FORTINET

Security Day

September 15th 2025
12:30 – 12:50 pm
Athens, Greece

InTTrust

FORTINET Security Day

ENGAGE
FORTINET ADVANCED PARTNER
Integrator, MSSP, Marketplace

InTTrust

Fortifying the Future

Defending the Banking Sector Against DDoS Threats

Manos Kokolakis, MSc
Customer Success Manager
mkokolakis@inttrust.gr

Distributed Denial of Service

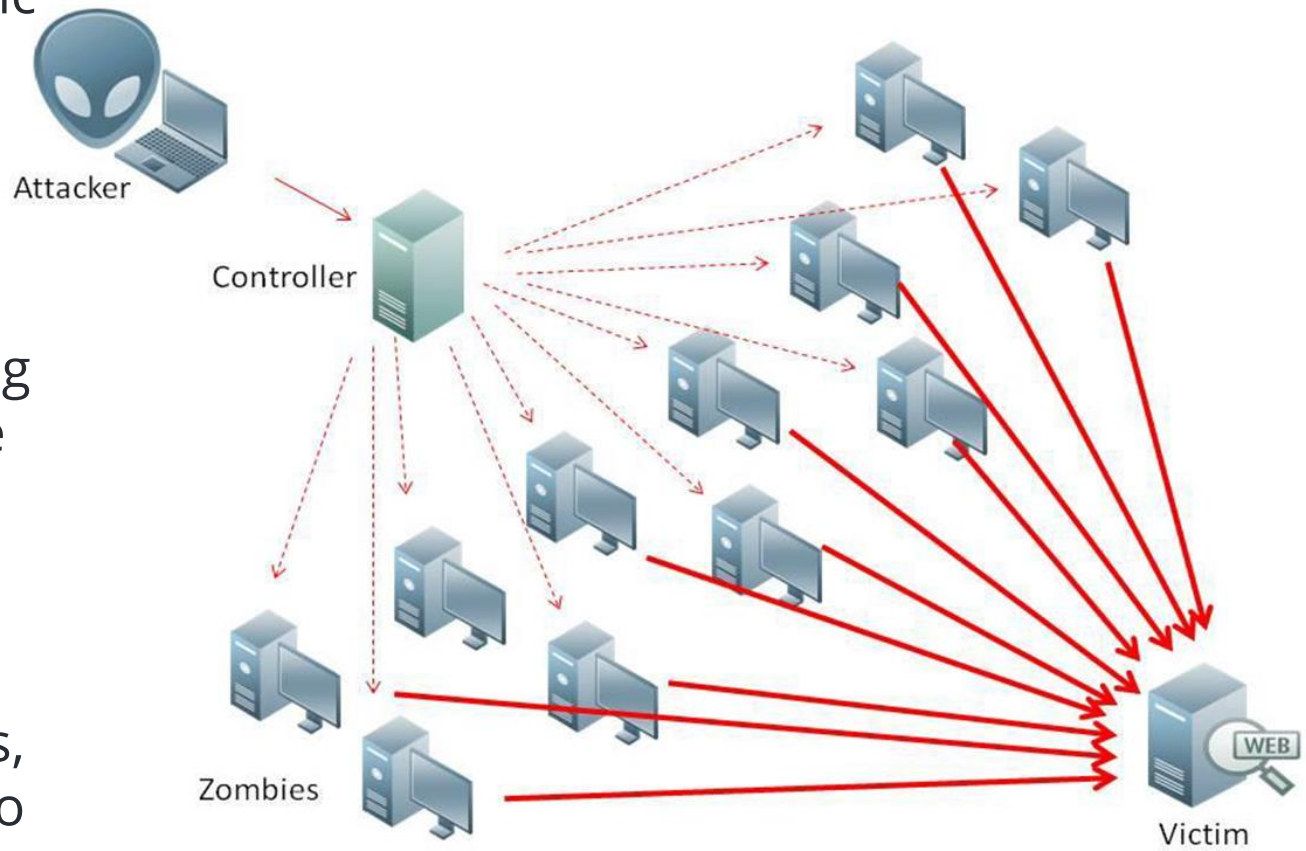
DoS or DDoS attacks

Denial-of-service is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network, typically accomplished *by flooding the targeted machine* or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

