TRAFFIC INSPECTOR NEXT GENERATION®

Traffic Inspector Next Generation

Quick Setup Guide

SMART-SOFT®

Getting started

Connect the power adapter to the power socket on the Traffic Inspector Next Generation device. Connect the power adapter to the mains.

Use the null modem cable to connect the RS-232 serial port of the device with the corresponding port of the computer which will be used to control the device. This step is optional, unless you need terminal access via the serial port.

Use the Ethernet-cable to connect the LAN-adapter of Traffic Inspector Next Generation device to the network of the organization. By default, the device is administered via network from the LAN adapter side.

Supported administrative access types for Traffic Inspector Next Generation:

- Terminal access via RS-232 serial port
- Terminal access using SSH-client via SSH protocol
- Access to the file system of the device via SFTP protocol
- Access to the web interface via a web browser (HTTP/HTTPS protocol)
- Regardless of the access method, you will need login root and password ting for authorization.

If you are using network access methods, you need to call the IP address 192.168.1.1. This is the default IP address is assigned to the LAN adapter of Traffic Inspector Next Generation device.

Terminal access via RS-232 serial port

Use the popular terminal emulator / SSH-client to connect to RS-232 serial portputty.
Connection settings:

Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

Terminal access using SSH-client via SSH protocol

Use the popular terminal emulator / SSH-client for terminal access putty.

Getting started

Access to the file system of the device via SFTP protocol

Use the free software to access the file system of the device via SFTP protocolWinSCP.

Access to the web interface via a web browser (HTTP/HTTPS protocol)

The easiest way to administer Traffic Inspector Next Generation device is to access its web interface via a web browser. Upon first logon, run Initial setup wizard, activate the purchased license and update Traffic Inspector Next Generation.

Initial setup wizard

Go to System –> Wizard and run the Setup wizard.

Specify the name of Traffic Inspector Next Generation device, Active Directory domain name, DNS servers, time zone, NTP server, TCP/IP settings for external and internal gateway adapters and set the gateway administrator password. Upon the execution of the setup wizard ensure that you have Internet access at Traffic Inspector Next Generation device. Go to Interfaces –> Diagnostics –> Ping and try to ping any Internet resource by its symbolic name and IP address.

Note For license activation and Traffic Inspector Next Generation update a working Internet connection is required.

License installation

Go to Summary –> License

Enter the license key for the Traffic Inspector Next Generation product that you have purchased into the license key field. Click «Activate License».

Note You will need the license at the next stage when you will be updating Traffic Inspector Next Generation. If you have reinstalled the Traffic Inspector Next Generation operating system, you will have to recover your private device key before you install the license.

Updating Traffic Inspector Next Generation

Go to **System** –> **Firmware** –> **Updates** and click **Check for updates.**

Reboot the device after updating Traffic Inspector Next Generation.

Now you can proceed to configuring specific functionality of Traffic Inspector Next Generation. For more information refer to the sections of the manual which cover the specific functions.

Firewall configuration

Firewall functions:

- Protection of the TING device and the computers in the intranet from unauthorized access from the Internet.
- Network Address Translation
- Internal services publication (port forwarding)
- Internal users'' access control to the computers on the Internet.
- Package interception and forwarding them to the TING device itself (as a part of transparent proxying and SSL Bump functionality).

Firewall processes the packages according to the rules and directives stored in the configuration file /tmp/rules.debug. Do not manually change the contents of the file, as it is generated automatically, based on the settings from the web interface of the TING device.

Configure the firewall via the web interface of the TING device.

For your convenience firewall rules are set in the web interface individually for each adapter configured in the system. The rules are presented in the form of the list. The network package is checked against the criteria in the list top down.

If the network package meets the criteria, the package is processed according the the matching rule. If rule was applied to the package, it is no longer processed by the firewall. This package will not be checked against other criteria in the list.

Block and Reject actions lead to blocking of the package by the firewall (note that in the first case – blocking – the other side is not anyhow notified of it). Pass action allows the package through the firewall and creates a state.

If the network package does not meet any criteria set in the rules, it is blocked and discarded (i.e. without notification to the remote side).

The order of the rules in the list is important and can be managed.

Firewall of Traffic Inspector Next Generation supports stateful packet inspection. This method allows not to examine each package individually, rather it implies the existence of connections, i.e. sequences of packages which are closely related to each other and which make up a interaction sessions between two hosts.

If the processed package can be associated with an existing connection (i.e. there is a corresponding status record), this package will not be checked against the filtering rules, which in turn significantly speeds up package processing for established connections.

Firewall rules also allow to redirect packages and network address translation (NAT).

Firewall configuration

Network address translation functionality is commonly known as ‘sharing Internet access in the Ethernet ’. In the most general scenario the company will be allocated one ‘whitelist’ IP-address which will be assigned to WAN adapter of Traffic Inspector Next Generation gateway. Computers in the Ethernet are configured using ‘grey list’ IP addresses (IP addresses from the range listed in RFC 1918). In order to work on the Internet, the computers connected to the Ethernet must have whitelist IP addresses. Ethernet computer do not have such addresses, so if they need to connect to the computers on the Internet their traffic has to go through Traffic Inspector Next Generation gateway. The gateway does not simply route the packages, it also rewrites the address of the source (and source port) of the packages if necessary. This method of package processing results in the situation when the computers in the Ethernet operate in the Internet under the ‘whitelist’ IP address of the WAN adapter of the gateway. The gateway itself can also operate under this address. Traffic Inspector Next Generation device tracks the connections and performs all the necessary direct and reverse address translations in packages.

Aliases

Aliases are a convenient mechanism of naming lists of hosts, networks, ports for the purposes of making firewall rules. In the event of input data changes, aliases reduce the number of chances made to the firewall rules.

Types of aliases

Types of aliases in TING:

Host(s)	Singke hosts specified by IP address or by FQDN name (**mydomain.com** or **192.168.1.11**)
Network(s)	Address of networks in IPv4 or IPv6 format (e.g., **192.0.0.0/24**)
Port(s)	Port number or port range, separated by a colon (**2000:3000**)
URL (IP address)	List of IP addresses, downloaded from a specified URL once
URL (IP address) table	List of IP addresses, downloaded from a specified URL with a set interval
GeoIP	Country or region
External (extended)	External alias (announcement only)

Firewall configuration

Pre-defined rules

By default the firewall has the following presets:

1. It blocks any unauthorized access form the Internet either to the TING device or to any computer in the Ethernet.
2. Allows the users in the Ethernet to freely access the computers in the Internet.
3. Ensures network address translation for computers in the Ethernet (NAT functionality)
4. Protects the user from self-blocking during access via web interface or SSH

Settings for (1) can be found in the section Firewall –> Rules on WAN tab (nothing allowed).

Settings for (2) are the following preset rules: Default allow LAN to any rule and Default allow LAN IPv6 to any rule in Firewall –> Rules on WAN thanks to which you can have any type of access to the gateway itself (gateway LAN adapter) and the Internet. Any responding traffic from the internet will freely pass the firewall.

