



Мистецтво DDoS захисту з рішеннями Fortinet

Євгеній Таран, Systems Engineer

ytaran@fortinet.com

Таран Євгеній

- 15+ років в IT
- останні 9 років будує/модернізую IT інфраструктури та змушую веб сервіси працювати «як має бути» 😊
- IT системи міжнародних заходів (спортивні змагання, вибори тощо)
- Досвід роботи в 10 країнах регіону
- Fortinet NSE 7 і багато іншого

P.S. Це моя друга кібервійна...



В попередніх серіях

- **Security Fabric**

Усунення загроз у будь-яких мережах, кінцевих точках та хмарахостанні 9 років будуємо/модернізуємо ІТ інфраструктури та змушуємо веб сервіси працювати «як має бути» 😊

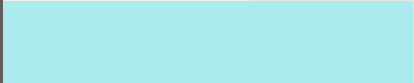
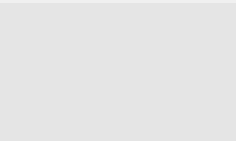
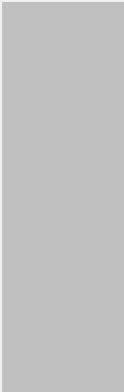
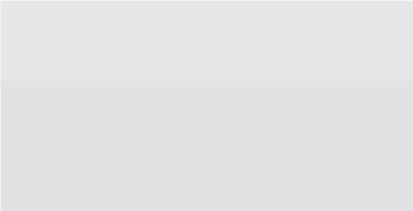
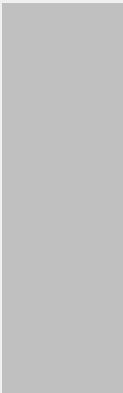
- Гібридні мережі з **Fortinet Fabric** Management Center. Побудова, адміністрування та безпека.

- **FortiMail**

Комплексний захист корпоративної пошти

- Захист веб та API сервісів за допомогою **FortiWeb**. Інтеграція з FortiGate.
- **FortiSASE**. Побудова ІТ інфраструктури та безпеки сервісів без датацентрів



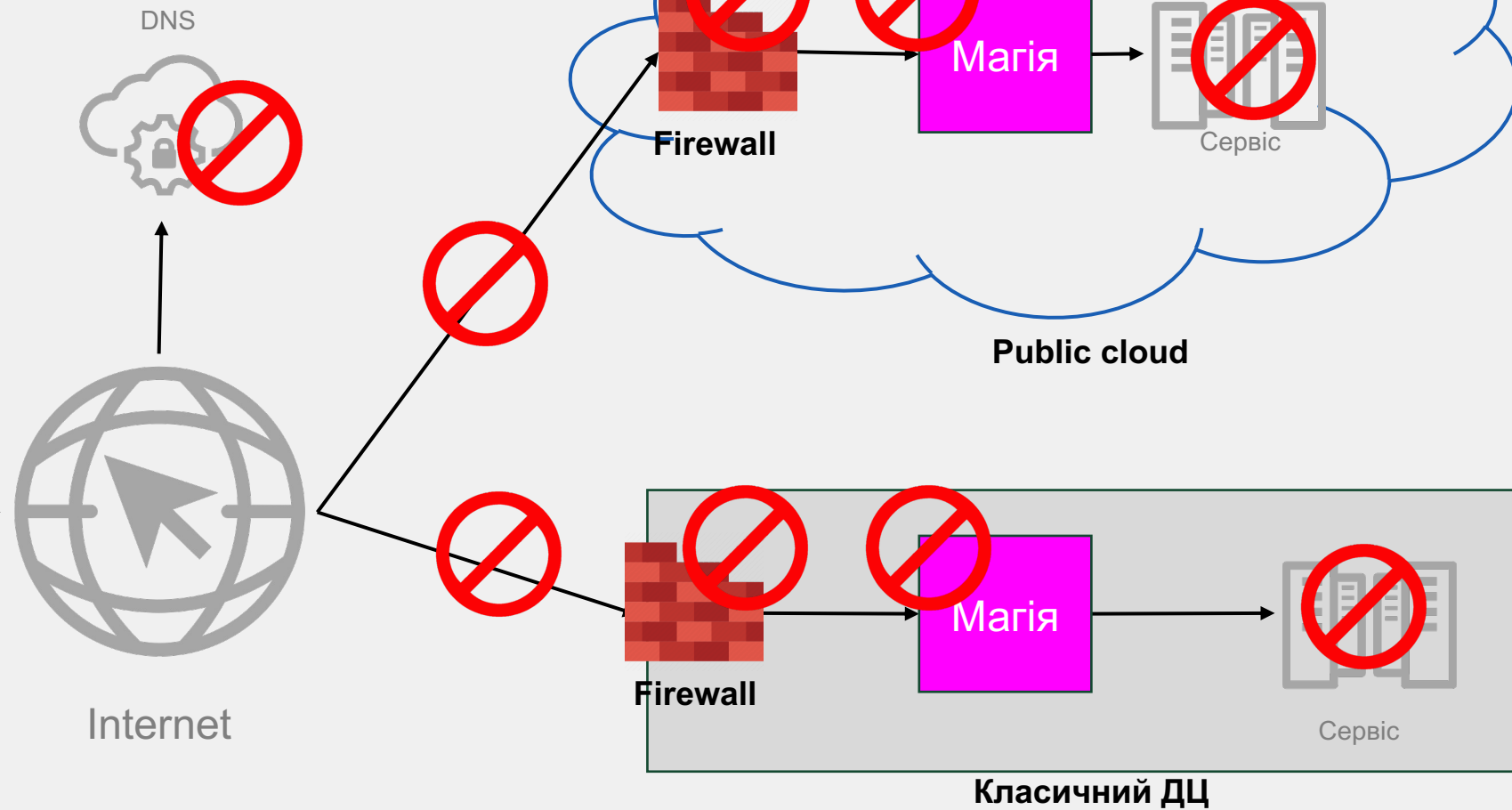
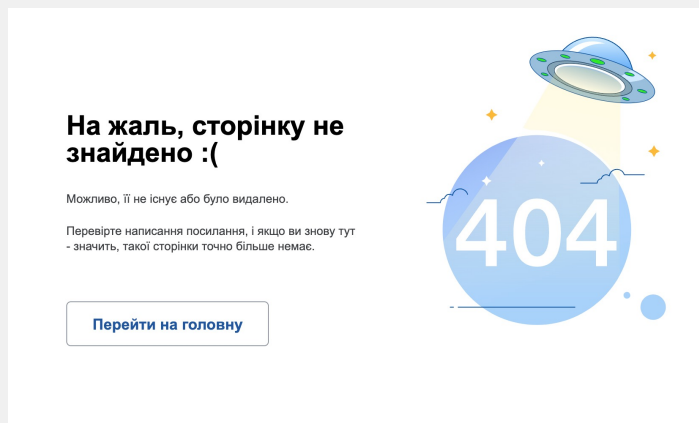


DDoS

Мета та реалізація



Мета DDoS



Приклади

Monobank зіткнувся з потужною DDoS-атакою



Автор:

Олександр Гайдамашко

13:18, 2 травня | 2 хв | Читати новість на руском



Monobank / Кол

До уваги клієнтів! DDoS атака

17.03.2018

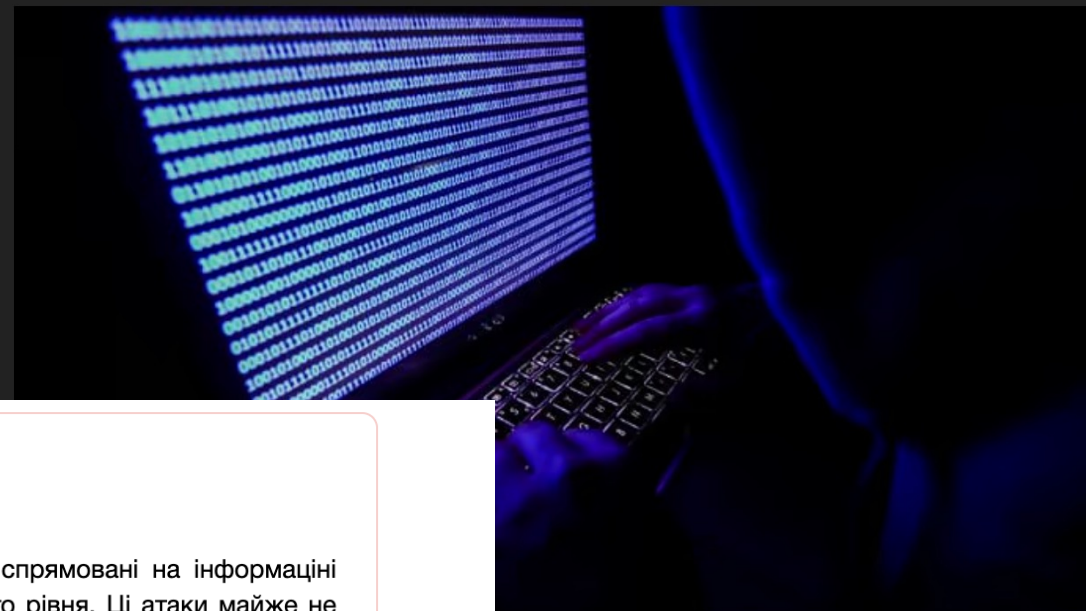
Дорогі клієнти, від учорашнього дня регулярно здійснюються DDoS-атаки, спрямовані на інформаційні системи 'Нова Пошта'. Максимальна потужність таких атак сягнула значного рівня. Ці атаки майже не впливають на надання сервісу, але інколи можливі короткострокові перебої в роботі системи. Вони не впливають на роботу відділень і всієї мережі 'Нова Пошта'. Зараз компанія працює в штатному режимі, проводить розслідування та детальний аналіз ситуації, фахівці IT працюють цілодобово.

Урядові сайти не відкриваються. Мінцифри повідомляють про масову DDoS-атаку

АЛЬОНА МАЗУРЕНКО — СЕРЕДА, 23 ЛЮТОГО 2022, 15:48



40360



ації Михайло Федоров повідомив про ржавні сайти України.



