Уніфікована операційна система FortiOS – основа Fortinet Security Fabric

Максим Порицький

Цель

Познакомить Вас с некоторыми возможностями унифицированной операционной системой FortiOS, функционирующей на нашем флагманском продукте и ядре Fortinet Security Fabric – FortiGate

FortiOS - единая ОС для FortiGate

Configuration	Log & Report	Diagnostics	Monitoring	**Operation**	Systems Integration	Central Mgmt. and Provisioning	Cloud & SDN Integration
					Visibility	Automation	
Policy Objects	Device Identification	SSL inspection	Actions	**Policy and Control**	AAA	Compliance & Security Rating	
Anti-Malware	IPS & DoS	Application Control	Web Filtering	**Security**	Advanced Threat Protection (ATP)	Vulnerability Assessment	IOC Detection
Firewall	VPN	DLP	Email Filtering				
SD WAN	Explicit Proxy	IPv6	High Availability	**Networking**	Wireless Controller	Switch Controller	WAN Interface Manager
Routing/NAT	L2/Switching	Offline Inspection	Essential Network Services				
Physical Appliance (+SPU)	Virtual System	Hypervisor	Cloud	**Platform Support**	**Security Fabric**		

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortios-6-2.pdf

* Features availability may varied by models

IPS & DOS

SECURITY

IPS & DOS

Эксплойты	Аномалии
Известные атаки на уязвимости системы (ОС, ПО и т.д.) с известными шаблонами	Неизвестные атаки на уязвимости системы (ОС, ПО и т.д.) или нестандартное поведение (чрезмерная загрузка CPU, сетевой трафик и т.д.)
Обнаруживаются на основе сигнатурных шаблонов	Обнаруживаются на основе поведенческого анализа
Могут быть выявлены ✓ Signature-based IPS ✓ WAF ✓ AV	Должны быть обнаружены/выявлены, заблокированы ✓ Rate-based IPS ✓ DoS политики ✓ Средствами проверки корректности протоколов ✓ Sandbox

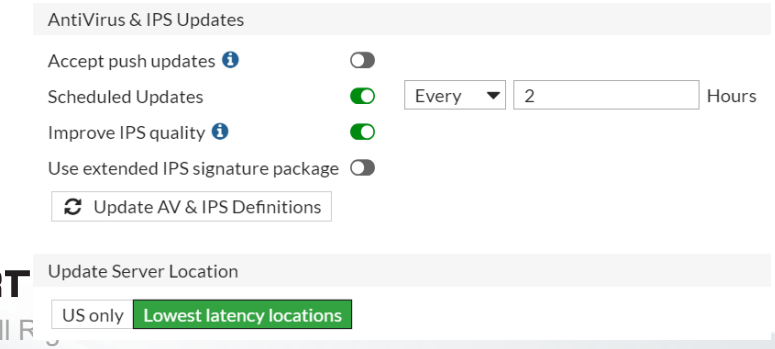
FORTINET

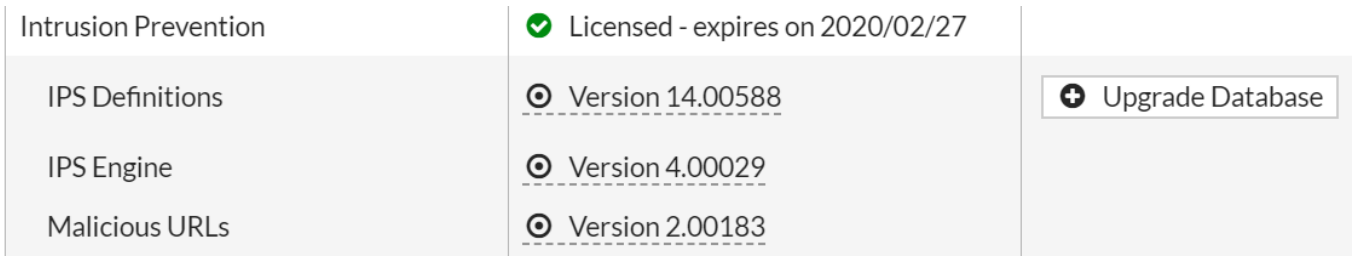
SECURITY

IPS & DOS

- **IPS состоит:**
  - ✓ **Protocol decoder** – определение протокола, проверка протокола на соответствие стандартам
  - ✓ **IPS Engine** (IPS Sensor) – сигнатурная проверка трафика определенного декодером протокола
  - ✓ **IPS DB** – база сигнатур известных уязвимостей, переодическое обновление из FortiGuard, требует подписку

Name	Severity	Target	OS	Action
3Com.3CDaemon.FTP.Server.Buffer.Overflow		Server	Windows	Block
3Com.3CDaemon.FTP.Server.Information.Disclosure		Client	Windows	Block
3Com.Intelligent.Management.Center.Information.Disclosure		Server	Windows	Block
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux	Block





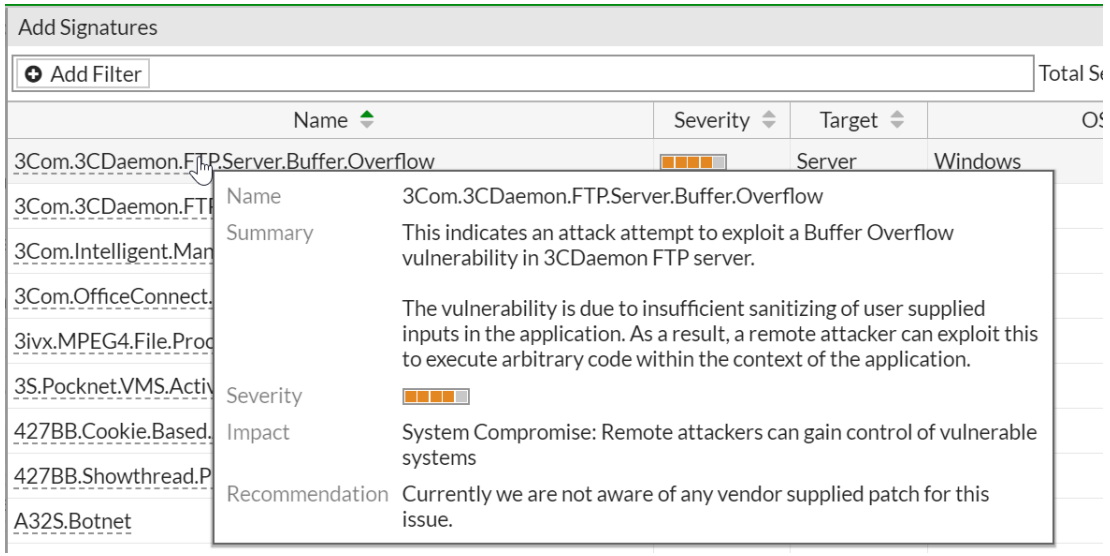
SECURITY

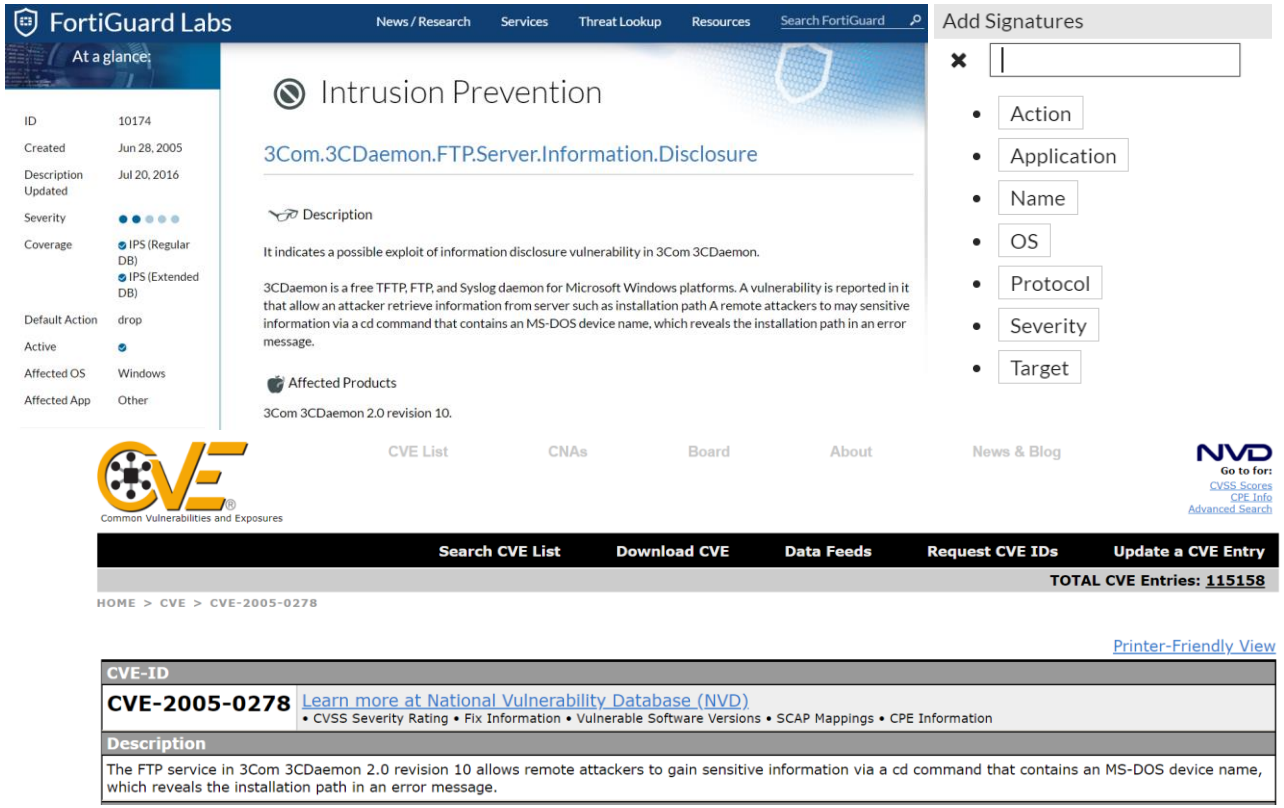
IPS & DOS

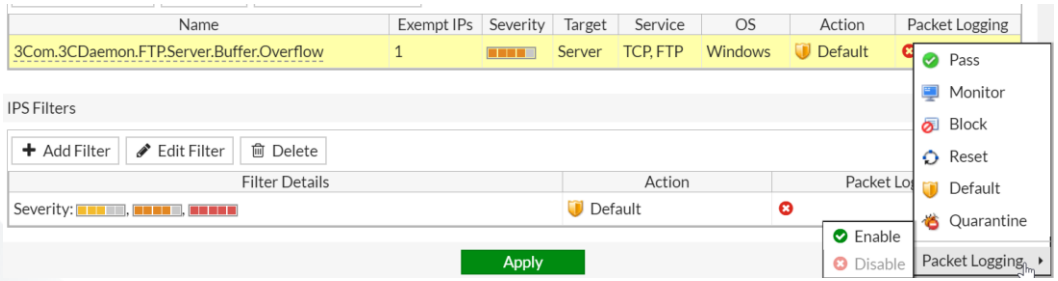
https://fortiguard.com/updates/ips

Signature-based IPS protection

- **Детальное описание** сигнатур в GUI
- **Ссылки** на описание на **FortiGuard** IPS encyclopedia и **CVE-ID** (Common Vulnerabilities and Exposures)
- **Создание** соответствующих вашей инфраструктуре **IPS сенсоров** с соответствующим набором сигнатур
- Создание **пользовательских сигнатур**
- **Добавление исключений** (для определенных IP) для конкретных сигнатур (при ложных срабатываниях)
- Определение **реакции (действия)** для сигнатур
- **Логирование** копии пакетов