Settings for (3) are the rules automatically created in the section Firewall –> NAT ->Outgoing

Settings for (4) are the preset Anti-blocking rule in the section Firewall –> Rules on LAN tab. This rule is at the top of the list, it cannot be neither moved nor deleted, and allows access to TCP ports 22 (SSH), 80 (HTTP), 443 (HTTPS). It means that any forbidding rule for such ports which is below the preset rule will have no effect and will not block access to the admin functions of TING. The other preset Anti-blocking rule in the section Firewall –> NAT –> Port Forwarding. This rule is at the top of the list, it cannot be neither moved nor deleted, and forbids redirect for TCP ports 22 (SSH), 80 (HTTP), 443 (HTTPS). It means that any redirect rule for such ports which is below the preset rule will have no effect and will not block access to the admin functions of TING.

Creating rules

You may need to create rules to:

- allow access to the TING device from the Internet;
- deny access to the Internet (IP address / protocol / port filtering) for Ethernet users;
- allow access to services executed on hosts in the internal LAN (port forwarding).

Access to the TING device from the Internet

E.g.: Let’s allow a connection from the WAN adapter side via SSH protocol to the Traffic Inspector Next Generation gateway.

Firewall configuration

Go to **Firewall** –>**Rules**, **WAN** tab. Click + to create a new rule. Create the rule with the following settings:

Action	Permission
Interface	WAN
TCP / IP version	IPv4
Protocol	TCP
Source	Any
Source ports range	Any - any
Beneficiary	WAN address
Target ports range	SSH
Description	Rules allowing SSH connection from the Internet

Click **Save** to apply the settings.

Blocking Internet access

E.g.: Let’s forbid access to the Internet for the Ethernet users via HTTPS protocol.

Firewall configuration

Go to **Firewall** –>**Rules, LAN** tab. Click + to create a new rule. Create the rule with the following settings:

Action	Permission
Interface	LAN
TCP / IP version	IPv4
Protocol	TCP
Sender	LAN
Source ports range	Any - any
Beneficiary	Any
Target ports range	HTTPS
Description	Rule for forbidding Internet connections via HTTPS

Click **Save** to apply the settings.

Port forwarding

NAT allows Internet access to several computers under a single 'whitelist' IP address. However, this mechanism makes it difficult to access Ethernet computers from the Internet, which in turn requires a separate setting, known as port forwarding.

E.g.: Let's allow access to a website in the Ethernet from the Internet. The website is on the computer with the IP address 192.168.1.80 and is listening port 80.

Firewall configuration

Go to **Firewall** –> **NAT** –> **Forwarding** Click Add button in the top right corner to create a new rule. Create the rule with the following settings:

Interface	WAN
TCP / IP version	IPv4
Protocol	TCP
Source	Any
Source ports range	Any - any
Beneficiary	WAN address
Target ports range	HTTP - HTTP
Redirect URL	192.168.1.80
Redirection port	HTTP
Description	Web server publication in the Internet
Mirror NAT	Enable (clean NAT)
Associated firewall rule	Add associated rule

Apart from creating a forwarding rule, you will have to create a rule for allowing translated traffic. This additional rule is created automatically if you enable **Add associated rule** while creating the main rule.

Firewall configuration

Here is an example of creating an additional rule for our scenario. Go to **Firewall** –>**Rules**, **WAN** tab. Click + to create a new rule. Create the rule with the following settings:

Action	Permission
Interface	WAN
TCP / IP version	IPv4
Protocol	TCP
Source	Any
Source ports range	Any - any
Address	192.168.1.80
Target ports range	80– 80
Description	Rule for allowing translated traffic

Internet users can now call <WAN adapter IP address: port 80> and will we redirected to the computer in the Ethernet, i.e. to <192.168.1.80:80>.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Intrusion Detection/ Prevention System (hereinafter IDS/IPS) in Traffic Inspector Next Generation is based on Suricata software and uses NETMAP package capture method to improve performance and minimize CPU load.

IDS/IPS significantly improves network security. IDS/IPS capabilities:

- Notify about compromised SSL-of certificates and prevent their use
- Notify about vulnerabilities in DNS, FTP, ICMP, IMAP, POP3, HTTP, NetBIOS, DCERPC, SNMP, TFTP, VOIP protocols and prevent their use
- Notify about exploits and vulnerabilities of network applications and prevent their use
- Prevent and block DOS attacks
- Notify about network scan events and block them
- Block botnet traffic
- Block traffic from compromised hosts
- Block traffic from hosts infected with trojan software and net worms
- Block traffic from spam networks.

IPS/IDS settings

Turn off Hardware Offloading mode

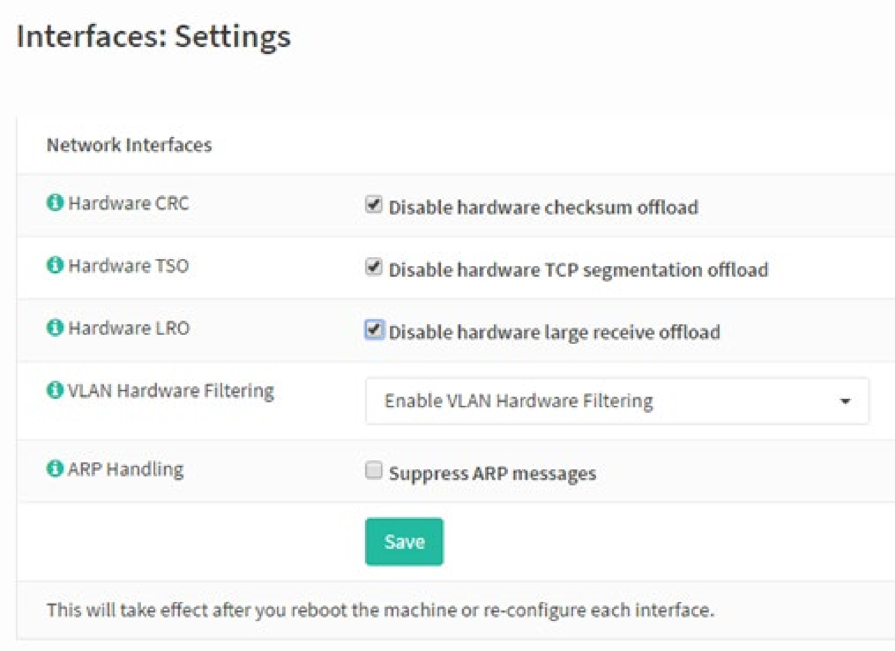
Go to **Interfaces** -> **Settings**. Clear the check boxes for Hardware Offloading mechanisms.

Modern network cards and their drivers provide a number of technologies that enable faster packet processing by shifting some aspects of their processing to the hardware components of the card itself. Examples of such technologies include: Hardware CRC, Hardware TSO, Hardware LRO.

Hardware CRC	Calculating the Ethernet frame checksum using the network card alone, not the CPU.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Hardware TSO (TCP Segmentation Offload)	TCP packet segmenting using network card hardware capabilities, with no CPU use.
Hardware LRO (Large Receive Offload)	Incoming packets buffering and sending them to the network stack in aggregate from to avoid inefficient transmission of each individual packet. These mechanisms need to be disabled when using IDS/IPS as their logic is not compatible with Netmap Fast Packet I/O mechanism.



