Integrated Firewall with IPS Service — Cisco® ASA

DATA SHEET

Integrated Firewall with IPS Service Summary

Firewalls have long served as core components of most organizations' security strategies. However, the growth of security threats both in volume and in severity — have required multi-tiered defense strategies to become necessary business requirements, rather than just organizational "best practices."

A sophisticated set of security policies and vigilant monitoring are also required to keep external and internal intruders from gaining access to privileged organizational data and systems, and to maintain the integrity of ongoing network operations. However, the internal labor commitment and financial investment required to implement multi-tiered security strategies can quickly occupy IT resources, leaving your organization little time or capital remaining to focus on day-to-day business processes and to protect network assets from being compromised.

CenturyLink® Integrated Firewall with IPS Service leverages Cisco's leading ASA technology to provide both Firewall and IPS (Network Intrusion Prevention System) to your organization, in a single, unified delivery platform. URL filtering is supported as well as part of firePower Services, if required, as an additional purchase. In addition, the service provides an IPSec VPN capability, which allows organizations to connect up to ten remote sites to the ASA device, utilizing 3DES or AES encryption standards. Client to LAN SSL VPN services leveraging the Cisco AnyConnect based client are also an available option to the unified platform.

Enhanced Data Protection with our Virtual Firewall Option

Our optional virtual firewall capability[1] enables your organization to establish multiple instances of virtual firewalls on the same integrated firewall/ IPS device. This permits you to segment different components of your hosting infrastructure within a single hardware platform (for example, segregating proprietary data housed on your database servers from other servers that reside in your environment). Compliance requirements often dictate that information be segmented to minimize the potential impact of security threats, making such arrangements a critical strategic consideration for your organization.

The CenturyLink Advantage

- Ease of Implementation: CenturyLink manages the complete solution, from hardware installation, to configuration, to ongoing management.
- Leading Technology: CenturyLink utilizes established, Cisco-based technology to deliver your organization's protection.
- Expertise: CenturyLink leverages the expertise of a staff with deep experience in installing firewalls & intrusion detection devices.
- Monitoring on a 24/7 basis: CenturyLink has skilled resources to react quickly to security problems at any time, day or night.

Cisco Powered

1 The virtual firewall capability is an optional add-on to our standard service, and results in an additional charge to your organization. Please note that content and URL filtering, email anti-virus/anti-spam functions are not included with the service.

CenturyLink®

Audit-Ready by Design™

Cisco-ASA-based Managed Firewall and Intrusion Prevention services from CenturyLink can play an important role in helping you achieve and maintain compliance with the PCI DSS. These services have passed a PCI audit, making it easier for your auditor to validate them as a part of your overall cardholder environment.

Support from the CenturyLink Security Team on a 24/7 Basis

Since security situations can evolve by the minute, it is important for your organization to receive immediate notification of potential security incidents, allowing a response plan to be put into action as quickly as possible. Toward that end, CenturyLink Integrated Firewall with IPS Service provides both management and maintenance of the service, including monitoring of activity on a 24/7 basis.

Additionally, to provide your organization with timely review of threat information, CenturyLink provides access to your firewall logs, firewall and intrusion detection/prevention policies and daily statistics on a continual basis, via our secure Web portal. (Sample reports provided in the Appendix).

CenturyLink provides this level of support at your premises or in our data centers. We first work with your organization to perform a review of your firewall & IPS needs, and your network & system topologies. We also review your security policies to develop and refine both your firewall and IPS security policies. Based on the information that we have reviewed, we then configure, install, and manage your integrated firewall with IPS systems, according to your organization's unique requirements. When CenturyLink detects a potential security compromise, Incident Response hours[2] are utilized to determine the potential source of the incident, and to develop a response plan.

The CenturyLink Security Legacy

CenturyLink is a recognized leader in Security Services and offers a full range of services that includes Managed Firewalls, Intrusion Detection, Network-based Intrusion Prevention, Web Application Firewall, Log Management and Web & Email Protection. We have deep corporate experience in installing, managing and monitoring both firewall & intrusion prevention services, whether at our data centers or at customers' premises. All security services are fully-supported by a skilled team of certified security professionals, who are capable of delivering operational protection to your organization, every minute of every day. At an additional customer charge, CenturyLink is able to provide a full range of security-related Professional Services to you, including Web Application Vulnerability and Penetration Testing.

2 Incident Response hours are charged separately from your managed firewall/IPS service, and are only activated with your approval

Appendix: SavvisStation Firewall Reporting

Reporting for CenturyLink's Integrated Firewall with IPS Service 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 basis, via a phone call or an email to the CenturyLink Support Center.

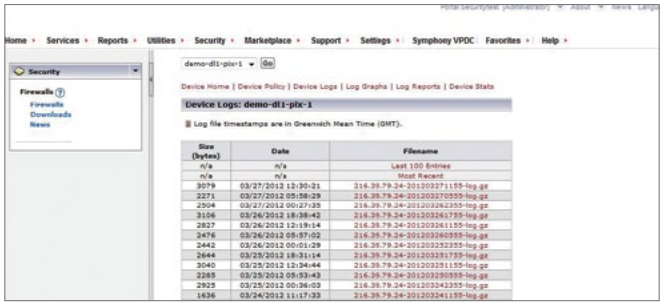
To provide you with some examples of the types of reports that are currently available on the portal, demo screen-shots follow on the next page. For a full explanation of SavvisStation Portal functionality (including server performance reporting, network performance reporting and billing invoice options), 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 CenturyLink's Firewall, Intrusion Detection, Threat Management Service (TMS), Log Management, Web Application firewall, DDOS mitigation and Integrity Monitoring Service (IMS) services. In this instance, summary information is displayed for demo Check Point and Cisco firewall devices.