FORTINET

SECURITY

IPS & DOS

Rate-based IPS protection (application based DoS and brute force attacks)

- Защита от угроз, на основе **достижении порогового значения за определенный интервал времени** (rate based)
- 30 **Rate-based IPS сигнатур**
- Определение **продолжительности** блокировки

Rate Based Signatures

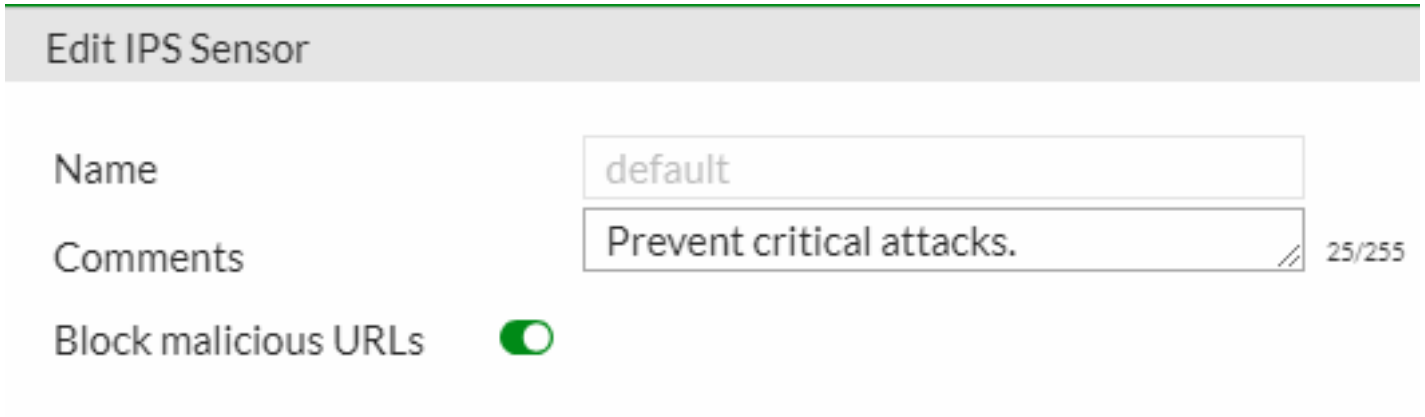
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Durat
ON	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	Expires 1 Da
ON	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	None
ON	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	None
ON	FTP.Login.Brute.Force	200	10	Any	Block	Expires 2 Da
ON	FreeBSD.TCP.Reassembly.DoS	10	2	Any Source IP Destination IP	Block	None
ON	IMAP.Login.Brute.Force	60	10		Block	None
ON	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	None

SECURITY

IPS & DOS

Malicious (malware and exploit) URL database

- **Мини Web-фильтр** :) в стоимости IPS подписки
- FortiGate содержит локальную DB **вредоносных сайтов** (до 1M)
- На FG61E и выше (с внутренним storage)
- **Активные вредоносные сайты** – за последний 1 месяц
- **Известные сайты с эксплоитами** – за последние 3 месяца
- Переодическое **обновление** из FortiGuard



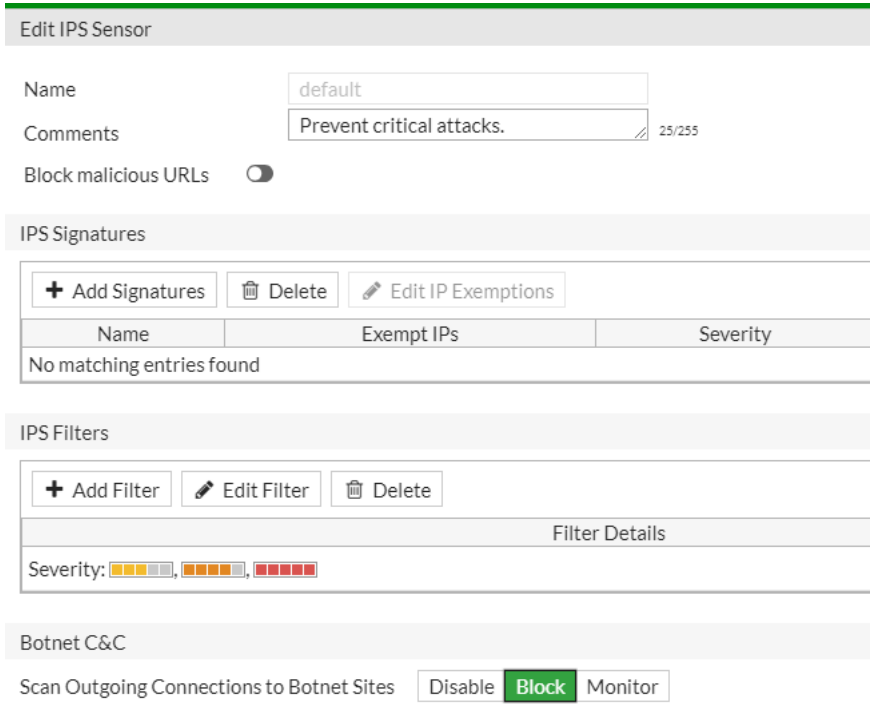
SECURITY

IPS & DOS

Botnet protection

- Обнаружение попыток **обращения** к известным **botnet command and control узлам**
- Включается в **IPS сенсоре** с соответствующей реакцией
- Переодическое **обновление** botnet command and control database из FortiGuard

Intrusion Prevention	Licensed - expires on 2020/02/26
IPS Definitions	Version 14.00597
IPS Engine	Version 4.00219
Malicious URLs	Version 2.00188
Botnet IPs	Version 4.00461
Botnet Domains	Version 2.00226

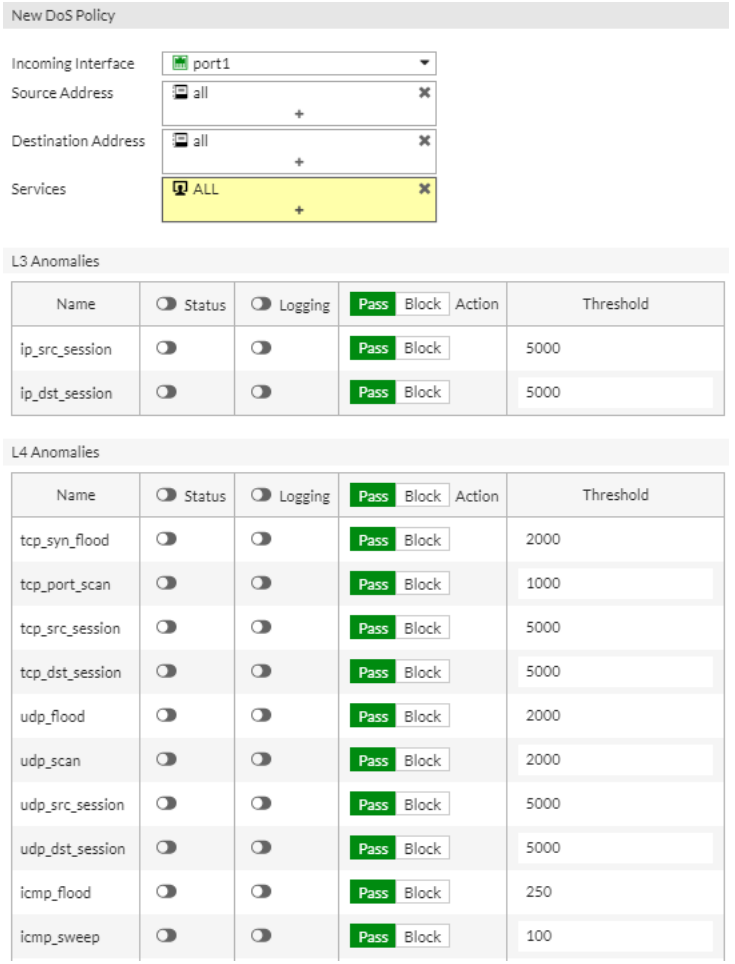


SECURITY

IPS & DOS

DoS protection

- Обнаруживает и противодействие трафику, который является частью **DoS атаки (L3/L4 OSI)**
- На основе **частоты повторения** (в минуту), задаются **пороговые значения**, привышение которых ведет к определенной реакции
- Применяется к **входящему** трафику
- Возможно вести **логирования** (вне зависимости от action)
- DoS policy **применяются до** Security Policy



Application Control

SECURITY

APPLICATION CONTROL

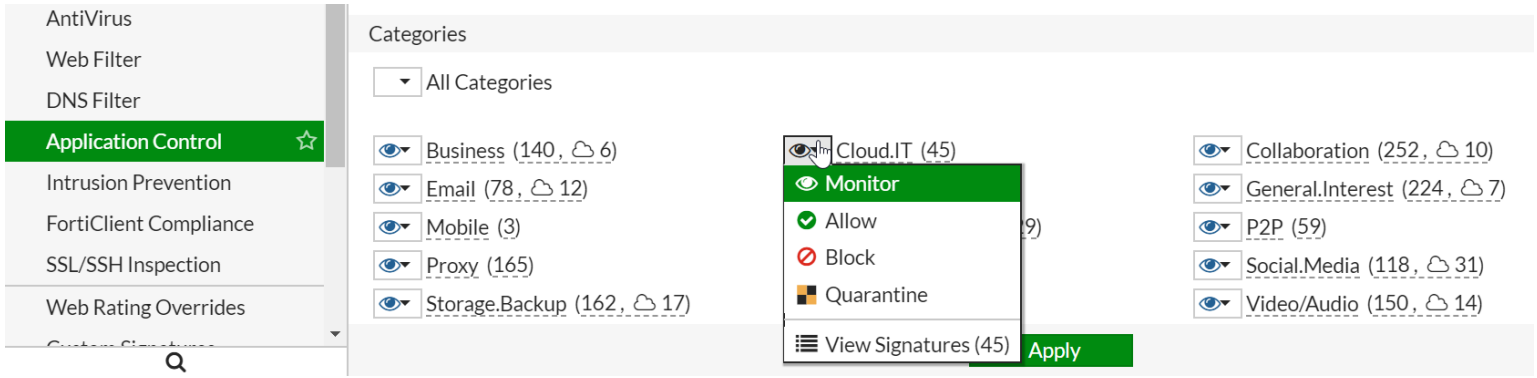
- **Для чего:**
  - Обнаружение и идентификация приложений, применение соответствующих политик безопасности и/или функция качества обслуживни (QoS)
- **Существующие сложности:**
  - Кол-во приложений возрастает, Client-Server → Peer-to-Peer приложения
  - Многие приложения не используют статические порты/протоколы, что усложняет их контроль FW
  - Есть необходимость в гранулярном доступе к функциям приложений

SECURITY

APPLICATION CONTROL

- **AC состоит:**
  - ✓ **Protocol decoder** + **IPS Engine -** определение трафика конкретных приложений (с учетом использование нестандартных портов/протоколов)
  - ✓ **AC DB** – база сигнатур известных приложений, переодическое обновление из FortiGuard, достаточно FortiCare контракта

FortiCare Support	Registered - cadet225@gmail.com	Launch Portal
Enhanced Support	8x5 support - expires on 2020/02/27	
Application Control Signatures	Version 14.00588	Upgrade Database