Interfaces: Settings

Network Interfaces

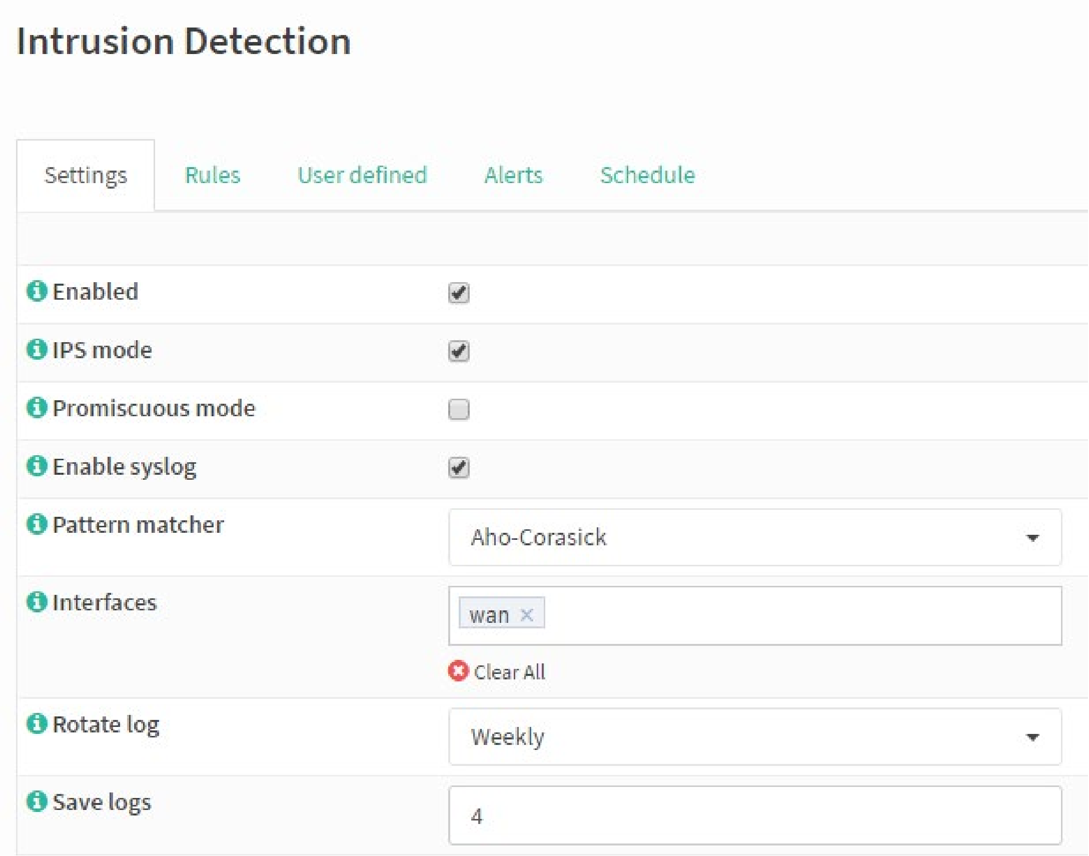
Hardware CRC	☑ Disable hardware checksum offload
Hardware TSO	☑ Disable hardware TCP segmentation offload
Hardware LRO	☑ Disable hardware large receive offload
VLAN Hardware Filtering	Enable VLAN Hardware Filtering
ARP Handling	☐ Suppress ARP messages

This will take effect after you reboot the machine or re-configure each interface.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Main IPS/IDS settings

Go to **Services** -> **Intrusion Detection** on the **Settings** tab.



Intrusion Detection

Enabled ☑

IPS mode ☑

Promiscuous mode □

Enable syslog ☑

Pattern matcher: Aho-Corasick

Interfaces: wan ×

Rotate log: Weekly

Save logs: 4

Tick **Enabled** check box to enable IDS.

Tick **IPS mode** check box to not only detect but also block malicious network activity.

Promiscuous mode flag enables the so-called unintelligible packet capture mode, which can be useful when IDS/IPS is used on a computer with VLAN interfaces.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

IDs/IPS writes warnings to **/var/log/suricata/eve.json.** If you want the IDS/IPS system to add messages to the syslog, tick the **Enable syslog** check box.

Configuring **Pattern matcher** Here you need to select the substring search algorithm used for packet processing.

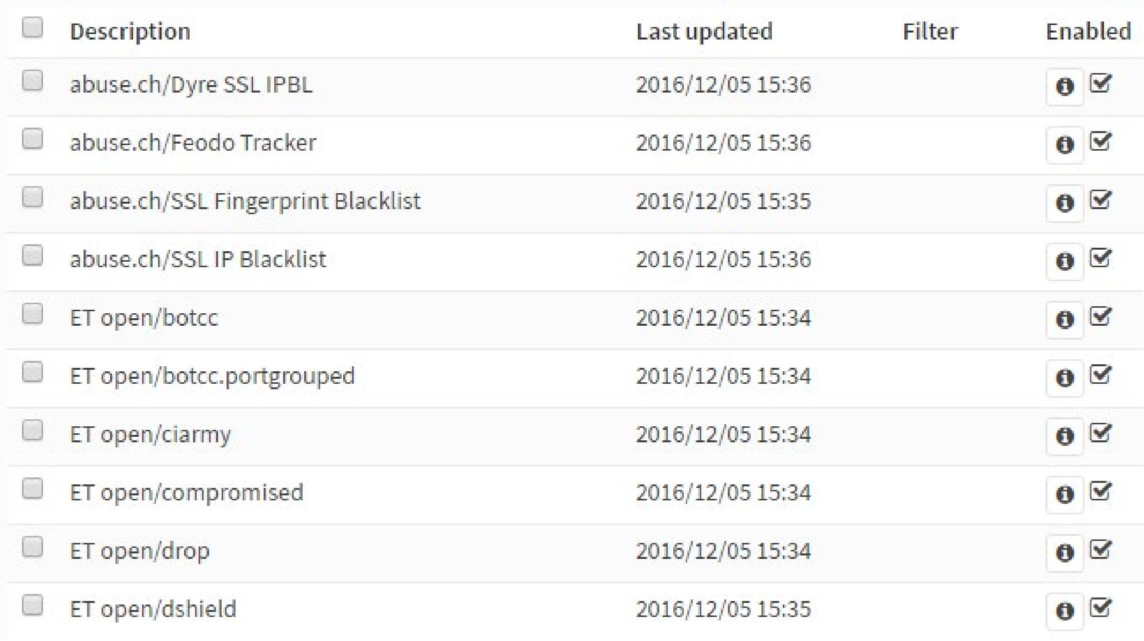
Configuring **Interfaces.** Here you have to select the interface that IDS/IPS will listen to.

Rotate log and **Save logs** settings control how often the alert log files are to be rotated and how many log files are to be rerotated respectively.

Loading rule lists

The IDS/IPS system operates according to established lists and enabled rules.

Go to **Services** -> **Intrusion Detection** on the **Settings tab**, configure **Rulesets** tab.



