



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			

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

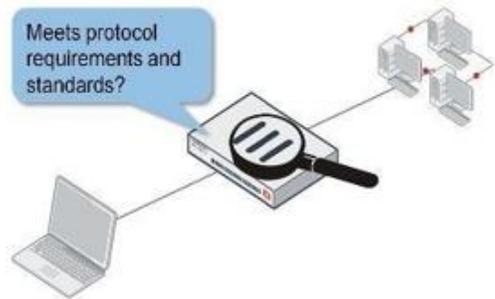
- ✓ Rate-based IPS
- ✓ DoS политики
- ✓ Средствами проверки корректности протоколов
- ✓ Sandbox

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, периодическое обновление из FortiGuard, требует подписку



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

AntiVirus & IPS Updates

Accept push updates

Scheduled Updates Every Hours

Improve IPS quality

Use extended IPS signature package

Update Server Location

US only

Intrusion Prevention

IPS Definitions

IPS Engine

Malicious URLs

Licensed - expires on 2020/02/27

Version 14.00588

Version 4.00029

Version 2.00183

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

The screenshot shows the FortiGuard IPS GUI. At the top, there is a table of signatures with columns: Name, Exempt IPs, Severity, Target, Service, OS, Action, and Packet Logging. The first row is highlighted: 3Com.3CDAemon.FTP.Server.Buffer.Overflow, 1, [Severity: 4/5], Server, TCP,FTP, Windows, Default, [Packet Logging: Pass]. Below the table, there are buttons for '+ Add Filter', 'Edit Filter', and 'Delete'. A 'Filter Details' section shows the selected signature's details, including 'Severity: [4/5]' and 'Action: Default'. A 'Packet Logging' dropdown menu is open, showing options: Pass, Monitor, Block, Reset, Default, Quarantine, Enable, and Disable.

The screenshot shows a detailed view of a signature in the FortiGuard IPS GUI. The signature is '3Com.3CDAemon.FTP.Server.Buffer.Overflow'. The 'Severity' is 4/5. The 'Target' is 'Server' and the 'OS' is 'Windows'. The 'Summary' states: 'This indicates an attack attempt to exploit a Buffer Overflow vulnerability in 3CDAemon FTP server.' The 'Impact' is 'System Compromise: Remote attackers can gain control of vulnerable systems'. The 'Recommendation' is 'Currently we are not aware of any vendor supplied patch for this issue.' The 'Affected Products' section lists '3Com 3CDAemon 2.0 revision 10.' There are also sections for 'Name', 'Description', and 'Affected Products'.

The screenshot shows the FortiGuard Labs website. The main content is a CVE entry for '3Com.3CDAemon.FTP.Server.Information.Disclosure'. The entry includes a description: 'It indicates a possible exploit of information disclosure vulnerability in 3Com 3CDAemon. 3CDAemon is a free TFTP, FTP, and Syslog daemon for Microsoft Windows platforms. A vulnerability is reported in it that allow an attacker retrieve information from server such as installation path A remote attackers to may sensitive information via a cd command that contains an MS-DOS device name, which reveals the installation path in an error message.' The entry also lists 'Affected Products' as '3Com 3CDAemon 2.0 revision 10.' The website has a navigation bar with 'News / Research', 'Services', 'Threat Lookup', 'Resources', and 'Search FortiGuard'. There is also a 'CVE List' section with buttons for 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request CVE IDs', and 'Update a CVE Entry'. The total number of CVE entries is 115158.

The screenshot shows the CVE website. The main content is a CVE entry for 'CVE-2005-0278'. The entry includes a description: 'The FTP service in 3Com 3CDAemon 2.0 revision 10 allows remote attackers to gain sensitive information via a cd command that contains an MS-DOS device name, which reveals the installation path in an error message.' The entry also lists 'Affected Products' as '3Com 3CDAemon 2.0 revision 10.' The website has a navigation bar with 'CVE List', 'CNAs', 'Board', 'About', and 'News & Blog'. There is also a 'NVD' section with buttons for 'Go to: CVSS Scores', 'CPE Info', and 'Advanced Search'.

