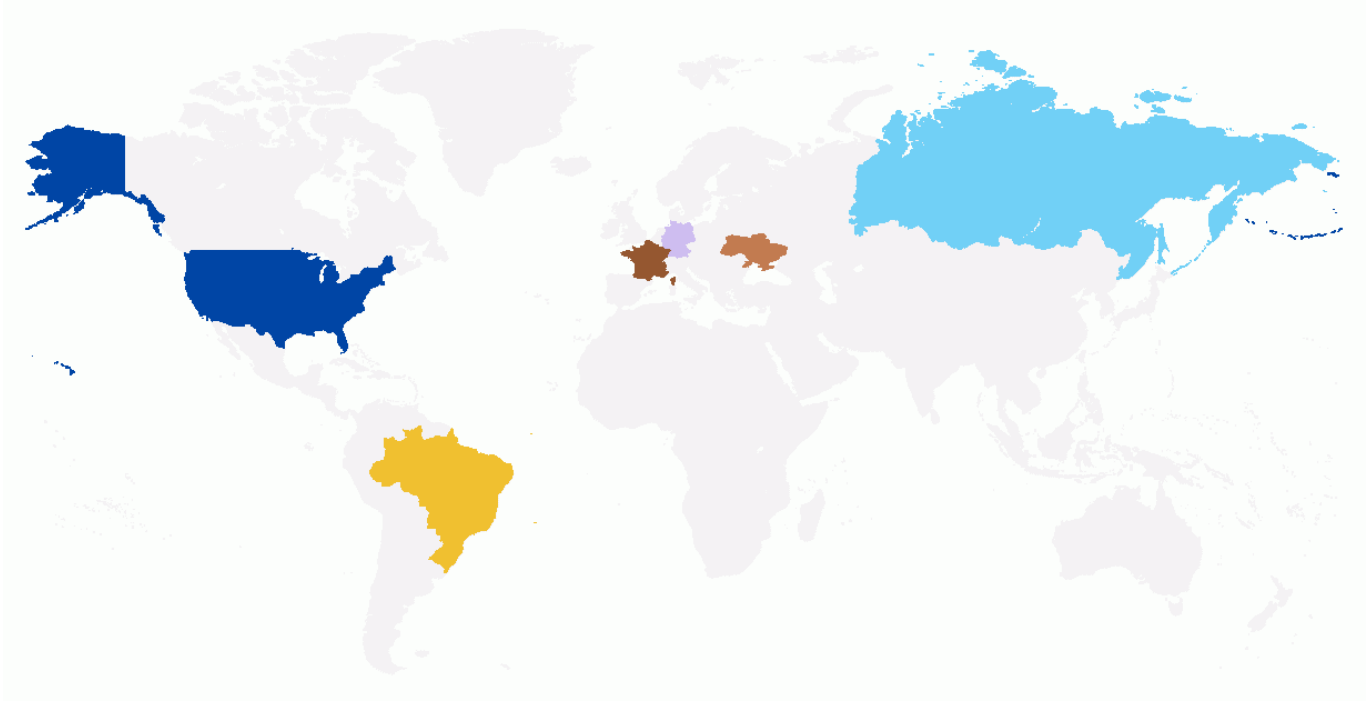
| Application Category | Traffic (%) ⇅ | Session/Count |
|---|---|---|
| None | 57 | 2709896 |
| Browser | 23 | 33777 |
| Application | 15 | 180977 |
| Network Infrastructure | 5 | 42040 |

⇅ = sorted by

# Top Countries by Traffic

The Top Countries by Traffic section provides an overview of the traffic that is either destined to a device behind your firewall or to a specific country. This data can be used to determine if traffic is going to a particular location and whether additional GeoIP or Botnet policies should be put in place to block those attempts.

