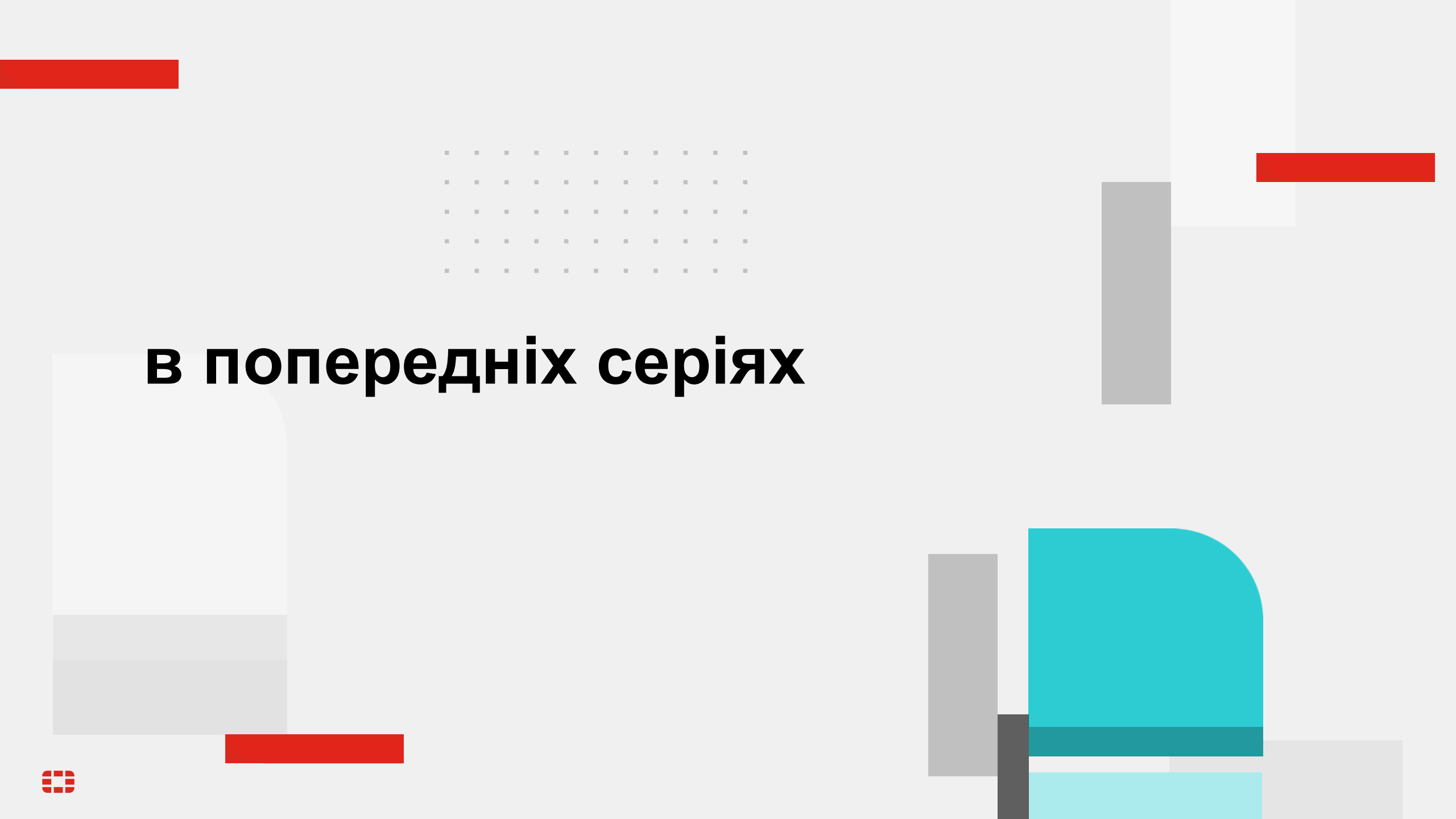




Покращення продуктивності та доступності додатків за допомогою FortiADC

Євгеній Таран, Systems Engineer

ytaran@fortinet.com



в попередніх серіях

Таран Євгеній

- 15 років в IT
- останні 8 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

P.S. Це моя друга кібервійна...



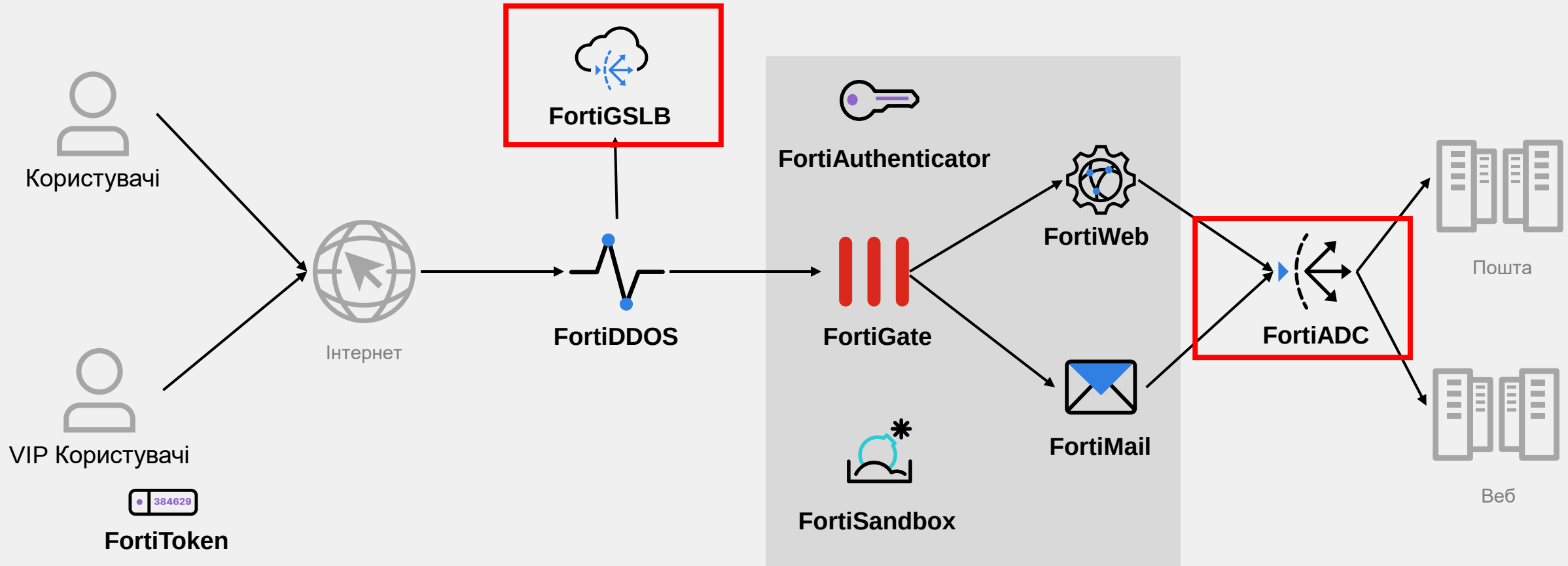
Гібридні мережі



Сучасні реалії

- Додатки різних типів
- Співробітники працюють звідусіль
- Непідконтрольні власні пристрої співробітників
- Все більше різних пристроїв
- Автоматизовані атаки
- Багато виробників
- Брак спеціалістів

ADC як засіб публікації сервісу





ADC для інженерів та бізнесу

3 проблеми з сервісами

- Безпека
- Доступність
- Швидкодія



Звідки вони з'являються?

