Authonet Firewall

Firewall Model:

F-10

Advanced Enterprise Cybersecurity

- Improve the security of your business by protecting access to your network
- Intrusion Detection (IDS) and Intrusion Prevention (IPS) systems keeping your network secure
- Device based authentication – restrict access to services based on device
- Integrate logging, reporting and monitoring to track your network
- Acts as a router giving you control of DHCP
- Firewall features include port and IP blocking
- Easy to install and operate, no specialist networking skills are required

Authonet firewall protects your network from both internal and external threats; with integrated device authentication and monitoring, giving you control of your network

Network Security Features

Businesses of every size and type are the targets of dangerous hackers.

The Authonet Firewall defends any computer network from external attack while additionally allowing enforcement of access rules within the local network to prevent unauthorized devices accessing protected systems.

Once installed, Authonet protects the network immediately because default access to the WAN side of the firewall is restricted. By utilizing the built in Access Control functionality, it is possible to manage what can be accessed on the WAN from your local network. The firewall can be configured down to individual IP addresses and ports; entire IP ranges or the entire Internet. It is also possible to configure which devices can access each resource either individually or as a group.

Integrated Intrusion detection systems report when the WAN is being scanned or when LAN devices are trying to access restricted services, permitting close monitoring of the network.

The Authonet Firewall also includes the added benefit of a default security policy, blocking all traffic traveling from the WAN to the LAN until permitted by the administrator.

Any Router, Firewall or other device on the network can be a security weak point; Authonet products mitigate this risk with a modern and easy to use Web based User Interface with an integrated Tutorial system, allowing easy setup and configuration.

Strong Network Security

Network security is strengthened by using access control technology to ensure that only authorized individuals have access to specific services and resources authorized for that device.

Authonet Benefits

Authonet manufactures a range of Cybersecurity products that protect any network. These include the Authonet Firewall and the Authonet IAM (Identity and Access Management).

The Authonet Firewall protects the network from attackers. With the inclusion of device based authentication, IDS and logging, the administrator has complete control over the network.

The Authonet IAM takes security to another level by implementing both role and identity based authentication in addition to device based authentication.

Authonet products integrate UTM solutions including network reporting and Content filtering to further protect the network from hackers.

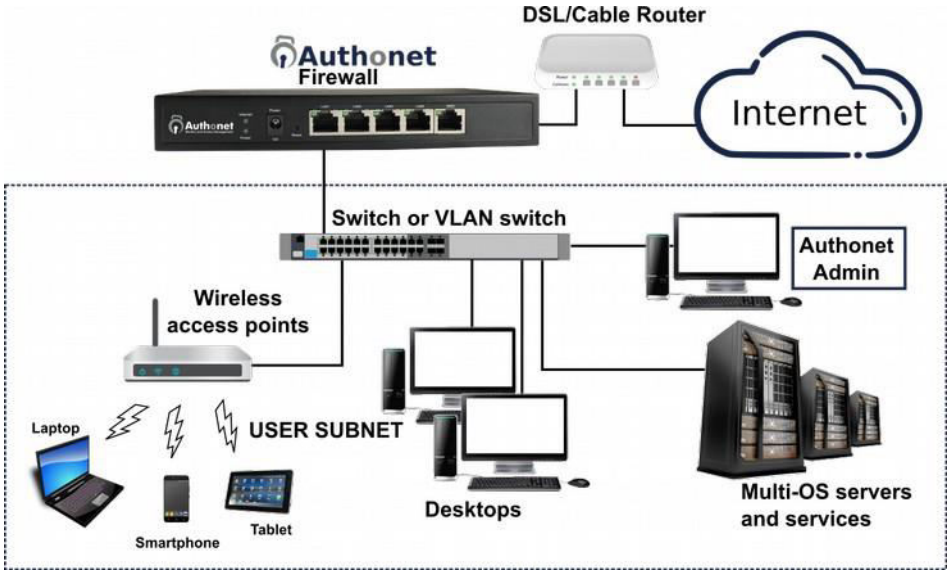
Authonet Firewall Implementation

The Authonet Firewall acts as a Gateway to provide security services between a WAN and a LAN segment. The Firewall can be installed with the WAN connected to the public Internet to protect the entire network from attackers. Alternatively the Firewall can manage and protect a smaller section of the network.

The Authonet firewall will defend the network against threats from both the WAN and LAN side of the network. Network usage can be tracked with integrated logging of DNS Queries, Port Scans, un-authorised access attempts and Administrator events.

The Authonet Firewall integrates advanced functionality to grant access to services on the WAN side of the network based on the privileges of the accessing device. This functionality can be used to regulate access to services and is especially useful in an increasingly diverse IT environment with BYOD being the new norm.

The Authonet Firewall is easy to install and operate, reducing the need to have trained IT staff to setup and manage the network. With advanced features that include VPN Clients, DMZ's and 1:1 NAT, the Authonet Firewall will meet most business security requirements.



Technical specifications:

PRINCIPLE MANAGEMENT FEATURES
Intrusion Prevention
Device Based Authentication
Service Management
DHCP
DNS
Logging

REPORTS
DNS Access
IPS/IDS reporting
Device authentication

OPERATION
Commercial grade equipment suitable for any ventilated environment
Ambient cooling is not required

SECURITY
Additional security for the administrator login

PERFORMANCE
Nominal throughput F-10: 80Mb/s

ETHERNET
WAN (secure network) RJ-45 Gbit
LAN (user network) RJ-45 Gbit

DIMENSIONS AND POWER
7.8" x 4.7" x 1.2"
12volt external power supply, 3amps, 110v/220v operation

SUPPORT
Free support via the Authonet website ticket system, Mon-Fri 9am to 5pm GMT

WARRANTY
1 year for product defects
3 years for free firmware upgrades
See terms and conditions of use

Applications for the Authonet Identity and Access Management Controller: Any business that is at risk of being attacked by hackers.

Call 1-800-213-0106 for further information, or see our website: www.authonet.com

AuthoNet: Network Authorization Systems 6073 NW 167 St., Suite C-12, Miami, FL 33015, US