Мистецтво DDoS захисту з рішеннями Fortinet

Євгеній Таран, Systems Engineer

ytaran@fortinet.com

Таран Євгеній

- 15+ років в IT
- останні 9 років будую/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…

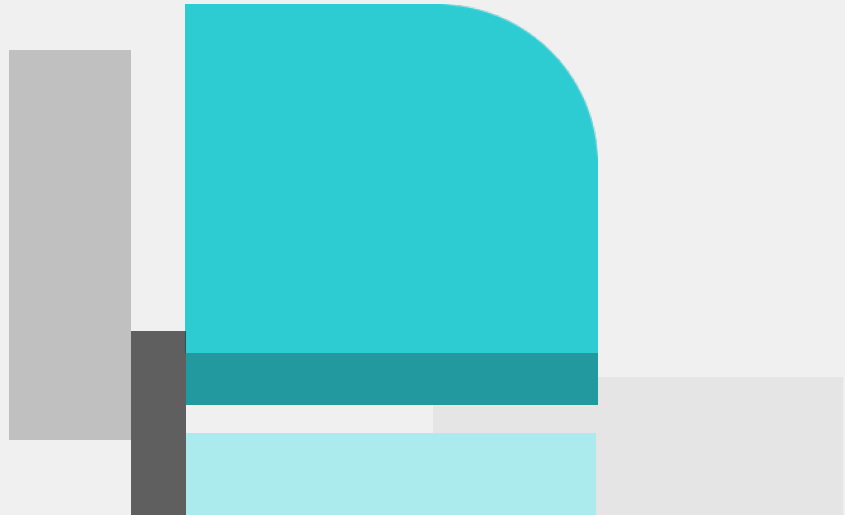
© Fortinet Inc. All Rights Reserved.

В попередніх серіях

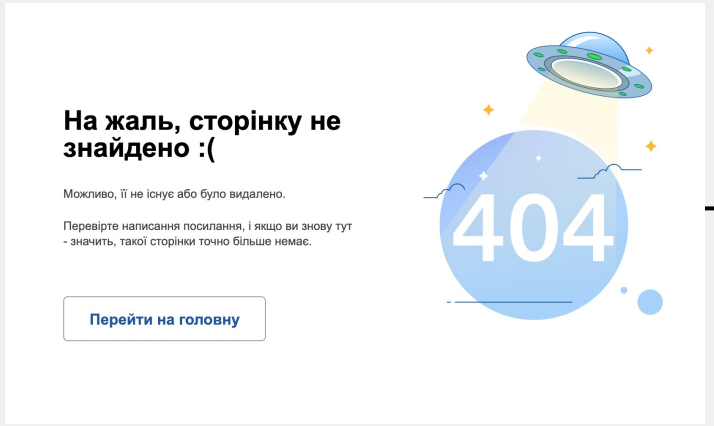
- **Security Fabric**
  Усунення загроз у будь-яких мережах, кінцевих точках та хмарахостанні 9 років будую/модернізую IT інфраструктури та змушую веб сервіси працювати «як має бути» ☺
- Гібридні мережі з **Fortinet Fabric** Management Center.
  Побудова, адміністрування та безпека.
- **FortiMail**
  Комплексний захист корпоративної пошти
- Захист веб та API сервісів за допомогою **FortiWeb**. Інтеграція з FortiGate.
- **FortiSASE**. Побудова IT інфраструктури та безпеки сервісів без датацентрів

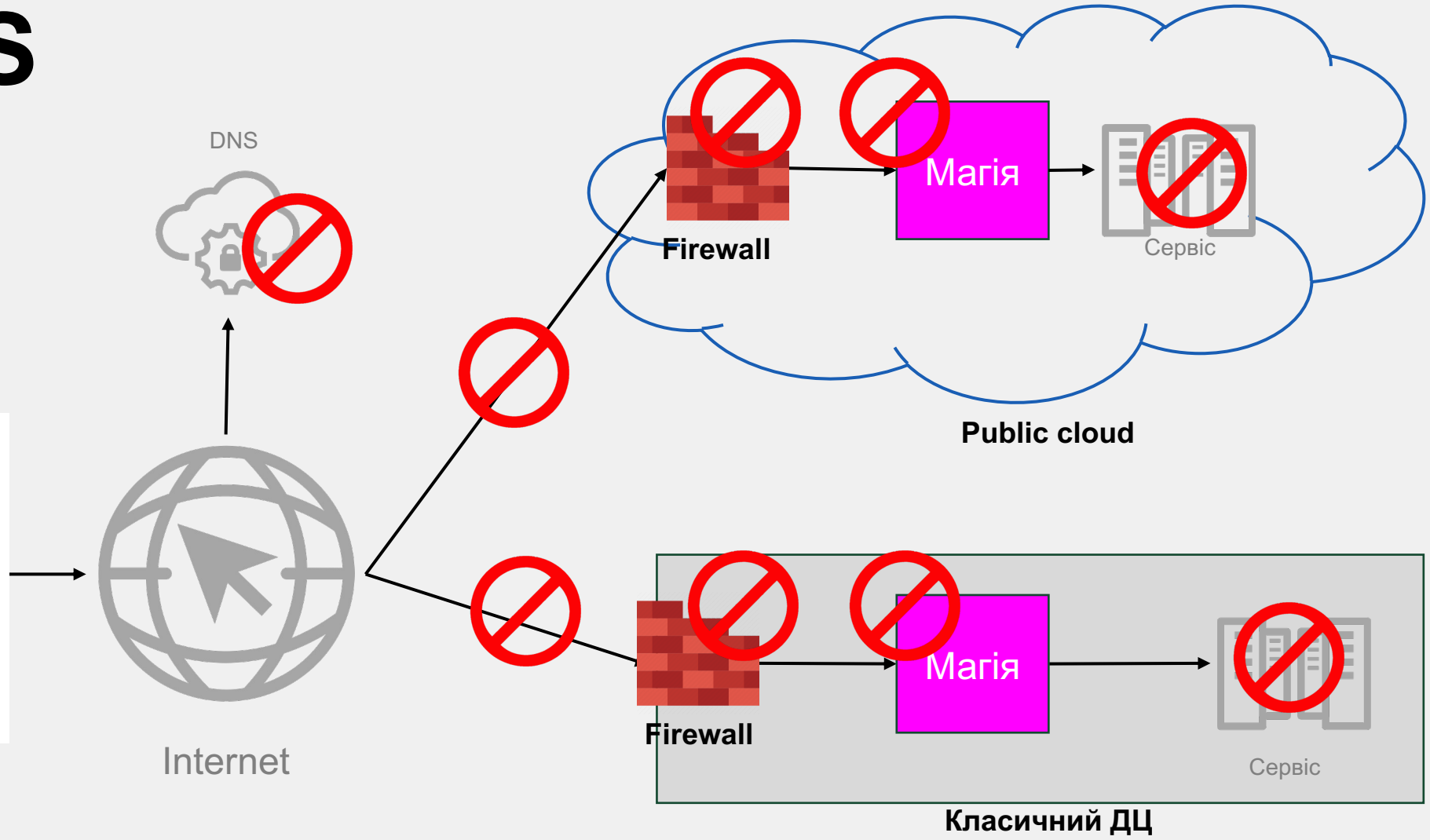
© Fortinet Inc. All Rights Reserved.

DDoS
Мета та реалізація



Мета DDoS





© Fortinet Inc. All Rights Reserved.

Приклади

Monobank зіткнувся з потужною DDoS-атакою

Автор:
Олександр Гайдамашко

13:18, 2 травня | 2 хв | Читать новость на русском

Monobank / Ко

До уваги клієнтів! DDoS атака

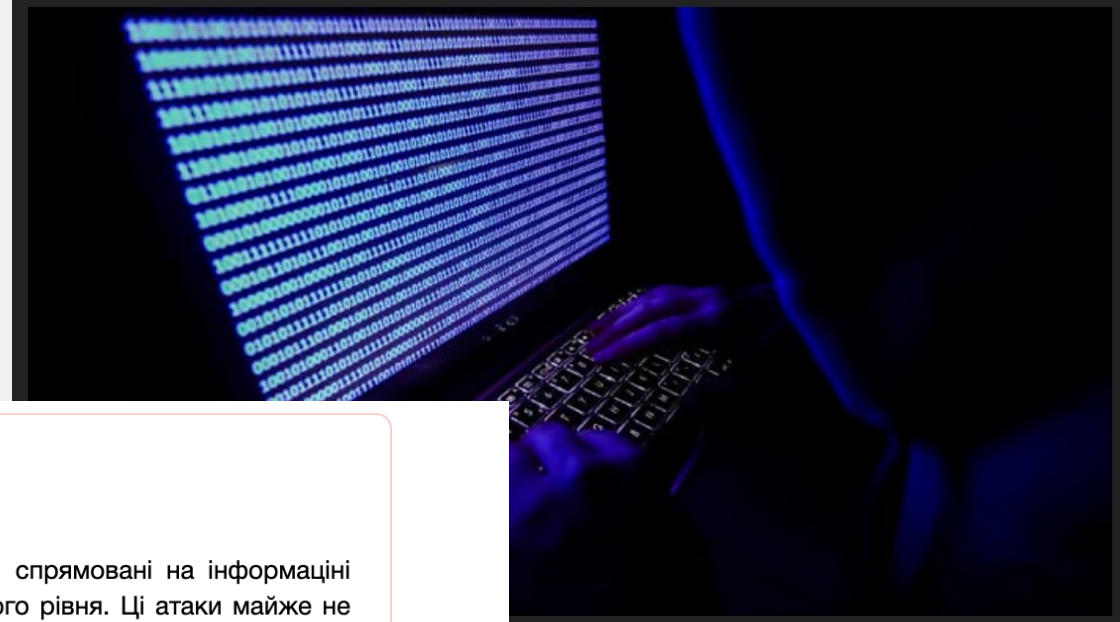
17.03.2018

Дорогі клієнти, від учорашнього дня регулярно здійнюються DDoS-атаки, спрямовані на інформаціні 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.

© Fortinet Inc. All Rights Reserved.

Еволюція DDoS

Хвилинка історії

Розвиток атак змушує розвивати захист

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

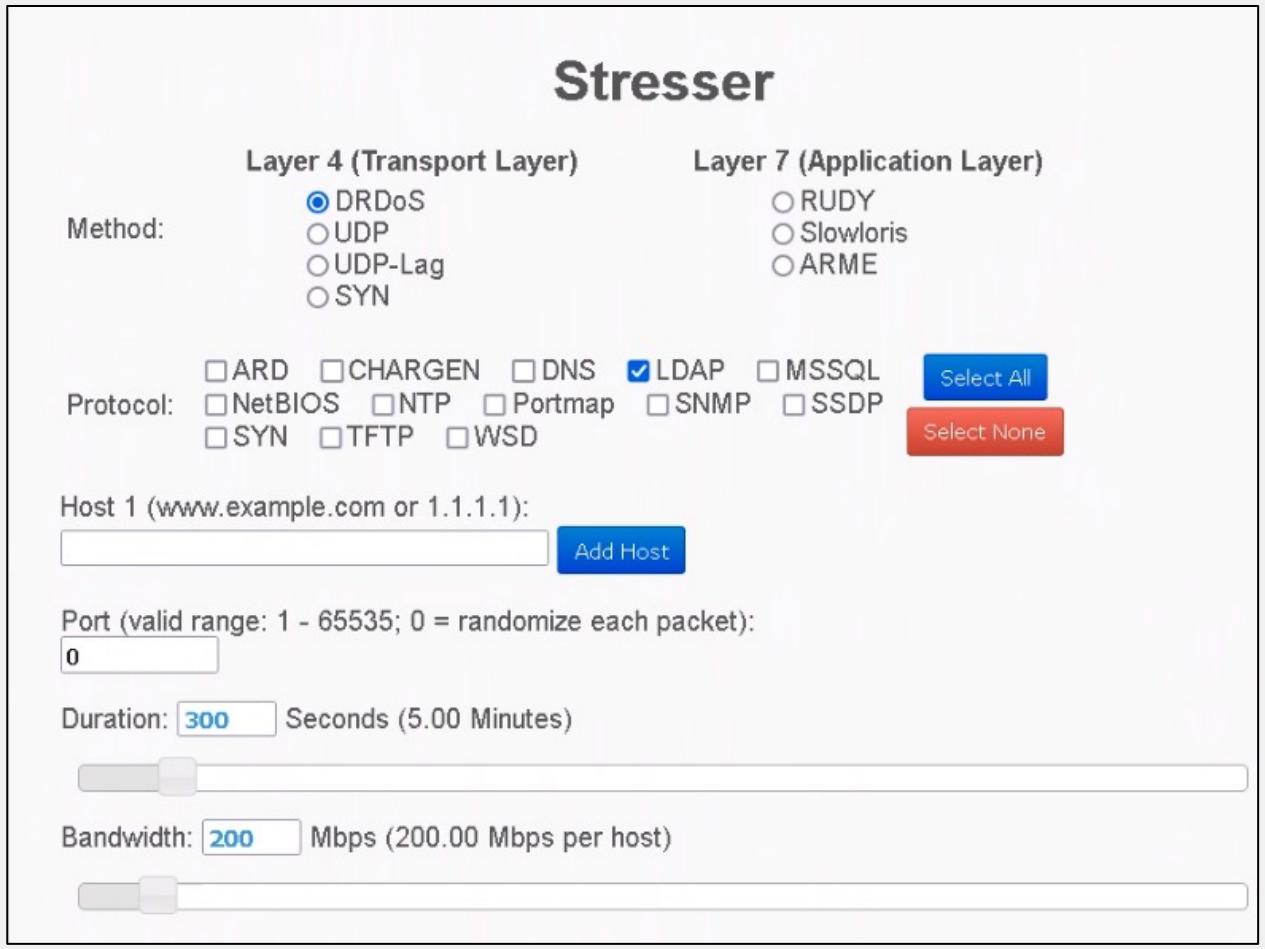
3) 2016+ Сучасність

- 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

© Fortinet Inc. All Rights Reserved.