The top 10 countries by source detected during the audit period are presented below:



| Country | Traffic | Sessions | Blocked |
|---|---|---|---|
| United States | 4.92 GB | 722788 | 0 |
| Germany | 66.77 MB | 314972 | 0 |
| Russian Federation | 13.73 MB | 267626 | 267626 |
| Brazil | 270.24 MB | 68676 | 0 |
| Ukraine | 3.11 MB | 60328 | 60328 |
| France | 91.61 MB | 40033 | 0 |

= sorted by

# Top Session Usage by IP

The Top Session Usage by IP section provides a list of the top IP addresses and total session counts from devices behind your firewall. This information provides insight into the largest consumers of traffic going out through your firewall.

| IP | Traffic | Session ⇅ |
|---|---|---|
| 255.255.255.255 | 9.82 GB | 5,865,292 |
| 173.240.215.30 | 2.58 GB | 1,682,405 |
| Remaining IPs | 3.00 GB | 1,135,288 |
| 192.168.150.64 | 170.89 MB | 396,875 |
| 192.168.150.168 | 133.55 MB | 350,953 |
| 192.168.150.62 | 434.84 MB | 260,300 |
| 192.168.150.63 | 908.04 MB | 175,632 |
| 103.19.168.10 | 165.78 MB | 33,330 |
| 118.200.192.189 | 150.00 MB | 32,291 |
| 65.123.159.194 | 164.85 MB | 31,086 |
| 192.168.150.56 | 193.62 MB | 28,654 |
| 192.168.150.167 | 102.94 MB | 26,305 |
| 164.177.29.33 | 72.70 MB | 19,658 |
| 46.4.82.37 | 1.53 MB | 16,579 |
| 176.9.74.238 | 1.53 MB | 16,574 |
| 176.9.60.144 | 1.53 MB | 16,572 |
| 176.9.139.141 | 1.53 MB | 16,569 |
| 176.9.42.48 | 1.53 MB | 16,568 |
| 78.47.242.106 | 1.53 MB | 16,567 |
| 176.9.139.66 | 1.53 MB | 16,565 |

⇅ = sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Top Session Usage by IP (continued)

The Top Session Usage by IP section provides a list of the top IP addresses and total session counts from devices behind your firewall. This information provides insight into the largest consumers of traffic going out through your firewall.

| IP | Traffic | Session ⇅ |
|---|---|---|
| 106.51.249.78 | 28.99 MB | 12,987 |
| 176.9.70.242 | 1.29 MB | 12,886 |
| 144.76.41.176 | 2.42 MB | 12,848 |
| 193.120.18.38 | 59.75 MB | 10,288 |

⇅ = sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Top Traffic Usage by IP

The Top Traffic Usage by IP section provides a list of the top IP addresses and the total traffic counts from devices behind your firewall. This information provides insight into the largest consumers of traffic by volume going through your firewall.

| IP | Traffic ⇅ | Session |
|---|---|---|
| 255.255.255.255 | 9.82 GB | 5,865,292 |
| Remaining IPs | 3.00 GB | 1,135,288 |
| 173.240.215.30 | 2.58 GB | 1,682,405 |
| 192.168.150.63 | 908.04 MB | 175,632 |
| 192.168.150.62 | 434.84 MB | 260,300 |
| 192.168.150.61 | 298.08 MB | 2,338 |
| 192.168.150.56 | 193.62 MB | 28,654 |
| 192.168.150.64 | 170.89 MB | 396,875 |
| 103.19.168.10 | 165.78 MB | 33,330 |
| 65.123.159.194 | 164.85 MB | 31,086 |
| 118.200.192.189 | 150.00 MB | 32,291 |
| 192.168.150.168 | 133.55 MB | 350,953 |
| 192.168.150.166 | 118.81 MB | 2,681 |
| 192.168.150.167 | 102.94 MB | 26,305 |
| 164.177.29.33 | 72.70 MB | 19,658 |
| 186.176.192.178 | 70.19 MB | 9,903 |
| 66.148.156.18 | 63.04 MB | 8,729 |
| 193.120.18.38 | 59.75 MB | 10,288 |
| 186.176.9.36 | 30.98 MB | 6,448 |
| 106.51.249.78 | 28.99 MB | 12,987 |

⇅ = sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Top Traffic Usage by IP (continued)

The Top Traffic Usage by IP section provides a list of the top IP addresses and the total traffic counts from devices behind your firewall. This information provides insight into the largest consumers of traffic by volume going through your firewall.

| IP | Traffic | Session |
|---|---|---|
| 103.246.160.150 | 26.18 MB | 6,304 |
| 89.190.195.82 | 25.05 MB | 6,186 |
| 2.50.8.110 | 18.77 MB | 2,435 |
| 192.168.150.171 | 11.86 MB | 4,244 |

= sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Top User Sessions

The Top User Sessions section provides a list of the top users by total session and name, which can provide insight into the largest consumers of traffic behind your Dell SonicWALL firewall.

| User | Traffic | Session ⇅ |
|---|---|---|
| All | 4.91 GB | 2,966,696 |
| UNKNOWN | 2.59 GB | 1,719,416 |
| whruska | 170.89 MB | 396,871 |
| madams | 133.55 MB | 350,953 |
| cparedes | 434.84 MB | 260,298 |
| kgates | 908.04 MB | 175,630 |
| rcarney | 193.62 MB | 28,653 |
| gsaunders | 102.94 MB | 26,304 |
| dsimmons | 118.81 MB | 2,680 |
| Unknown (SSO failed) | 10.49 MB | 2,602 |
| klinh | 298.08 MB | 2,337 |
| rparker | 6.59 MB | 952 |

⇅ = sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Top User Traffic

The Top User Traffic sesion provides a list of the top users by total traffic and name, which can provide insight into the largest consumers of traffic behind you Dell SonicWALL firewall.

| User | Traffic ⇅ | Session |
|---|---|---|
| All | 4.91 GB | 2,966,696 |
| UNKNOWN | 2.59 GB | 1,719,416 |
| kgates | 908.04 MB | 175,630 |
| cparedes | 434.84 MB | 260,298 |
| klinh | 298.08 MB | 2,337 |
| rcarney | 193.62 MB | 28,653 |
| whruska | 170.89 MB | 396,871 |
| madams | 133.55 MB | 350,953 |
| dsimmons | 118.81 MB | 2,680 |
| gsaunders | 102.94 MB | 26,304 |
| Unknown (SSO failed) | 10.49 MB | 2,602 |
| rparker | 6.59 MB | 952 |

⇅ = sorted by

## Next Steps

Your Dell SonicWALL firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

# Report Configuration

In order to provide the full set of reports, you should enable the following options in the management GUI of your Dell SonicWALL next-generation firewall. If these options are not configured, then the final SWARM report will only contain only a subset of all available data.

| Page | Status | |
|---|---|---|
| Aggregate Reporting | ✓ | Enabled. Reporting for aggregate data logs enabled. |
| App Reporting | ✓ | Enabled. Reporting for aggregate application data logs enabled. |
| URL Reporting | ✓ | Enabled. Reporting for aggregate URL data logs enabled. |
| URL Category Reporting | ✓ | Enabled. Reporting for URL category data logs enabled. |
| GAV Reporting | ✓ | Enabled. Either GAV is licensed or GAV status is enabled. |
| Spyware Reporting | ✓ | Enabled. Either Spyware is licensed or Spyware status is enabled. |
| IPS Reporting | ✓ | Enabled. Either IPS is licensed or IPS status is enabled. |
| Geo IP Reporting | ✓ | Enabled. Reporting for aggregate geo IP data logs enabled. |
| App IP Reporting | ✓ | Enabled. Reporting for aggregate app IP data logs enabled. |
| User IP Reporting | ✓ | Enabled. Reporting for aggregate user IP data logs enabled. |

# Appendix 1: Risk Definitions

## Low

This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under there conditions, only a routine security posture, designed to defeat normal rating threats, is warranted.

## Elevated

This application may not have a legitimate purpose on the network. The application can also be a source of unwanted traffic to the internal network. Some messenger services, such as Meebo, fall into this category.

## High

This application may be either resource hungry or may provide a service that circumvents normal network rules. Allowing this application to run may result in users unknowingly downloading malicious files. Some proxy services, such as Ultrasurf, fall into this categroy. It also includes some peer-to-peer applications, such as BitComet.

## Severe

This application is resource hungry and consumes a large amount of network bandwidth. The application is also a well known facilitator of malicious activity, and is often used to infect enpoints. Some peer-to-peer services, such as eMule, fall into this category.

# Appendix 2: Vulnerability Descriptions

### Suspicious XML File -l 01

This signature detects a XML file which indicates allow access from all domains.

### SSLv2.0 Client Hello 2

SSL 2.0 was deprecated in 2011 by RFC 6176.

