Managed Firewall Security Services

Manage Services for Firewall Security

For organizations that can't afford to have their servers, PCs or data unavailable.

Is This You?

- Not sure how to define Secure Firewall Policies
- Don't have the TIME to properly configure, monitor and maintain
- Don't have the Expertise
- Need to be Compliant
- Need to Secure Remote Offices
- Not Happy with Current Security Solutions

At eSecurity Solutions, security is our only business. Since 2003, we have focused exclusively on products, services and managed services especially for business. We don't sleep until your data and business is secure and compliant.

Flexible Gateway Security Solutions to Protect your Internet Access, VPN, Data Centers and Wireless Network

In a Dangerous World Can You Protect Yourself

It is a dangerous world and there are many ways that your precious data can be stolen, destroyed or made unusable. Firewalls are the first line of defense against these threats.

External attacks on your data can be rendered through an insecure firewall. With more and more employees working at home, on the road or from remote offices; data can be also be accessed by unauthorized parties through insecure connections or inadequate authentication.

IT'S A DANGEROUS WORLD

- Hacking & Denial of Services
- Advanced Persistent Threats (APT)
- Wireless Hacks & Network Access
- Need for Secure Remote Access

Many employees spend most their day accessing the internet, sending and receiving emails, and accessing cloud based applications. The internet and emails both frequently contain malicious Web links that harbor malicious code. Malicious code once on your computers can allow others access to your data. Phishing, Spam, viruses and spyware need to be detected and blocked before they get into your networks.

Firewalls Can Protect and Increase Productivity

Firewalls protect against these threats and can provide companies with costs savings by helping employees to be more productive. Firewalls also are required to comply with many security regulations such as PCI-DSS, HIPAA, SOX, GLBA, and state based personal privacy laws.

A Firewalls primary purpose is to block traffic that is not authorized. But beyond that, firewalls can block threats through the usage of Unified Threat Management (UTM).

Surprisingly, employee productivity can also be enhanced by current generation UTM firewalls. In addition to blocking access to unwanted Websites (such as pornography, job sites and entertainment), it is possible to monitor, block and report on access to undesirable Web applications. Application control features, control access to streaming video, music, game sites, peer-peer networking, file sharing, downloads and other Web services. Companies can also control internet bandwidth usage reducing ISP costs and increasing productivity for all other users. User control features reduce corporate liability for employee activity.

FIREWALLS CAN:

- **Protect Against:**
  - External Hackers
  - Advanced Persistent Threats (APT)
- **Protect Employees from:**
  - Web Threats
  - Email Threats
  - Viruses, Phishing & Spam
- **Enhance Employee Productivity**
  - Control Web Usage
  - Control Web Applications
- **Protect & Monitor Wireless**
- **Provide Regulation Compliance**
  - PCI, HIPAA, SOX, GLBA …

Is a Secure Firewall Incorrectly Set Up Secure?

Along with firewall polices, ports and network settings, there are a multitude of other features you might need in your secure firewall. This includes the ability to define policies by user or user group for granular control. For secure remote access, site-site, SSL and client based secure VPNs should be used. UTM should be implemented to prevent viruses, spyware, intrusions, Web and mail threats, and application control for monitoring and controlling Web usage. Secure Wi-Fi is often implemented along with control of multiple Wi-Fi access points. For high availability, WAN and HA unit failover is required. Companies with Web servers may also need special settings for server or database security.

A properly set up firewall can provide amazing security. Using a security expert to define policies, set it up and maintain it is a must.

eSecurity Solutions is there to help you define secure policies, and then configure, monitor and maintain your firewall so that it remains secure even as your company changes. A secure firewall improperly set up is no more secure than no firewall at all.

FIREWALL SECURITY REQUIRES:

- Secure Business Class Firewall
- Purchase and Enabled UTM Features
- Secure Policies
- Configuration by a Security Expert
- Monitor/Revise Policies
- Modify Configurations
- Maintain and Update

MANAGED SERVICES

- Secure Policy Creation
- Secure Setup
- 24 x 7 Monitoring
- Alert Response
- Security Tuning
- Configuration Changes
- Maintenance & Updates
- Reports
- Support

BENEFITS

- Security that Matches Your Network & Usage
- Expert Security
- Ongoing Maintenance & Support
- Regular Security Reviews

Peace of Mind

DO YOU NEED THESE SPECIAL FEATURES?

