Delivering secure application and messaging

FortiMail and FortiADC

Khaled Hassan
khassan@fortinet.com

October 2, 2014

Why secure messaging ?

90% mail traffic is not legitimate

- SPAM
- Phishing: Identity Thief
- Trojan
- Virus
- Zombie

✓ **Filter incoming messages to block threats**

✓ **Filter outgoing messages to avoid IP blacklisting**

FortiMail

FortiMail Overview

Summary

FortiMail e-mail and messaging security

- Industry leading price/performance
- Flexible deployment modes and architectures support the widest range of organizations
- Multi-layer Advanced Threat Protection delivers highest level of user protection
- Scalable solution delivers long term investment protection
- Data Leak Prevention, and Policy Based Encryption and Archiving enable compliance with SOX, GLBA, HIPAA, PCI DSS
- FortiGuard Threat Research and Response Network

Trusted Solution

Fortinet email security solutions trusted by over 50,000 customers

vodafone, Telefónica telecom, ERICSSON, HOT mobile, WIND, State of Oregon, CenturyLink, Enterprise Bank, UW Health, United Methodist communications, NPS Naval Postgraduate School, CDE Consejo de Defensa del Estado, Florida Institute of Technology, Canadian Red Cross, Capgemini Consulting.Technology.Outsourcing, Sprint, SIGMA

Independent Validation

Tolly., SC Magazine for IT Security Professionals ★★★★★, vb VERIFIED SPAM virusbtn.com, vb 100 VIRUS virusbtn.com

FORTINET

Advanced Spam and Anti-Malware Protection

Low impact scanning

Avoid queuing mail when destination is available

- Global FortiGuard IP Reputation
- FortiGuard Botnet Tracking Database
- Local Dynamic Sender Reputation

Reject spam at connection stage

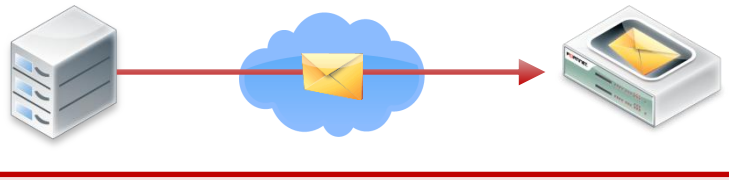
- FortiGuard Spam Content Database
- Content & Behavior Based Heuristic Detection
- Mail Content URL Filtering – Adult, Malware

Real time updated, 3rd party validated

- FortiGuard Malware Detection
- Policy Based Archiving and Encryption

FortiGuard Threat Research

Layered Spam Detection



```
Connection from 1.2.3.4 [mail.testsender.com]

HELO mail.testsender.com
250 mail2.fe-ott.dnsalias.net Hello mail.testsender.com [1.2.3.4],
pleased to meet you
MAIL FROM: user@testsender.com
250 2.1.0 user@testsender.com... Sender ok
RCPT TO: user@domain.com
250 2.1.5 user@domain.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: Subject goes here


Buy viagara here http://www.viagarasales.com

.

QUIT

250 2.0.0 qBGKvjFw031970-qBGKvjFx031970 Message accepted for
delivery
```

Connection Level Filtering:
Discard spam as early as possible for greatest performance

Connection level

- **Global FortiGuard IP Reputation**
- **FortiGuard Botnet Tracking Database**
- **Dynamic Sender Reputation**
- **Connection Rate Limiting**

Layered Spam Detection

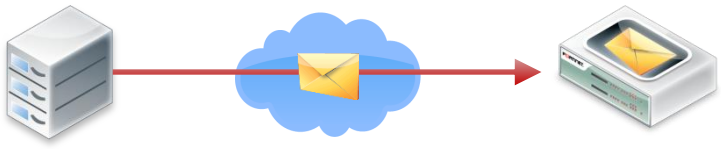
```
Connection from 1.2.3.4 [mail.testsender.com]

HELO mail.testsender.com
250 mail2.fe-ott.dnsalias.net Hello mail.testsender.com [1.2.3.4],
pleased to meet you
MAIL FROM: user@testsender.com
250 2.1.0 user@testsender.com... Sender ok
RCPT TO: user@domain.com
250 2.1.5 user@domain.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: Subject goes here

Buy viagara here http://www.viagarasales.com

.

QUIT

250 2.0.0 qBGKvjFw031970-qBGKvjFx031970 Message accepted for
delivery
```

Envelope Filtering:
Verify valid destination
Support for latest RFCs

Envelope and header level

- Recipient verification
- RFC Compliancy
- SMTP Error Rate Control
- Sender White / Black Lists
- DHA Protection
- SPF Support
- Greylisting

Layered Spam Detection



```
Connection from 1.2.3.4 [mail.testsender.com]

HELO mail.testsender.com
250 mail2.fe-ott.dnsalias.net Hello mail.testsender.com [1.2.3.4],
pleased to meet you
MAIL FROM: user@testsender.com
250 2.1.0 user@testsender.com... Sender ok
RCPT TO: user@domain.com
250 2.1.5 user@domain.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: Subject goes here

Buy viagara here http://www.viagarasales.com

.

QUIT

250 2.0.0 qBGKvjFw031970-qBGKvjFx031970 Message accepted for
delivery
```

