Equinox Communications

MANAGED FIREWALL

Protect Your Communication Assets.

Managed Firewall Service

Compliance

Apply consistent policies and comply with regulations

Data security

Protect your reputation and business secrets

Legal issues

Reduce risk with compliance and legal hold

Your communications assets are vital to the success of your operation. **Equinox Communications Managed Firewall** service, available with our Dedicated Internet Access service, is a fully managed stand-alone firewall device that provides a barrier between your internal communications network and the outside network world. It allows authorized users access and keeps destructive forces at bay. Hackers and malicious users grow in numbers and sophistication every year. While the loss in productivity from an external attack can be debilitating, the loss in dollar terms can be even more dramatic. The Managed Firewall service provides turnkey management of your security services to help address these needs.

Business Solutions

- ✓ Comprehensive Protection: Expert security monitoring and management resources on your premises.
- ✓ Fully Managed: Offload security management from your in-house IT resources to free them for other tasks.
- ✓ Advanced Appliances: We deliver one of the greatest coverage areas available from a single network provider.
- ✓ Grows with Your Business: Our high-performance, scalable network can easily accommodate your current and future traffic.

$559.7 million dollars — the 2009 dollar loss related to Internet crimes based on reports to the U.S. federal Internet Crime Complaint Center — a 100% increase over the previous year.

Internet Crime Complaint Center
2009 IC3 Annual Report
www.ic3.gov/media/annualreports.aspx

FEATURES	DEFINITION	BASIC	ENHANCED	PREMIUM
Firewall with Stateful Inspection	A firewall blocks attacks by inspecting traffic, keeping track of valid sessions across the network and filtering traffic that looks suspect so that it cannot pass into the network.			
Number of Sites	A site can be a company location or it can be services located within a data center.	Unlimited	Unlimited	Unlimited
Configuration Backup and Restore	The configuration of your security device is backed up, so that in the event of hardware failure, the original configuration can be restored to a new device.			
URL Filtering	URL Filtering uses a method called Whitelist and Blacklist for filtering. A whitelist is a list of URLs that are allowed. Conversely, a blacklist is a list of URLs that are denied.			
Content Filtering	Allows you to choose categories of websites to block at the firewall. This feature can be used to block or allow access to common Internet categories like Social Networking (e.g., Facebook, Google and MySpace)			
Intrusion Prevention System (IP)	IPS monitors network and/or system activities for malicious activities or policy violations and reports or blocks them.			
Antivirus/ Malware/Spyware	Antivirus is used to prevent, detect and remove malware. Malware is software designed to secretly access a computer system without the owner's consent. Spyware is a type of malware that can be installed on computers to collect small pieces of information about users without their knowledge.			
Application Control	Uses dynamic application identification engines that recognize applications based on their behavior. By coupling application control policies with sophisticated security features, you can achieve a more granular level of security at the individual application level or by managing categories of applications.