Проблема



Agile Dev
CI/CD Pipeline

Рішення



Динамічне керування
сервісами

Проблема



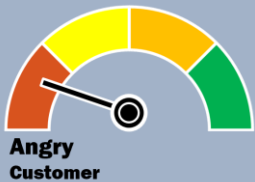
Збої сервісу

Рішення



Global Server
Load Balancing

Проблема



Швидкодія сервісів

Рішення



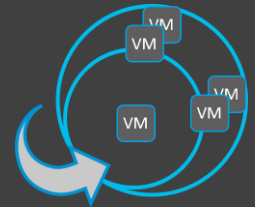
Механізми прискорення роботи

Проблема

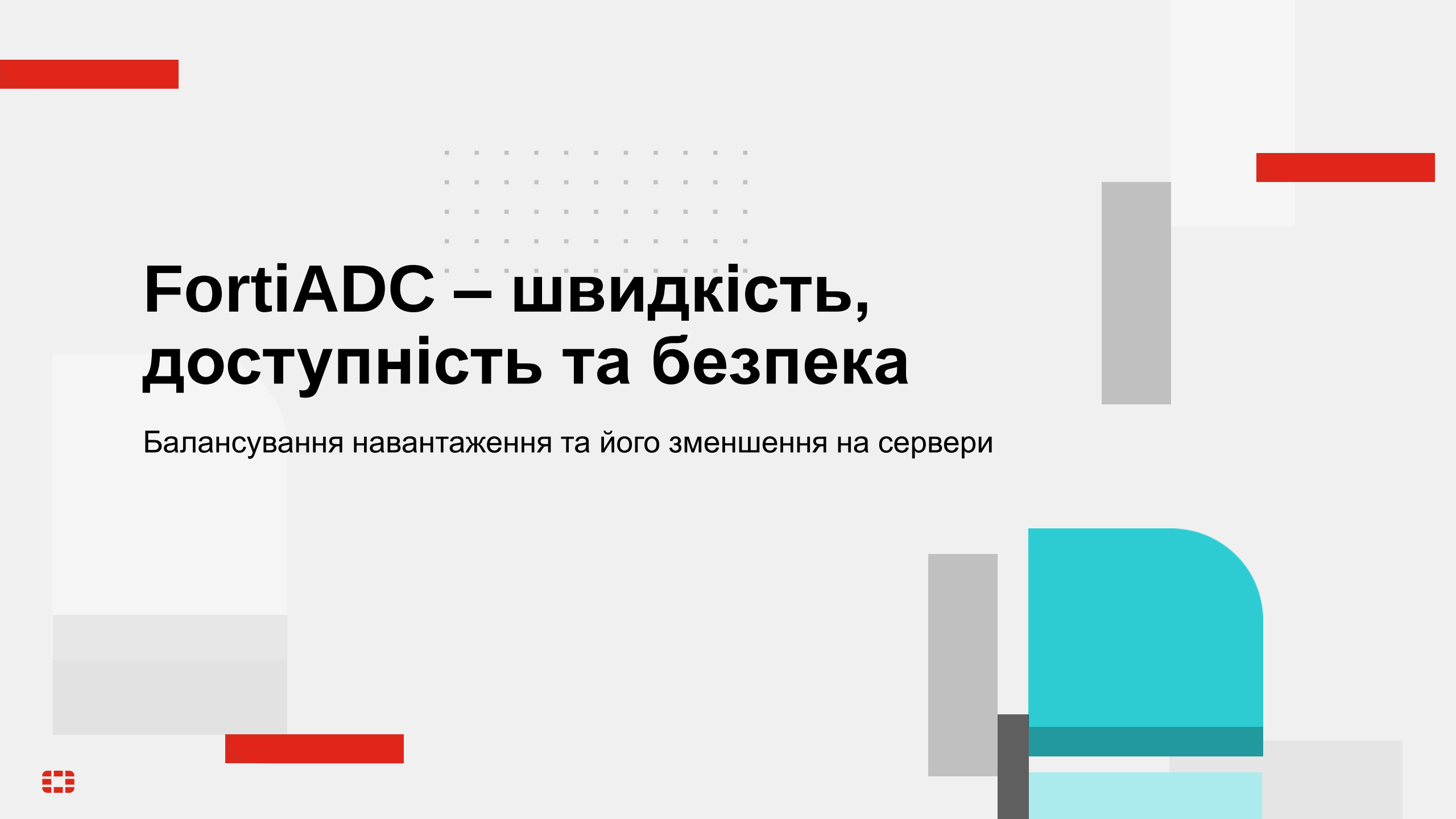


Зміна масштабу бізнесу

Рішення



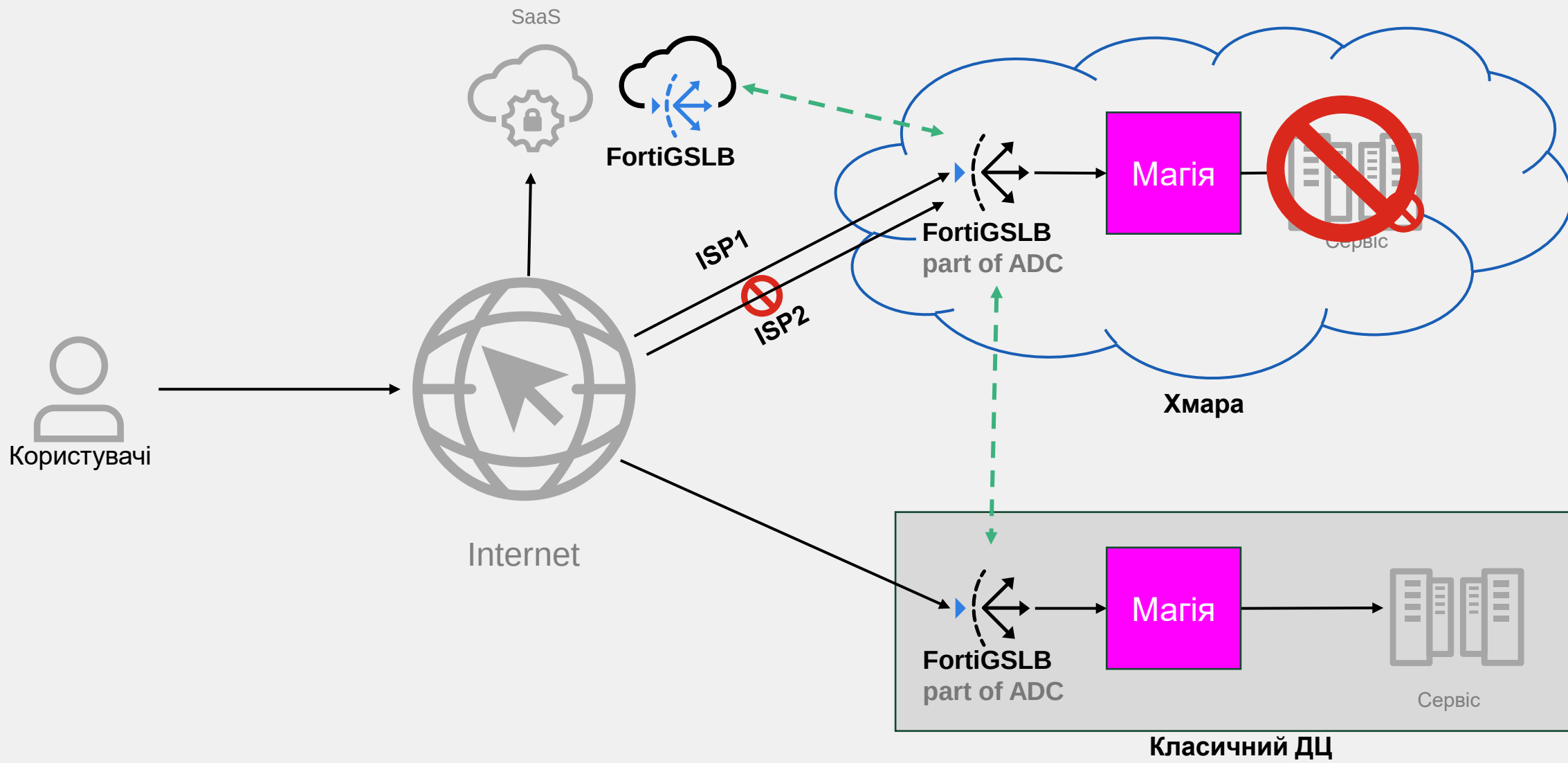
Динамічне масштабування



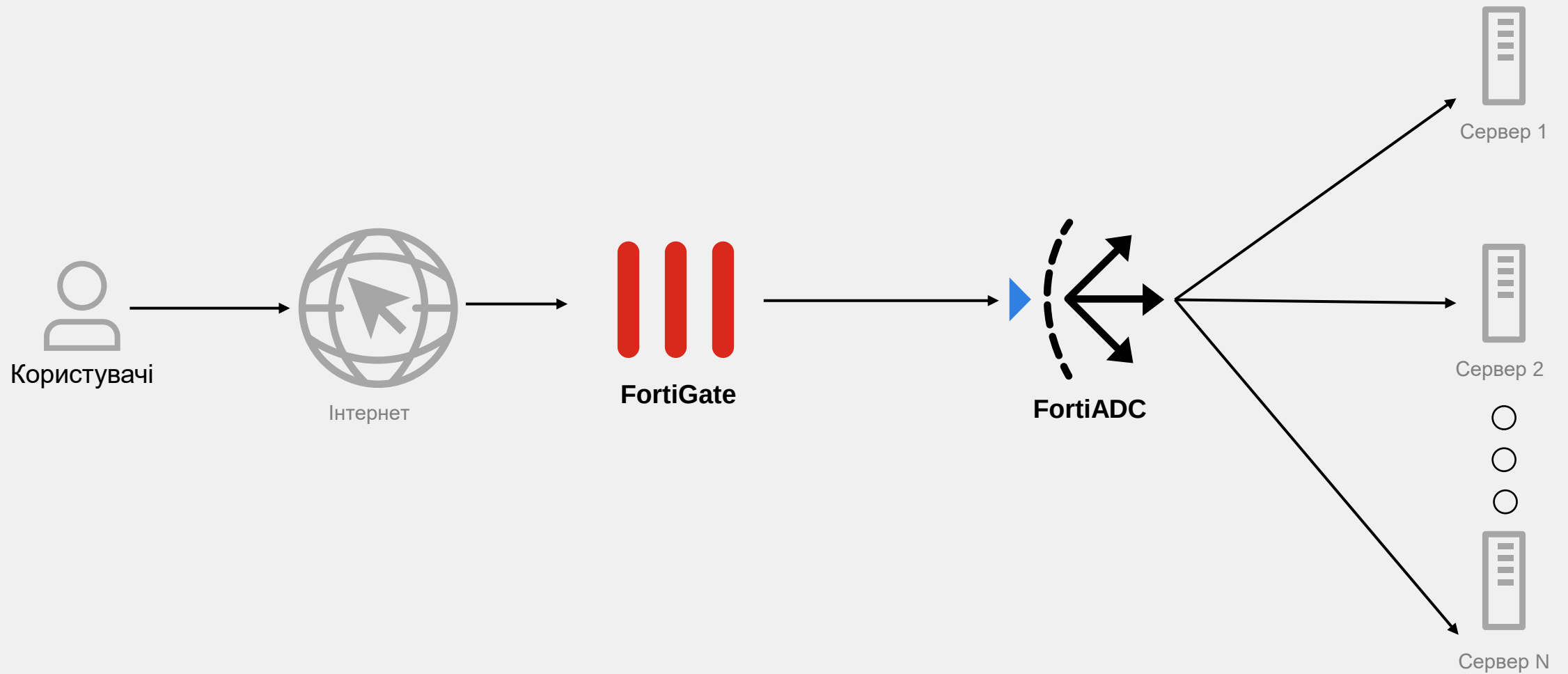
FortiADC – швидкість, доступність та безпека

