



ADVANTAGES:

- **24 x 7 Monitoring** – SAVVIS has the resources to react quickly to security problems any time day or night.
- **Comprehensive Choice of Options** –From virtual to dedicated firewall platforms, SAVVIS offers a tremendous range of value and performance options.
- **Ease of Implementation** – SAVVIS takes care of the complete solution, including hardware, installation, configuration, and ongoing management.
- **Expertise** – SAVVIS leverages the experience of a staff that has installed thousands of firewalls at customer sites around the world.

For more information about SAVVIS, visit www.savvis.net or call 1-800-463-8294.

MANAGED FIREWALL SERVICES

Managed Firewall Services

Firewalls have long been considered the primary defense against cyber intrusion, but today's cyber criminals are using vastly more sophisticated techniques to bypass firewall protection and compromise business systems. Keeping intruders out while enabling daily Internet operations requires a comprehensive set of security policies and constant monitoring to ensure your systems and data are protected. But the labor and financial investment required to implement this kind of firewall security can quickly drain IT resources, leaving no time or money to focus on day-to-day business processes, and potentially leaving network assets open to attack.

SAVVIS is a recognized leader in managed Internet and security services. We offer a broad portfolio of effective, industry-leading managed firewall services, from virtual to dedicated firewall platforms. With experience gained from installing and managing thousands of firewalls, SAVVIS provides proactive security services supported by certified security professionals stationed around the world to deliver operational protection every minute of every day.

SAVVIS provides this level of support cost-effectively at your site, at third-party sites, or in our own data centers. We will work with you to perform a security review of your firewall needs, your network and system topology, and security policies to develop and define your firewall security policy. We will then configure, install, and manage your firewall systems according to your requirements, provisioning your service on a range of platforms, including network-based and virtual firewalls, or on dedicated appliances such as Cisco® ASA and Check Point Firewall-1®.

SAVVIS provides monitoring, management, and maintenance, and access to your firewall logs, policies, and performance statistics for viewing 24 hours a day, 365 days a year via SAVVIS' secure Web portal¹. (For examples of the types of firewall reports that are provided on our SAVVISStation portal, please refer to the Appendix that follows this summary).

System Ownership Options

SAVVIS offers two options for firewall hardware provisioning and software licenses. SAVVIS' Managed Firewall Service is a complete solution that includes SAVVIS-provided hardware, software licenses, maintenance, monitoring, and management by our team of security experts. SAVVIS' Firewall Care Service provides the same monitoring and management benefits to customer-provided Check Point FireWall-1, Cisco PIX® or Cisco ASA hardware and software. Both service options include comprehensive firewall security services and can be implemented at a SAVVIS data center, your own facility, or at a third-party site.

Failover and High-Availability Firewall Solutions

To achieve consistent firewall availability, SAVVIS offers active/passive failover configurations with a hot standby, and active/active load-balanced firewall configurations. In the event of the failure of one firewall, dedicated secondary equipment detects the failure and begins operating. SAVVIS' Managed Firewall Service is available at locations around the world to support your global business needs, including the United States, the United Kingdom, Europe, and Asia, to support your global business needs.

¹ Available firewall reporting options may vary by service. Please contact your SAVVIS account executive for further details.

About SAVVIS

SAVVIS, Inc. (NASDAQ:SVVS) is a leader in providing and managing global IT infrastructure and end-to-end managed services that enable quick and strategic response to the demands and technology needs of business and government. SAVVIS combines virtualization technology, a global network and data centers with automated management and provisioning systems to provide a full suite of hosting, utility compute, network, security and professional services. These services give customers an ideal balance of support and control that enables them to focus their resources on their core business while SAVVIS ensures the quality of their IT infrastructure.

Appendix: SAVVISStation Firewall Reporting

Reporting for SAVVIS' Managed Firewall Services is currently available through our SAVVISStation Portal, which is a secure, Web-based reporting interface. To enhance your organization's overall security, access to the portal is available solely to individuals who have previously been identified as "security contacts" by your organization. Portal support is available to customers on a 24/7/365 basis via a phone call or an e-mail to the SAVVIS Support Center.

To provide you with some examples of the types of reports that are currently available on the portal, some demo screen-shots appear below. For a full explanation of SAVVISStation portal functionality (including server performance reporting, network performance reporting and billing invoice options), please contact your SAVVIS account executive.