- ☑ VPNs (Site-Site & Remote)
- ☑ Unified Threat Management
- ☑ Application Control
- ☑ User or Group Based Policies
- ☑ High Availability
  - WAN Failover
  - Device HA (Failover)
- ☑ Secure Wi-Fi
- ☑ Traffic Shaping
- ☑ Multi-Factor Authentication
- ☑ Virtual Domains
- ☑ Virtual Networks
- ☑ Compliances Regulations
- ☑ Server Protection

Managed Firewall Services

eSecurity Solutions provides three (3) ways to help you implement a secure firewall. For customers that want to manage their own firewall but don't want the up-front cost of the management infrastructure, we can provide a secure Hosted Firewall Management Portal. For those that need help up front, but want to manage the firewall thereafter, we can provide Installation Services or Retained Security Services. For customers who want the ease and peace of mind of completely outsourcing management to an expert, we provide Fully Managed Services designed specifically for your firewall.

FIREWALL SERVICES OPTIONS

Installation Services
- Hourly or Retained Services
- We help you set it up, then you take over

Fully Managed Firewall
- Managed Device Security & Internet Productivity

Managed Detection & Response (MDR)
- Manage Integrated System including Firewall
- Detect, Incidence Response, Contain

Contact us for a quote or information today:
886-661-6685
sales@esecuritysolutions.com
www.eSecuritySolutions.com

Why eSecurity Solutions Managed Firewall Services

	Managed Firewall Security Services vs. Do-it-Yourself with Manufacturer Support	
Define Policies & Setup	Security experts listen to your requirements & determine correct firewall policies to secure gateway and enable productivity features.	This is now your job. Firewall vendors won't help you define policies and set up your firewalls.
Monitoring	We use **monitoring tools** to monitor your firewall 24x7 and alert us to threats and issues. We save your event Logs offsite & back them up.	You are likely to set up your firewall and never know about threats and issues.
Alert Response	We respond to all alerts and quickly determine the root cause and respond with solutions.	Without monitoring tools, you have limited alert options with your firewall.
Security/Policy Tuning	Experts continually adjust settings to optimize your security, performance and any changes you have to your Environment or requirements.	Do you have the time and expertise to make secure configuration changes as required?
Internet High Availability	We can recommend the necessary solutions and install, configure and maintain the necessary solutions to provide you with redundant Internet and firewall security. Without these types of solutions, you can be down for days.	Do you have the expertise and time to design and setup your gateway for redundant internet and firewall operation?
Disaster Recovery	In the event of a disaster (hardware failure, power outage, internet failure, security issue), we are there to diagnose, advise and recovery your firewall and make sure that you are back up and running.	Having the right expertise to diagnose where the problem is and how to fix it is key. Lost time is lost money.
Reports	We set up standard and custom reports that are reviewed by us and available to you on a regular basis. If you have compliance requirements these reports can help document your compliance.	Setting up these reports can be time consuming. Reviewing & interpreting them can be even more time consuming.
Security Reviews	Included in your service is either Mid-year or quarterly security reviews. We review your service with you to make sure you are satisfied.	You must review your own work and results.
Essential Firewall Software maintenance, Updates & Hardware diagnostic Support	You are entitled to software updates and hardware troubleshooting support when you purchase your Firewall Support Agreement from the firewall manufacturer. This is included in UTM subscriptions.	
	eSecurity Solutions is alerted by the firewall manufacturer when new versions of software are available. We backup your software and install all appropriate updates to make your firewall safer, faster and enable new features.	Though vendors make these updates available, it is likely you will either not know about them or will not know whether these updates are worth installing. You will have to install them yourself and ensure that there are no negative consequences.
Hardware Warranty	Hardware warranties come from manufacturers and are in effect in accordance with the manufacturers policies.	
	eSecurity Solutions' Managed Security for Firewalls does not affect these warranties. eSecurity Solutions will work with manufacturers to diagnose problems, exchange hardware and reconfigure your new firewall when it fails.	This is your responsibility to call manufacturers, diagnose the problem and then exchange hardware and reconfigure your firewall.

Contact us for a quote or information today:

886-661-6685

sales@esecuritySolutions.com