Балансування навантаження та його зменшення на сервери

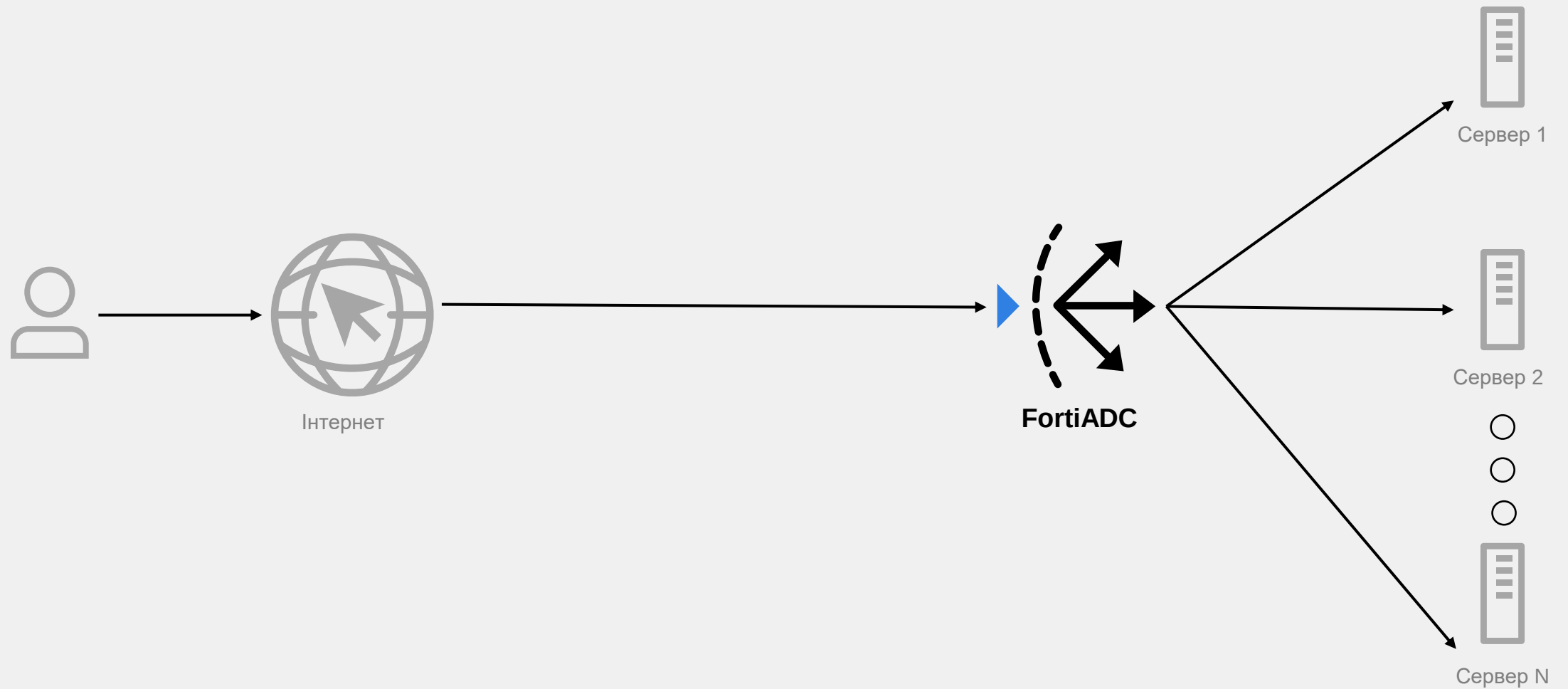
Міждатацентрове балансування



Балансування в рамках ДЦ



Балансування в рамках ДЦ



Основи розподілення навантаження

1. Алгоритм балансування
2. Прив'язка сесій до серверу/ДЦ
3. Перевірка працездатності сервісу



FortiADC SSL Proxy

Розшифровка SSL-трафіку

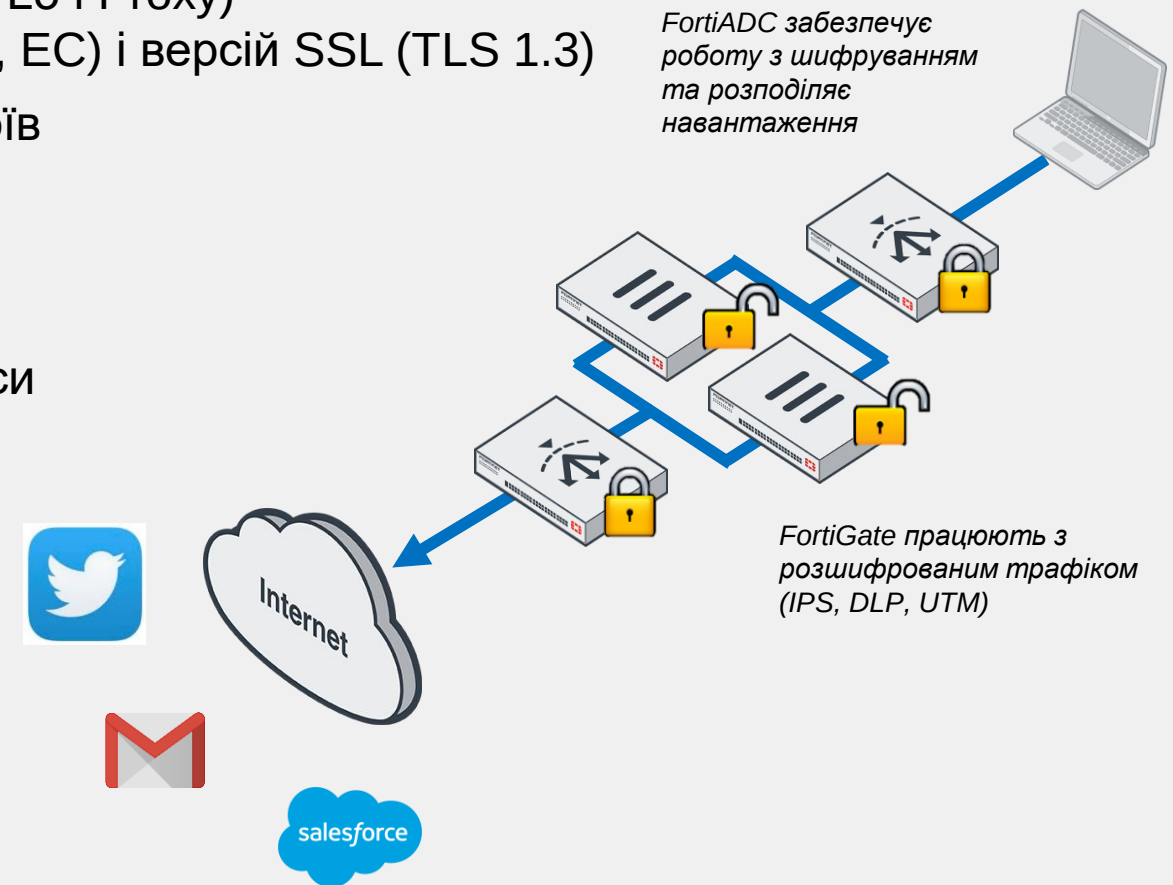
- Підтримка всіх режимів розгортання (прозорий L2-L3 і Proxy)
Підтримка декількох SSL-сертифікатів (DHE, RSA, EC) і версій SSL (TLS 1.3)
- Розвантаження FortiGate або аналогічних пристроїв