DDoS це дешево

і таких інструментів багато



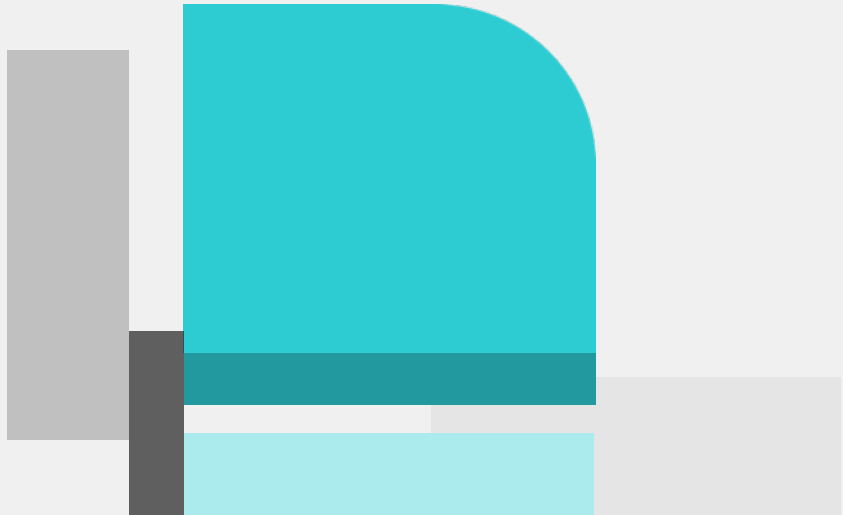
IP Stresser

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

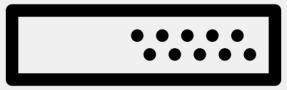
Приклад:
SYN-ACK flood на TCP
порт що не моніториться

© Fortinet Inc. All Rights Reserved.

Варіанти захисту
Що обрати?



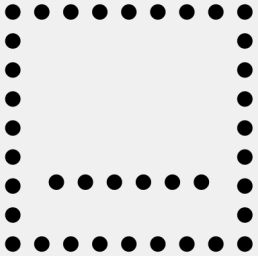
Формфактори



Апаратний пристрій

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

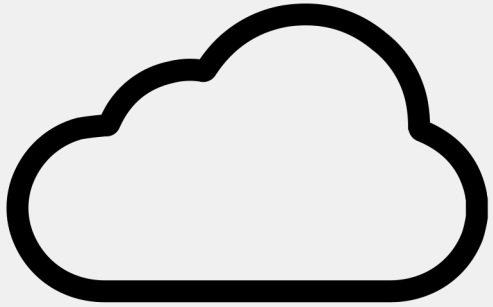
Рішення «поставити на канал» собі або провайдеру для захисту від мережевих та атак та нешифрованих протоколів



VM

- Гнучкість ліцензування та швидкодії
- Можливість переїзду
- Детальні налаштування

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



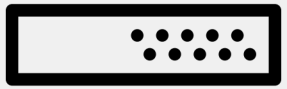
Хмара

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

Базовий функціонал з безлімітною швидкодією

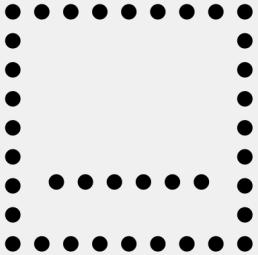
© Fortinet Inc. All Rights Reserved.

Формфактори і їх нюанси



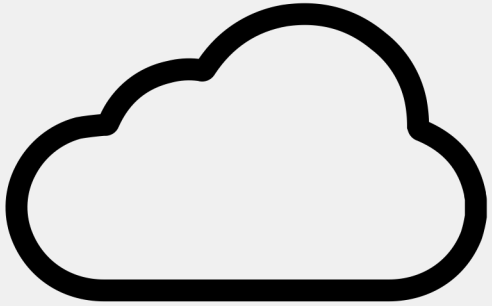
Апаратний пристрій

- 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

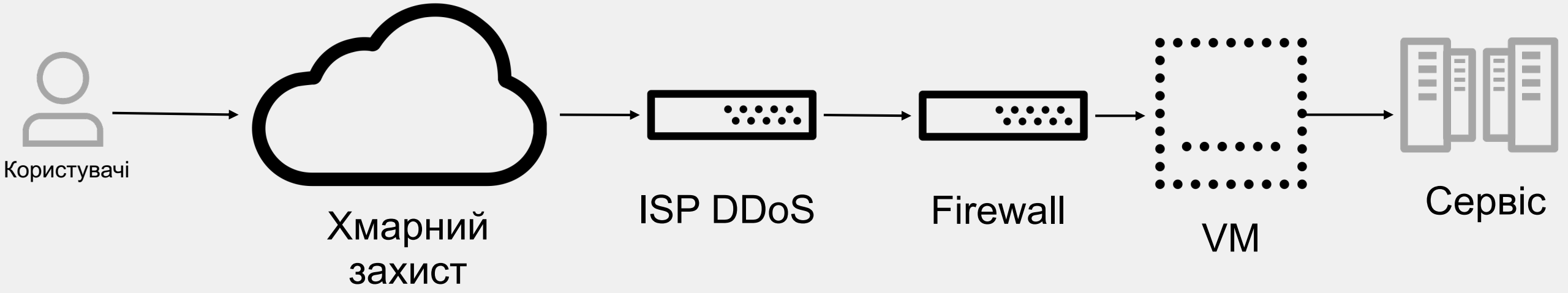


Хмара

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

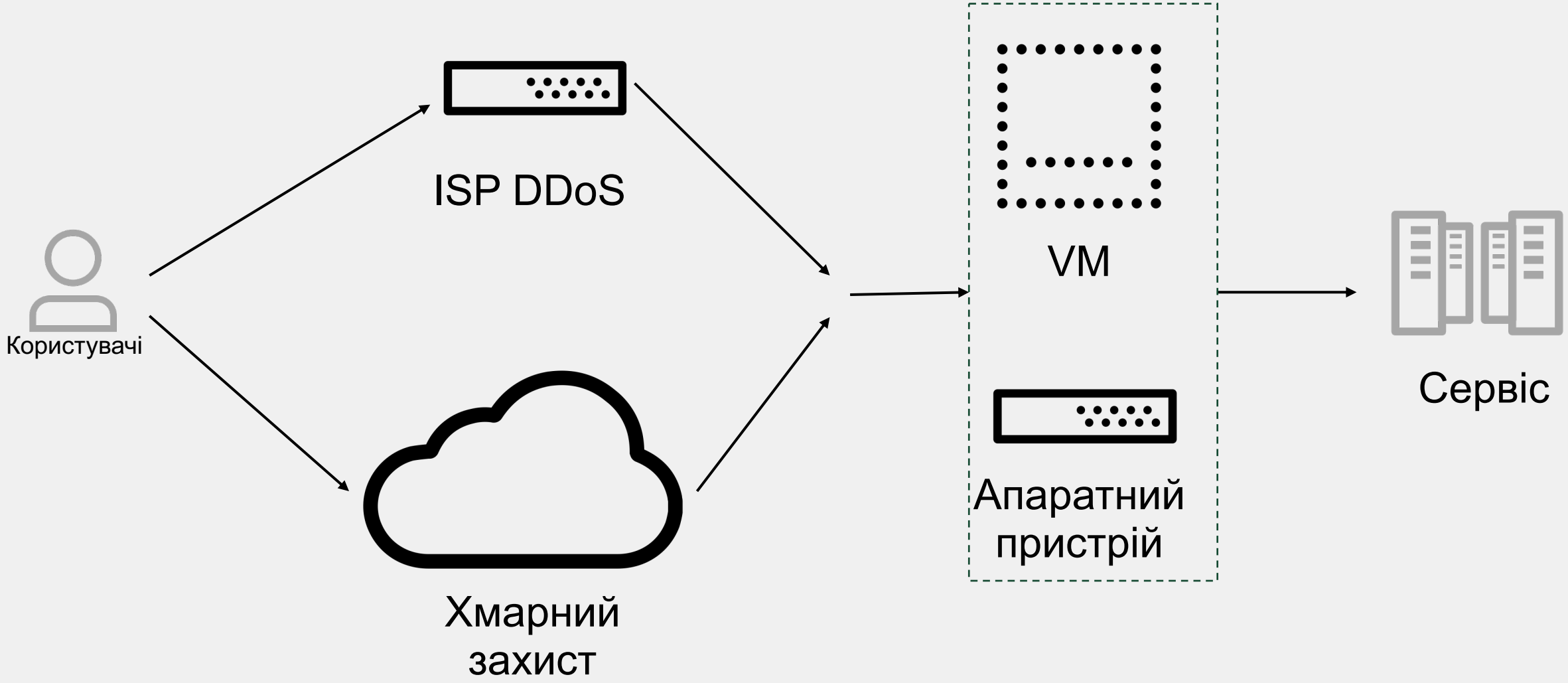
© Fortinet Inc. All Rights Reserved.

Ідеальний світ



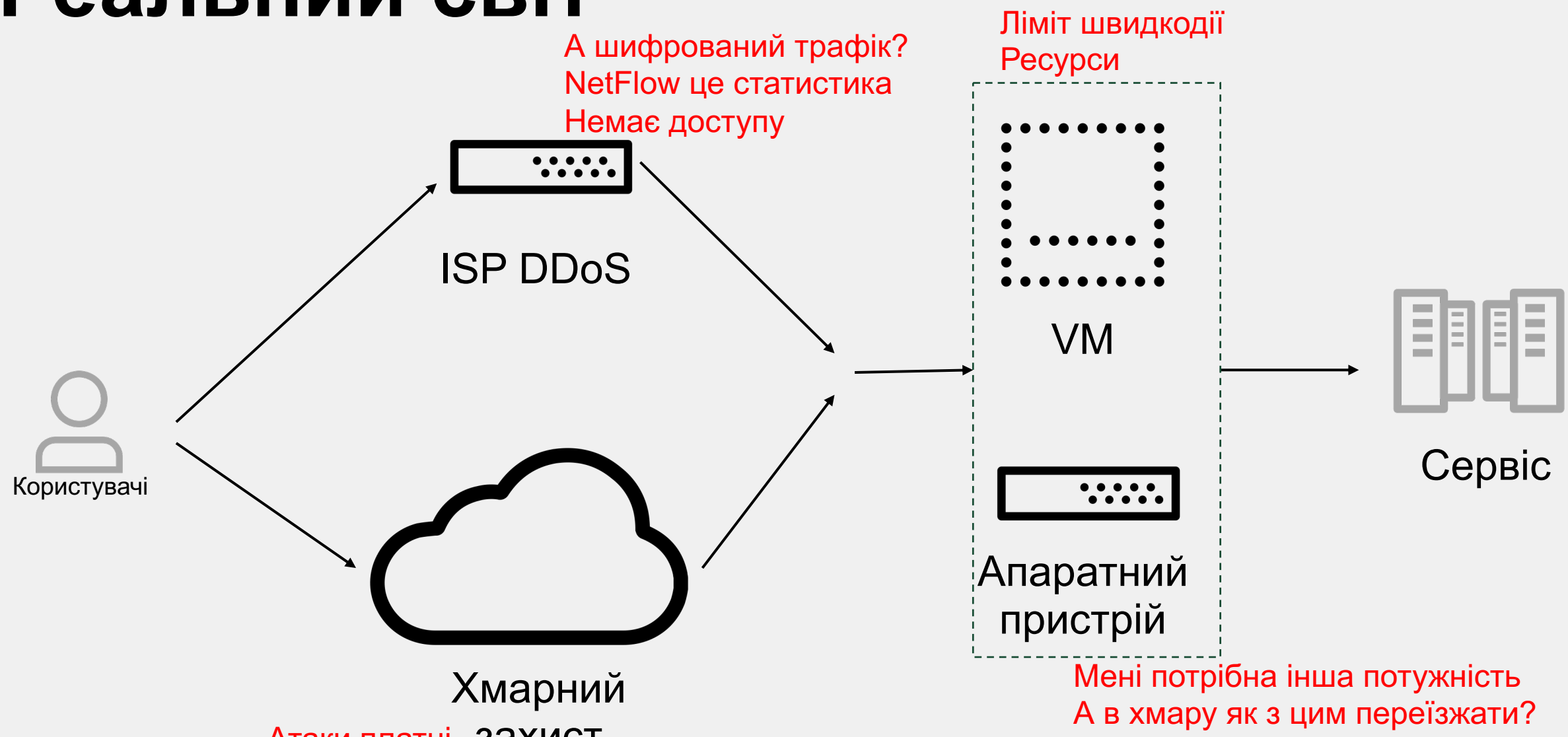
© Fortinet Inc. All Rights Reserved.

Трохи ближче до реальності



© Fortinet Inc. All Rights Reserved.

