



MANAGED FIREWALL SERVICES

SECURITY 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.

CenturyLink Technology Solutions 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, CenturyLink provides proactive security services supported by certified security professionals stationed around the world to deliver operational protection every minute of every day.

CenturyLink 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 Unified Threat Management (UTM) from Check Point Software Technologies Ltd.

ADVANTAGES

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



CenturyLink®
Technology Solutions

CenturyLink provides monitoring, management, and maintenance, and access to your firewall logs, policies, and performance statistics for viewing 24/7 via CenturyLink’s secure Web portal¹. (For examples of the types of firewall reports that are provided on our Station Portal, please refer to the Appendix that follows this summary).

SYSTEM OWNERSHIP OPTIONS

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

FAILOVER AND HIGH-AVAILABILITY FIREWALL SOLUTIONS

To achieve consistent firewall availability, CenturyLink 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. 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.

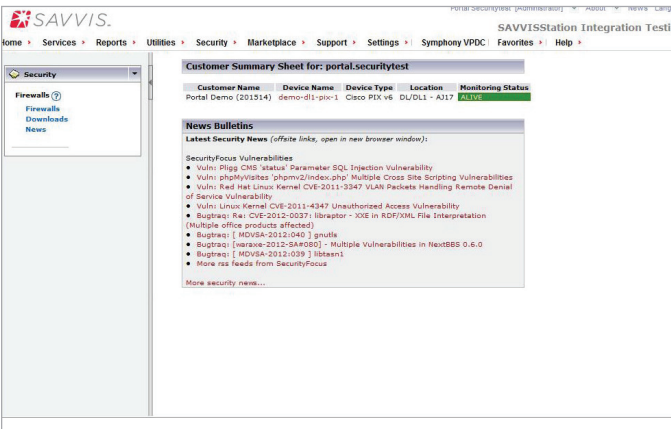
APPENDIX: CENTURYLINKSTATION FIREWALL REPORTING

Reporting for Managed Firewall Services is currently available through our Station 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 basis via a phone call or an e-mail to the 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 here. For a full explanation of CenturyLinkStation Portal functionality (including server performance reporting, network performance reporting and billing invoice options), please contact your CenturyLink Account Executive.

MANAGED SECURITY SERVICES “HOME” SCREEN

This screen provides access to the various types of Managed Security reports that are available through the portal, including reports for 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

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

SAVVIS. Portal SecurityTest [Administrator] About News Language

Home Services Reports Utilities Security Marketplace Support Settings Symphony VPOC SAVVISStation Integration Testin Favorites Help

Security

demo-d1-pix-1

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

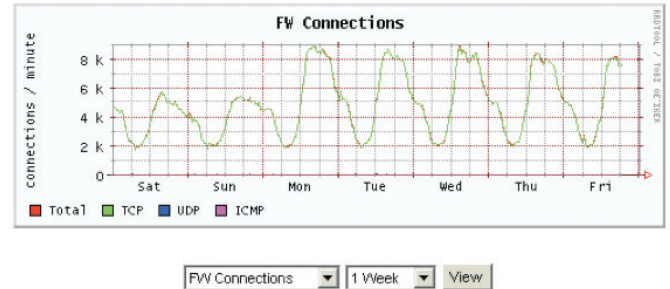
Device Logs: demo-d1-pix-1

Log file timestamps are in Greenwich Mean Time (GMT).

Size (bytes)	Date	Filename
n/a	n/a	Last 100 Entries
n/a	n/a	Most Recent
2079	03/27/2012 12:30:21	216.39.79.24-201203271155-log.gz
2271	03/27/2012 05:58:29	216.39.79.24-201203270558-log.gz
2504	03/27/2012 00:27:35	216.39.79.24-201203262355-log.gz
3196	03/26/2012 18:38:40	216.39.79.24-201203261755-log.gz
2827	03/26/2012 12:19:14	216.39.79.24-201203261155-log.gz
2476	03/26/2012 09:07:02	216.39.79.24-201203260555-log.gz
2442	03/26/2012 00:51:29	216.39.79.24-201203252355-log.gz
2644	03/25/2012 18:31:14	216.39.79.24-201203251755-log.gz
2040	03/25/2012 12:34:44	216.39.79.24-201203251155-log.gz
2283	03/25/2012 05:53:43	216.39.79.24-201203250555-log.gz
2923	03/25/2012 00:36:03	216.39.79.24-201203242355-log.gz
1636	03/24/2012 11:17:33	216.39.79.24-201203241155-log.gz
2612	03/24/2012 06:38:07	216.39.79.24-201203240555-log.gz
2270	03/23/2012 23:43:04	216.39.79.24-201203232355-log.gz
1963	03/23/2012 17:48:48	216.39.79.24-201203231755-log.gz
2047	03/23/2012 12:09:26	216.39.79.24-201203231155-log.gz
2430	03/23/2012 06:37:34	216.39.79.24-201203230555-log.gz
2470	03/23/2012 00:20:49	216.39.79.24-201203222355-log.gz

