



## *Firewall*

***With the evolution of the Internet and sophisticated LANs / WANs, security is becoming more and more of a concern.***

### **Who needs a PenTeleData firewall?**

Security has been an issue since the first computers were networked together. With the evolution of the Internet, security is becoming more and more of a concern. Whether it is a single computer connecting to the Internet, or a Corporation with multiple computers networked together, a Firewall from PenTeleData is a necessity to prevent unauthorized access. Anyone who is responsible for a private network (such as a LAN or WAN) that has connectivity to a public network (such as the Internet) needs firewall protection from PenTeleData.

### **What is a firewall?**

A firewall is an approach to security; it implements a security layer that defines the services and access permitted. The term firewall relates to the manner in which a device segments a network into different physical sub networks, it limits the damage that could spread from one subnet to another just like fire doors or firewalls. The main purpose of a firewall system is to control access to or from a protected network. It forces defined traffic to undergo inspection by the firewall, and permits or denies the traffic access to its destination. Ultimately a PenTeleData firewall protects networked computers from unintentional or intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service.

### **How does a PenTeleData firewall work?**

There are two access denial methodologies used by PenTeleData firewalls. A PenTeleData firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. PenTeleData firewalls may be concerned with the type of traffic, or with source or destination addresses and ports. A firewall may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a PenTeleData firewall determines what traffic to let through depends on which network layer it operates at.

PenTeleData firewalls protect private local area networks from hostile intrusion from the Internet. Consequently, many LANs are now connected to the Internet where Internet connectivity would otherwise have been too great a risk. PenTeleData Firewalls allow network administrators to offer access, of specific types of Internet services, to selected LAN users. This selectivity is an essential part of any information management program. It involves not only protecting private information assets, but also knowing who has access to what. Even privileges can be granted according to job description and need rather than on an all-or-nothing basis.

*“Ultimately a PenTeleData firewall protects networked computers from unintentional or intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service.”*

**Jeff Reinhard**

*General Manager  
- PenTeleData*

## Firewall

A PenTeleData firewall can greatly improve network security and reduce risks to hosts on the subnet by filtering inherently insecure services. As a result, the subnet network environment is exposed to fewer risks, since only selected protocols will be able to pass through the firewall.

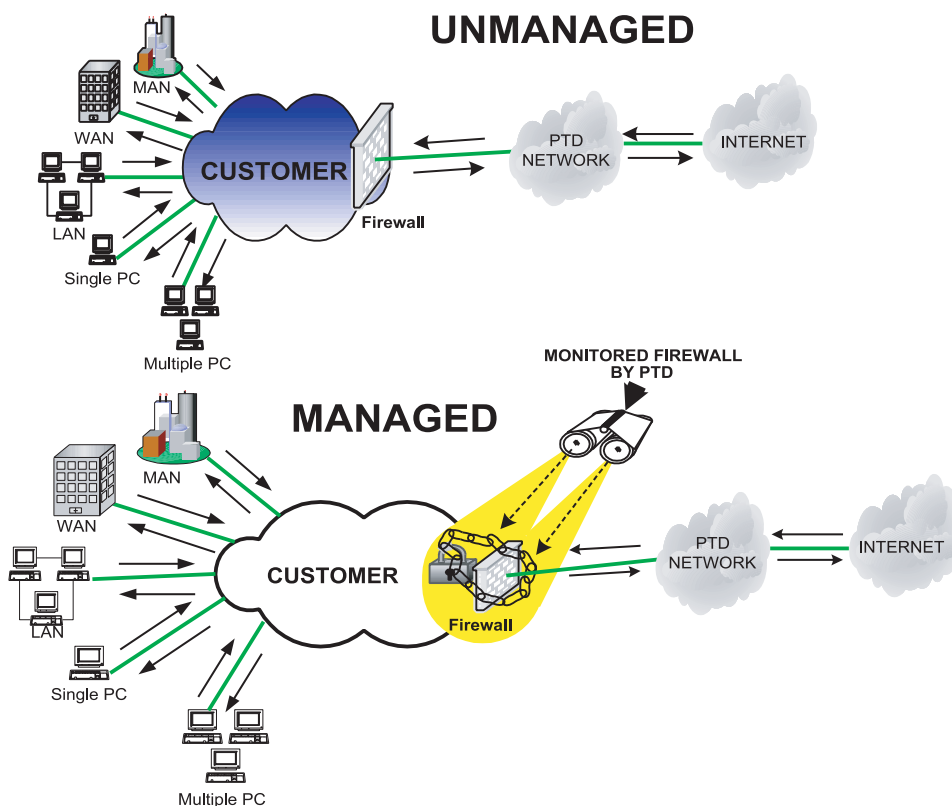
For example, a PenTeleData firewall could prohibit certain vulnerable services such as NFS from entering or leaving a protected subnet. This provides the benefit of preventing the services from being exploited by outside attackers, but at the same time permits the use of these services with greatly reduced risk to exploitation. Services such as NIS or NFS are particularly useful on a local area network, thus can be enjoyed and used to reduce the host management burden.

PenTeleData Firewalls can also provide protection from routing-based attacks, such as source routing and attempts to redirect routing paths to compromised sites via ICMP redirects. It could reject all source-routed packets and ICMP redirects and then inform administrators of the incidents.

### PenTeleData firewalls are categorized into two types:

**Unmanaged** – The Customer is responsible for all maintenance; Hardware is located on the Customer's premises; All support is T & M (Time & Material); The Customer has access to the Firewall; PenTeleData will direct logging to the Customer's logging server (Syslog); All Firewall changes are T & M.

**Managed** – Requires PenTeleData Plus and corresponding hardware maintenance for Firewall hardware; The Customer does not have access to the Firewall; Hardware is located on the Customer's premises; PenTeleData is responsible for maintaining the Firewall; PenTeleData monitors and responds to all Firewall Alerts; Access to PenTeleData NCC and Security Engineers for support; 24x7x365 monitoring of Firewall hardware and connectivity.



### PenTeleData firewalls can:

- Log accesses and provide valuable statistics about network usage.
- Provide the means for implementing and enforcing a network access policy.
- Block DNS information about site systems - the names and IP addresses of the site system will not be readily available.
- Protect private local area networks from hostile intrusion from the Internet.
- Monitor suspicious network activity and prevent attacks.

### FOR MORE INFORMATION

To learn how your company can take advantage of this and the other industry leading technologies from PenTeleData - call us at 1-800-281-3564 or

E-Mail: [prosales@ptd.net](mailto:prosales@ptd.net)

## PenTeleData

540 Delaware Avenue  
PO Box 197  
Palmerton, PA 18071  
Tele: 1.800.281.3564  
Fax: 610.826.4707

### Product Information:

E-mail: [prosales@ptd.net](mailto:prosales@ptd.net)  
Web: [www.penteledata.net](http://www.penteledata.net)

 PenTeleData

CS-FW-NM-090502