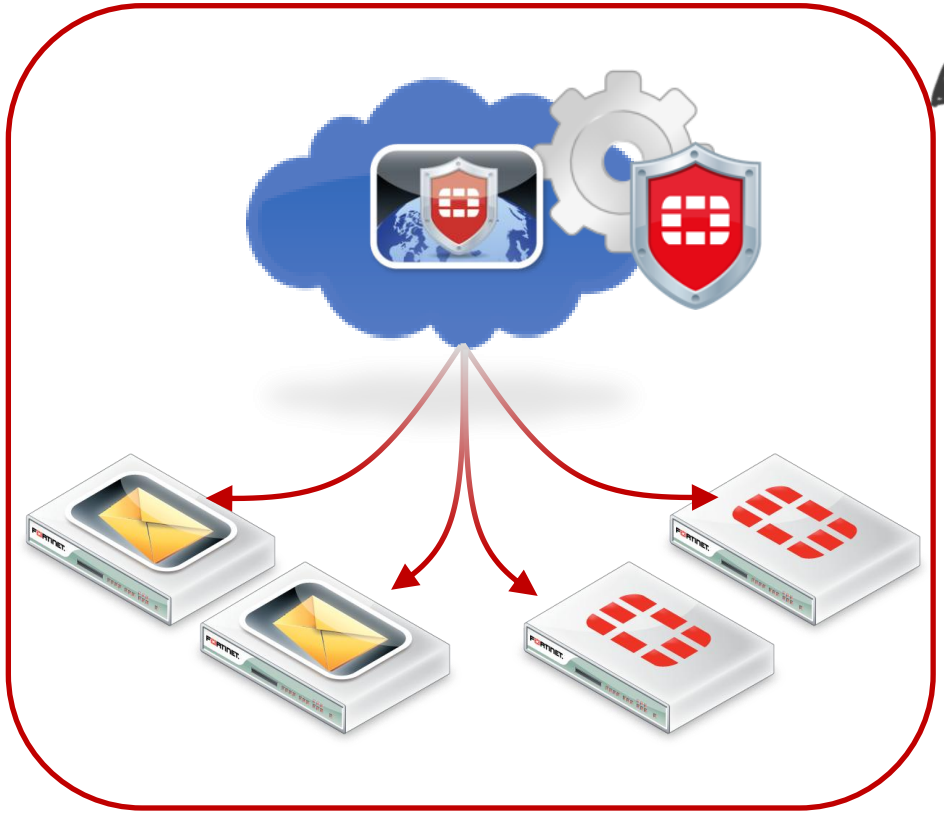
Full Content Filtering:
Multiple Detection Methods

FortiGuard Spam DB

- Heuristic Detection
- Bayesian Filtering
- Newsletter Detection
- Anti-Malware Detection
- Advanced Threat Protection
- Web Content Filtering
- DKIM support

FortiGuard Threat Research

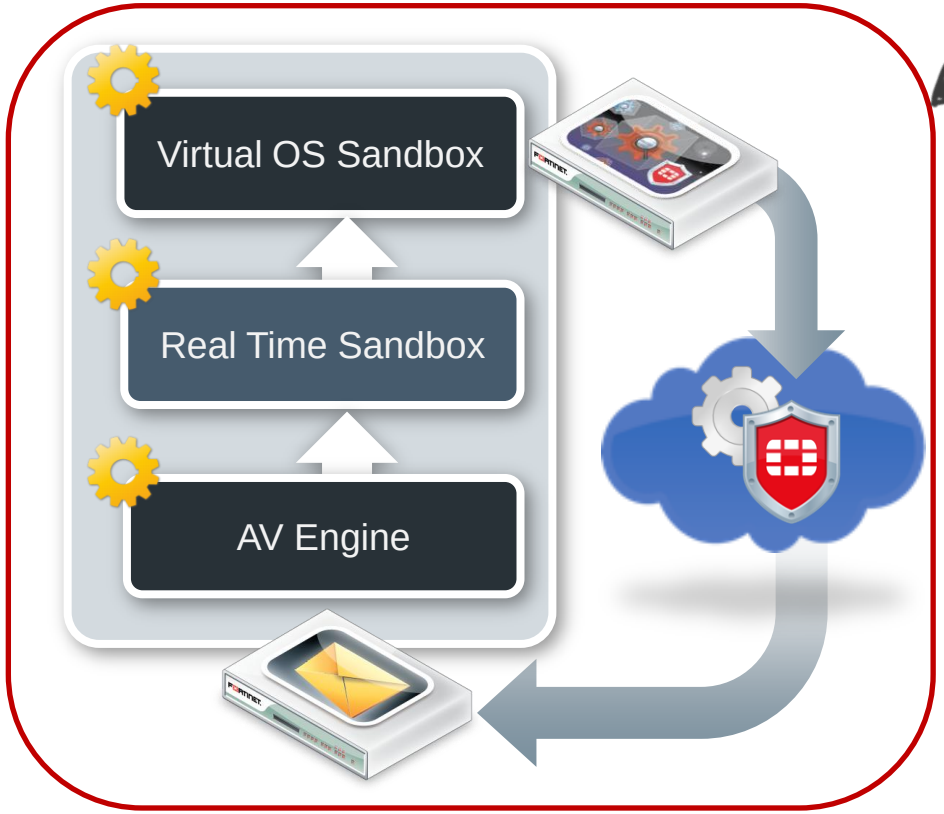
Security experts working for you 24x7!



24x7 Threat Research

- Cloud based antispam and antimalware service
- Visibility of millions of messages per day with global feedback
- Discovers zero day threats and tracks global botnets
  www.fortiguard.com

Advanced Threat Protection



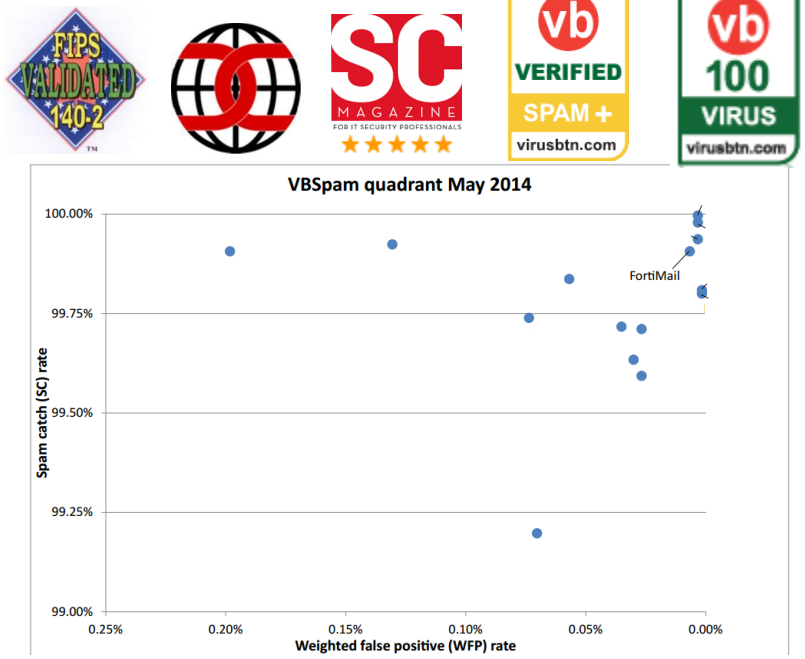
Detect unknown, targeted threats

Multi-layer advanced threat protection

- Award winning VB100 rated AV engine
- Real-time sandbox behavioural analysis
- FortiMail integrates with FortiSandbox to analyze files in a full sandbox before forwarding

