IDECO UTM

ideco

IDECO UTM

Complex Threat Protection and Management.

Ideco UTM is a modern UTM (Unified Threat Management) solution based on the Linux kernel using Open Source and proprietary modules, including a convenient web interface for server configuration.

The main modules of our solution are: intrusion prevention system (IDS/IPS), application control, content filter, multi-level antivirus and anti-spam traffic checking, WAF, protection against botnets, phishing and spyware.

Our solution is ideally built to provide secure Internet access for SOHO/SMB organizations and does not require complex configuration and deep knowledge of the product for its implementation.

KEY FEATURES

- User-friendly and simple web-based administrative interface.
- Diversified Network Protection: firewall, content filter, application control, anti-virus traffic scanning, intrusion prevention system, IP-Reputation blocking, spam filtering, protection of published web applications.
- Access Control: to access the Internet, devices must necessarily be authorized using one of several options, including Single Sign-On authentication via Active Directory.
- A VPN server with the ability to establish site-to-site and client-to-site connections over a secure IPsec protocol.
- Reporting on the use of Internet resources by users.
- Support of x86-64 compatible hardware or any modern hypervisor.
- Quick installation and deployment: for a small network, installation and complete product configuration takes from 1 to 3 hours.

SERVER AND NETWORK PROTECTION

Ideco UTM combines many modules designed to provide security for both the server itself and the enterprise local network.

Intrusion Prevention (IDS/IPS)

- The integrated intrusion prevention system allows enterprises to block attacks on their server (access to internal and published services, DoS attacks, attempts to execute arbitrary code, etc.) and the local network protected by it. The system also logs suspicious activity, including that caused by viruses and Trojans inside network, identifies and blocks botnets' activity.
- The system blocks attempts to bypass filtering rules: use of the TOR network, anonymizers, p2p and torrent clients.
- Daily updated sets of rules help to protect against new types of attacks and block intruders based on IP Reputation.

Server Protection

- The server is built on Linux and uses only stable versions of the kernel and components with all security patches.
- The server protection is seriously strengthened in comparison with the usual Linux distributions: the file system is divided into a unmodifiable and modifiable part, while it is impossible to execute files from the modifiable part; there is no root super user in the default mode; all ports are not accessible to external interfaces; the system checks the checksums of all executable files during loading, which makes it impossible to use rootkits.
- Each version of Ideco UTM is tested for security with several vulnerability scanners. The developers quickly eliminate all discovered vulnerabilities in components and the kernel. Automatic updating allows installing patches without the help of an administrator.
- All services are configured with only the minimum necessary access rights to the file system and network. This minimizes possible vectors of attacks, even if the components are found to be vulnerable.

- The firewall is configured by default to protect all network interfaces of the server from DoS attacks, MIT attacks, aggressive, illegitimate and obviously viral traffic, taking into account its nature, but not its type.
- All secure protocols (SSH, TLS, HTTPS) use only the most crypto-resistant encryption keys, which excludes man-in-the-middle attacks.
- The system uses reliable and secure protocols for VPN connection of offices: OpenVPN and IPsec with the AES-256 cryptographic encryption algorithm.
- Connecting clients to the mail server from the outside is possible only using encrypted protocols: SSL and TLS. It also encrypts traffic between mail servers that support SMTP encryption. This excludes the interception of messages when analyzing traffic at the provider side.
- The server blocks brute force attacks (attempts to brute passwords) on SSH, SMTP, IMAP, POP3 services, webmail, and the web server administration console.
- The entire distribution package, including the kernel, is assembled from the sources tested by the FSTEC of the Russian Federation for the absence of undeclared capabilities and security vulnerabilities.

Protection of Published Services

- The Web Application Firewall protects published web applications from scanning for vulnerabilities, SQLi, XSS, DoS, and other attacks.
- Publication of the mail server through a mail relay allows spam filtering of Ideco UTM emails (Kaspersky Anti-Spam, greylisting, DNSBL, mail rules), blocking viruses (Kaspersky Antivirus and ClamAV) and protecting the server from DoS attacks.
- Publish services using the DNAT portmapper. In this case, the service is protected by the intrusion prevention system and becomes resistant to intrusion attempts, use of malicious scripts and exploits.

Local Network Protection

- Anti-virus scanning of web and mail traffic: antivirus Kaspersky Lab and ClamAV.
- Content Filter allows administrator to close access to dangerous sites: sites distributing illegal software and spyware, infected with viruses, fraudulent and phishing sites. Site categories updates automatically in real time with the help of cloud technologies, therefore databases are always up-to-date.
- Encrypted HTTPS traffic is controlled by all services: antivirus, content filter and reporting system, which avoids hidden deployment of viruses through secure SSL connections.
- The built-in system and user firewall are convenient in settings: you can apply them both for the entire network, individual subnets, as well as for individual users or groups, even if they use dynamic IP addresses.
- It is possible to limit users by the number of sessions to prevent virus outbreaks. In addition, exceeding the limit for the number of sessions is logged, so overly active users and devices can be easily detected.
- The system uses a secure IPsec protocol to connect users via VPN from the outside, which allows connecting all modern operating systems, including mobile ones with AES-256 resistant encryption.
- Reports and statistics on users in a convenient visual form allow you to identify suspicious activity in case of infection of their devices with viruses or trojans.
- The possibility of integration with DLP solutions (Data Leak Prevention) by ICAP allows avoiding accidental leakage of confidential information.
- A DNS server with the ability to intercept requests to external servers makes it easy to use cloud-based DNS filtering services and effectively filter traffic at the DNS requests level to protect against malicious sites and botnets.

ideco.com