SSL Offload

- Менше навантаження на сервери = швидші сервіси
- Апаратна розшифровка з використанням ASIC
- Підтримка HSM

Сервіси без збоїв + обслуговування в бізнес час

- Робота бізнесу 24x7
- Зміна масштабу сервісів
- Інженери працюють в робочий час ☺



Дзеркалювання розшифрованого трафіку

HTTP/S & TCP/S ДЗЕРКАЛЮВАННЯ



МОЖЛИВОСТІ

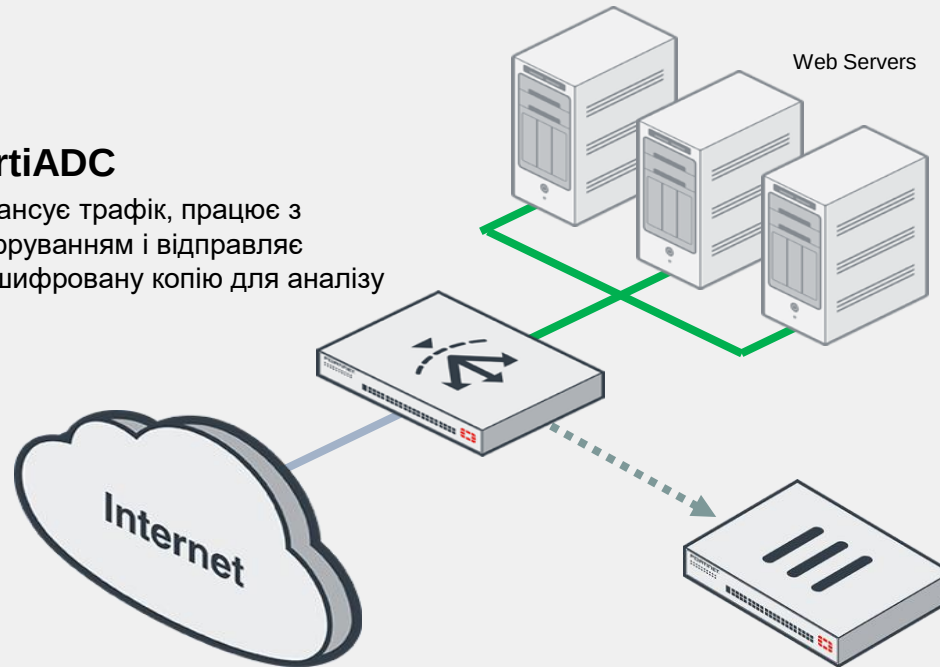
- Дзеркалювання HTTP/S та TCP/S трафіку на виділений інтерфейс
- Підтримка IPv4 та IPv6

РЕЗУЛЬТАТИ

- Виділений пристрій для роботи з SSL
- Відправка даних на аналітичні пристрої
- Економія на пристроях безпеки та покращена безпека

FortiADC

Балансує трафік, працює з шифруванням і відправляє розшифровану копію для аналізу



HTTP/чистий

шифрований

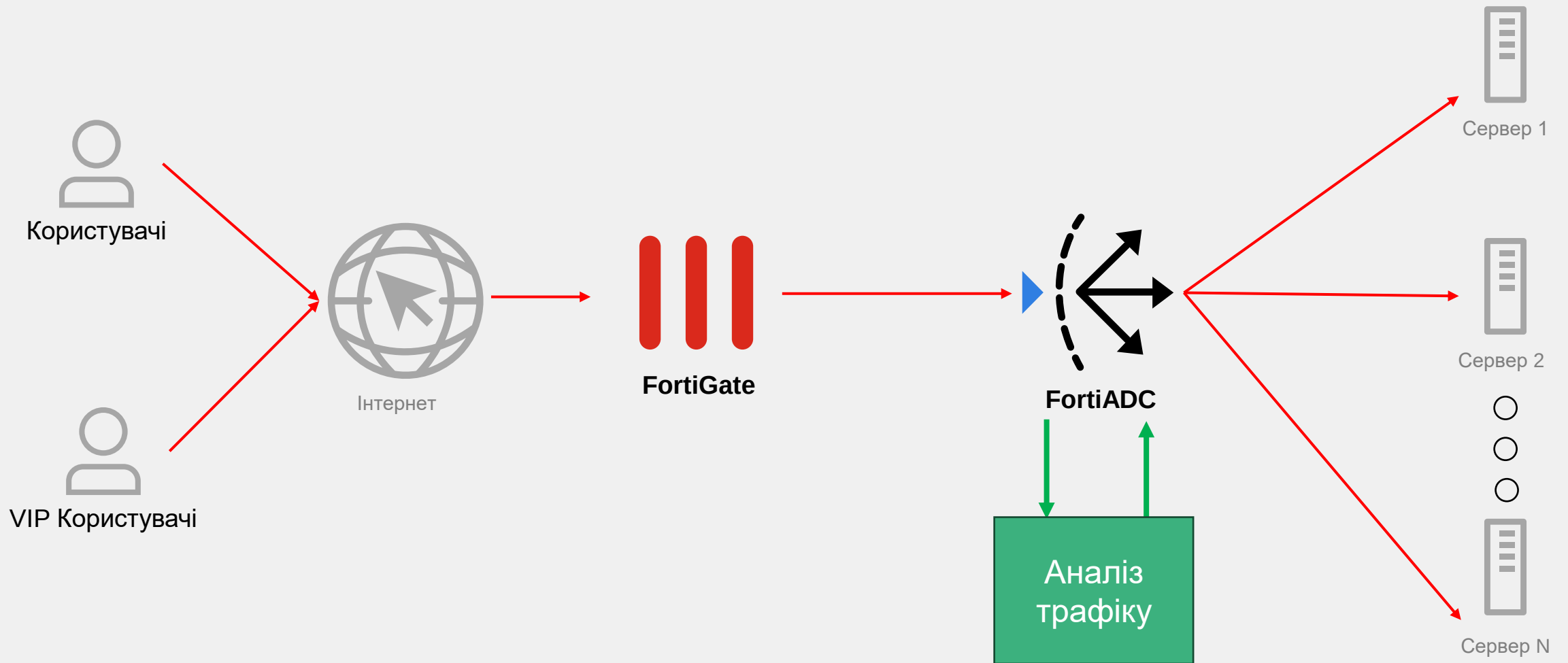
нешифрований

FortiGate

Шукає загрози в режимі
сніферу

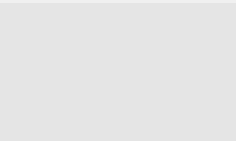
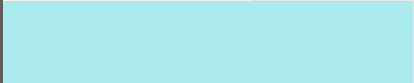
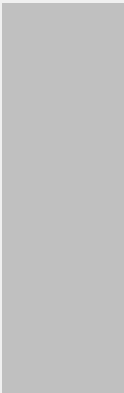
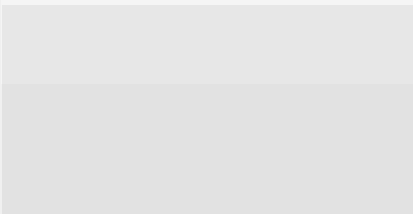
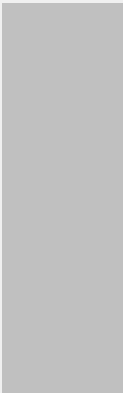


SSLi режим*



*з версії 7.4

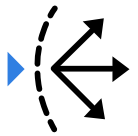
<https://docs.fortinet.com/document/fortiadc/7.4.0/ssli-deployment-guide/545986/introduction>