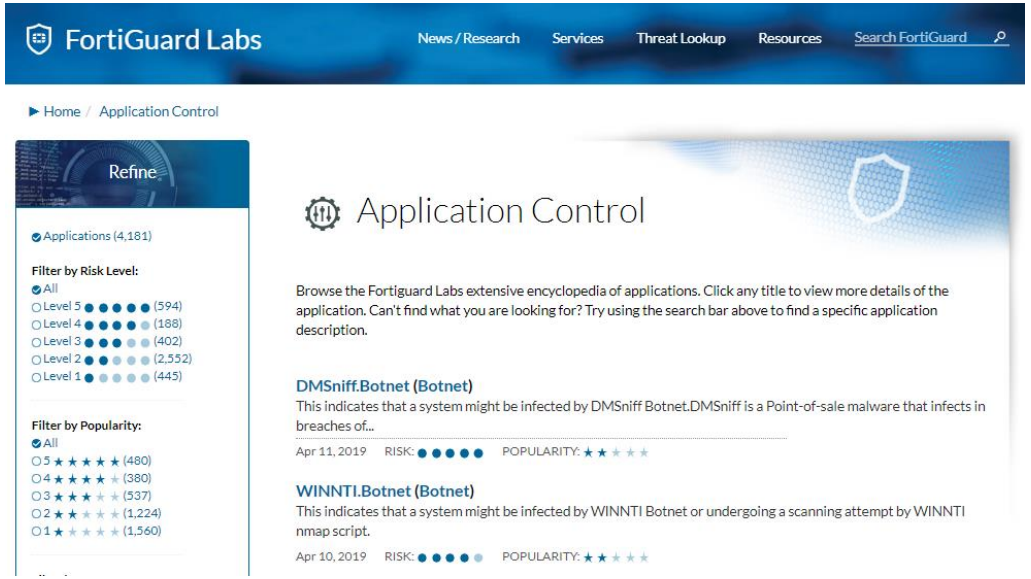


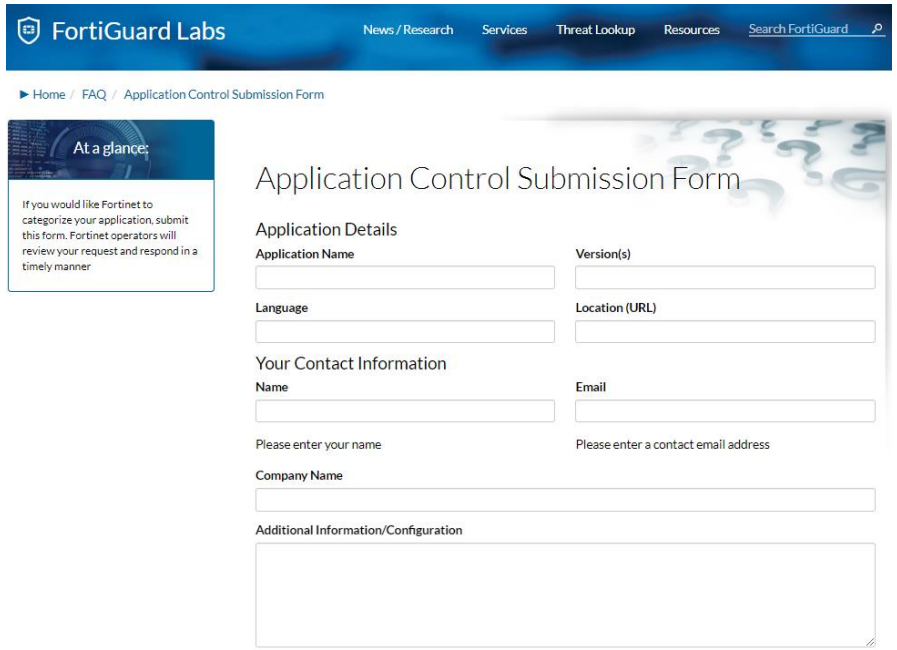
SECURITY

APPLICATION CONTROL

http://fortiguard.com/appcontrol

- **20 категорий** (>4000 приложений)
- **FortiASIC CP** для сигнатурного анализа
- Ссылки на **описание сигнатур** на FortiGuard
- AC DB включает **также сигнатуры “облачных” приложений**, приложения которые используют **шифрованние** требуют **SSL deep inspection**
- **Запрос на добавление сигнатур** под специфичные пользовательские приложения на FortiGuard





97 Cloud Applications require deep inspection.
0 policies are using this profile.

FORTINET

SECURITY

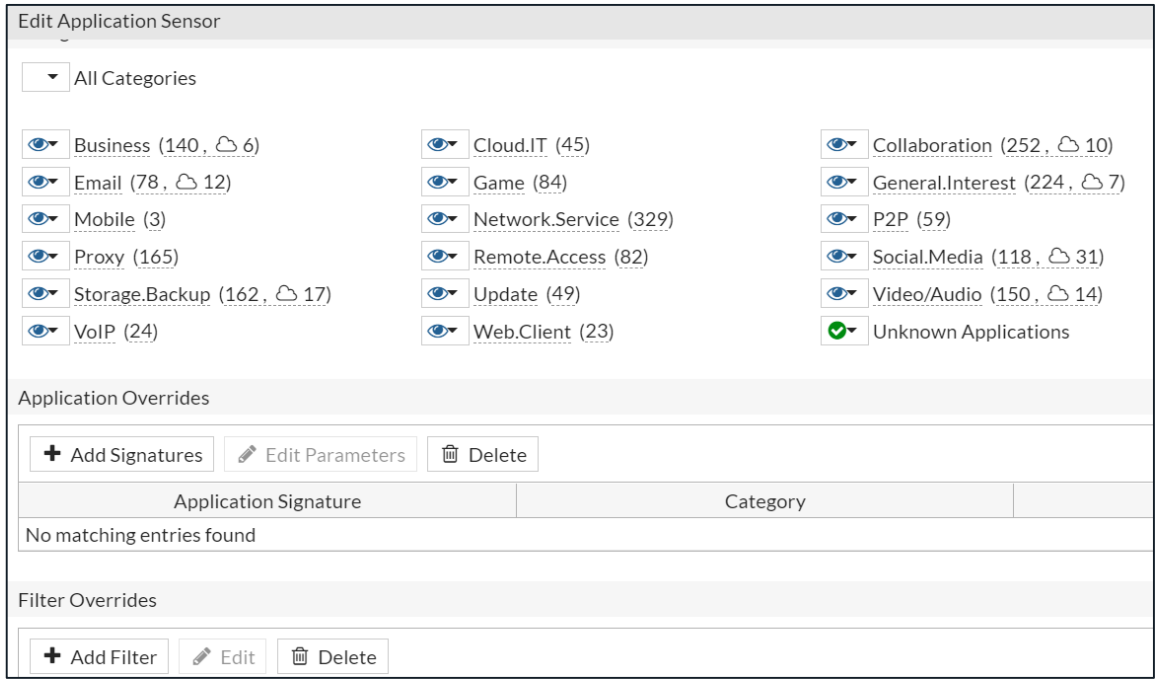
APPLICATION CONTROL

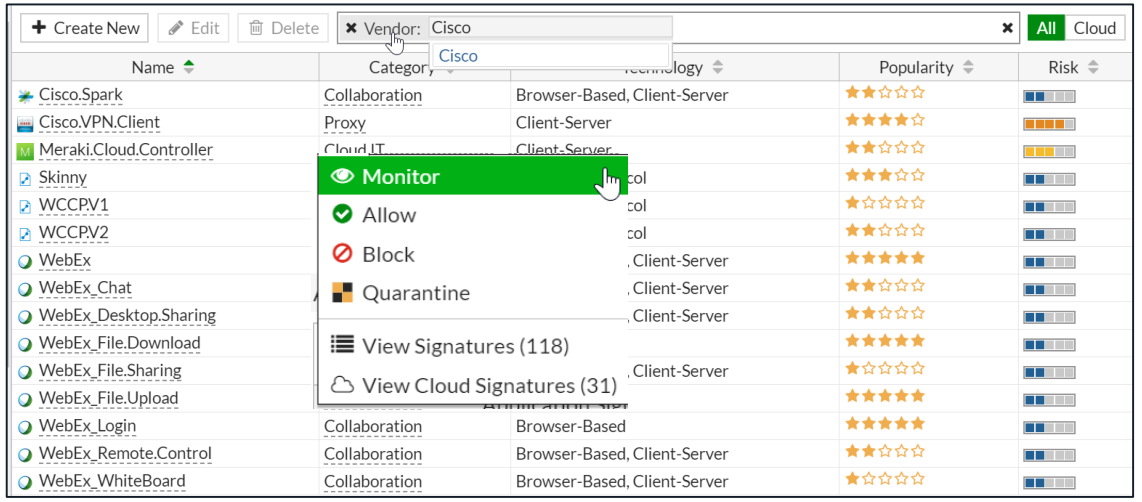
- Создание соответствующих вашей инфраструктуре **AC сенсоров** с соответствующим набором сигнатур приложений и реакциями (action)
- **Добавление исключений** (Application overrides + filter overrides) – **необходимая рекция** (action) для конкретных приложений или их групп, отличная от предконфигуренной
- Добавление **индустриальных сигнатур** (CLI)
- Создание **пользовательских сигнатур**
- Возможны **гранулярные политики** по регулированию доступа к элементам приложений
- Применение **AC сенсоров** к **security policy**

```
FGVM04TM19000624 # config ips global

FGVM04TM19000624 (global) # set exclude-signatures
none          No signatures excluded.
industrial    Exclude industrial signatures.

FGVM04TM19000624 (global) # set exclude-signatures none
```





SECURITY

APPLICATION CONTROL

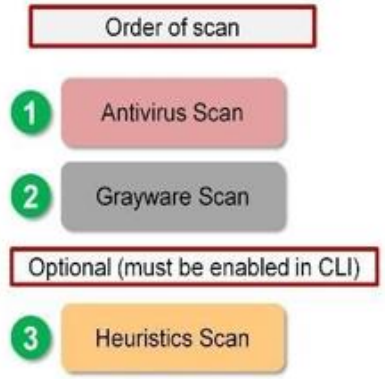
- **Traffic shaping** - качество обслуживания трафика для разных приложений с конфигурацияе гарантированной и максимальной пропускной способностью (maximum or guaranteed bandwidth)
- **User notification -** отображение сообщения о блокировке приложения (только для HTTP/HTTPS app), для non-HTTP/HTTPS приложений → drop the packets or reset the TCP connection
- **Deep inspection for cloud applications** – анализ работы пользователей с популярными облачными приложениями и фиксация (FortiView and logs) действий, связанных с этими приложениями (идентификаторы пользователей, действия в облаке, имена файлов, размеры файлов)
- **SSL inspection for encrypted traffic –** инспекция приложений в расшифрованном трафике
- **Monitoring, logging, and reporting** – представление в детальном графическом виде информации о приложениях (top, users…), архивирование через syslog

```
config application list
   edit <name of the sensor>
      set app-replacemsg {enable | disable}
   end
```

ANTIVIRUS / ANTIMALWARE

ANTIVIRUS / ANTIMALWARE

- **Цель:**
  - За счет интегрированных технологий **предотвратить** проникновени разнообразных **вредоносных программ** (malware) в вашу сеть
    - ✓ Известные malware
    - ✓ Неизвестные malware
  - **Проверка файлов** передаваемых по протоколам - HTTP, FTP, IMAP, POP3, SMTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS, FTPS.



