SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Система предотвращения вторжений

www.smart-soft.ru

1. Вступление

Система предотвращения вторжений Traffic Inspector Next Generation основана на проекте Suricata и использует Netmap для улучшения производительности и минимизации нагрузки на процессор.

Система предотвращения вторжений использует наработки свободных проектов abuse.ch и Emerging Threats.

Suricata осуществляет свою работ в соответствии с заданными правилами и списками. В Traffic Inspector Next Generation доступны следующие правила и списки:

- https://sslbl.abuse.ch/

SSL Blacklist содержит списки «плохих» SSL сертификатов, т.е. сертификатов, в отношении которых устнановлен факт их использования вредоносным ПО и ботнетами. В списках содержатся SHA1 отпечатки публичных ключей из SSL сертификатов.

- https://feodotracker.abuse.ch/

Feodo Tracker - список управляющих серверов для троянской программы Feodo. Feodo (также известный как Cridex или Bugat) используется злоумышленниками для кражи чувствительной информации в сфере электронного банкинга (данные по кредитным картам, логины/пароли) с компьютеров пользователей. В настоящее время существует четыре версии троянской программы (версии A, B, C и D), главным образом отличающиеся инфраструктурой управляющих серверов.

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

Данные правила описывают известные ботнеты и управляющие сервера. Источники: Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker.

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

Данные правила описывают вредоносные хосты по классификации проекта www.cinsarmy.com.

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

Данные правила описывают известные скомпрометированные и вредоносные хосты. Источники: Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects.

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

Данные правила описывают спамерские хосты / сети по классификации проекта www.spamhaus.org.

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

Данные правила описывают вредоносные хосты по классификации проекта www.dshield.org.

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

Данные правила содержат сигнатуры использования ActiveX-контента.

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

Правила, детектирующие поведение хоста после успешно проведенных атак.

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

Данные правила описывают признаки обращения к популярным чатам.

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

Временные правила, ожидающие возможного включения в постоянные списки правил.

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

Устаревшие правила, ожидающие удаления в следующих версиях.

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

Данные правила содержат сигнатуры уязвимостей в протоколе DNS, признаки использования DNS вредоносным ПО, некорректного использования протокола DNS.

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

Данные правила содержат сигнатуры DOS-атак.

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

Данные правила содержат сигнатуры эксплойтов.

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

Данные правила содержат сигнатуры уязвимостей в протоколе FTP, признаки некорректного использования протокола FTP.

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

Данные правила описывают признаки обращения к популярным игровым сайтам: World of Warcraft, Starcraft и т.п.

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

Данные правила содержат сигнатуры некорректного использования протокола ICMP.

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

Данные правила содержат сигнатуры информационных ICMP-сообщений.

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

Данные правила содержат сигнатуры уязвимостей в протоколе IMAP, признаки некорректного использования протокола IMAP.

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

Данные правила описывают признаки обращения к нежелательным ресурсам.

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

Данные правила содержат сигнатуры различных уязвимостей.

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

Данные правила содержат сигнатуры вредоносного ПО, использующего в своей работе протокол HTTP.

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

Данные правила содержат сигнатуры различных уязвимостей.

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

Данные правила содержат сигнатуры вредоносного ПО для мобильных платформ.

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

Данные правила содержат сигнатуры уязвимостей в протоколе NetBIOS, признаки некорректного использования протокола NetBIOS.

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

Данные правила описывают признаки обращения к P2P-сетям (Bittorrent, Gnutella, Limewire).

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

Данные правила описывают нежелательную сетевую активность (обращение к MySpace, Ebay).

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

Данные правила содержат сигнатуры уязвимостей в протоколе POP3, признаки некорректного использования протокола POP3.

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

Данные правила содержат сигнатуры уязвимостей в протоколе RPC, признаки некорректного использования протокола RPC.

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

Данные правила содержат сигнатуры уязвимостей для SCADA-систем.

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

Данные правила описывают признаки активности, связанной с сетевым сканированием (Nessus, Nikto, portscanning).

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

Данные правила описывают признаки активности, связанной с попытками получить шелл-доступ в результате выполнения эксплойтов.

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

Данные правила содержат сигнатуры уязвимостей в протоколе SMTP, признаки некорректного использования протокола SMTP.

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

Данные правила содержат сигнатуры уязвимостей в протоколе SNMP, признаки некорректного использования протокола SNMP.

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

Данные правила содержат сигнатуры уязвимостей для СУБД SQL.

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

Данные правила содержат сигнатуры уязвимостей для протокола telnet, признаки некорректного использования протокола telnet.

