

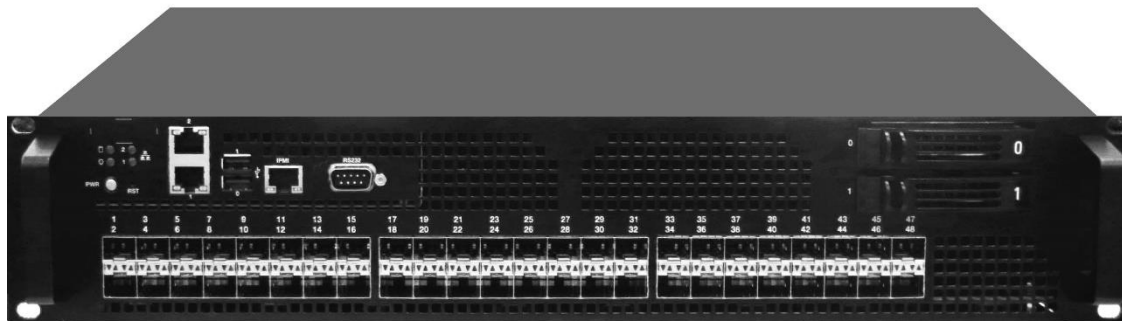
Leo^{L7 DPI}

A Multilevel Analysis and Traffic Filter Device

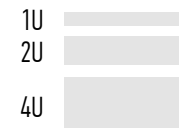
LEO is a hardware device for IP-traffic monitoring and filtration on high bandwidth lines up to 100 Gbit/s based on:

- specified criteria,
- real-time mode,
- zero packet loss.

LEO is used for addressing a wide variety of complex network challenges. The device is capable to deploy it's feature set scaling up to IPS systems and LIS Solution.



form factor



LEO Meets Effectively Three Principal Types of Challenges

Aggregation and Balancing

Traffic Analysis

Traffic Filtering

- Makes traffic analysis in the carrier network:
 - detects bottlenecks and the loaded protocols, specifies the traffic sources by countries, etc.;
 - records data on a disk;
 - determines peak periods by inbound/output traffic, etc.;
 - conducts on-line monitoring.
- Blocks undesirable types of traffic.
- Forwards inbound traffic to other network interfaces for further analysis.

⚠ *To work correctly LEO should receive all the packages with content traffic and control heading data.*

⚠ *Up to 64 GbE ports each of which can independently enable receiving /RX/ and transferring /TX/ data.*

LEO – a Versatile Network Filter

matching / rules

filter criteria	appliance type
	geolocation
	signature
	regular expressions
	IP-address, IP-IP, subnet /IP + Mask/
	port, port span
	subnet, subnet-subnet
	URL
	login on the authorization server
	IMSI

ID	Rule	Action	Deadline	Speed
7	Lanister log-in	Record	05.01.2018 15:16	0 bit/s 0%
6	Port 53	Block	28.12.2017 15:14	160.4 kbps < 1%
5	Signature /List of IP127.0.0.1 + Challenge Handshake Authentication Protocol (Dxc223)	Block	30.12.2017 15:10	0 bit/s 0%
4	Signature / Traffic type AVI + ESP/IPSEC 03	Skip	07.01.2018 15:08	0 bit/s 0%
3	Country Arulco	Forward	28.12.2017 15:07	0 bit/s 0%
1	Traffic type HTTP	DocExtractor	∞	0 bit/s 0%
2	Traffic type WhatsApp	Block	31.12.2017 14:35	0 bit/s 0%