Еволюція DDoS

Хвилинка історії

Розвиток атак змушує розвивати захист

3) 2016+ Сучасність

- L3/4/7
- **Bulk Volumetric even at L7**
- SYN Flooding back
- Millions of compromised IoT devices, (home) routers and servers
- >500k random, spoofed Source IPs PER SECOND

1) Перші атаки

- Layer 3 and 4
- Bulk volumetric (SYN, ICMP)
- Spoofed / Random Source IP addresses
- Larger and larger attacks
- Used compromised servers

2) Друга ітерація

- L4 / L7 focus
- Connections / HTTP Floods
- Small, targeted attacks
- Blended 3/4/7 approaches
- Fewer attack servers needed
- “Real” Source IPs



DDoS це дешево

і таких інструментів багато

Stresser

Method:

Layer 4 (Transport Layer)

☒ DRDoS
☐ UDP
☐ UDP-Lag
☐ SYN

Layer 7 (Application Layer)

☐ RUDY
☐ Slowloris
☐ ARME

Protocol:

☐ ARD ☐ CHARGEN ☐ DNS ☒ LDAP ☐ MSSQL
☐ NetBIOS ☐ NTP ☐ Portmap ☐ SNMP ☐ SSDP
☐ SYN ☐ TFTP ☐ WSD

Select All

Select None

Host 1 (www.example.com or 1.1.1.1):

Add Host

Port (valid range: 1 - 65535; 0 = randomize each packet):

Duration:

Seconds (5.00 Minutes)

Bandwidth:

Mbps (200.00 Mbps per host)

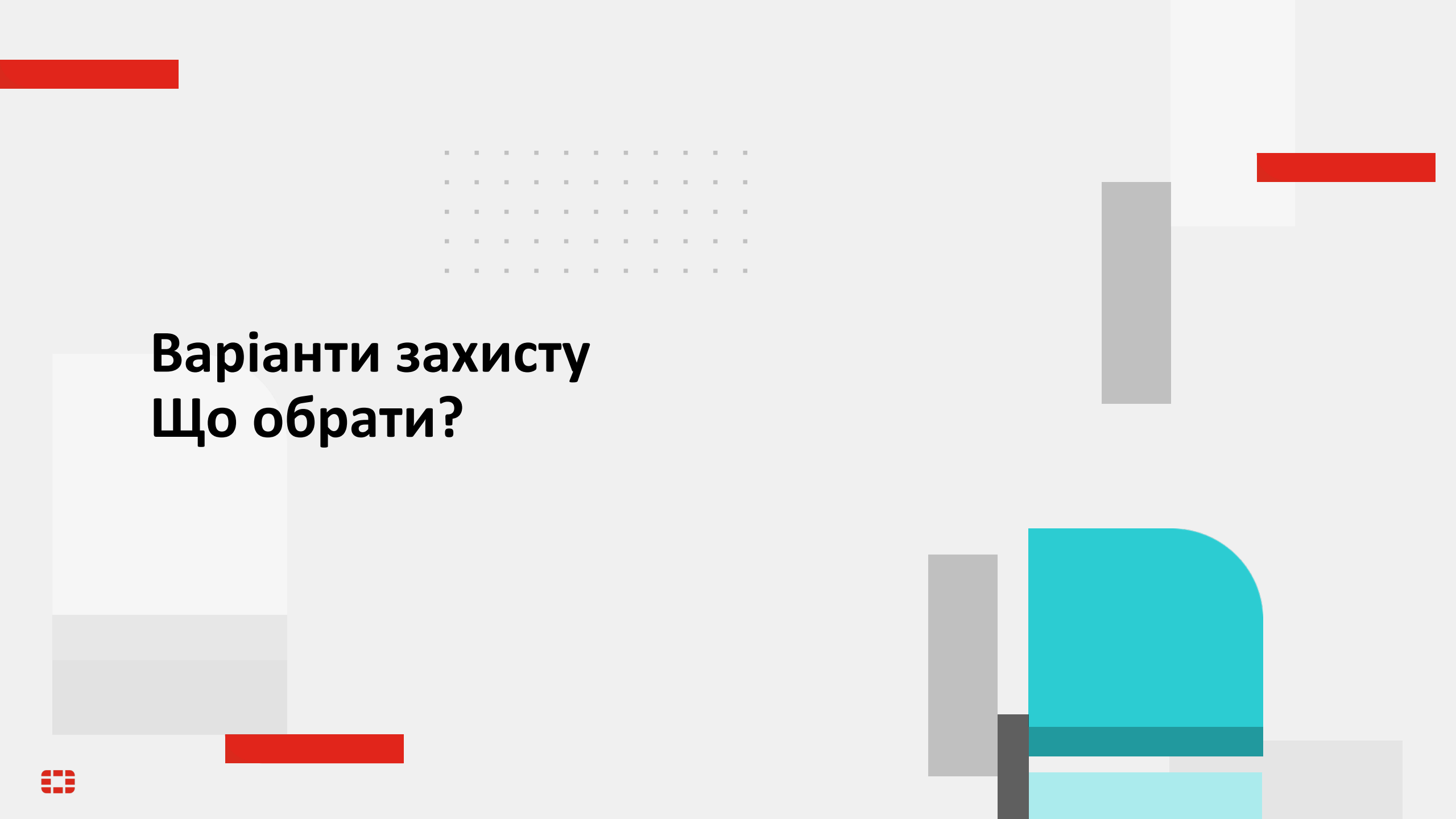
IP Stresser

- \$15 на місяць
- Ліміт в 1.5 Gbps
- Атаки від 200 Mbps до 5Gbps по 19 векторах та їх комбінація

Приклад:
SYN-ACK flood на TCP
порт що не моніториться

© Fortinet Inc. All Rights Reserved.

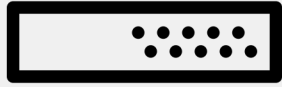
8



Варіанти захисту Що обрати?



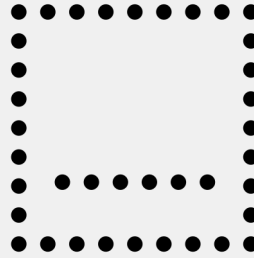
Формфактори



Апаратний пристрій

- Гарантована швидкодія та швидкість реакції
- Профільна апаратна платформа
- Stateless підхід
- Можливість використання bypass
- Детальні налаштування

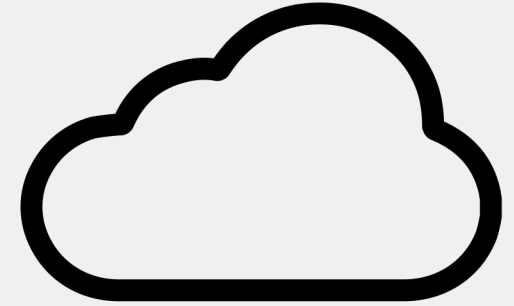
Рішення «поставити на канал» собі або провайдеру для захисту від мережесих та атак та нешифрованих протоколів



VM

- Гнучкість ліцензування та швидкодії
- Можливість переїзду
- Детальні налаштування

Чудове рішення для детальної stateful інспекції шифрованих протоколів веб та пошти (SMTPs та HTTPs)

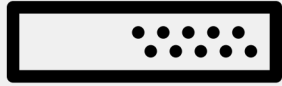


Хмара

- Безлімітна швидкодія
- Можливість розшифровки трафіку і його інспекції
- Адміністрування платформи на плечах виробника

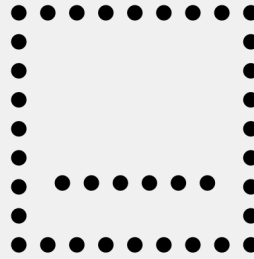
Базовий функціонал з безлімітною швидкістю

Формфактори і їх нюанси



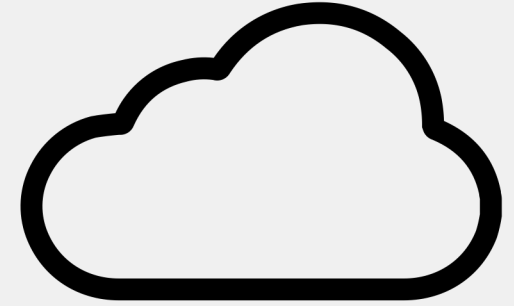
Апаратний пристрій

- В апаратний пристрій може «прилетіти»
- Відсутність гнучкості ліцензування



VM

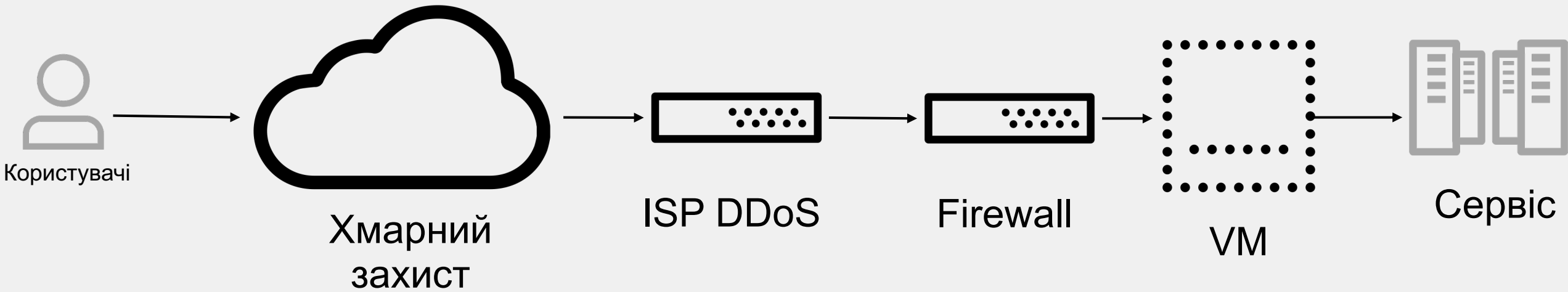
- Резервування ресурсів віртуалізації
- Швидкодія нижче ніж у апаратних пристроїв
- Все робить CPU
- Bypass
- DDoS атаки на хмари



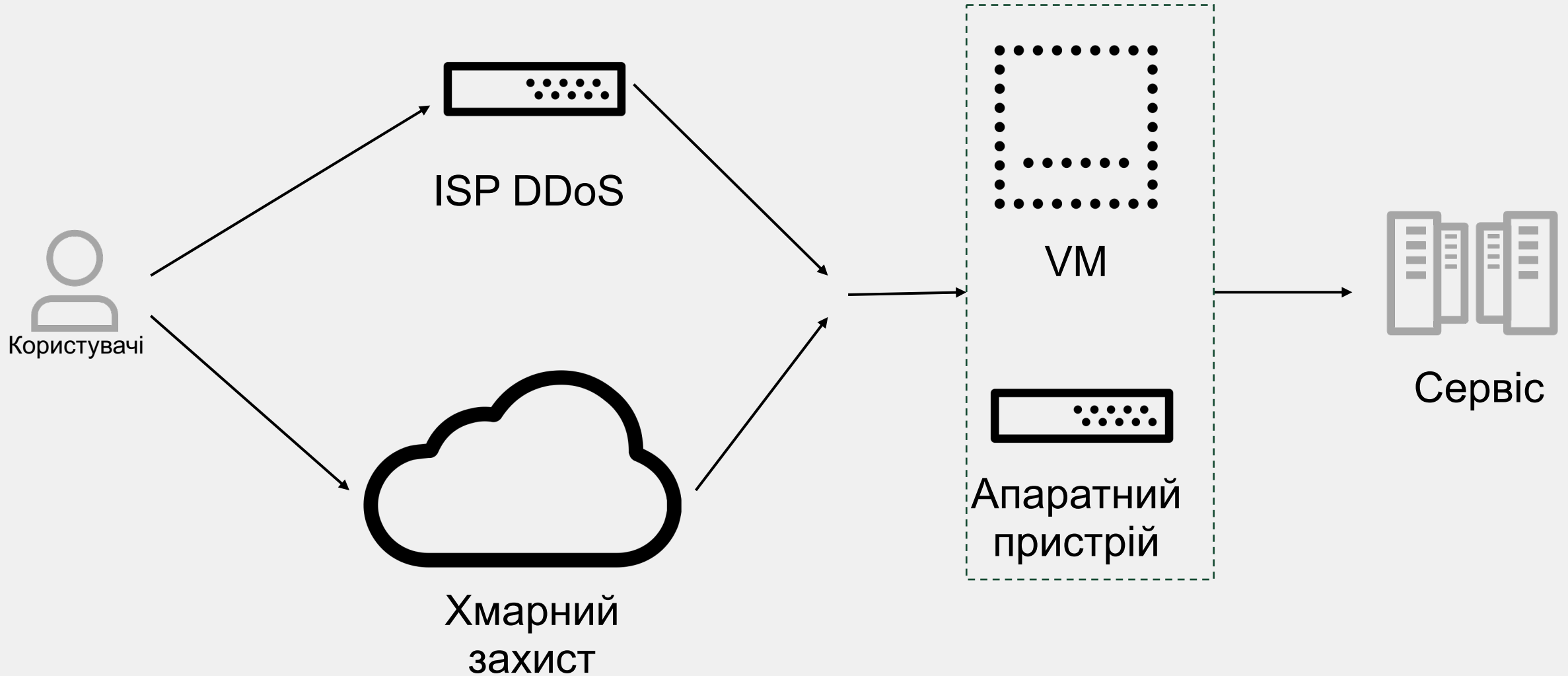
Хмара

- Обмежені налаштування
- Не всім можна використовувати особливо з розшифровкою
- Треба впевнитись що за кожну атаку не виставлять рахунок