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
<input checked="" type="checkbox"/>	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	Expires 1 Da
<input checked="" type="checkbox"/>	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	None
<input checked="" type="checkbox"/>	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	None
<input checked="" type="checkbox"/>	FTP.Login.Brute.Force	<input type="text" value="200"/>	<input type="text" value="10"/>	<div style="border: 1px solid black; padding: 2px;"><div style="background-color: #e0e0e0; padding: 2px;">Any</div><div style="background-color: #0070c0; color: white; padding: 2px;">Any</div><div style="padding: 2px;">Source IP</div><div style="padding: 2px;">Destination IP</div></div>	<div style="border: 1px solid black; padding: 2px;"><div style="background-color: #e0e0e0; padding: 2px;">Block</div></div>	Expires 2 Da
<input checked="" type="checkbox"/>	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	None
<input checked="" type="checkbox"/>	IMAP.Login.Brute.Force	60	10	Any	Block	None
<input checked="" type="checkbox"/>	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	None

IPS & DOS

Malicious (malware and exploit) URL database

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

Edit IPS Sensor

Name

Comments

25/255

Block malicious URLs



SECURITY

IPS & DOS

DoS protection

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

New DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

L3 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000

L4 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
tcp_syn_flood	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		2000
tcp_port_scan	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		1000
tcp_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
tcp_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
udp_flood	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		2000
udp_scan	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		2000
udp_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
udp_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
icmp_flood	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		250
icmp_sweep	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		100

Application Control

APPLICATION CONTROL

- **Для чего:**
 - Обнаружение и идентификация приложений, применение соответствующих политик безопасности и/или функция качества обслуживания (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

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

The screenshot shows the Fortinet management console interface for Application Control. On the left, a sidebar menu lists various security features, with 'Application Control' highlighted in green. The main area displays a 'Categories' list with items like Business, Email, Mobile, Proxy, and Storage.Backup. A 'Monitor' dropdown menu is open for the 'Cloud.IT' category, showing options: Allow (checked), Block, and Quarantine. At the bottom right, there is an 'Apply' button.

SECURITY

APPLICATION CONTROL

- 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 шифрование требуют SSL deep inspection
- Запрос на добавление сигнатур под специфичные пользовательские приложения на FortiGuard

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

<http://fortiguard.com/appcontrol>

FortiGuard Labs News / Research Services Threat Lookup Resources Search FortiGuard

Home / Application Control

Application Control

Browse the FortiGuard Labs extensive encyclopedia of applications. Click any title to view more details of the application. Can't find what you are looking for? Try using the search bar above to find a specific application description.

DMSniff.Botnet (Botnet)
This indicates that a system might be infected by DMSniff Botnet. DMSniff is a Point-of-sale malware that infects in breaches of...
Apr 11, 2019 RISK: POPULARITY: ★★★★★

WINNTI.Botnet (Botnet)
This indicates that a system might be infected by WINNTI Botnet or undergoing a scanning attempt by WINNTI nmap script.
Apr 10, 2019 RISK: POPULARITY: ★★★★★

FortiGuard Labs News / Research Services Threat Lookup Resources Search FortiGuard

Home / FAQ / Application Control Submission Form

Application Control Submission Form

At a glance:
If you would like Fortinet to categorize your application, submit this form. Fortinet operators will review your request and respond in a timely manner.

Application Details

Application Name Version(s)

Language Location (URL)