Independently Validated

Industry validated solution



* http://www.virusbtn.com/ May 2014 VB Spam Report

Independently tested and highly awarded

- 27 VB100 Awards
- 30 VBSpam Awards with 99.91% catch rate and 0.00% False Positives*
- FIPS and Common criteria EAL2+ certified for Government use

Policy Based Encryption

Simple, secured communication

TLS & S/MIME Encryption Support

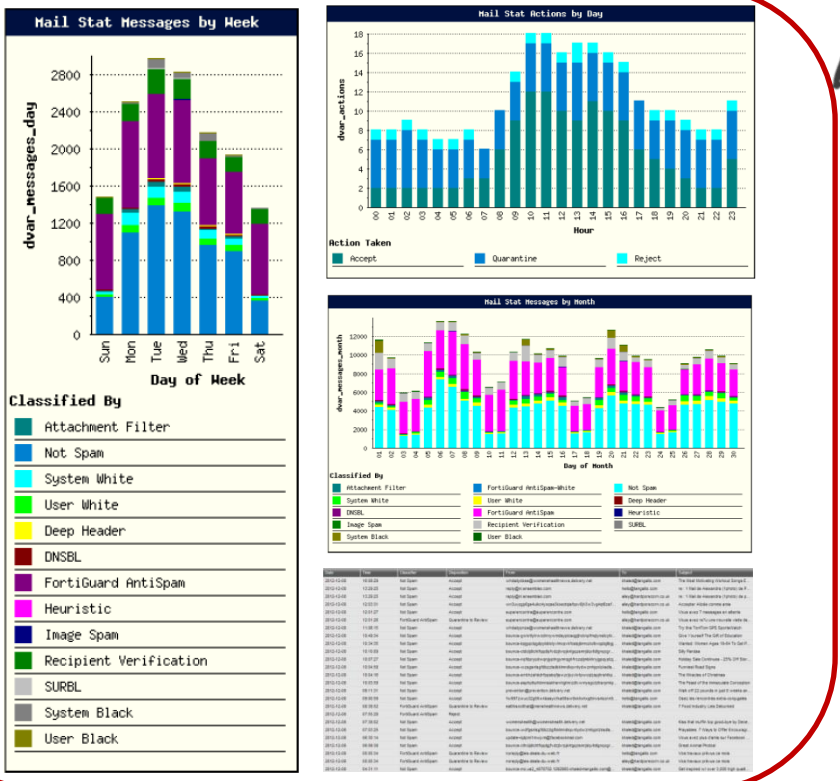
Identity Based Encryption:

- No additional license required
- Sender or rule triggered encryption
- HIPAA, GLBA, SOX, PCI Encryption Policy

Additional Features

Compliance & Visibility

Knowledge is power!



Pre-defined DLP for HIPAA, GLB, SOX compliance and custom filters

Drill-Down Statistics

Message Tracking

Global & per-domain reporting

FORTINET

Message Archiving

Comply with regulatory obligations

Per mailbox policy based archiving:

