Authonet cybersecurity

A300

Zero Trust Cybersecurity Product

- Allow only pre-approved devices to connect to the business network
- Authenticate users to connect to the network with or without approved devices using a password
- For added security authenticate users with 2-Factor authentication, an authorization code is obtained from the users mobile device
- Determine what network devices 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 authentication page is configurable; use the default settings or customized it

Authonet Zero Trust cybersecurity products will reduce the risk of data theft and ransomware attacks with multi-factor authentication for users

Cyber attacks on businesses

Cyber criminals attack business networks to steal information or for ransomware extortion. Stolen information such as credit card data or personal information can be sold on the dark web. With ransomware extortion the hacker will lock the business data making it inaccessible, then demand a ransom to unlock the data. In 35% of cases the business pays the ransom but the data is not unlocked.

The volume of ransomware attacks increasing faster then data theft.

Criminals may try a direct attack on the business network but a firewall will stop them.

The most popular method of attack is to send phishing messages that will install a Trojan virus on a users computer. The hacker will then access the computer without the users knowledge and attack the business servers.

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

Authonet cybersecurity

The Authonet Zero Trust cybersecurity gateway controls and monitors the connection of devices and users to the network where 75% of cyber attacks originate.

The Authonet gateway ensures that only approved devices and users can connect to the network. User authentication includes multi-factor authentication.

The Authonet Zero Trust gateway also determines what the user can and cannot access both in the local area network, and in the Internet.

Authonet has a subscription cloud management and monitoring service that IT service providers use to provide security surveillance for their customers.

Affordability

Authonet has invested in product development to design products that incorporate the most advanced Zero Trust cybersecurity technology.

Authonet products are compatible with the IT budgets of small to medium businesses so that they can have the best cybersecurity possible.

Authonet Zero-Trust Cybersecurity Products

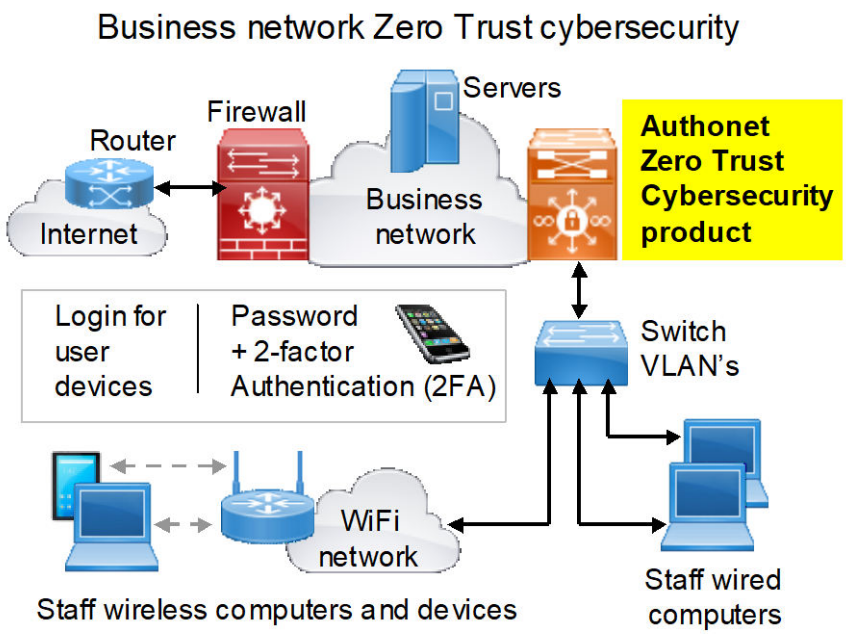
Authonet installation

The Authonet Zero Trust cybersecurity gateway is installed in the network between the user devices and the network servers. Both wired computers and WiFi wireless access points are connected to an Ethernet switch which then connects to the Authonet gateway.

Authonet gateway products are identified by the network throughput required. The A300 has 300 Mb/s throughput and there is no limit with the number of staff that can be authenticated.

Remote staff must also be authenticated through the Authonet Zero Trust cybersecurity gateway. Remote staff connections are described in the product manual.

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



Network cybersecurity

A comprehensive cybersecurity plan should include the following;

- Staff awareness training to recognize a potential hacker attack.
- Firewall Internet security to block a direct cyber attack.
- Zero Trust cybersecurity with multi-factor authentication.
- A comprehensive and tested recovery plan to prepare for a cyberattack.

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.