Ідеальний світ

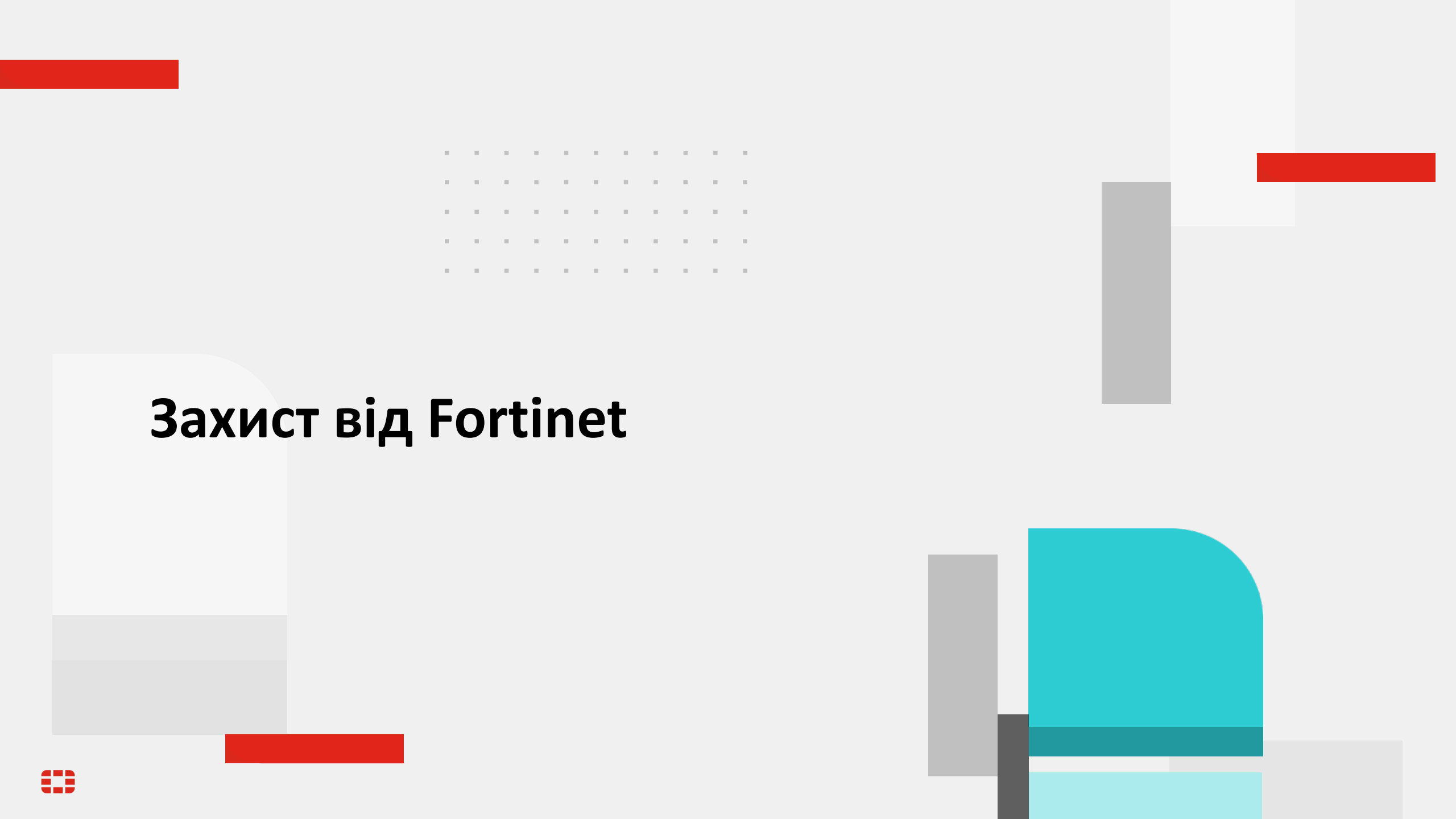


Трохи ближче до реальності



Реальний світ

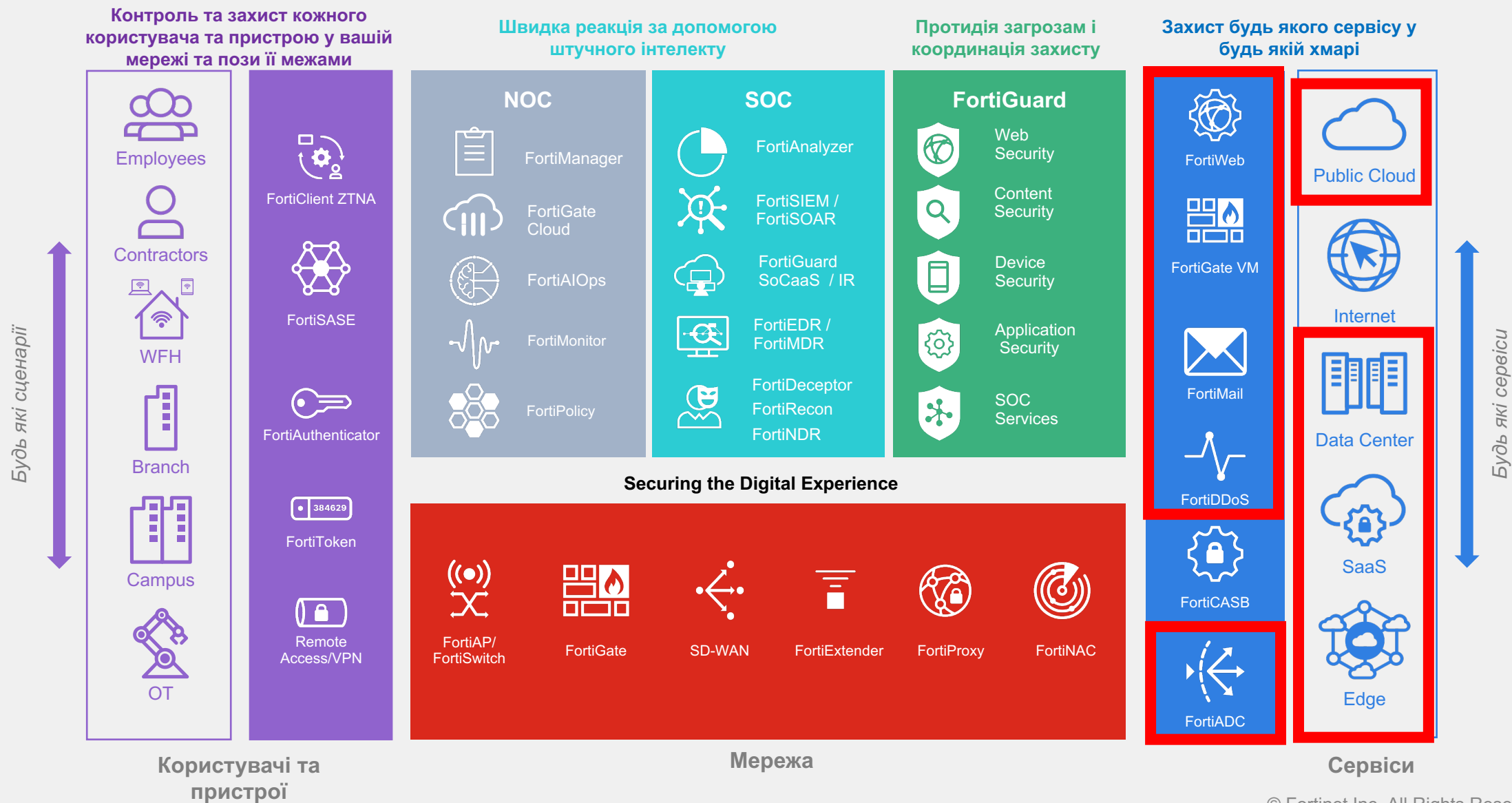




Захист від Fortinet



Коротко про портфоліо Fortinet



Варіант 1. FortiDDoS



Appliance



Профільний пристрій захисту від DDoS



SPU захист L3 3, 4, and 7 DDoS



Захист на основі самонавчання на додачу до баз



Мінімум хибних спрацювань



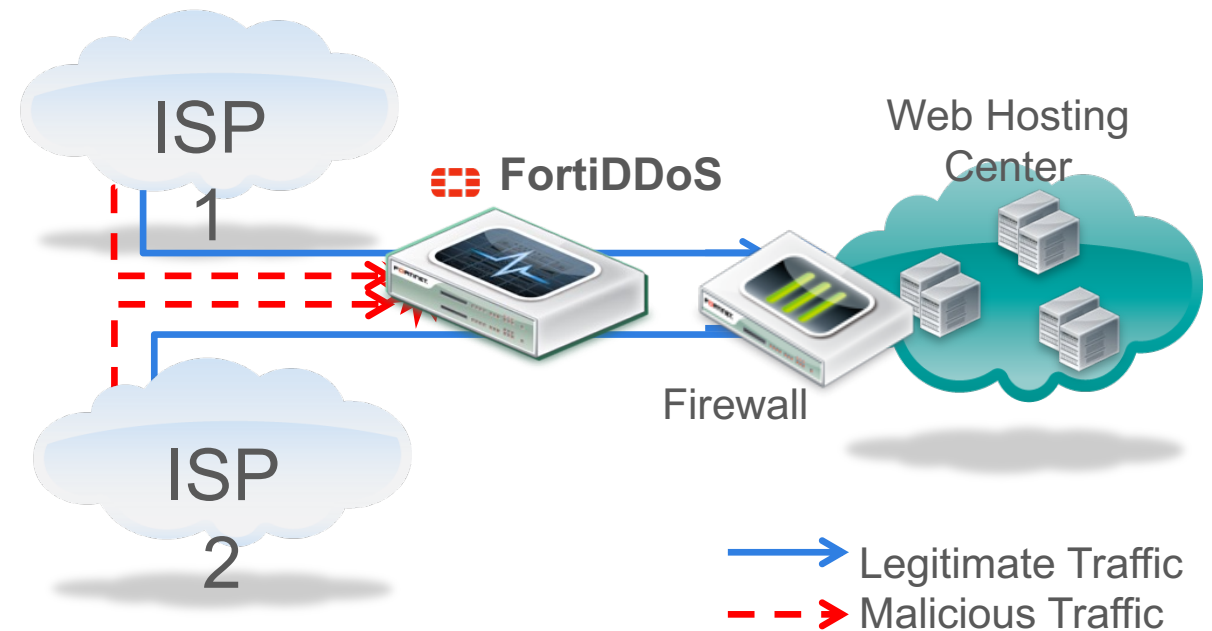
Моніторинг та захист рівня сервісу



Окремий підхід до volumetric та L7



Профільний DNS захист



FortiDDoS

віртуальні пристрої

	FortiDDoS-VM04	FortiDDoS-VM08	FortiDDoS-VM16
Specifications			
Hypervisor Support	VMware ESX/ESXi from 6.x / 7.x with hardware-assisted virtualization (VT) enabled in the BIOS KVM from libvirt 6.0.0		
Throughput¹	3 Gbps	5 Gbps	10 Gbps
Mitigation^{2,3}	3 Gbps / 4 Mpps	5 Gbps / 6 Mpps	10 Gbps / 10 Mpps
Service Protection Profiles	4	8	16
vCPU Support	4	8	16
Network Interface Support	8 (4 bridged port-pairs - promiscuous mode). Interface speeds dependent on hardware.		
