



FAST. SECURE. GLOBAL.



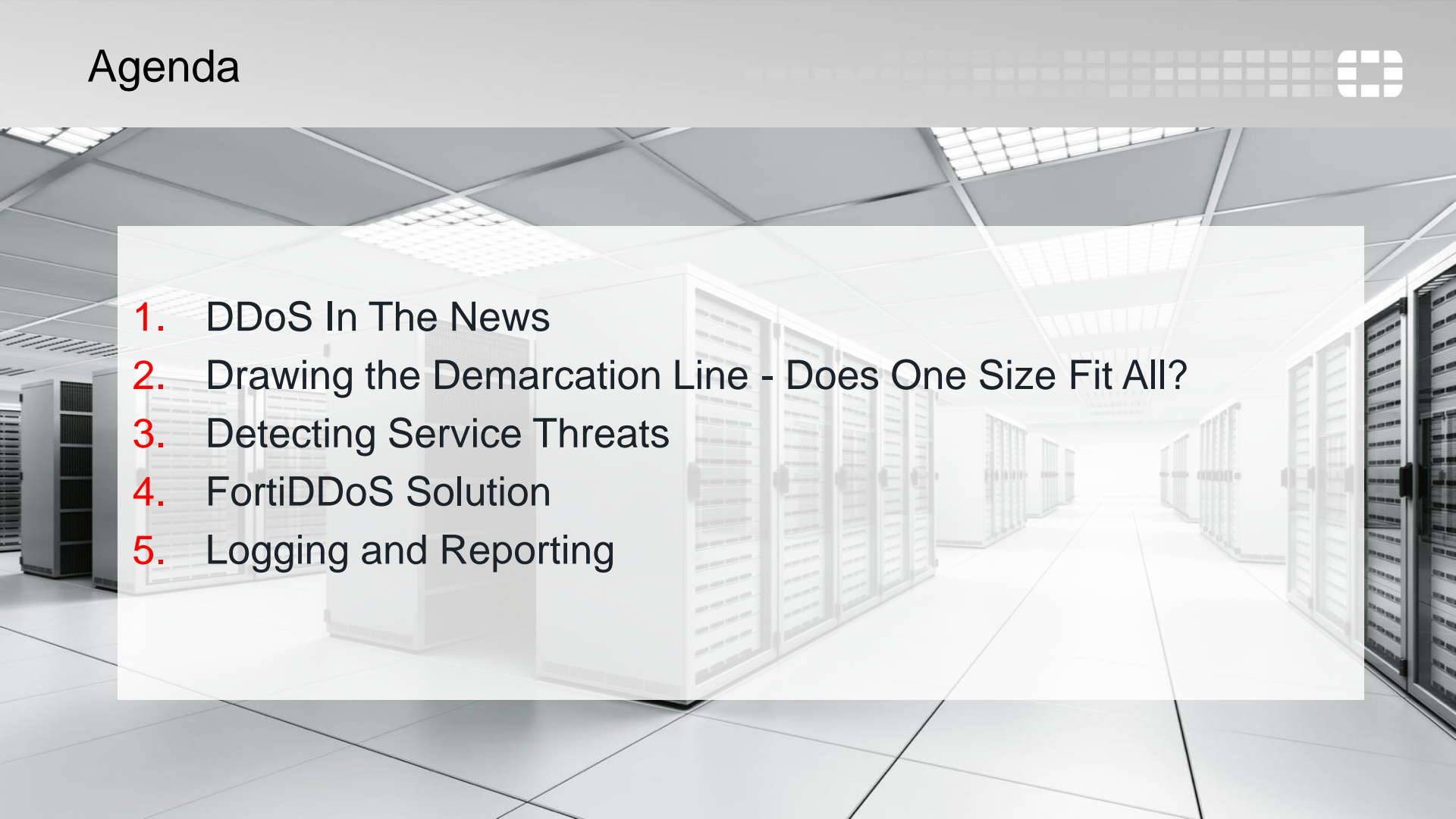
FortiDDos – Size isn't everything

Martijn Duijm – Director Sales Engineering

April - 2015

Agenda



- 
1. DDoS In The News
 2. Drawing the Demarcation Line - Does One Size Fit All?
 3. Detecting Service Threats
 4. FortiDDoS Solution
 5. Logging and Reporting



DDoS In the News



Stack Overflow goes down for an hour on Sunday due to DDoS attack

February 17

Stack Overflow

Sunday n

TechCrunch

Bitcoin Value Plunges as DDoS Strikes Currency Exchanges Read

February 14, 2014 - admin - 0 Comment

Largest ever DDoS attack

February 11, 2014 - admin - 0 Comment

CloudFlare said that the attack was close to CNET > News > Security & Privacy > Record-breaking DDoS attack in Europe hits 400Gbps