□	Description	Last updated	Filter	Enabled
□	abuse.ch/Dyre SSL IPBL	2016/12/05 15:36		ℹ ☑
□	abuse.ch/Feodo Tracker	2016/12/05 15:36		ℹ ☑
□	abuse.ch/SSL Fingerprint Blacklist	2016/12/05 15:35		ℹ ☑
□	abuse.ch/SSL IP Blacklist	2016/12/05 15:36		ℹ ☑
□	ET open/botcc	2016/12/05 15:34		ℹ ☑
□	ET open/botcc.portgrouped	2016/12/05 15:34		ℹ ☑
□	ET open/ciarmy	2016/12/05 15:34		ℹ ☑
□	ET open/compromised	2016/12/05 15:34		ℹ ☑
□	ET open/drop	2016/12/05 15:34		ℹ ☑
□	ET open/dshield	2016/12/05 15:35		ℹ ☑

Here you can set / delete and enable / disable rule lists for IDS/IPS.

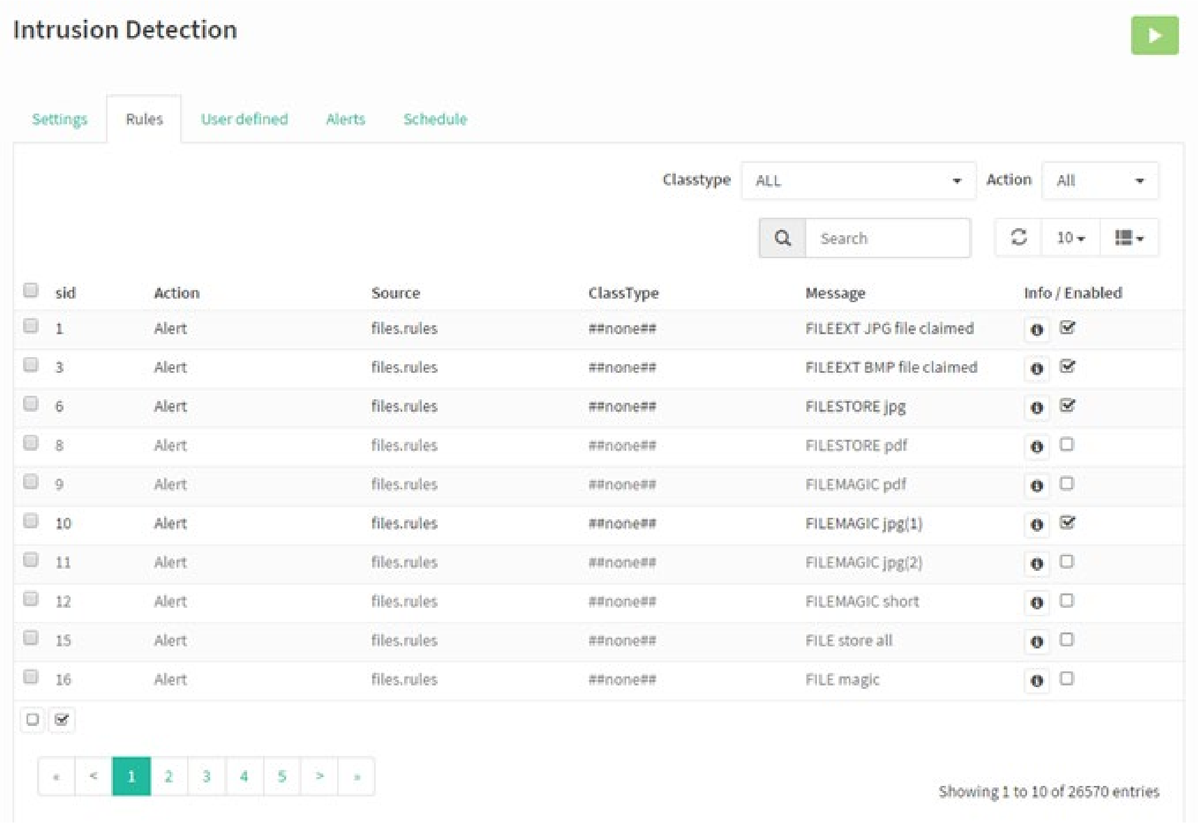
Select the required rule list. Select the check box next to this rule list and click **Download and Update Rules**.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Configure rules

After downloading the list, all the rules defined in it appear in **Services**-> **Intrusion Detection** -> **Rules.**

Enable the required rules (tick the check box next to the list of rules in **Enabled** column).



Intrusion Detection

Classtype: ALL
Action: All

☐	sid	Action	Source	ClassType	Message	Info / Enabled
☐	1	Alert	files.rules	##none##	FILEEXT JPG file claimed	☑
☐	3	Alert	files.rules	##none##	FILEEXT BMP file claimed	☑
☐	6	Alert	files.rules	##none##	FILESTORE jpg	☑
☐	8	Alert	files.rules	##none##	FILESTORE pdf	☐
☐	9	Alert	files.rules	##none##	FILEMAGIC pdf	☐
☐	10	Alert	files.rules	##none##	FILEMAGIC jpg(1)	☑
☐	11	Alert	files.rules	##none##	FILEMAGIC jpg(2)	☐
☐	12	Alert	files.rules	##none##	FILEMAGIC short	☐
☐	15	Alert	files.rules	##none##	FILE store all	☐
☐	16	Alert	files.rules	##none##	FILE magic	☐

Showing 1 to 10 of 26570 entries

Go to the rule properties (Info icon) and set the required administrative action –**Alert** or **Drop**. Click the **Apply** button.