Management Interfaces	2	2	2
Electric/Optical Bypass	Function of the underlying NICs and not controllable from FortiDDoS		
Memory Requirements	16 GB	16 GB	32 GB
Storage Requirements	Requires at least 200 GB		



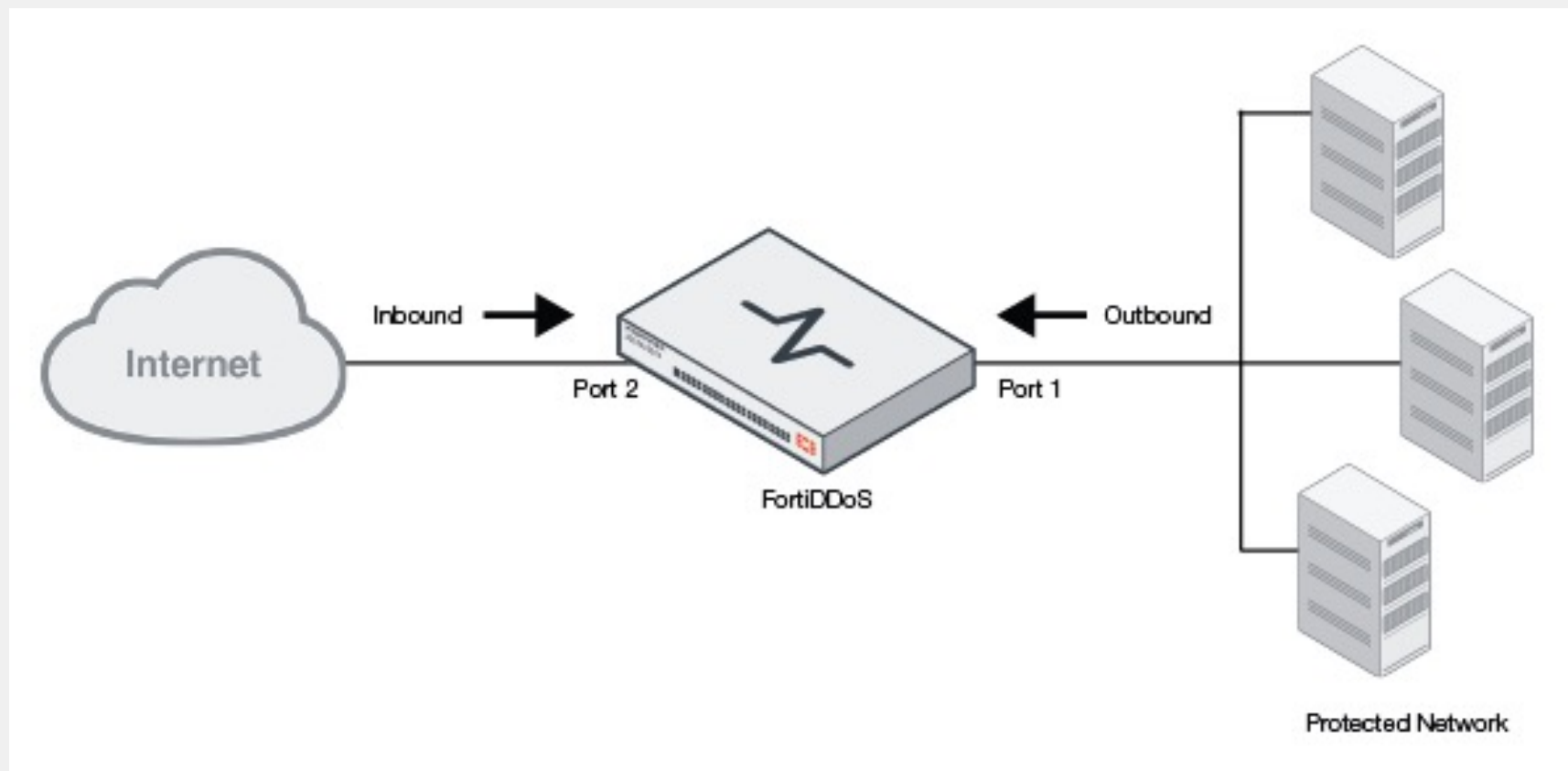
FortiDDoS

апаратні пристрої

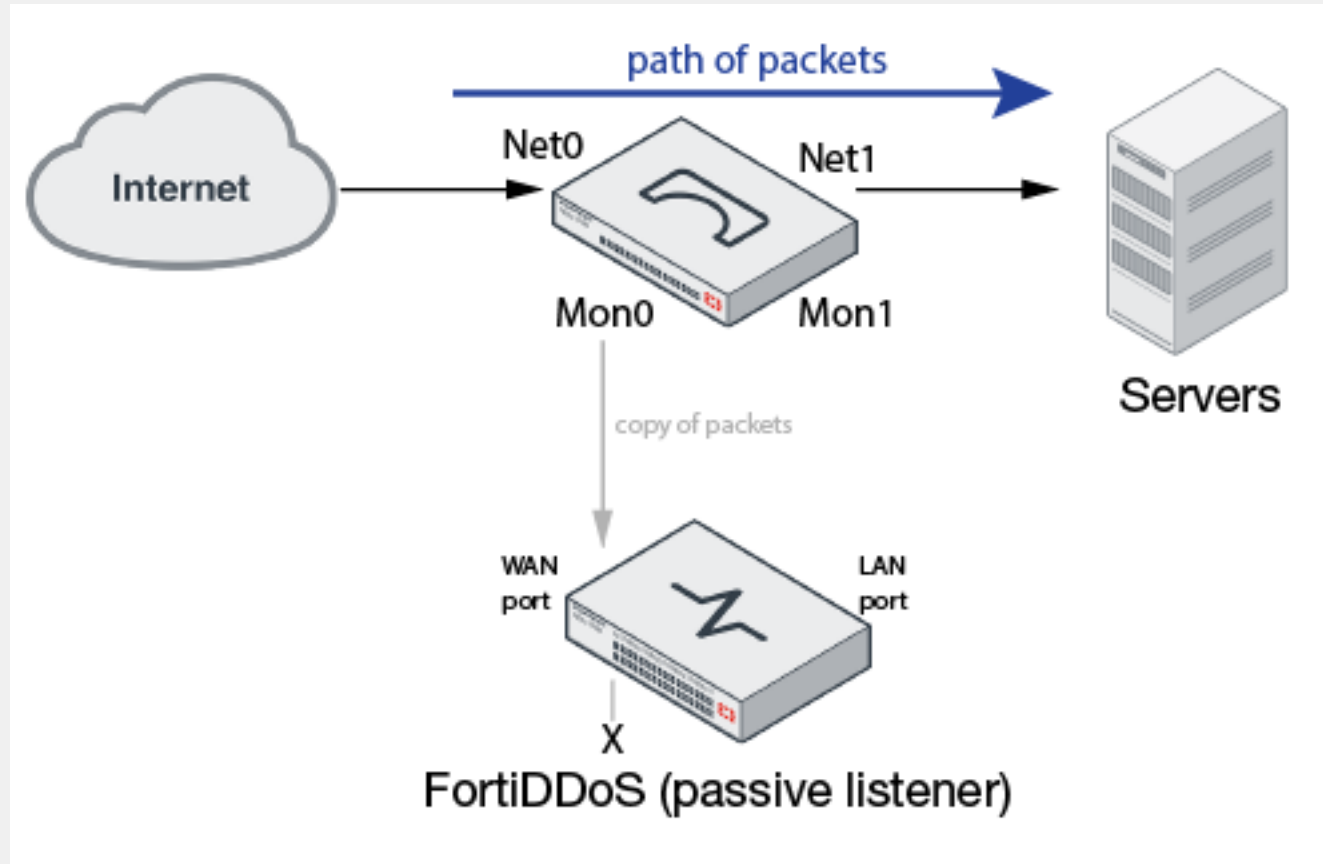
	FDD-200F	FDD-1500E/-DC	FDD-1500F/-LR	FDD-2000E/-DC	FDD-2000F	FDD-3000F
Throughput (Full Duplex)	8 Gbps	35 Gbps	30 Gbps	70 Gbps	76 Gbps	74 Gbps
Simultaneous Connections	4.2 Mil	12 Mil	16.7 Mil	25 Mil	33 Mil	64 Mil
Session Setup/ Teardown (kcps)	375	>1500	>905	>3000	>3000	3087
Latency (μs) Maximum/Typical	<100	<50/<10	<100	<50/<10	< 50 μs	<100
Interfaces	8 LAN/WAN Interfaces (Copper/SFP)	16x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 100GE QSFP28	4x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 10GE SFP/+	16x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 100GE QSFP28	4x LAN & WAN 10GE SFP/+, 4x LAN & WAN 40GE QSFP+	4x LAN & WAN 10GE SFP/+, 4x LAN & WAN 40GE QSFP+
Advanced DNS Mitigation	Yes	Yes	Yes	Yes	Yes	Yes