actions

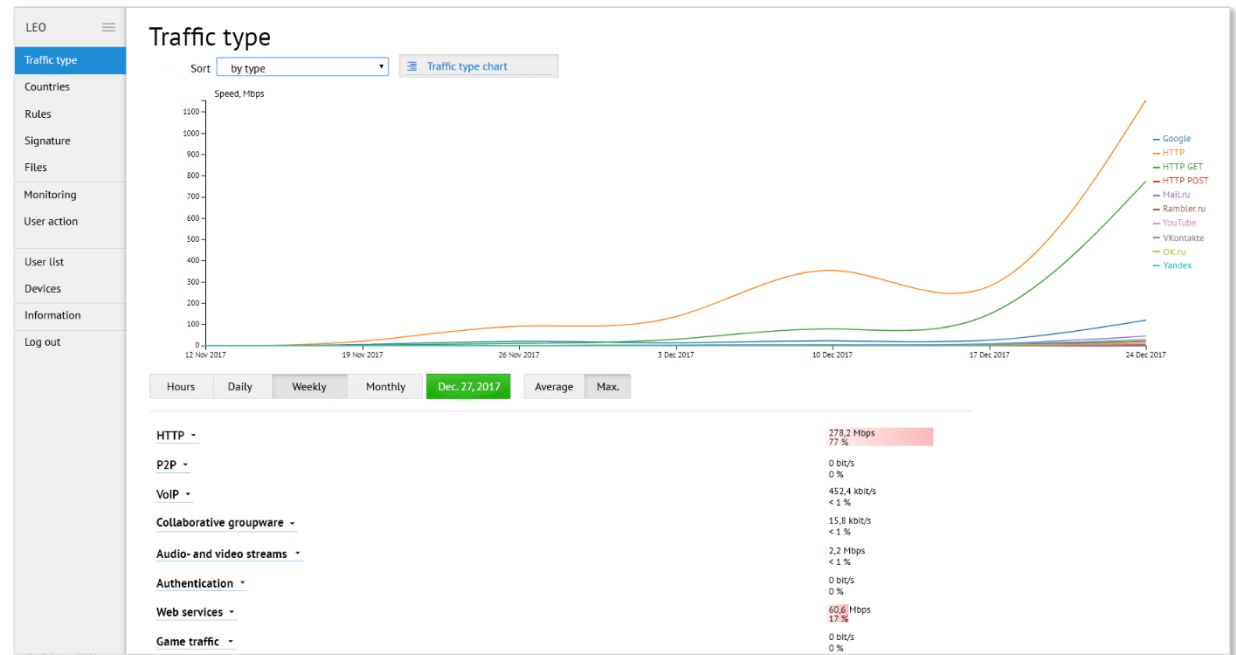
block	the Block Action is used when you install LEO inline to filter the unsolicited types of traffic off
record	Record Action provides a traffic recording of certain types for further analysis
forward	Forward Action can copy and/or select a part of a traffic flow and send it to the free network interface for example, to bypass filtering or sending data to the monitoring device
DocExtractor	DocExtractor Action can extract and export documents from the data stream
Traffic Shaping	a channel bandwidth limitation allows to control the traffic going out an interface, matching the traffic flow to the speed of the interface



application classifier

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
messengers / VoIP	Cisco skinny, FaceTime and iMessages, H.323, IAX, MGCP, RTCP, RTP, SIP, Skype, TeamSpeak, Truphone, Viber, Oscar, WathsApp, IRC, Jabber, meebo, MMS, MSN, OSCAR, Popo, QQ
collaborative groupware business applications	CitrixOnline/GoToMeeting, Lotus Notes, WebEx
audio- and video streams	Adobe Flash, Apple iTunes, AVI, Feidian, Grooveshark, Icecast, Last.fm, MPEG, Netflix, OGG, QuickTime, RealMedia, RTSP, RuTube, Spotify, WebM, Windowsmedia, YouTube
authentication	Kerberos, LDAP, RADIUS, XDMCP
web services	Google, Google Maps, Mail.ru, Rambler.ru, Yahoo!, Yandex
game services / game traffic	Armagetron, Battlefield, Crossfire, Dofus, Fiesta, Florensia, GTP, GuildWars, Halflife2, MapleStory, Quake, Steam, WARCRAFT 3, World of Kung Fu, World of Warcraft, XBOX
streaming video software	PPLive, PPStream, QQLive, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, Zattoo
corporate services	Kontiki, SAP, Vmware

LEO. Integrated Classifier for Identifying 180 Types of Applications



unrecognized	TCP unknown, UDP unknown, Unidentified
cloud storage services	Apple iCloud, Dropbox, Ubuntu One
mail	Gmail, IMAP, POP3, SkyFile Rudics, SkyFile post-paid, SkyFile pre-paid , SMTP
service protocols	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

social networks	facebook, Tuenti, Twitter, VKontakte, OK.ru
DBMS	MSSQL, MySQL, Oracle, PostgreSQL, TDS
remote access	Citrix, PcAnywhere, RDP, TeamViewer, TELNET, VNC
files	AFP, FTP, NFS, Rsync, SMB, TFTP, Usenet, Windows Update
encrypted protocols	CiscoVPN, Cobra, HTTP Connect (SSL over HTTP), IPSEC, OpenVPN SSH, SSL, SSL without a certificate, Tor