Record-breaking DDoS attack in Europe hits 400Gbps

A distributed-denial-of-service attack peaked some 33 percent higher than last year's Spamhaus attack, the previous DDoS record-holder, revealing the reality of the customer under

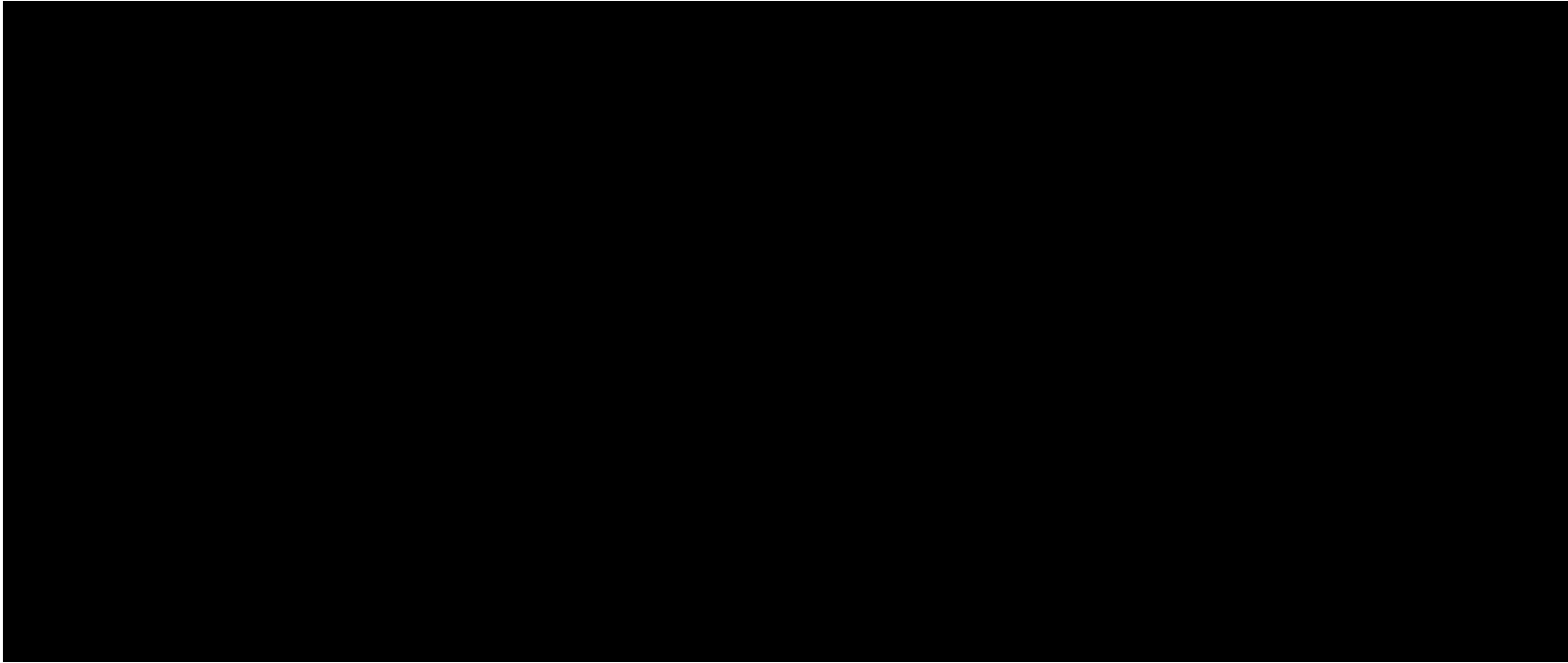
attack, and there were few details on how many other companies had been affected. The DDoS attack did, however,...

- DDoS attacks still #1 threat to data centers
- Size of volume-based attacks increasing
- 80% of attacks less than 50 Mbps
- Most successful attacks under 1 Gbps
- Attacks getting more sophisticated
- Layer 7 attacks fastest growing type
- Hackers using DDoS to mask data breaches

