Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

IDECO UTM

Information is one of the most valuable resources in the modern world. Loss of data can lead to invaluable losses for organizations of any scale. Thus, cyberspace protection is becoming increasingly important. To ensure maximum network security, you need to carefully choose the tools.

Ideco UTM (Unified Threat Management) is a software UTM solution that makes access to the Internet manageable, safe and reliable.

Intended Use

- Secure and controlled Internet access for all employees.
- Protection of internal servers against Internet attacks, server access control, creation of shared and private network servers.
- Secure connection of remote users, implementation of a secure channel between branches.

MAJOR THREATS TO INFORMATION SECURITY

- Data-encrypting malware.
- Non-targeted attacks.
- Targeted attacks.
- Botnets.
- Web application attacks.
- Phishing.
- Direct espionage.
- Tools of intelligence agencies used by hackers.
- Vulnerabilities in popular systems.

Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

THREAT PREVENTION

The Intrusion Prevention System blocks:

- Botnet command centers.
- Vulnerability scanners.
- Spyware traffic, Windows telemetry and other software traffic.
- Exploits used by popular cryptographic viruses.
- Known attackers by IP Reputation and GeoIP.

The Application Control blocks:

- TOR (which can be used by botnets for communication).
- Potentially dangerous applications for remote access (TeamViewer).
- Messengers and other software.

The Content Filter blocks:

- Phishing sites.
- Infected sites and sites that spread viruses.
- Sites with illegal software and hacking utilities.
- Web trackers, ads, banners, and sites that anonymously collect information about users.

Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

MAJOR VIRUS ATTACKS IN 2017

WannaCry

The global hacker attack has now affected thousands of users around the world. By May 12, 45 thousand attacks were recorded in 74 countries.

Wannacry uses e-mail as a mechanism of penetration (this mechanism allows it to overcome protective firewalls). This vulnerability allows the virus to spread within an infected network and hit the maximum number of vulnerable devices.

Petya

Like WannaCry, this encryptor combines the functions of virus, trojan, and network worms. The software is able to penetrate into a protected network and spread further through the Windows vulnerabilities in NetBIOS or RPC.