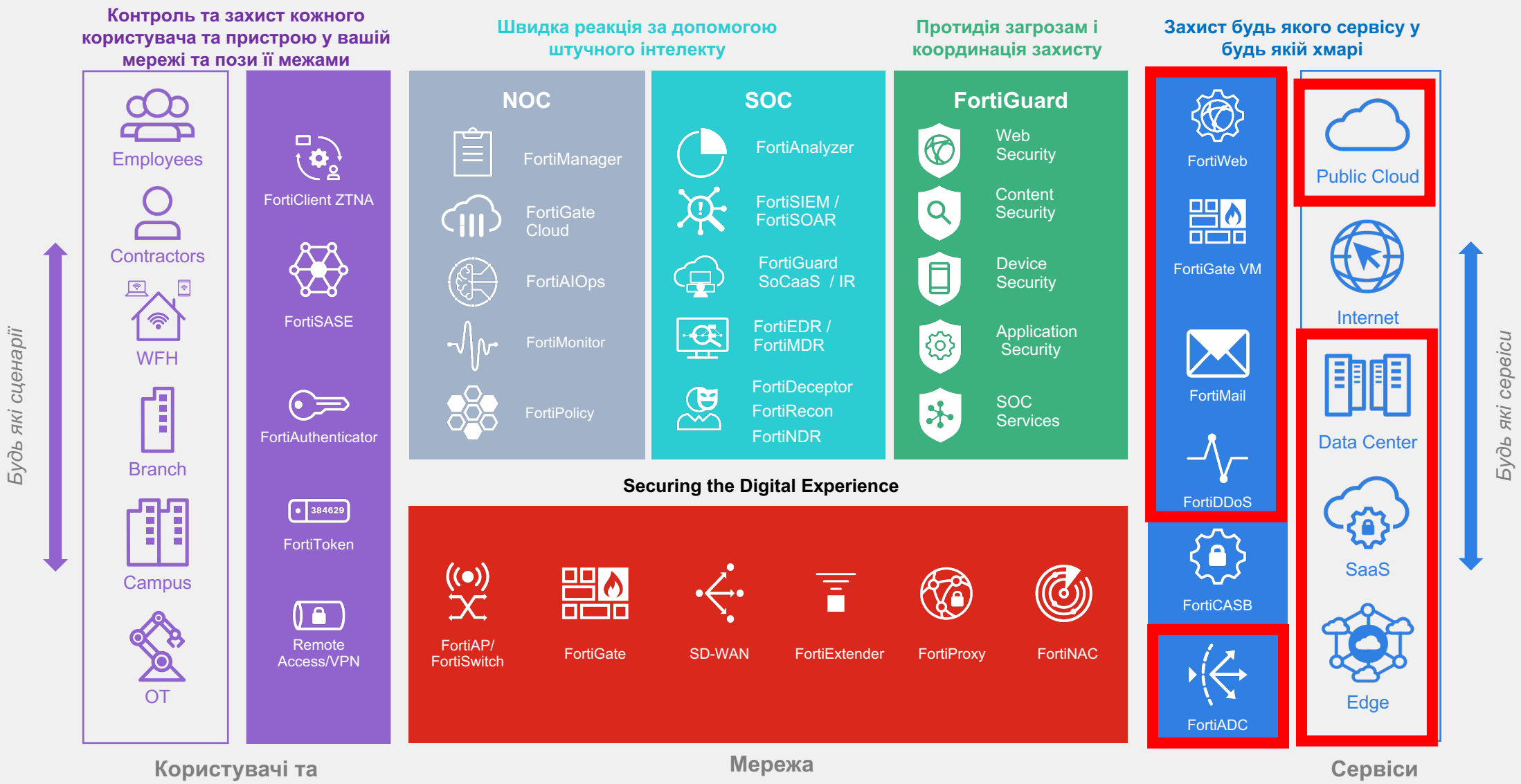
Реальний світ



© Fortinet Inc. All Rights Reserved.

Захист від Fortinet

Коротко про портфоліо Fortinet



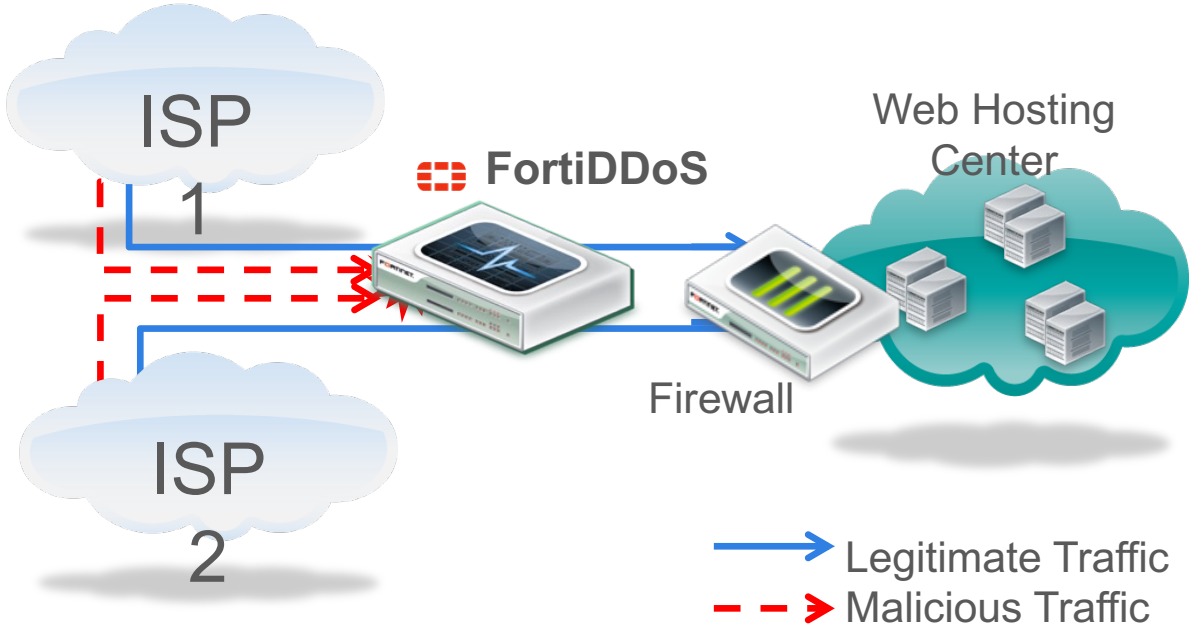
© Fortinet Inc. All Rights Reserved.

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



© Fortinet Inc. All Rights Reserved.

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
Mitigation2,3	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		

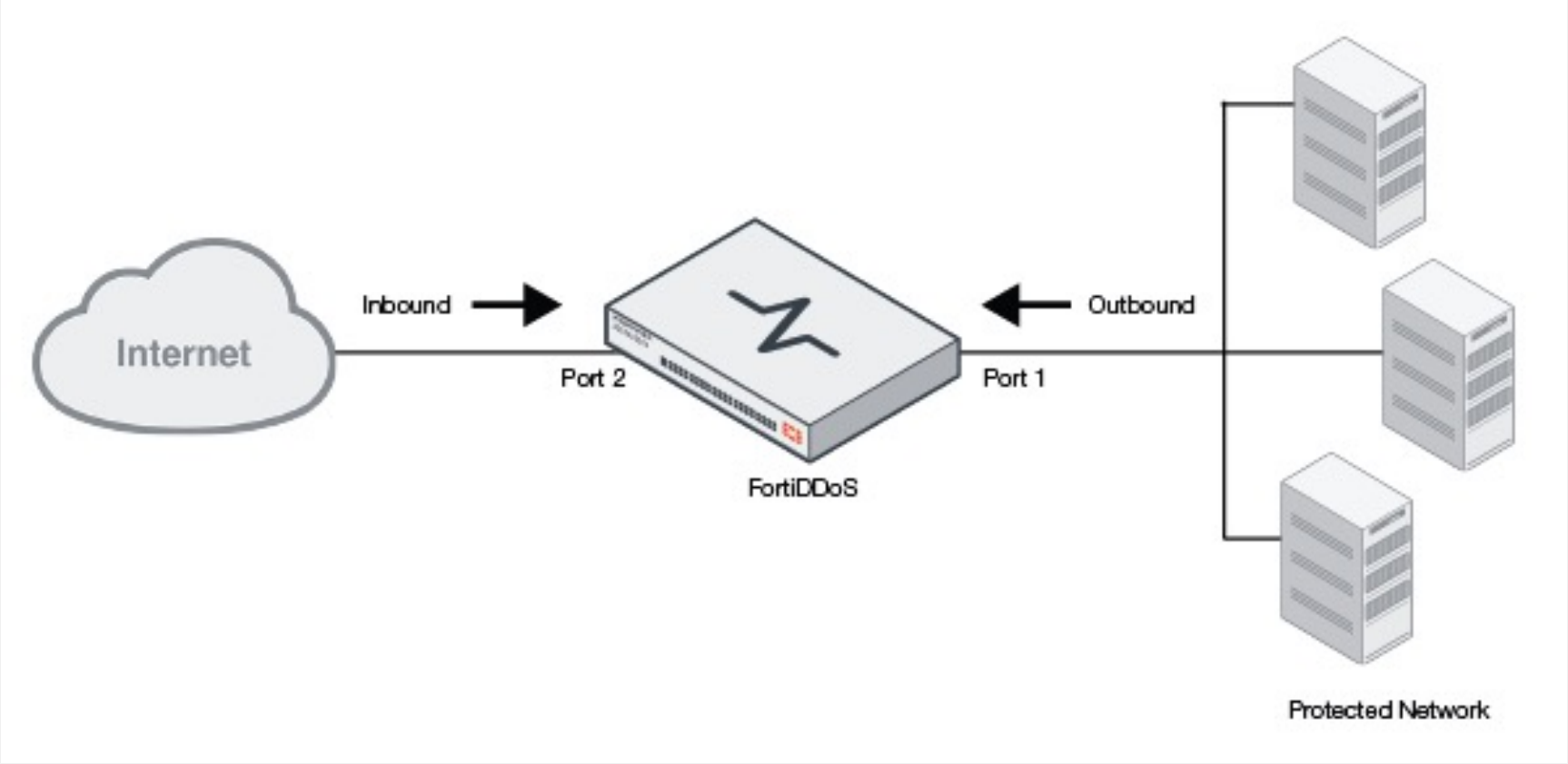
© Fortinet Inc. All Rights Reserved.

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

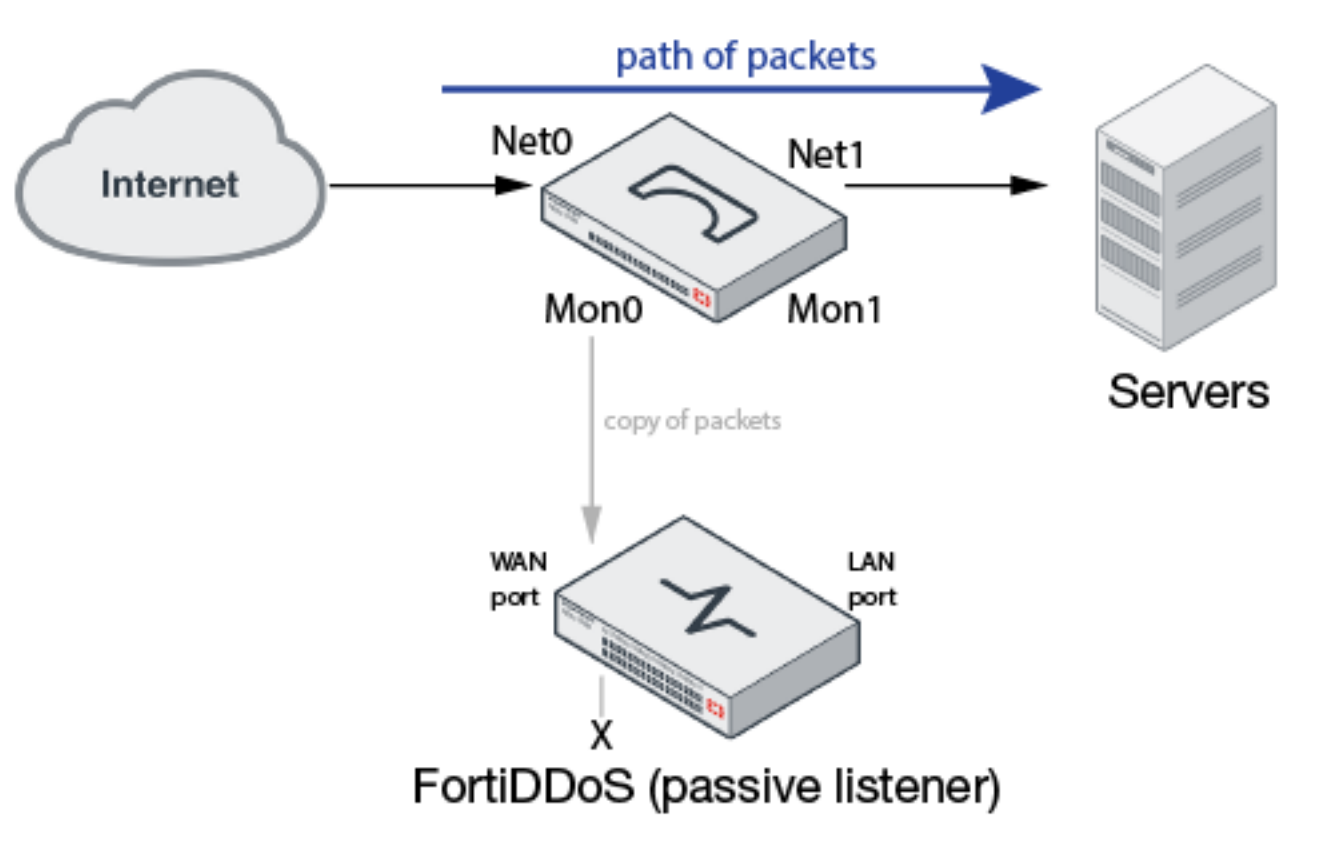
© Fortinet Inc. All Rights Reserved.