### Destination Unreachable (Port Unreachable)

Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite. ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes.

ICMP traffic may be used to map a network, or help fingerprint an OS. The information used from these methods may be used for illegitimate purposes.

### Obfuscated JavaScript Code 13

This signature indicates obfuscated JavaScript being sent to an HTTP client.

### Time-To-Live Exceeded in Transit

Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite. ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes.

ICMP traffic may be used to map a network, or help fingerprint an OS. The information used from these methods may be used for illegitimate purposes.

# Appendix 3: Application Descriptions

## AIM

Available in one form or another since 1997, AOL Instant Messenger (or AIM) is an instant messaging application that allows registered users to communicate in real time via text, voice, and video transmission over the Internet. Users can talk online with other people connected with the service, transfer files up to 10mb, message a cell phone, etc. It is maintained by AOL, LLC, and uses the proprietary OSCAR and TOC protocols. AIM has been subject to vulnerabilities in the past where it was maliciously exploited using third-party software to send viruses to users' computers and used to harvest IP addresses.

## AOL Advertising

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## Akamai CDN

Akamai is a content delivery network.

## Amazon CloudFront

Amazon CloudFront is a content delivery web service. It integrates with other Amazon Web Services products to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

## Amazon.com

Amazon.com, Inc. (NASDAQ: AMZN) is an American-based multinational electronic commerce company. Headquartered in Seattle, Washington, it is America's largest online retailer, with nearly three times the Internet sales revenue of the runner up, Staples, Inc., as of January 2010.Jeff Bezos founded Amazon.com, Inc. in 1994 and launched it online in 1995 as Cadabra.com. It started as an online bookstore, but soon diversified, selling DVDs, CDs, MP3 downloads, computer software, video games, electronics, apparel, furniture, food, and toys. Amazon has established separate websites in Canada, the United Kingdom, Germany, France, Japan, and China. It also provides international shipping to certain countries for some of its products. A 2009 survey found that Amazon was the UK's favorite music and video retailer, and third overall retailer.

## AppNexus

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## Apple Updates

Apple (or Apple Inc.) designs and manufactures consumer electronics and software products. Enabling blocking for this application will also block most Apple Inc. network traffic. (Use with caution.)

# Appendix 3: Application Descriptions

## Archive

RPM files are software files packaged by the RPM Package Manager system.

## Audio Video Stream

This SonicWALL signature identifies Audio, Video, Graphic, and other Multimedia file streams.

## Betr Ad

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## Bing

Bing is the newest incarnation of a web search engine portal from Microsoft Corporation.

## BitTorrent Protocol

BitTorrent Protocol is a peer-to-peer file sharing (P2P) communications protocol, famous (or infamous) for its ability to distribute large data files--movies, software, photos, documents, etc. Usage of the protocol accounts for significant traffic on the Internet. Peer-to-peer networks are characterized by a decentralized topology of temporary peer nodes that join and leave the network, unlike traditional client-server networks. BitTorrent is maintained by BitTorrent, Inc. There are numerous compatible BitTorrent clients, such as uTorrent, BitComet, Deluge, TurboBT, and Transmission, and Xunlei (a Chinese-language file sharing client). Many of these BT Clients, in addition to using the BitTorrent Protocol proper, also use other file-sharing protocols and downloading methods, such as eMule/eDonkey protocol, and so-called HTTP Download Acceleration. (HTTP Download Acceleration is clever use of the HTTP 'Range' header in HTTP requests. Multiple HTTP requests are made in parallel for different byte ranges of the file.) BitTorrent clients also use encryption techniques to evade firewall application control over both TCP and UDP. To block all file-sharing applications we recommend enabling the entire P2P category, both SonicWALL Encrypted Key Exchange application signatures (sids: 5 & 7), and the PROTOCOLS >> HTTP Range header signature (sid: 6872).

## Box

Box (box.net and box.com) is a web-based file storage system that lets users store, and then remotely access file content.

## Chart Beat

Chart Beat is a web-analytics company that collects notifications from its partner's software: website, web applications, desktop apps, etc. about user activity: how long did the user stay at partners site, etc.

## DNS Protocol

The Domain Name System (DNS) is a naming system for computers and services connected to the Internet, where DNS translates the hostnames into IP addresses.