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

Данные правила содержат сигнатуры уязвимостей в протоколе TFTP, признаки некорректного использования протокола TFTP.

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

Данные правила содержат признаки сетевой активности троянских программ.

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

Данные правила содержат признаки подозрительных и потенциально опасных HTTP-клиентов (идентифицируются по значениям в HTTP-заголовке User-Agent).

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

Данные правила содержат сигнатуры уязвимостей в VOIP-протокола.

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

Данные правила содержат сигнатуры уязвимостей для веб-клиентов.

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

Данные правила содержат сигнатуры уязвимостей для веб-серверов.

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

Данные правила содержат сигнатуры эксплуатации уязвимостей веб-приложений.

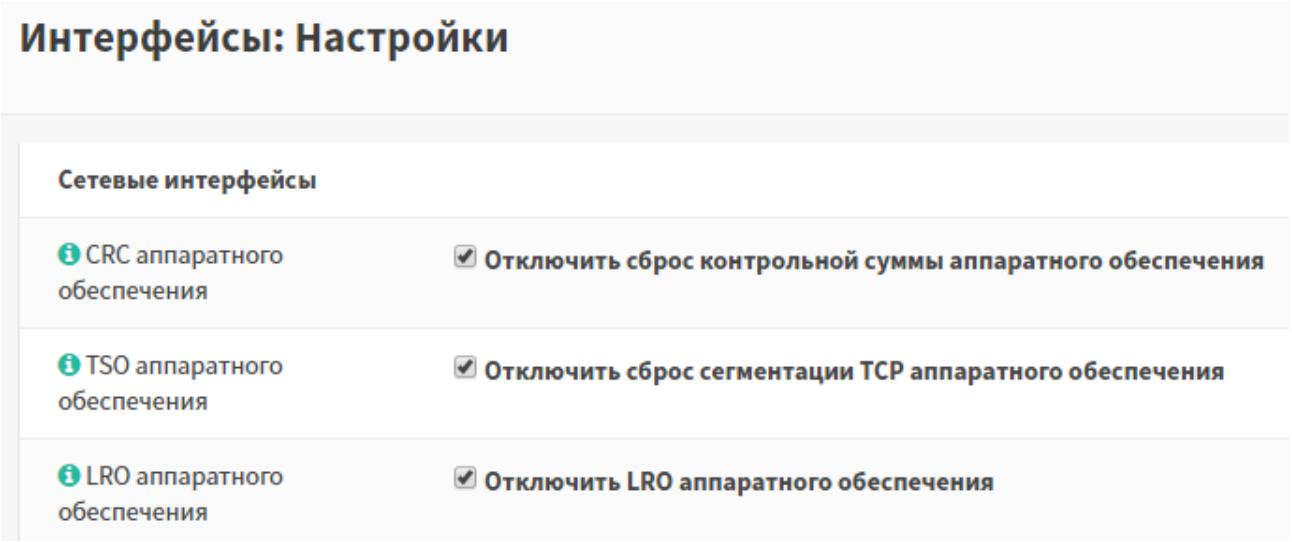
- https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules

Данные правила описывают признаки активности сетевых червей.