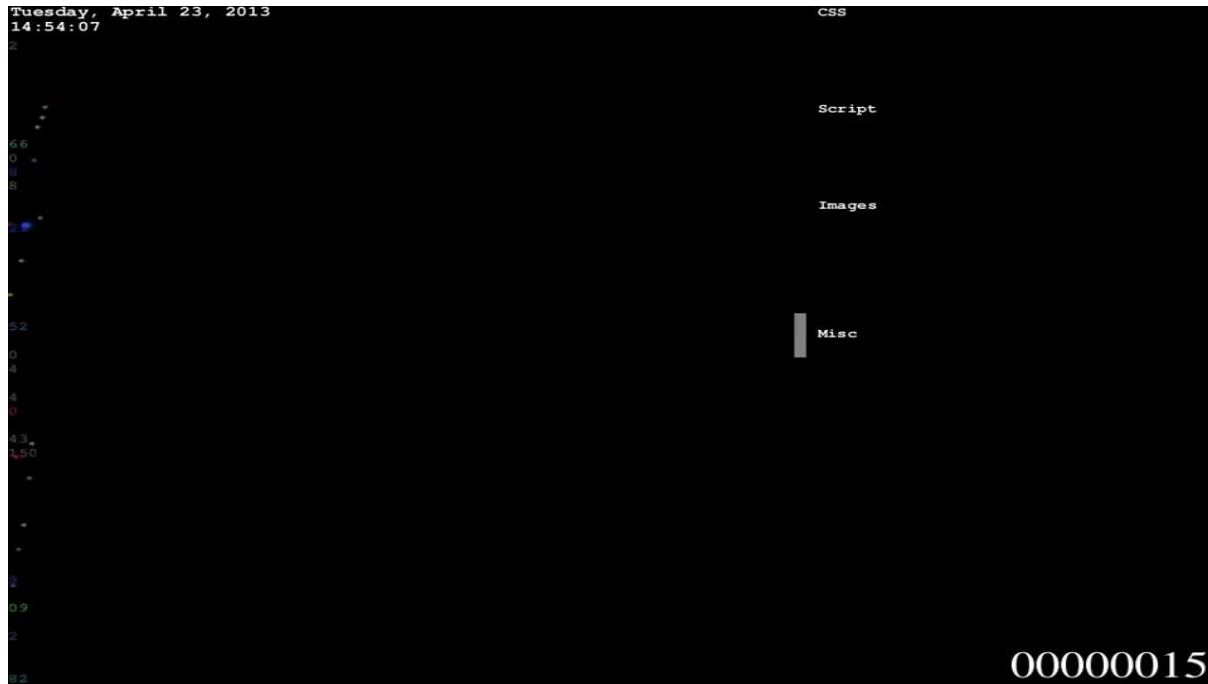
Enterprises Need Protection

- Finance and Government primary targets
- Disruptions to operations and commerce
- Customer and financial data at risk
- Traditional protections can't detect small attacks
- Layer 7 attacks making through to data centers

Normal traffic (Logstalgia)



'Bad' traffic— attack at Videolan download platform



Verisign DDoS report Q4/2014



- Sustained volumetric DDoS activity, with attacks reaching 60 Gbps/16 Millions of packets per second (Mpps) for User Datagram Protocol (UDP) floods and 55 Gbps/60 Mpps for Transmission Control Protocol (TCP)-based attacks.
- Average attack size increased to 7.39 gigabits per second (Gbps), rising 14 percent higher than in Q3 2014 and 245 percent higher than Q4 2013
- The most frequently targeted industry in Q4 was IT Services/Cloud/SaaS, representing one third of all mitigation activity and peaking at just over 60 Gbps
- 42 percent of attacks peaked at more than 1 Gbps, with 17 percent leveraging more than 10 Gbps of DDoS traffic.
- Own conclusion: 58 percent of the attacks are below 1Gbps of DDoS traffic

Types of DDoS Attacks



Bulk Volumetric

Designed to overwhelm and consume available internet bandwidth or overload servers (e.g. SYN, UDP, ICMP floods).

Problems:

- Services unavailable to users
- Can mask data breaches
- Attack sizes getting larger
- Easy to implement attack



Application Layer

Smaller, more sophisticated attacks that target layer 7 application services on servers like HTTP, SMTP and HTTPS.

Problems:

- Slip past traditional defenses
- Fastest growing attack type
- Detection difficult
- Easier for botmasters to implement

Bulk Volumetric



Bulk Volumetric

Designed to overwhelm and consume available internet bandwidth or overload servers (e.g. SYN, UDP, ICMP floods).

Problems:

- Services unavailable to users
- Can mask data breaches
- Attack sizes getting larger
- Easy to implement attack

SYN Flood: Spoofed SYN Packets fill the connection table of servers, and all other devices in your network path

Zombie Flood: In zombie or botnet floods, non-spoofed connections overload network and application services.

ICMP Flood: In these floods, ICMP packets, such as those used for “ping”, overload servers and network connections.

TCP/UDP Port Flood: TCP/UDP packets overload the servers and network ports not being used for a service, such as TCP port 81.

Fragment Flood: Fragmented packets overload the servers.

Anomalous Packet Flood: Deliberate or accidental packet errors in scripts by hackers easily overload network equipment and servers as they attempt to deal with anomalies.

Unwanted Geographical Area Floods: Packets are flooding in from an unwanted or potentially malicious geographic area (country, region, etc.).

Blended Attacks: More and more DDoS events are using combinations of the basic attack types and some are even masking service-level attacks within high-volume basic ones to throw off detection services.

Application Layer Attacks

L7

Application Layer

Smaller, more sophisticated attacks that target layer 7 application services on servers like HTTP, SMTP and HTTPS.