# Appendix 3: Application Descriptions

## Double Verify

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## DoubleClick

\
DoubleClick is a subsidiary of Google that develops and provides Internet ad serving services. Its clients include agencies, marketers (Universal McCann Interactive, AKQA etc.) and publishers who serve customers like Microsoft, General Motors, Coca-Cola, Motorola, L'Oréal, Palm, Inc., Visa USA, Nike, Carlsberg among others. DoubleClick's headquarters are in New York City, United States. DoubleClick embeds code in its partners websites that cause the web visitors browser to send a notification back indicating a visit to the site.\
\
\
This SonicWALL signature identifies DoubleClick HTTP traffic.\

## Dropbox

Dropbox is storage service that allows users to store and synchronize file content between computers, over the Internet. Dropbox has is compatible with Windows, Mac OS X and Linux platform clients. No-cost user accounts offer 2 GB of storage space, while paid accounts offer significantly higher storage space.

## Electronic Arts

Electronic Arts, Inc. (EA) (NASDAQ: ERTS) is an international developer, marketer, publisher and distributor of video games. Currently, EAs most successful products are sports games published under its EA Sports label, games based on popular movie licenses such as Harry Potter and games from long-running franchises like Need for Speed, Medal of Honor, The Sims, Battlefield and the later games in the Burnout and Command & Conquer series. They are also the distributors of the Rock Band series.

## Encrypted Key Exchange

Encrypted Key Exchange (also known as EKE) is a family of password-authenticated key agreement methods described by Steven M. Bellovin and Michael Merritt. Although several of the forms of EKE in this paper were later found to be flawed, the surviving, refined, and enhanced forms of EKE effectively make this the first method to amplify a shared password into a shared key, where the shared key may subsequently be used to provide a zero-knowledge password proof or other functions.
This application identifies randomness in a TCP and UDP sessions between an application and a peer or server. Many applications that want to evade firewall detection—including Ultrasurf, Ammy Admin, Skype, Psiphon, eMule, and other—use encrypted TCP and UDP sessions. By nature an encrypted session is just a bunch of seemingly random bytes within the transport layer payload--how the bytes are interpreted is a mystery that only the application's protocol designers know. For this reason, all encrypted sessions look alike at the firewall, and there is no way to identify from which application the encrypted TCP session is coming. Therefore, enabling prevention for these signatures--SID 5 for TCP, and SID 7 for UDP—will necessarily block all and any encrypted sessions emanating from these evasive applications. There is no way to distinguish between them.

# Appendix 3: Application Descriptions

## Evernote

Evernote is a suite of software and services designed for notetaking and archiving that can be had in a paid version or a more restricted, advertising-supported, free version. A note can be a piece of formatted text, a full webpage or webpage excerpt, a photograph, a voice memo, or a handwritten ink note. Notes can also have file attachments.Notes can then be sorted into folders, tagged, annotated, edited, given comments, and searched.Evernote supports a number of operating system platforms (including Android, Mac OS X, Windows and WebOS), and also offers online synchronization and backup services. Use of the online server is free up to a certain monthly usage limit, with additional monthly use reserved for paying subscribers..

## Executable

Executable and Linking Format files (.exe) are a common standard file format for executable files and libraries.

## Facebook

facebook is an enormously popular social networking site that lets users build a profile page and then seek out and connect with other friends on the service. Users can also join networks for various interests or geographic locations, upload digital media content, and even play games online through the site. facebook is subject to blocking and censure in some countries, and the site appears to continually be re-vamping their privacy policy in an effort to balance user security and business needs.

## Fastly CDN

Fastly CDN is a Content Delivery Network, an array of distributed servers that cache web content for performance optimization.

## Google

Google Inc. is most universally known for its leading Internet search capabilities. Google also provides a myriad of additional free services to users, including email, messaging, mapping services, and office productivity tools and applications.

## Google Analytics

Google Analytics is a no-cost service from Google that generates statistics on a website's visitors, in the hope of helping site owners have greater success in Google AdWords campaigns through optimized language and site content.

## Google Mail (Gmail)

Google Mail (Gmail) is the no-cost email service available from Google, Inc. Gmail also provides access to address book, calendar, and office productivity services.