- **Sender/Recipient**
- **Subject/Body/Attachment filename keywords**

IMAP archive access

Remote archival support

Deployment Options

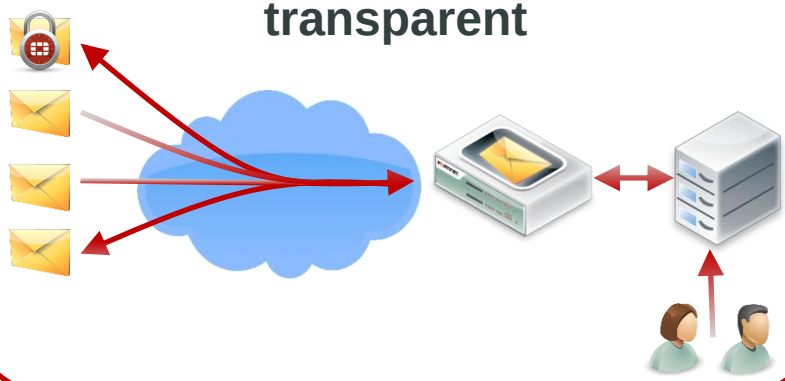
Full email server at no extra cost

Gateway

Deploy on-site or in the cloud to relay mail to destination

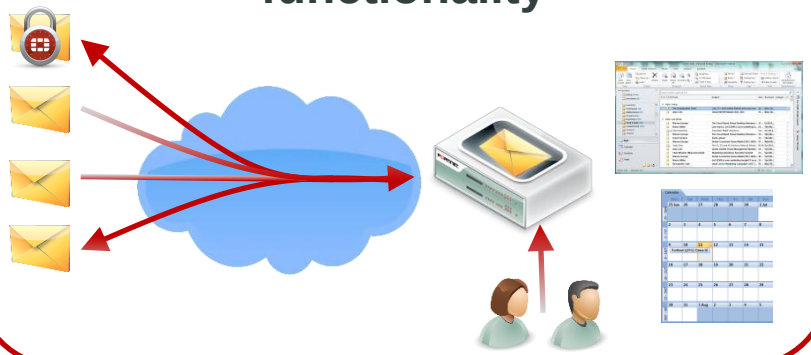
Transparent Inline

Network and application transparent

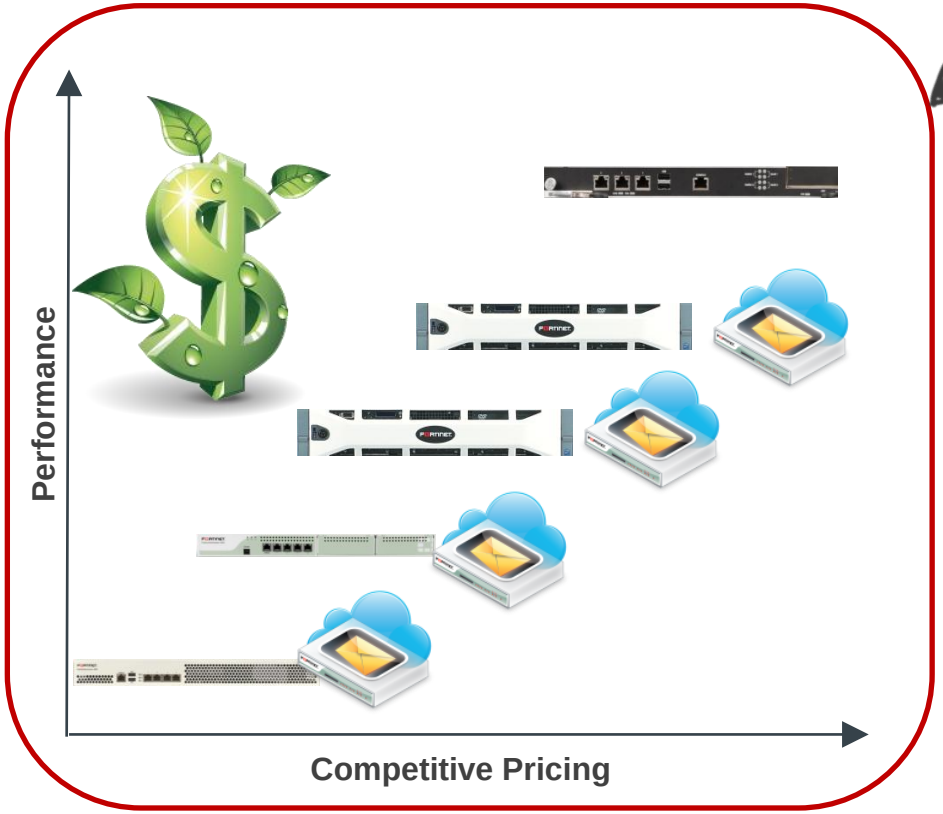


Server

Full mail server and groupware functionality



Competitive Pricing



No third party licenses required

- Highest performance MTA
- Range of deployment sizes to suit SMB to Carriers
- Hardware & VM Options
- No per mailbox licensing
- No IBE licensing
- Single SKU for FortiGuard Services + IBE bundle

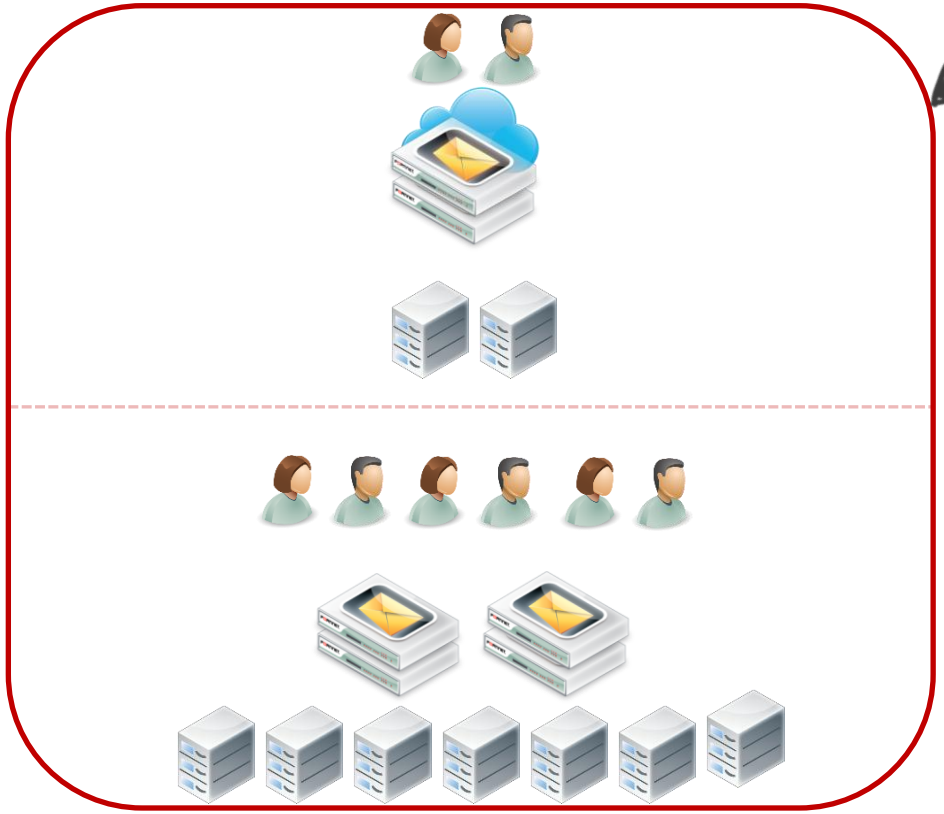
Resilience

Full Mailbox and queue synchronization

Active–Passive Clustering

- Limited to Two Devices, Failover Protection
- Heartbeat and Service Monitoring
- Full mailbox, archive, quarantine, log and queue synchronization

Resilience, Growth & Scalability



Simple capacity planning and growth

Config Only HA

- Scales up to 25 devices with linear scalability
- Centralized quarantine, management and IBE
- Enables DR and geographic redundancy

