

Firewall Profile Report

Powered by Congruity Technologies'



Network Quality Assurance Software

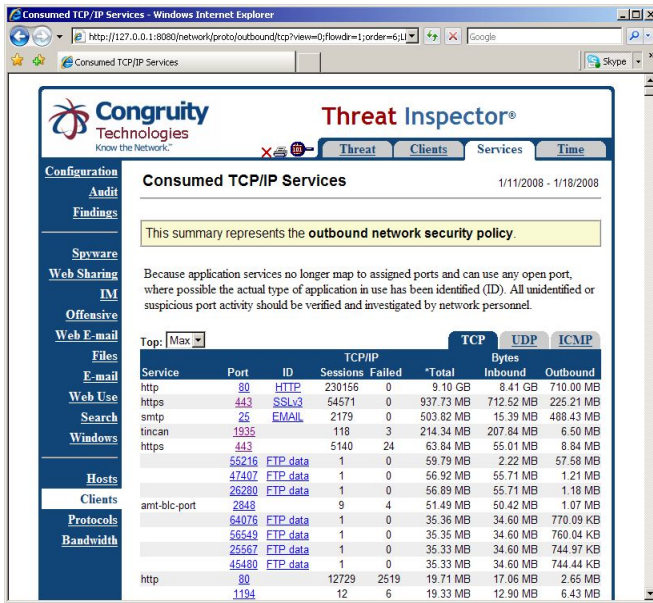
Documents firewall policy status, penetration test details and provides independent verification of internal controls and compliance efforts for improved stakeholder management and planning

Prepared for: Sample Compliance Report

Contents:

- Introduction** 3
- Bandwidth Summary** 4
 - Top Protocols 6
- Inbound Firewall Profile** 11
 - Active Protocols 12
 - Inactive Protocols 14
 - TCP/IP Access 16
 - UDP/IP Access 19
- Outbound Firewall Profile** 23
 - Active Protocols 24
 - Inactive Protocols 26
 - TCP/IP Access 28
 - UDP/IP Access 30

Threat Inspector's interactive report interface offer drill-down data review and analysis for fast, easy troubleshooting and planning



Screen Capture of Client' services detail representing outbound policy



Screen Capture of Host' services detail representing inbound policy/Pen-test

Introduction

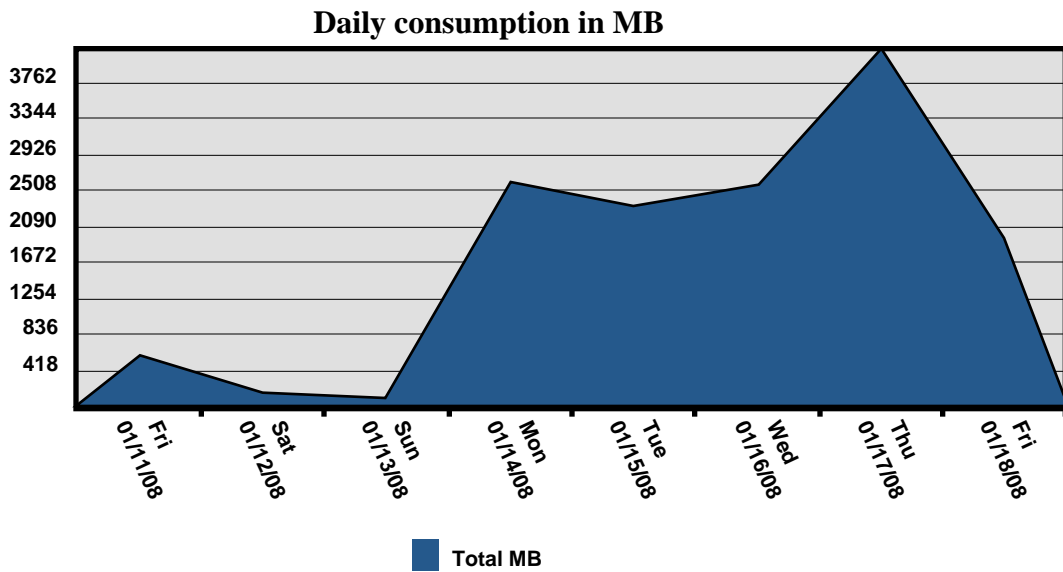
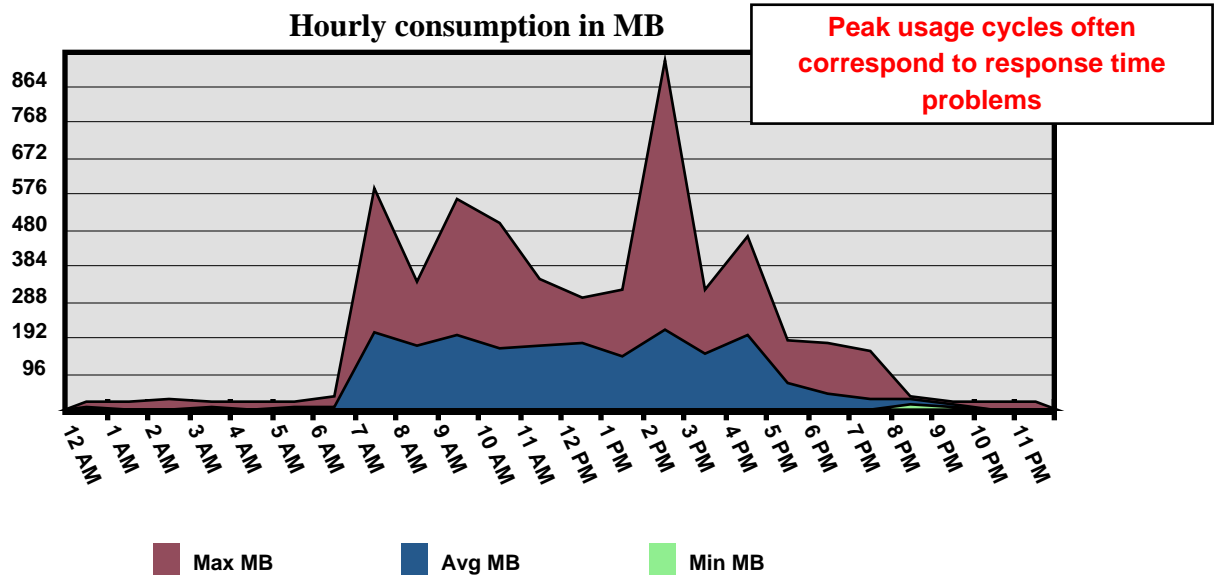
To effectively manage, an organization need facts for setting, verifying, and evaluating the effectiveness of its security policies. The purpose of this report is to review the actual implementation of the current security policy and controls by monitoring and aggregating network traffic over a one week period. Specifically, this report focuses on the inbound and outbound security policies implemented by the firewall. Compare this data to the current security policies to determine whether operational practices, equipment and policies are up-to-date and performing as expected.

Use this report to:

- Verify and evaluate the implementation of the current inbound and outbound security policies and determine if internal controls are effective.
- Discover the number of systems and protocols exposed to the Internet and document the number of external clients, networks and bandwidth impact for each.
- Discover the number of protocols in use by internal clients and document the bandwidth impact for each.

Bandwidth Summary

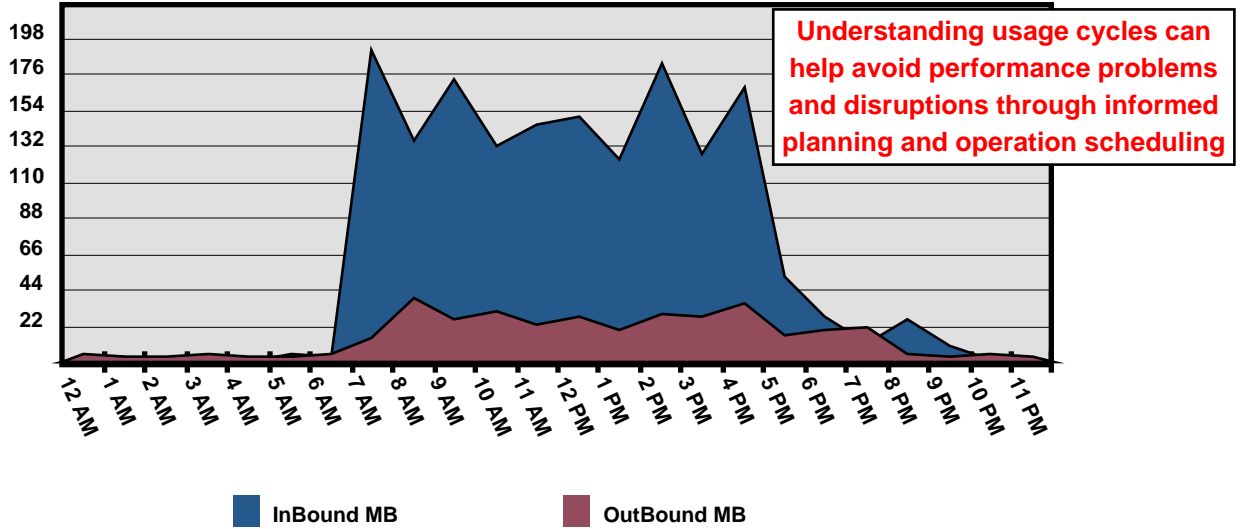
The following graphs show the number of megabytes exchanged between the local network and the Internet for each hour and day of the audit. The hourly consumption graph shows the times that the network is under the least, average and maximum load. The daily consumption graph shows the daily bandwidth totals.