Your Contact Information

Name Email

Please enter your name Please enter a contact email address

Company Name

Additional Information/Configuration

SECURITY

APPLICATION CONTROL

- Создание соответствующих вашей инфраструктуре **АС 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 **АС 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
```

Application Sensor Configuration Interface

Categories:

- Business (140, ☁ 6)
- Email (78, ☁ 12)
- Mobile (3)
- Proxy (165)
- Storage.Backup (162, ☁ 17)
- VoIP (24)
- Cloud.IT (45)
- Game (84)
- Network.Service (329)
- Remote.Access (82)
- Update (49)
- Web.Client (23)
- Collaboration (252, ☁ 10)
- General.Interest (224, ☁ 7)
- P2P (59)
- Social.Media (118, ☁ 31)
- Video/Audio (150, ☁ 14)
- Unknown Applications

Application Overrides: + Add Signatures, Edit Parameters, Delete

Filter Overrides: + Add Filter, Edit, Delete

Application Signature List

Name	Category	Technology	Popularity	Risk
Cisco.Spark	Collaboration	Browser-Based, Client-Server	★★★★☆	Low
Cisco.VPN.Client	Proxy	Client-Server	★★★★☆	Low
Meraki.Cloud.Controller	Cloud.IT	Client-Server	★★★★☆	Low
Skinny	Collaboration	Client-Server	★★★★☆	Low
WCCPV1	Collaboration	Client-Server	★★★★☆	Low
WCCPV2	Collaboration	Client-Server	★★★★☆	Low
WebEx	Collaboration	Client-Server	★★★★☆	Low
WebEx_Chat	Collaboration	Client-Server	★★★★☆	Low
WebEx_Desktop.Sharing	Collaboration	Client-Server	★★★★☆	Low
WebEx_File.Download	Collaboration	Client-Server	★★★★☆	Low
WebEx_File.Sharing	Collaboration	Client-Server	★★★★☆	Low
WebEx_File.Upload	Collaboration	Client-Server	★★★★☆	Low
WebEx_Login	Collaboration	Browser-Based	★★★★☆	Low
WebEx_Remote.Control	Collaboration	Browser-Based, Client-Server	★★★★☆	Low
WebEx_WhiteBoard	Collaboration	Browser-Based, Client-Server	★★★★☆	Low

Facebook_Post ☁ 🔒	Social.Media	Allow
Facebook_Search 🔒	Social.Media	Monitor
Facebook_Video.Play	Social.Media	Block

APPLICATION CONTROL

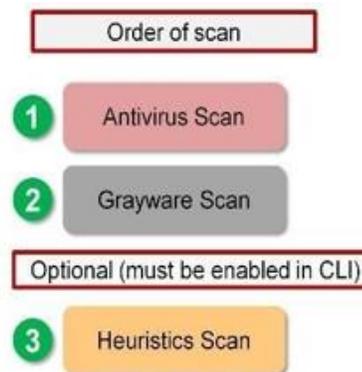
- **Traffic shaping** - качество обслуживания трафика для разных приложений с конфигурацией гарантированной и максимальной пропускной способностью (maximum or guaranteed bandwidth)
- **User notification** - отображение сообщения о блокировке приложения (только для HTTP/HTTPS app), для non-HTTP/HTTPS 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

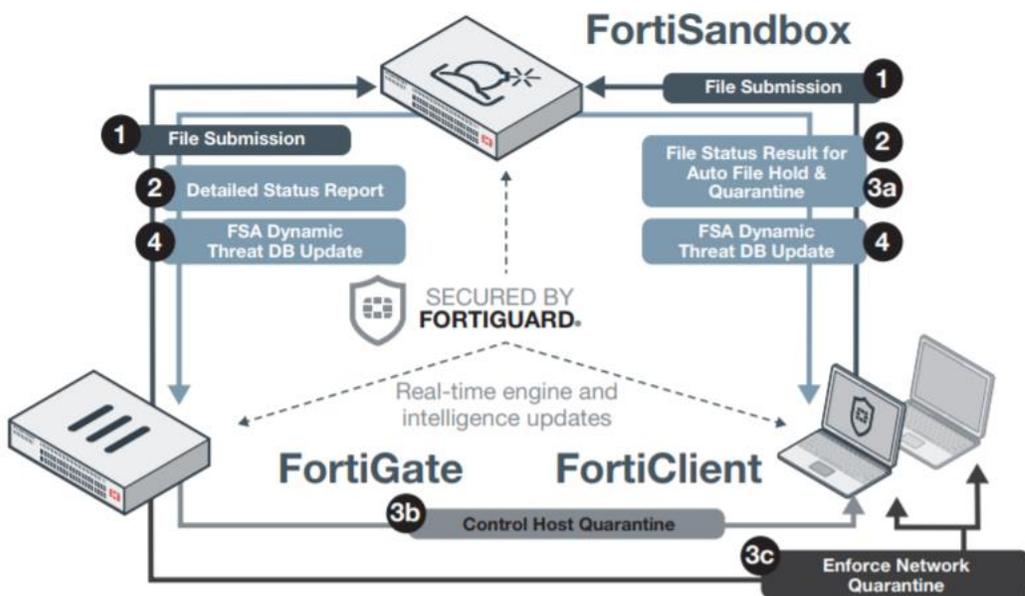
- **Цель:**