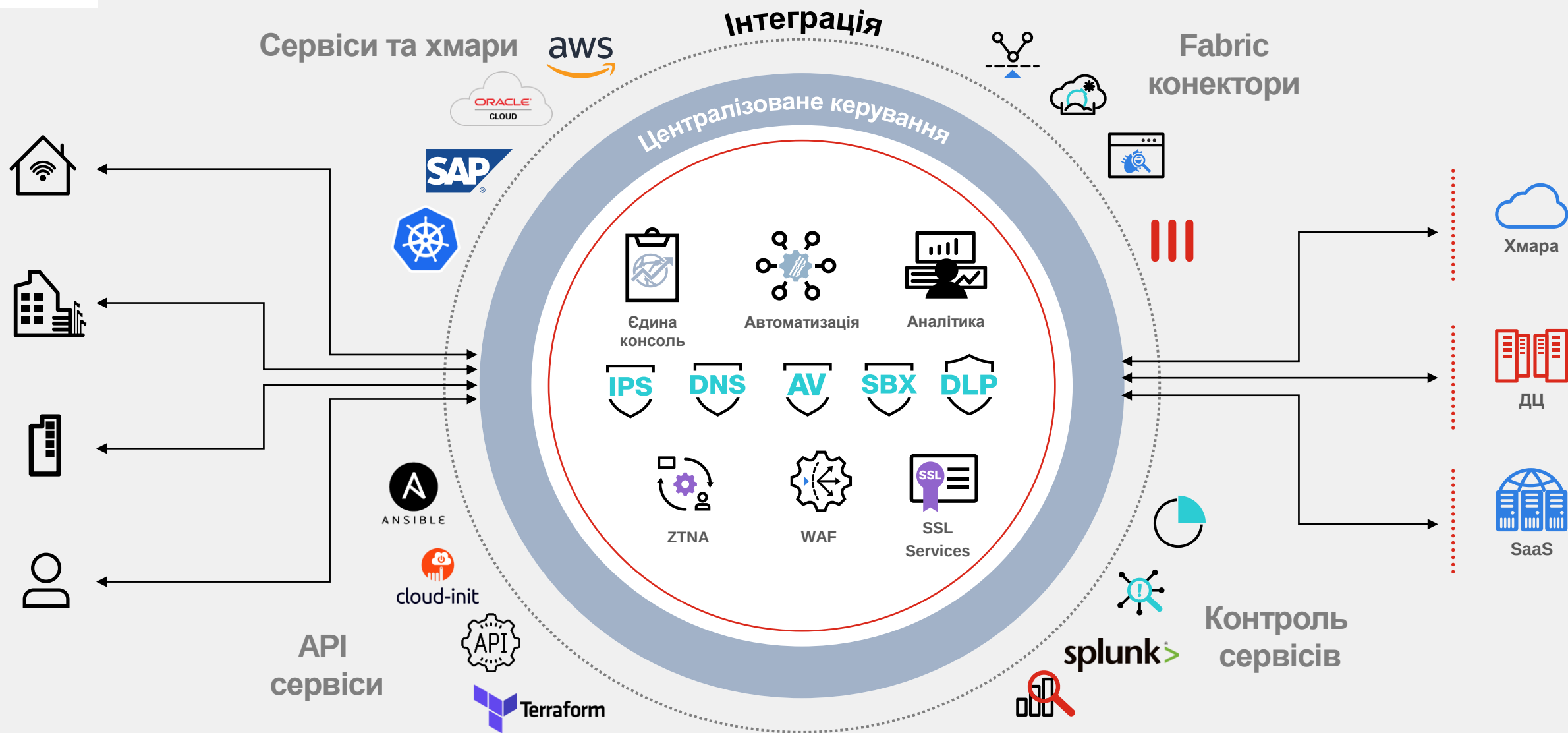
FortiADC в деталях

Формфактори та ліцензування





FortiADC



Публікація додатків з Fortinet

Балансування сервісу Автоматизація



Динамічна публікація
сервісів

Auto-scaling сервісу

Видимість

Доступність

GLSB в пару кліків

Масштаб Продуктивність



Робота з шифрованим трафіком

Висока
швидкодія

Балансування
FortiGate

Різні формфактори

“Always-on”
Security

Покращений
QoE

Інтеграція з Fortinet Fabric



Дії на основі метрик

Автоматизація сервісу

Покращена робота сервісів в
SD-WAN

WAN
оптимізація

Безперервність



Форм фактори



Бажаємо повний контроль

Рішення для організацій, які віддають перевагу повному контролю та управлінню над ADC



Пристрої

- Від 3Gbps до 250Gbps
- Апаратні ASICs
- Підтримка 100GE

FORTINET



Віртуальні машини

- 6 VM моделей
- Ліцензування на основі vCPU
- Підписка

vmware®

Hyper-V

CITRIX®
XenServer

KVM



Хмара

- 5 моделей
- Підтримка BYOL/PAYG
- Готові шаблони розгортання

aws

Azure

Google Cloud

ORACLE
CLOUD



Alibaba Cloud



Бажаємо готовий сервіс

Рішення для організацій, яким потрібен GSLB як готовий сервіс



GSLB SaaS

- За інфраструктуру відповідає Fortinet
- Ліцензування на основі QPS та Health-Checks
- Балансування для сервісів та VPN



FortiGuard Services для FortiADC



WAF Security Service

- Application layer signatures
- Web Application signature to prevent any web attack



IP Reputation

- Protection for automated attacks and malicious sources
- DDoS, Phishing, Botnet, Spam, Anonymous proxies and infected sources



Антивірус та IPS

- Scan file uploads
- Regular and extended AV databases
- Protect the network against exploitable vulnerabilities



FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Subscription-based
- No separate sandbox required



Credential stuffing Defense

- Identifies login attempts using stolen credentials from numerous sources
- Automatic updates
- Prevents unwanted access and defends against data breaches



Web Filtering

- Manage SSL FP scanning exceptions
- Enable/disable SSL inspection by category
- Automatic updates

STANDARD BUNDLE

ADVANCED BUNDLE

FortiGSLB Cloud



- AWS, Azure, GCP та OCI
- Найпопулярніший варіант в Україні - BYOL

The screenshot displays three overlapping web browser windows illustrating cloud marketplace interfaces:

- Google Cloud Marketplace:** Shows the Google Cloud logo and a sidebar with navigation links like 'Marketplace home', 'Your products', and 'Your orders'. A search bar is visible.
- Azure Marketplace:** Shows the Microsoft Azure Marketplace interface. The search results for 'Fortinet FortiADC Application Delivery...' are displayed, including a 'Get it now' button and a 'Bring your own license' option.
- AWS Marketplace:** Shows the AWS Marketplace interface. The search results for 'fortiadc' are displayed, including filters for Publisher (Fortinet Inc., Exaprobe, Joy Comm, KINMAX TECHNOLOGY INC.), Pricing model (Upfront Commitment, Usage Based, Bring Your Own License), and Operating system (All Linux/Unix).



FortiGSLB Cloud як Сервіс

The screenshot displays the FortiCloud dashboard interface. The browser address bar shows the URL <https://support.fortinet.com/asset/#/dashboard>. The dashboard header includes the FortiCloud logo, navigation links for Services and Support, a search icon, a notification bell, and the user email ytaran@fo.

The main content area is divided into three sections:

- ASSET MANAGEMENT** (Left sidebar):
 - Dashboard
 - Products
 - Marketplace
 - Account Services
- ASSETS & ACCOUNTS** (Top middle):
 - Asset Management
 - FortiFlex
 - IAM
- CLOUD MANAGEMENT** (Bottom middle):
 - FortiClient EMS Cloud
 - FortiManager Cloud
 - FortiLAN Cloud
 - FortiExtender Cloud
 - FortiGate Cloud
 - FortiAnalyzer Cloud
 - FortiSOAR Cloud
 - FortiSIEM Cloud
- CLOUD SERVICES** (Right side):
 - FortiMail
 - FortiMonitor
 - FortiSASE
 - FortiZTP (Beta)
 - FortiSandbox Cloud
 - FortiVoice
 - FortiCASB
 - FortiPresence
 - FortiDAST
 - FortiTrustID
 - FortiGate CNF
 - FortiIPAM
 - OC-VPN Portal
 - Managed FortiGate
 - SOCaaS
 - FortiConverter
 - FortiWeb Cloud
 - FortiRecon
 - FortiToken Cloud
 - FortiCNP
 - FortiGSLB** (highlighted with a red box)
 - FortiPhish
 - FortiDevSec
 - FortiCamera Cloud (Beta)
 - FortiCare Elite (Beta)
 - FortiInsight
 - Overlay as a Service

A "Show Less" link is located at the bottom of the Cloud Services section.

