General information

Intrusion Prevention System (IPS) – network and computer security software system that detects intrusion or security violations and automatically protects against them.

ESR series devices — service routers that are capable to perform a wide range of tasks related to network protection. The key elements are means of hardware acceleration of data processing, that allow to achieve a high level of performance. The ESR series routers includes a wide range of models with different performance, that allow to use the routers in stand-alone solutions for small and medium-sized businesses as well as in large distributed networks.

The IPS solution on ESR allows to install the router on the border of a network to prevent and/or identify attacks on the network being protected. It can also be installed inside a network to reduce routing overhead when used as a firewall. ESR combining the functionality of a boundary router and firewall allows you to prevent attacks at early stage and protect all elements of the network.

Also, ESR supports IPS logs uploading in EVE and syslog formats for interaction with SIEM systems. Flexible configuration of rule sources allows you to load signatures from the global and internal network, in the format of Suricata rules.

The ESR software includes built-in rules from open sources — Emerging threads, and functionality for creating your own rules — easy configuration in the form of a constructor and more flexible — in the format of Suricata rules.

Open source rules allow you to identify and block malicious software, DoS attacks, botnets, information events, exploits, zero-day vulnerabilities, SCADA network protocols, etc. Additionally, you can download "black lists" of centers that control botnets, sites that distribute viruses and malware, etc.

IPS features

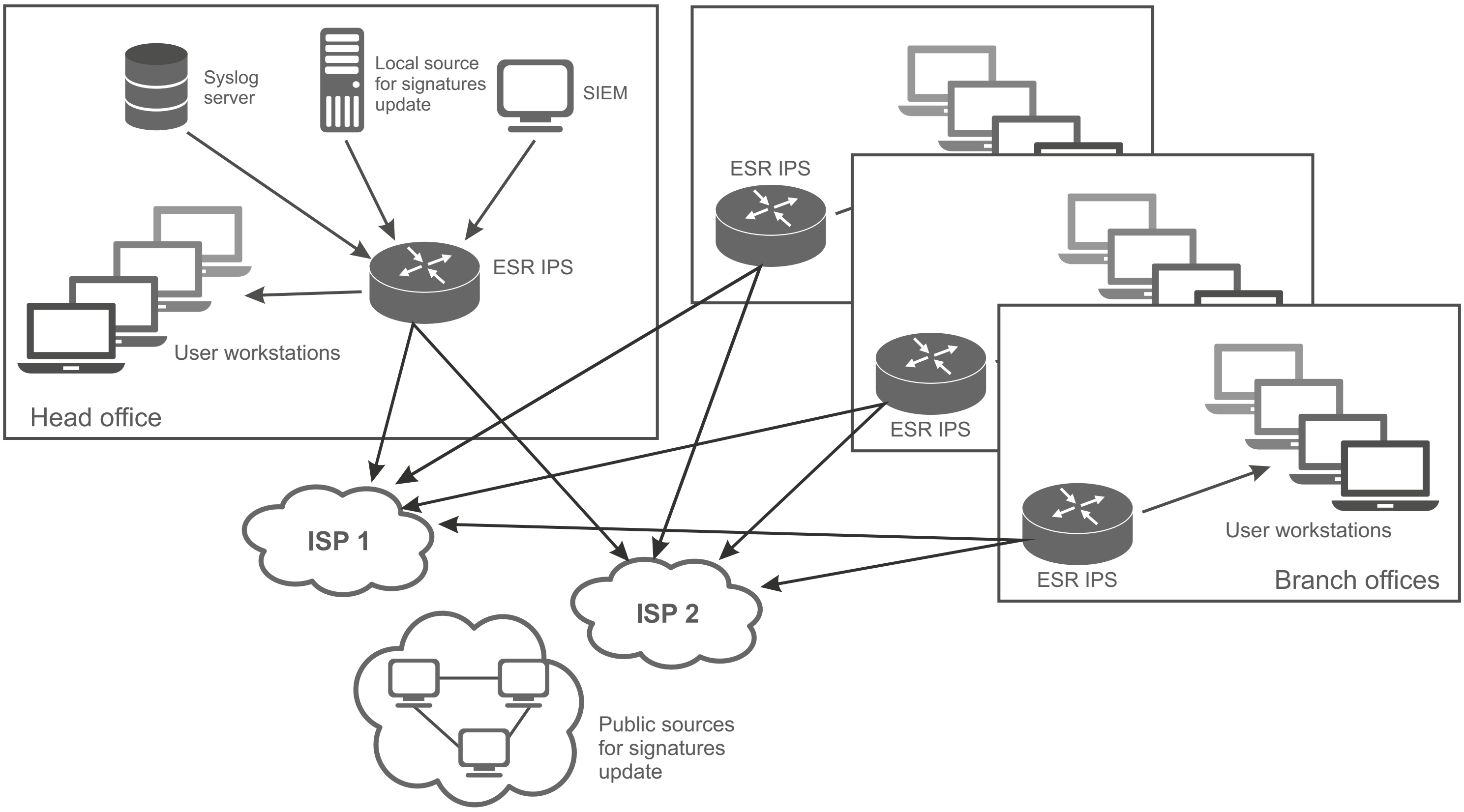
- **Support for EVE format**
- **Syslog support**
- **Rule designer support**
- **Up to 32 update servers**
- **Suricata-compatible rules**
- **Built-in Emerging Threats rules**
- **Support for service router functionality**

Features of ESR firewall with IPS

- **Firewall performance: 9.8 Gbps[1]**
- **IPS performance: 1.1 Gbps[1]**
- **Filtering by applications**
- **Protection against DoS/DDoS**

[1] according to ESR-1000 tests

Use case



Why IPS?

The ESR service router can operate in the IPS mode as well as in IDS mode (Intrusion Detection system), depending on the action applied when the rule is triggered. However, IDS mode does not provide active protection, so we highly recommend that you modify the rules and use the device in IPS mode, that will significantly increase the network security.

The network audit will help to create an optimal set of rules that provide reliable protection of the network and high performance of the device. It is also important that the rules always be up to date, updated and supplemented in a timely manner, depending on current needs.

The use of IPS on the border of a network will allow to avoid many types of untargeted attacks by bots, to protect the internal network from external penetration in case of incorrect configuration of the border router or vulnerabilities in the software used. In addition, IPS can be used as a simple streaming file scanner.

When using SIEM systems, you can achieve maximum protection efficiency. You may configure the downloading and rotation of the log in IPS - this will allow to configure the rules flexibly, evaluate level of current threat to the network and perform an audit in real time.

Ordering information

For more detailed information, as well as to order or test the equipment, please contact ELTEX managers directly.

Contact us

☎ +7 (383) 274 10 01
+7 (383) 274 48 48

eltex@eltex-co.ru

www.eltex-co.com

About Eltex

Eltex company is a leading Russian developer and manufacturer of telecommunication equipment with 25 years of history. Integrity of solutions and seamless integration capability into Customer infrastructure is a priority area of company development.