Problems:

- Slip past traditional defenses
- Fastest growing attack type
- Detection difficult
- Easier for botmasters to implement

HTTP GET: These attacks involve connection-oriented bots that attempt to overload servers and connections on service ports (such as HTTP) by mimicking legitimate users.

HTTP POST: POST body messages are sent at a very slow rate and disrupt proper connection completion.

HTTP Slow Read: Attackers force servers to send a large amount of data, however it forced to be sent in many small fragments and read at a very slow rate by the receiver.

Slowloris: Using HTTP GET, attackers launch multiple partial and time-delayed HTTP refer headers to keep the connections open as long as needed to deplete resources.

HTTPS: Similar to HTTP attacks, these attack SSL services on servers.

SMTP: Attacks targeted at SMTP mail server services.

VoIP: Attacks target at SIP INVITE services.

DDoS Defense Options



DDoS Service Provider

Managed service subscription model usually with separate detection and mitigation.

Pros:

- Easy sign up
- Easy deployment

Cons:

- Expensive overages
- Unpredictable costs
- Limited flexibility



Firewall/IPS

Integrated device that includes firewall, intrusion protection and DDoS prevention.

Pros:

- Single device
- Less units to manage

Cons:

- Poor level 7 attack detection
- May require licensing
- Performance impacts



Dedicated Appliance

Inline data center appliance that provides layer 3, 4 and 7 DDoS detection and mitigation.

Pros:

- Predictable costs
- Advanced layer 7 protection

Cons*:

- Additional device management
- Can be vulnerable to large attack
- May require signature updates