## Google Picasa

Picasa, owned by Google, is an client application for compiling and editing digital photos, and creating albums for users to share. This is a cross-platform application with support for Windows, Linux, and Mac OS X environments.

# Appendix 3: Application Descriptions

## HTTP Protocol

Hypertext Transfer Protocol (HTTP) is the standard transmission protocol of requests and information between Internet servers and browsers.

## HTTP User-Agent

HTTP User-Agent is a collection of signatures that identify network traffic based on HTTP User-Agent header, or elements within the header.

## ICMP

The Internet Control Message Protocol (ICMP) is used by networked computers' operating systems to send error messages.

## IDM

Internet Download Manager (IDM) is a tool to increase download speeds by up to 5 times, resume and schedule downloads. Comprehensive error recovery and resume capability will restart broken or interrupted downloads due to lost connections, network problems, computer shutdowns, or unexpected power outages.This signature detects the download traffic for application Internet Download Manager. There is nothing special about IDM traffic. It uses standard HTTP protocol. However, it does use the 'Range' HTTP header. It spawns multiple simultaneous TCP connections; each thread downloads a chunk of the file by specifying a byte range in the HTTP request. By using multiple threads running in parallel IDM is able to accelerate the download. You can block IDM from spawning multiple, parallel threads by blocking the Range header. However, you cannot block IDM from running a single thread as it is indistinguishable from regular HTTP requests.

## IMAP

The Internet Message Access Protocol (IMAP) is the two most used Internet standard protocol for e-mail retrieval.

## Image

BMP (.bmp), also known as BitMap, is a file format for storing digital image data.

## LogMeIn

LogMeIn offers users services for remote access to client systems via the Internet. The various product versions use a proprietary remote desktop protocol transmitted via SSL, and connects remote desktops and the local computer using SSL over TCP, utilizing NAT for a peer-to-peer connection.

## Media Innovation Group

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

# Appendix 3: Application Descriptions

## MediaMath

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## Microsoft CryptoAPI

The Microsoft Cryptographic Application Programming Interface (or CAPI) is an application programming interface that is part of Microsoft Windows operating systems.

## Microsoft Internet Explorer

Microsoft Internet Explorer is the popular web browser from Microsoft.

## Microsoft Windows Updates

Microsoft Windows is the collective name for operating systems designed and produced by Microsoft Corporation. The company that develops, manufactures, licenses, and supports a wide range of software products for computing devices. This application includes updates and patches from Microsoft to any of these platforms.

## OCSP

The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

## Quantcast

Quantcast is a media measurement, web analytics service that allows users to view audience statistics for millions of websites. Quantcast Corporation's prime focus is to analyze the Internet's web sites in order to obtain accurate usage statistics by surfers from the USA. Like Alexa, Quantcast rates Web pages by ranks. Quantcast statistics always refer to the usage from the United States, therefore Alexa data and Quantcast data do not always show the same results. Quantcast does not require a toolbar to be installed upon one's web browser to obtain statistics. Instead participating websites voluntarily insert Quantcast HTML code inside Web pages they wish to have included in statistics. This code allows Quantcast to keep track of the traffic directed towards those Web sites.

## Quicktime

The QuickTime client uses HTTP to download digital content for users to view in the QuickTime player. QuickTime is an application that supports a number of media standards.

# Appendix 3: Application Descriptions

## SSL

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications on the Internet.

## STUN

Session Traversal Utilities for NAT (STUN) is a protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal. It can be used by an endpoint to determine the IP address and port allocated to it by a NAT. It can also be used to check connectivity between two endpoints, and as a keep-alive protocol to maintain NAT bindings. STUN works with many existing NATs, and does not require any special behavior from them.STUN is not a NAT traversal solution by itself. Rather, it is a tool to be used in the context of a NAT traversal solution. This is an important change from the previous version of this specification (RFC 3489), which presented STUN as a complete solution.

## ScoreCard Research

ScorecardResearch, a service of Full Circle Studies, Inc., is part of the comScore, Inc. market research community, a leading global market research effort that studies and reports on Internet trends and behavior. ScorecardResearch conducts research by collecting Internet web browsing data and then uses that data to help show how people use the Internet, what they like about it, and what they do not.