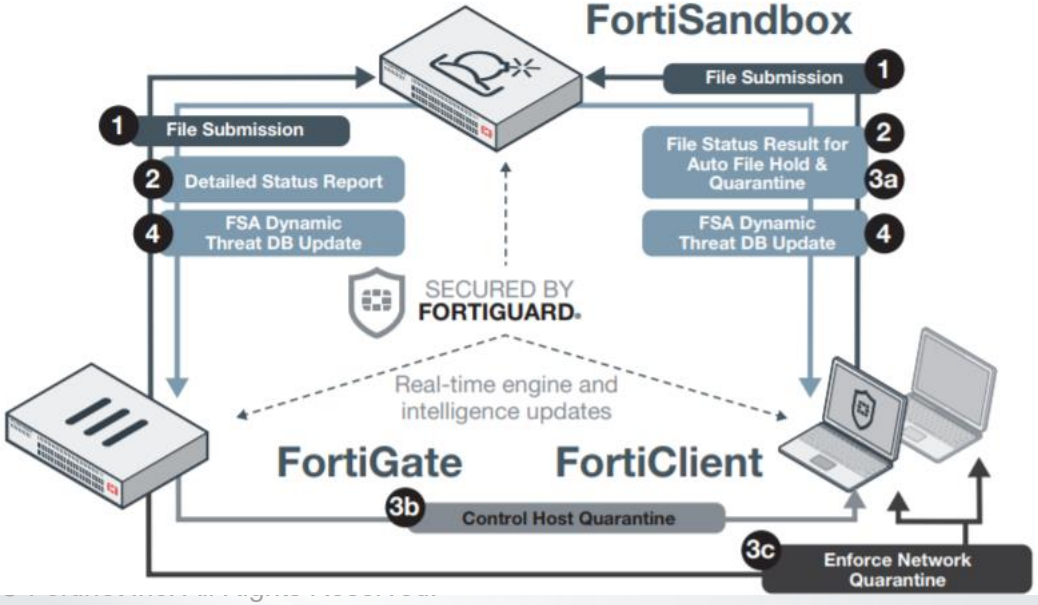
- **Antivirus scan** - обнаружение известных вирусов на основе сопостовления сигнатур (antivirus signature)
- **Grayware scan** - обнаружение “нежелательных” программ на основе сопостовления сигнатур (grayware signature)
- **Heuristics scan** - сканирования основаные на вероятности идентификации неизвестных угроз - подозрительных файлов (suspicious файл)

SECURITY

ANTIVIRUS / ANTIMALWARE

ИНТЕГРАЦИЯ С SANDBOX

- Для выявления **угроз 0-дня** используется интеграция с **FortiSandbox** / **FortiSandbox Cloud** (активировать FortiCloud account)
- Выявление происходит на основе **поведенческого анализа** файла **в изолированной среде** (VM)
- FortiSandbox **возвращает вердикт по файлу** + **new antivirus и web-filtering signatures**



Query

1. File submission for analysis
2. Respective analysis results are returned

Remediation

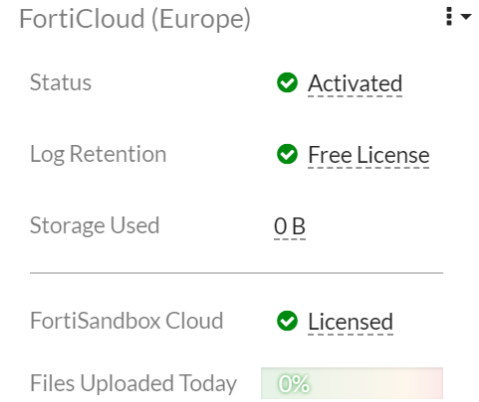
3a. Auto File Quarantine on host with option to hold file until result

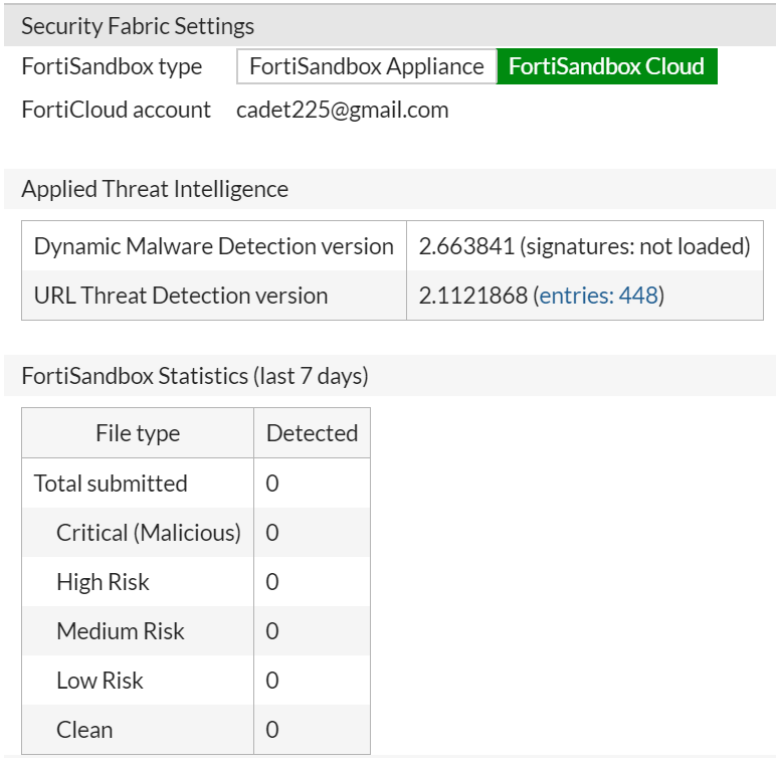
3b. Manual Host Quarantine by administrator

3c. Manual Source IP Quarantine using firewall

Protection

4. Proactive dynamic Threat DB update to gateway and host



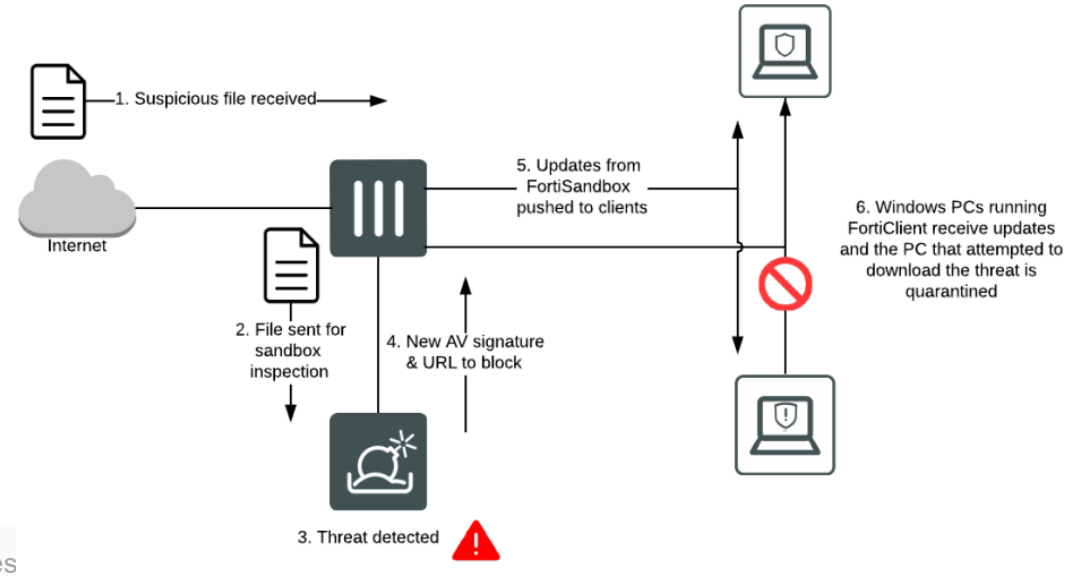


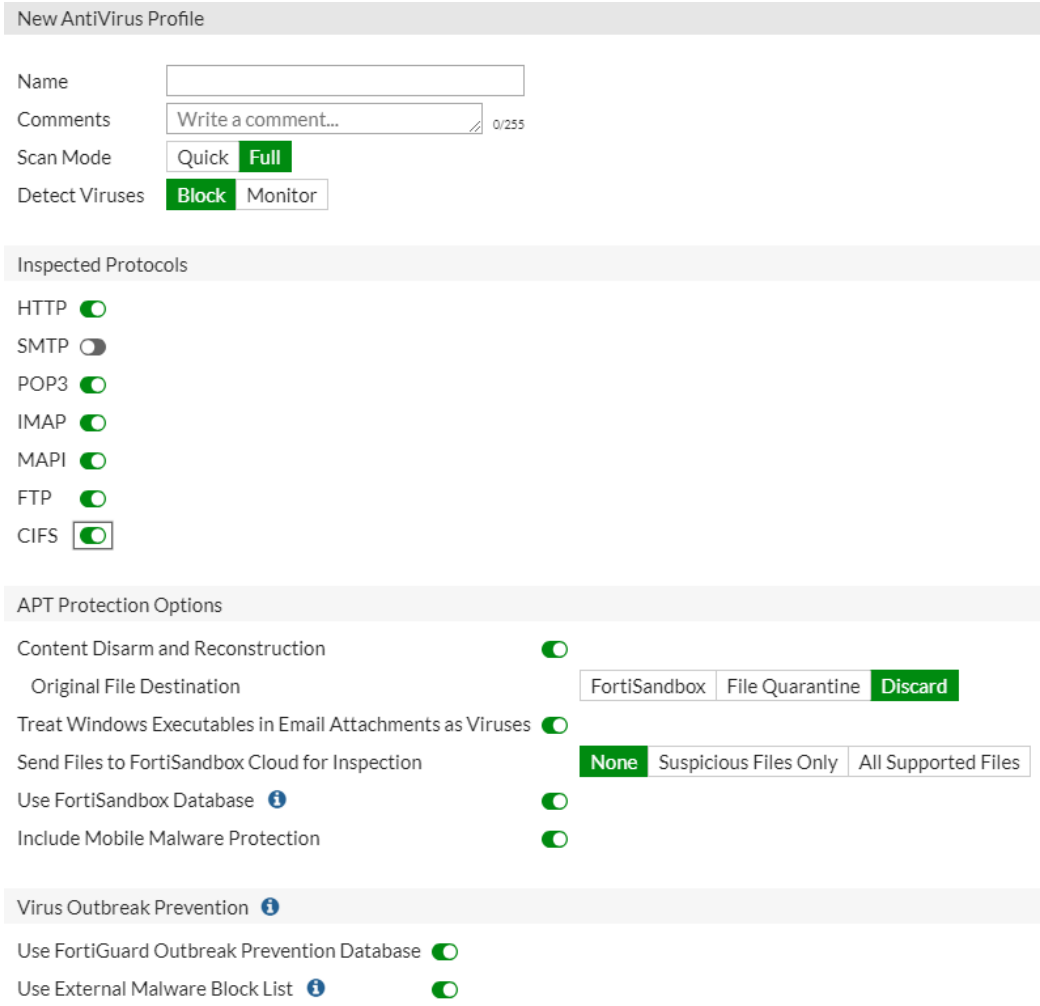
SECURITY

ANTIVIRUS / ANTIMALWARE

ИНТЕГРАЦИЯ С SANDBOX

- Можно определить **какие файлы посылать на анализ** в FortiSandbox
  - ✓ Определенных типов
  - ✓ Подозрительные (suspicious) - на основе “климата угроз” от FortiGuard
- Усиление безопасности за счет использования **FortiSandbox database** в сочетании с **FortiGuard AV database**