Типова інсталяція «inline»



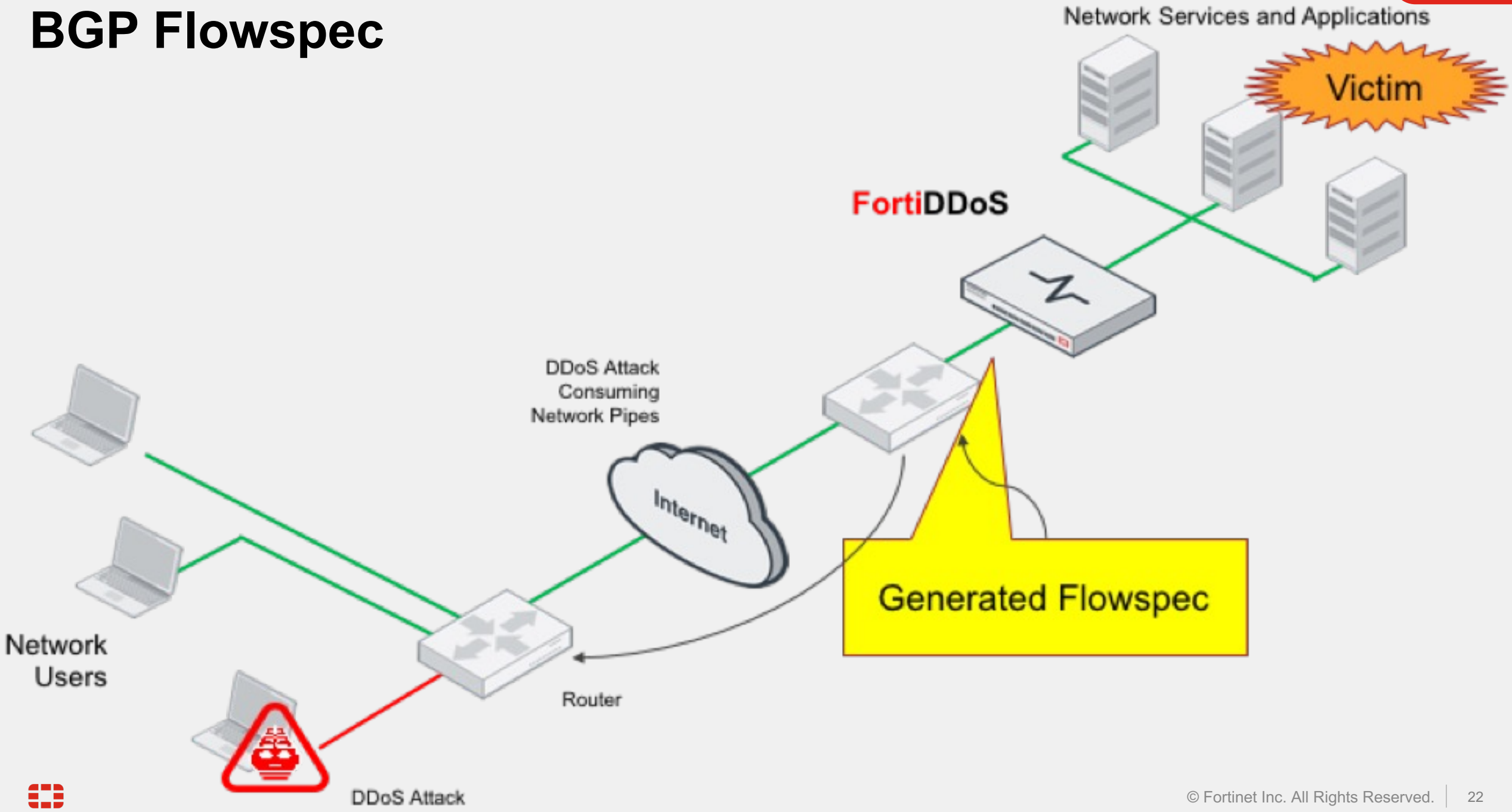
© Fortinet Inc. All Rights Reserved.

Типова інсталяція «в стороні»



© Fortinet Inc. All Rights Reserved.

BGP Flowspec



© Fortinet Inc. All Rights Reserved.

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:

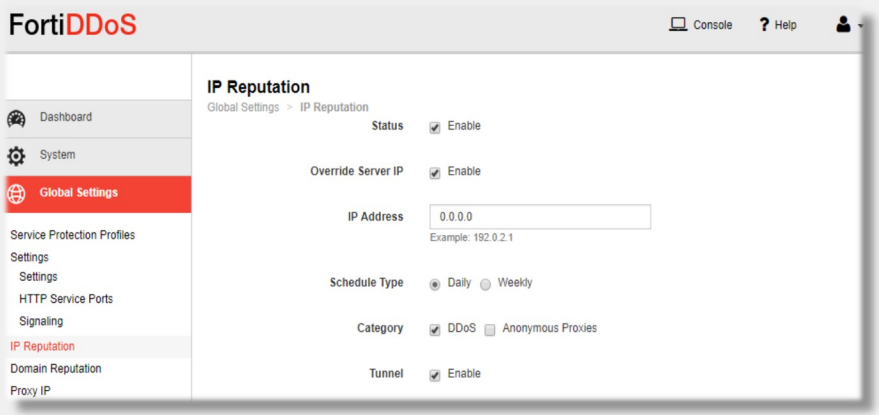
```
config ddos global cloud-signaling
  set mode { customer-premises | service-provider }
  set timeout <integer>
  config devices
    edit <device_name>
      set enable { enable | disable }
      set device-type { FortiDDoS | Third-Party }
      set serial-number <string>
      set shared-secret <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
```

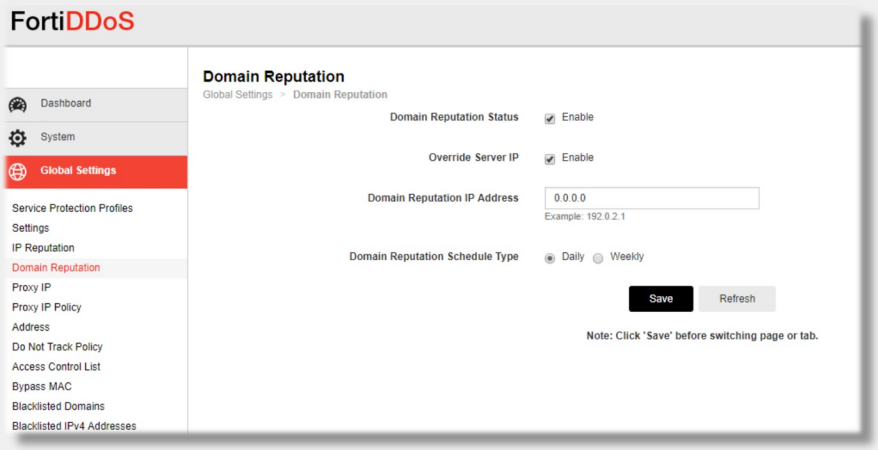
© Fortinet Inc. All Rights Reserved.

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

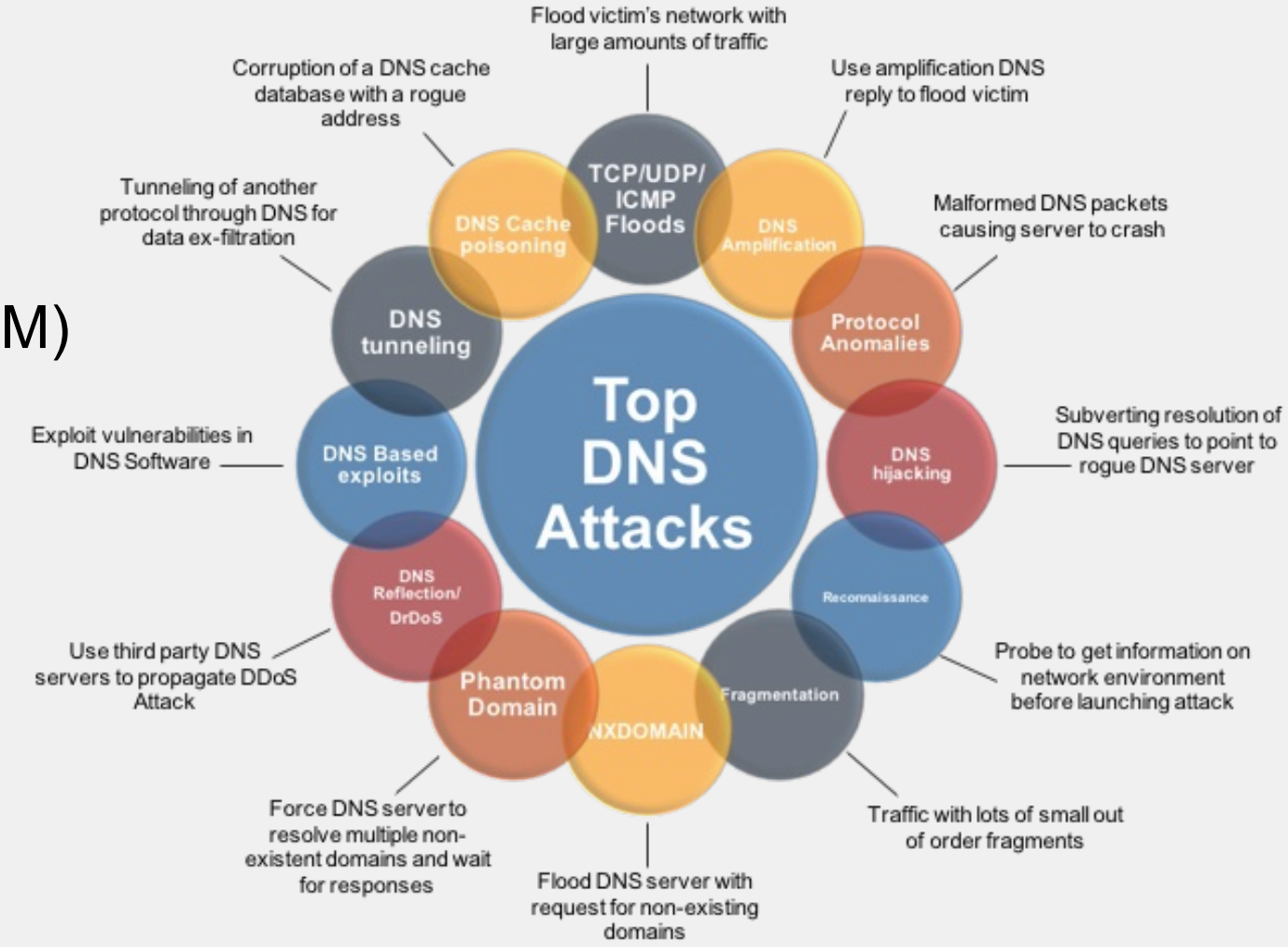




© Fortinet Inc. All Rights Reserved.

FortiDDoS: DNS захист

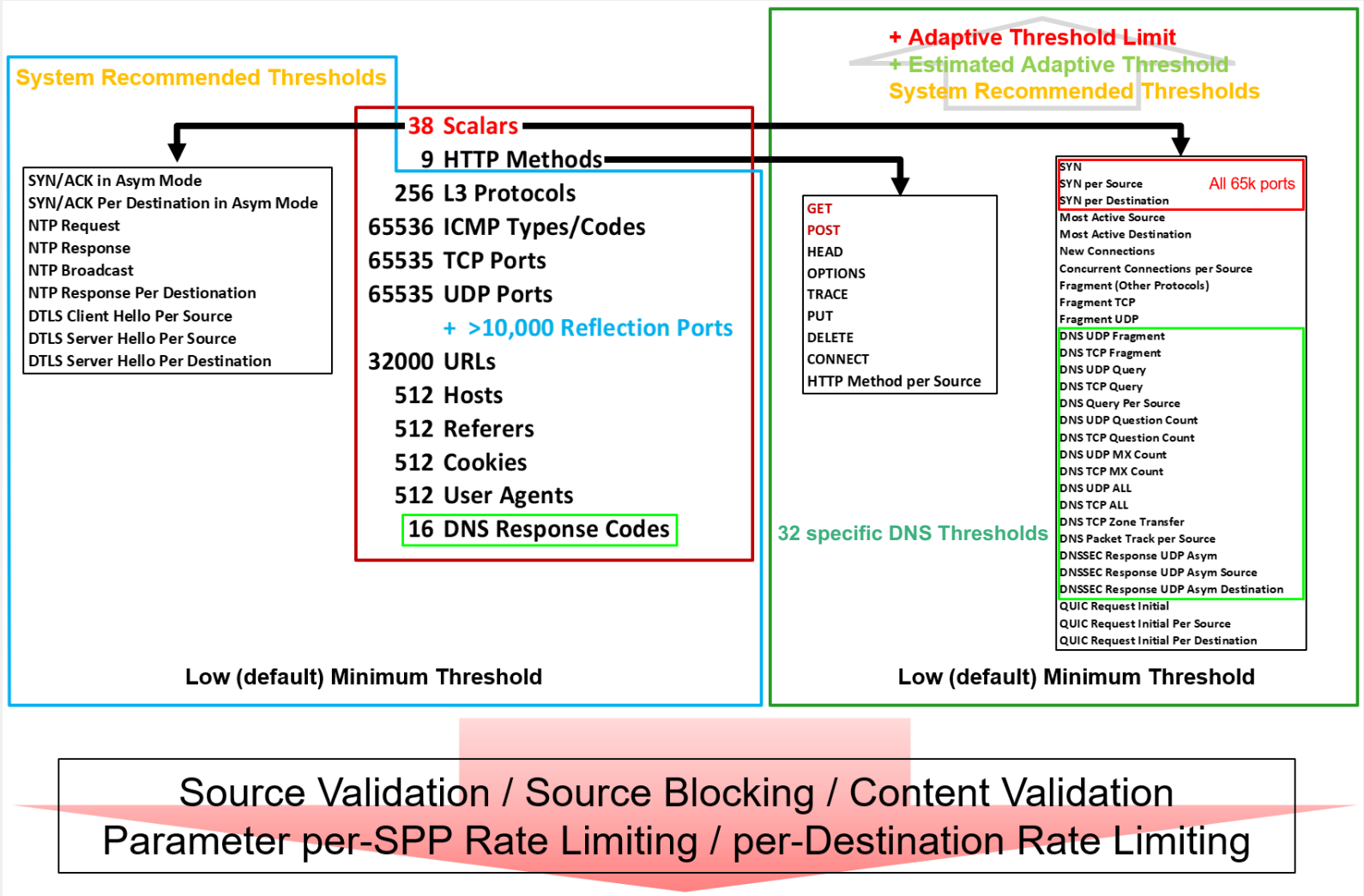
- FQDN Allowlist
- DNS Anomaly Prevention
- DNS Query Response Match (DQRM)
- Legitimate Query (LQ)
- Legitimate IP Table
- DNS Cache
- Source Tracking



© Fortinet Inc. All Rights Reserved.