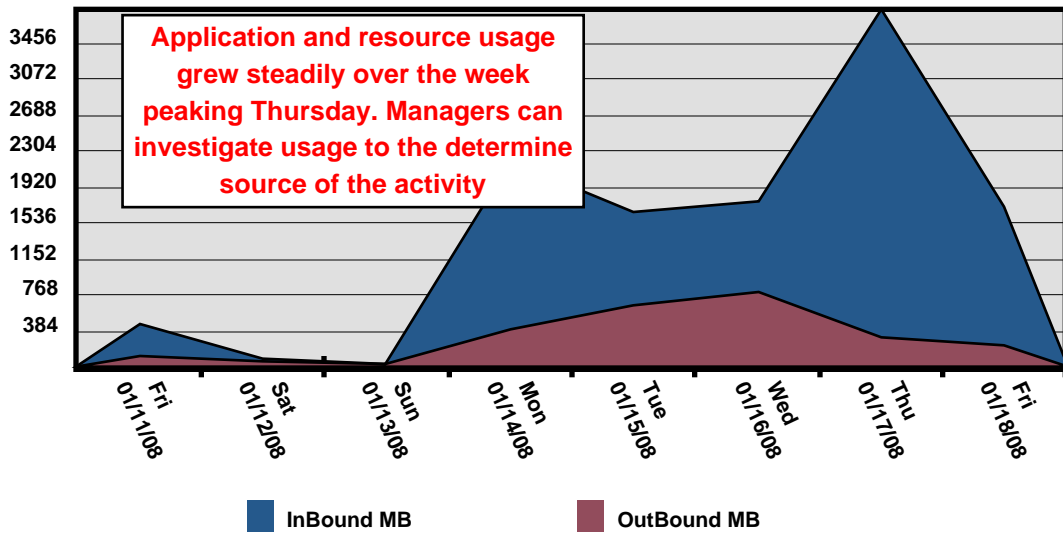
Total Consumption:	14.17 GB	Over 167.00 hours	~202.40 Kbps
Inbound:	11.50 GB	81.18%	~164.31 Kbps
Outbound:	2.67 GB	18.82%	~38.08 Kbps
Maximum hour:	937.64 MB	Thu Jan 17 2008 02:00 PM	~13109.12 Kbps
Minimum hour:	957.19 KB	Sat Jan 12 2008 06:00 PM	~13.07 Kbps

The following graphs show the total amount of Inbound and Outbound megabytes exchanged between the local network and the Internet for each hour and day of the audit.

Inbound / Outbound Hourly consumption in MB



Inbound / Outbound Daily consumption in MB



Top Protocols

The top protocols table lists the networks bandwidth consumption by standard service names and ports.

Protocol:	tcp - 80			
Name:	http Hypertext-Transport-Protocol			
This is the primary protocol of the Internet. Every time a user opens a web browser to surf the net HTTP is used.				
Sessions	Total Bytes	Inbound	Outbound	Time
249,986 65.7%	9.33 GB 71.4%	8.42 GB	938.25 MB	830h 17m

Note: 8,183 (3.3%) of sessions were inbound to exposed hosts.

Protocol:	tcp - 25			
Name:	smtp Simple Mail Transfer Protocol			
This is the standard internet protocol used for sending and receiving e-mail.				
Sessions	Total Bytes	Inbound	Outbound	Time
5,365 1.4%	1.10 GB 8.4%	641.38 MB	482.39 MB	12h 3m

Note: 2,855 (53.2%) of sessions were inbound to exposed hosts.

Protocol:	tcp - 443			
Name:	https Hypertext-Transport-Protocol over a Secure Socket Layer			
This is a secured version of HTTP whereby data exchanged between the web server and client is encrypted. HTTPS is primarily used for commercial transactions; however it can also be used to hide a user's activity from web filtering and monitoring software				
Sessions	Total Bytes	Inbound	Outbound	Time
59,627 15.7%	1001.08 MB 7.5%	767.14 MB	233.94 MB	534h 34m

Protocol:	tcp - 1696			
Name:	rrifmm rrifmm			
Sessions	Total Bytes	Inbound	Outbound	Time
1 %	427.24 MB 3.2%	414.39 MB	12.85 MB	2h 56m

Note: 1 (100%) of sessions were inbound to exposed hosts.

Protocol:	tcp - 1456			
Name:	dca DCA			
Sessions	Total Bytes	Inbound	Outbound	Time
1 %	277.12 MB 2.1%	269.52 MB	7.60 MB	39m 50s

Note: 1 (100%) of sessions were inbound to exposed hosts.

Protocol:	tcp - 1935			
Name:	tincan RTMP Real Time Messaging Protocol.			
This port has now been assigned for use with the Macromedia Flash Communication Server. This port is typically used to stream multimedia to flash applications.				
Sessions	Total Bytes	Inbound	Outbound	Time
116 %	204.10 MB 1.5%	197.88 MB	6.21 MB	3h 6m

Protocol: tcp - 55216
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	59.79 MB .4%	2.22 MB	57.58 MB	9m 44s

Protocol: tcp - 47407
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	56.92 MB .4%	55.71 MB	1.21 MB	2m 52s

Protocol: tcp - 26280
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	56.89 MB .4%	55.71 MB	1.18 MB	2m 40s

Protocol: tcp - 2848
Name: amt-blc-port AMT-BLC-PORT

Sessions	Total Bytes	Inbound	Outbound	Time
12 %	51.51 MB .4%	50.43 MB	1.08 MB	17m 48s

Protocol: udp - 4500
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
426 .1%	42.79 MB .3%	20.79 MB	22.00 MB	159h 2m

Protocol: tcp - 64076
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	35.36 MB .3%	34.60 MB	770.09 KB	1m 42s

Protocol: tcp - 56549
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	35.35 MB .3%	34.60 MB	760.04 KB	1m 40s

Protocol: tcp - 25567
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	35.33 MB .3%	34.60 MB	744.97 KB	1m 38s

Protocol: tcp - 45480
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	35.33 MB .3%	34.60 MB	744.44 KB	1m 40s

Protocol: udp - 53
Name: dns Domain Name System
 This is the protocol used to locate the IP address of Internet domain names.

Sessions	Total Bytes	Inbound	Outbound	Time
7,281 1.9%	24.77 MB .2%	19.88 MB	4.89 MB	55h 38m

Protocol: tcp - 1194
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
12 %	19.33 MB .1%	12.90 MB	6.43 MB	50h 53m

Protocol: tcp - 46629
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
112 %	17.06 MB .1%	15.86 MB	1.21 MB	1h 51m

Protocol: tcp - 40236
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	15.34 MB .1%	15.02 MB	324.79 KB	48s

Protocol: tcp - 42081
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	14.68 MB .1%	14.38 MB	310.67 KB	53s

Protocol: tcp - 554
Name: rtsp Real Time Streaming Protocol
 This protocol is used to stream audio and video content to clients over the Internet, typically consisting of non-business related information.

Sessions	Total Bytes	Inbound	Outbound	Time
15 %	8.97 MB .1%	8.70 MB	278.77 KB	7m 4s

Protocol: tcp - 3389
Name: ms-wbt-server MS WBT Server

Sessions	Total Bytes	Inbound	Outbound	Time
33 %	8.33 MB .1%	1.53 MB	6.79 MB	1h 23m

Note: 32 (97%) of sessions were inbound to exposed hosts.