the classifier could be scaled to meet specific customer requirements

country classifier

integrated country classifier based on geolocation database

inbound traffic classifier by country

output traffic classifier by country

monitoring and statistics

real time monitoring

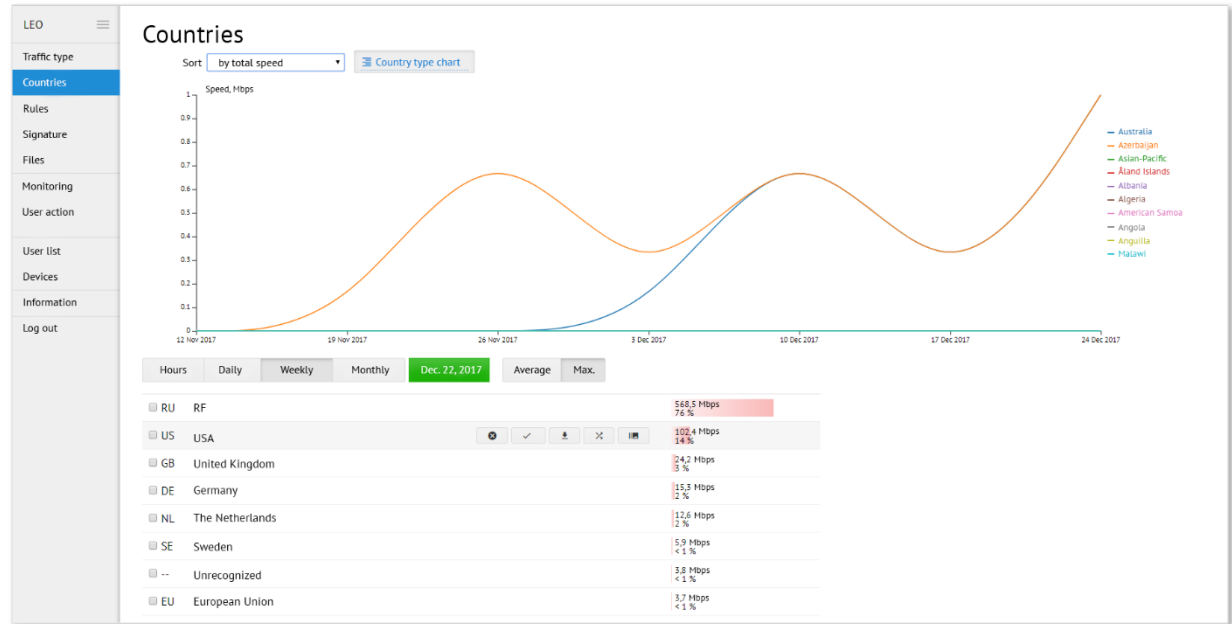
long-term statistics accumulating and aggregating

statistics by traffic types/countries

user actions history log

management of access rights

LEO. Country Classifier. Monitoring and Statistics



User action

All actions

Date	Action	User
22.12.2017 14:35	A new Rule "Traffic type WhatsApp" was created	admin
19.12.2017 14:02	A new Rule "Traffic type HTTP" was created	admin
22.12.2017 15:07	A new Rule "Country Arulco" was created	supervisor
22.12.2017 15:09	A new Rule "Signature / Traffic type AVI + ESP/IPSEC 03" was created	supervisor
22.12.2017 15:11	A new Rule "Signature / IP list 127.0.0.1/24, 192.168.0.1. + ESP/IPSEC 02" was created	supervisor
22.12.2017 15:11	A new Rule "Port 53" was created	petrov
22.12.2017 15:14	A new Rule "Lanister Login" was created	petrov
22.12.2017 15:16	A new Rule was created	petrov
22.12.2017 15:03	"supervisor" user account was created	admin
22.12.2017 15:13	"petrov" user account was created	admin
22.12.2017 15:19	The Rule "Traffic type WhatsApp" was edited	petrov
22.12.2017 15:17	The Rule "Traffic type WhatsApp" was edited	petrov
22.12.2017 15:16	The Rule "Traffic type WhatsApp" was edited	petrov
21.12.2017 19:50	The Rule "Traffic type HTTP" was disabled	admin
22.12.2017 14:27	Unauthorized Access Attempt	nobody
21.12.2017 16:35	Unauthorized Access Attempt	nobody
21.12.2017 16:35	Unauthorized Access Attempt	nobody