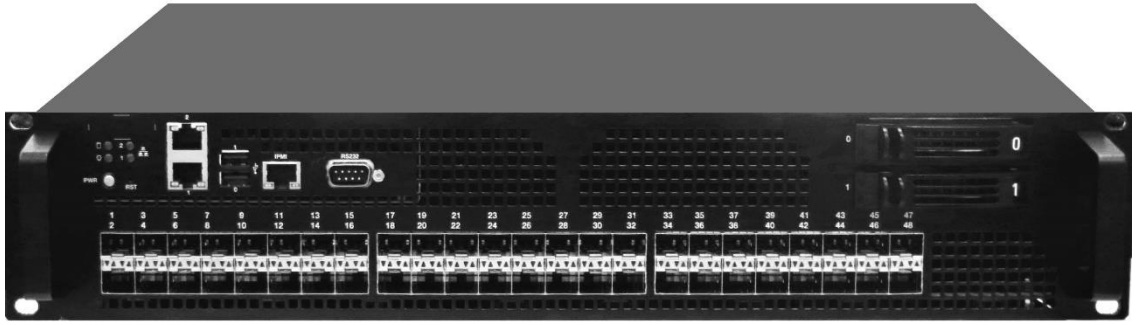


Leo

L7 DPI

форм-фактор

1U

2U

4U

Устройство многоуровневого анализа и фильтрации трафика

LEO – аппаратно-программный комплекс мониторинга и фильтрации IP-трафика на каналах со скоростями до 100 Гбит/сек:

- в соответствии с заданными правилами,
- в режиме реального времени,
- без потерь.

LEO используется для решения широкого спектра сетевых задач, может расширять свой функционал, масштабируясь до систем типа IPS и съёмника СОРМ3.

LEO эффективно решает задачи трех основных типов

Агрегация и балансировка | Анализ трафика | Фильтрация трафика

- Анализирует трафик в сети оператора:
  - → выявляет узкие места, нагруженные протоколы, распределение трафика по странам и т. п.;
  - → записывает данные на диск;
  - → определяет часы-пик по входящему / исходящему трафику и т. д.;
  - → проводит мониторинг в режиме on-line.
- Блокирует нежелательные виды трафика.
- Перенаправляет трафик на другие сетевые интерфейсы для дополнительного анализа.

⚠ *Для правильной работы LEO должен в полном объёме получать пакеты, содержащие контентный трафик и служебные управляющие сообщения.*

До 64 GbE портов, каждый из которых может независимо работать на приём /RX/ и передачу /TX/.

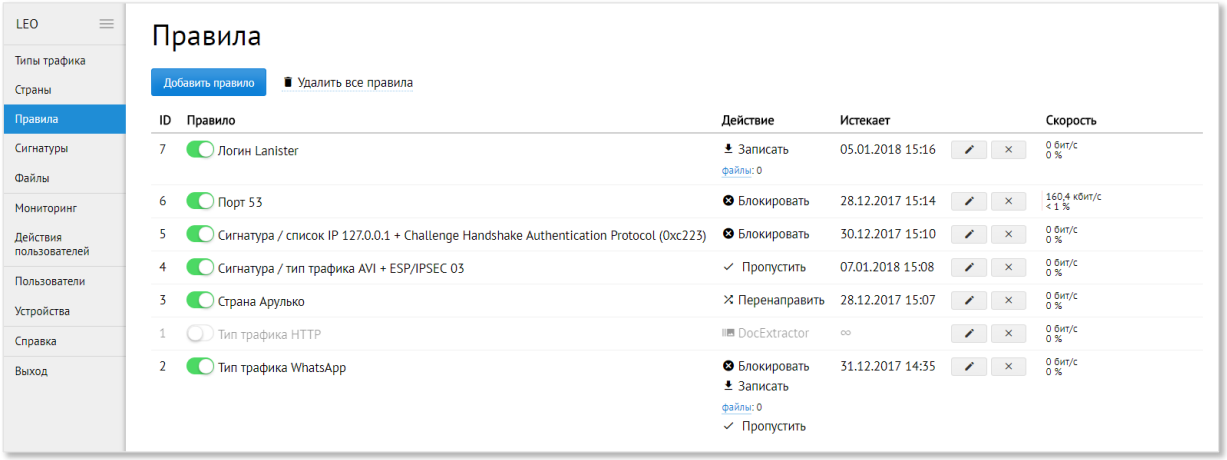
LEO - многофункциональный сетевой фильтр