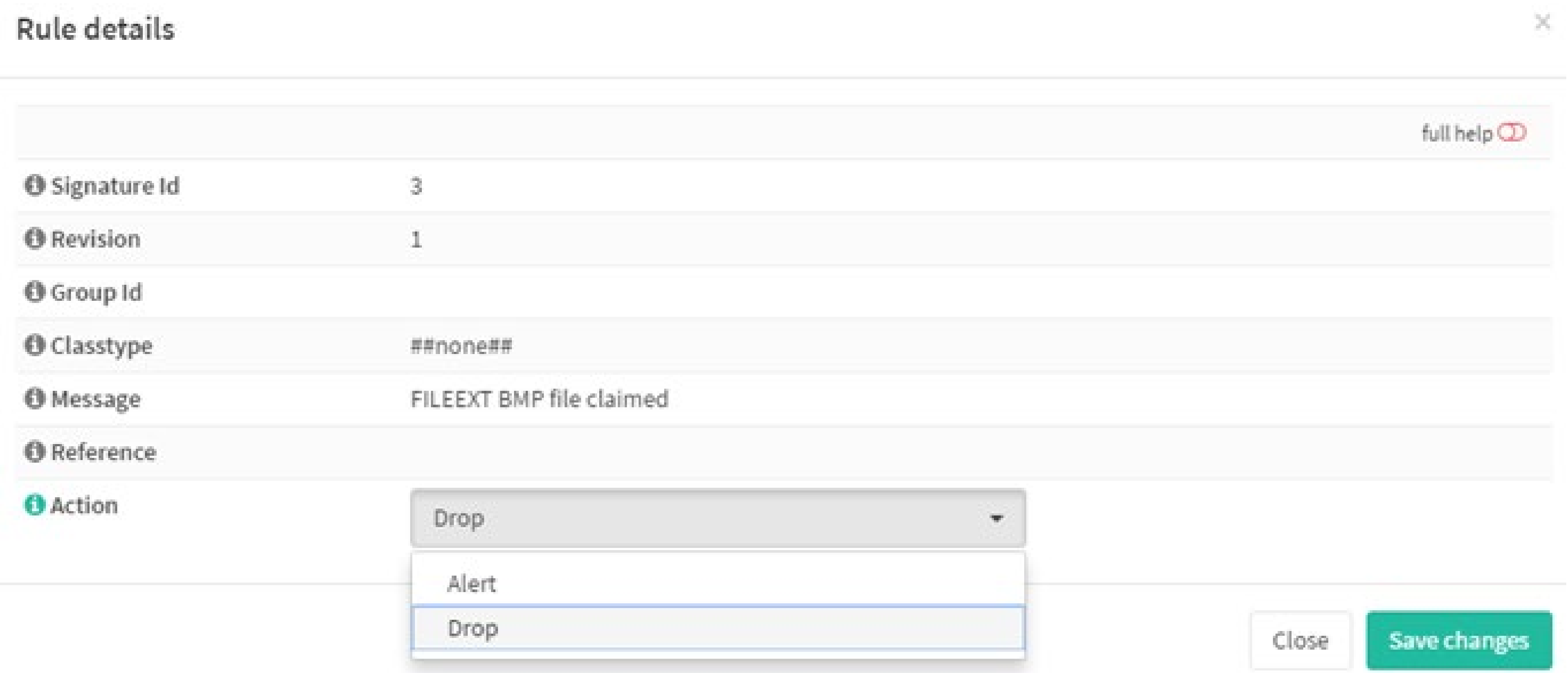
Intrusion Detection and Prevention System Configuration (IDS/IPS)

Alert administrative action

If a rule is triggered by **Alert** action, the IDS/IPS system will send a warning to the program’s web interface and syslog.

Administrative action Drop

If a rule is triggered with **Drop** action, the IDS/IPS system blocks suspicious network activity.



Rule details

Signature Id	3
Revision	1
Group Id	
Classtype	##none##
Message	FILEEXT BMP file claimed
Reference	
Action	Drop

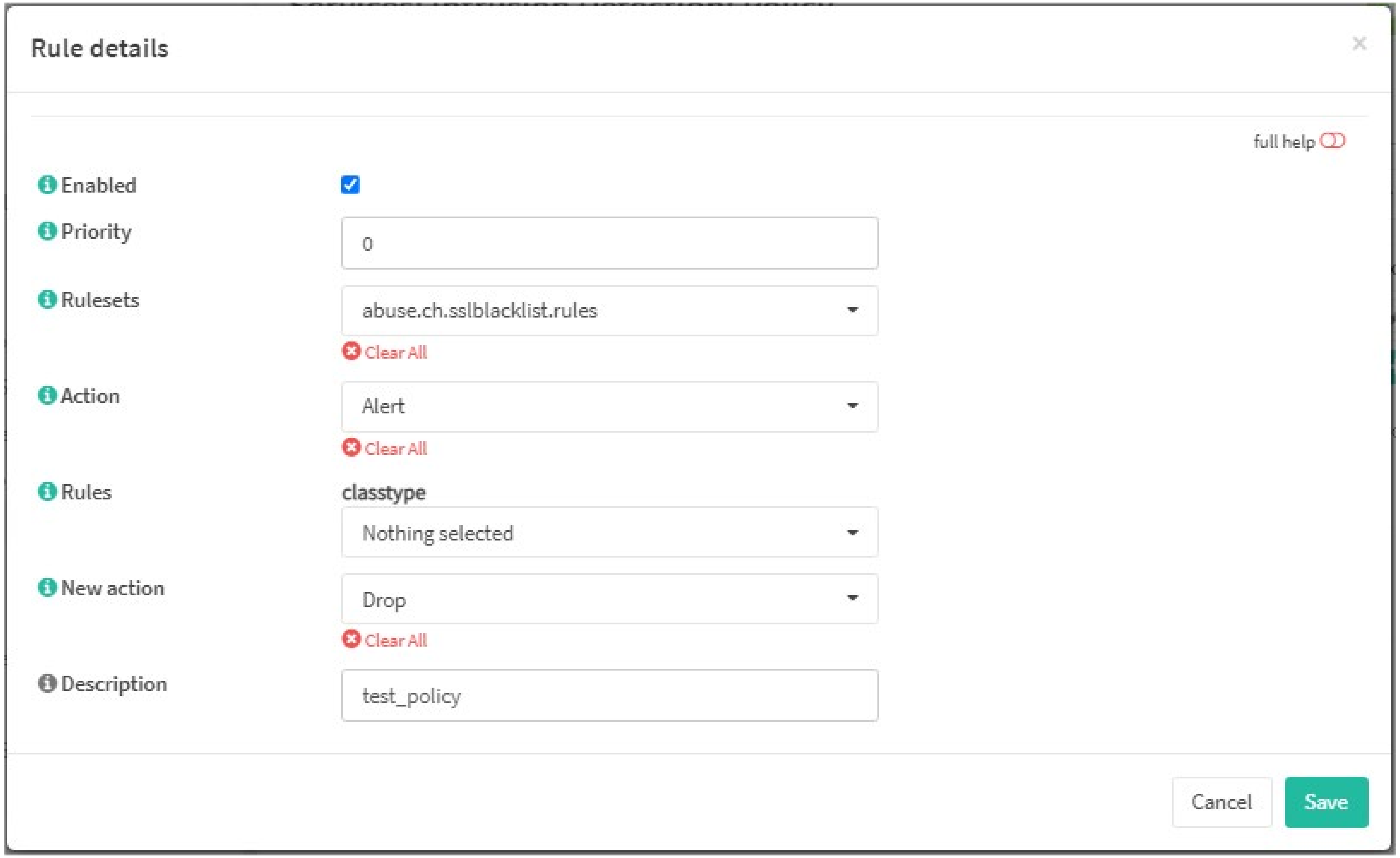
Intrusion Detection and Prevention System Configuration (IDS/IPS)

Policies configuring

Policies allow you to manage rule sets based on your chosen criteria and help you control which rules you want to use and how.

Suppose we have rules from ET open/emerging-scan, ET open/emerging-dos and ET open/emerging-exploit set enabled

In TING Services menu: Intrusion detection: Policy. Create a new policy on the Policies tab.



Rule details

full help

Enabled	☑
Priority	0
Rulesets	abuse.ch.sslblacklist.rules
Action	Alert
Rules	classtype: Nothing selected
New action	Drop
Description	test_policy

Enable the policy by ticking Enabled check box.

The priority is left by default.