Protocol: tcp - 16592
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	6.37 MB %	6.24 MB	134.36 KB	18s

Protocol: tcp - 4692
Name: Unidentified

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	5.13 MB %	4.99 MB	143.50 KB	15s

Note: 1 (100%) of sessions were inbound to exposed hosts.

Protocol:	udp - 1900				
Name:	ssdp	SSDP			
Sessions	688 .2%	Total Bytes	3.61 MB %	Inbound	0.00 B
				Outbound	3.61 MB
				Time	9h 51m

Protocol:	udp - 3478				
Name:	Unidentified				
Sessions	341 .1%	Total Bytes	3.41 MB %	Inbound	1.81 MB
				Outbound	1.60 MB
				Time	824h 54m

Protocol:	tcp - 5050				
Name:	mmcc	multimedia conference control tool			
Sessions	46 %	Total Bytes	3.41 MB %	Inbound	1.73 MB
				Outbound	1.68 MB
				Time	214h 29m

Protocol:	tcp - 88				
Name:	kerberos	Kerberos			
Sessions	1 %	Total Bytes	2.74 MB %	Inbound	2.64 MB
				Outbound	101.44 KB
				Time	26s

Protocol:	tcp - 1863				
Name:	msnp	MSNP			
Sessions	131 %	Total Bytes	2.39 MB %	Inbound	1.03 MB
				Outbound	1.36 MB
				Time	129h 5m

Protocol:	tcp - 21				
Name:	ftp	File Transfer [Control]			
Sessions	19 %	Total Bytes	2.28 MB %	Inbound	1.45 MB
				Outbound	851.77 KB
				Time	2h 56m

Protocol:	tcp - 15416				
Name:	Unidentified				
Sessions	1 %	Total Bytes	1.99 MB %	Inbound	1.95 MB
				Outbound	44.60 KB
				Time	5s

Protocol:	tcp - 61886				
Name:	Unidentified				
Sessions	1 %	Total Bytes	1.99 MB %	Inbound	1.95 MB
				Outbound	41.96 KB
				Time	6s

Protocol:	tcp - 35193				
Name:	Unidentified				

Sessions	Total Bytes	Inbound	Outbound	Time
1 %	1.98 MB %	75.59 KB	1.91 MB	20s
<hr/>				
Protocol:	tcp - 12350			
Name:	Unidentified			
Sessions	Total Bytes	Inbound	Outbound	Time
43 %	1.94 MB %	1.84 MB	95.08 KB	27m 35s
<hr/>				
Protocol:	tcp - 55425			
Name:	Unidentified			
Sessions	Total Bytes	Inbound	Outbound	Time
1 %	1.89 MB %	1.85 MB	40.08 KB	5s
<hr/>				
35 listed: 324,271	12.84 GB	11.08 GB	1.76 GB	
Percent: 85.2%	98.2%	98.5%	96.6%	
Total: 380,751	13.07 GB	11.26 GB	1.82 GB	

Inbound Firewall Profile

This section profiles the systems and services accessed by external network clients over one week of monitoring. It reveals what inbound access the current security policy is permitting and should be used to verify and evaluate the effectiveness of the security policy and controls as implemented by firewall.

Things to consider:

- As a general rule, the number and kinds of systems exposed to the Internet should be kept to a bare minimum, as each one represents additional work for the IT department and additional opportunities for hackers to compromise the network.
- The merit of each exposed system should be carefully evaluated relative to the benefits offered vs. impact if compromised.
- Over time, virtually all security policies degrade due to changing business requirements, equipment configuration issues and day-to-day activities. Without verification of security policies through reviewing the network activity and use, many organizations become vulnerable to attack, exploitation and operation disruption.
- Network administrators should not be surprised to discover that exposed systems are frequently being scanned.

Note: All systems or accesses that aren't specifically part of normal operations, or seem to be unusual, should be thoroughly investigated by security personnel.

Summary:

- 2 IP addresses are hosting "active protocols".
- Hosted protocols were accessed by 187 external clients from 59 different networks.
- 4 IP addresses were scanned for services that did not reply. These "inactive protocols" may be an indication of holes in the firewall, down services or network scanning.
- Access attempts on inactive protocols were made by 5 external clients from 5 different networks.

Threat Inspector's Host' Services detail represents a very comprehensive Firewall Penetration Test, providing qualitative information to assess the validity of external user activity

Active Protocols

The inbound active protocol table lists internal hosts and protocols that were contacted by external clients. Only servers that replied or had outbound traffic are listed here.

Note: TCP protocols that have failed sessions did not establish a valid connection with external clients but have leaked information about a service's existence to the client. A moderate amount of this is to be expected and is the signature of external clients scanning the network and firewall permissions.

Fields:

- **Host** - IP address of internal host communicating with clients from external networks.
- **Protocol** -Port number, IANA assigned protocol name or Threat Inspector assigned name when the protocol has been positively identified. Note: Just because traffic is flowing on an IANA assigned protocol does not mean that it's what it says.
- **Sessions (Est / Fail)** -Established sessions represent valid TCP or continuous UDP conversations. Failed sessions only apply to TCP protocols and represent failed attempts to establish a valid TCP session.
- **Clients/Nets** -Clients are the number of unique external IP addresses accessing this service. Nets are the number of unique networks that the IP addresses originated from. Networks are grouped based on defined classes A, B, and C.
- **Bytes (Total, Inbound, Outbound)** -Total number of data bytes exchanged between a host and its clients broken out by inbound, outbound and total amounts.

Active Servers and Protocols

Host Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients/Nets		Inbound	Outbound
192.168.10.6					
tcp - 25 EMAIL	2633 / 0	28 / 20	644.73 MB	626.81 MB	17.92 MB
tcp - 80 HTTP	5242 / 0	118 / 17	146.21 MB	24.96 MB	121.25 MB
tcp - 80 http	2939 / 0	28 / 18	113.94 MB	11.63 MB	102.31 MB
tcp - 3389 ms-wbt-server	32 / 0	6 / 6	8.27 MB	1.51 MB	6.76 MB
tcp - 80 EMAIL	17 / 0	4 / 2	5.51 MB	246.35 KB	5.27 MB
tcp - 1723 pptp	32 / 0	8 / 5	1.28 MB	822.25 KB	488.80 KB
tcp - 110 pop3	624 / 0	8 / 3	283.62 KB	155.74 KB	127.89 KB
tcp - 25 smtp	228 / 0	19 / 17	196.58 KB	86.09 KB	110.49 KB
Protocols: 8	11747 / 0		920.41 MB	666.19 MB	254.22 MB
192.168.10.101					
udp - 1068 instl_bootc	1 / x	1 / 1	3.11 KB	1.34 KB	1.77 KB

Host	Sessions		Bytes		
Protocol	Est/Fail	Clients/Nets	*Total	Inbound	Outbound
udp - 1476 clvm-cfg	1 / x	1 / 1	429.00 B	248.00 B	181.00 B
Protocols: 2	2 / 0		3.53 KB	1.58 KB	1.94 KB
Hosts: 2	11749 / 0	187 / 59	920.41 MB	666.19 MB	254.22 MB

Inactive Protocols

The inactive protocol table lists hosts and protocols that were contacted by external clients but did not respond to requests. In other words requests were made but the service did not answer. Protocols listed in this table may be an indication of a down or malfunctioning server or a hole in the firewall rule set left open by the decommissioning of an old service.

Note: If the audit was performed outside of the firewall, this table can be very large and mostly represents the traffic that failed to penetrate the firewall.

Fields:

- **Host** - IP address of internal host communicating with clients from external networks.
- **Protocol** -Port number, IANA assigned protocol name or Threat Inspector assigned name when the protocol has been positively identified. Note: Just because traffic is flowing on an IANA assigned protocol does not mean that it's what it says.
- **Sessions (Est / Fail)** -Established sessions represent valid TCP or continuous UDP conversations. Failed sessions only apply to TCP protocols and represent failed attempts to establish a valid TCP session.
- **Clients/Nets** -Clients are the number of unique external IP addresses accessing this service. Nets are the number of unique networks that the IP addresses originated from. Networks are grouped based on defined classes A, B, and C.
- **Bytes (Total, Inbound, Outbound)** -Total number of data bytes exchanged between a host and its clients broken out by inbound, outbound and total amounts.