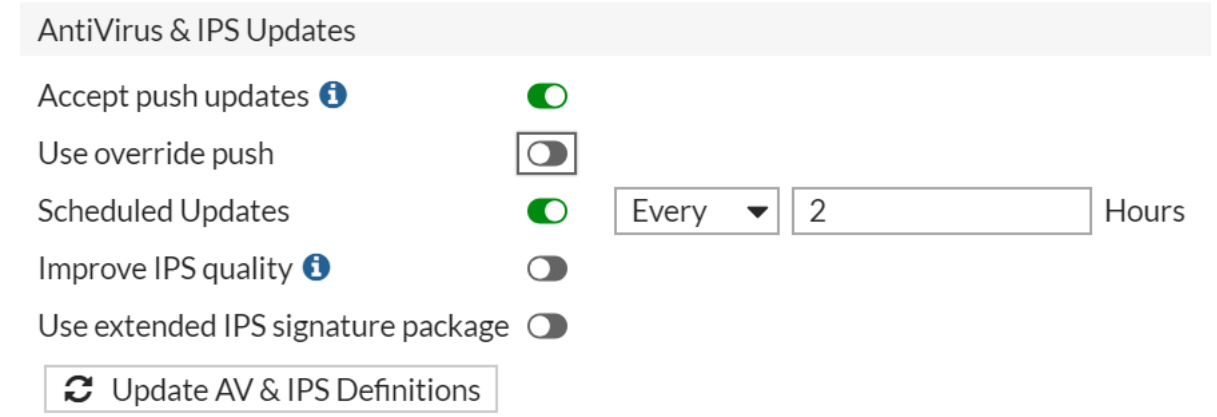


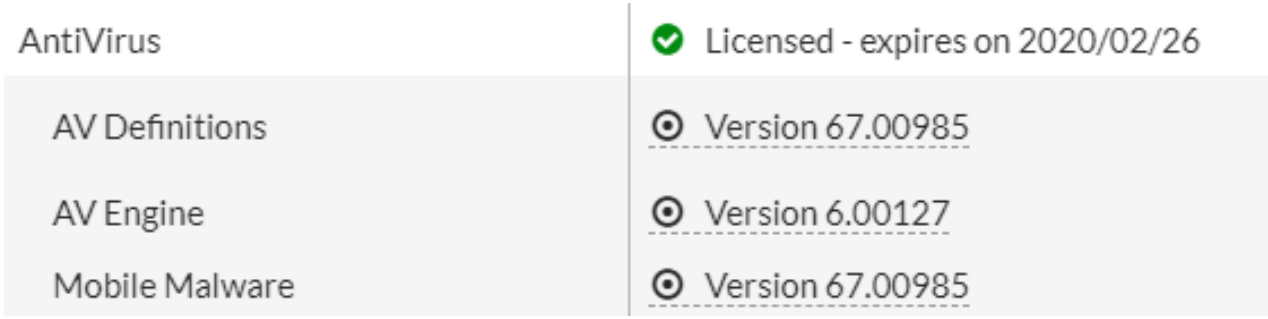
SECURITY

ANTIVIRUS / ANTIMALWARE

ОБНОВЛЕНИЯ ANTIVIRUS DB

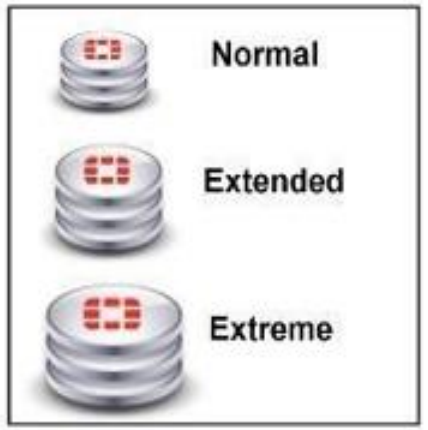
- Обновления FortiGuard **AV database** доступны:
  - ✓ Автоматически по расписанию
  - ✓ Accept push-обновления (сразу при выпуске обновлений)
  - ✓ В ручном режиме
- **Mobile Malware** подписка являются частью **FortiGuard AntiVirus license**





ANTIVIRUS / ANTIMALWARE

ВЫБОР ANTIVIRUS DB



- **AV engine** использует одну из DB сигнатур, зачастую это **Normal**, но на некоторых моделях можно выбрать и другую

Normal	DB актуальных malware, используется по умолчанию
Extended	Normal + DB практически исчезнувших malware
Extreme	Extended + DB бездействующих или устаревших malware (к старым системам)

```
config antivirus settings
    set default-db {normal | extended | extreme}
```

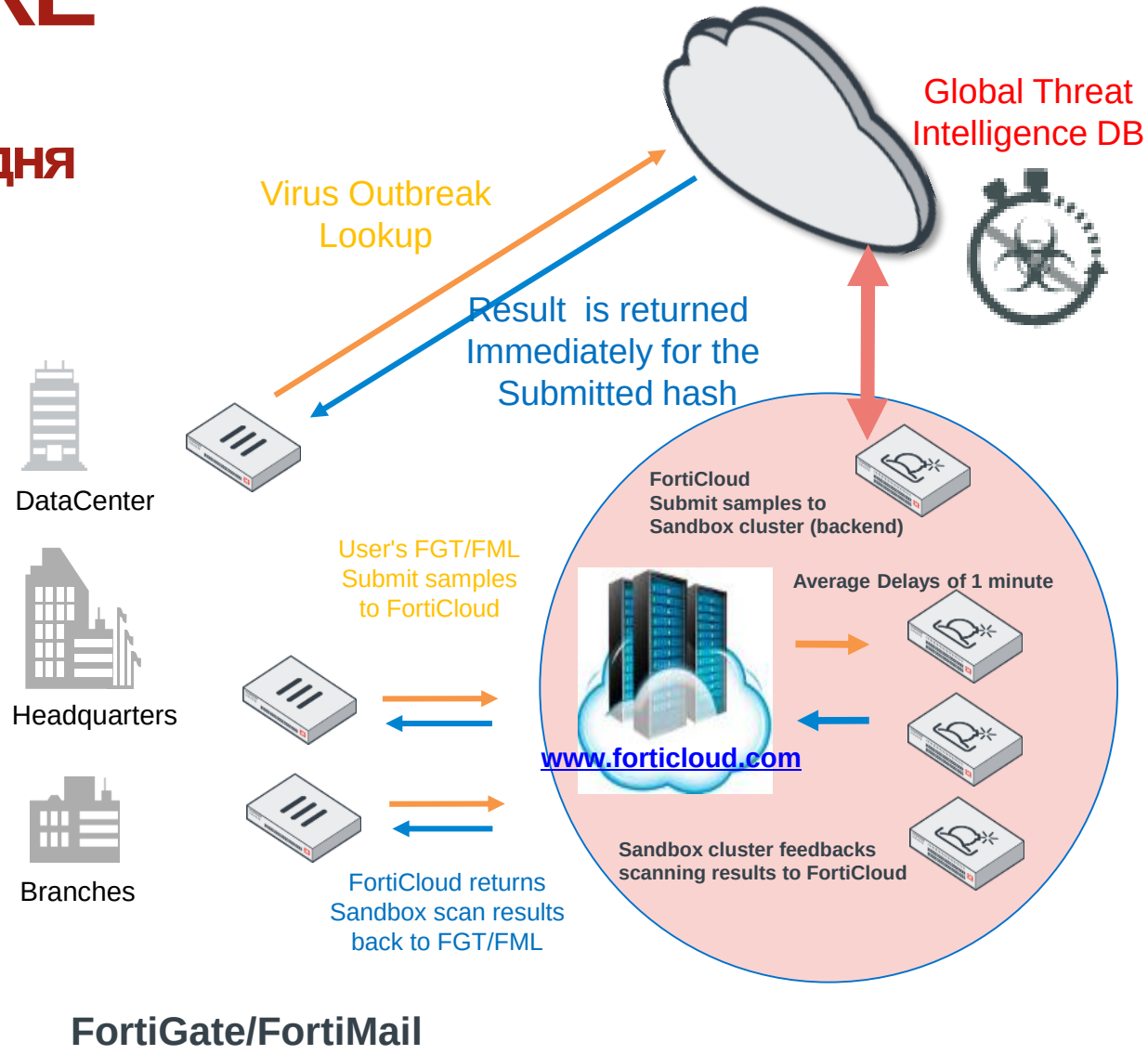
compact DB (меньше сигнатур, в IPS Engine) – только для Quick scan mode

SECURITY

ANTIVIRUS / ANTIMALWARE

Virus Outbreak Protection Service (VOS) дополнительная защита от атак нулевого дня

- Сервис обнаружение неизвестных угроз в период **между выпуском новых сигнатур для AV DB**
- Дополняет функционал Sandbox (включен в Enterprise подписку)
- Если AV не обнаружил malware, отправляется **запрос на VOS**
- **Анализ** осуществляется на основе **хеша файла** (real-time hash lookup to the Global Threat Intelligence DB)
- Запросы обрабатываются **в режиме реального времени**

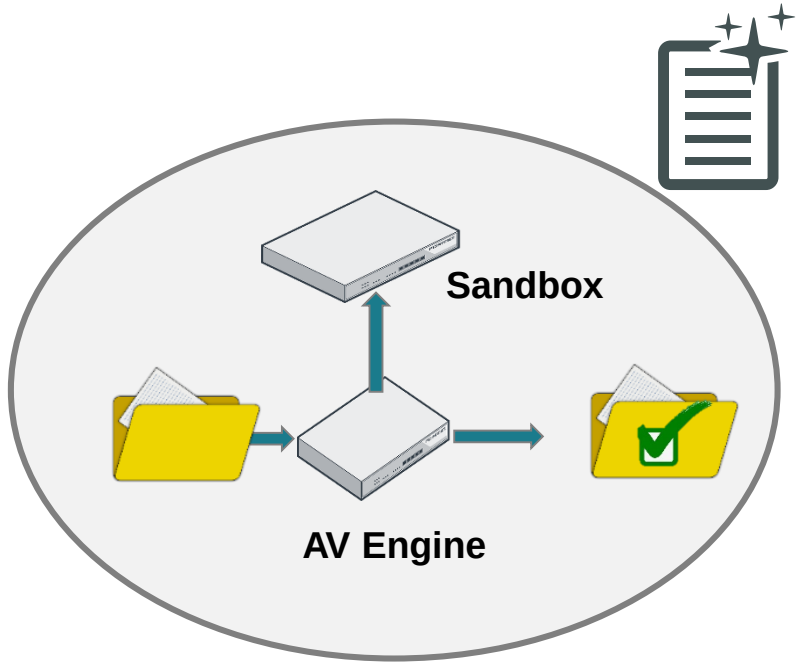


SECURITY

ANTIVIRUS / ANTIMALWARE

Content Disarm and Reconstruction (CDR)
сервис удаления активных элементов из файлов

- **Весь активный контент** (который может нести угрозу) рассматривается как **подозрительный** и извлекается из файла перед отправкой пользователю
- CDR доступен для **PDF и MS Office** файлов (HTTP, SMTP, IMAP, POP3)
- Опционально **оригинальный файл** можно послать на проверку в **FortiSandbox**
- **Оригинальный файл** (в случае Clean) может быть **доступен из FortiSandbox**