 - За счет интегрированных технологий **предотвратить** проникновени разнообразных **вредоносных программ** (malware) в вашу сеть
 - ✓ Известные malware
 - ✓ Неизвестные malware
 - **Проверка файлов** передаваемых по протоколам - HTTP, FTP, IMAP, POP3, SMTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS, FTPS.
- **Antivirus scan** - обнаружение известных вирусов на основе сопоставления сигнатур (antivirus signature)
- **Grayware scan** - обнаружение “нежелательных” программ на основе сопоставления сигнатур (grayware signature)
- **Heuristics scan** - сканирования основанные на вероятности идентификации неизвестных угроз - подозрительных файлов (suspicious файл)



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

FortiCloud (Europe) ⋮Status ✔ [Activated](#)Log Retention ✔ [Free License](#)Storage Used 0BFortiSandbox Cloud ✔ [Licensed](#)Files Uploaded Today 0%

Security Fabric Settings

FortiSandbox type FortiSandbox CloudFortiCloud account

Applied Threat Intelligence

Dynamic Malware Detection version	2.663841 (signatures: not loaded)
URL Threat Detection version	2.1121868 (entries: 448)

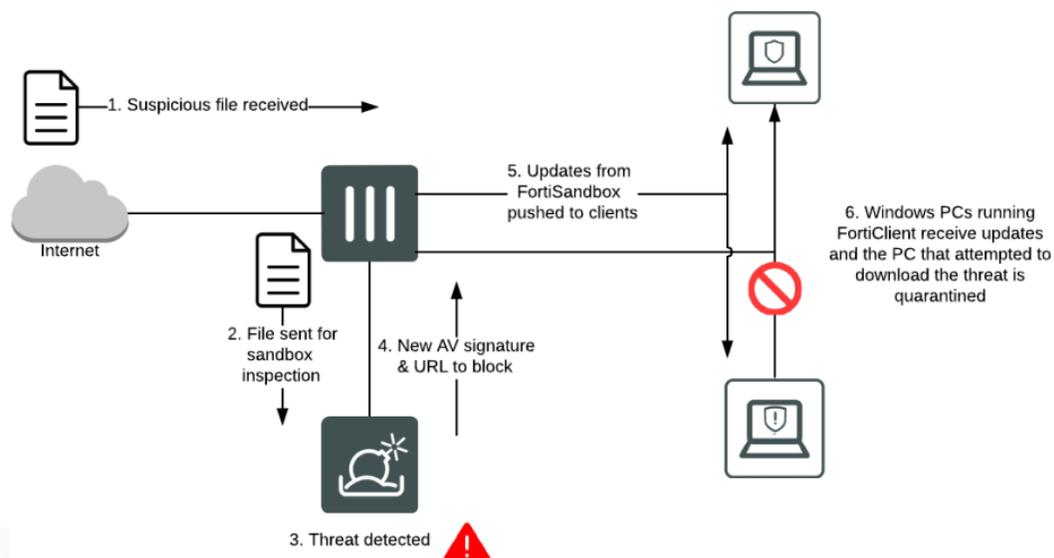
FortiSandbox Statistics (last 7 days)

File type	Detected
Total submitted	0
Critical (Malicious)	0
High Risk	0
Medium Risk	0
Low Risk	0
Clean	0

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**



New AntiVirus Profile

Name

Comments 0/255

Scan Mode Quick Full

Detect Viruses Block Monitor

Inspected Protocols

HTTP

SMTP

POP3

IMAP

MAPI

FTP

CIFS

APT Protection Options

Content Disarm and Reconstruction

Original File Destination FortiSandbox File Quarantine Discard

Treat Windows Executables in Email Attachments as Viruses

Send Files to FortiSandbox Cloud for Inspection None Suspicious Files Only All Supported Files

Use FortiSandbox Database

Include Mobile Malware Protection

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List

ANTIVIRUS / ANTIMALWARE

ОБНОВЛЕНИЯ ANTIVIRUS DB

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

AntiVirus & IPS Updates

Accept push updates 

Use override push

Scheduled Updates

Improve IPS quality 

Use extended IPS signature package

Every Hours

 Update AV & IPS Definitions

AntiVirus

 Licensed - expires on 2020/02/26

AV Definitions

 Version 67.00985

AV Engine

 Version 6.00127

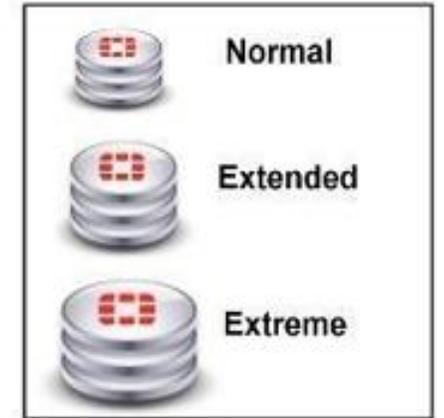
Mobile Malware

 Version 67.00985

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}
```