Inactive Servers and Protocols

Host Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients/Nets		Inbound	Outbound
192.168.10.108					
udp - 2952 mpfwsas	1 / x	1 / 1	586.00 B	586.00 B	0.00 B
udp - 54842	1 / x	1 / 1	586.00 B	586.00 B	0.00 B
udp - 46352	1 / x	1 / 1	293.00 B	293.00 B	0.00 B
udp - 40374	1 / x	1 / 1	106.00 B	106.00 B	0.00 B
Protocols: 4	4 / 0		1.53 KB	1.53 KB	0 B
192.168.10.101					
udp - 1476 clvm-cfg	1 / x	1 / 1	124.00 B	124.00 B	0.00 B
192.168.10.106					
udp - 12475	1 / x	1 / 1	117.00 B	117.00 B	0.00 B

Host Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients/Nets		Inbound	Outbound
udp - 15554	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 17206	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 21627	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 22705	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 23147	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 25202	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 34279	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 37789	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 39526	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 47078	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 47120	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 56427	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 57170	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 58915	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 62331	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
udp - 65087	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
Protocols: 17	17 / 0		1.94 KB	1.94 KB	0 B
192.168.10.123					
udp - 53161	1 / x	1 / 1	117.00 B	117.00 B	0.00 B
Hosts: 4	23 / 0	5 / 5	3.71 KB	3.71 KB	0 B

TCP/IP Access

This section lists the top external clients that accessed the network using TCP/IP protocols.

Top External TCP Networks

External Networks	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
91.0.0.0	2	0	427.45 MB	414.59 MB	12.86 MB
218.65.144.0 - US	1684	0	354.78 MB	344.77 MB	10.01 MB
218.65.145.0 - US	1107	0	289.81 MB	281.85 MB	7.95 MB
83.0.0.0	4	0	277.13 MB	269.53 MB	7.60 MB
226.9.248.0 - CA	3666	0	204.75 MB	14.98 MB	189.77 MB
68.0.0.0	312	0	15.16 MB	10.00 MB	5.16 MB
99.0.0.0	602	0	15.15 MB	3.10 MB	12.04 MB
218.54.14.0 - US	3074	0	7.33 MB	4.58 MB	2.76 MB
98.0.0.0	14	0	7.29 MB	1.01 MB	6.27 MB
64.0.0.0					MB
219.146.1					MB
15.0.0.0					KB
70.0.0.0					MB
69.0.0.0					MB
219.169.105.0 - US	11	0	2.24 MB	555.78 KB	1.91 MB
66.0.0.0	25	0	1.49 MB	221.07 KB	1.27 MB
218.54.15.0 - US	9	0	1.23 MB	214.54 KB	1.02 MB
24.0.0.0	17	0	1.06 MB	281.88 KB	808.44 KB
67.0.0.0	8	0	636.73 KB	612.53 KB	24.21 KB
75.0.0.0 - US	7	0	574.59 KB	361.09 KB	213.49 KB
226.9.249.0 - CA	74	0	446.71 KB	240.91 KB	205.80 KB
74.0.0.0 - US	16	0	216.29 KB	135.14 KB	81.15 KB
226.34.91.0 - US	393	0	178.61 KB	98.01 KB	80.60 KB
218.65.148.0 - US	10	0	30.83 KB	16.48 KB	14.35 KB
71.0.0.0 - US	1	0	28.26 KB	17.84 KB	10.42 KB
169.9.0.0 - US	20	0	22.53 KB	7.18 KB	15.35 KB
85.0.0.0	7	0	14.15 KB	9.35 KB	4.80 KB
89.0.0.0	4	0	13.77 KB	9.81 KB	3.96 KB
41.0.0.0	2	0	6.77 KB	4.78 KB	1.99 KB
84.0.0.0	3	0	6.60 KB	4.47 KB	2.13 KB
Sub Totals: 30	11,694		1.59 GB	1.32 GB	274.73 MB
Percent: 51%	100%	NaN	100%	100%	100%
Totals: 59	11,731		1.59 GB	1.32 GB	274.75 MB

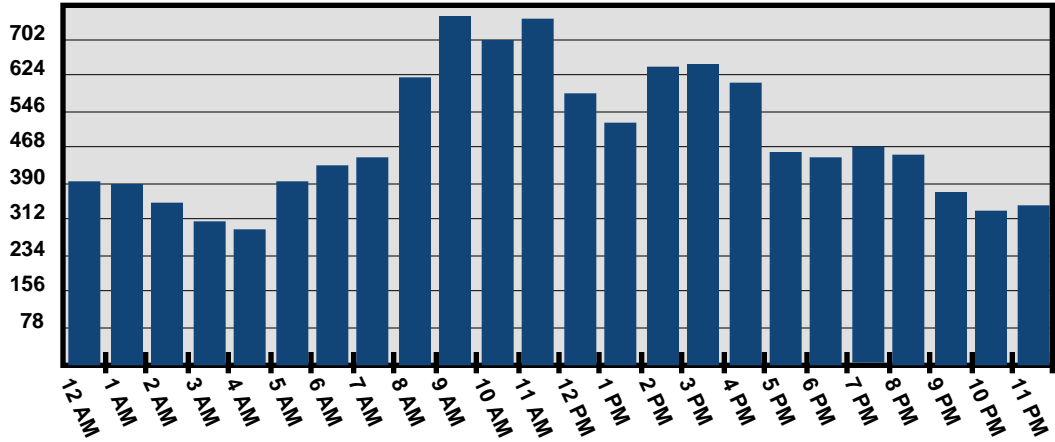
Users can evaluate the usage behavior of external clients, first determining if they are legitimate users based on identifying the two letter Country Code identification and the network address. If unfriendly, users can narrow or specify allowable IP range for external clients. Can see how much activity and when they were active.

Top External TCP Clients

External Clients	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
92.121.98.54 - FR	2	0	427.45 MB	414.59 MB	12.86 MB
218.65.144.247 - US	1687	0	354.90 MB	344.88 MB	10.02 MB
218.65.145.247 - US	1110	0	289.88 MB	281.93 MB	7.96 MB
85.216.195.154 - AT	1	0	277.12 MB	269.52 MB	7.60 MB
226.9.248.162 - CA	1794	0	116.62 MB	7.80 MB	108.82 MB
226.9.248.137 - CA	717	0	59.15 MB	3.64 MB	55.51 MB
226.9.248.161 - CA	396	0	21.48 MB	1.66 MB	19.82 MB
69.167.173.2 - US	311	0	15.16 MB	10.00 MB	5.16 MB
94.227.4.247 - CA	602	0	15.15 MB	3.10 MB	12.04 MB
226.9.248.208 - CA	765	0	7.56 MB	1.89 MB	5.67 MB
99.194.95.106 -	3	0	7.07 MB	986.52 KB	6.10 MB
219.146.168.34 - CA	64	0	5.25 MB	868.70 KB	4.40 MB
16.201.49.21 - US	1	0	5.13 MB	4.99 MB	143.50 KB
71.237.26.98 - US	95	0	4.54 MB	646.21 KB	3.91 MB
65.174.147.34 - US	76	0	3.31 MB	910.43 KB	2.42 MB
65.91.165.57 - US	102	0	2.46 MB	558.97 KB	1.91 MB
219.169.103.178 - US	11	0	2.24 MB	335.78 KB	1.91 MB
67.93.76.62 - US	25	0	1.49 MB	221.07 KB	1.27 MB
66.181.68.217 - US	17	0	1.38 MB	206.16 KB	1.18 MB
64.121.34.103 - US	26	0	1.20 MB	557.55 KB	675.31 KB
218.54.15.107 - US	7	0	846.44 KB	185.32 KB	661.12 KB
218.54.14.6 - US	455	0	732.45 KB	525.07 KB	207.38 KB
24.4.8.124 - US	7	0	731.10 KB	208.16 KB	522.94 KB
63.133.239.49 - US	2	0	626.37 KB	607.92 KB	18.46 KB
218.54.14.88 - US	223	0	519.03 KB	339.59 KB	179.44 KB
218.54.15.110 - US	2	0	414.19 KB	29.22 KB	384.98 KB
218.54.14.75 - US	124	0	394.14 KB	229.00 KB	165.13 KB
71.172.112.200 -	6	0	390.54 KB	244.54 KB	145.99 KB
25.65.83.233 - CA	5	0	351.82 KB	69.89 KB	281.93 KB
218.54.14.126 - US	120	0	349.09 KB	205.91 KB	143.18 KB
218.54.14.16 - US	168	0	311.19 KB	215.28 KB	95.91 KB
218.54.14.80 - US	189	0	302.43 KB	220.41 KB	82.02 KB
218.54.14.27 - US	91	0	293.86 KB	166.73 KB	127.13 KB
218.54.14.68 - US	90	0	254.98 KB	155.44 KB	99.53 KB
218.54.14.104 - US	64	0	253.41 KB	130.44 KB	122.97 KB
Sub-total: 35	9,358		1.59 GB	1.32 GB	272.52 MB
Percent: 19%	80%	NaN	100%	100%	99%
Totals: 189	11,753		1.59 GB	1.32 GB	274.83 MB