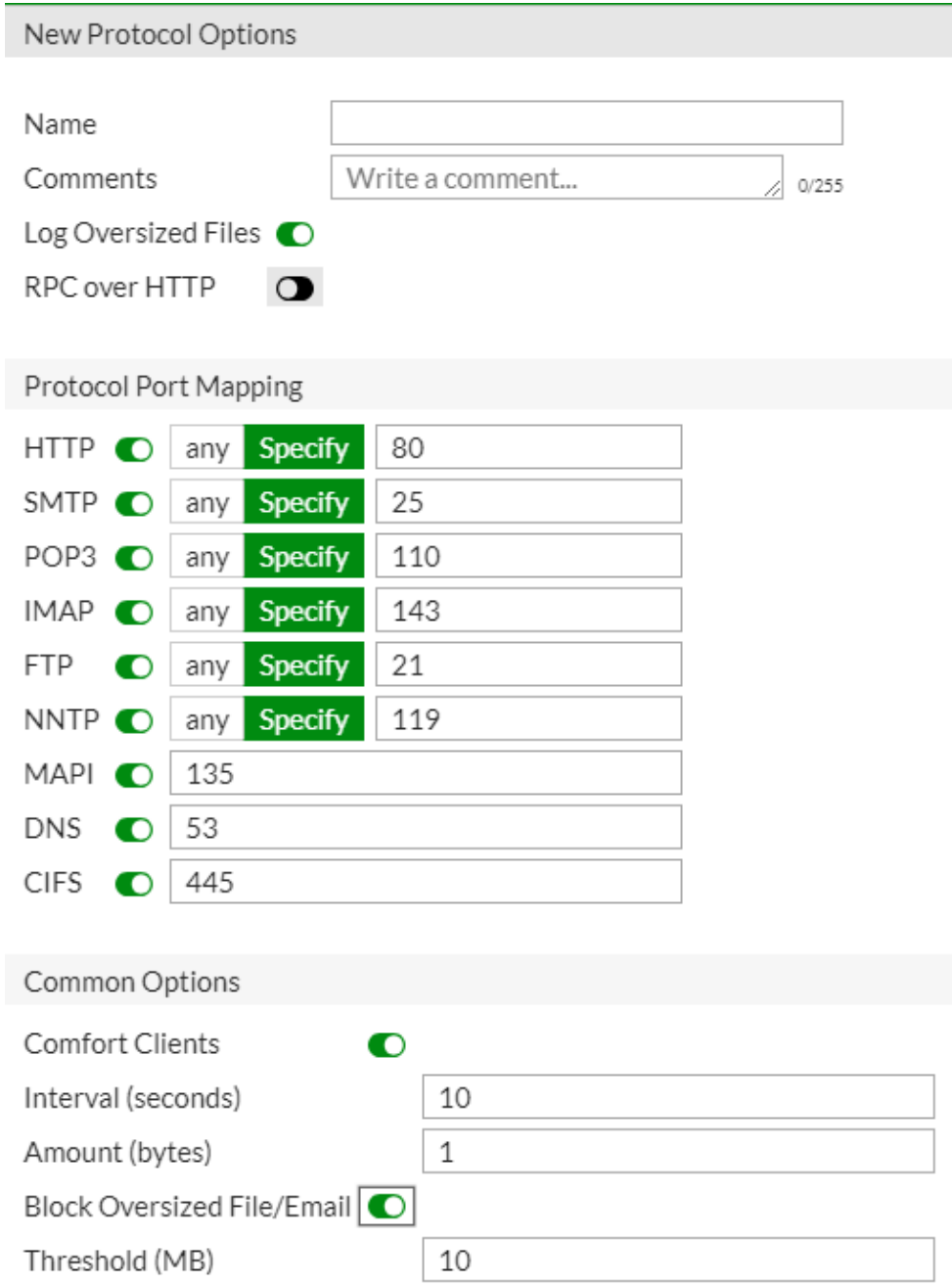
SECURITY

ANTIVIRUS / ANTIMALWARE

граничные параметры

- **Block Oversized files and emails** (10MB) - граничный размер загружаемых файлов, которые будут проверяться. При привышении, можно задать блокировку
- **Log Oversized files –** логирование о таких файлах
- **Uncompressed-oversize** (10MB) - граничный размер файла после разархивирования, которые будут проверяться (CLI)
- **Сканирование архивов** – nest-limit - (def =12, max = 100)

```
config firewall profile-protocol-options
    edit "new"
        config http
            set ports 80
            unset options
            unset post-lang
            set uncompressed-oversize-limit 20
            set uncompressed-nest-limit 20
```

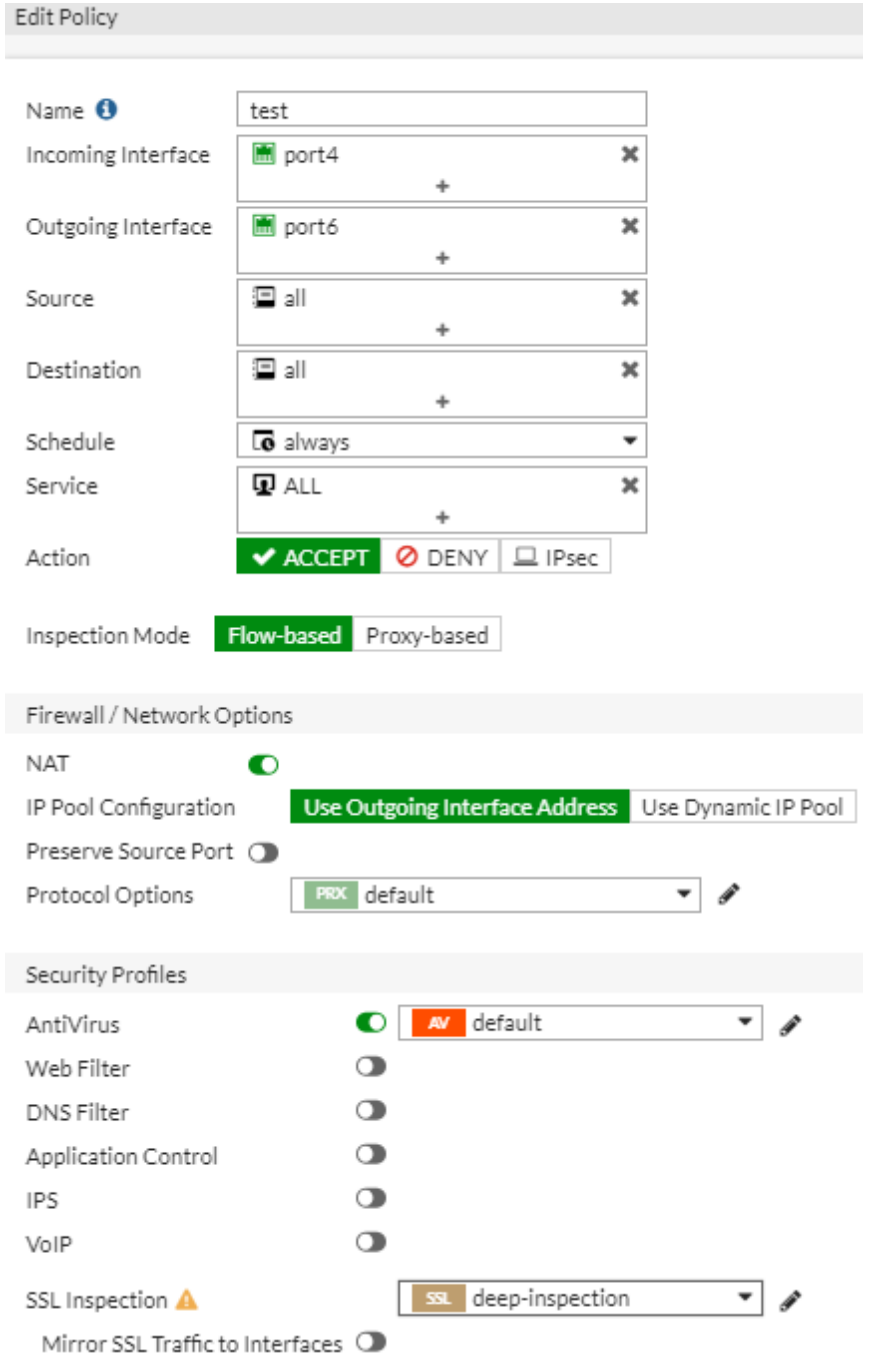


SECURITY

ANTIVIRUS / ANTIMALWARE

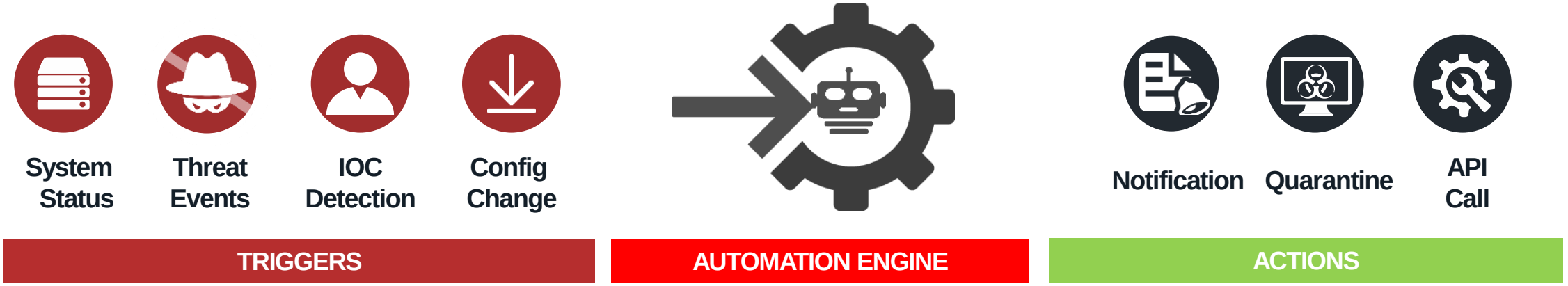
Сканирование файлов https

- Для проверки файлов, передаваемых зашифрованными протоколами необходима их SSL deep inspection



Автоматизация (Automation)

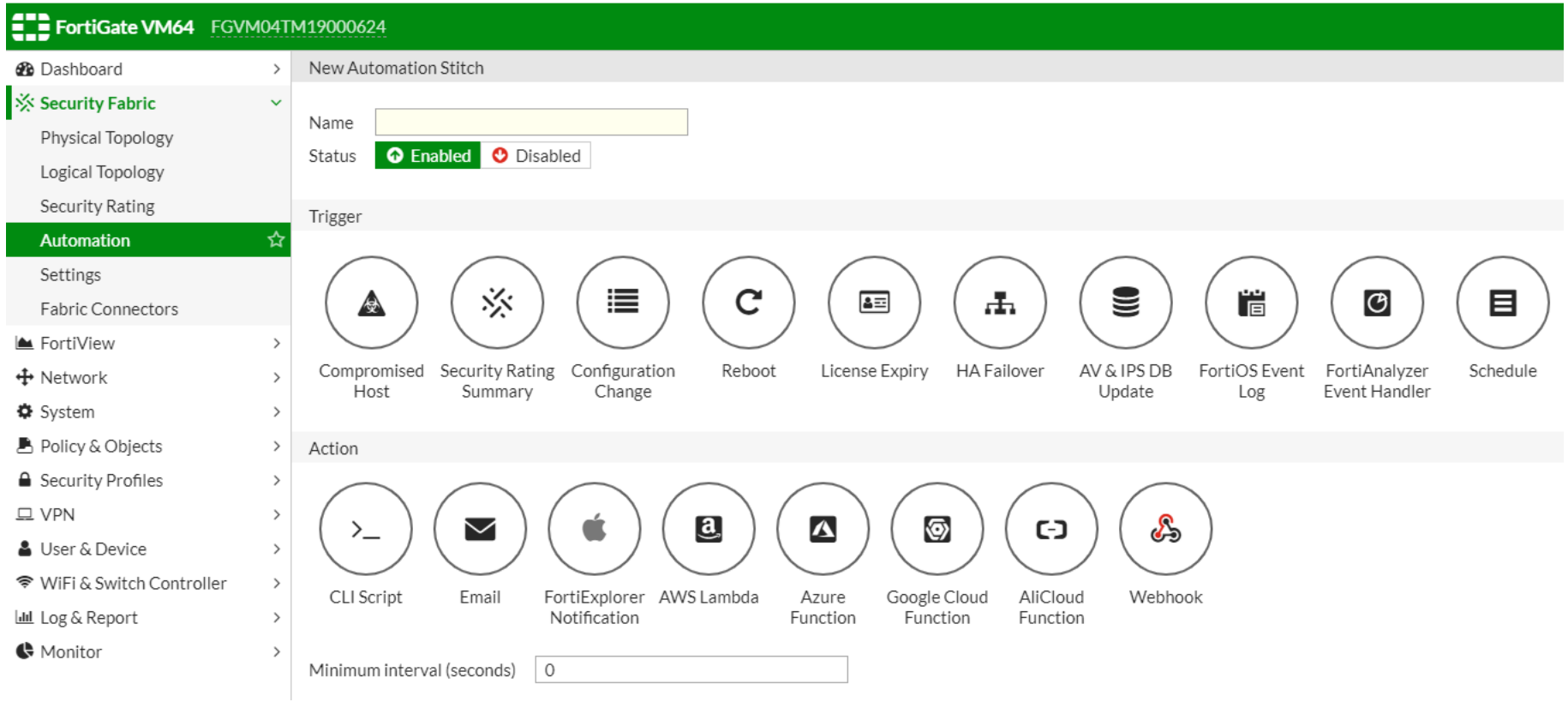
Автоматизация (Automation)