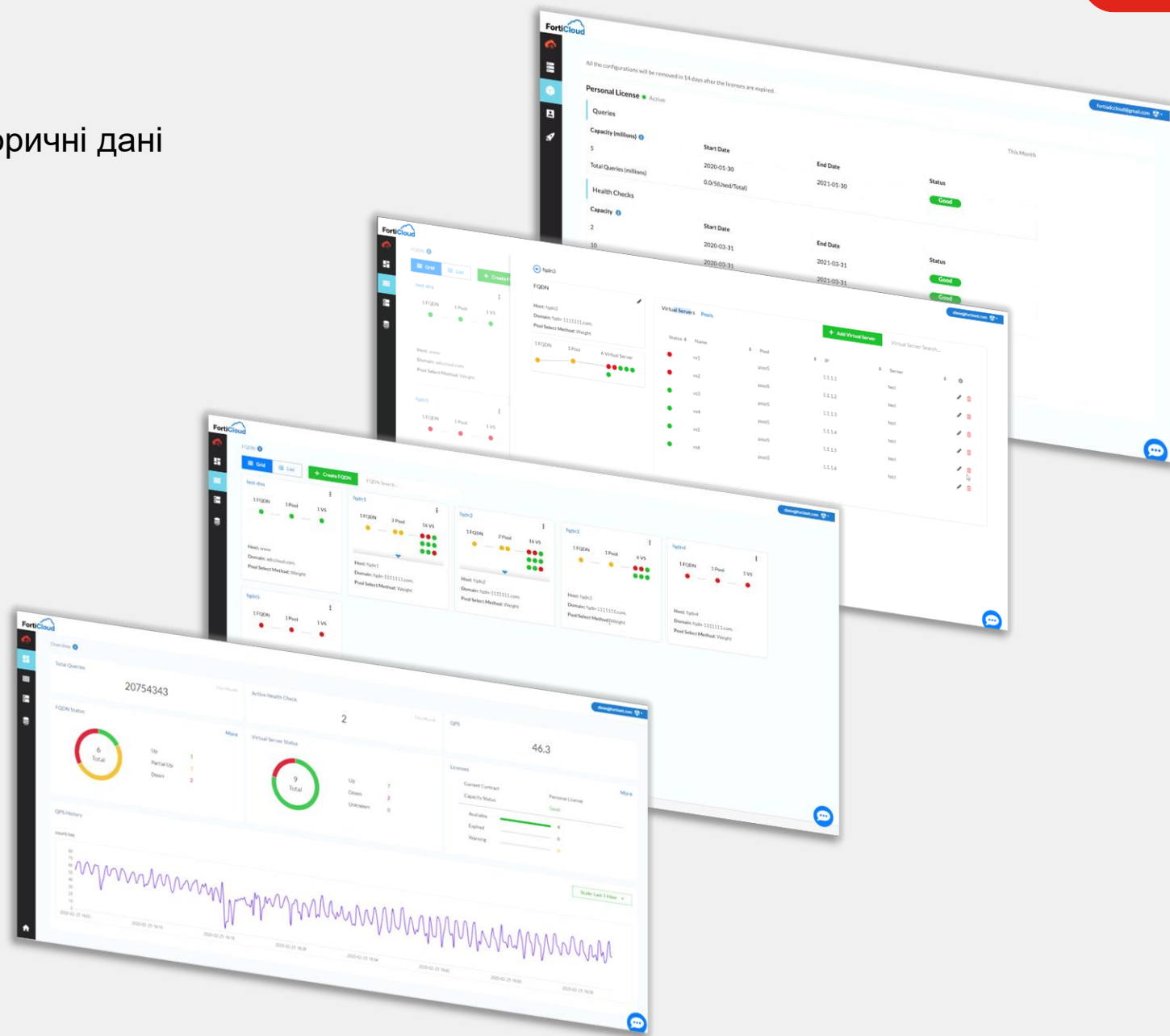


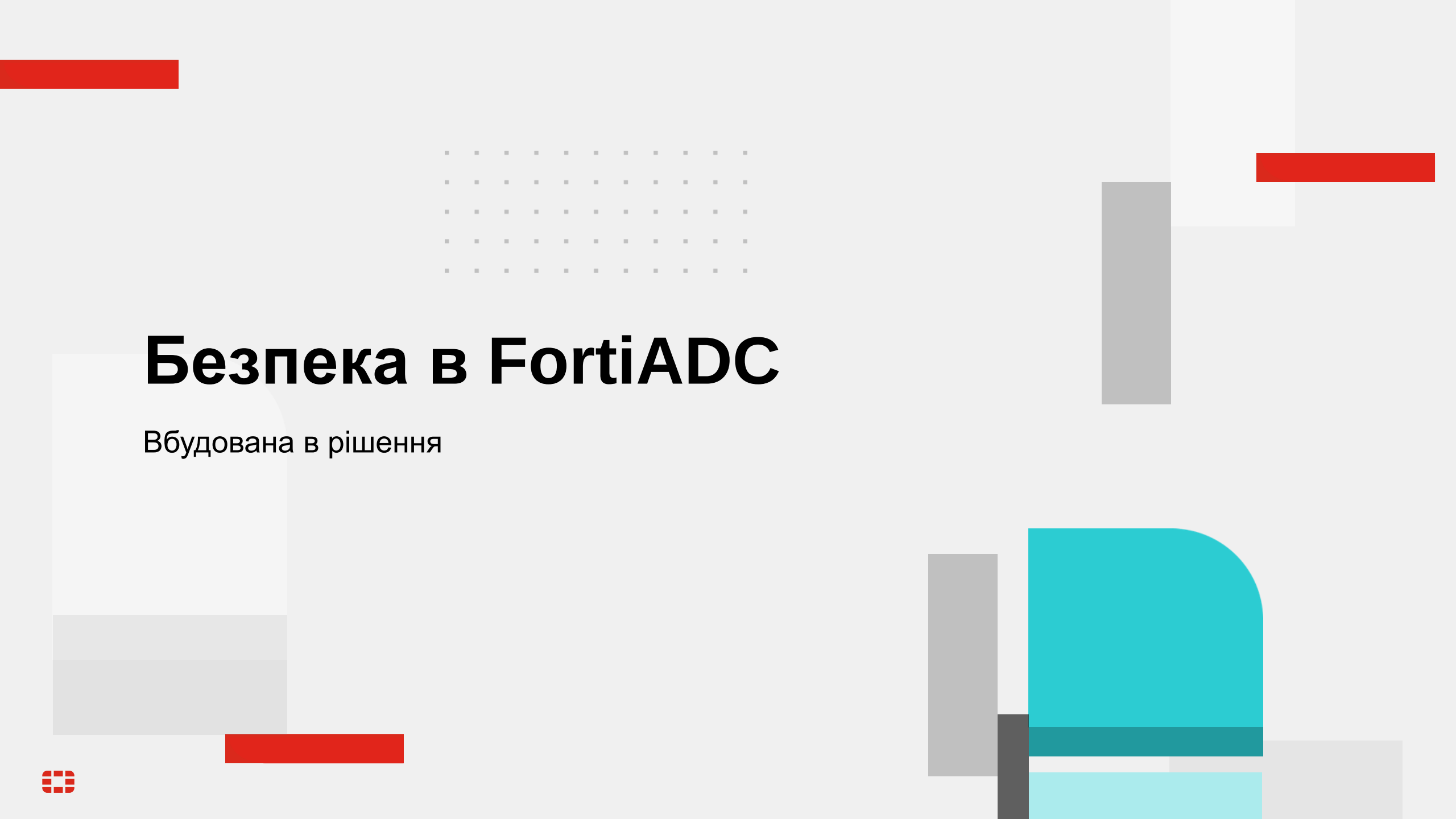
FortiGSLB Cloud WebUI

Забезпечує моніторинг у реальному часі та історичні дані DNS-трафіку

Простота та швидкість:

- » Швидке підключення
- » Готове для холдингів або ж MSP
- » Простий інтерфейс
- » Контроль ліцензій
- » Інформативний головний екран
- » Моніторинг сервісів
- » Історичні дані DNS запитів
- » Вбудована база Geo-IP
- » Підтримка «GSLB в один клік»





Безпека в FortiADC

Вбудована в рішення

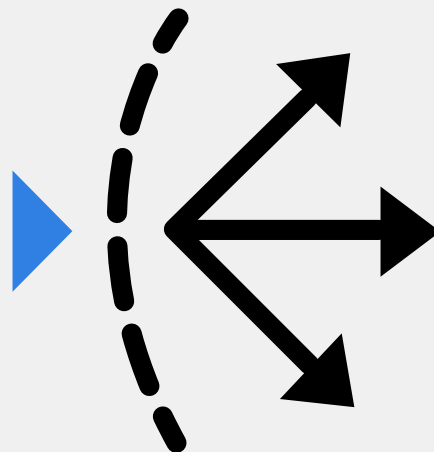


FortiWeb (з попередніх серій)