Managed Security Services "Home" Screen

The screenshot shows the SAVVISStation Portal DEMO (SAVVISStation Demo) interface. The top navigation bar includes links for Home, My Services, My Reports, Security, My Invoice, My Orders, Support, Settings, News, Help, and About. The main content area is titled "Customer Summary Sheet for: ssdemo" and contains a table with the following data:

Customer Name	Device Name	Device Type	Location	Monitoring Status
Demo Account (198362)	demo-se2-fw1-1	Checkpoint NG	SE/SE2 - 1.28.05	ALIVE
	demo-dl1-plix-1	PIX 6 SSH-3DES	DL/DL1 - A117	ALIVE

Below the table, there is a "News Bulletins" section with the heading "Latest Security News (offsite links, open in new browser window):". The news items include:

- SecurityFocus Vulnerabilities
 - Vuln: PHP Prior to 5.2.2/4.4.7 Multiple Remote Buffer Overflow Vulnerabilities
 - Vuln: PHP FTP_Putcmd Function HTTP Response Splitting Vulnerability
 - Vuln: GNU Image Manipulation Program Multiple Integer Overflow Vulnerabilities
 - Vuln: GIMP PSD File Integer Overflow Vulnerability
- Bugtraq: Re: COSEINC Linux Advisory #2: IA32 System CallEmulation Vulnerability
- Bugtraq: Re: Confirmed: Windows Explorer bad PNG file preview integer overflow handling
- Bugtraq: Re: New Shell For Linux & Windows
- Bugtraq: [USN-520-1] fetchmail vulnerabilities
- More rss feeds from SecurityFocus

More security news...

This screen provides access to the various types of Managed Security reports that are available through the portal, including reports for SAVVIS' Firewall, Intrusion Detection and Integrity Monitoring Service (IMS) services. In this instance, summary information is displayed for a demo Check Point firewall device.

Firewall Device Logs

SAVVIS SAVVISStation Portal DEMO (SAVVISStation Demo) News | Help | About

2007-09-26 7:03:23 PM Home My Services My Reports Security My Invoices My Orders Support Settings

Firewalls | IDS Reports | demo-dl1-pix-1 Go

Device Home | Device Policy | Device Logs | Log Graphs | Log Reports | Device Stats

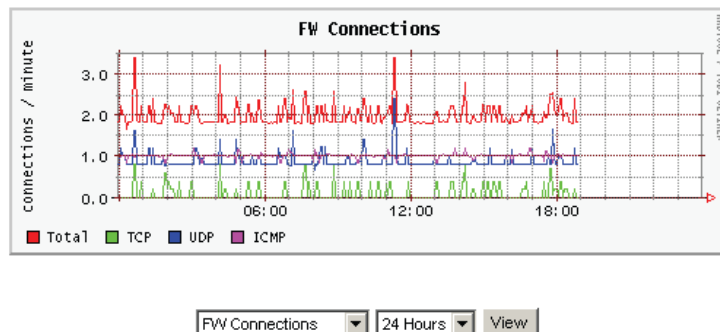
Device Logs: demo-dl1-pix-1

- Log file timestamps are in Greenwich Mean Time (GMT).
- Log files are rotated every six (6) hours.

Size (bytes)	Date	Filename
n/a	n/a	Last 100 Entries
n/a	n/a	Most Recent
3560	09/26/2007 18:13:10	216.39.79.24-200709261755-log.gz
3597	09/26/2007 12:26:11	216.39.79.24-200709261155-log.gz
3725	09/26/2007 06:20:50	216.39.79.24-200709260555-log.gz
3778	09/26/2007 00:07:56	216.39.79.24-200709252355-log.gz
3553	09/25/2007 18:09:45	216.39.79.24-200709251755-log.gz
3779	09/25/2007 12:28:25	216.39.79.24-200709251155-log.gz
3608	09/25/2007 06:15:51	216.39.79.24-200709250555-log.gz
3562	09/25/2007 00:07:49	216.39.79.24-200709242355-log.gz
3343	09/24/2007 18:09:10	216.39.79.24-200709241755-log.gz
3662	09/24/2007 12:28:15	216.39.79.24-200709241155-log.gz
3702	09/24/2007 06:12:20	216.39.79.24-200709240555-log.gz
3968	09/24/2007 00:09:04	216.39.79.24-200709232355-log.gz
3500	09/23/2007 19:11:50	216.39.79.24-200709231755-log.gz
3760	09/23/2007 12:19:21	216.39.79.24-200709231155-log.gz
3762	09/23/2007 06:18:13	216.39.79.24-200709230555-log.gz
3786	09/23/2007 00:06:21	216.39.79.24-200709222355-log.gz
3719	09/22/2007 18:12:34	216.39.79.24-200709221755-log.gz
3622	09/22/2007 12:21:13	216.39.79.24-200709221155-log.gz
3576	09/22/2007 06:17:02	216.39.79.24-200709220555-log.gz
3795	09/22/2007 00:06:12	216.39.79.24-200709212355-log.gz
3546	09/21/2007 18:17:45	216.39.79.24-200709211755-log.gz

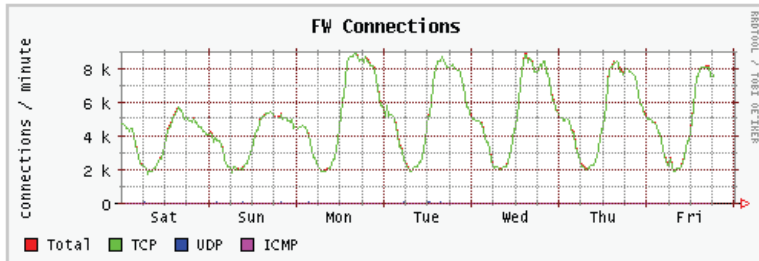
A detailed log of firewall activity is available for 30 days on a rotating basis, as it appears above. Logs are time-stamped for your convenience.