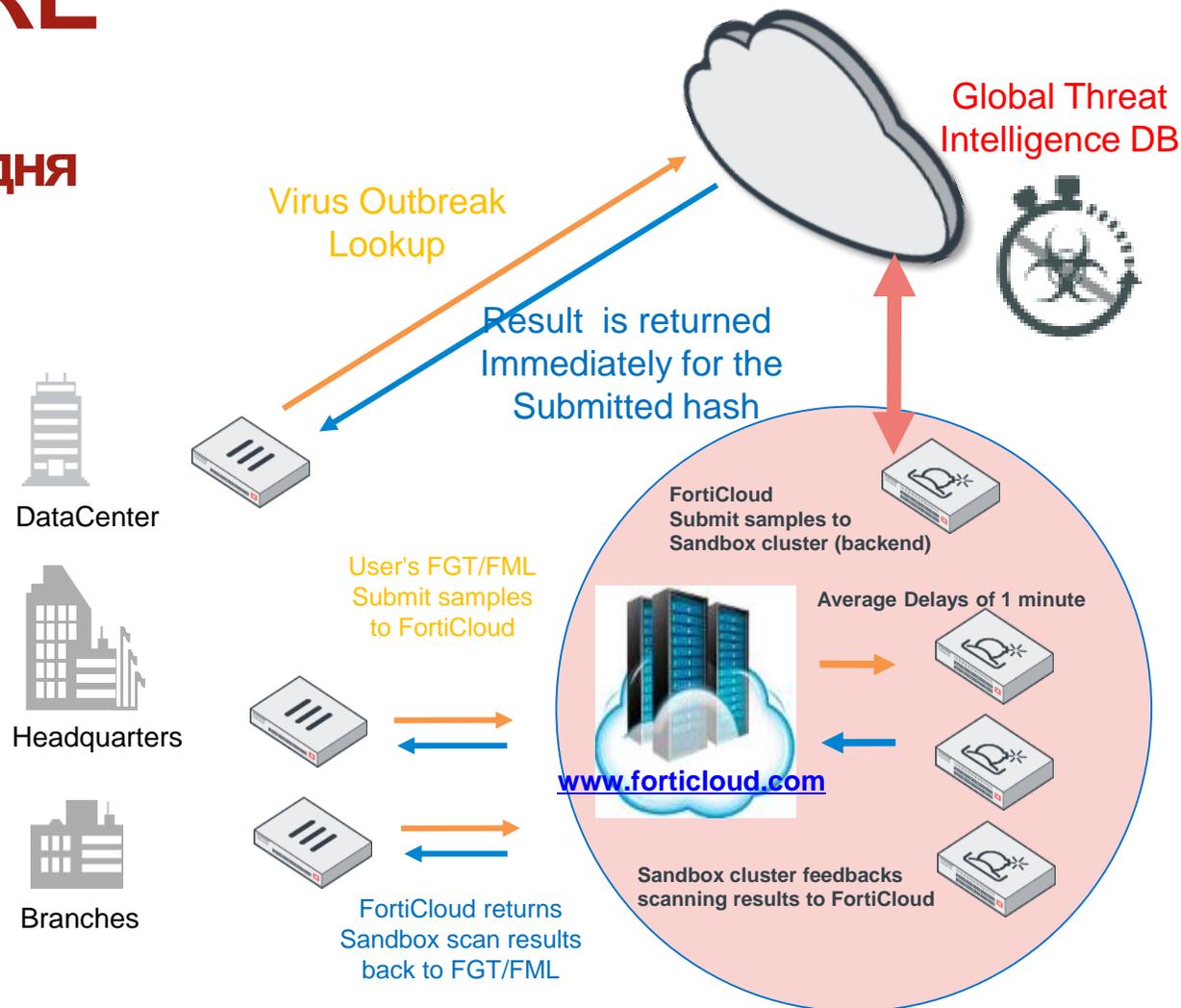
compact DB (меньше сигнатур, в IPS Engine) – только для Quick scan mode