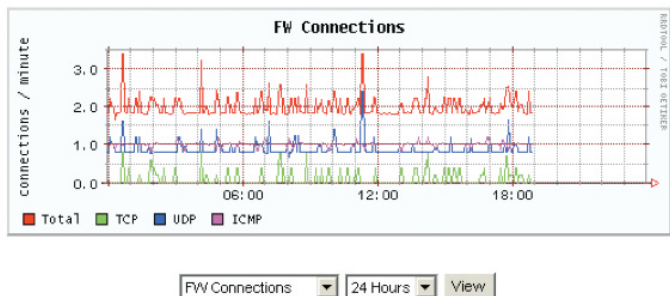
FIREWALL CONNECTIONS (WEEKLY VIEW)

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.



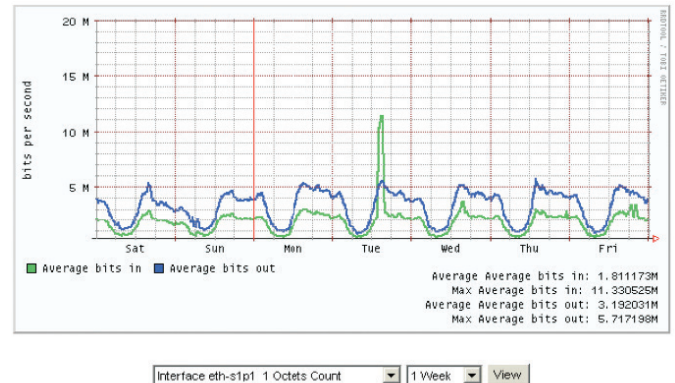
FIREWALL CONNECTIONS (DAILY VIEW)

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.



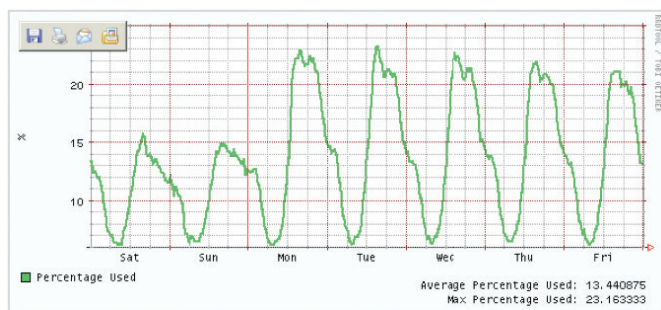
WEEKLY REPORTING OF "AVERAGE BITS IN / AVERAGE BITS OUT" ACTIVITY

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)

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.

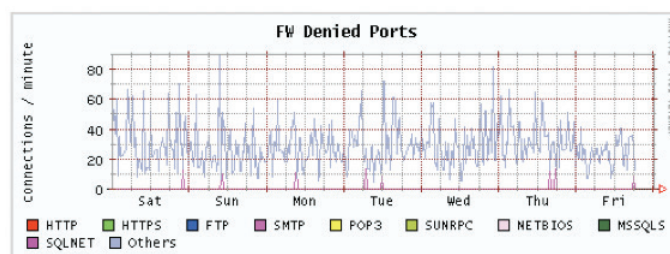


CPU Usage 1 Week View

FIREWALL DEVICE STATISTICS (DENIED PORTS — WEEKLY 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 CenturyLink's Managed Firewall Services or the CenturyLinkStation Portal, please contact your CenturyLink 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.



FW Denied Ports 1 Week View

For more information about CenturyLink Technology Solutions, visit www.centurylink.com/technology or call 1.800.728.8471.