- Способность FortiOS автоматически реагировать на события предварительно запрограммированным способом (stitches)
- Администратором создаются автоматизированные действия (actions) при наступлении определенных условий (triggers)
- Интеграция с элементами Security Fabric

Автоматизация - wizard

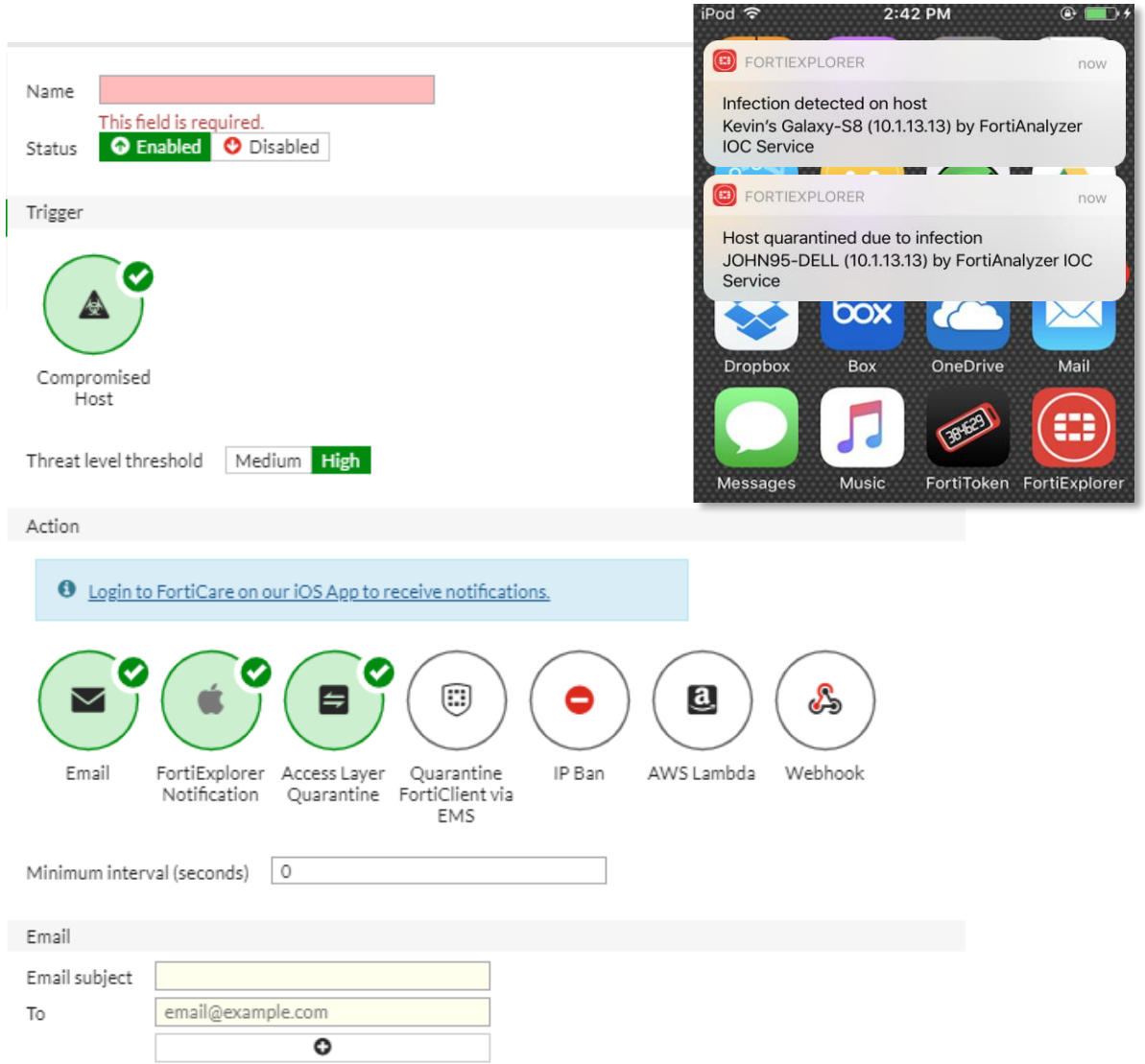
Wizard, помогающий администратору легко настроить автоматизацию с помощью существующих компонентов



Low-memory (CLI)
High-cpu (CLI)

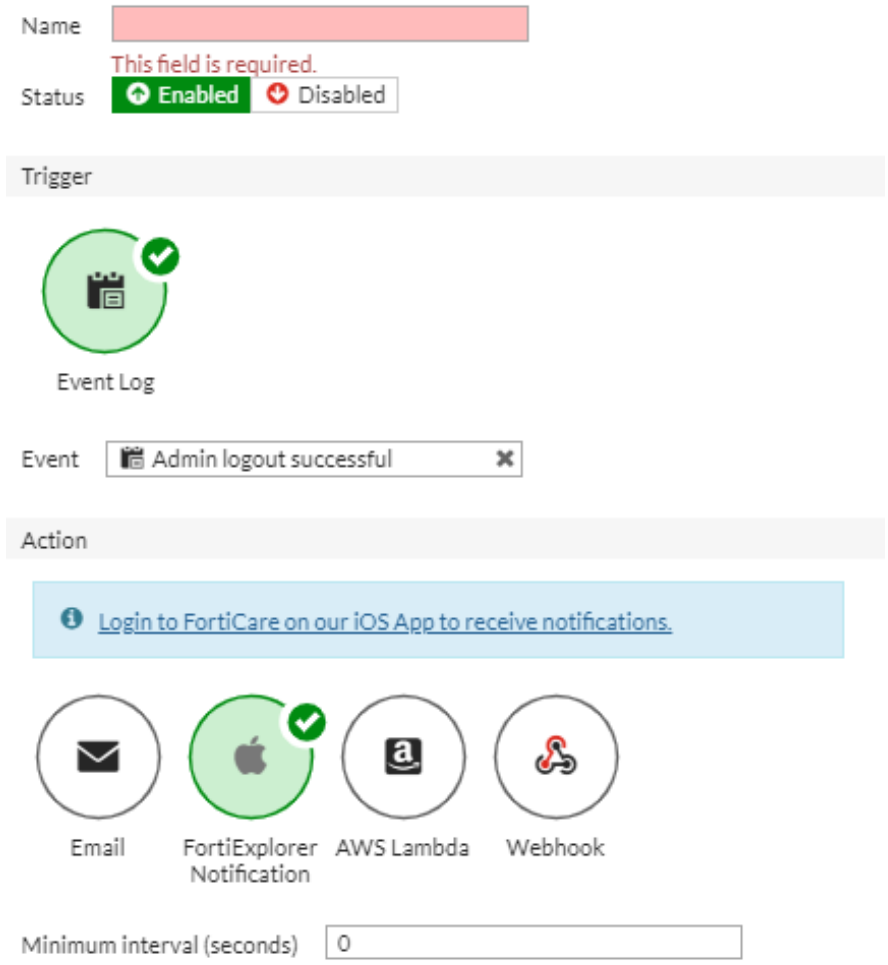
Автоматизация - реакция на события на примере: “компроментация → карантин + уведомление”

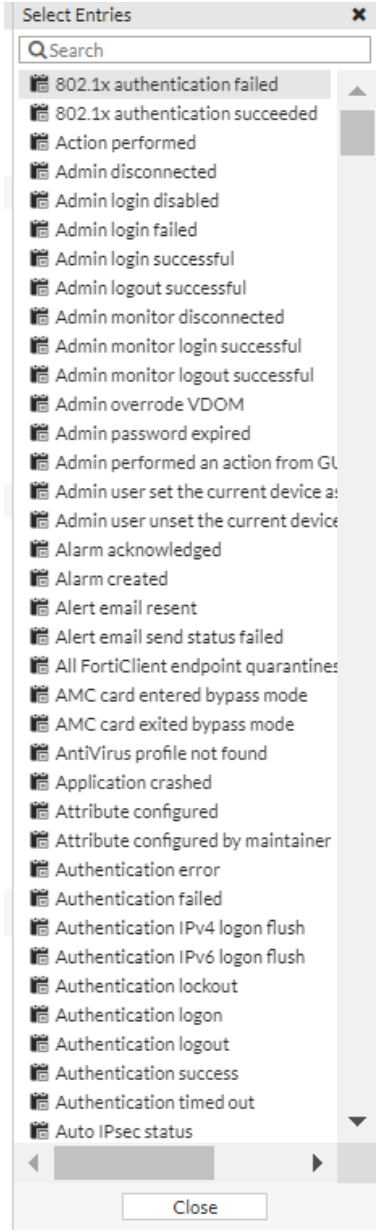
- **Автоматически изолировать** скомпрометированный хост (Threat/IOC от FAZ на FG)
- Отправить **уведомление по email** и через **FortiExplorer**
- Задать **интервал повторения** (кол-во срабатываний)
- Опционально сделать это возможно, через EMS (для FortiClient)



Автоматизация - реакция на события на примере “event log → уведомление”

- **Автоматически отправить уведомление** через **FortiExplorer** при срабатывании одного из событий (Event Log)
- Задать **интервал повторения** (кол-во срабатываний)