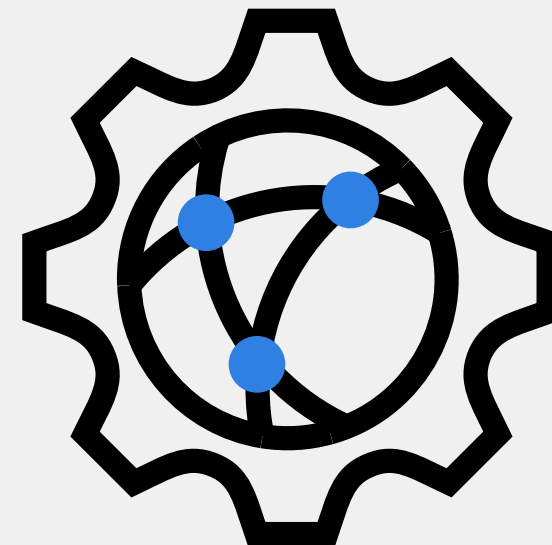
Web Application Firewall

+



Балансувальник
в рамках ДЦ

=



FortiWeb

FortiADC



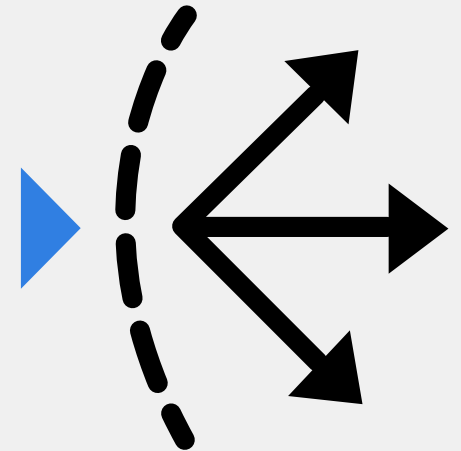
**Балансувальник в
рамках ДЦ та між ДЦ**

+



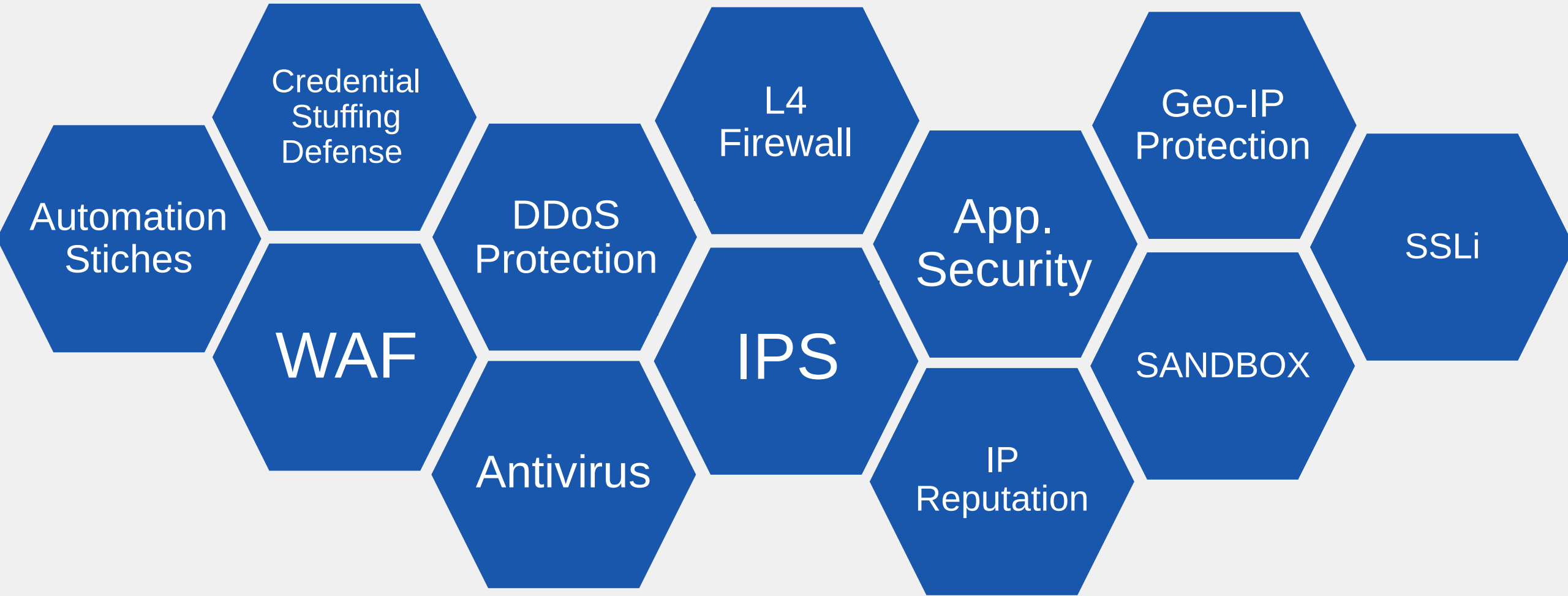
Web Application Firewall

=



FortiADC

FortiADC Security Features



Web Application Firewall

OWASP Top 10 Protection

SQLi/XSS Protection, Web Scraping, Brute Force, Web Defacement, CSRF Protection

Web Vulnerability Scanner

Security Fabric Integration

FortiSandbox & FortiGate

Web Attack Signatures

Protocol Validation

HTTP/S, URL Protection

Input Validation

File Restriction, Hidden Files

API Protection

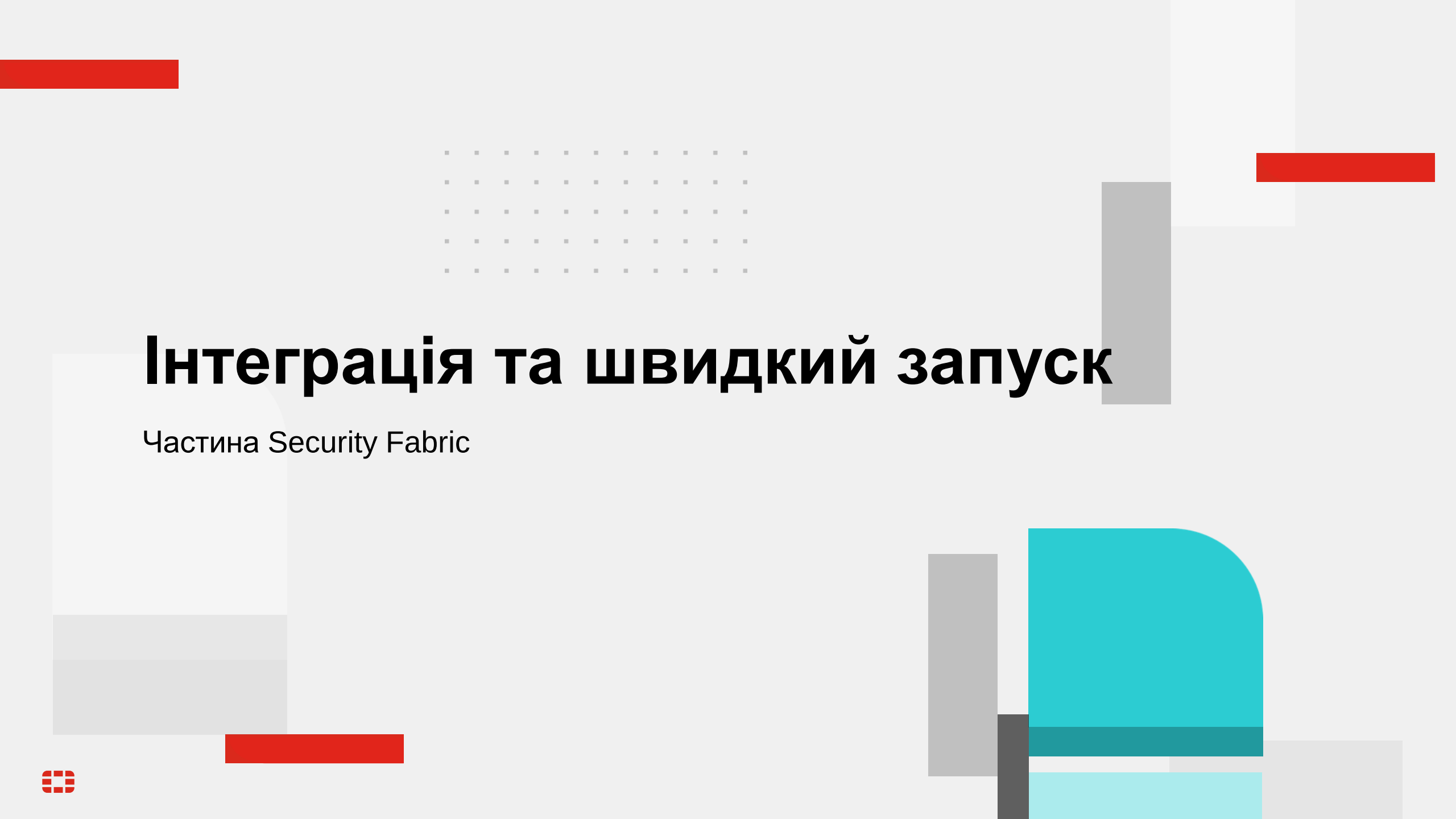
API Gateway, XML, JSON and SOAP validation. OpenAPI validation