Firewall Connections (Daily View)



This screen summarizes Firewall Connections per Minute, by type (including TCP, UDP and ICMP connections). When analyzing this demo data, you should pay particular attention to the activity that occurred between 10.00 and 12.00, unless the spike in connections/minute was anticipated by normal business activity.

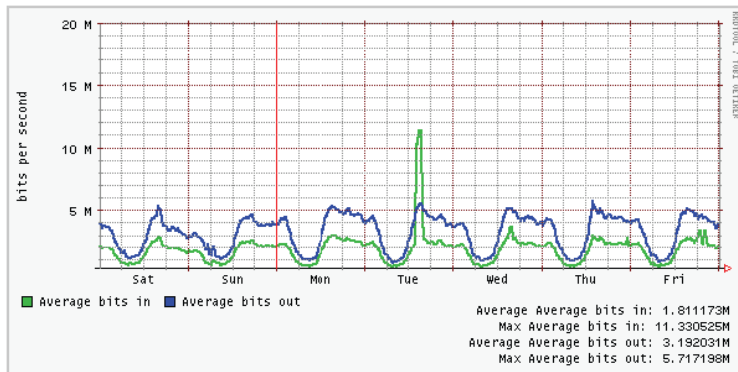
Firewall Connections (Weekly View)



FW Connections | 1 Week | View

Similar to the previous screen shot, this screen summarizes Firewall Connections per Minute, by type (including TCP, UDP and ICMP connections), but this time for a full week. The firewall connections show a consistent activity pattern throughout the course of the week.

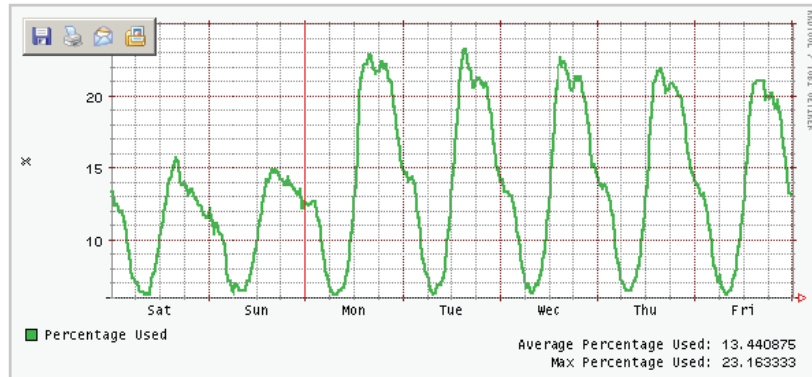
Weekly Reporting of “Average Bits In / Average Bits Out” Activity



Interface eth-s1p1 1 Octets Count | 1 Week | View

Here, we are presented with activity on a single firewall interface. If this graph represented your customer traffic activity you would pay special attention to the “Average Bits In” results for Tuesday morning.

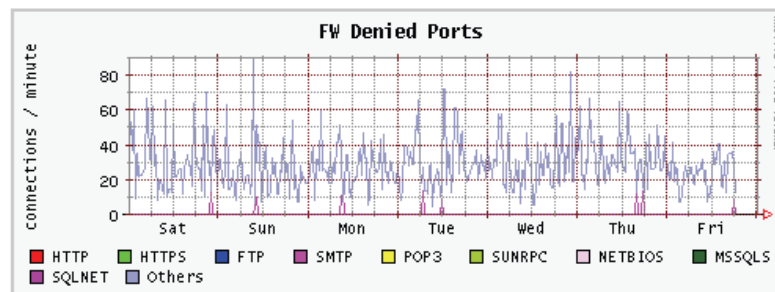
Firewall Device Statistics (Weekly CPU Utilization)



CPU Usage 1 Week View

This screen summarizes CPU usage over a weekly time period. If this represented your actual CPU usage, you would pay particular attention to the spikes in CPU utilization that occurred outside of traditional high-volume business hours.

Firewall Device Statistics (Denied Ports- Weekly View)



FW Denied Ports 1 Week View

This screen summarizes Denied Ports (by type), over a weekly time period. If this graph reflected actual customer activity, the activity that occurred on late Wednesday would have warranted your further investigation.

For additional information regarding SAVVIS' Managed Firewall Services or the SAVVISStation portal, please contact your SAVVIS account executive, who can provide you with additional information regarding a portal demonstration for your organization. In addition, Professional Services support is available if your organization requires assistance with firewall log review, or if you wish to investigate any unusual device activity in further detail.

For more information about SAVVIS, visit www.savvis.net or call 1-800-463-8294.