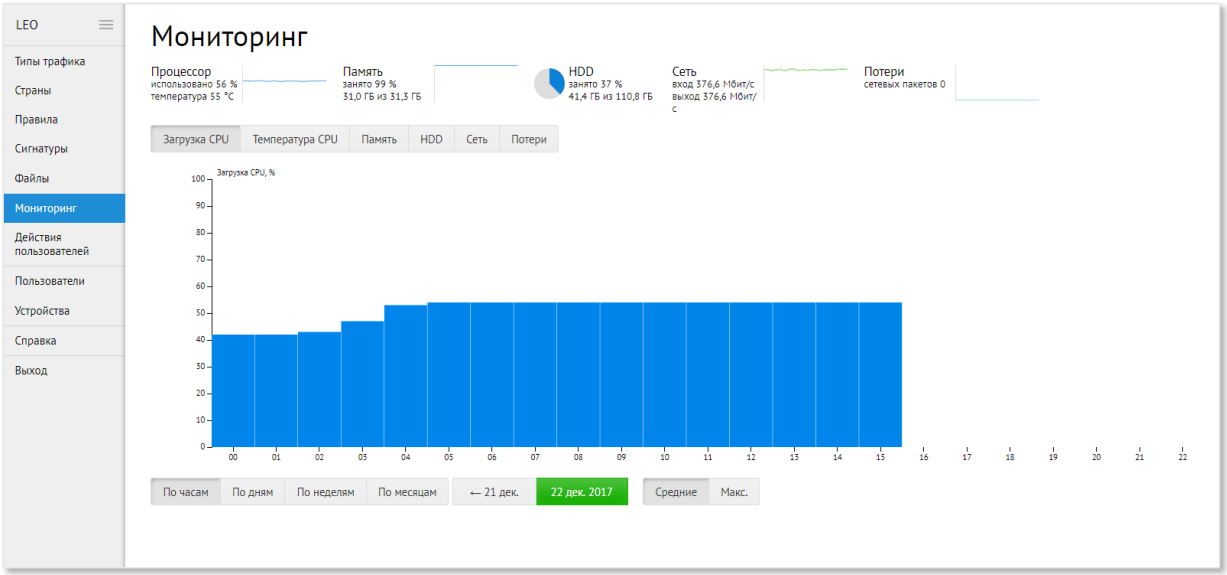
matching / критерии для правил

критерии фильтрации	тип приложения
	геолокация
	сигнатура
	регулярные выражения
	IP-адрес, IP-IP, подсети /IP + Mask/
	порт, диапазон портов
	подсеть, подсеть-подсеть
	URL
	логин на сервере авторизации
	IMSI

действия

блокировка	блокировка используется при установке LEO «в разрыв» для фильтрации из выходного потока нежелательных типов трафика
запись	запись определённого вида трафика в файл для дальнейшего анализа
перенаправление трафика	возможность выделить из основного потока часть трафика и отправить его в свободный сетевой интерфейс
	например, для обхода фильтрации или подачи на устройство мониторинга
DocExtractor	извлечение и экспорт из потока данных документов
Traffic Shaping	ограничение полосы канала
	позволяет управлять скоростью посылки пакетов в интерфейс во избежание перегрузки линка