* We'll demonstrate how FortiDDoS was designed to address these issues

The Evolving Threat



Traditional Attacks

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

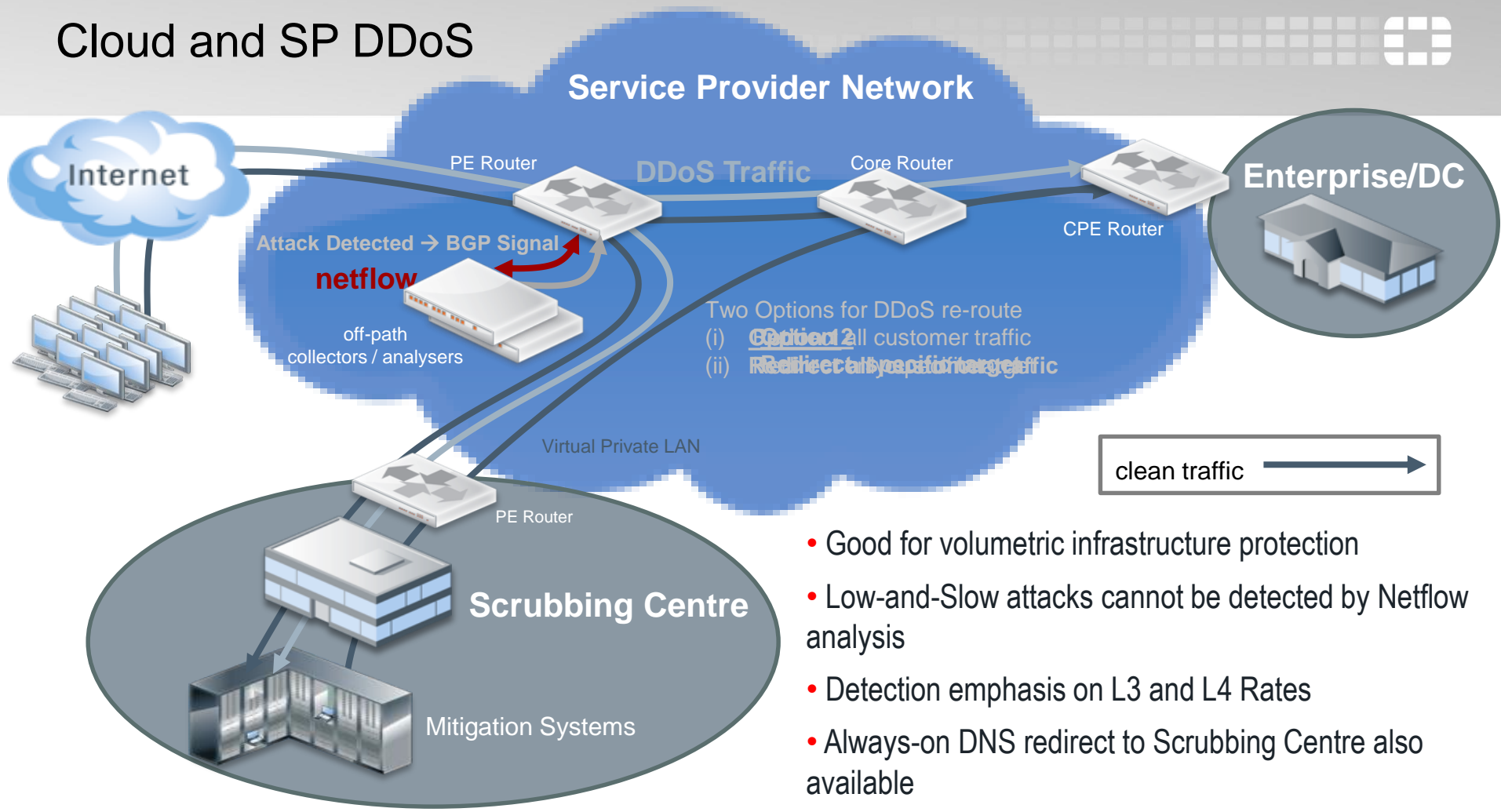
Today and Future

- Service layer 7 focus
- Small, targeted attacks
- Blended 3/4/7 approaches
- Cloud service targets
- Skirting of ISP DDoS defenses
- Larger attacks are more for show

A New Approach

- Behavioral Detection
- Service and port monitoring
- Detect any size of attack
- Hardware-assisted
- Can't rely solely on ISP
- Automatic mitigation

Cloud and SP DDoS

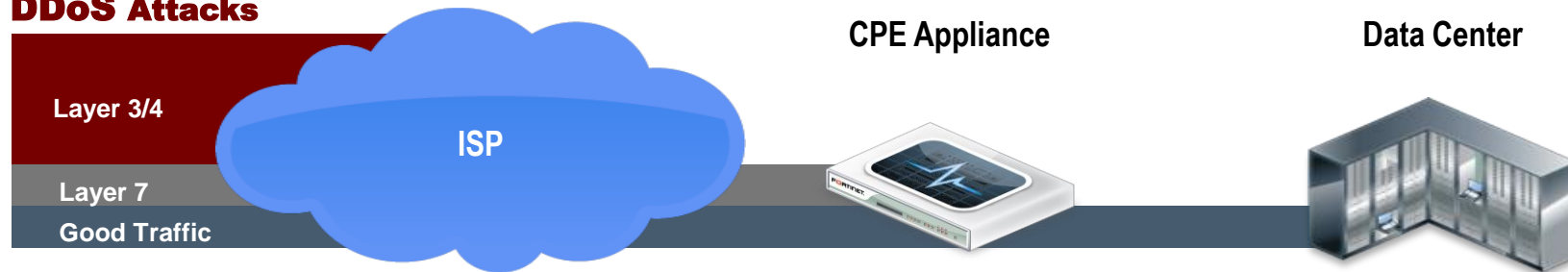


- Good for volumetric infrastructure protection
- Low-and-Slow attacks cannot be detected by Netflow analysis
- Detection emphasis on L3 and L4 Rates
- Always-on DNS redirect to Scrubbing Centre also available

Appliance with an ISP for Congestion Protection

- A dedicated appliance can't protect "pipes" by itself
- Used with an ISP's DDoS protections, data centers are protected from high-volume layer 3/4 attacks and smaller layer 7 attacks