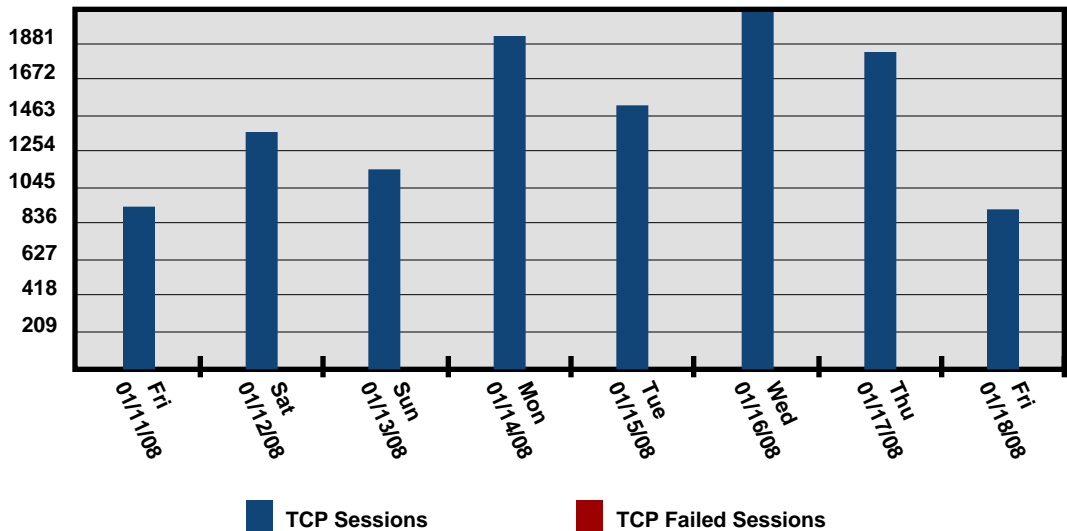
The following graphs show the number of Inbound TCP/IP Sessions for each hour and day of the audit. Sessions marked in red failed to establish a connection and may represent network scanning.

Inbound TCP/IP Sessions by Hour



Users can access the level of external client activity using the report graphs [here](#), or can drill into the interactive report interface to examine specific usage patterns for individual client and host devices.

Inbound TCP/IP Sessions by Date



UDP/IP Access

This section lists the top external clients that accessed the network using UDP/IP protocols.

Top External UDP Networks

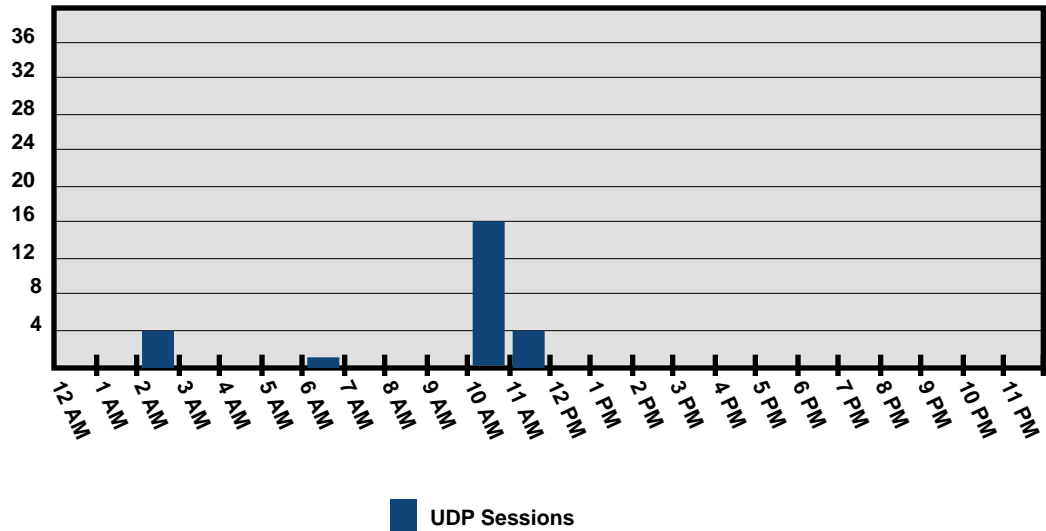
External Networks	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
226.246.66.0 - US	2	n/a	3.23 KB	1.46 KB	1.77 KB
77.0.0.0 - US	16	n/a	1.83 KB	1.83 KB	0.00 B
223.119.154.0 - BE	4	n/a	1.53 KB	1.53 KB	0.00 B
223.200.111.0 - EU	1	n/a	429.00 B	248.00 B	181.00 B
65.0.0.0	1	n/a	117.00 B	117.00 B	0.00 B
201.30.217.0 - AU	1	n/a	117.00 B	117.00 B	0.00 B
Totals: 6	25		7.24 KB	5.3 KB	1.94 KB

Top External UDP Clients

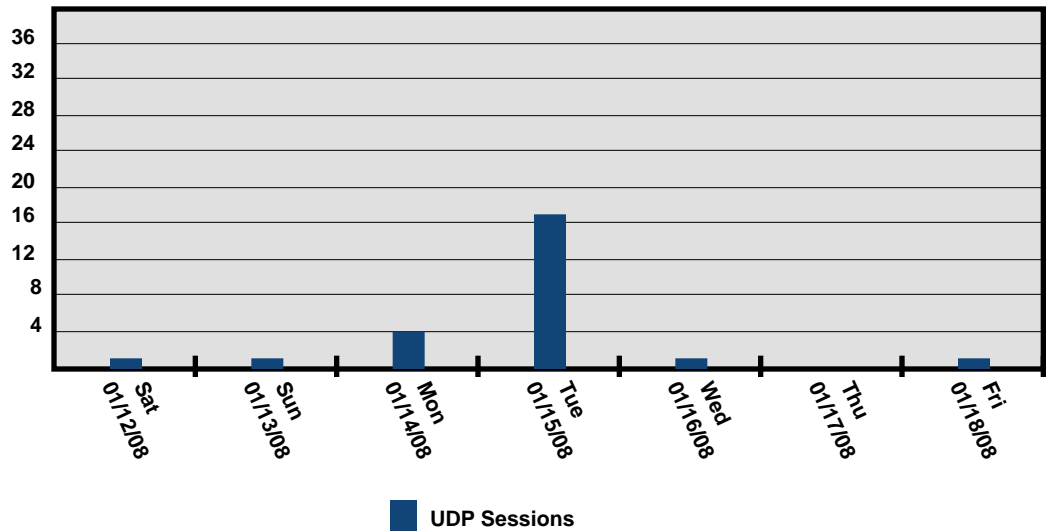
External Clients	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
226.246.66.159 - US	1	n/a	3.11 KB	1.34 KB	1.77 KB
77.64.59.61 - CA	16	n/a	1.83 KB	1.83 KB	0.00 B
223.119.154.173 - BE	4	n/a	1.53 KB	1.53 KB	0.00 B
223.200.111.115 - EU	1	n/a	429.00 B	248.00 B	181.00 B
226.246.66.151 - US	1	n/a	124.00 B	124.00 B	0.00 B
65.178.205.253 - AT	1	n/a	117.00 B	117.00 B	0.00 B
201.30.217.225 - AU	1	n/a	117.00 B	117.00 B	0.00 B
Totals: 7	25		7.24 KB	5.3 KB	1.94 KB

The following graphs show the number of Inbound UDP/IP conversations for each hour and day of the audit.

Inbound UDP/IP Sessions by Hour



Inbound UDP/IP Sessions by Date



Outbound Firewall Profile

This section profiles the protocols in use by internal clients over one week of monitoring. It reveals what outbound access the current security policy is permitting and should be used to verify and evaluate the effectiveness of the security policy as implemented by firewalling equipment.

Things to consider:

- Securing the organization from the outside is not enough any more. Network security threats exist both outside and within the network.
- Non-essential outbound ports should be blocked by the firewall. Malware, Peer-to-Peer applications and Viruses often take advantage of unrestricted outbound network access.