2. Настройка IPS/IDS Suricata

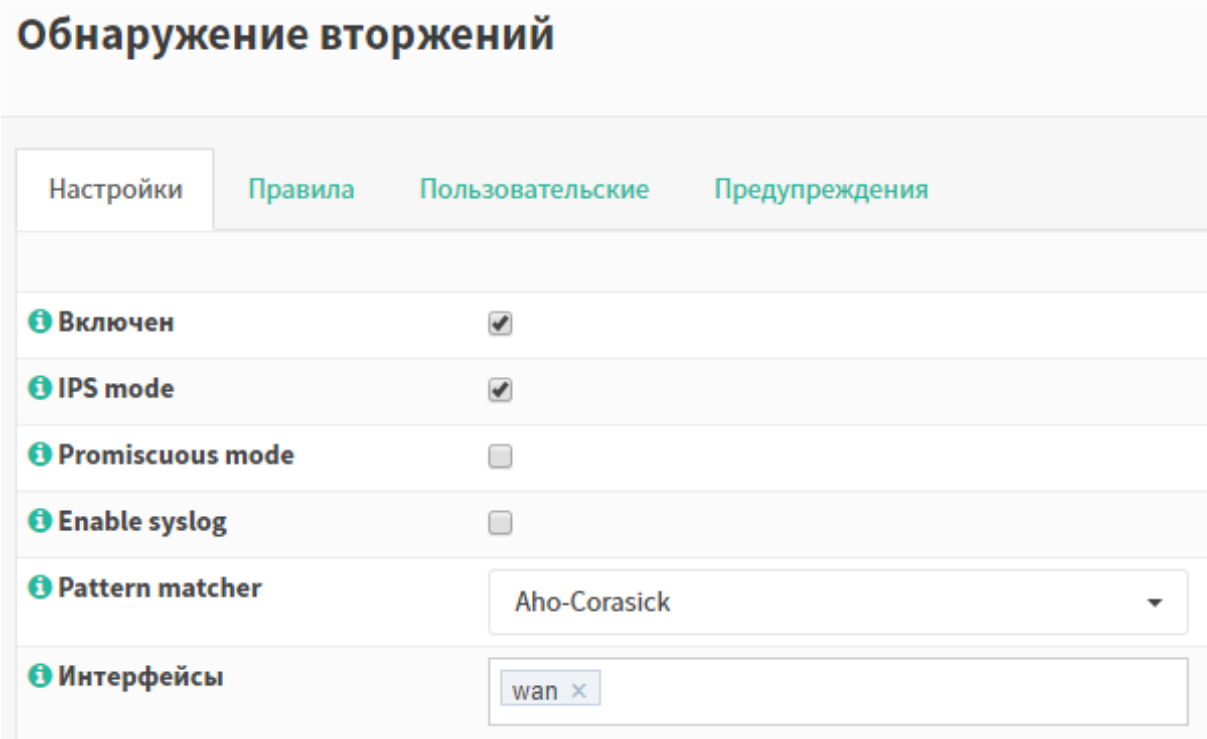
2.1 Выключение режима Hardware Offloading

Пройдите в раздел Интерфейсы -> Настройки. Снимите флажки напротив механизмов *Hardware Offloading*.



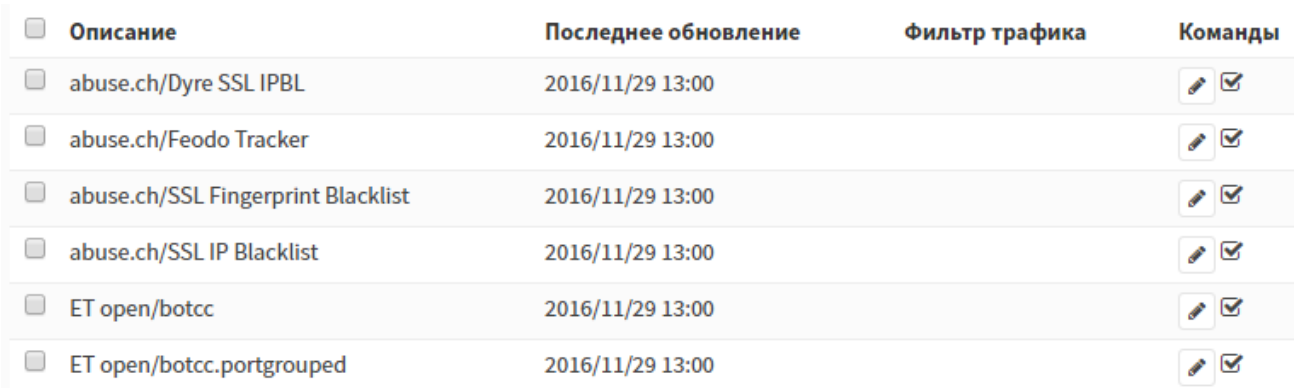
2.2 Включение IPS/IDS Suricata

Пройдите в раздел Службы -> Обнаружение вторжений, на вкладку Настройки. Установите флажки Включен и IPS mode. Выберите интерфейс, который будет прослушивать система обнаружения вторжений. Нажмите Применить.