DDoS Attacks



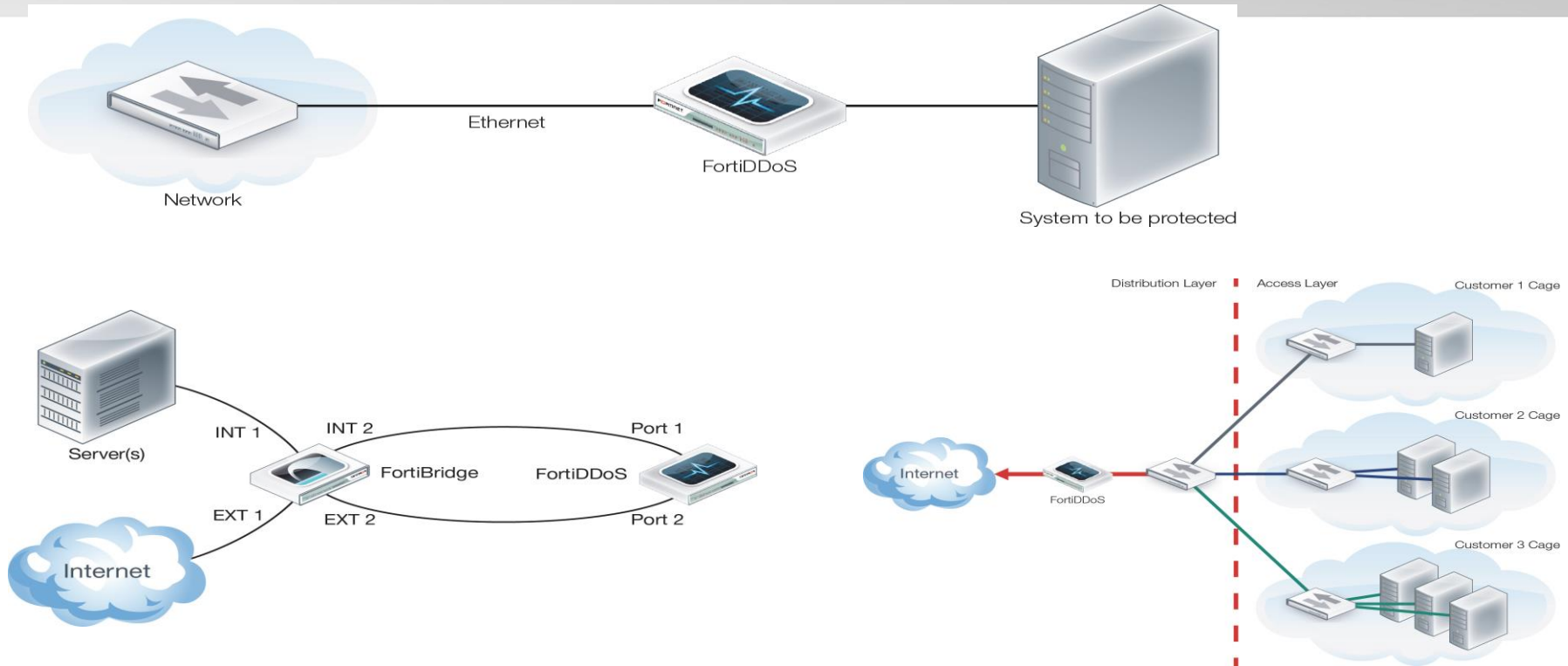
Bulk Protection

ISPs offer bulk DDoS protections at the layer 3 and 4 level and can screen those out to minimize congestion on the links into the data center

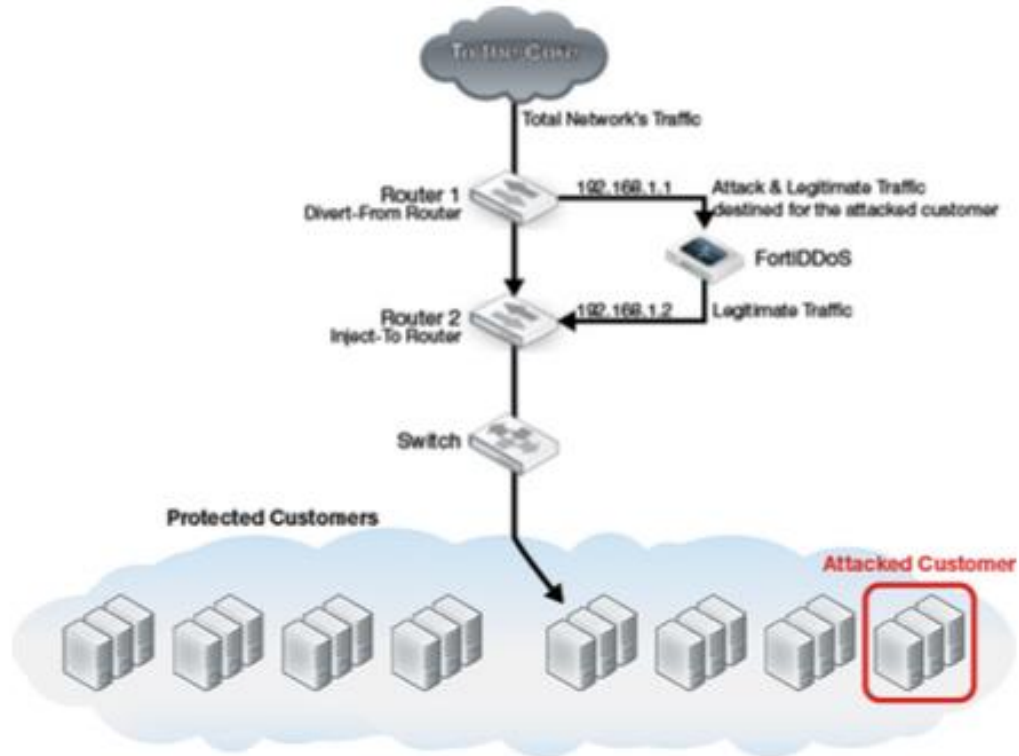
Application Protection

FortiDDoS detects and mitigates smaller layer 7 attacks that are passed by the ISP to the data center and can detect small layer 3 and 4 attacks that may not be detected by the ISP