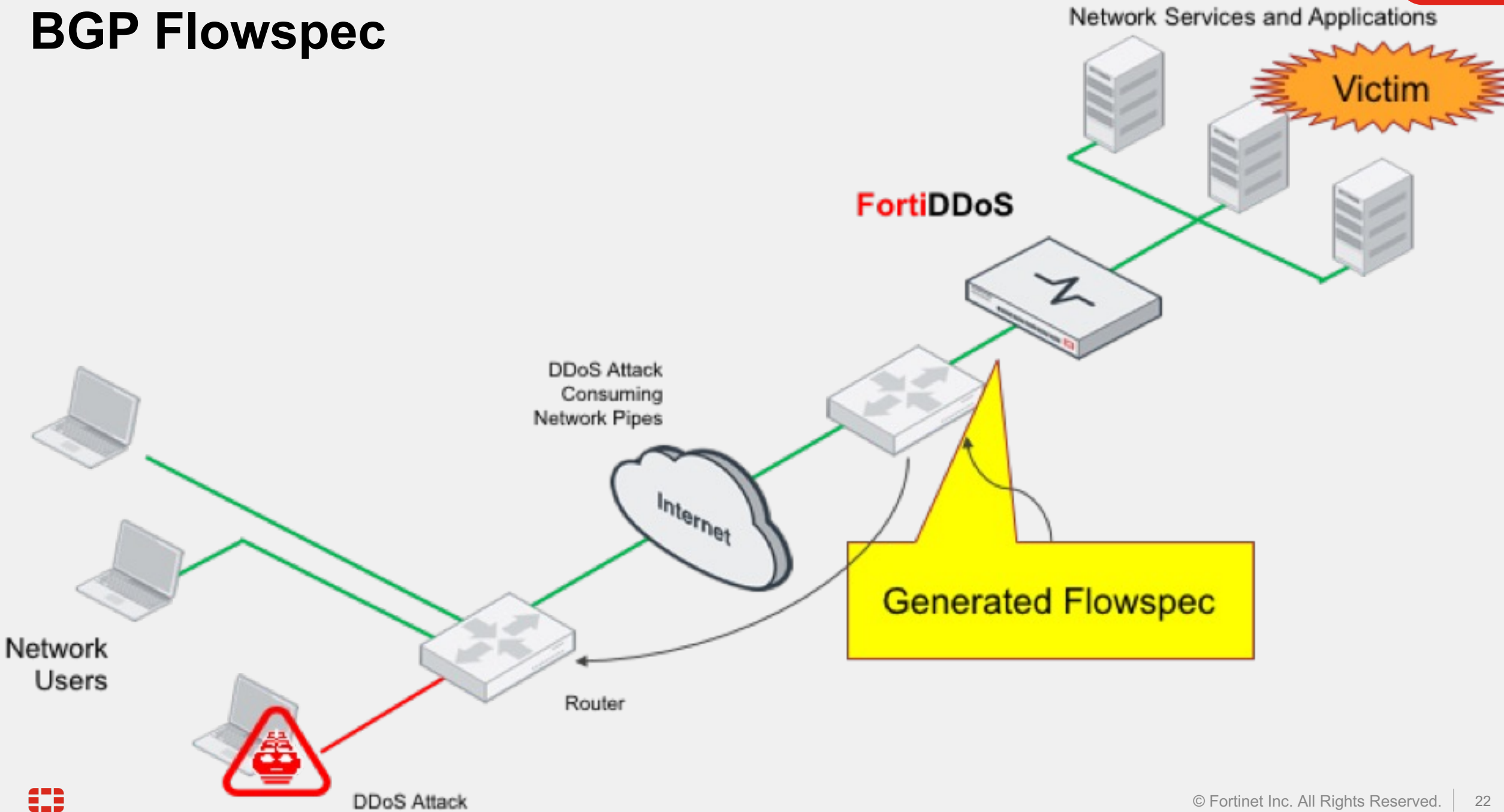
Типова інсталяція «inline»



Типова інсталяція «в стороні»



BGP Flowspec



Cloud Signaling

Cloud Signaling

The Service Provider Signaling feature enables small/medium businesses and enterprises to work with participating service providers to route traffic through a "scrubbing station" in the service provider network (SP) before it is forwarded through the WAN link to the customer premises network (CP).

For details on deployments with signaling between FortiDDoS devices, see [Service Protection](#).

For information on deployments with signaling to 3rd-party Cloud DDoS Mitigation services, please contact your local sales team or Fortinet TAC.

To configure using the CLI:

```
config ddos global cloud-signaling
  set mode { customer-premises | service-provider }
  set timeout <integer>
config devices
  edit <device_name>
    set enable { enable | disable }
    set device-type { FortiDDoS | Third-Party }
    set serial-number <string>
    set shared-secret <passwd>
    set address-type { ipv4 | ipv6 }
    set ipv4-address <ipv4_addr>
    set ipv6-address <ipv6_addr>
    set account-id <string>
    set url <string>
  next
end
end
```

IP and Domain репутація (FortiGuard)

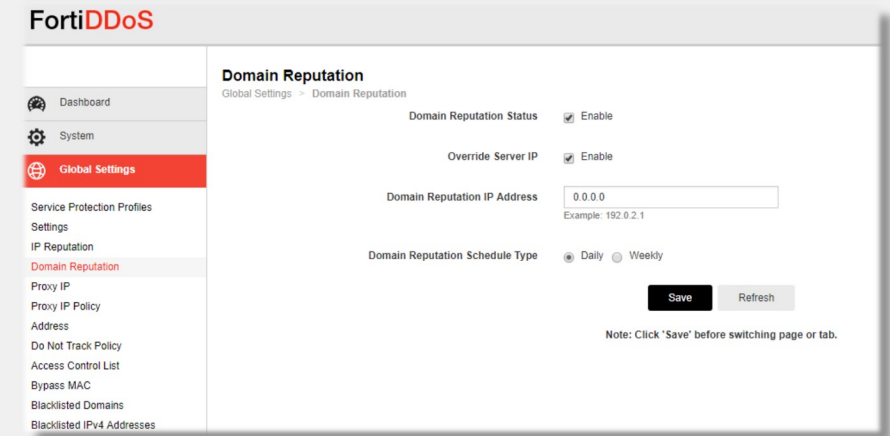
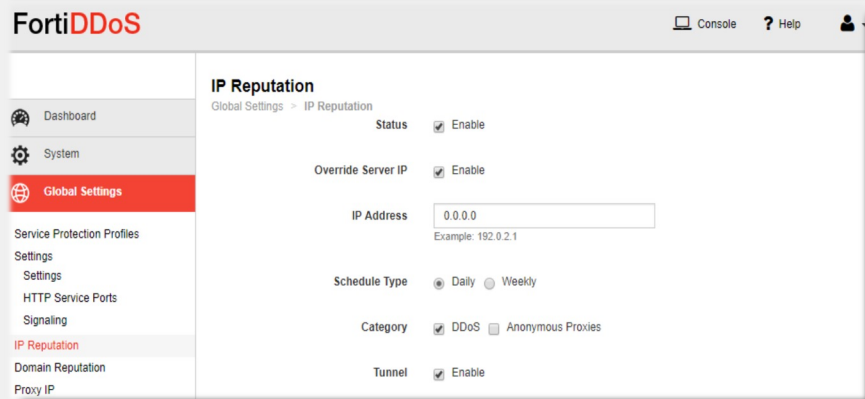


■ IP репутація

- » Шкідливі IP адреси та мережі
- » DDoS та анонімні проксі
- » Захист від відомих шкідливих IP

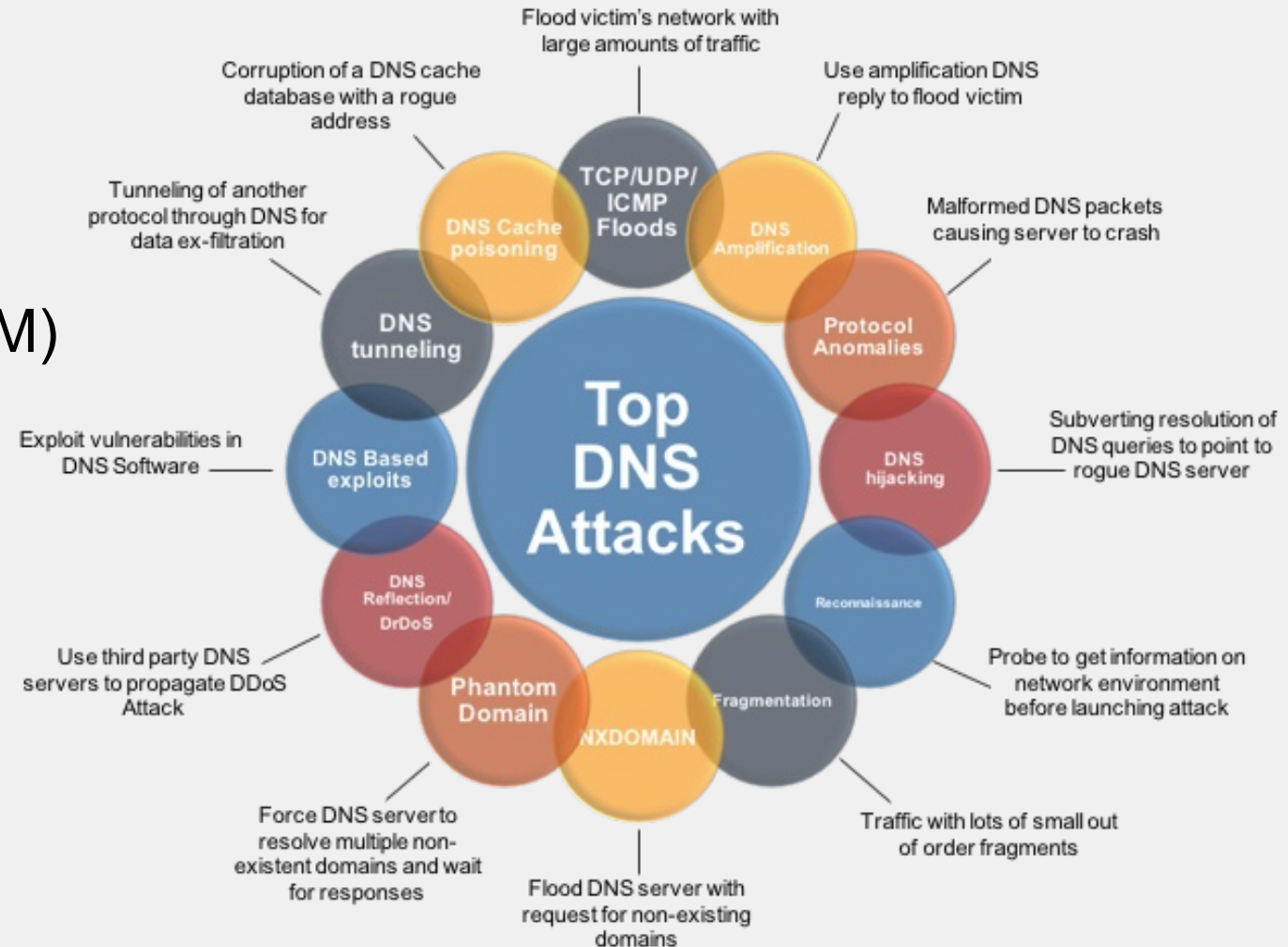
■ Domain репутація

- » Шкідливі DNS імена
- » Блокування C&C
- » Блокування доступу від/до шкідливих доменів