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Note

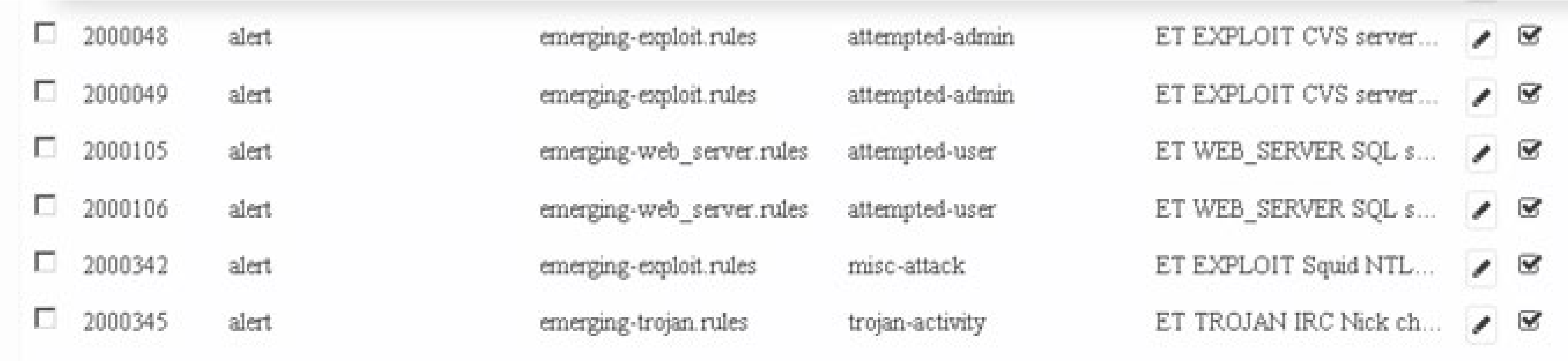
Overlapping policies are processed sequentially, a policy with a lower number has a higher priority.

Select the rule sets to which the policy applies and the action configured for the rule (disabled by default, warning, or deletion).

The following is a set of metadata collected from established rules. It contains settings such as the affected product (Android, Firefox, etc.) and deployment (data center, perimeter, etc.)

You can see which metadata matches the rules in the Services menu: Intrusion detection: Administration: Select the required metadata in Rules in Filter row.

Services: Intrusion Detection: Administration



□	2000048	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server...	✎	☑
□	2000049	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server...	✎	☑
□	2000105	alert	emerging-web_server.rules	attempted-user	ET WEB_SERVER SQL s...	✎	☑
□	2000106	alert	emerging-web_server.rules	attempted-user	ET WEB_SERVER SQL s...	✎	☑
□	2000342	alert	emerging-exploit.rules	misc-attack	ET EXPLOIT Squid NTL...	✎	☑
□	2000345	alert	emerging-trojan.rules	trojan-activity	ET TROJAN IRC Nick ch...	✎	☑

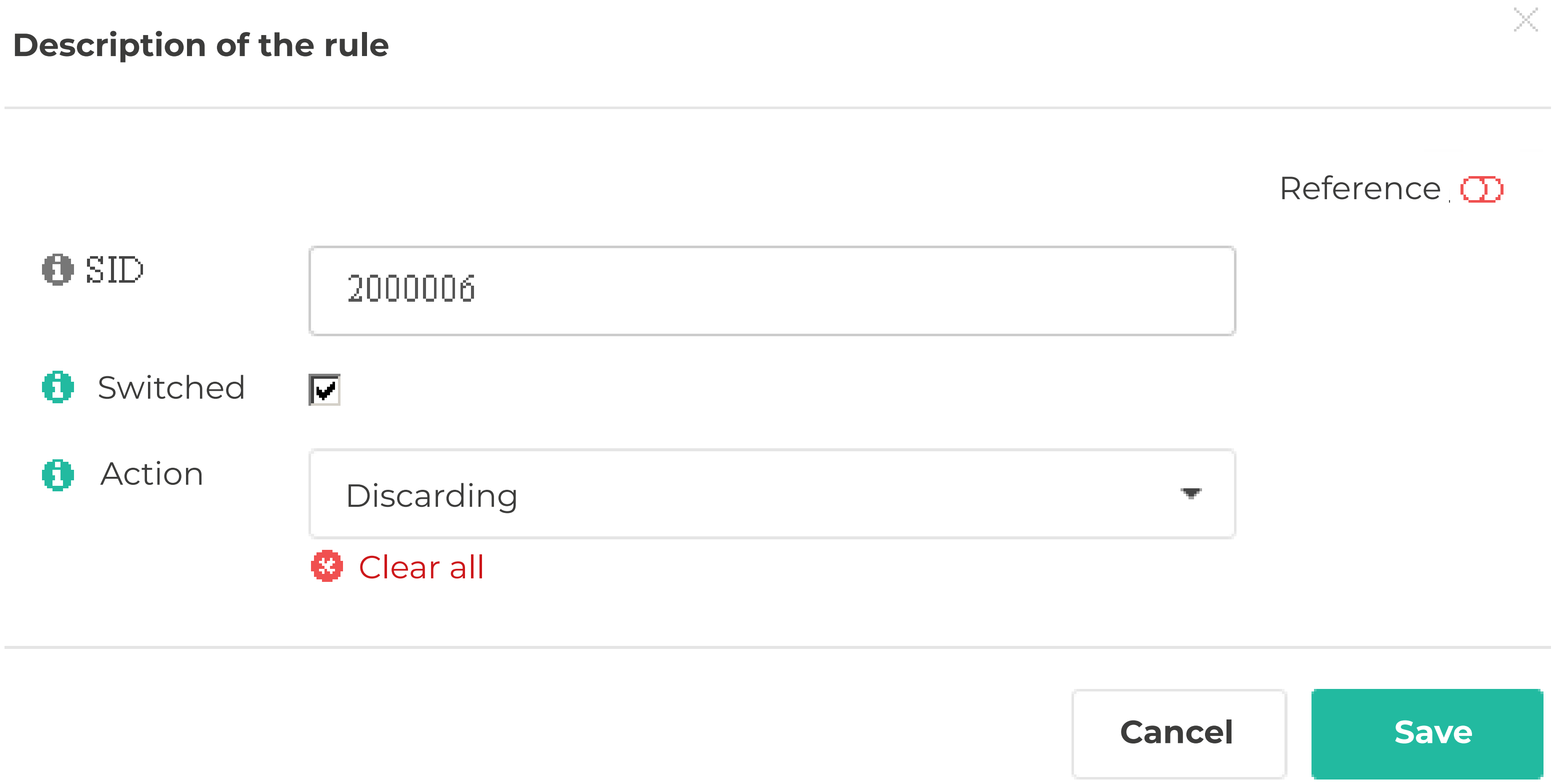
For example, if you select affected_product - Apache_HTTP_server, you will get a list of rules that the product matches.

The final step in setting the policy is the New Action field. This is the action that will be applied to the selected rules: warning, discard, disable.

Setup is complete.

Rule adjustment tab allows you to manually change the action for a specific rule.