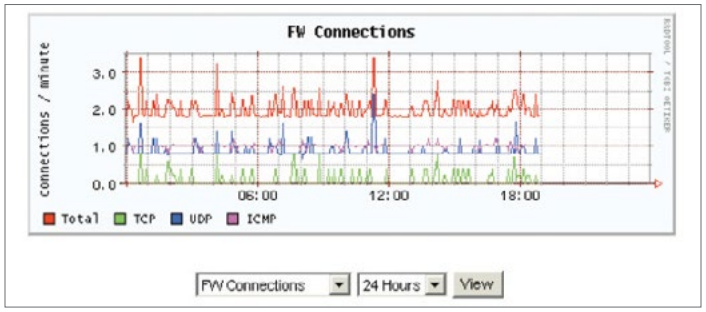
Firewall Device Logs

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



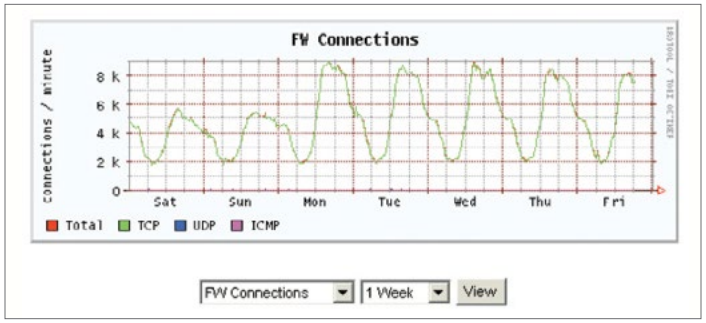
Firewall Connections (Daily View)

This screen summarizes Firewall Connections per Minute, by type (including TCP, UDP and ICMP connections). When analyzing this demo data, the employee in your organization who reviewed the report would have paid 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.



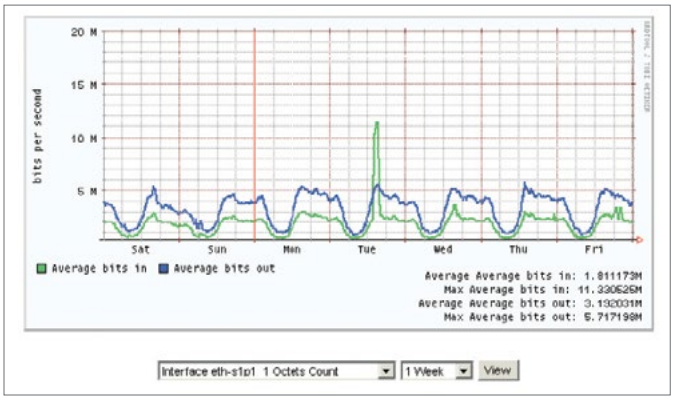
Firewall Connections (Weekly View)

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



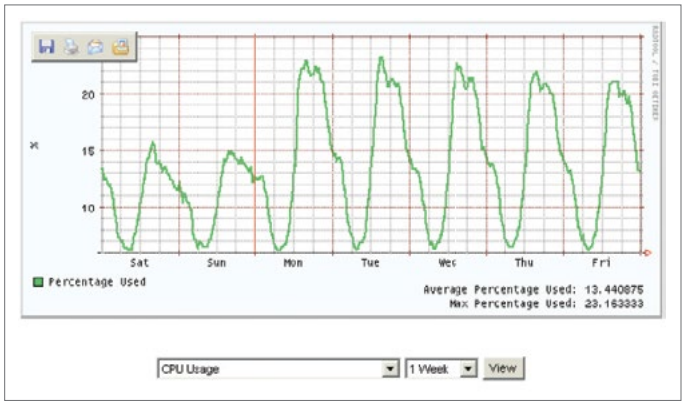
Weekly Reporting of "Average Bits In/Average Bits Out" Activity

Here, we are presented with activity on a single firewall interface. If this graph represented actual customer traffic activity (instead of demo activity), the employee in your organization who reviewed the report would have paid special attention to the "Average Bits In" results for Tuesday morning.



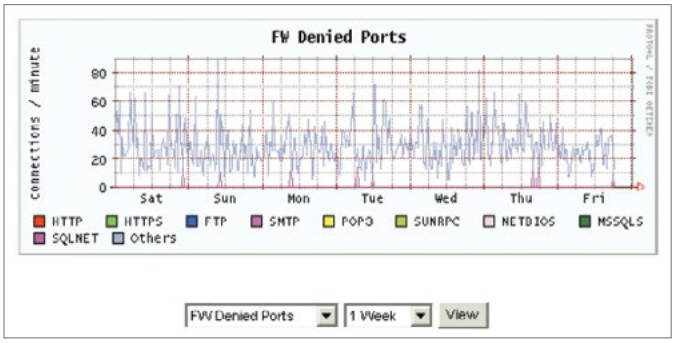
Firewall Device Statistics (Weekly CPU Utilization)

This screen summarizes CPU usage, for a weekly timeframe. The employee in your organization who reviewed the report would have paid particular attention to the spikes in CPU utilization that occurred outside of traditional high-volume business hours.



Firewall Device Statistics (Denied Ports — Weekly View)

This screen summarizes Denied Ports (by type), for a weekly time period. If this graph reflected actual customer activity, the activity that occurred on late Wednesday would have warranted further investigation by the employee in your organization who is responsible for reviewing daily reports.



For additional information regarding CenturyLink's Managed Firewall Services or the SavvisStation 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 of the unusual device activity in further detail.

For more information visit www.centurylink.com/enterprise.