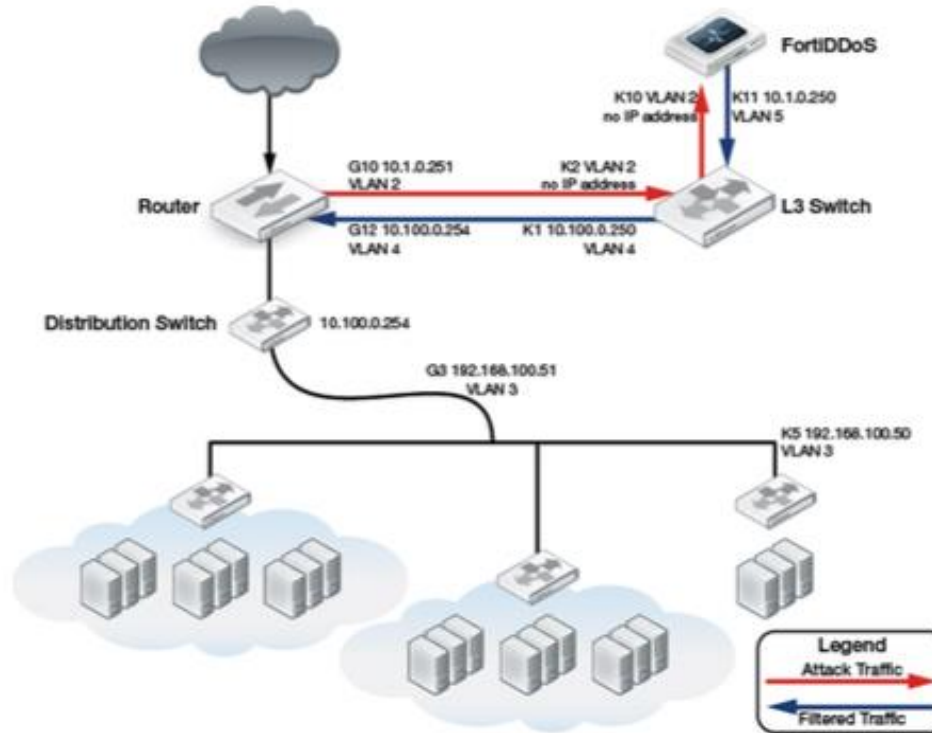
Deployment Scenarios



Traffic Diversion in MSSP environment



Traffic Diversion - variation





- No Signatures
- Because the FortiDDoS uses behavior and rate-based analysis, it provides positive security model for protection against attacks the hackers haven't even thought up yet. No administrative intervention is required, and the Intrusion Gateway is on guard 24/7, automatically protecting your network systems and bandwidth.

Key Features and Benefits

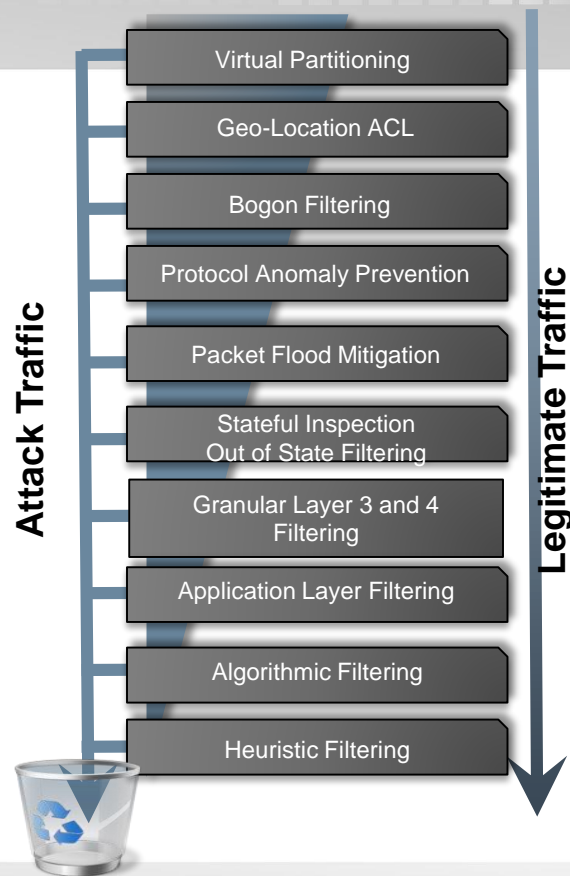


100% Behavioral	FortiDDoS doesn't rely on signature files that need to be updated with the latest threats so you're protected from both known and unknown "zero-day" attacks
100% Hardware	The FortiASIC-TP2 transaction processor provides full bi-directional detection and mitigation of Layer 2, 3 and 7 DDoS attacks for industry-leading performance
Continuous Attack Evaluation	Minimizes the risk of "false positive" detection by reevaluating the attack to ensure that "good" traffic isn't disrupted
Congestion Resistant	FortiDDoS won't easily be overwhelmed and succumb to a DDoS threat, with high throughput rates and full line rate detection and mitigation.
Automated Learning	With minimal configuration, FortiDDoS will automatically build normal traffic and resources behavior profiles saving you time and IT management resources
Multi-Attack Protection	By understanding behaviors FortiDDoS can detect any DDoS attack from basic Bulk Volumetric to sophisticated Layer 7 SSL-based attacks without the need to decrypt traffic

Detection and Mitigation

How it works

- Detection is performed in hardware
- Mitigation occurs inline





- **Adaptive Thresholds** fine tunes/automatically adjusts configured minimum thresholds over time by predicting traffic flows based on current and past statistics
- **Adaptive Threshold Limit** restricts the threshold adjustments to a set maximum percent (default 150%) above the set minimum threshold value

.

