Authonet cybersecurity

A300

Network End-point Cybersecurity

- Select the option to allow only pre-approved devices to connect to the business network
- Optionally authenticate users with or without approved devices using a password
- For added security authenticate users with 2-Factor authentication, an authorization code SMS message is sent to the users mobile device
- Determine what network device that the user can access and what network devices are blocked to the user
- Determine what Internet IP addresses or domain names that users can access or are blocked from accessing
- Content filtering blocks user access to malicious website categories
- The login page is configurable; use the default settings or create a customized login page

Authonet adds a layer of security at network end-points that will reduce the risk of data theft and ransomware attacks

Hacker attacks on businesses

Computer hackers attack business networks for one of two reasons. The first reason is to steal information that the hacker can sell on the dark Web; this might be credit card data or personal information. The second reason is ransomware extortion; the hacker will lock the business data and make it inaccessible, then demand a ransom to unlock the data. In many cases the business pays the ransom but the data is not unlocked.

Hacker attacks are increasing, and ransomware attacks are increasing at an exponential rate.

Hackers will try a direct attack on the business network but with a firewall installed that will not be successful.

The hacker will then try to attack the network end-point by sending phishing messages to install a Trojan virus on a users computer. The hacker will then share the computer unknown to the user and attack the business servers.

Direct attacks are successful in 25% of cases where the business has no firewall. End-point attacks are successful in 75% of ransomware cases.

The benefits of Authonet

Understanding that 75% of hacker attacks originate through the connection of the user to the network, Authonet developed an end-point firewall that monitors all user connections and ensures that only approved devices and users can connect to the network. This is especially important because most business staff connect to the network using WiFi and many use personal devices to access business applications.

Authonet end-point appliances also determine what the user can and cannot access both in the local area network, and in the Internet. Authonet provides the information that IT service providers' require for security surveillance.

Affordability

The Authonet product range has full-featured end-point security appliances designed for small, medium and large business installations. Authonet invested in product development to design products that not only incorporate the most advanced technologies but also are compatible with the IT budgets of small to medium businesses.

Authonet installation

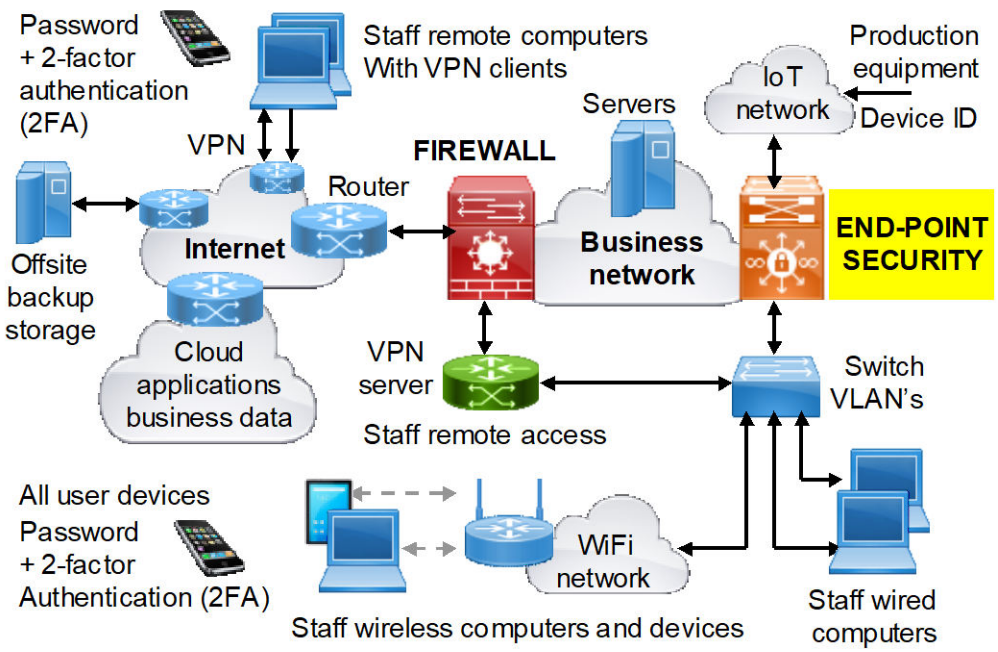
The Authonet end-point security appliance is installed in the network between the user devices and the network servers and equipment. Both wired computers and WiFi wireless access points are connected to an Ethernet switch which then connects to the Authonet appliance.

Authonet products are chosen for the network throughput required. The A300 with 300 Mb/s throughput is suitable for small to medium businesses.

Remote staff must also be authenticated through the Authonet end-point security appliance. Remote staff will connect through a VPN circuit with strong encryption for security, and the VPN router then connects to the Authonet appliance.

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

Business network data security



Network cybersecurity

A comprehensive network security plan should include the following;

- End-point user access security and firewall Internet security; the network edge.
- Off-site secure data backup with secure cloud based applications.
- A comprehensive and tested recovery plan to prepare for a hacker attack.
- Staff training to recognize a potential hacker attack.

A300 Technical specifications:

Authentication configurations
Verify MAC of device, if approved user can connect
MAC not verified, user required to enter password
MAC not verified, user required to 2FA with OTP
Verify MAC of device, user required to enter password
Verify MAC of device, user required to 2FA with OTP

Filtering configurations
Specify allowed network IP range
Specify blocked network IP range
Specify allowed Internet public IP's /domains
Specify blocked Internet public IP's /domains
Category filtering, Cisco openDNS subscription

Monitoring configurations
Check identified devices in LAN network
Report of device status
On a device failure send an alert to admin

Reporting
List the authenticated users
List IP requests not authenticated
Alert admin unknown MAC IP request
Failed authentication, alert admin
Network performance report

Authonet Cloud subscription
Remote configuration of gateway
Create groups, group gateways
Performance reports from gateways
Group performance reports
Alerting if any gateway fails

Warranty
1 year for product defects
Free firmware upgrades
See terms and conditions of use

Performance
Nominal throughput: 300Mb/s

Ethernet
WAN (secure network) RJ-45 1G
LAN (user network) RJ-45 4 ports, 1G

Dimensions and power
22cm x 13.3cm x 3cm
12 volt external supply, 1A 110v/220v

Support
Free support via the online system
Mon-Fri 9am to 5pm GMT

Operation
Commercial grade equipment
Suitable to install in any ventilated environment
Ambient cooling is not required

Call 1-800-213-0106 for further information, or see our website: www.authonet.com
Authonet is part of the Fire4 Systems Group 6073 NW 167 St., Suite C-12, Miami, FL 33015, USA

There is no limit to number of concurrent users for Authonet products. Network performance 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.