Authonet
Identity and Access Management

IAM Controllers:

A-200 (200 Mb/s)
A-400 (400 Mb/s)

Advanced Enterprise Cybersecurity

- Improve the security of business data by controlling access to business information and services
- Combined User Identity and User Role based authentication
- Role Accounts are created and associated with the services permitted for each role
- User Identity Accounts are created for each member of the staff and associated with a Role account that authorizes access to services
- Strong passwords can be specified (minimum characters) and periodic password change can be forced
- Login is via a welcome page; logout can be automatic after a period without activity
- Transaction Records are logged during each user session and accessible for subsequent analysis

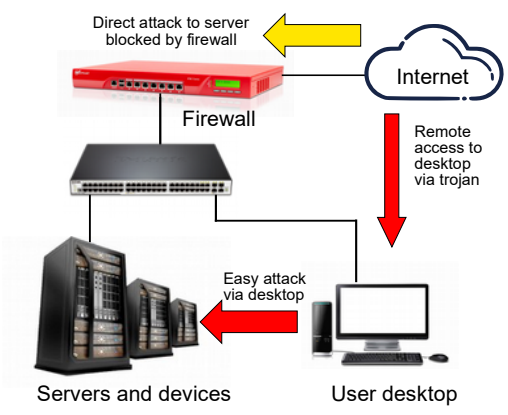
Identity and Access Management (IAM) Controllers:

Authonet enables the right individuals to access the right resources at the right times and for the right reasons.

Network Security Weak Points

Businesses of every type are targets for hackers with motives of data theft, ransomware and vandalism. The weak point of the business network is the connection between the business network and the Internet router, and so a Firewall is installed to block hacker intrusions.

The easy path for hackers however is to install a Trojan on a user computer which will give the hacker remote access to that computer, bypassing the firewall. The Trojan communicates to the hacker from inside the network and is not detected by the Firewall. The user is often tricked to click on an email link which installs the Trojan. For this reason, email filtering and anti-virus software is very important for all business networks. The diagram shows the path of attack.



Strengthen 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 individual, a process called Identity and Access Management (IAM).

Authentication of individuals is both role based and identity based to insure that individuals have access only to the information that is essential for the role they perform in the business.

Authonet Benefits

Authonet manufactures Identity and Access Management (IAM) products that implement both role and identity based authentication. Each role account authorizes access to the services and information required for that role. Each User Identity account has information about the individual, and the role to which that individual has been assigned.

The authentication process requires the presentation of credentials: safeguards ensure that any attempt to bypass the authentication process is blocked. After the authentication process has been completed the actions of each user are logged in a record that can be accessed by the administrator. The log is a valuable resource that can be used to monitor the actions of staff, and pinpoint the cause of any data breach.

Authonet Implementation

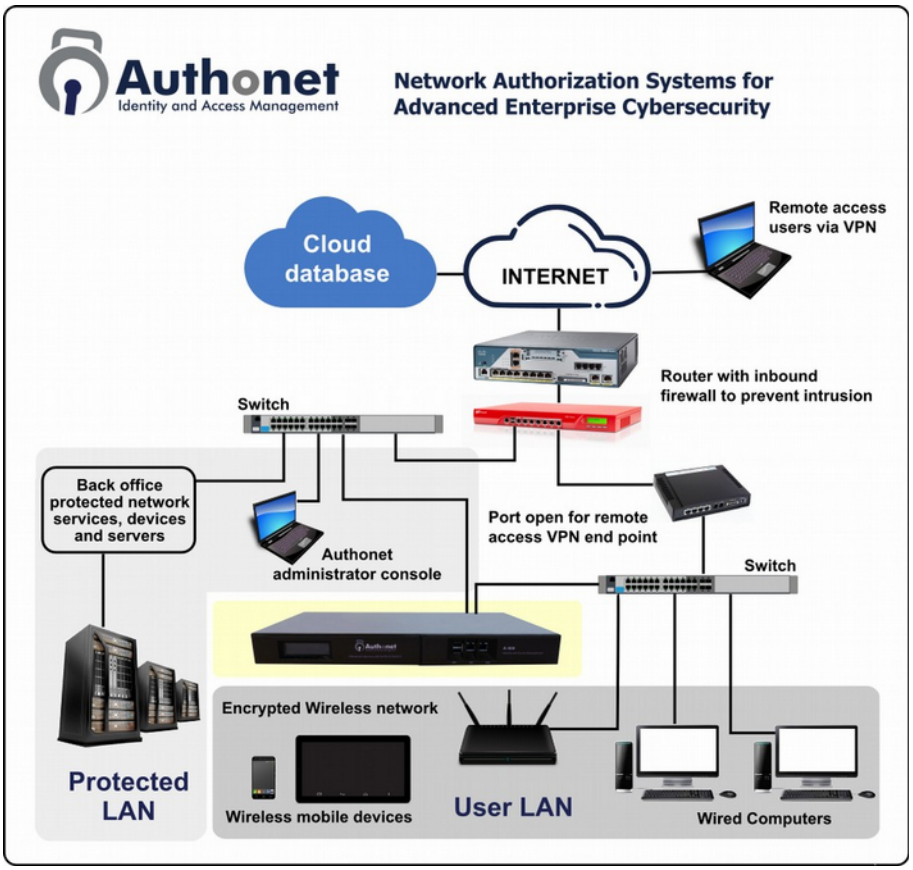
The Authonet Identity and Access Management Controller is a gateway between a network segment that has both mobile and desktop user devices, to a secure network segment with data servers and network devices such as printers and scanners.

Authonet ensures that only authorized users have access to the secure network, and that they can access only to services for which they are authorized. All unauthorized access attempts are blocked. Authonet also controls access to Internet services.

Authonet will block hackers who attempt to access the network data services from user computers, usually via remote access to a Trojan installed on a user computer.

The system administrator has access to a data log that lists the transactions that each user made while connected to the network.

Authonet products are easy to install and operate, and do not require specialist network skills for configuration.



Technical specifications:

PRINCIPLE MANAGEMENT FEATURES
User identity management, create/edit
User Role management, create/edit
Authentication via user identity and role
Authentication and use statistics
Blocking of non-authorized access attempts
Log of user network transactions
Local and remote admin configuration

REPORTS
Network traffic statistics, select time period
User services accessed with time/date stamps
Frequency of access to services, time period

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

USER AUTHENTICATION
User must authenticate to access services
Identify role and device authentication credential
2-factor authentication via mobile phone
Administrator alerts sent via email

SECURITY
User authentication via SSL
Additional security for the administrator login

PERFORMANCE
Nominal throughput A-200: 200Mb/s
Nominal throughput A-400: 400Mb/s
Storage: 128 Gbytes internal, and external backup

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

DIMENSIONS AND POWER
17" x 8" x 1.75". Rack mount kit included
12volt external power supply, 3amps, 110v/220v operation

RELIABILITY
Equipment failure monitoring via the Cloud
Administrator alert on failure via email

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

WARRANTY
1 year for product defects
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, USA

The recommended maximum number of concurrent users for Authonet products is based on the product throughput and the data traffic estimates per user. Consult Authonet for additional information regarding the applications and deployment of Authonet products.