Захист сервісу (SPP)

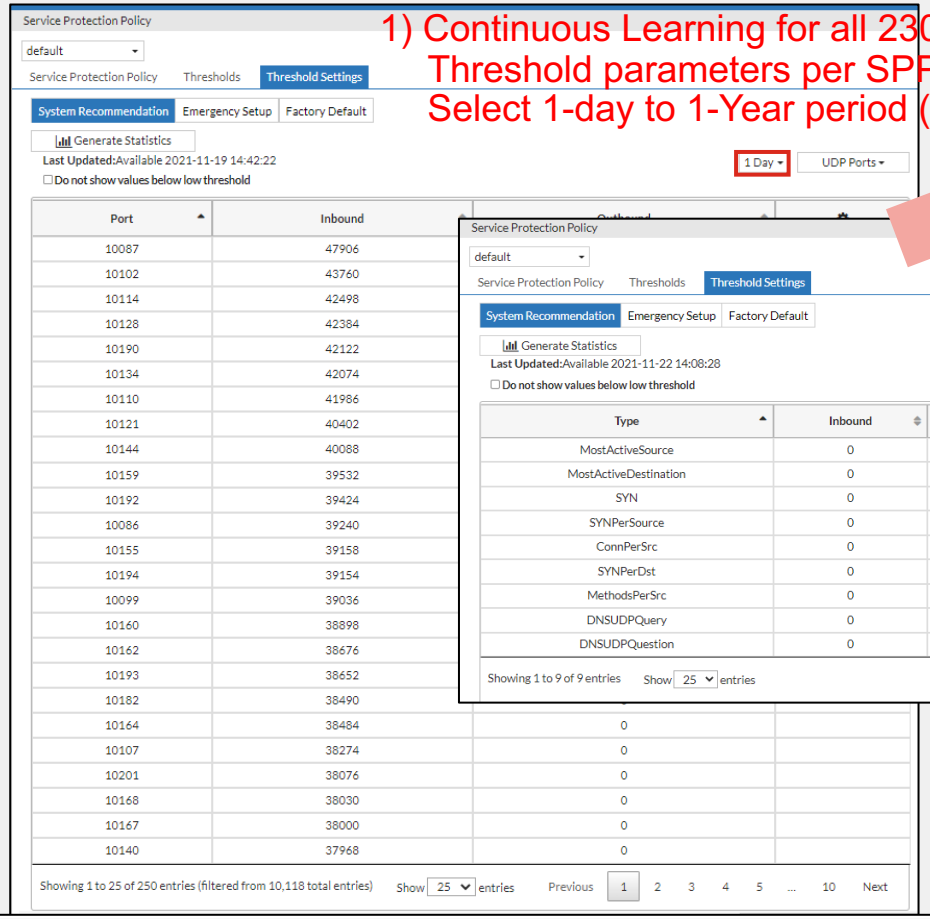
Моніторинг більше 230,000 параметрів
Час реакції <1 секунди!

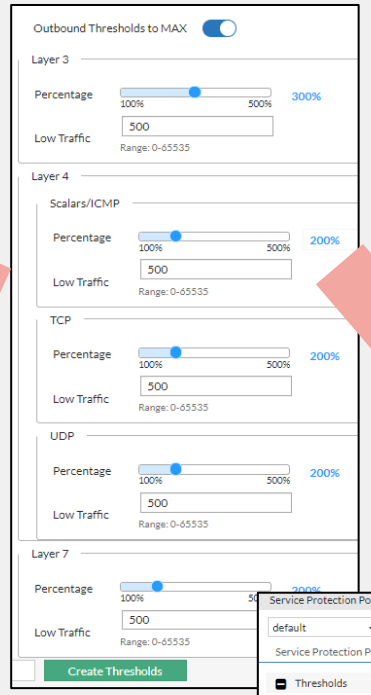


© Fortinet Inc. All Rights Reserved.

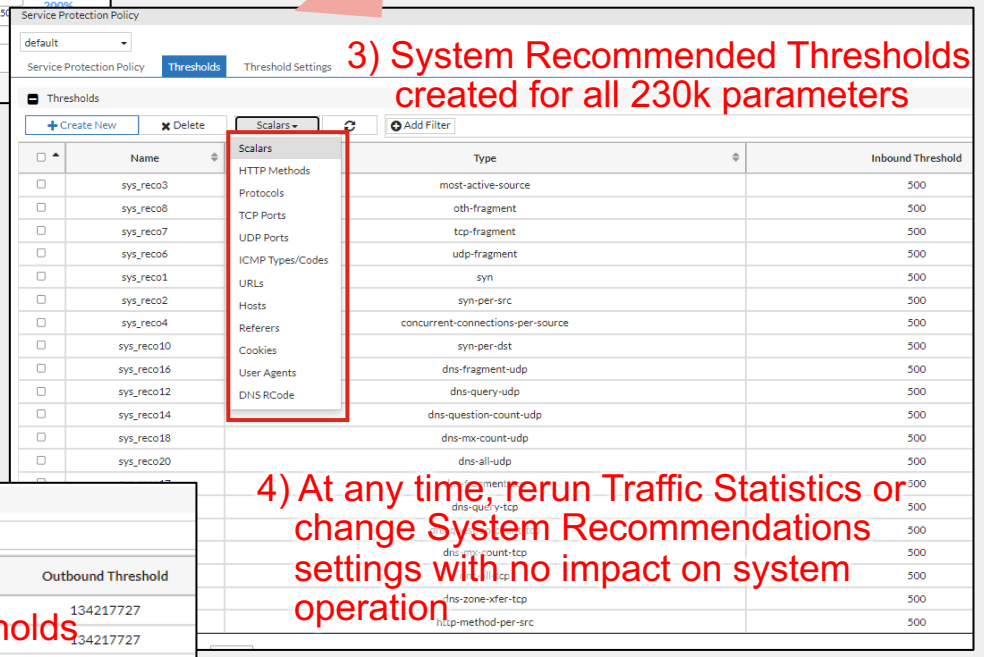
Машинне навчання

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

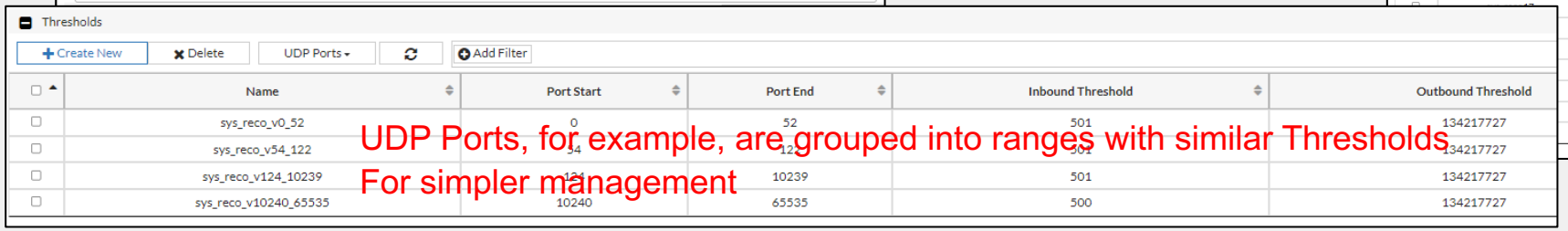




2) Apply System Recommended Minimum Threshold and/or Multiplier (Defaults almost always used.)



3) System Recommended Thresholds created for all 230k parameters

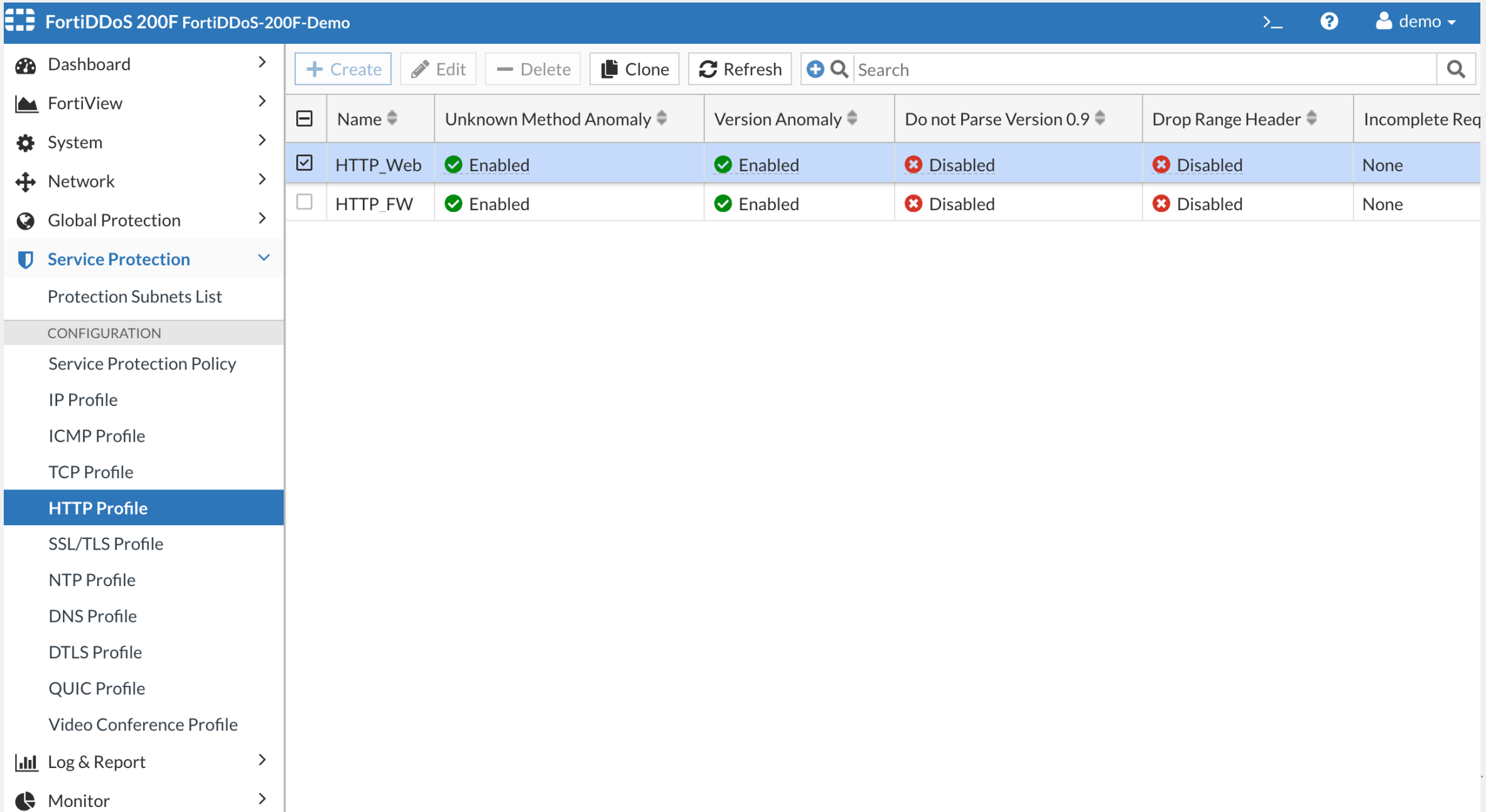


UDP Ports, for example, are grouped into ranges with similar Thresholds
For simpler management

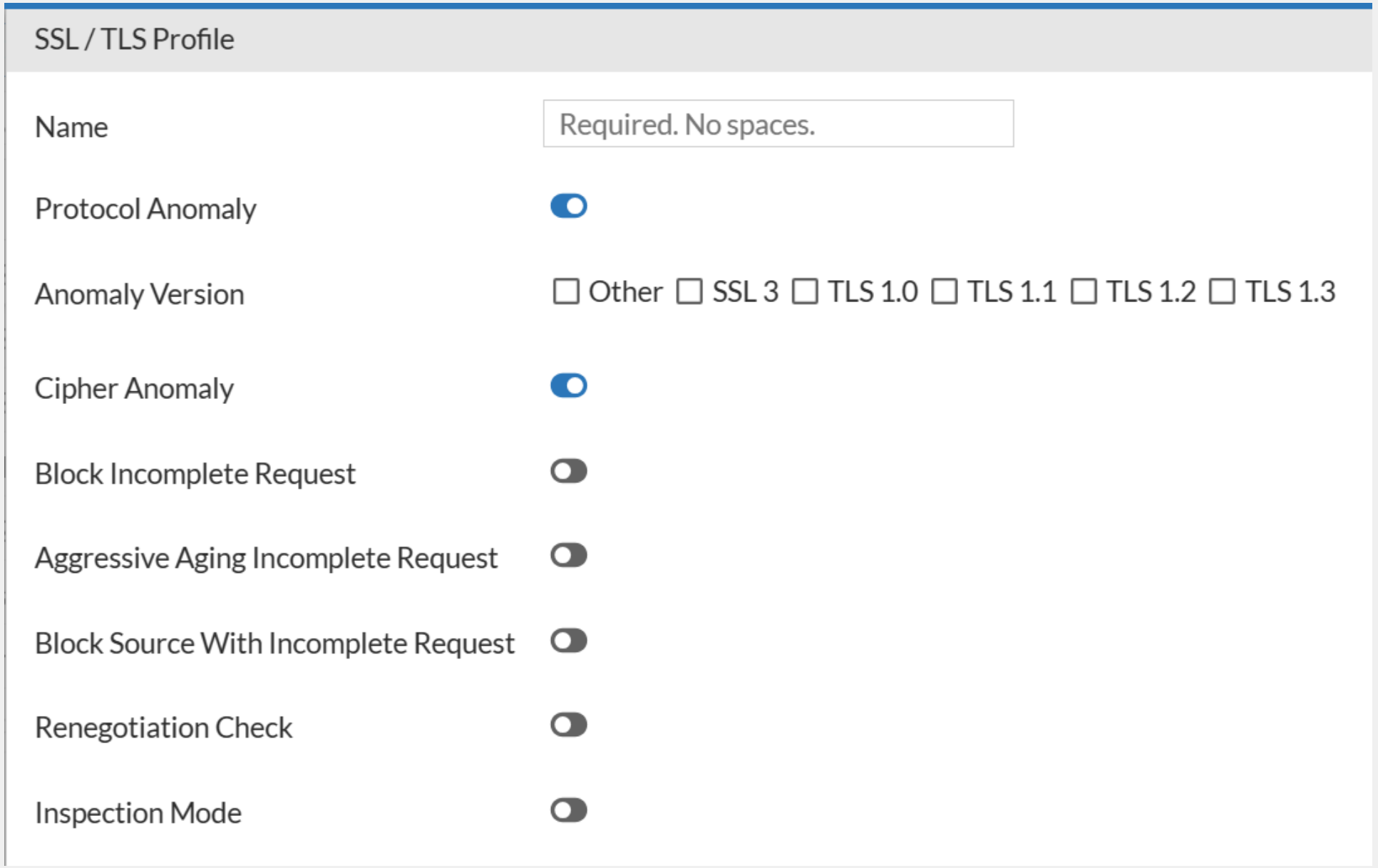
4) At any time, rerun Traffic Statistics or change System Recommendations settings with no impact on system operation

© Fortinet Inc. All Rights Reserved.