Intrusion Detection and Prevention System Configuration (IDS/IPS)



Description of the rule

Reference

SID: 2000006

Switched: ☑

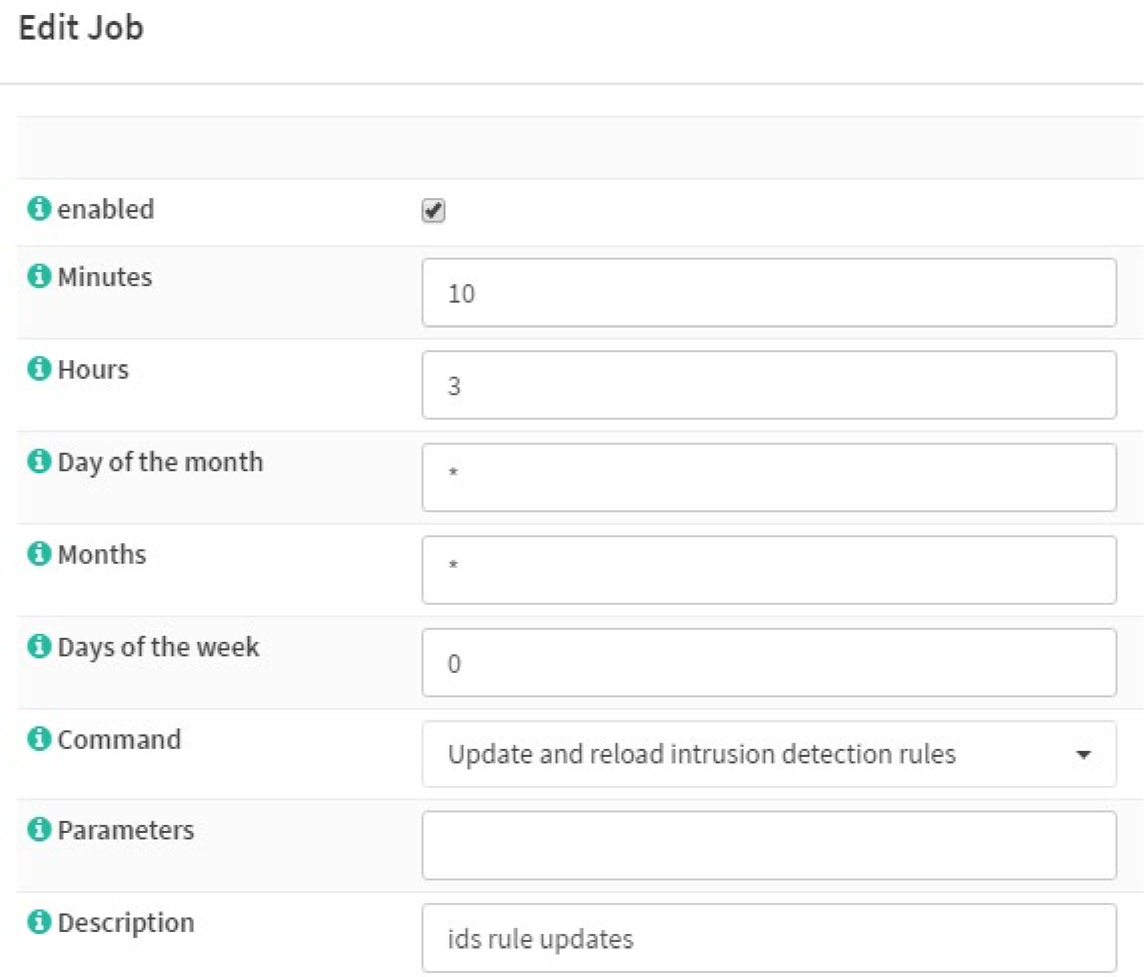
Action: Discarding

Note The SID can be viewed in the Service menu: Intrusion detection: Administration: Rules

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Automatic scheduled rule updates

Automatic scheduled rule updates supported. To configure this feature, go to **Services** -> **Intrusion Detection** -> **Schedule** and specify the update download interval.



Edit Job

enabled	☑
Minutes	10
Hours	3
Day of the month	*
Months	*
Days of the week	0
Command	Update and reload intrusion detection rules
Parameters	
Description	ids rule updates

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Enabled flag. Check this box to enable automatic scheduled rule updates.

Minutes field. Specifies the minutes when the update should be performed.

Hours field. Specifies the hours when the update should be performed.

Day of the month field. Specifies the days of the month when the update should be performed.

Months field. Specifies the months when the update should be performed.

Days of the Week field. Specifies the days of the week when the update should be performed.

Command field. This field must be set to **Update and reload intrusion detection rules.**

Parameters field. Optional field, can be left blank.

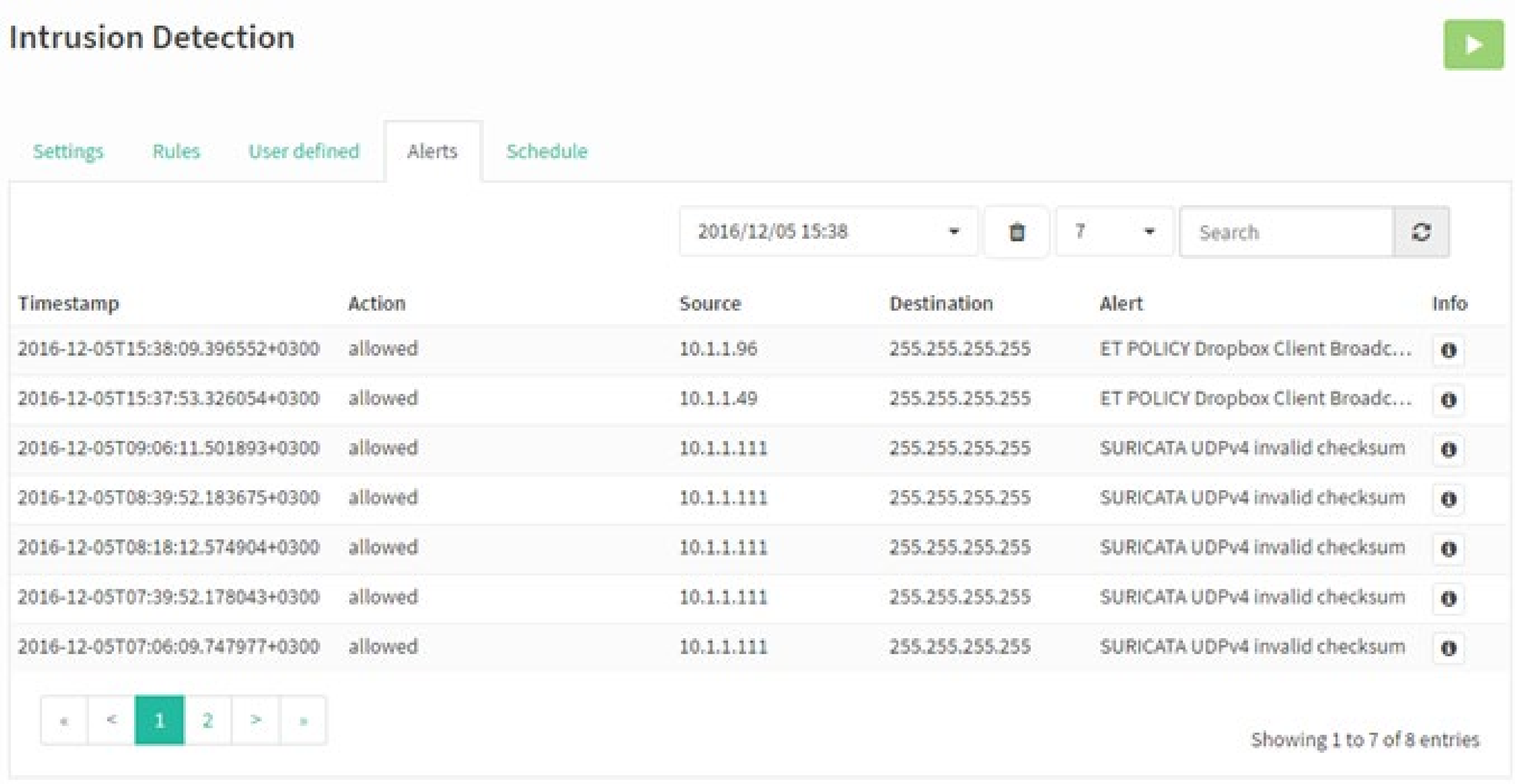
Description field. Specifies an arbitrary and user-friendly cron task name. In our case, we type **ids rule updates.**