FortiDDoS: DNS захист

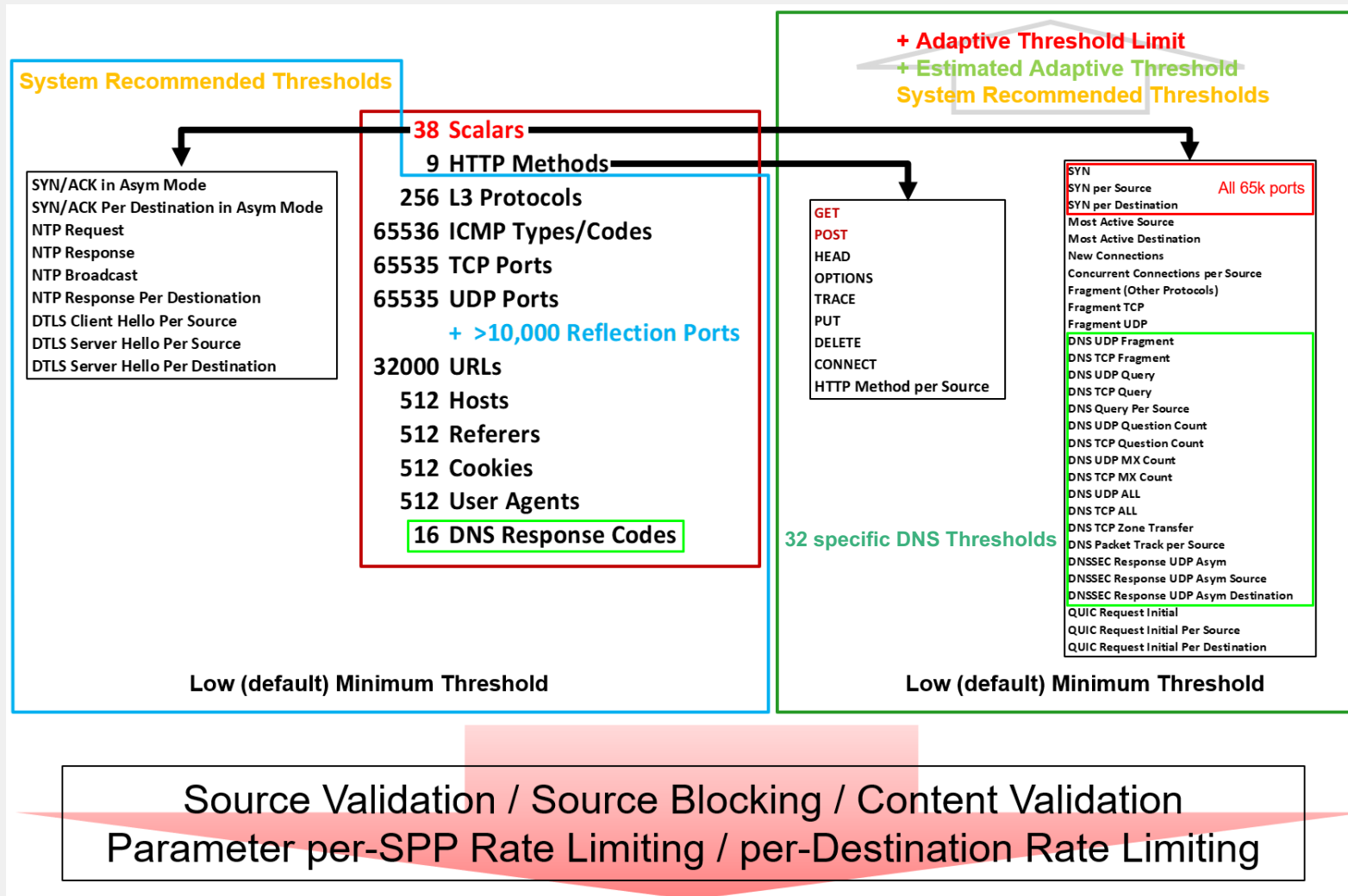
- FQDN Allowlist
- DNS Anomaly Prevention
- DNS Query Response Match (DQRM)
- Legitimate Query (LQ)
- Legitimate IP Table
- DNS Cache
- Source Tracking



Захист сервісу (SPP)

Моніторинг більше 230,000 параметрів

Час реакції <1 секунди!



Машинне навчання

- 1) Continuous Learning for all 230,000 Threshold parameters per SPP.
Select 1-day to 1-Year period (back from today)

Service Protection Policy

default

Service Protection Policy Thresholds Threshold Settings

System Recommendation Emergency Setup Factory Default

Generate Statistics

Last Updated: Available 2021-11-19 14:42:22

1 Day UDP Ports

Port	Inbound
10087	47906
10102	43760
10114	42498
10128	42384
10190	42122
10134	42074
10110	41986
10121	40402
10144	40088
10159	39532
10192	39424
10086	39240
10155	39158
10194	39154
10099	39036
10160	38898
10162	38676
10193	38652
10182	38490
10164	38484
10107	38274
10201	38076
10168	38030
10167	38000
10140	37968

Showing 1 to 25 of 250 entries (filtered from 10,118 total entries)

Outbound Thresholds to MAX

Layer 3

Percentage 100% 500% 300%

Low Traffic 500 Range: 0-65535

Layer 4

Scalars/ICMP

Percentage 100% 500% 200%

Low Traffic 500 Range: 0-65535

TCP

Percentage 100% 500% 200%

Low Traffic 500 Range: 0-65535

UDP

Percentage 100% 500% 200%

Low Traffic 500 Range: 0-65535

Layer 7

Percentage 100% 500% 300%

Low Traffic 500 Range: 0-65535

Create Thresholds

- 2) Apply System Recommended Minimum Threshold and/or Multiplier (Defaults almost always used.)

- 3) System Recommended Thresholds created for all 230k parameters

Service Protection Policy

default

Service Protection Policy Thresholds Threshold Settings

Threats

Create New Delete

Scalars

HTTP Methods

Protocols

TCP Ports

UDP Ports

ICMP Types/Codes

URLs

Hosts

Referers

Cookies

User Agents

DNS RCode

Name	Type	Inbound Threshold
sys_reco3	most-active-source	500
sys_reco8	oth-fragment	500
sys_reco7	tcp-fragment	500
sys_reco6	udp-fragment	500
sys_reco1	syn	500
sys_reco2	syn-per-src	500
sys_reco4	concurrent-connections-per-source	500
sys_reco10	syn-per-dst	500
sys_reco16	dns-fragment-udp	500
sys_reco12	dns-query-udp	500
sys_reco14	dns-question-count-udp	500
sys_reco18	dns-mx-count-udp	500
sys_reco20	dns-all-udp	500
sys_reco_v0_52	dns-question-count-tcp	500
sys_reco_v54_122	dns-query-tcp	500
sys_reco_v124_10239	dns-mx-count-tcp	500
sys_reco_v10240_65535	dns-zone-xfer-tcp	500
	http-method-per-src	500

- 4) At any time, rerun Traffic Statistics or change System Recommendations settings with no impact on system operation

UDP Ports, for example, are grouped into ranges with similar Thresholds
For simpler management



Протоколи

FortiDDoS 200F FortiDDoS-200F-Demo

>_

?

demo

Dashboard

FortiView

System

Network

Global Protection

Service Protection

Protection Subnets List

CONFIGURATION

Service Protection Policy

IP Profile

ICMP Profile

TCP Profile

HTTP Profile

SSL/TLS Profile

NTP Profile

DNS Profile

DTLS Profile

QUIC Profile

Video Conference Profile

Log & Report

Monitor

+ Create

Edit

Delete

Clone

Refresh

Search

	Name	Unknown Method Anomaly	Version Anomaly	Do not Parse Version 0.9	Drop Range Header	Incomplete Req
☒	HTTP_Web	Enabled	Enabled	Disabled	Disabled	None
☐	HTTP_FW	Enabled	Enabled	Disabled	Disabled	None

SSL/TLS

SSL / TLS Profile

Name	Required. No spaces.
Protocol Anomaly	☒
Anomaly Version	☐ Other ☐ SSL 3 ☐ TLS 1.0 ☐ TLS 1.1 ☐ TLS 1.2 ☐ TLS 1.3
Cipher Anomaly	☒
Block Incomplete Request	☐
Aggressive Aging Incomplete Request	☐
Block Source With Incomplete Request	☐
Renegotiation Check	☐
Inspection Mode	☐



Варіант 2. Класичні наземні рішення

FGVMSLTM24003296

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Authentication Rules

Addresses

ZTNA

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

New Policy

L3 Anomalies

Name	Logging	Action	Threshold
ip_src_session	☐	Disable Block Monitor	5000
ip_dst_session	☐	Disable Block Monitor	5000

L4 Anomalies

Name	Logging	Action	Threshold
tcp_syn_flood	☐	Disable Block Monitor	2000
tcp_port_scan	☐	Disable Block Monitor	1000
tcp_src_session	☐	Disable Block Monitor	5000
tcp_dst_session	☐	Disable Block Monitor	5000
udp_flood	☐	Disable Block Monitor	2000
udp_scan	☐	Disable Block Monitor	2000

OK

Cancel

Additional Information

API Preview

Online Guides

Relevant Documentation

Video Tutorials

Consolidated Policy Configuration

Fortinet Community

Technical Tip: How to locate the DoS Policy log in the FortiAnalyzer

1 Answers 1 Votes 4,800 Views

Troubleshooting Tip: How to set DoS policy exceptions

1 Answers 1 Votes 1,100 Views

IPv4 DoS Policy

4 Answers 0 Votes 600 Views

See More



Варіант 2. Класичні наземні рішення

NP version	Description
NP7	NP7 processors offload most IPv4 and IPv6 traffic, IPsec VPN encryption (including Suite B), GTP traffic, CAPWAP traffic, VXLAN traffic, multicast traffic, NAT session setup, and DoS protection. On FortiGates licensed for hyperscale firewall support, NP7 processors offload session setup, Carrier Grade NAT (CGN), hardware logging, HA hardware session synchronization, and data communication from the FortiGate CPU. The NP7 processor has a maximum throughput of 200 Gbps using 2 × 100 GigE interfaces. For details about the NP7 processor, see NP7 and NP7Lite acceleration and for information about FortiGate models with NP7 processors, see FortiGate NP7 architectures . For information about hyperscale firewall functionality, see the Hyperscale Firewall Guide .
NP7Lite	NP7Lite processors are a component of the Fortinet SOC5 (also called the SP5). The NP7Lite processor is a lower capacity version of the NP7 processor. The NP7Lite processor supports all NP7 processor features except hyperscale firewall (hardware sessions). The NP7Lite also does not include support for defrag/reassembly (DFR) to re-assemble fragmented packets. The NP7Lite max throughput is 40 Gbps, using one 40GigE interface. For details about the NP7Lite processor, see NP7Lite processors and for information about FortiGate models with NP7Lite processors, see FortiGate NP7Lite architectures .