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



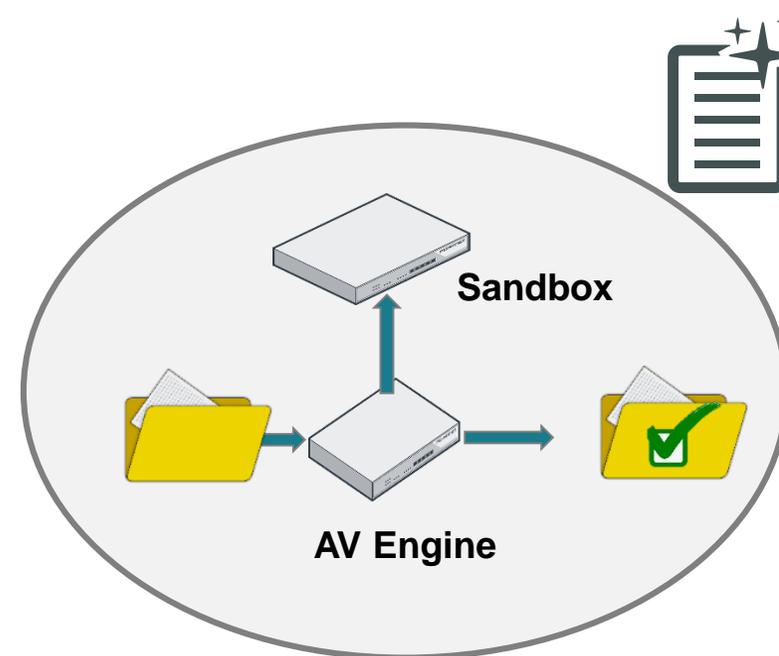
FortiGate/FortiMail

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**



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
```

New Protocol Options

Name

Comments 0/255

Log Oversized Files

RPC over HTTP

Protocol Port Mapping

HTTP	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="80"/>
SMTP	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="25"/>
POP3	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="110"/>
IMAP	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="143"/>
FTP	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="21"/>
NNTP	<input checked="" type="checkbox"/>	any	Specify	<input type="text" value="119"/>
MAPI	<input checked="" type="checkbox"/>			<input type="text" value="135"/>
DNS	<input checked="" type="checkbox"/>			<input type="text" value="53"/>
CIFS	<input checked="" type="checkbox"/>			<input type="text" value="445"/>

Common Options

Comfort Clients

Interval (seconds)

Amount (bytes)

Block Oversized File/Email

Threshold (MB)

ANTIVIRUS / ANTIMALWARE

Сканирование файлов https

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

Edit Policy

Name ⓘ	test
Incoming Interface	port4 + x
Outgoing Interface	port6 + x
Source	all + x
Destination	all + x
Schedule	always v
Service	ALL + x
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

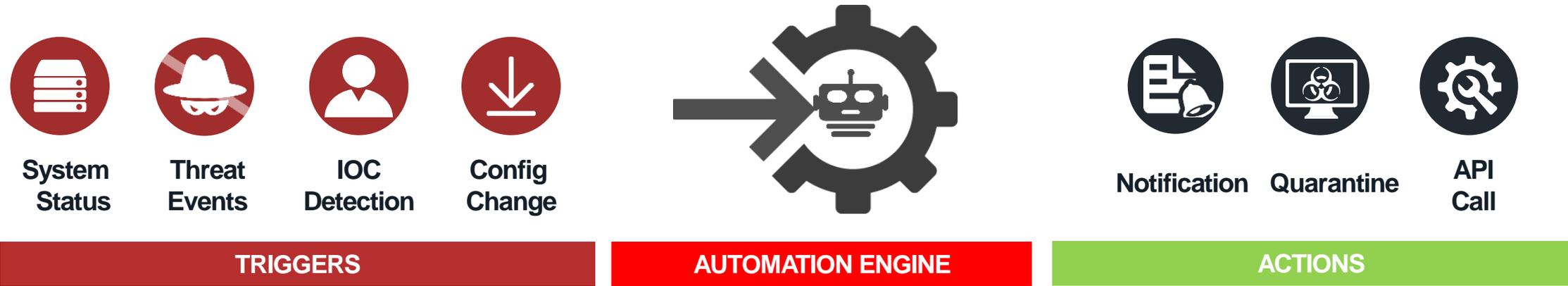
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool
Preserve Source Port	<input type="checkbox"/>
Protocol Options	PRX default v

Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV default v
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
VoIP	<input type="checkbox"/>
SSL Inspection ⚠	SSL deep-inspection v
Mirror SSL Traffic to Interfaces	<input type="checkbox"/>

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

FortiGate VM64 FGVM04TM19000624

Dashboard > New Automation Stitch

Security Fabric >

Physical Topology

Logical Topology

Security Rating

Automation ☆

Settings

Fabric Connectors

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Name

Status Enabled Disabled

Trigger

Compromised Host

Security Rating Summary

Configuration Change

Reboot

License Expiry

HA Failover

AV & IPS DB Update

FortiOS Event Log

FortiAnalyzer Event Handler

Schedule

Action

CLI Script

Email

FortiExplorer Notification

AWS Lambda

Azure Function

Google Cloud Function

AliCloud Function

Webhook

Minimum interval (seconds)

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)

The image shows a configuration interface for an automation rule in FortiGuard Manager. The rule is named "Compromised Host" and is currently "Enabled". The trigger is set to "Compromised Host" with a "High" threat level threshold. The action section includes a link to login to the FortiCare iOS app for notifications and several action options: Email, FortiExplorer Notification, Access Layer Quarantine, Quarantine FortiClient via EMS, IP Ban, AWS Lambda, and Webhook. The "Email" action is selected. Below the action options, the "Minimum interval (seconds)" is set to 0. The "Email" configuration section shows the "To" field set to "email@example.com".