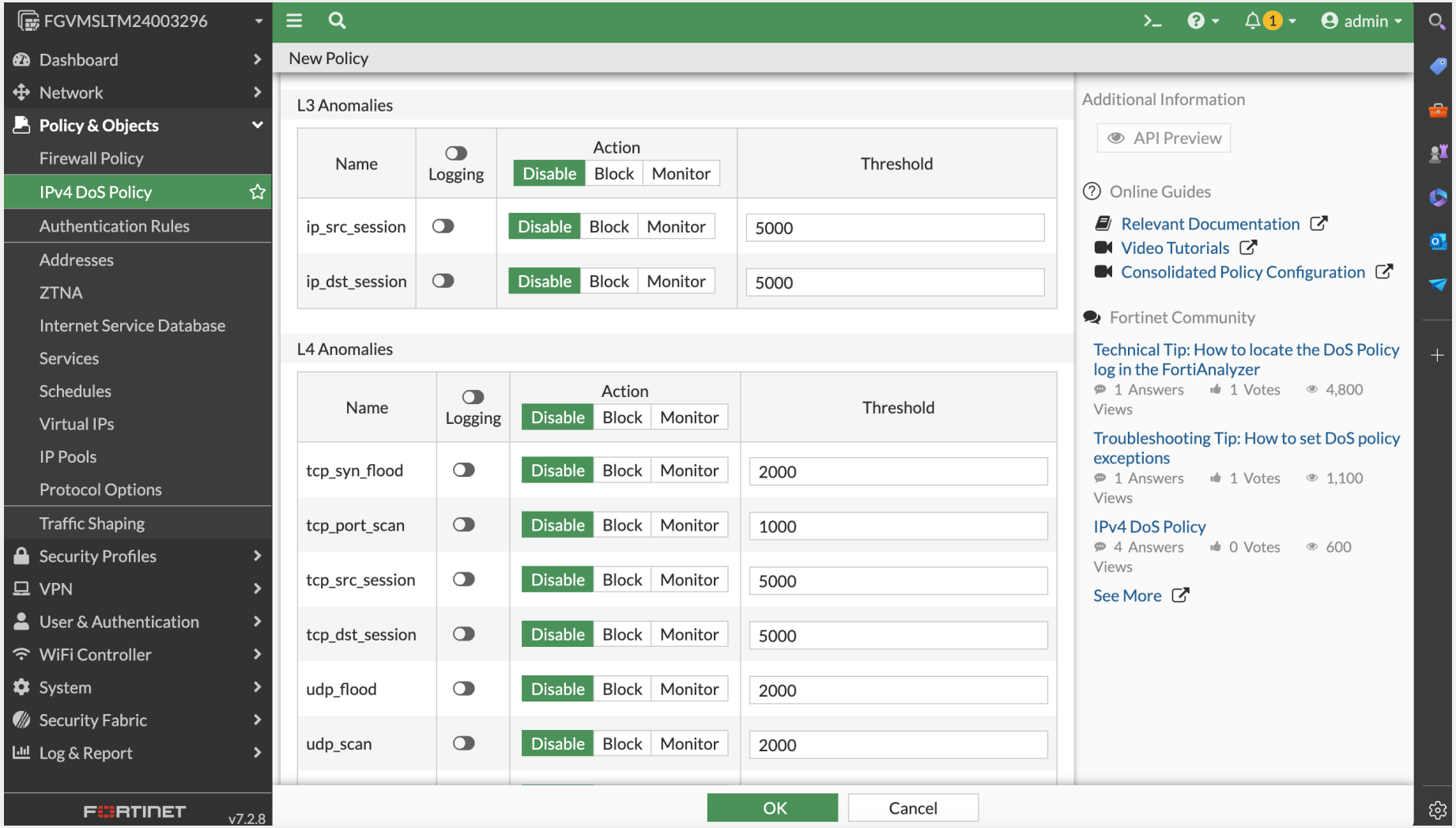
Протоколи


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



FortiGate

© Fortinet Inc. All Rights Reserved.

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

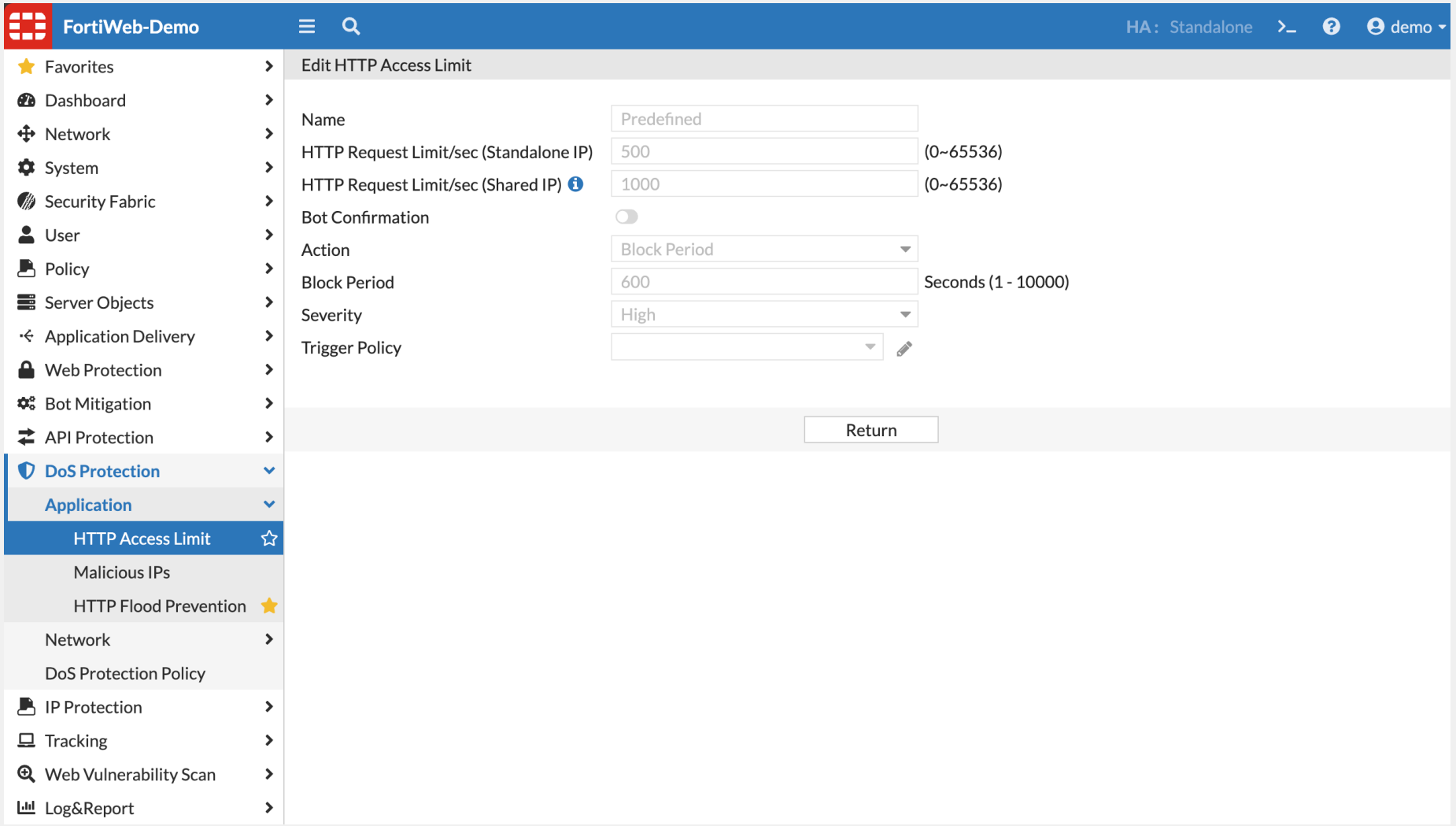
© Fortinet Inc. All Rights Reserved.

Варіант 2. Класичні наземні рішення

FortiGate

© Fortinet Inc. All Rights Reserved.

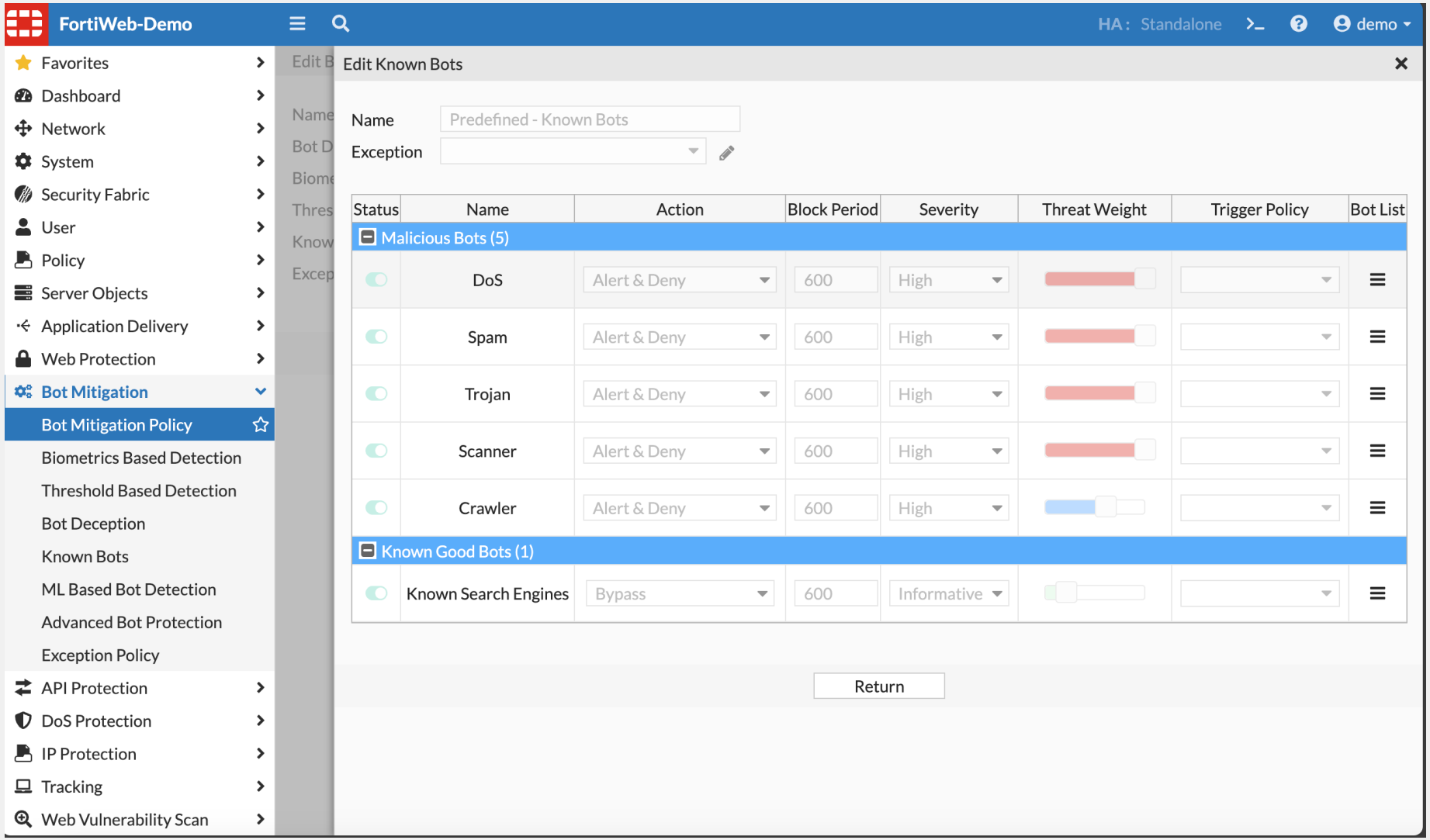
Варіант 2. Класичні наземні рішення



FortiWeb

© Fortinet Inc. All Rights Reserved.