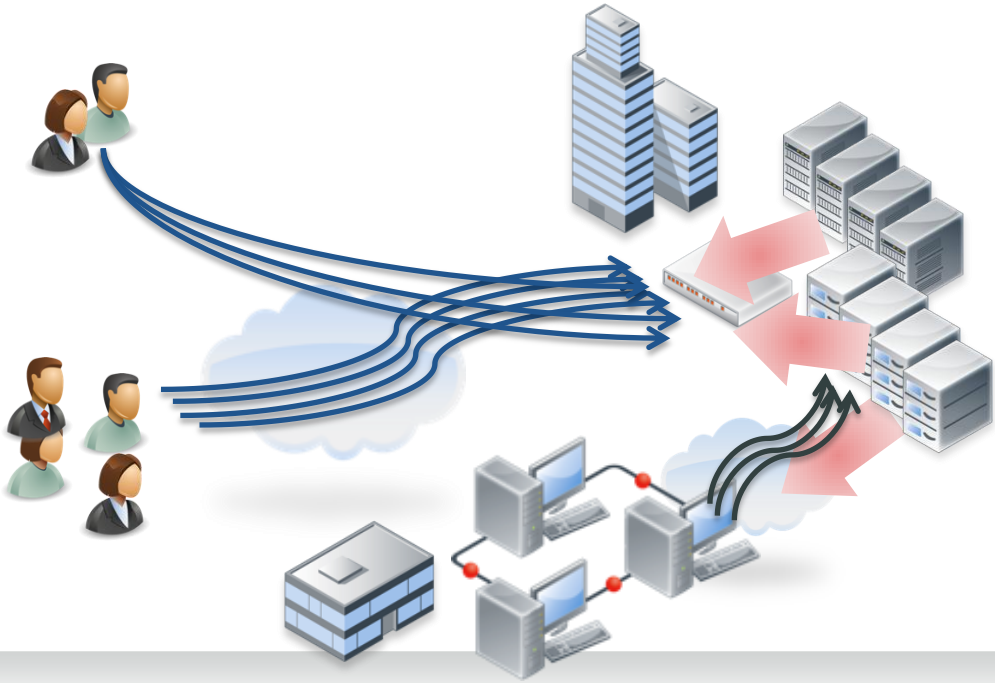
FortiADC

Common Application Delivery Issues

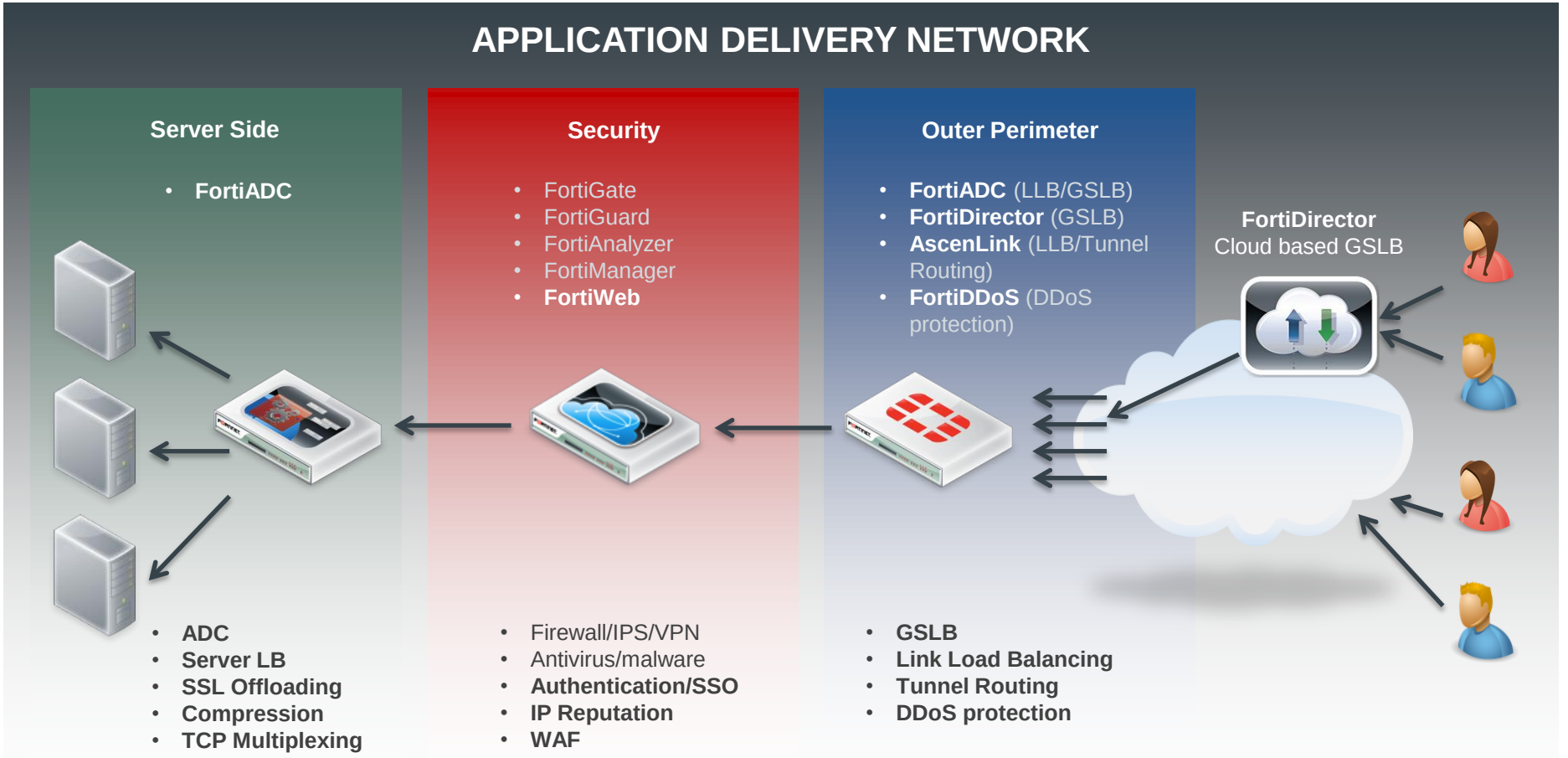
- Single points of failure in infrastructure
- Server resource limitations reached
- Bloated content wastes network and server resources, reduces performance and increases latency
- SSL encryption has heavy impact on server resources

Application performance, scalability and resiliency is key

But non of this matters unless end user completes the transaction and has good experience

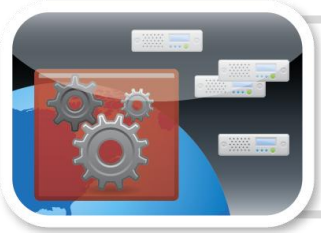


From Edge to Core Network



An ADN can consist of many different components to deliver a complete solution. FortiADCs are evolving to include many functions on a single appliance that combines Fortinet's network security platform with core ADC features to deliver a complete end-to-end solution.