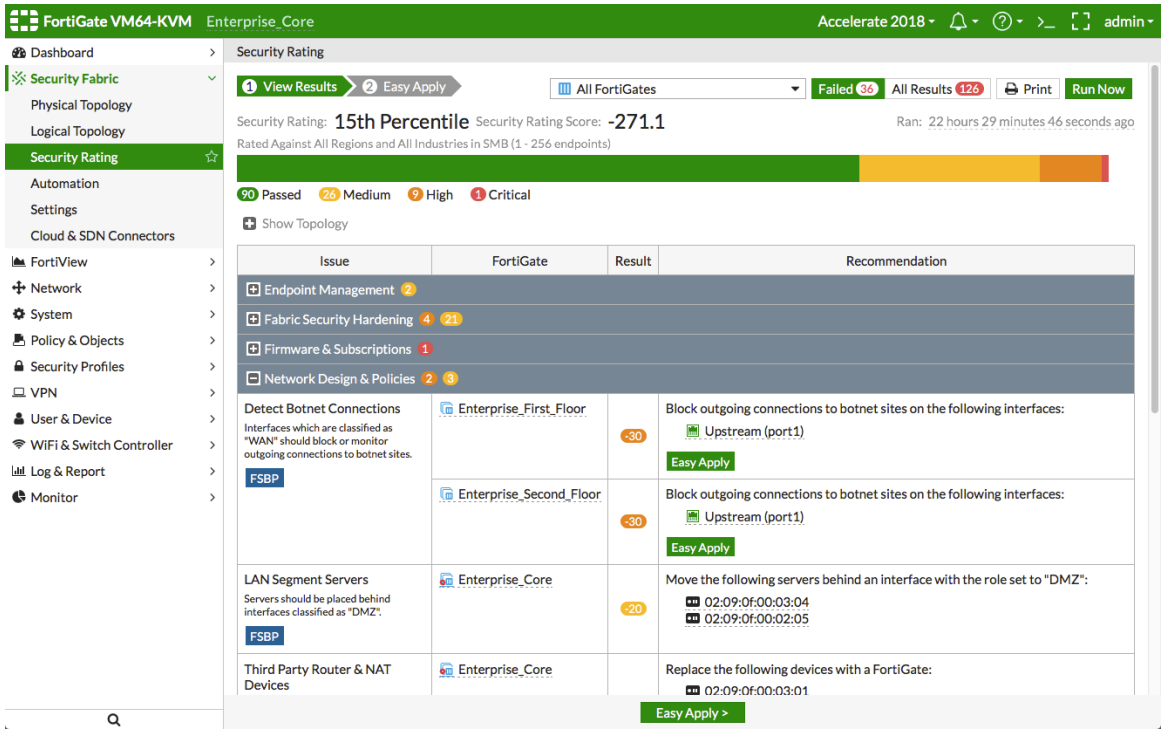




Security Fabric Rating

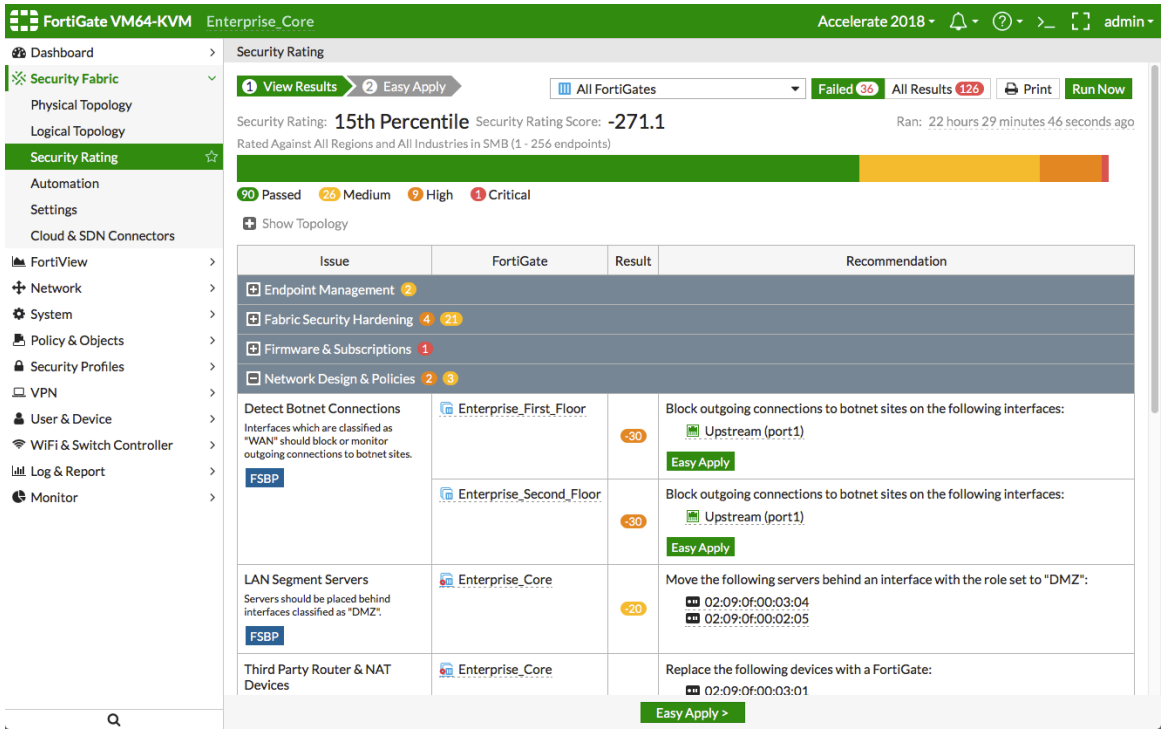
Security Fabric Rating
Адаптивный анализ защищенности

- **Анализ безопасности** инфраструктуры
- Запускается **по расписанию или по требованию**
- Позволяет оценить **уровень защищенности и корректность настроек на основе рекомендаций Fortinet**
- Результат анализа – рейтинг безопасности с отображением рекомендуемых действий для усиления защиты, пройденных и непройденных проверок
- Требует **Security Rating License** на каждое устройство в Security Fabric



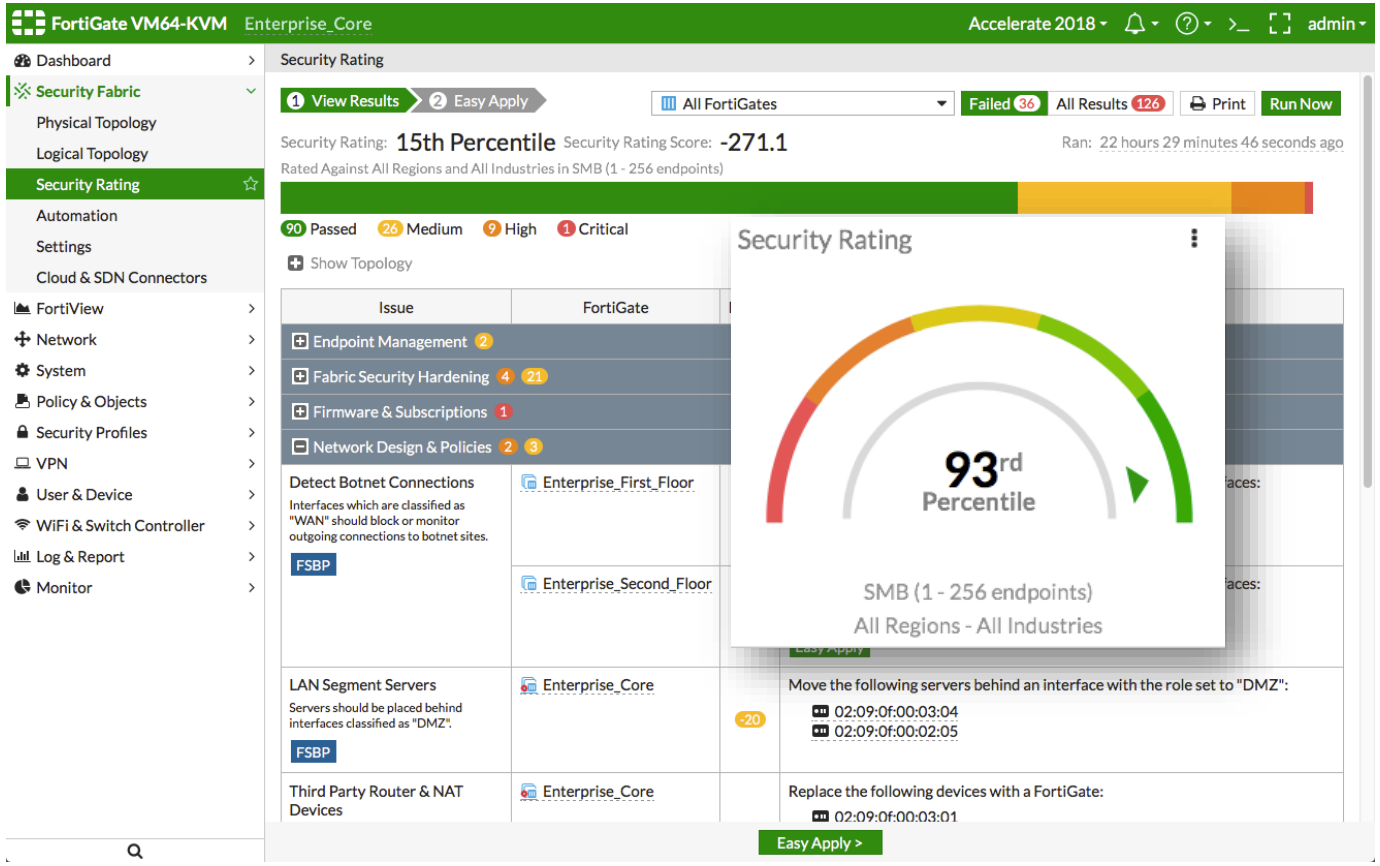
Security Fabric Rating примеры проверок

- **Проверки устройств и всей security fabric:**
  - Наличие защиты конечных станций
  - Корректность конфигурации
  - Статус подписок на сервисы безопасности
  - Сетевой дизайн и политики
  - Наличие средств защиты от ATP
- Рекомендации по исправлению или возможность автоматического исправления **“one-click Easy Apply”**



Security Fabric Rating рейтинг по отрасли

- Рейтинг по сравнению с **аналогичными организациями** по размеру и отрасли (при отправке своего рейтинга в FortiGuard)
- **Ранжирование по отрасли**



ЗАКЛЮЧЕНИЕ

FortiOS - единая ОС для FortiGate

Configuration	Log & Report	Diagnostics	Monitoring	**Operation**	Systems Integration	Central Mgmt. and Provisioning	Cloud & SDN Integration
					Visibility	Automation	
Policy Objects	Device Identification	SSL inspection	Actions	**Policy and Control**	AAA	Compliance & Security Rating	
Anti-Malware	IPS & DoS	Application Control	Web Filtering	**Security**	Advanced Threat Protection (ATP)	Vulnerability Assessment	IOC Detection
Firewall	VPN	DLP	Email Filtering				
SD WAN	Explicit Proxy	IPv6	High Availability	**Networking**	Wireless Controller	Switch Controller	WAN Interface Manager
Routing/NAT	L2/Switching	Offline Inspection	Essential Network Services				
Physical Appliance (+SPU)	Virtual System	Hypervisor	Cloud	**Platform Support**	**Security Fabric**		

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortios-6-2.pdf

* Features availability may varied by models

Варианты подписок на сервисы безопасности

FortiGuard

Advance Malware Protection

- Anti-Bot
- Antivirus
- Virus Outbreak Protection
- Content Disarm & Reconstruction
- Mobile AV Security
- FortiSandbox Cloud

Advanced Threat Protection

Advance Malware Protection

+

Intrusion Prevention

Unified Protection

Advance Malware Protection

+

Intrusion Prevention

Web Filtering

Anti-Spam

Enterprise Protection

Advance Malware Protection

+

Intrusion Prevention

Web Filtering

Anti-Spam

Security Rating Service

FortiCASB

Industrial Signatures

Very Flexible and Diverse Advanced Security Offerings

Спасибо !

Вопросы ?

Максим Порицький
Systems Engineer, CCIE
mporytskyy@fortinet.com