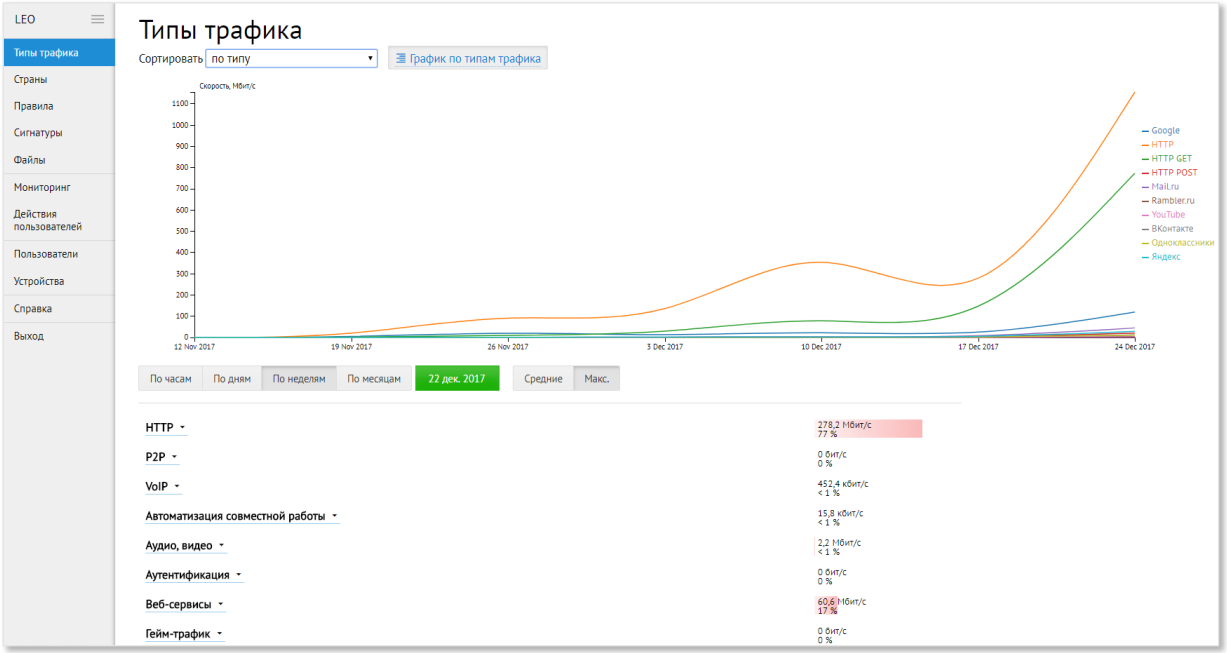




LEO. Встроенный классификатор на 180 типов приложений

классификатор приложений

HTTP	HTTP, HTTP ActiveSync, HTTP GET, HTTP POST, HTTP Proxy
P2P	Aimini, AppleJuice, BitTorrent, Direct Download Link, DirectConnect, Edonkey, FileTopia, Gnutella, iMESH, Kazaa/Fasttrack, OFF, OpenFT, PANDO, Soulseek, StealthNet, Thunder, WinMX
мессенджеры / VoIP	Cisco skinny, FaceTime и iMessages, H.323, IAX, MGCP, RTCP, RTP, SIP, Skype, TeamSpeak, Truphone, Viber, Oscar, WathsApp, IRC, Jabber, meebo, MMS, MSN, OSCAR, Popo, QQ
автоматизация совместной работы	CitrixOnline/GoToMeeting, Lotus Notes, WebEx
аудио- и видеопотоки	Adobe Flash, Apple iTunes, AVI, Feidian, Grooveshark, Icecast, Last.fm, MPEG, Netflix, OGG, QuickTime, RealMedia, RTSP, RuTube, Spotify, WebM, Windowsmedia, YouTube
аутентификация	Kerberos, LDAP, RADIUS, XDMCP
веб-сервисы	Google, Google Maps, Mail.ru, Rambler.ru, Yahoo!, Яндекс
игровые сервисы / гейм-трафик	Armagetron, Battlefield, Crossfire, Dofus, Fiesta, Florensia, GTP, GuildWars, Halflife2, MapleStory, Quake, Steam, WARCRAFT 3, World of Kung Fu, World of Warcraft, XBOX
интернет ТВ	PPLive, PPStream, QQLive, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, Zattoo
корпоративные сервисы	Kontiki, SAP, Vmware