FortiGate



Варіант 2. Класичні наземні рішення



FortiGate

Варіант 2. Класичні наземні рішення

FortiWeb-Demo

HA: Standalone

demo

★ Favorites

Dashboard

Network

System

Security Fabric

User

Policy

Server Objects

Application Delivery

Web Protection

Bot Mitigation

API Protection

DoS Protection

Application

HTTP Access Limit

Malicious IPs

HTTP Flood Prevention

Network

DoS Protection Policy

IP Protection

Tracking

Web Vulnerability Scan

Log&Report

Edit HTTP Access Limit

Name

Predefined

HTTP Request Limit/sec (Standalone IP)

500

(0~65536)

HTTP Request Limit/sec (Shared IP)

1000

(0~65536)

Bot Confirmation

☐

Action

Block Period

Block Period

600

Seconds (1 - 10000)

Severity

High

Trigger Policy

Return



FortiWeb



Варіант 2. Класичні наземні рішення

FortiWeb-Demo

HA: Standalone

demo

★ Favorites

Dashboard

Network

System

Security Fabric

User

Policy

Server Objects

Application Delivery

Web Protection

Bot Mitigation

Bot Mitigation Policy

Biometrics Based Detection

Threshold Based Detection

Bot Deception

Known Bots

ML Based Bot Detection

Advanced Bot Protection

Exception Policy

API Protection

DoS Protection

IP Protection

Tracking

Web Vulnerability Scan

Edit Bots

Name

Bot Deception

Biometrics Based Detection

Threshold Based Detection

Known Bots

Exception Policy

Edit Known Bots

Name

Predefined - Known Bots

Exception

Status	Name	Action	Block Period	Severity	Threat Weight	Trigger Policy	Bot List
Malicious Bots (5)							
☒	DoS	Alert & Deny	600	High			
☒	Spam	Alert & Deny	600	High			
☒	Trojan	Alert & Deny	600	High			
☒	Scanner	Alert & Deny	600	High			
☒	Crawler	Alert & Deny	600	High			
Known Good Bots (1)							
☒	Known Search Engines	Bypass	600	Informative			

Return



FortiWeb



Варіант 2. Класичні наземні рішення

FortiMail VMFortiMail

Dashboard

FortiView

Monitor

System

Domain & User

Policy

Profile

Session

AntiSpam

AntiVirus

Content

Replacement Message

Resource

Authentication

LDAP

Dictionary

Security

IP Pool

Group

Notification

Security

Encryption

Data Loss Prevention

?

>_

[]

demo

Session Profile

Profile name

Inbound_Session

Comment

Connection Setting

Restrict the number of connections per client per 30 minutes to

1200

Restrict the number of messages per client per 30 minutes to

0

Restrict the number of recipients per client per 30 minutes to

0

Maximum concurrent connections for each client

2

Connection idle timeout (seconds)

30

Sender Reputation

Endpoint Reputation

Sender Validation

Session Setting

Unauthenticated Session Setting

SMTP Limits

Error Handling

You do not have permission to edit this setting.

Close

Selected: 1 / 3

Ref.
2
0
1



FortiMail



Варіант 3. SaaS рішення

Перевірена безпека та зв'язок усюди

ASSETS & ACCOUNTS

 Asset Management

 IAM

CLOUD MANAGEMENT

 FortiClient EMS Cloud

 FortiGate Cloud

 FortiManager Cloud

 FortiAnalyzer Cloud

 FortiLAN Cloud

 FortiSOAR Cloud

 FortiExtender Cloud

 FortiSIEM Cloud

CLOUD SERVICES

 FortiMail

 FortiMonitor

 FortiSASE

 FortiZTP (Beta)

 FortiSandbox Cloud

 FortiVoice

 FortiCASB

 FortiPresence

 FortiDAST

 FortiTrustID

 FortiGate CNF

 FortiIPAM

 OC-VPN Portal

 SOCaaS

 FortiConverter

 FortiWeb Cloud

 FortiRecon

 FortiToken Cloud

 FortiCNP

 FortiGSLB

 FortiPhish

 FortiDevSec

 FortiCamera Cloud (Beta)

 FortiCare Elite (Beta)

 FortiInsight

 Managed FortiGate

[Show Less](#) ^

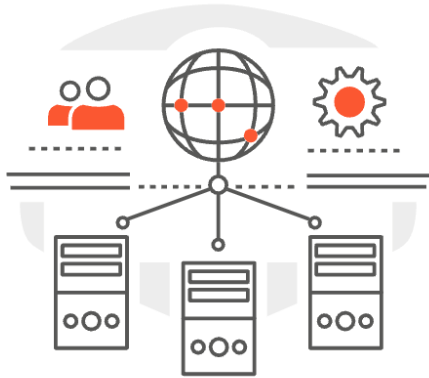


Наприклад FortiWeb



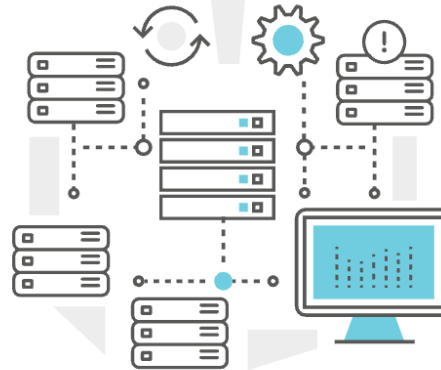
Варіант 3. SaaS рішення

FortiGSLB



Global App. Load Balancing

Provides load-sharing and failover functionality with a reach and level of resiliency that exceeds that of traditional device-based solutions.



DNS Service

Provides primary authoritative DNS server with standard DNS type zone - A/AAAA, NS, CNAME, MX, TXT, PTR, SRV and advanced security function DNSSEC.

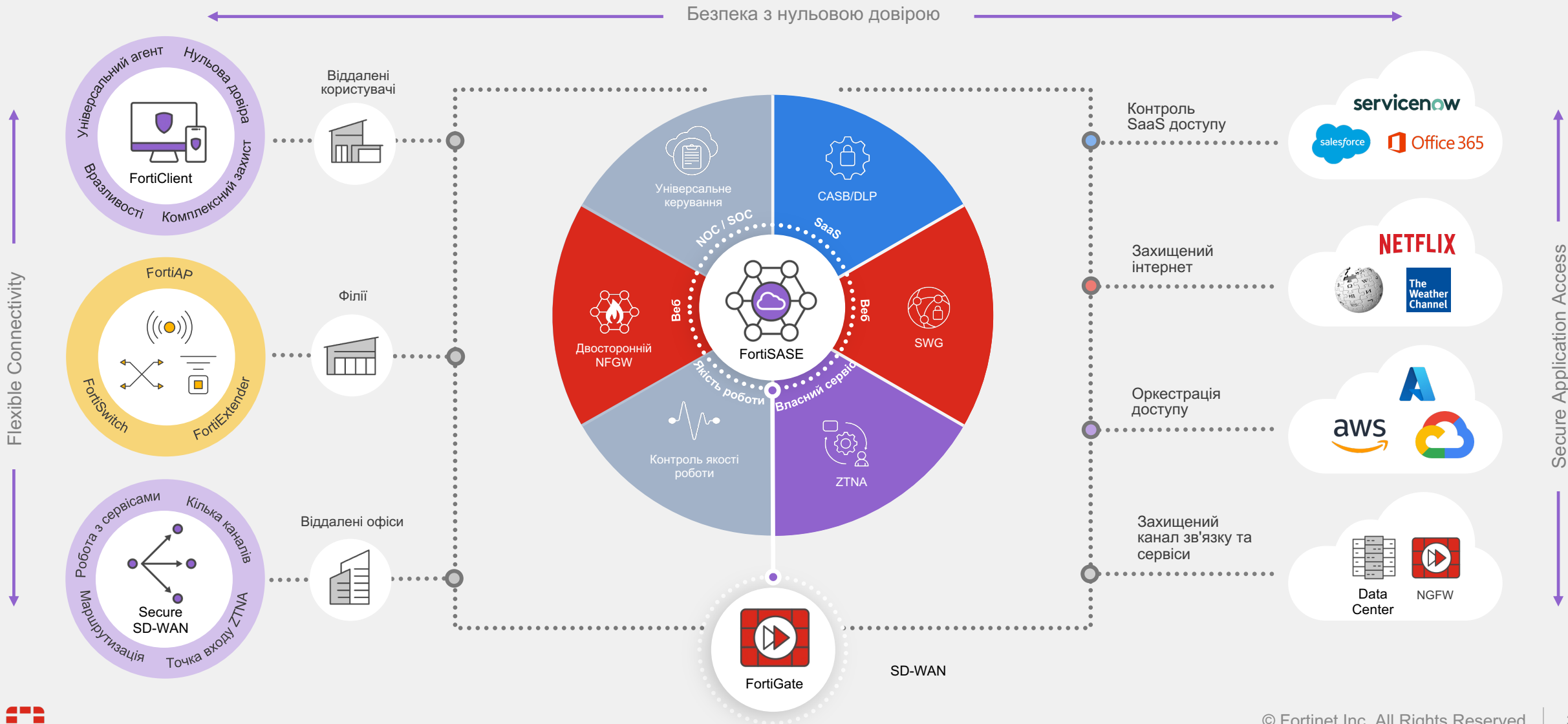


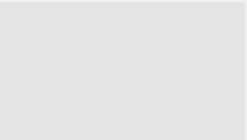
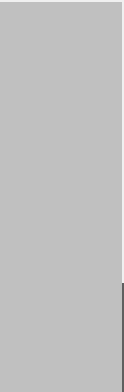
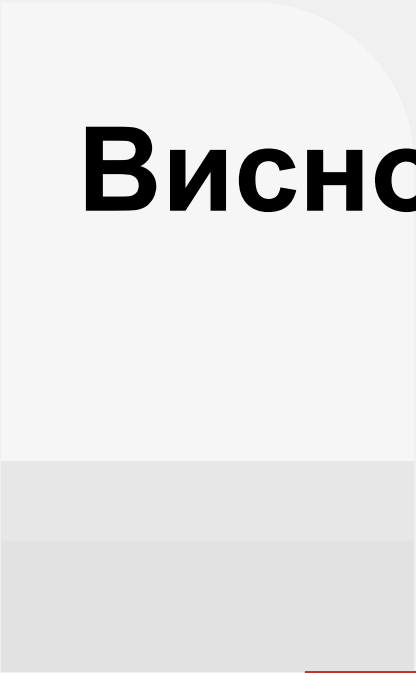
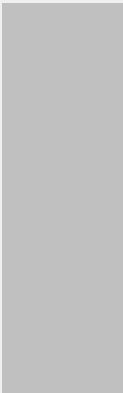
Synthetic Testing

Offers multisite application visibility with advanced application testing.