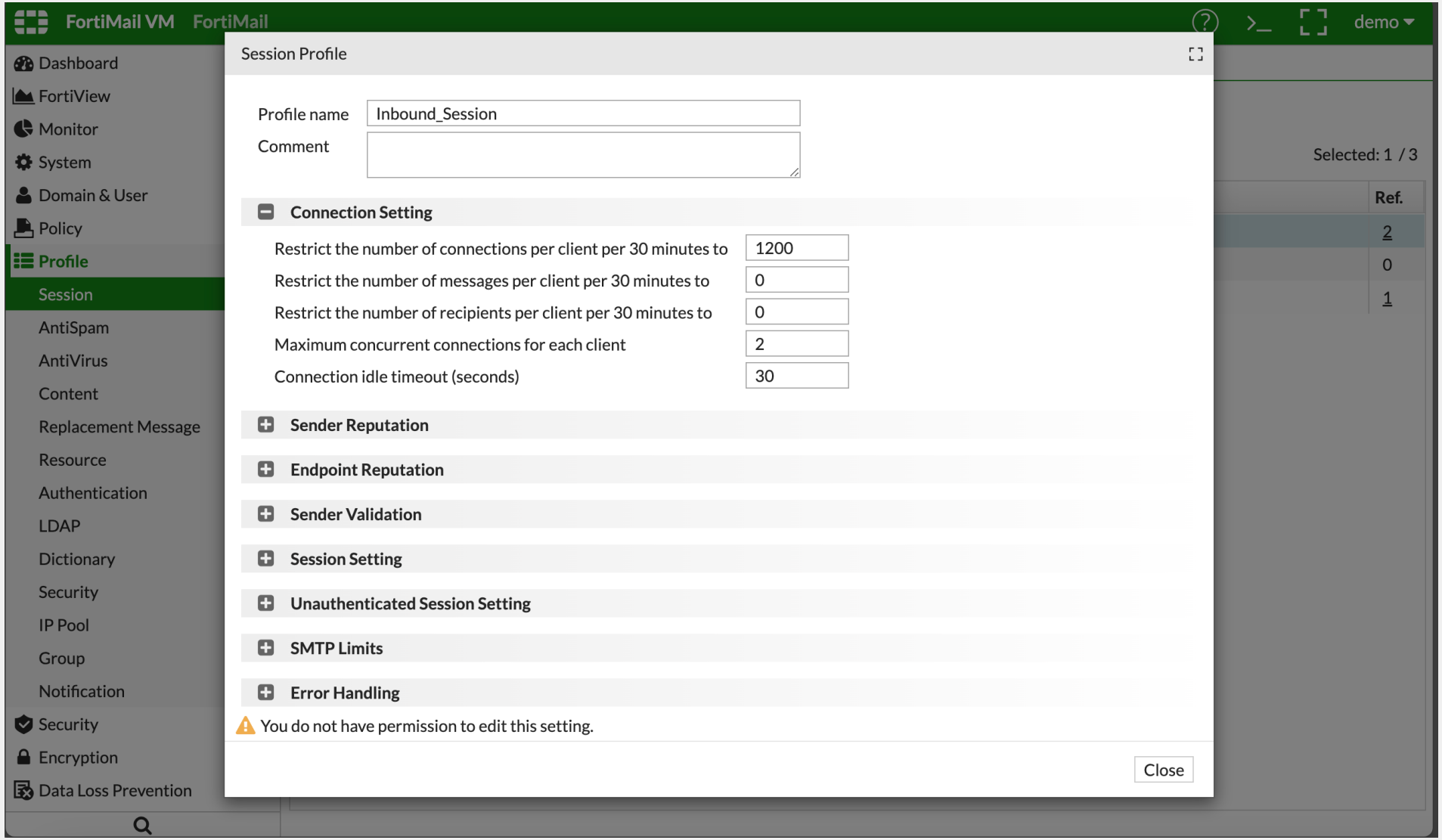
Варіант 2. Класичні наземні рішення



FortiWeb

© Fortinet Inc. All Rights Reserved.

Варіант 2. Класичні наземні рішення

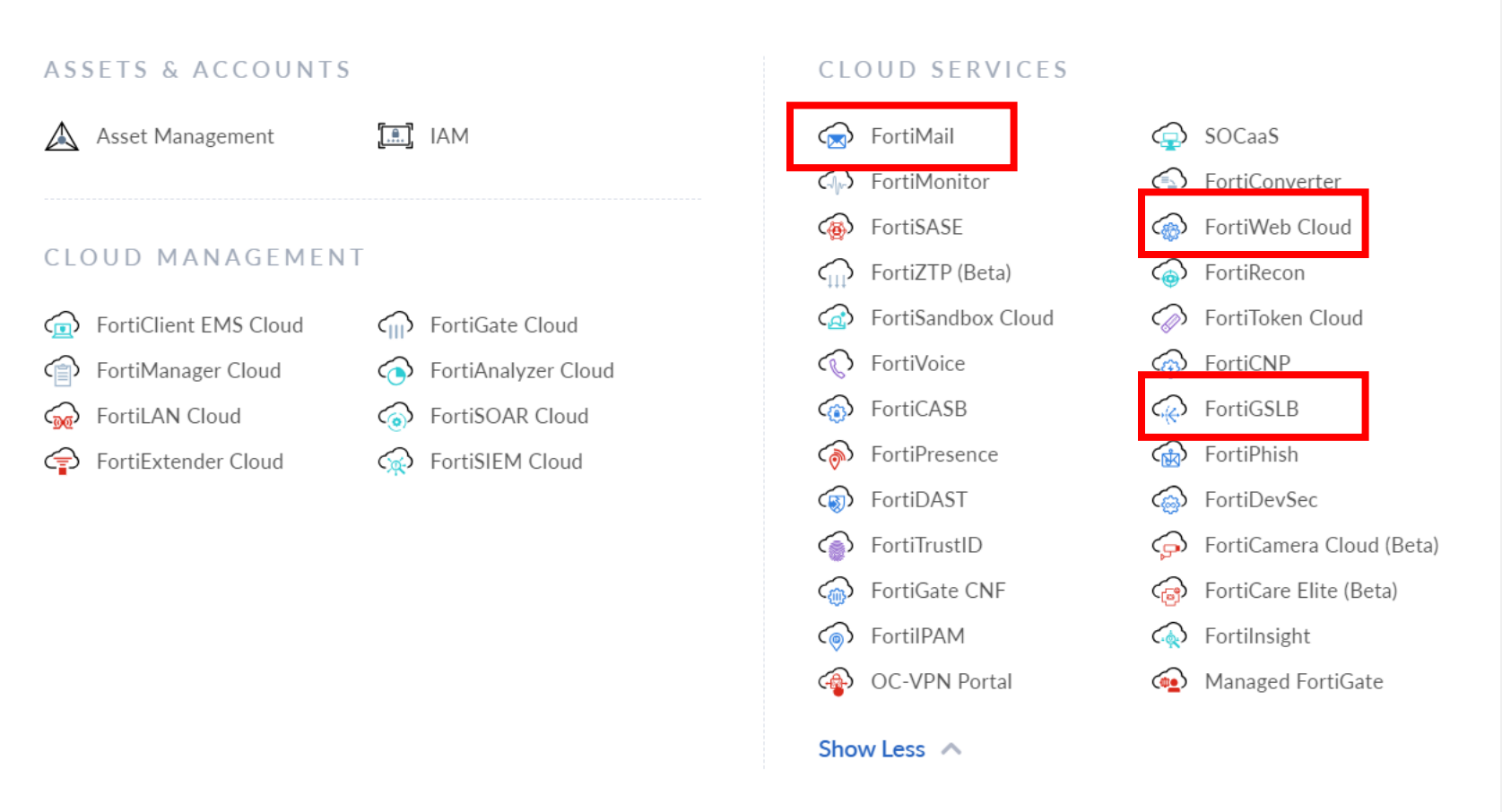


FortiMail

© Fortinet Inc. All Rights Reserved.

Варіант 3. SaaS рішення

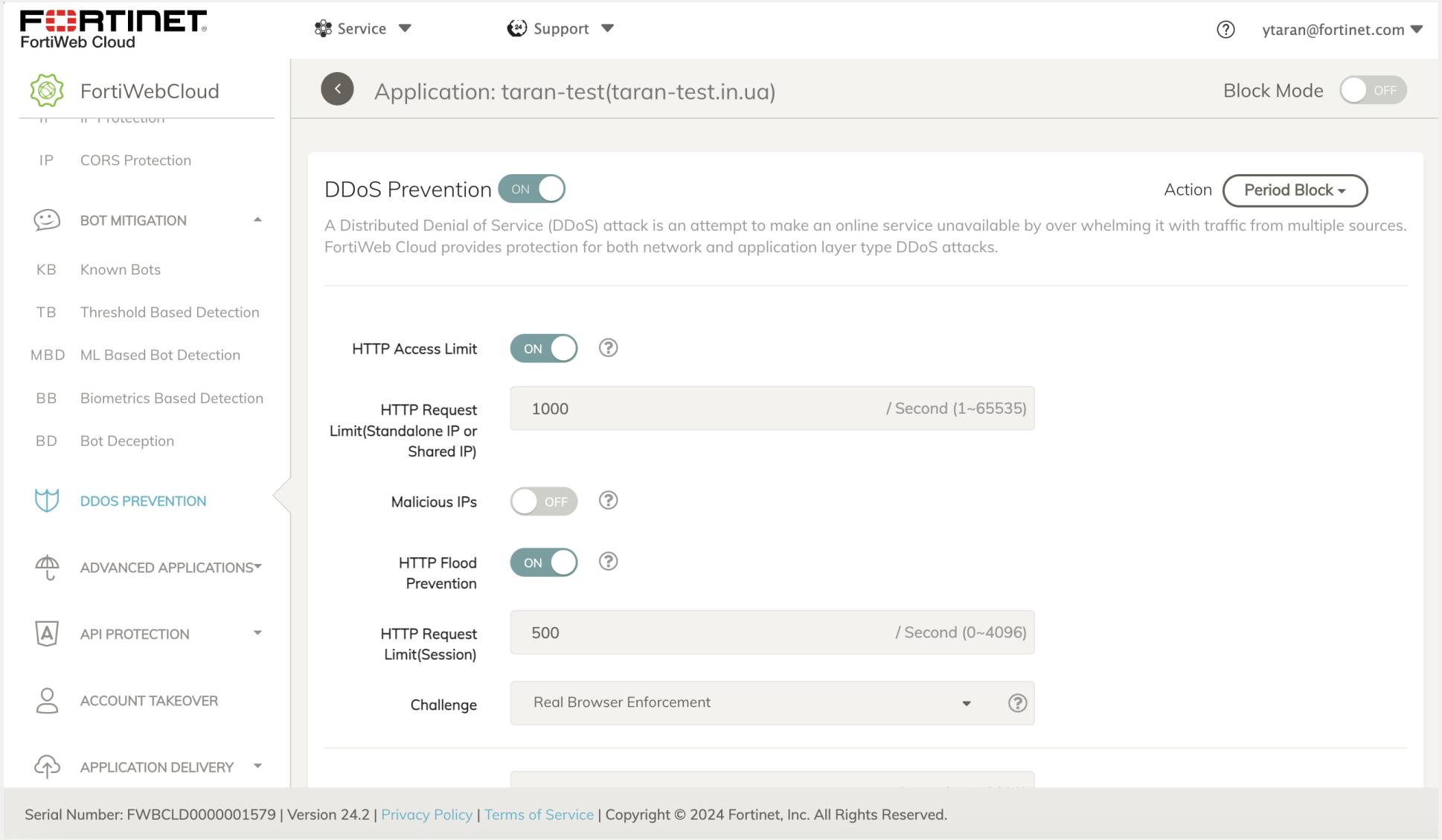
Перевірена безпека та зв’язок усюди



© Fortinet Inc. All Rights Reserved.

Варіант 3. SaaS рішення

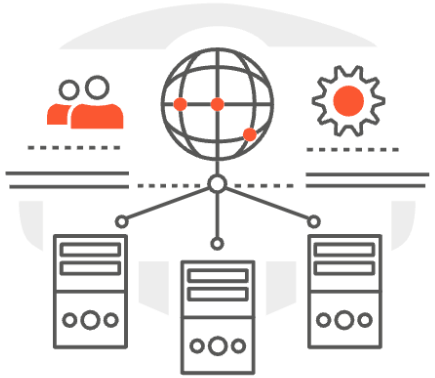
Наприклад FortiWeb



© Fortinet Inc. All Rights Reserved.

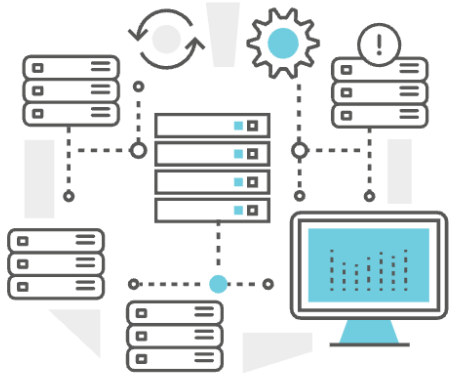
Варіант 3. SaaS рішення

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.