Introducing FortiADC



Application Delivery Controllers

Optimize the availability, user experience, performance and scalability of mobile, cloud and enterprise application delivery from anywhere-to-anywhere.

Application Availability

- Layer 4 and 7 load balancing techniques
- Application session persistence
- Global Server Load Balancing (GSLB) for geographic resilience. Free!
- Link Load Balancing
- Quality of Service (QoS)
- Virtual Domains (VDOM)
- IPv6 Support

Application Acceleration

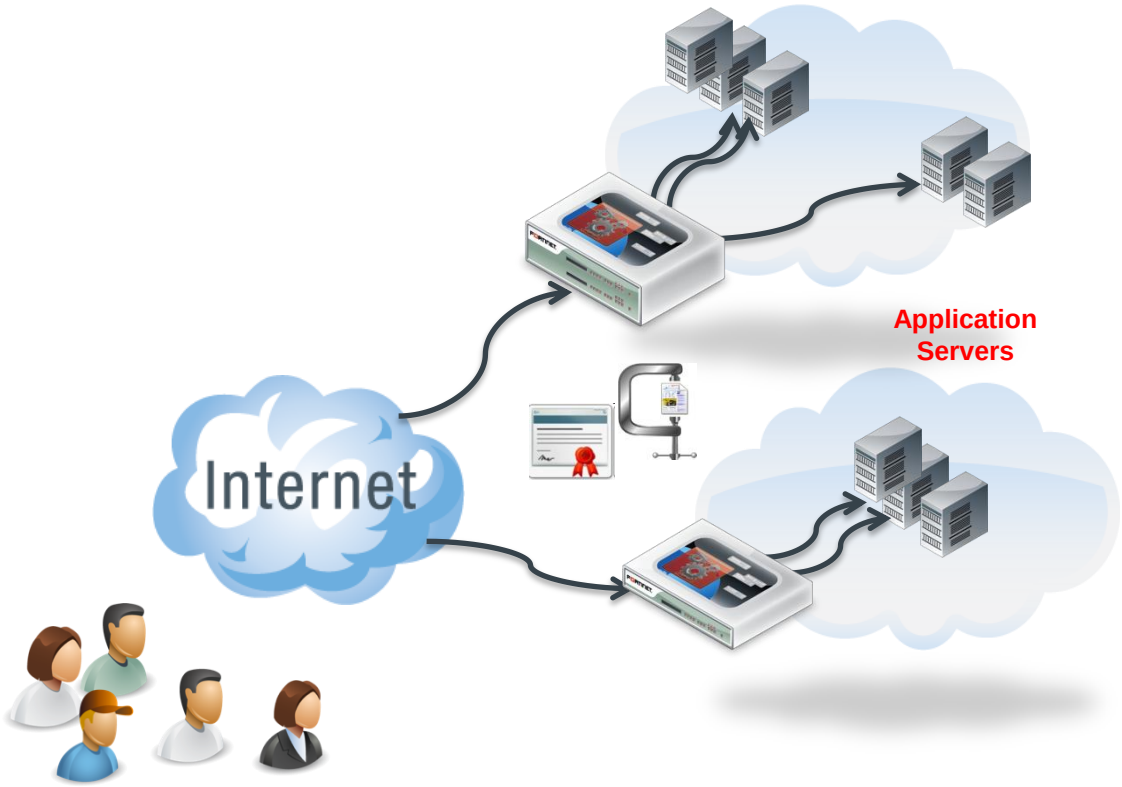
- TCP Optimization/Multiplexing
- SSL Offload and acceleration
- Compression
- Caching

Application Aware Intelligence

- Advanced content routing and URL rewriting capabilities

Security

- IP Reputation
- IPv4 and IPv6 firewall ACL rules
- SYN Flood protection



FORTINET

Fortinet's ADC Products

FortiADC VMs

01 – 1.0 Gbps
02 – 2.1 Gbps
04 – 5.0 Gbps
08 – 8.0 Gbps

(actual speeds are hardware dependent)

DATA CENTER

FortiADC-300E
- 6 GbE
- 4.8 Gbps

FortiADC-600E
- Hardware SSL
- 8 GbE/2 SFP-10
- 12.0 Gbps

FortiADC-1000E
- Hardware SSL
- Dual power/fans
- 8 GbE/2 SFP-10
- 15.0 Gbps

FortiADC-1500D
- Hardware SSL
- Dual power/fans
- 8 GbE/4 SFP-10
- 20.0 Gbps

FortiADC-2000D
- Hardware SSL
- Dual power/fans
- 16 GbE/4 SFP-10
- 30.0 Gbps

FortiADC-4000D
- Hardware SSL
- Dual power/fans
- 16 GbE/8 SFP-10
- 50.0 Gbps

FortiADC-400E
- Hardware SSL
- 8 GbE
- 8.0 Gbps

FortiADC-200D
- 4 GbE
- 2.7 Gbps

SMB

Products Include:

Global Server Load Balancing
Link Load Balancing
QoS (FortiADC D only)
Firewall
Compression
Caching (FortiADC D only)
Virtual Domains (FortiADC D only)

FORTINET

Server Load Balance

Application Availability

Load Balancing Methods

- Methods: Round Robin, Least Connection, Shortest Response

✓ **Distribute connections using different methods**

Server Persistence

- Persistence methods: Persistent IP, Hash Header, Rewrite Cookie, Embedded Cookie, Hash IP, Hash Query, Insert Cookie, Radius Attribute, Hash IP Port, Persistent Cookie, Hash Cookie