- **Sep 1996**, **Panix**, SYN flood attack
- **Feb 2000** “Mafiaboy” **Yahoo** shutdown for an hour and weeks later other corporations such as **CNN**, **Amazon**, **Dell**, **eBay**, **FIFA**.
- **Sep 2017**, **Google Cloud** attack peak volume of 2.54 Tb/s
- **July 2021**, Cloudflare boasted of protecting its client from a DDoS attack up to 17.2 million requests per second
- **Feb 2023**, Cloudflare faced a 71 million/requests per second
- **Aug 2023**, hacktivists NoName057 targeted several Italian financial institutions.
- **Oct 2023**, largest HTTP DDoS attack being broken twice, once with a 201 million requests per second reported by Cloudflare, and with a 398 million requests per second attack reported by Google
- **Jan 2024**, a DDoS attack by NoName057 on Swiss federal websites, on Zelensky’s visit at the Davos World Economic Forum.
- **Aug 2024**, DDoS at 3.15 billion packets per second, targeted an undisclosed number of unofficial Minecraft game servers.

DDoS attack types

- Volumetric
  Employ massive amounts of malicious traffic to overwhelm a server with so much traffic that it eventually exhausts all available bandwidth.
- TCP State-Exhaustion
  Focus on taking down services or underlying network infrastructure which is responsible for delivering content to the end users.
- Application Layer
  Designed to attack a specific application, focusing on specific vulnerabilities or issues, resulting in the application not being able to deliver content to the user.



Forti DDoS proposal

Evolving Threats

Traditional Attacks

Bulk Volumetric attacks

Tactics:

- Layer 3 and 4
- Bulk volumetric
- Spoofing IP addresses
- Large attacks

L7

Today and Future

Targeted Application Layer attacks

Tactics:

- Service Layer 7 focus
- Small, targeted attacks
- Blended 3/4/7 approaches
- Mimicking the behavior of a large number of clients

A New Approach

Modern attacks target all cloud infrastructure elements including firewalls, mail, and web servers

Defense:

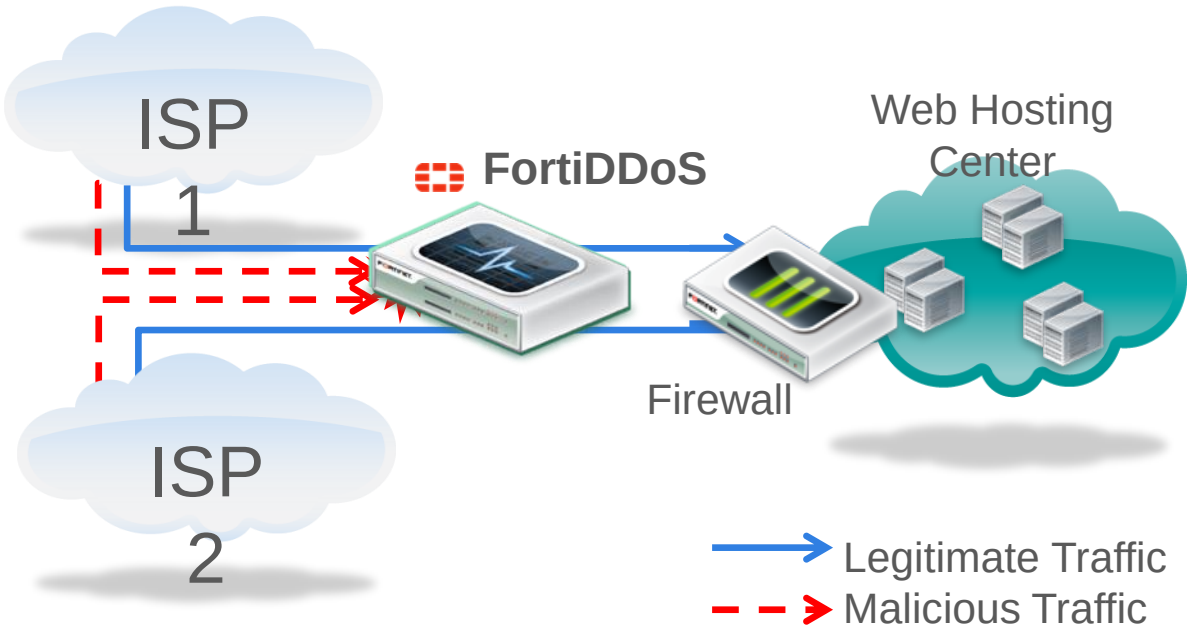
- Behavioral detection
- Service and port monitoring
- Detect any attack size
- Hardware assisted
- Automatic mitigation

FortiDDoS

Appliance

Hardware Accelerated DDoS Intent Based Defense

- (SPU)-based layer 3, 4, and 7 DDoS protection
- Behavior-based DDoS protection to eliminate need for signature files
- Minimal false-positive detections through continuous threat evaluation
- Ability to monitor enormous parameters simultaneously
- Advanced defense against bulk volumetric, layer 7 applications
- Attack protection for DNS services via specialized tools