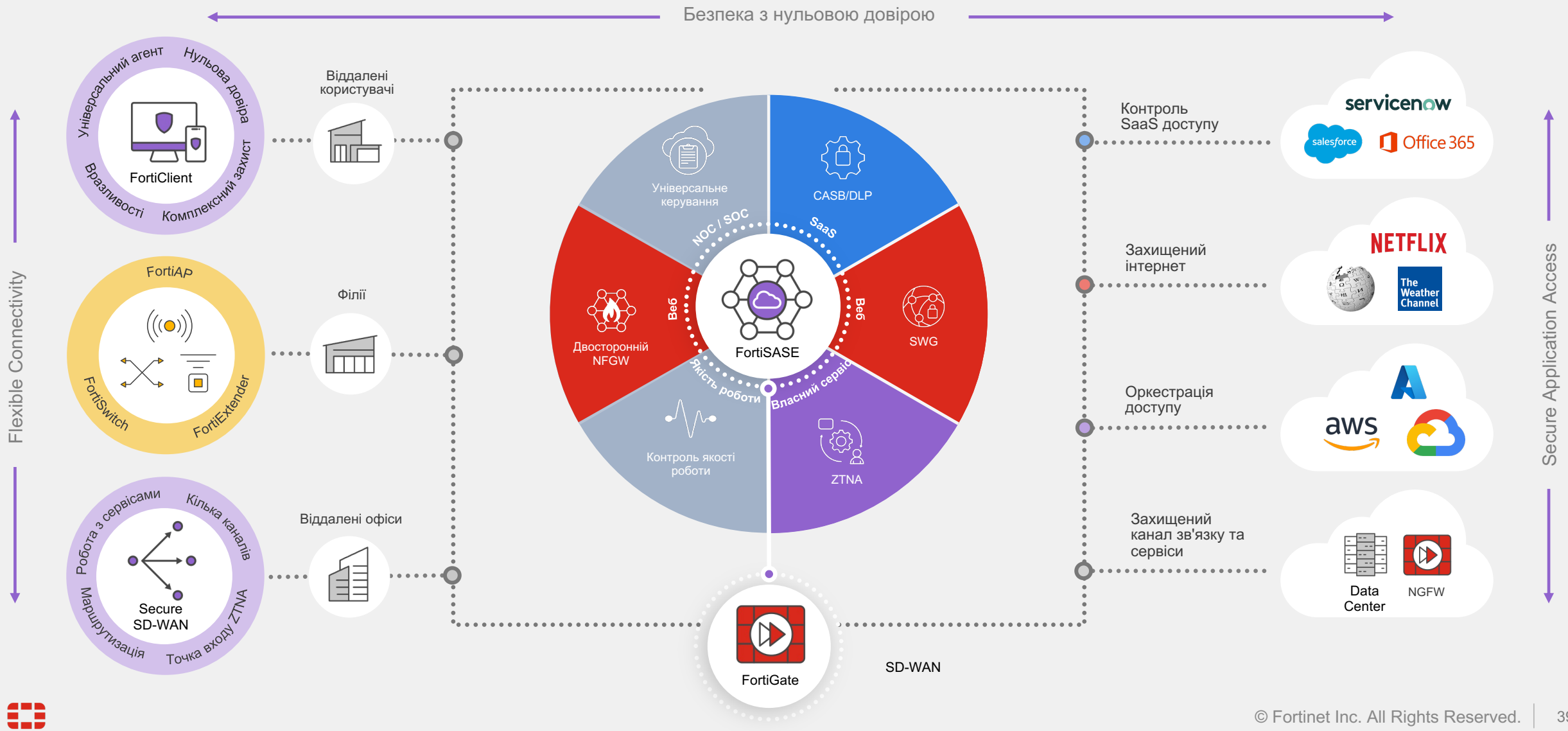
Synthetic Testing

Offers multisite application visibility with advanced application testing.

© Fortinet Inc. All Rights Reserved.

Варіант 4. Fortinet Universal SASE

Перевірена безпека та зв’язок усюди

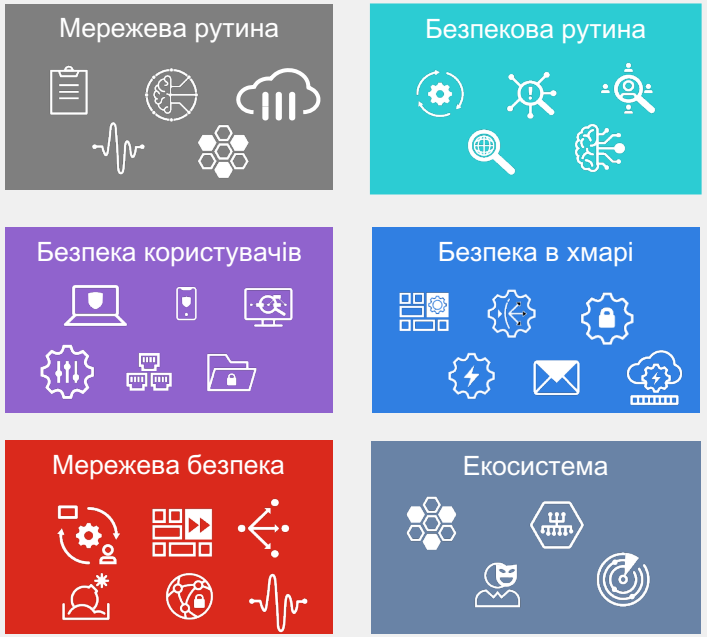


© Fortinet Inc. All Rights Reserved.

Висновки

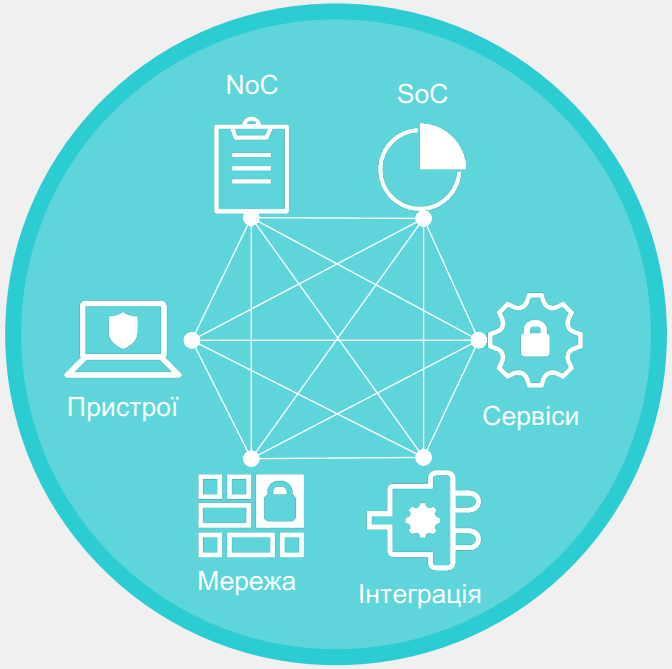
Комплексне рішення

30+ виробників



10 виробників

2-3 платформи



Розвиток замовника

© Fortinet Inc. All Rights Reserved.

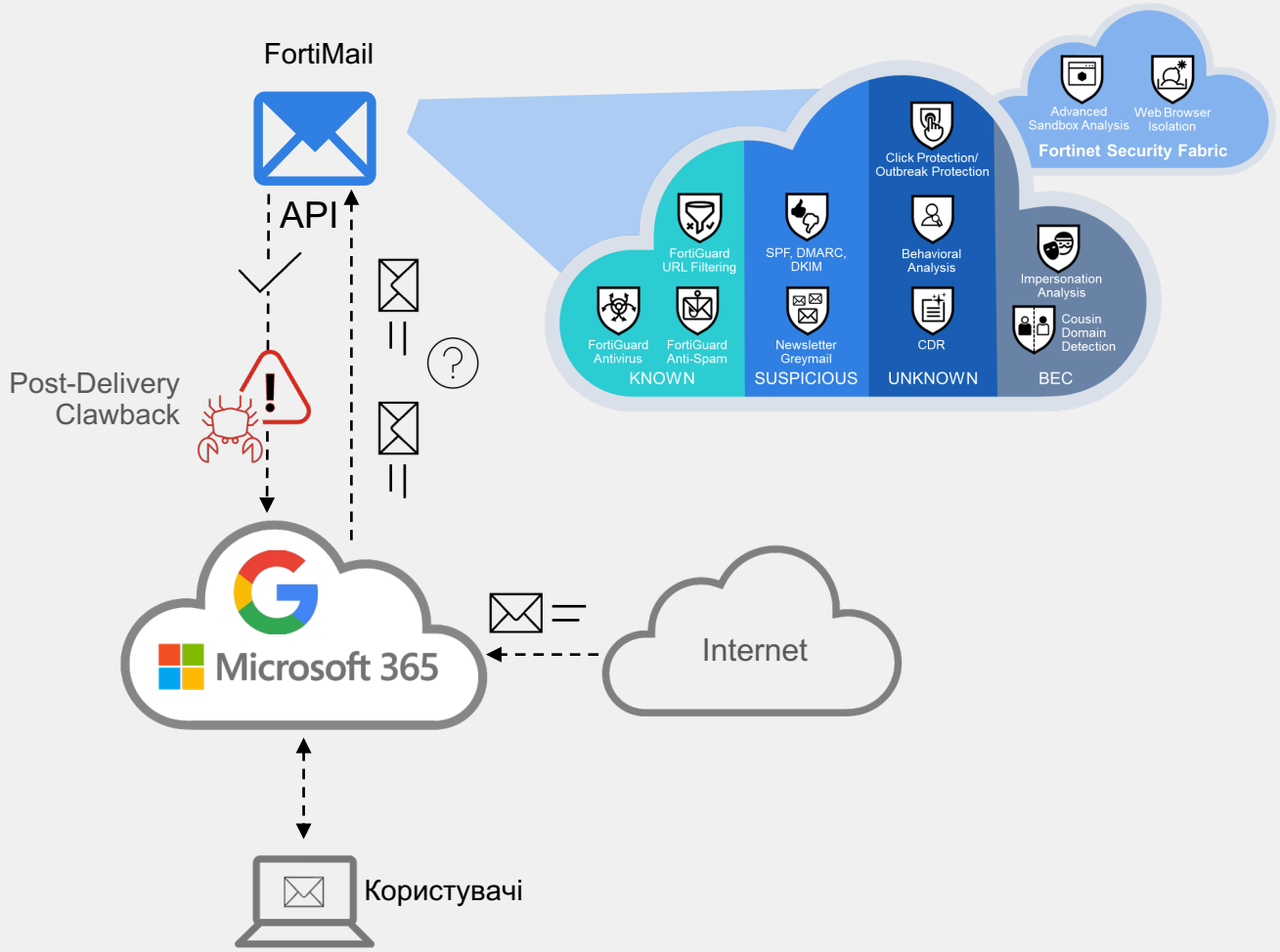
Архітектура 1.

Захист веб сервісів

© Fortinet Inc. All Rights Reserved.

Архітектура 2.

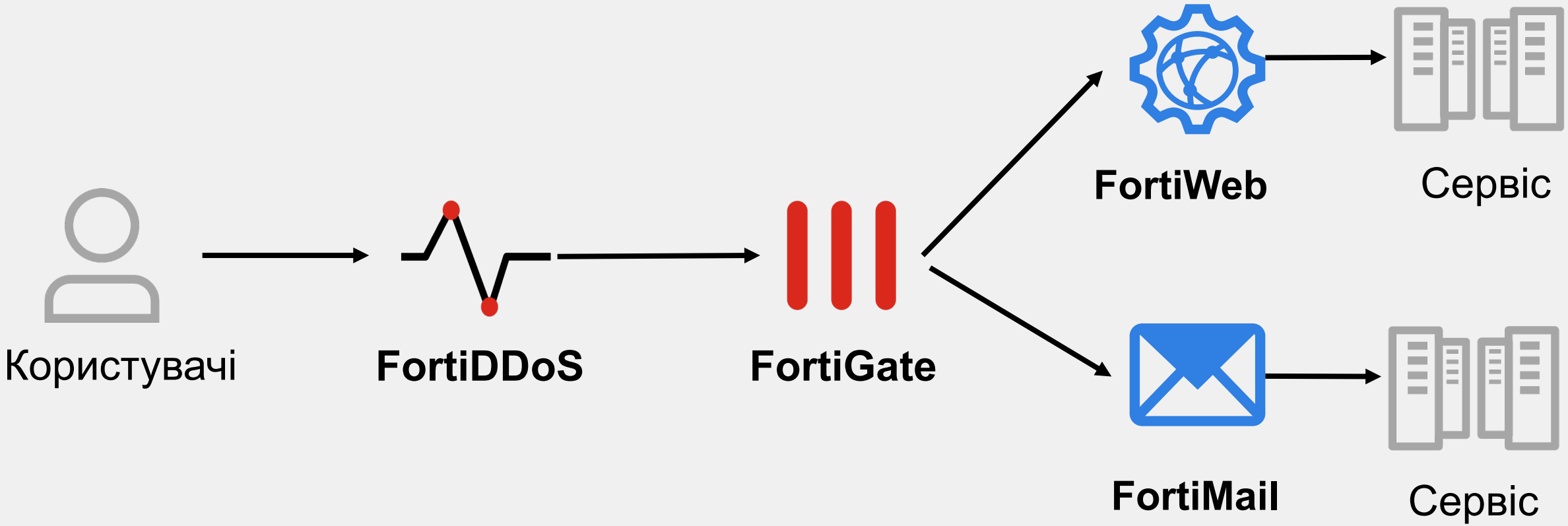
Захист пошти. Office 365 та Google



© Fortinet Inc. All Rights Reserved.

Архітектура 3.

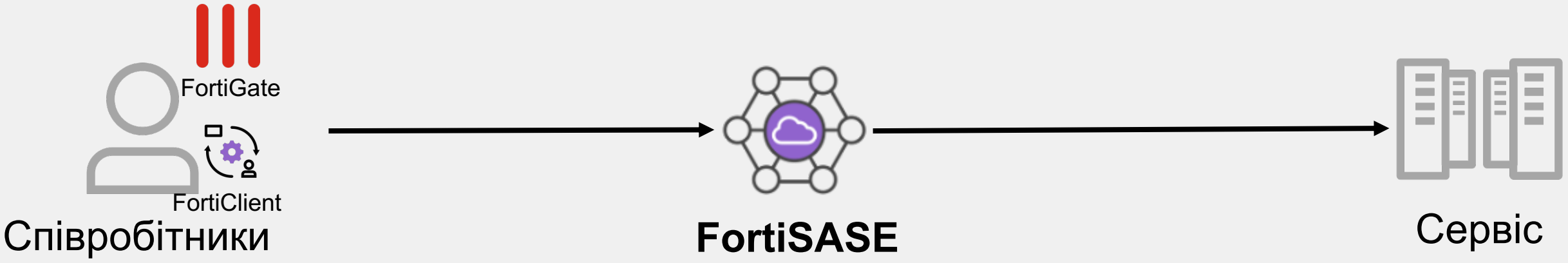
Якщо «в хмари» неможна



© Fortinet Inc. All Rights Reserved.

Архітектура 4.

Внутрішні сервіси для віддалених співробітників



© Fortinet Inc. All Rights Reserved.

Дякую за увагу!