## Serving-Sys

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## Shockwave Flash (SWF)

The SWF file format (also known as Shockwave Flash) delivers text, audio, graphics and video over the Internet and is supported by Adobe Flash Player and Adobe AIR software.

## Skype

Skype is an application that allows users to make voice calls over the Internet, using a proprietary VoIP network called the Skype protocol. After a user installs client software, calls to fellow Skype users are free-of-charge, while calls to landlines and mobile phones can be made for a fee. Additional features include instant messaging, file transfer and video conferencing. Skype is owned by Microsoft Corporation. Skype uses firewall evasion techniques and requires Encrypted Key Exchange signatures, in order to prevent or detect it.

## Steam Software

Steam Engine (Valve Corp) is a digital distribution service that can send game software directly to a user's system. Steam distributes a wide range of game content and entertainment.

# Appendix 3: Application Descriptions

## Syncplicity

Syncplicity is an online storage provider that also offers central file management and anywhere access, backup, and synchronization for its users.

## TeamViewer

Compatible with Windows, Mac OS X, and Linux operating systems, TeamViewer is a package of software tools that provide users with remote control of PCs over the Internet. The software allows for screen sharing, file transfer and chat functionality.

## The Weather Channel

The Weather Channel (www.weather.com) is a website for weather. This application includes a Weather Desktop App is a widget that runs on the user's desktop PC. It provides up-to-the-minute updates of current weather conditions.

## Twitter

Twitter is a no-cost-to-user, micro-blogging messaging service, known for allowing user posts of up to 140 characters. Users can send and receive "tweets" through the Twitter website, Short Message Service (SMS), or third-party applications.

## WeatherBug

WeatherBug is a website and desktop client application that provides users with live weather data and information.

## WebSocket

The WebSocket Protocol enables two-way communication between a client running untrusted code in a controlled environment to a remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The goal of this technology is to provide a mechanism for browser-based applications that need two-way communication with servers that does not rely on opening multiple HTTP connections (e.g., using XMLHttpRequest or <iframe>s and long polling).

## WidgiToolbar

WidgiToolbar is installed as a browser utility. However, users often regret the installation due to advertising that is then delivered through the utility.

## Yahoo! Mail

Yahoo Mail is the online mail service available from Yahoo, Inc. Yahoo Mail also offers users access to address book, messaging, and calendar tools.

## Yahoo! Messenger

Yahoo Messenger is the instant messaging service available from Yahoo, a global provider of an enormous array of internet services.

# Appendix 3: Application Descriptions

## YouTube

YouTube is a popular video sharing website which lets users upload, view, and share video clips. The company uses Adobe Flash Video technology to display a wide variety of user-generated video content, including movie clips.

## eXelate Media

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

# Appendix 4: Applications

The following applications were detected on your network. Applications shown in red have a risk level of severe.

## Application (data transmitted)

1. General HTTPS MGMT (2.44 GB)
2. Executable (675.86 MB)
3. Microsoft Internet Explorer (354.67 MB)
4. Shockwave Flash (SWF) (266.47 MB)
5. SSL (203.85 MB)
6. Amazon CloudFront (163.56 MB)
7. Image (134.17 MB)
8. Steam Software (81.40 MB)
9. HTTP User-Agent (80.21 MB)
10. ICMP (68.51 MB)
11. BitTorrent Protocol (65.38 MB)
12. General UDP (61.79 MB)
13. General HTTP (57.36 MB)
14. HTTP Protocol (49.86 MB)
15. General TCP (47.73 MB)
16. Encrypted Key Exchange (41.76 MB)
17. Google (33.33 MB)
18. General HTTPS (29.19 MB)
19. General HTTP MGMT (24.91 MB)
20. Service RPC Services (IANA) (21.51 MB)
21. Audio Video Stream (9.40 MB)
22. WebSocket (8.68 MB)
23. Dropbox (6.37 MB)
24. Syncplicity (5.60 MB)
25. Microsoft Windows Updates (2.63 MB)
26. General Multicast (2.52 MB)
27. Facebook (2.12 MB)
28. Microsoft CryptoAPI (2.08 MB)
29. Google Mail (Gmail) (1.93 MB)
30. Google Analytics (1.90 MB)
31. Apple Updates (1.87 MB)
32. Electronic Arts (1.76 MB)
33. Service RPC Services (1.69 MB)
34. Box (1.48 MB)
35. AppNexus (1.35 MB)
36. Service Echo (1.29 MB)
37. Twitter (1.20 MB)
38. General LDAP (1.08 MB)
39. IMAP (1.06 MB)
40. Service iMesh (933.92 KB)
41. ScoreCard Research (861.79 KB)
42. Service SSO Agent 1 (788.63 KB)
43. Skype (611.39 KB)
44. Service Edonkey TCP (598.24 KB)
45. Fastly CDN (546.25 KB)
46. General IKE (521.57 KB)
47. The Weather Channel (507.53 KB)
48. Media Innovation Group (488.91 KB)
49. Akamai CDN (445.55 KB)
50. Serving-Sys (445.42 KB)
51. Chart Beat (434.74 KB)
52. Yahoo! Messenger (401.33 KB)
53. General DNS (378.27 KB)
54. Service NetBios SSN TCP (350.96 KB)
55. TeamViewer (337.69 KB)
56. Evernote (287.34 KB)
57. Quicktime (272.55 KB)
58. OCSP (248.20 KB)
59. Yahoo! Mail (196.34 KB)
60. Betr Ad (196.33 KB)
61. MediaMath (178.82 KB)
62. Service NetFlow / IPFIX (126.23 KB)
63. Service Yahoo Messenger TCP (114.61 KB)
64. Google Picasa (112.01 KB)
65. General NETBIOS (108.54 KB)
66. Service NT Domain Login Port 1025 (106.69 KB)