Features and Benefits

Fully Autonomous Mitigation. During attacks, no user intervention is required. Also, no additional subscriptions are required

Expansive Monitoring. 230,000 parameters are simultaneously monitored to stop zero-day attacks

100% PACKET INSPECTION. All mitigations take place in less than one second. No sampling

HIGH SMALL-PACKET INSPECTION. 77 Mpps small-packet inspection ensures detection and network performance

ADVANCED LAYERS 4 AND 7 MITIGATION. TCP flag, DNS, NTP, DTLS, QUIC direct/reflected attacks are mitigated from the first packet

UNMATCHED UDP REFLECTION MITIGATION. More than 10,000 possible UDP Reflection ports are monitored

InTTrust

Customer Case

The Problem …

Lately financial sector is the top industry for volumetric DDoS attacks.

Banks operating in a highly **regulated** and **demanding** environment, face increased threats of DDoS attacks on critical **digital services**, such as e-banking, mobile banking, POS transactions, Partner APIs and more.

Financial Sector is a **High-Value Target** with **Increased Attack Surface**. Also interesting for Hactivists and cybercriminals due to Geopolitical factors. Additionally new sophisticated tactics make attacks more powerful, adaptable, and cost-effective.

InTTrust

The Scope ….

To Increase protection & availability of all digital channels and avoid interruption of critical services our customer decided to evolve the current deployment based on the following success criteria