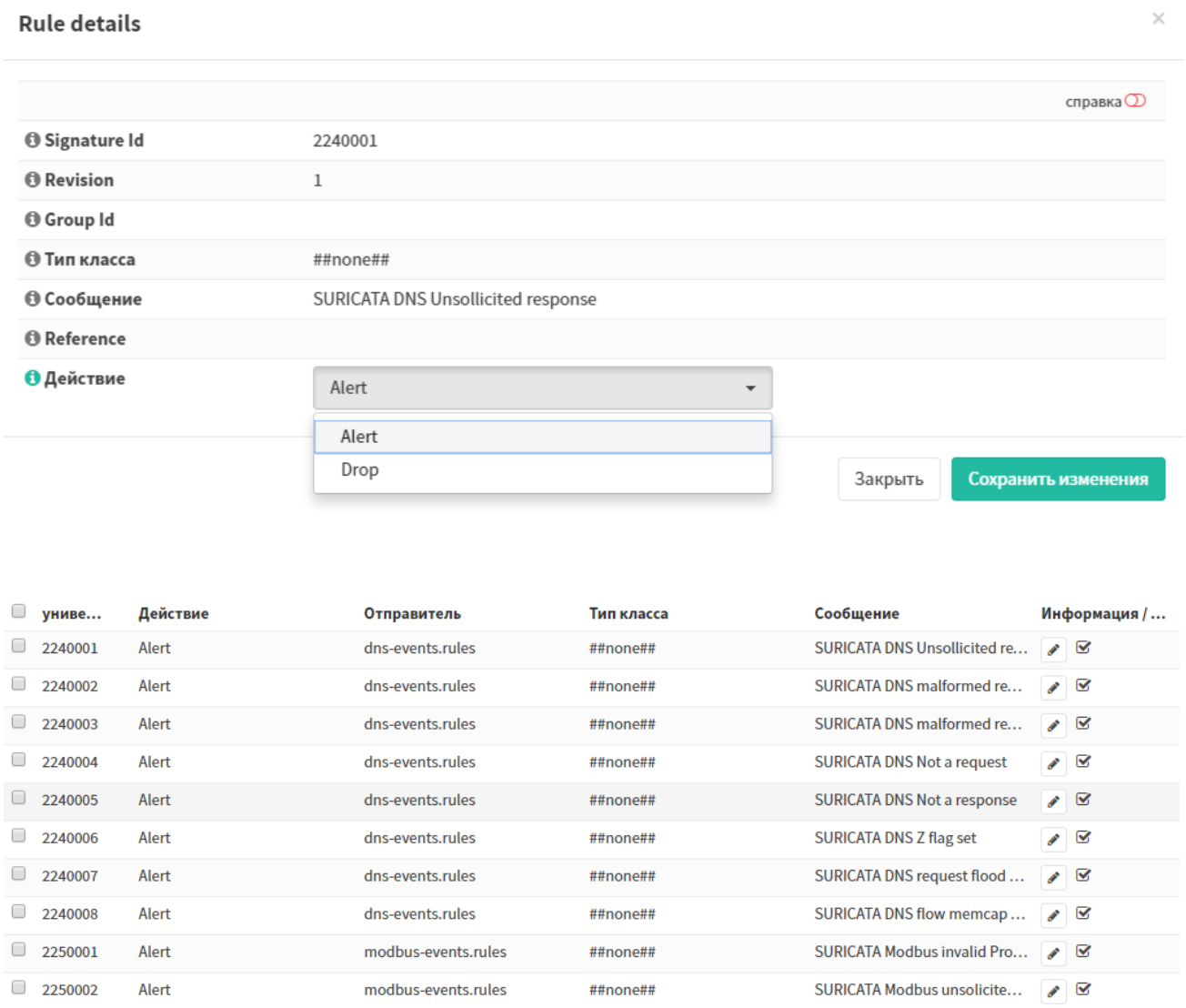
2.3 Загрузка списков правил

На вкладке Настройки, выберите нужный список правил. Убедитесь, что список еще не установлен (колонка Последнее обновление). Установите напротив данного списка флажок и нажмите на кнопку Скачать и обновить правила.



2.4 Настройка правил

После скачивания списка, все определенные в нем правила появляются на вкладке Правила. Включите нужное правило (установите флажок напротив правила в колонке Enabled). Зайдите в свойства правила (иконка Info) и задайте желаемое административное действие – Alert или Drop. Нажмите на кнопку Применить.



унив...	Действие	Отправитель	Тип класса	Сообщение	Информация / ...
2240001	Alert	dns-events.rules	##none##	SURICATA DNS Unsollicited re...	
2240002	Alert	dns-events.rules	##none##	SURICATA DNS malformed re...	
2240003	Alert	dns-events.rules	##none##	SURICATA DNS malformed re...	
2240004	Alert	dns-events.rules	##none##	SURICATA DNS Not a request	
2240005	Alert	dns-events.rules	##none##	SURICATA DNS Not a response	
2240006	Alert	dns-events.rules	##none##	SURICATA DNS Z flag set	
2240007	Alert	dns-events.rules	##none##	SURICATA DNS request flood ...	
2240008	Alert	dns-events.rules	##none##	SURICATA DNS flow memcap ...	
2250001	Alert	modbus-events.rules	##none##	SURICATA Modbus invalid Pro...	
2250002	Alert	modbus-events.rules	##none##	SURICATA Modbus unsolicite...	

2.5 Автоматическое обновление правил по расписанию

Можно настроить автоматическое обновление правил по расписанию. Кликните на вкладку Расписание и укажите нужные настройки периодичной загрузки.