Next to the configuration interface is a screenshot of an iPod home screen at 2:42 PM. It displays two notifications from the FortiExplorer app. The first notification says: "Infection detected on host Kevin's Galaxy-S8 (10.1.13.13) by FortiAnalyzer IOC Service". The second notification says: "Host quarantined due to infection JOHN95-DELL (10.1.13.13) by FortiAnalyzer IOC Service". The home screen also shows various app icons like Dropbox, Box, OneDrive, Mail, Messages, Music, FortiToken, and FortiExplorer.

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)

Name

This field is required.

Status Enabled Disabled

Trigger



Event Log

Event

Action

[Login to FortiCare on our iOS App to receive notifications.](#)



Email



FortiExplorer
Notification



AWS Lambda



Webhook

Minimum interval (seconds)

Select Entries

- 802.1x authentication failed
- 802.1x authentication succeeded
- Action performed
- Admin disconnected
- Admin login disabled
- Admin login failed
- Admin login successful
- Admin logout successful
- Admin monitor disconnected
- Admin monitor login successful
- Admin monitor logout successful
- Admin override VDOM
- Admin password expired
- Admin performed an action from GL
- Admin user set the current device a:
- Admin user unset the current device
- Alarm acknowledged
- Alarm created
- Alert email resent
- Alert email send status failed
- All FortiClient endpoint quarantines
- AMC card entered bypass mode
- AMC card exited bypass mode
- AntiVirus profile not found
- Application crashed
- Attribute configured
- Attribute configured by maintainer
- Authentication error
- Authentication failed
- Authentication IPv4 logon flush
- Authentication IPv6 logon flush
- Authentication lockout
- Authentication logon
- Authentication logout
- Authentication success
- Authentication timed out
- Auto IPsec status

Close

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
- Требуется **Security Rating License** на каждое устройство в Security Fabric

FortiGate VM64-KVM Enterprise_Core Accelerate 2018 admin

Security Rating

1 View Results 2 Easy Apply All FortiGates Failed 36 All Results 126 Print Run Now

Security Rating: **15th Percentile** Security Rating Score: **-271.1** Ran: 22 hours 29 minutes 46 seconds ago
Rated Against All Regions and All Industries in SMB (1 - 256 endpoints)

90 Passed 26 Medium 9 High 1 Critical

Show Topology

Issue	FortiGate	Result	Recommendation
Endpoint Management 2			
Fabric Security Hardening 4 21			
Firmware & Subscriptions 1			
Network Design & Policies 2 3			
Detect Botnet Connections Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites. FSBP	Enterprise_First_Floor	-30	Block outgoing connections to botnet sites on the following interfaces: Upstream (port1) Easy Apply
	Enterprise_Second_Floor	-30	Block outgoing connections to botnet sites on the following interfaces: Upstream (port1) Easy Apply
LAN Segment Servers Servers should be placed behind interfaces classified as "DMZ". FSBP	Enterprise_Core	-20	Move the following servers behind an interface with the role set to "DMZ": 02:09:0f:00:03:04 02:09:0f:00:02:05
Third Party Router & NAT Devices	Enterprise_Core		Replace the following devices with a FortiGate: 02:09:0f:00:03:01 Easy Apply >