Service Availability

Regulatory compliance

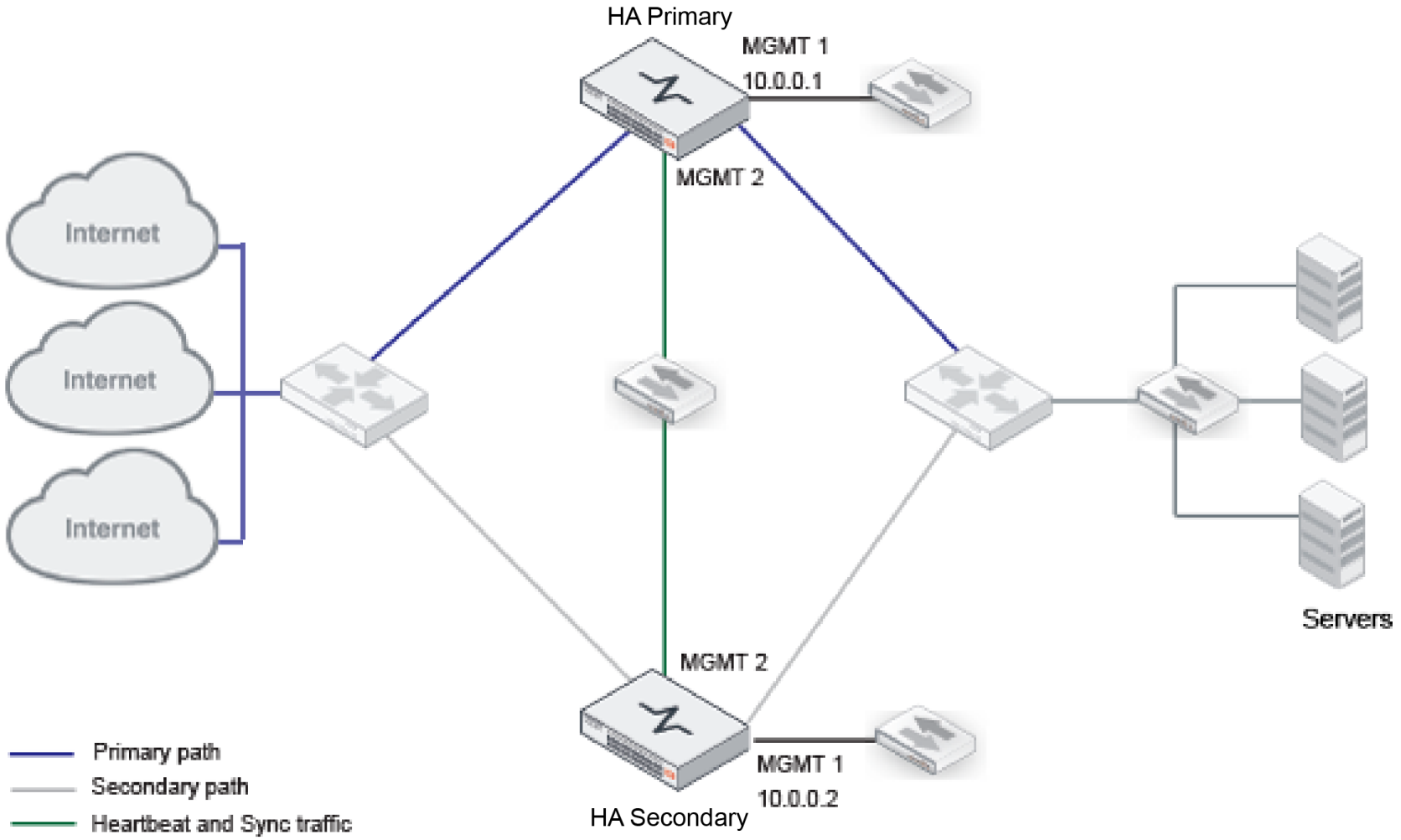
Customer Trust & Corporate Reputation

Defense Independence & Flexibility

Real-Time Response

Business Continuity (BCP/DR)

HA deployment



The Solution …

To meet the requirements, we deployed a solution that would protect all critical digital channels. FortiDDos deployment allowed us to:

- **Protect at all network entry points**. Placing FortiDDoS in both Main and DR DC sites, filtering internet traffic before reaching critical banking applications.
- **Operate in High Availability.** Installation of two nodes with the ability to operate in a pair. In case of failure on primary device, traffic switches to secondary seamlessly.
- **Automated Mitigation**. Automatically mitigate threats and maintain business continuity, requiring no user or vendor intervention during an attack.

The Solution …

- **Collaborate with existing security Infrastructure**. Interconnecting with existing firewalls (FortiGate), as well as with monitoring systems (FortiAnalyzer, SOC), providing unified view and centralized control.
- **Clear Visibility & Reporting.** Provides real-time dashboards and detailed, granular reports to help users understand attack trends and mitigation responses.
- **Autonomous, Behavioral Detection.** Using machine learning can build a baseline of normal traffic and identify deviations, protecting against both known and unknown (zero-day) attacks.
- **Minimal False Positives.** Continuously reevaluating attacks and focusing on deviations from normal behavior, FortiDDoS minimizes the disruption of legitimate traffic.

InTTrust

The Solution …

- **High Performance & Speed.** Industry-leading performance, detecting and mitigating attacks from the first packet and handling high-volume attacks without being overwhelmed.
- **Multi-Service coverage**. Protecting all critical applications and services such as e-banking, mobile banking, card systems, POS transactions, third-party APIs and back-end applications.
- **Comprehensive Attack Coverage**. Able to defend against various types of attacks, including
  - *Volumetric Attacks (Layer 3/4)*
  - *Application Layer Attacks (Layer 7)*
  - *DNS-Based Attacks*
  - *SSL/HTTPS Attacks*
  - *Slow Rate Attacks*
  - *Protocol Anomalies*
  - *Spoofing and Source Tracking*

InTTrust

SECURITY/NETWORK OPERATING CENTER

- **FortiAnalyzer** — Central Log & report
- **FortiNAC** — IoT Access Control
- **FortiSandbox** — File Analysis
- **FortiNDR** — Virtual Security Analyst ™
- **FortiSIEM** — SIEM / UEBA
- **FortiXDR** — XDR
- **FortiManager** — Central Device Mgmt.
- **FortiAuthenticator** — User Access Mgmt.
- **FortiTester** — Network Tester
- **FortiDeceptor** — Honeypot
- **FortiSOAR** — SOAR

HOSTED SERVICES

Cloud mgmt.

FortiGate Cloud | FortiLAN Cloud | FortiExtender Cloud | FortiManager Cloud | FortiAnalyzer Cloud | FortiClient EMS Cloud | FortiToken Cloud | FortiSOAR Cloud

Cloud services

FortiPresence | FortiMail Cloud | FortiPhish | FortiGSLB | FortiConverter | Fortinet SOCaaS | FortiSASE | FortiPenTest | FortiWeb Cloud | FortiSandbox Cloud | FortiVoice Cloud | FortiMonitor

MOBILE USERS

- **FortiToken** — 2 Factor OTP Token
- **FortiClient / FortiEDR** — VPN, ZTNA, EPP, and SASE Client

SaaS

- **FortiCASB**
- **FortiCNP**

NETWORK SECURITY

- Secure SD-WAN
- IPsec / SSL VPN
- SASE
- **FortiGate** — Security Gateway
- ZTNA