Intrusion Detection and Prevention System Configuration (IDS/IPS)

Example of IDS/IPS alerts

If a rule is triggered with **Alert** action, IDS/IPS will issue a warning to **Services** -> **Intrusion Detection** -> **Web interface alerts**(corresponds to /**var/log/suricata/eve.json**).

Additionally, if **Enable syslog** flag is set in IDS/IPS general settings, a warning is also written to syslog.



Timestamp	Action	Source	Destination	Alert	Info
2016-12-05T15:38:09.396552+0300	allowed	10.1.1.96	255.255.255.255	ET POLICY Dropbox Client Broadc…	●
2016-12-05T15:37:53.326054+0300	allowed	10.1.1.49	255.255.255.255	ET POLICY Dropbox Client Broadc…	●
2016-12-05T09:06:11.501893+0300	allowed	10.1.1.111	255.255.255.255	SURICATA UDPv4 invalid checksum	●
2016-12-05T08:39:52.183675+0300	allowed	10.1.1.111	255.255.255.255	SURICATA UDPv4 invalid checksum	●
2016-12-05T08:18:12.574904+0300	allowed	10.1.1.111	255.255.255.255	SURICATA UDPv4 invalid checksum	●
2016-12-05T07:39:52.178043+0300	allowed	10.1.1.111	255.255.255.255	SURICATA UDPv4 invalid checksum	●
2016-12-05T07:06:09.747977+0300	allowed	10.1.1.111	255.255.255.255	SURICATA UDPv4 invalid checksum	●

Showing 1 to 7 of 8 entries

Rules lists

https://sslbl.abuse.ch/

SSL Blacklist contains lists of «bad» SSL certificates, i.e. certificates that have been used by malware and botnests. The lists contain SHA1 public key prints from SSL certificates.

---

https://feodotracker.abuse.ch/

Feodo Tracker - list of management servers for Feodo Trojan. Feodo (also known as Cridex or Bugat) is used by attackers to steal sensitive electronic banking data (credit card data, logins/passwords) from users' computers. There are currently four versions of the Trojan (versions A, B, C, and D), mainly distinguished by the management server infrastructure.

---

https://rules.emergingthreats.net/open/suricata/rules/botcc.rules

These rules describe known botnets and management servers. Sources: Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker.

---

https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules

These rules describe malicious hosts by www.cinsarmy.com project classification.

---

https://rules.emergingthreats.net/open/suricata/rules/compromised.rules

These rules describe known compromised and malicious hosts. Sources: Daniel Gerzo's BruteForceBlocker, the OpenBL, emerging threats Sandnet, SidReporter Projects.

---

https://rules.emergingthreats.net/open/suricata/rules/drop.rules

These rules describe spam host / networks according to www.spamhaus.org project classification.

---

https://rules.emergingthreats.net/open/suricata/rules/dshield.rules

These rules describe malicious hosts by www.dshield.org project classification.

Rules lists

https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules

These rules contain signatures for the use of ActiveX content.

https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules

Rules that detect host behavior after successful attacks.

https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules

These rules describe the signs of accessing popular chats.

https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules

Temporary rules awaiting possible inclusion into permanent rule lists.

https://rules.emergingthreats.net/open/suricata/rules/emerging-deleted.rules

Outdated rules that are pending removal in future versions.

https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules

These rules contain signatures of vulnerabilities in DNS, indications of DNS being used by malicious software, and incorrect use of DNS.

https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules

These rules contain DOS-attack signatures.

https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules

These rules contain signatures of exploits.

Rules lists

https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules

These rules contain signatures of vulnerabilities in FTP, and indications that FTP is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules

These rules describe the signs of accessing popular gaming sites: World of Warcraft, Starcraft, etc..

https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules

These rules contain signatures of incorrect use of ICMP protocol.

https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules

These rules contain signatures of ICMP information messages.

https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules

These rules contain signatures of vulnerabilities in IMAP, and indications that IMAP is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules

These rules describe the symptoms of accessing unwanted resources.

https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules

These rules contain signatures of various vulnerabilities.

https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules

These rules contain signatures of malware that uses HTTP.

Rules lists

https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules

These rules contain signatures of various vulnerabilities.

https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules

These rules contain malware signatures for mobile platforms.

https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules

These rules contain signatures of vulnerabilities in NetBIOS, and indications of incorrect use of NetBIOS.

https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules

These rules describe the signs of accessing P2P networks (Bittorrent, Gnutella, Limewire).

https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules

These rules describe unwanted network activity (calling MySpace, Ebay).

https://rules.emergingthreats.net/open/suricata/rules/emerging-pop3.rules

These rules contain signatures of vulnerabilities in POP3, and indications that POP3 is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules

These rules contain signatures of vulnerabilities in RPC, and indications that RPC is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules

These rules contain signatures of vulnerabilities for SCADA systems.

Rules lists

https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules

These rules describe signs of activity related to network scanning (Nessus, Nikto, portscanning).

https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules

These rules describe signs of activity associated with attempts to gain shell access as a result of exploits.

https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules

These rules contain signatures of vulnerabilities in SMTP, and indications that SMTP is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-snmp.rules

These rules contain signatures of vulnerabilities in SNMP, and indications that SNMP is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules

These rules contain vulnerability signatures for SQL databases.

https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules

These rules contain signatures of vulnerabilities for telnet, and indications that telnet is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules

These rules contain signatures of vulnerabilities in TFTP, and indications that TFTP is not being used correctly.

https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules

These rules show signs of Trojan network activity.

Rules lists

https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules

These rules contain signs of suspicious and potentially dangerous HTTP clients (identified by the values in the HTTP header of the User-Agent).

https://rules.emergingthreats.net/open/suricata/rules/emerging-voip.rules

These rules contain signatures of vulnerabilities in VOIP protocol.

https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules

These rules contain signatures of web client vulnerabilities.

https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules

These rules contain signatures of web servers vulnerabilities.

https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules

These rules contain signatures of exploiting web application vulnerabilities.

https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules

These rules describe the signs of network worms.

Contacts

Smart-Soft®

☎ +7 495 775 59 91

✉ info@smart-soft.ru

www.smart-soft.ru