Note: Applications don't always map to assigned ports and, where possible, the audit identifies the actual type of network use. Some ports may be listed multiple times due to different applications running on the same network port. For example, AOL's chat program often masquerades on ports belonging to other applications in order to bypass firewall settings.

Summary:

- 66 internal clients made 348,076 requests to 20226 external servers transferring over 10.93 GB s of data.
- Outbound requests were over 5520 active TCP and UDP ports.
- A large number (5520) of active outbound TCP and UDP ports is often an indication of P2P, VOIP, Games, or compromised systems and should be investigated.

Monitoring and defending the network from inside is just as important as defending from threats on the outside. Many exploits and threats can be initiated through misuse, errors or misconfigurations by an internal user accessing an external service or through creating communication vector through which confidential information can be moved outside the network.

Active Protocols

The outbound active protocol table lists protocols that have two-way communication with servers outside the network.

Fields:

- **Protocol** -Port number, IANA assigned protocol name or Threat Inspector assigned name when the protocol has been positively identified. Note: Just because traffic is flowing on an IANA assigned protocol does not mean that it's what it says.
- **Sessions (Est / Fail)** -Established sessions represent valid TCP or continuous UDP conversations. Failed sessions only apply to TCP protocols and represent failed attempts to establish a valid TCP session.
- **Clients** - The number of unique internal IP addresses using this protocol.
- **Bytes (Total, Inbound, Outbound)** -Total number of data bytes exchanged between a host and its clients broken out by inbound, outbound and total amounts.

Outbound Active Protocols

Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients		Inbound	Outbound
tcp-80 HTTP	229095/0	63	9.06 GB	8.37 GB	706.85 MB
tcp-443 SSLv3	54482/0	64	937.14 MB	712.07 MB	225.07 MB
tcp-25 EMAIL	2150/0	2	478.94 MB	14.63 MB	464.31 MB
tcp-1935 tincan	116/3	20	204.10 MB	197.88 MB	6.21 MB
tcp-443 https	5124/11	46	63.82 MB	54.99 MB	8.83 MB
tcp-2848 amt-blc-port	9/4	1	51.49 MB	50.42 MB	1.07 MB
udp-4500	426/x	4	42.79 MB	20.79 MB	22.00 MB
udp-53 DNS	7270/x	6	24.77 MB	19.88 MB	4.89 MB
tcp-80 http	10936/743	63	19.45 MB	17.05 MB	2.39 MB
tcp-1194	6/0	1	19.33 MB	12.90 MB	6.42 MB
tcp-46629 SSLv3	98/0	4	16.81 MB	15.64 MB	1.17 MB
tcp-554 RTSP	9/0	4	8.97 MB	8.70 MB	277.68 KB
udp-3478	341/x	9	3.41 MB	1.81 MB	1.60 MB
tcp-5050 YMSG	44/0	9	3.41 MB	1.73 MB	1.68 MB
tcp-88 HTTP	1/0	1	2.74 MB	2.64 MB	101.44 KB
tcp-1863 MSN	65/0	8	2.31 MB	1013.18 KB	1.32 MB
tcp-21 FTP	19/0	4	2.28 MB	1.45 MB	851.77 KB
tcp-12350	42/0	7	1.94 MB	1.84 MB	95.02 KB
udp-500 isakmp	569/x	4	1.33 MB	504.26 KB	861.61 KB
udp-56781	4/x	1	593.21 KB	263.90 KB	329.31 KB
tcp-8080 HTTP	9/0	5	495.89 KB	461.68 KB	34.21 KB
tcp-3101 hp-pxpib	1/0	1	447.51 KB	190.13 KB	257.38 KB
tcp-6936	1/0	1	437.08 KB	155.21 KB	281.88 KB
tcp-5190 AOL	25/0	1	411.94 KB	257.05 KB	154.89 KB
tcp-41833	1/0	1	390.95 KB	75.82 KB	315.13 KB

Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients		Inbound	Outbound
tcp-6660	8/0	1	382.05 KB	204.27 KB	177.78 KB
tcp-27225	1/0	1	360.84 KB	113.64 KB	247.20 KB
udp-11979	398/x	6	285.31 KB	225.23 KB	60.07 KB
udp-23460	232/x	5	267.07 KB	131.98 KB	135.09 KB
udp-57587	45/x	3	263.66 KB	85.73 KB	177.92 KB
tcp-110 EMAIL	9/0	1	257.49 KB	245.51 KB	11.99 KB
tcp-2156	1/0	1	256.80 KB	85.17 KB	171.63 KB
tcp-46629	14/0	4	255.15 KB	222.63 KB	32.52 KB
tcp-24231	1/0	1	253.78 KB	82.18 KB	171.61 KB
udp-11113	6/x	1	239.48 KB	143.41 KB	96.07 KB
tcp-42589	1/0	1	236.42 KB	83.03 KB	153.39 KB
tcp-34335	1/0	1	226.63 KB	68.95 KB	157.68 KB
tcp-11979	3/0	2	217.32 KB	92.36 KB	124.96 KB
tcp-8080 SSLv3	10/0	1	214.93 KB	154.41 KB	60.53 KB
tcp-4011 altserviceboot	1/0	1	210.59 KB	73.25 KB	137.34 KB
tcp-1675 pdp	1/0	1	208.43 KB	54.89 KB	153.54 KB
tcp-14917	1/0	1	199.70 KB	74.97 KB	124.73 KB
tcp-12351	1/0	1	195.97 KB	186.45 KB	9.52 KB
udp-64214	85/x	3	192.09 KB	43.60 KB	148.49 KB
tcp-41942	1/0	1	187.87 KB	103.84 KB	84.04 KB
udp-123 ntp	953/x	6	177.89 KB	88.77 KB	89.12 KB
udp-9814	52/x	4	169.40 KB	43.06 KB	126.34 KB
tcp-50011	1/0	1	167.77 KB	65.59 KB	102.18 KB
tcp-58369	1/0	1	162.55 KB	65.47 KB	97.09 KB
tcp-5658	2/0	1	159.84 KB	38.92 KB	120.92 KB
tcp-455 creativepartnr	1/0	1	158.08 KB	127.96 KB	30.12 KB
tcp-9000 HTTP	74/0	5	156.73 KB	45.03 KB	111.70 KB
udp-10105	265/x	5	151.17 KB	126.02 KB	25.15 KB
udp-18133	169/x	3	149.45 KB	45.53 KB	103.92 KB
udp-5750	3/x	1	146.34 KB	121.99 KB	24.35 KB
tcp-10612	1/0	1	144.21 KB	62.82 KB	81.39 KB
tcp-52398	2/0	1	141.87 KB	36.30 KB	105.57 KB
udp-19525	5/x	2	141.00 KB	91.35 KB	49.65 KB
tcp-32390	2/0	2	133.89 KB	52.89 KB	81.00 KB
udp-44907	18/x	3	133.20 KB	38.21 KB	94.99 KB
Sub Totals: 60	313,212/761		10.91 GB	9.48 GB	1.43 GB
Percent: 1%	90% / 72%		100%	100%	99%
Protocols: 5520	348,076 /1,056	66	10.93 GB	9.49 GB	1.44 GB

Inactive Protocols

The outbound inactive protocol table lists protocols that have outbound requests but no replies. A protocol may be listed here if the requested server or protocol is unavailable. A moderate amount of this is to be expected. Pay attention to large numbers of failed sessions on a single port or over a large number of ports, this may be an indication of compromised internal clients. Clients may be running a network scan, a DOS attack, or in the case of a "bot" trying to phone home for further instructions.

Fields:

- **Protocol** -Port number, IANA assigned protocol name or Threat Inspector assigned name when the protocol has been positively identified. Note: Just because traffic is flowing on an IANA assigned protocol does not mean that it's what it says.
- **Sessions (Est / Fail)** -Established sessions represent valid TCP or continuous UDP conversations. Failed sessions only apply to TCP protocols and represent failed attempts to establish a valid TCP session.
- **Clients** - The number of unique internal IP addresses using this protocol.
- **Bytes (Total, Inbound, Outbound)** -Total number of data bytes exchanged between a host and its clients broken out by inbound, outbound and total amounts.