DATA CENTER

- **FortiDDoS** — L7 D/DOS Mitigator
- **FortiADC** — Load Balancer
- **FortiMail** — Mail Sec. Gateway
- **FortiWeb** — Web App. Firewall
- **FortiIsolator** — Browser Isolation
- **FortiProxy** — Secure Web Gateway

BRANCH OFFICE

- **FortiWiFi** — Secure WiFi Access
- **FortiExtender** — 3G/4G/5G WAN

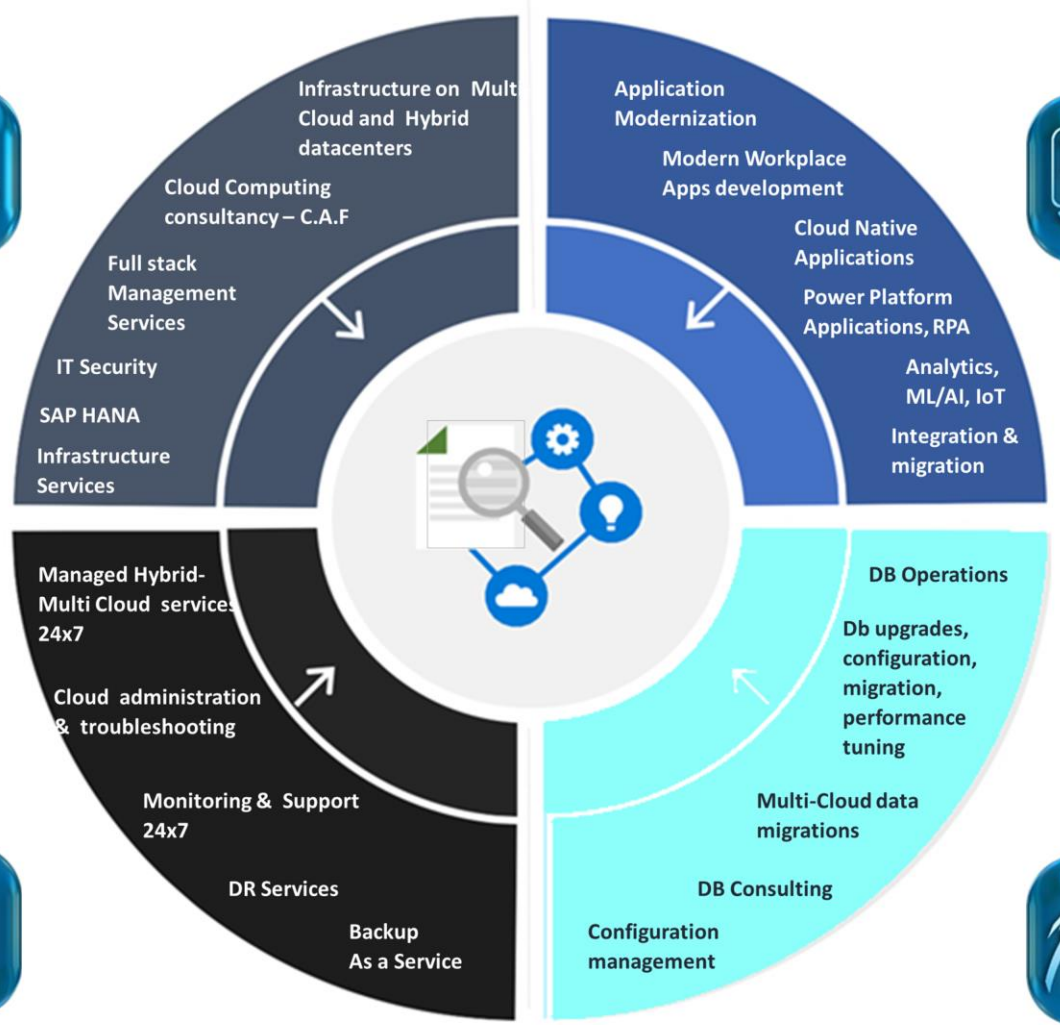
LAN

- **FortiSwitch** — Switch
- **FortiAP** — Wireless Access Point
- **FortiRecorder** — Surveillance Manager
- **FortiVoice** — IP PBX
- **FortiCamera**
- **FortiFone**

InTTrust Services & Key differentiators

Dynamic Infrastructure

Application Development



Managed

DBA

InTTrust

ENGAGE
FORTINET ADVANCED PARTNER
Integrator, MSSP, Marketplace

Thank you.

FORTINET
Security
Day
Sep.2025

Manos Kokolakis, MSc
Customer Success Manager
mkokolakis@inttrust.gr