нераспознанное	TCP unknown, UDP unknown, Нераспознанное
облачные хранилища	Apple iCloud, Dropbox, Ubuntu One
почта	Gmail, IMAP, POP3, SkyFile Rudics, SkyFile постоплатный, SkyFile предоплатный, SMTP
служебные протоколы	BGP, DCE/RPC, DHCP, DHCPv6, DNS, EGP, GRE, i23v5, ICMP, ICMPv6, IGMP, IP in IP, IPP, LLMNR, MDNS, MOVE, NETBIOS, NetFlow, NOE, NTP, OSPF, PPTP, RemoteScan, SCTP, sFlow, SNMP, Socrates, SSDP, STUN, Syslog, UPnP, VRRP

социальные сети	facebook, Tuenti, Twitter, ВКонтакте, Одноклассники
СУБД	MSSQL, MySQL, Oracle, PostgreSQL, TDS
удаленный доступ	Citrix, PcAnywhere, RDP, TeamViewer, TELNET, VNC
файлы	AFP, FTP, NFS, Rsync, SMB, TFTP, Usenet, Windows Update
шифрованные протоколы	CiscoVPN, Cobra, HTTP Connect (SSL over HTTP), IPSEC, OpenVPN SSH, SSL, SSL без сертификата, Tor

классификатор может быть расширен под специфические требования заказчика

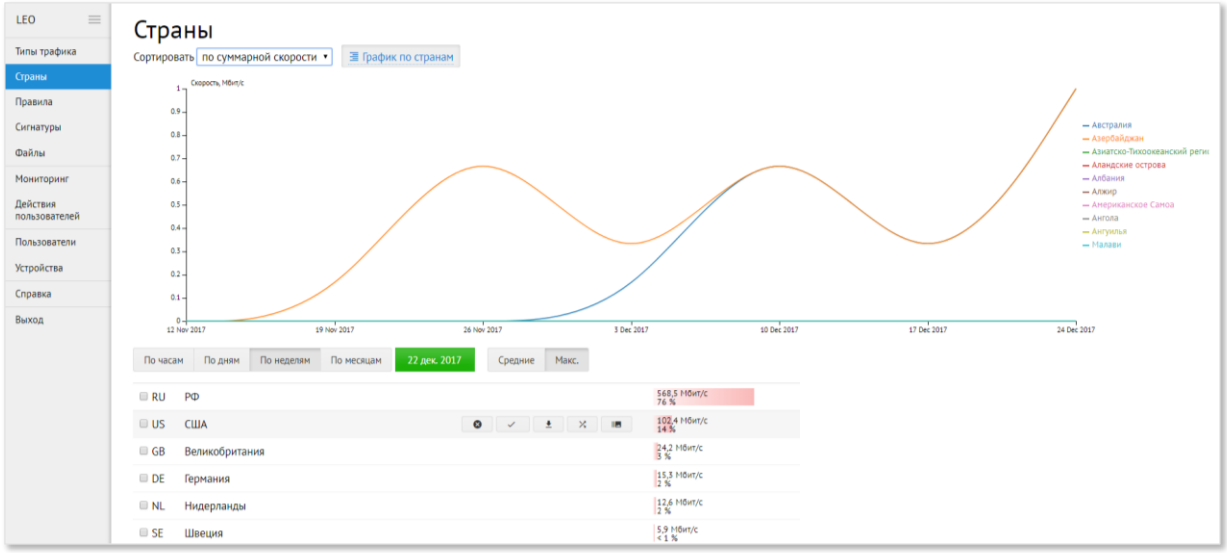
LEO. Классификатор стран. Мониторинг и статистика

классификатор стран

встроенный классификатор стран на основе базы данных геолокации

классификация входящего трафика на страну

классификация исходящего трафика на страну



мониторинг и статистика

мониторинг в реальном времени

долговременное накопление и агрегация статистики

статистика по типам трафика / странам

журнал действий пользователя

система управления правами доступа