Outbound Inactive Protocols

Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients		Inbound	Outbound
udp-1900 sstp	688/x	23	3.61 MB	0.00 B	3.61 MB
udp-9814	416/x	4	632.22 KB	0.00 B	632.22 KB
tcp-2967 ssc-agent	1640/1640	4	297.77 KB	0.00 B	297.77 KB
udp-64214	158/x	3	293.24 KB	0.00 B	293.24 KB
tcp-80 http	1771/1771	44	260.44 KB	0.00 B	260.44 KB
udp-59565	15/x	2	251.28 KB	0.00 B	251.28 KB
udp-61739	7/x	2	196.11 KB	0.00 B	196.11 KB
tcp-135 epmap	1043/1043	1	189.45 KB	0.00 B	189.45 KB
udp-28851	17/x	2	171.46 KB	0.00 B	171.46 KB
udp-16115	10/x	3	156.76 KB	0.00 B	156.76 KB
udp-3702	22/x	2	146.30 KB	0.00 B	146.30 KB
udp-30017	45/x	2	126.87 KB	0.00 B	126.87 KB
tcp-445 microsoft-ds	669/669	5	121.17 KB	0.00 B	121.17 KB
udp-34884	11/x	2	114.68 KB	0.00 B	114.68 KB
tcp-139 netbios-ssn	612/612	1	111.16 KB	0.00 B	111.16 KB
tcp-110 pop3	544/544	1	98.81 KB	0.00 B	98.81 KB
udp-49807	4/x	1	94.73 KB	0.00 B	94.73 KB
udp-4371	3/x	1	94.48 KB	0.00 B	94.48 KB
udp-9673	68/x	4	93.02 KB	0.00 B	93.02 KB
udp-21296	5/x	1	84.59 KB	0.00 B	84.59 KB

Protocol	Sessions		*Total	Bytes	
	Est/Fail	Clients		Inbound	Outbound
udp-52522	18/x	4	83.14 KB	0.00 B	83.14 KB
udp-18115	36/x	1	79.35 KB	0.00 B	79.35 KB
udp-40220	24/x	1	69.24 KB	0.00 B	69.24 KB
udp-52777	21/x	2	68.57 KB	0.00 B	68.57 KB
udp-28239	46/x	2	63.76 KB	0.00 B	63.76 KB
udp-3649	50/x	3	60.68 KB	0.00 B	60.68 KB
udp-20275	2/x	1	53.26 KB	0.00 B	53.26 KB
udp-25909	1/x	1	50.37 KB	0.00 B	50.37 KB
udp-29687	2/x	1	49.15 KB	0.00 B	49.15 KB
udp-5968 mppolicy-v5	3/x	1	48.74 KB	0.00 B	48.74 KB
udp-36595	5/x	2	43.67 KB	0.00 B	43.67 KB
udp-20166	35/x	1	41.03 KB	0.00 B	41.03 KB
udp-59362	4/x	1	36.71 KB	0.00 B	36.71 KB
udp-30369	2/x	3	33.19 KB	0.00 B	33.19 KB
udp-32018	2/x	2	31.23 KB	0.00 B	31.23 KB
udp-31866	2/x	1	30.01 KB	0.00 B	30.01 KB
udp-23609	3/x	1	28.57 KB	0.00 B	28.57 KB
udp-6278	1/x	1	25.59 KB	0.00 B	25.59 KB
udp-5355	183/x	2	23.81 KB	0.00 B	23.81 KB
udp-13078	19/x	1	22.81 KB	0.00 B	22.81 KB
udp-1504 evb-elm	41/x	1	21.91 KB	0.00 B	21.91 KB
udp-500 isakmp	4/x	2	21.76 KB	0.00 B	21.76 KB
udp-5353 iTunes	10/x	3	21.29 KB	0.00 B	21.29 KB
udp-52398	2/x	2	20.33 KB	0.00 B	20.33 KB
udp-4254	4/x	1	19.95 KB	0.00 B	19.95 KB
udp-8245	1/x	1	18.70 KB	0.00 B	18.70 KB
udp-33938	25/x	2	18.19 KB	0.00 B	18.19 KB
udp-123 ntp	140/x	13	17.23 KB	0.00 B	17.23 KB
udp-33311	40/x	2	16.53 KB	0.00 B	16.53 KB
udp-57854	2/x	1	16.49 KB	0.00 B	16.49 KB
udp-48557	11/x	2	15.69 KB	0.00 B	15.69 KB
udp-48328	65/x	1	14.47 KB	0.00 B	14.47 KB
udp-137 netbios-ns	43/x	4	14.29 KB	0.00 B	14.29 KB
udp-34163	64/x	1	14.25 KB	0.00 B	14.25 KB
udp-35671	64/x	1	14.25 KB	0.00 B	14.25 KB
udp-29271	20/x	1	14.00 KB	0.00 B	14.00 KB
tcp-25 smtp	73/73	1	13.26 KB	0.00 B	13.26 KB
udp-9753 rasadv	166/x	1	12.81 KB	0.00 B	12.81 KB
udp-28240	55/x	1	12.24 KB	0.00 B	12.24 KB
udp-27782	54/x	1	12.02 KB	0.00 B	12.02 KB
Sub Totals: 60	9,091/6,352		8.31 MB	0 B	8.31 MB
Percent: 6%	78% / 97%		92%	NaN	92%
Protocols: 960	11,720 /6,581	70	9.07 MB	0 B	9.07 MB

TCP/IP Access

This section lists the top internal clients that accessed the Internet using TCP/IP protocols.

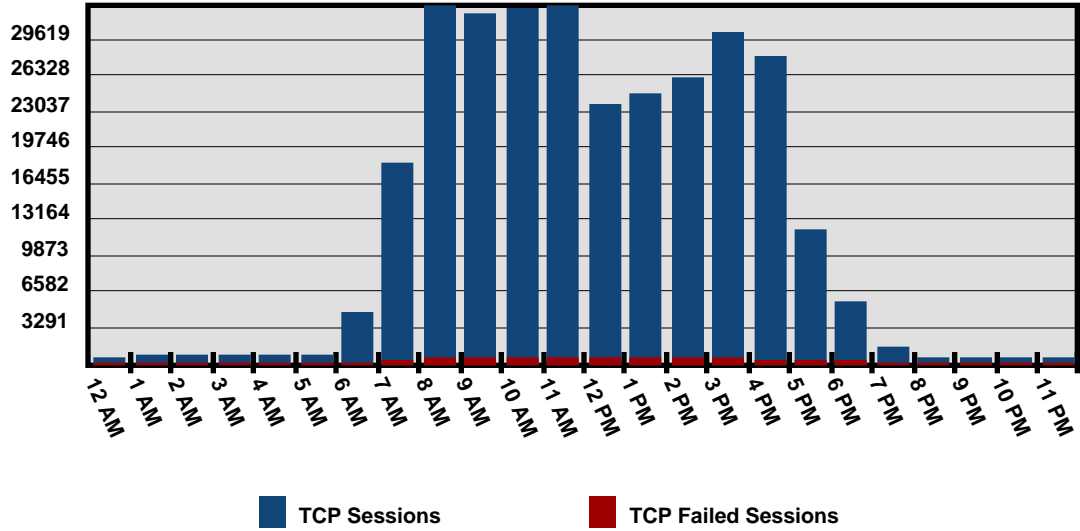
Top Internal TCP Clients

Internal Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.101	29166	76	2.78 GB	2.58 GB	208.51 MB
192.168.10.106	10613	76	1.25 GB	1.20 GB	51.98 MB
192.168.10.91	10702	28	1.06 GB	1.01 GB	50.58 MB
192.168.10.6	2885	332	561.40 MB	90.75 MB	470.65 MB
192.168.10.98	5467	11	478.39 MB	448.91 MB	29.48 MB
192.168.10.112	13538	27	445.01 MB	391.17 MB	53.84 MB
192.168.10.129	57900	557	428.41 MB	336.13 MB	92.28 MB
192.168.10.108	20317	2512	281.30 MB	233.79 MB	47.51 MB
192.168.10.7	1505	1358	219.74 MB	213.23 MB	6.52 MB
192.168.10.81	3071	14	218.27 MB	208.86 MB	9.41 MB
192.168.10.142	22720	175	217.08 MB	179.16 MB	37.92 MB
192.168.10.82	6897	34	215.21 MB	192.76 MB	22.45 MB
192.168.10.116	6291	6	209.50 MB	188.22 MB	21.28 MB
192.168.10.97	8309	6	192.68 MB	146.79 MB	45.89 MB
192.168.10.99	4022	31	191.25 MB	180.71 MB	10.54 MB
192.168.10.100	3845	17	186.88 MB	172.88 MB	14.00 MB
192.168.10.101	3845	17	186.88 MB	172.88 MB	14.00 MB
192.168.10.102	3845	17	186.88 MB	172.88 MB	14.00 MB
192.168.10.103	3845	17	186.88 MB	172.88 MB	14.00 MB
192.168.10.104	3845	17	186.88 MB	172.88 MB	14.00 MB
192.168.10.140	3737	12	139.97 MB	119.36 MB	20.61 MB
192.168.10.95	3952	28	135.70 MB	123.28 MB	12.42 MB
192.168.10.103	9230	76	123.81 MB	107.65 MB	16.16 MB
192.168.10.141	8330	1	110.91 MB	96.60 MB	14.31 MB
192.168.10.123	4454	2	83.29 MB	70.49 MB	12.80 MB
192.168.10.119	2774	7	76.86 MB	67.26 MB	9.60 MB
192.168.10.93	922	1	72.47 MB	68.68 MB	3.79 MB
192.168.10.127	1381	1	70.92 MB	65.83 MB	5.09 MB
192.168.10.120	2762	30	65.21 MB	59.08 MB	6.13 MB
Sub Totals: 30	272,658	5,520	10.45 GB	9.09 GB	1.36 GB
Percent: 43%	87%	72%	92%	92%	90%
Totals: 69	313,982	7,637	11.38 GB	9.88 GB	1.5 GB