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 АТР

■ Рекомендации по исправлению или возможность автоматического исправления “one-click Easy Apply”

The screenshot displays the FortiGate VM64-KVM Security Rating interface. The top navigation bar includes the FortiGate logo, the device name 'Enterprise_Core', and the user 'admin'. The main content area shows the 'Security Rating' section with a 'View Results' button and a 'Failed 36' indicator. The current Security Rating is '15th Percentile' with a score of '-271.1'. A progress bar indicates the status: 90 Passed, 26 Medium, 9 High, and 1 Critical. Below this, a table lists several issues with 'Easy Apply' buttons for each.

Issue	FortiGate	Result	Recommendation
Endpoint Management 2			
Fabric Security Hardening 4 21			
Firmware & Subscriptions 1			
Network Design & Policies 2 3			
Detect Botnet Connections Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites. FSBP	Enterprise_First_Floor	-30	Block outgoing connections to botnet sites on the following interfaces: Upstream (port1) Easy Apply
	Enterprise_Second_Floor	-30	Block outgoing connections to botnet sites on the following interfaces: Upstream (port1) Easy Apply
LAN Segment Servers Servers should be placed behind interfaces classified as "DMZ". FSBP	Enterprise_Core	-20	Move the following servers behind an interface with the role set to "DMZ": 02:09:0f:00:03:04 02:09:0f:00:02:05
Third Party Router & NAT Devices	Enterprise_Core		Replace the following devices with a FortiGate: 02:09:0f:00:03:01

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

The screenshot displays the FortiGate VM64-KVM Security Rating interface. The top navigation bar includes 'FortiGate VM64-KVM Enterprise_Core' and 'Accelerate 2018'. The left sidebar lists various system components, with 'Security Rating' selected. The main content area shows the 'Security Rating' section with a 'View Results' button and a dropdown menu set to 'All FortiGates'. The current status is 'Failed 36' out of 'All Results 126'. The security rating is '15th Percentile' with a score of '-271.1', rated against all regions and industries in SMB (1-256 endpoints). A progress bar indicates 90% Passed, 26% Medium, 9% High, and 1% Critical. A table lists issues such as 'Endpoint Management', 'Fabric Security Hardening', 'Firmware & Subscriptions', and 'Network Design & Policies'. A detailed view of the 'Detect Botnet Connections' issue is shown, highlighting 'Enterprise_First_Floor' and 'Enterprise_Second_Floor' interfaces. A 'LAN Segment Servers' issue is also visible, suggesting moving servers behind DMZ interfaces. The interface includes an 'Easy Apply' button and a search bar at the bottom.

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		

Варианты подписок на сервисы безопасности



FortiGuard

Advanced Threat Protection

Unified Protection

Enterprise Protection

Advance Malware Protection



Anti-Bot



Antivirus



Virus Outbreak Protection



Content Disarm & Reconstruction



Mobile AV Security



FortiSandbox Cloud



Advance Malware Protection



Intrusion Prevention



Advance Malware Protection



Intrusion Prevention



Web Filtering



Anti-Spam



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