✓ **Maintains persistency across clients and servers**

✓ **All connections from the same client routed to the same server**

Health Checks

- Probes & Health Checks: ICMP, HTTP, HTTPS, TCP, TCP Echo, DNS and RADIUS
- Configure interval, timeout Down and Up retry

✓ **verifies that real servers are able respond to network connection attempts**

*Functionality may vary according to platform type

Link Load Balancing

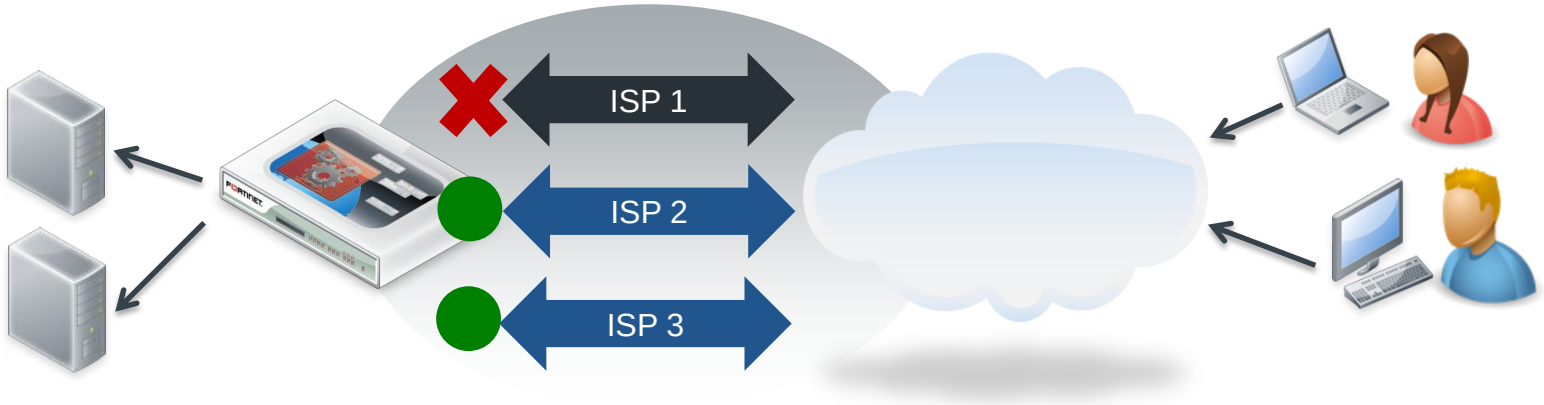
Application Availability

Features

- Manage inbound and outbound traffic
- Routes traffic to best performing ISPs
- Up to 16 links can be added for capacity or redundancy
- Multiple point link health check support
- SNAT and Policy Routes for routing flexibility

Benefits

- Reduce congestion and improve user experience
- Dynamic ability to add capacity
- Improve application availability and ensure business continuity
- Reduce costs by routing traffic to lower cost providers



FORTINET

Quality of Service

Application Availability

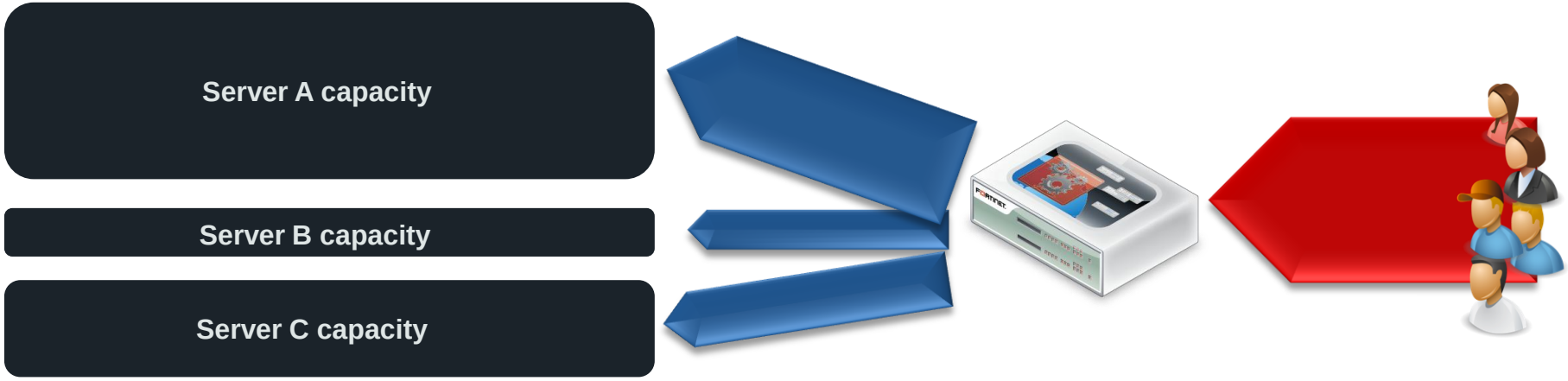
QoS

- Define per source and destination
- Type of Service (TOS) & Differentiated Services (DiffServ) Support

Connection Control

- Limit number of connections per interface, srd/dst IP and service

- ✓ **Ensure required access to critical applications**
- ✓ **Protects critical traffic from being overwhelmed by other traffic**
- ✓ **Prioritize time sensitive traffic such as VoIP & streaming videos**