Варіант 4. Fortinet Universal SASE

Перевірена безпека та зв'язок усюди



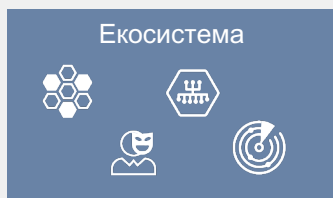
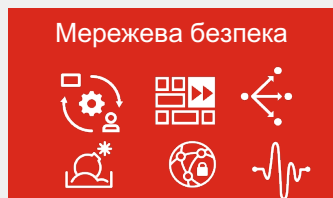
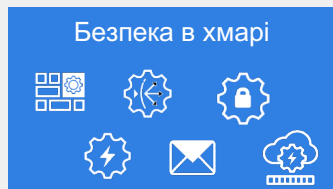
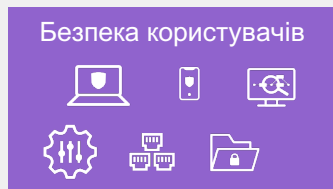
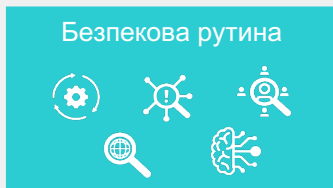
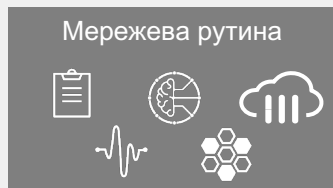


Висновки

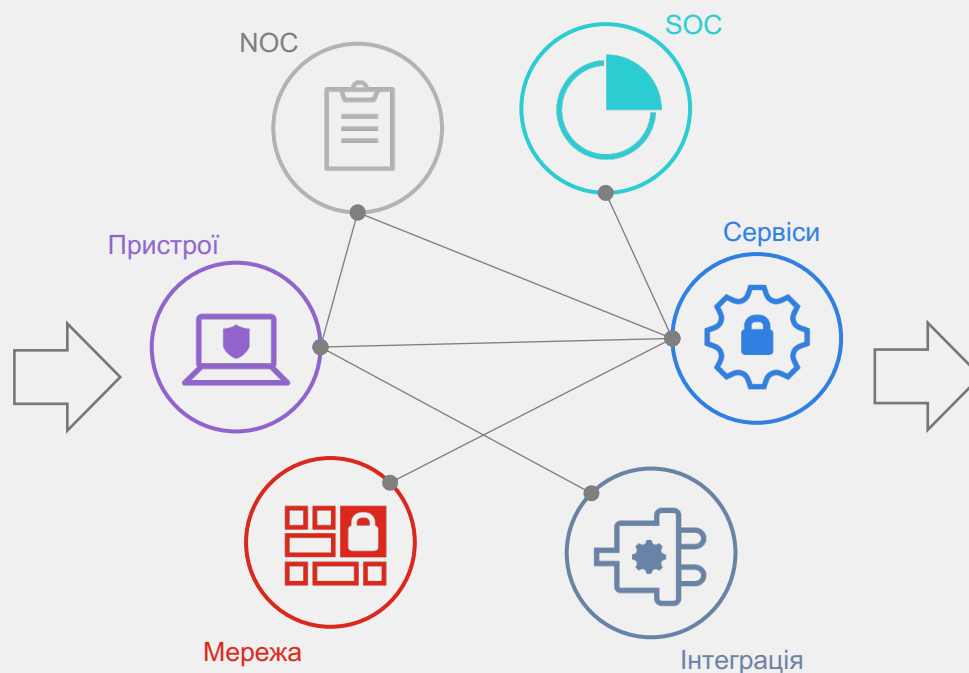


Комплексне рішення

30+ виробників



10 виробників



2-3 платформи



Розвиток замовника



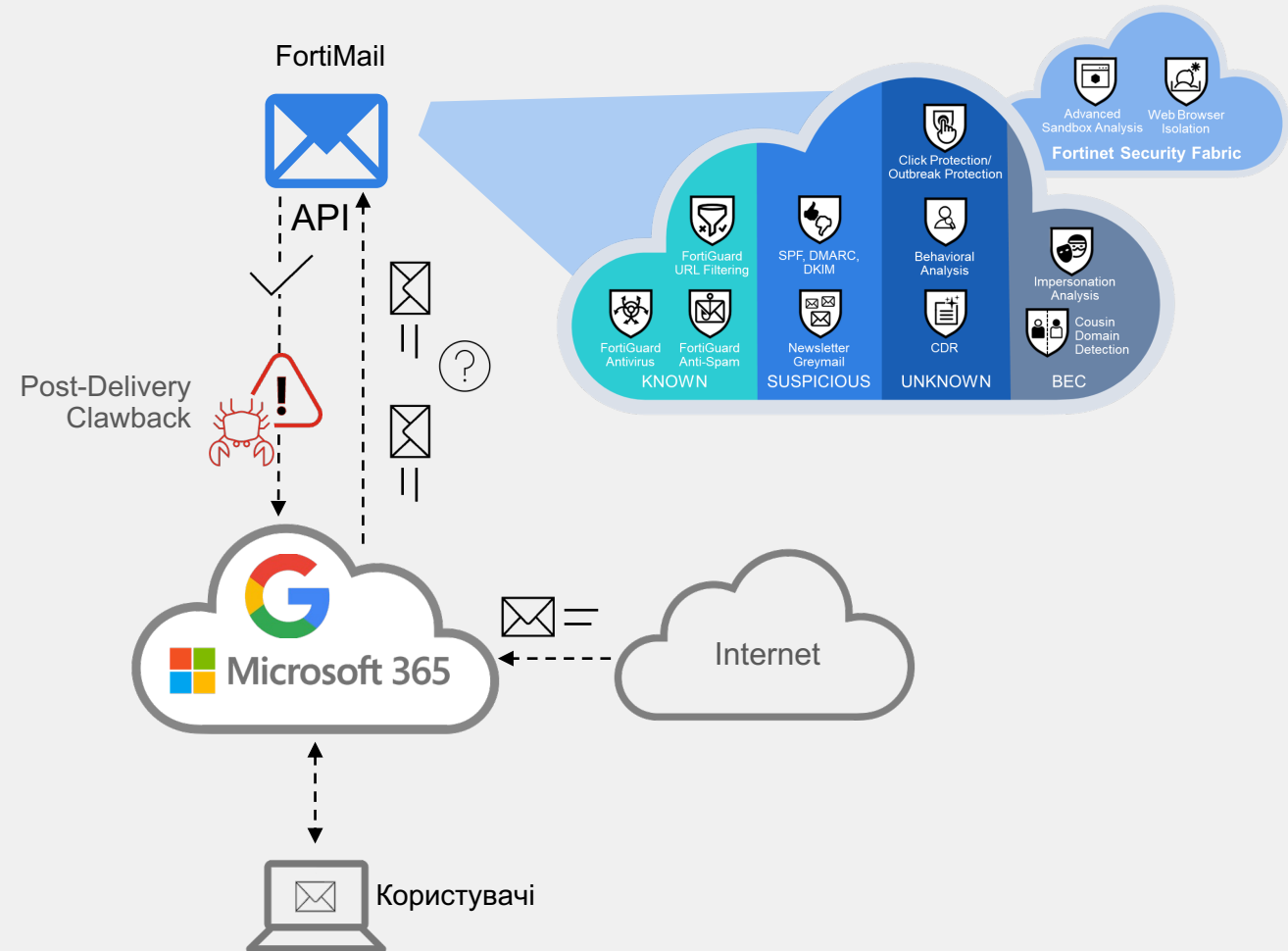
Архітектура 1.

Захист веб сервісів



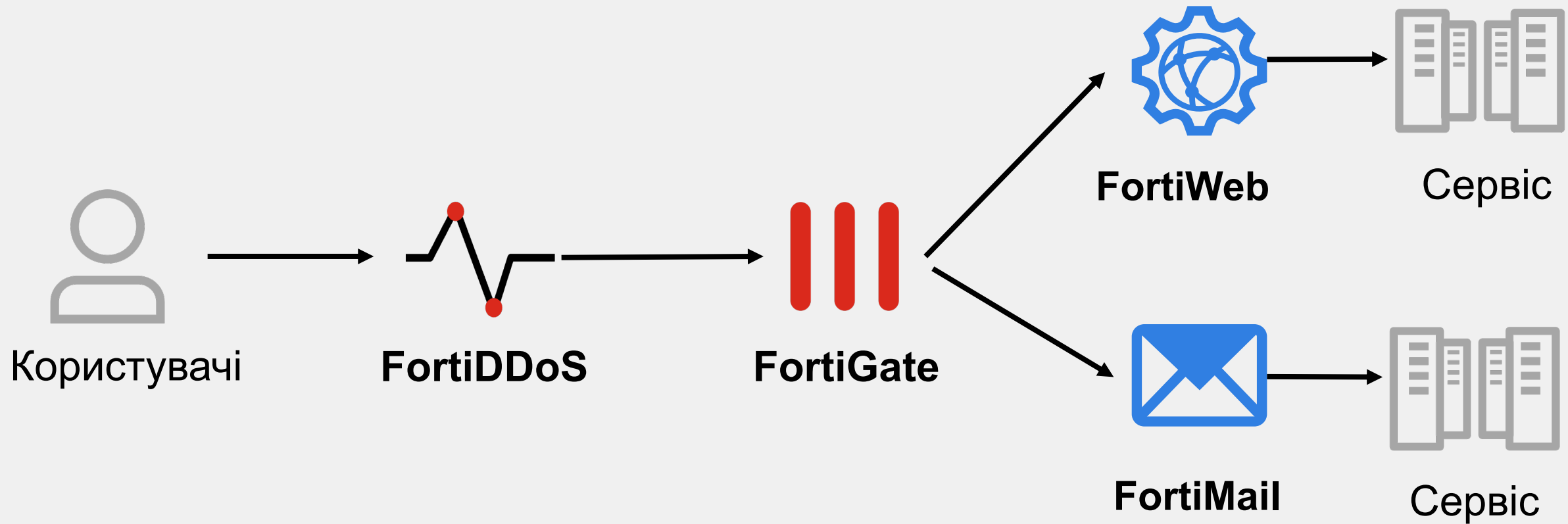
Архітектура 2.

Захист пошти. Office 365 та Google



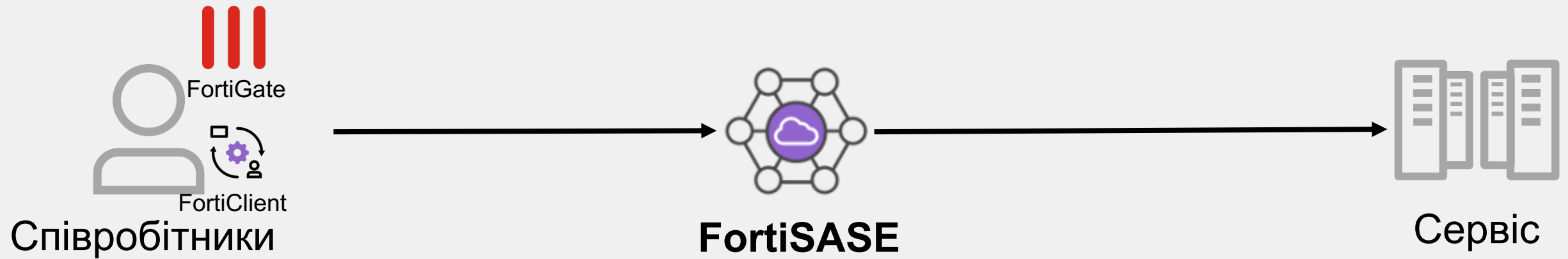
Архітектура 3.

Якщо «в хмари» неможна



Архітектура 4.

Внутрішні сервіси для віддалених співробітників



Дякую за увагу!

FORTINET®