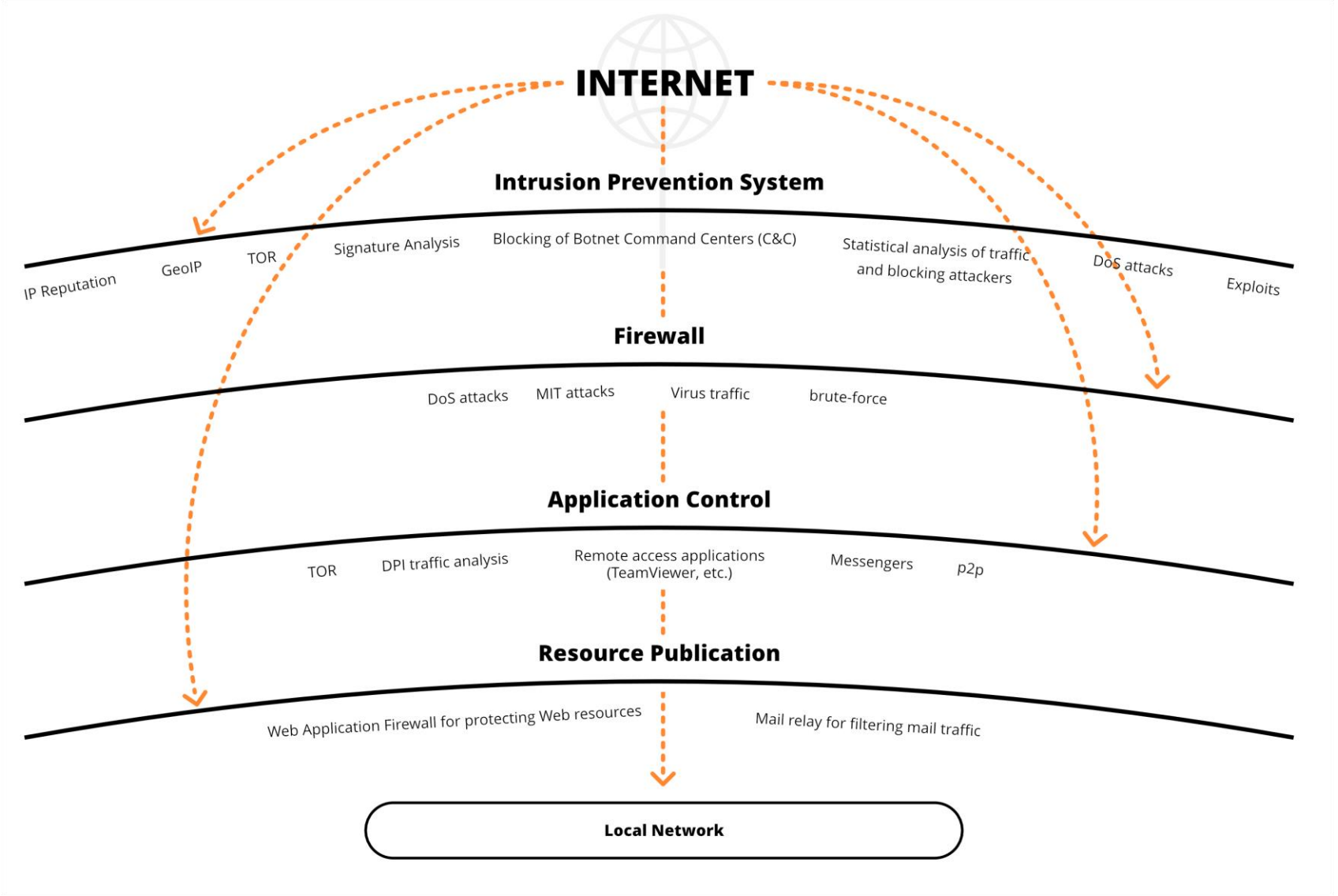
The malware can spread in completely silent mode, but at the zero hour it locks the computer and demands ransom. And even in the case of payment, user does not have a guarantee of the information decryption. Often ransomware does not have decryption functions or they may contain errors.

Bad Rabbit

Rabbit behaves in a similar way to Petya. After the "incubation period" of unknown duration, when it is distributing within the corporate network, and with the help of brute-force attacks on computers running Windows, the ransomware activates file encryption functions and displays a ransom message on the computer screen.

Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

DEEP TRAFFIC ANALYSIS TOOLS



Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

COMPARISON WITH COMPETITORS

Functions	Ideco ICS	Kerio Control	Microsoft TMG	Check Point	Fortinet
Bandwidth control	+	+	–	+	+
Mail traffic filtering (antivirus, antispam)	+	–	+	+	+
Outlook Web Access publishing	+	–	+	+	+
Application control (DPI)	+	+	–	+	+
Mail server	+	–	–	–	-
Blocking by IP Reputation	+	–	–	–	+
Blocking anonymizers	+	–	–	–	+

Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

VALUE OF IDECO

- Simple and intuitive graphical interface
- Simple and convenient administration
- Quite moderate hardware requirements
- Flexible pricing policy
- Ability to customize solutions for a particular region or country
- Competitive all-in-one security solution
- Support for all virtual machine formats
- Simple implementation (1–2 days)

Russia, Yekaterinburg, Kulibina str., No. 2, office 501
+7 495 268 01 74
sales@ideco.com
ideco.com

SYSTEM REQUIREMENTS

CPU	Intel Pentium G/i3/i5/i7/Xeon E3/Xeon E5 supporting SSE 4.2
RAM	4 GB (up to 30 users). 8 GB for using the intrusion prevention system, anti-virus scanning of traffic, and to support more users.
Storage	Hard disk or SSD, 64 GB or more, with SATA interface, SAS or compatible hardware RAID.
Network	Two network cards (or two network ports) 10/100/1000 Mbps. It is recommended to use cards based on Intel, Broadcom chipsets. Realtek, D-Link and others are supported.
Hypervisors	VMware, Microsoft Hyper-V (1st generation), VirtualBox, KVM, Citrix XenServer.