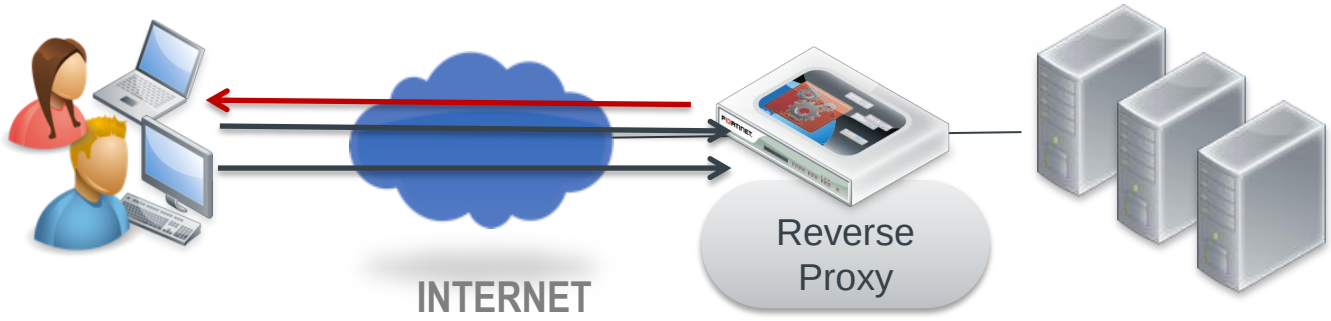


Per IP, interface and service QoS

FORTINET

Web Caching

Application Acceleration



RAM Caching

Name*:	WebCache
Maximum Object Size:	1M
Maximum Cache Size:	100M
Maximum Entries:	10000
Maximum Age (sec):	43200

URI Exclude List (1)

Add | Delete | Edit: *Double-Click*

ID	URI
1	/app1/

- ✓ **Reduce repetitive requests to server**
- ✓ **Increase server capacity and reduce server load**
- ✓ **Fine grain control over which content types to support**

FORTINET

SSL Offload

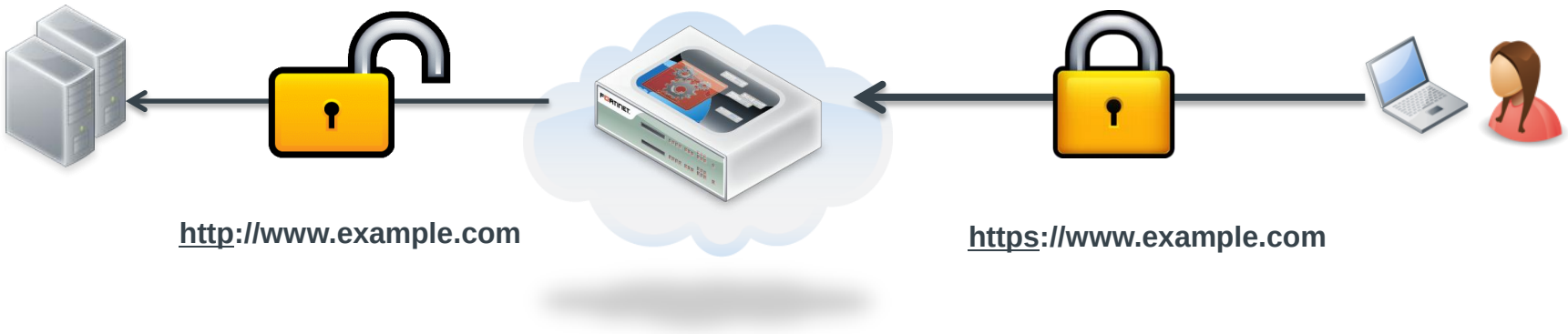
Application Acceleration

High Performance

- Offload CPU intensive SSL processing from servers
- Accelerate performance and overall user experience
- Dramatic increase in transaction processing

Easily integrate with applications

- Full Certificate Management
- Advanced certification verification and revocation capabilities



FORTINET

Overview

FortiGuard IP Reputation

Threats

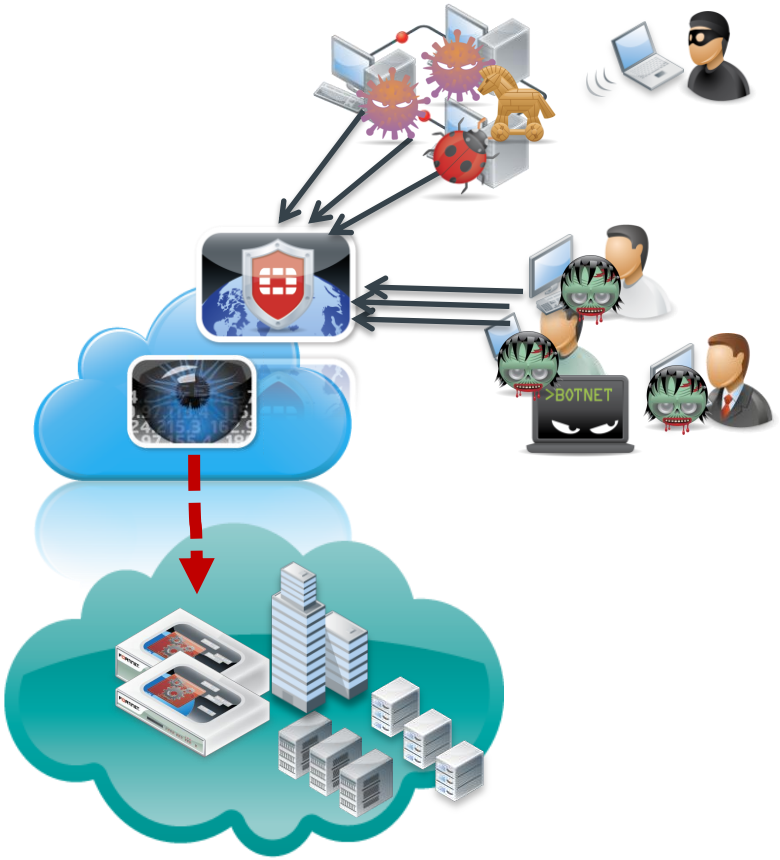
- DDoS
- Phishing
- Botnets
- C&C communication
- Infected source
- SPAM hosts

IP Reputation Service

- Daily feed updates
- Automated downloads
- Immediate protection
- Visibility and reporting

FortiGuard Techniques

- FortiGuard historical analysis
- Honeypots
- Botnet analysis
- Anonymous proxies
- Third party sources



FortiGuard IP Reputation Service:
Protect against automated attacks and malicious source

FORTINET

Questions

Thank you