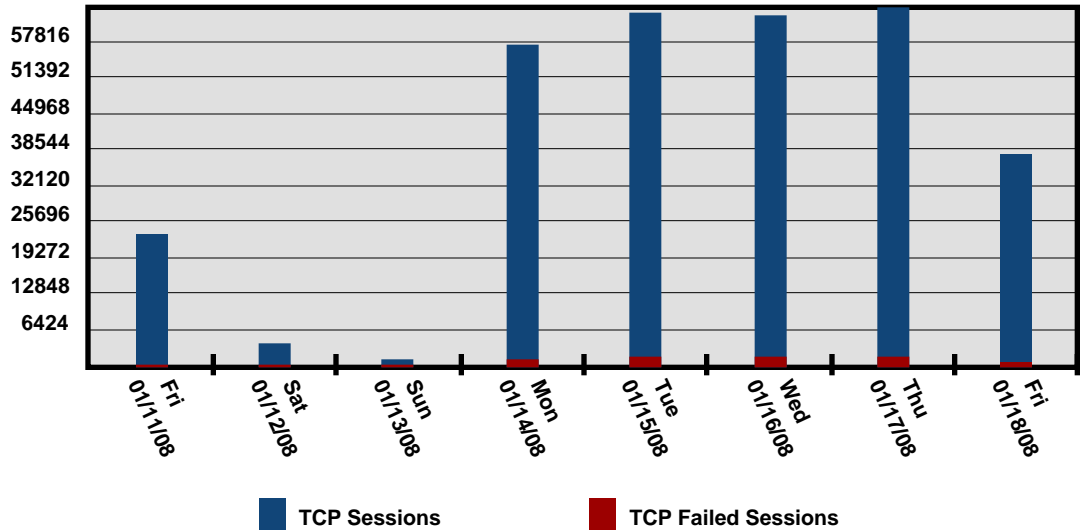
Where there is activity, and data moving in and out of the network, there is an increased threat. All usage should be mapped to legitimate business purposes or acceptable entertainment as a basis for understanding and managing what's on the network. A keen familiarity breeds confidence, improved planning and budgeting and helps achieve company goals with minimal risks.

The following graphs show the number of Outbound TCP/IP Sessions for each hour and day of the audit. Sessions marked in red failed to establish a connection and may represent network scanning.

Outbound TCP/IP Sessions by Hour



Outbound TCP/IP Sessions by Date



UDP/IP Access

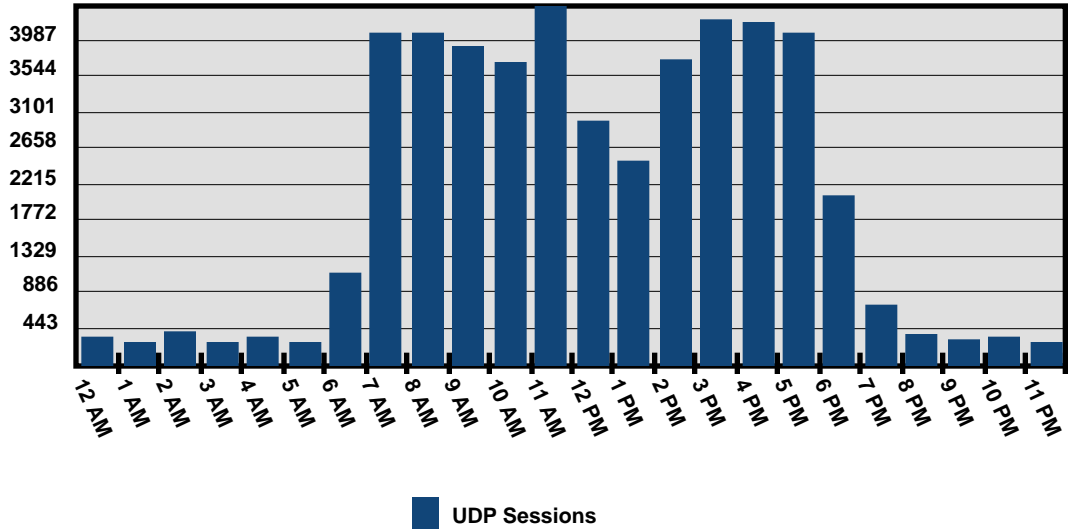
This section lists the top internal clients that accessed the Internet using UDP/IP protocols.

Top Internal UDP Clients

Internal Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.128	745	n/a	25.23 MB	12.10 MB	13.14 MB
192.168.10.129	14005	n/a	25.18 MB	11.85 MB	13.34 MB
192.168.10.7	3462	n/a	21.47 MB	17.26 MB	4.21 MB
192.168.10.145	12474	n/a	9.79 MB	4.79 MB	5.00 MB
192.168.10.101	349	n/a	3.43 MB	1.81 MB	1.63 MB
192.168.10.6	4554	n/a	3.41 MB	2.67 MB	761.50 KB
192.168.10.117	433	n/a	2.84 MB	806.00 B	2.84 MB
192.168.10.139	3784	n/a	2.46 MB	1.17 MB	1.29 MB
192.168.10.106	2780	n/a	2.22 MB	1.27 MB	972.33 KB
192.168.10.108	2835	n/a	1.59 MB	709.20 KB	919.73 KB
192.168.10.124	23	n/a	1.54 MB	777.89 KB	799.66 KB
192.168.10.142	1789	n/a	1.38 MB	390.71 KB	1.00 MB
192.168.10.123	1503	n/a	698.63 KB	450.90 KB	247.73 KB
192.168.10.135	20	n/a	682.94 KB	230.81 KB	452.13 KB
192.168.10.98	58	n/a	480.54 KB	2.45 KB	478.09 KB
192.168.10.80	203	n/a	139.92 KB	43.02 KB	96.91 KB
192.168.10.5	28	n/a	15.47 KB	7.73 KB	7.73 KB
192.168.10.22	2	n/a	12.41 KB	0.00 B	12.41 KB
192.168.10.140	18	n/a	11.99 KB	1.60 KB	10.39 KB
192.168.10.83	26	n/a	9.52 KB	0.00 B	9.52 KB
192.168.10.81	21	n/a	7.69 KB	0.00 B	7.69 KB
192.168.10.94	11	n/a	7.21 KB	1008.00 B	6.22 KB
192.168.10.95	11	n/a	6.69 KB	756.00 B	5.95 KB
192.168.10.85	20	n/a	5.71 KB	1.84 KB	3.87 KB
192.168.10.109	5	n/a	5.49 KB	0.00 B	5.49 KB
192.168.10.91	7	n/a	4.46 KB	504.00 B	3.96 KB
192.168.10.116	8	n/a	4.10 KB	0.00 B	4.10 KB
192.168.10.131	20	n/a	3.81 KB	0.00 B	3.81 KB
192.168.10.127	8	n/a	3.76 KB	0.00 B	3.76 KB
192.168.10.122	7	n/a	3.59 KB	0.00 B	3.59 KB
Sub Totals: 30	49,209		102.6 MB	55.47 MB	47.13 MB
Percent: 60%	100%	NaN	100%	100%	100%
Totals: 50	49,274		102.62 MB	55.47 MB	47.15 MB

The following graphs show the number of Outbound UDP/IP conversations for each hour and day of the audit.

Outbound UDP/IP Sessions by Hour



Outbound UDP/IP Sessions by Date