# Appendix 4: Applications

The following applications were detected on your network. Applications shown in red have a risk level of severe.

## Application (data transmitted)

67. Quantcast (103.93 KB)
68. AIM (81.54 KB)
69. DNS Protocol (77.20 KB)
70. Double Verify (54.83 KB)
71. Archive (50.10 KB)
72. DoubleClick (26.80 KB)
73. WeatherBug (25.32 KB)
74. YouTube (25.04 KB)
75. AOL Advertising (23.46 KB)
76. Service NTP (21.61 KB)
77. General SIP control (20.80 KB)
78. LogMeIn (13.86 KB)
79. Amazon.com (12.38 KB)
80. Service SSH (11.09 KB)
81. Bing (10.51 KB)
82. Service ZebTelnet (9.95 KB)
83. Service Tivo TCP Data (9.15 KB)
84. eXelate Media (7.79 KB)
85. Service Kazaa / FastTrack (7.65 KB)
86. General Telnet (6.46 KB)
87. STUN (5.25 KB)
88. General H323 control (4.65 KB)
89. Service MS SQL (3.98 KB)
90. General RADIUS (3.59 KB)
91. General RAS control (3.57 KB)
92. WidgiToolbar (2.90 KB)
93. Service MMS TCP (2.23 KB)
94. IDM (2.10 KB)
95. Service Enhanced TV (1.74 KB)
96. Service MMS UDP (1.55 KB)
97. Service Terminal Services TCP (1.35 KB)
98. Service PC Anywhere UDP (1.10 KB)
99. General Oracle data (936.00 Bytes)
100. Service SonicWALL Console Proxy (870.00 Bytes)
101. Service Quake (870.00 Bytes)
102. General PPTP control (631.00 Bytes)
103. Service WinMX TCP 7729-7735 (608.00 Bytes)
104. Service ShoreTel Call Control (576.00 Bytes)
105. Service SIP (563.00 Bytes)
106. Service Timbuktu TCP 1417-1420 (456.00 Bytes)
107. Service MSN TCP (456.00 Bytes)
108. General SNMP (448.00 Bytes)
109. Service MSN UDP (432.00 Bytes)
110. General SMTP (328.00 Bytes)
111. Service VNC 5900 (282.00 Bytes)
112. Service SMB (250.00 Bytes)
113. Service Redirect (224.00 Bytes)
114. General FTP control (198.00 Bytes)
115. Service T120 (Whiteboard+A43) (152.00 Bytes)
116. Service Apple Bonjour (149.00 Bytes)
117. General Tftp (138.00 Bytes)
118. Service Squid (138.00 Bytes)
119. Service ShoreTel RTP (131.00 Bytes)
120. Service IRC (Chat) 6666-6670 (92.00 Bytes)