Sensitive Data Protection

Cookie Security, DLP

Bot Detection



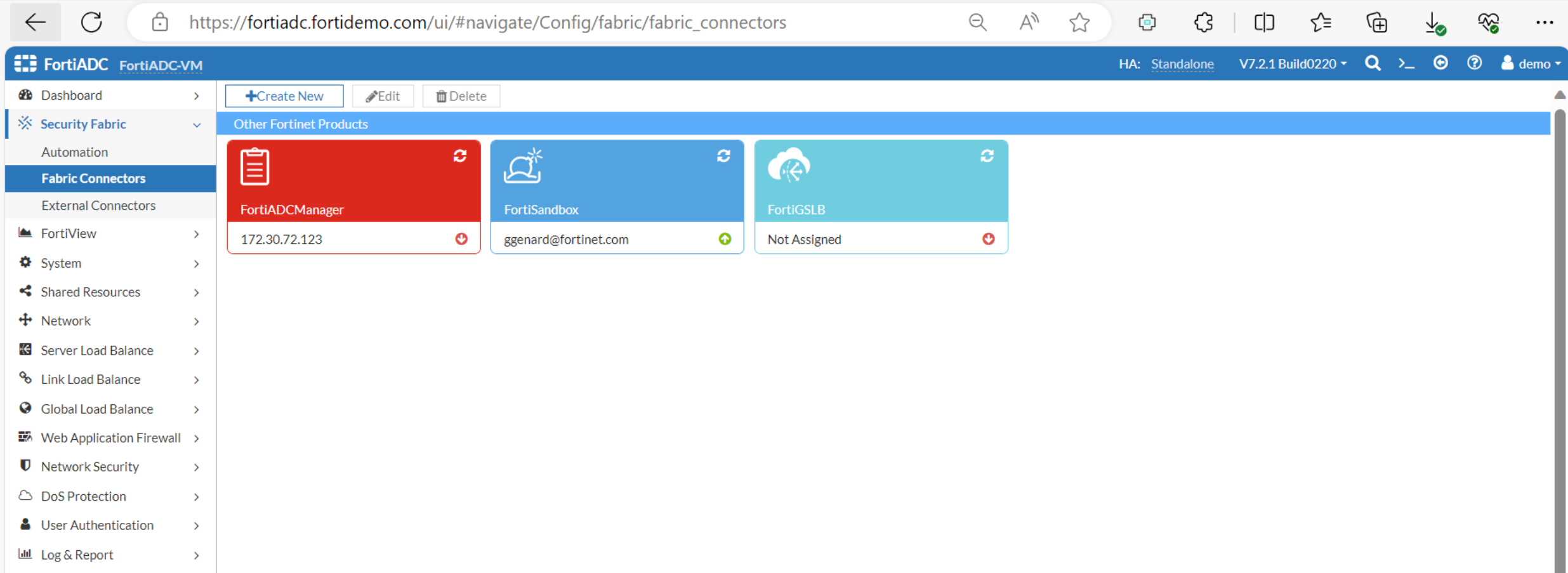


Інтеграція та швидкий запуск

Частина Security Fabric



Інтеграція з іншими компонентами



Інтеграція з іншими компонентами

FortiADC FortiADC-VM

HA: Standalone V7.2.1 Build0220

demo

Dashboard

Security Fabric

Automation

Fabric Connectors

External Connectors

FortiView

System

Shared Resources

Network

Server Load Balance

Link Load Balance

Global Load Balance

Web Application Firewall

Network Security

DoS Protection

User Authentication

Log & Report

New Fabric Connector

Core Network Security



FortiClient EMS

Other Fortinet Products



FortiSIEM



FortiAnalyzer

Return



Інтеграція з іншими компонентами

← ↻ 🔒 https://fortiadc.fortidemo.com/ui/#navigate/Config/fabric/external_connectors 🔍 A ☆ 🖨 ⚙ | 📄 ☆ 📌 ⬇️ 🔄 ⋮

FortiADC FortiADC-VM HA: Standalone V7.2.1 Build0220 🔍 > ⌂ ? demo ▾

- Dashboard >
- Security Fabric ▾
 - Automation
 - Fabric Connectors
- External Connectors**
- FortiView >
- System >
- Shared Resources >
- Network >
- Server Load Balance >
- Link Load Balance >
- Global Load Balance >
- Web Application Firewall >
- Network Security >
- DoS Protection >
- User Authentication >
- Log & Report >

New External Connector

Public SDN

-  Amazon Web Services (AWS)
-  Oracle Cloud Infrastructure (OCI)

Private SDN

-  Kubernetes
-  Splunk
-  SAP

Authentication

-  FortiAuthenticator (FAC)

Threat Feeds

-  IP Address



Найрозповсюдженіша автоматизація з FortiGate

- FortiADC детектує IP що атакує додаток (SQLi, XSS тощо);
- За допомогою автоматизація FortiADC дає команду FortiGate заблокувати IP;
- Шкідливий IP блокується периметральним пристроєм для економії ресурсів FortiADC/FortiWeb для L7 задач;

New Automation Stitch

Name

Status Disable Enable

Trigger

 Period Block IP

Fetch FortiADC Source IP addresses from Period Block list

Action

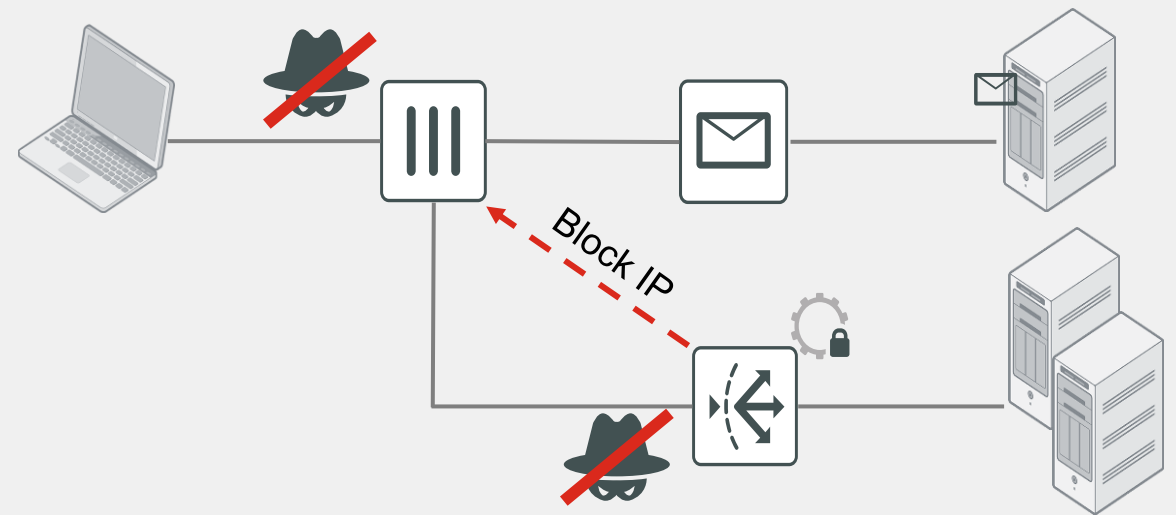
 Email

 Syslog

 SNMP Trap

 Webhook

 FortiGate IP Ban



Скрипти

←

↺

🔒 https://fortiadc.fortidemo.com/ui/#navigate/Config/slb/scripting

🔍

A

☆

🖨

⚙

|

📄

☰

🔗

↓

🔄

⋮

FortiADC FortiADC-VM

HA: Standalone V7.2.1 Build0220 🔍 >_ 🔄 ? demo ▾

Dashboard >

Security Fabric >

FortiView >

System >

Shared Resources >

Network >

Server Load Balance ▾

Virtual Server

Application Resources

Application Optimization

Real Server Pool

Scripting

SSL-FP Resources

Link Load Balance >

Global Load Balance >

Web Application Firewall >

Network Security >

DoS Protection >

User Authentication >

Log & Report >

HTTP

Name HTTP_DATA_FIND_REMOVE_REPLACE_DEMO

```
1 when HTTP_REQUEST{
2   --HTTP:collect command can be used in both HTTP_REQUEST
3   --and HTTP_RESPONSE events
4   --size is optional, otherwise, it will collect up to the full length
5   --or when 1.25M is reached
6
7   t={};
8   t["size"] = 100;
9   HTTP:collect(t)
10 }
11 when HTTP_DATA_REQUEST{
12
13   --check the size of the content
14   t={};
15   t["operation"]="size";
16   sz=HTTP:payload(t);
17   debug("content size: %s\n", sz);
18
19   --find a string or a regular expression in the buffered data
20   --offset, size and scope are optional, if scope is missing, "all" is assumed
21   t={};
22   t["operation"]="find";
```

Cancel



Висновки



- Балансувальник для будь яких задач
- Пришвидшує роботу сервісів без їх зміни та зменшує навантаження
- Забезпечує безпеку сервісів
- Наявність антивірусу для файлів
- Проста автоматизація
- Скрипти для нестандартних задач
- Форм фактори на будь який смак

Вирішення проблеми доступності та швидкодії сервісів
а не тільки безпеки



для бізнесу і інженерів