A decorative graphic in the top-left corner consisting of a grid of dark gray squares and rectangles, some of which are rounded or partially cut off.

FortiDDoS Logging Options



High Performance Partnerships

Local Logs

- DDoS Attack Log

System

Global Settings

Protection Profiles

Monitor

Log & Report

Log Configuration

- Log Settings
- Log Remote
- DDoS Attack Log Remote
- Alert Mail
- Purge Settings

Log Access

- Event Log
- DDoS Attack Log
- Log Backup

Report Configuration

- Report Browse
- Report Browse
- Executive Summary

Attack Graphs

- Attack Graphs

Diagnostics

- Sessions
- Sources

DDoS Attack Log

Filter Settings

#	Event ID	Time Stamp	SPP	DIR	Event Type	Drop Count
1	3385678	2014-03-14 00:25:00	SPP-Web	Outbound	Most Active Source	-
2	3385679	2014-03-14 00:25:00	SPP-Web	Outbound	Most Active Destination	-
3	3385676	2014-03-14 00:10:00	SPP-Web	Outbound	Most Active Source	-
4	3385677	2014-03-14 00:10:00	SPP-Web	Outbound	Most Active Destination	-
5	3385674	2014-03-14 00:00:00	SPP-Web	Outbound	Most Active Source	-
6	3385675	2014-03-14 00:00:00	SPP-Web	Outbound	Most Active Destination	-
7	3385672	2014-03-13 23:55:00	SPP-Web	Outbound	Most Active Source	-
8	3385673	2014-03-13 23:55:00	SPP-Web	Outbound	Most Active Destination	-
9	3385670	2014-03-13 23:45:00	SPP-Web	Outbound	Most Active Source	-
10	3385671	2014-03-13 23:45:00	SPP-Web	Outbound	Most Active Destination	-
11	3385668	2014-03-13 23:40:00	SPP-Web	Outbound	Most Active Source	-
12	3385669	2014-03-13 23:40:00	SPP-Web	Outbound	Most Active Destination	-
13	3385666	2014-03-13 23:35:00	SPP-Web	Outbound	Most Active Source	-
14	3385667	2014-03-13 23:35:00	SPP-Web	Outbound	Most Active Destination	-
15	3385664	2014-03-13 23:25:00	SPP-Web	Outbound	Most Active Source	-

Page 1 of 7003

Displaying 1 - 20 of 140044

Event ID

3385678

TimeStamp

2014-03-14 00:25:00

SPP Id

1

DIR

Outbound

Source IP

192.168.235.101

Destination IP

-

Protocol

-

ICMP Type/Code

-

Event Type

Most Active Source

Event Detail

'Packet Rate: 1'

Destination Port

-

Unique ID

0

Local Logs - Report Summary

- Attack Executive Summary

The screenshot displays the Fortinet Local Logs - Report Summary interface. The left sidebar contains a navigation menu with the following items: System, Global Settings, Protection Profiles, Monitor, Log & Report (highlighted), Log Configuration (Log Settings, Log Remote, DDoS Attack Log Remote, Alert Mail, Purge Settings), Log Access (Event Log, DDoS Attack Log, Log Backup), Report Configuration (Report Configuration), Report Browse (Report Browse, Executive Summary), Attack Graphs (Attack Graphs), Diagnostics (Sessions, Sources), and Sources.

The main content area is titled "Attack Executive Summary" and contains several portlets:

- Top Attacks**: A table showing the top attacks by event count.
- Top Attacked Subnets**: A table showing the top attacked subnets by drop count.
- Top Attackers**: A table showing the top attackers by drop count.
- Top ACL Subnet Drops**: A table showing the top ACL subnet drops.
- Top Attacked TCP Ports**: A table showing the top attacked TCP ports.

The "Top Attacks" portlet displays the following data:

Attack	SPP	Direction	Drops	Events
TCP invalid flag combination	SPP-Web	Inbound	269191250359	2237
SYN flood	SPP-Web	Inbound	2013990066	49193
Protocol flood	SPP-Web	Inbound	1261962459	58313
TCP checksum error	SPP-0	Inbound	427515455	140
IP Header checksum error	SPP-0	Inbound	427515443	129
L4 anomalies	SPP-Web	Inbound	382746854	24
TCP invalid flag combination	SPP-0	Inbound	250513749	5
Destination flood	SPP-Web	Inbound	219787735	410
Excessive TCP Packets Per Des...	SPP-Web	Inbound	167383486	2825
Source flood	SPP-Web	Outbound	122929672	226
TCP port flood	SPP-Web	Inbound	94234284	127

The "Top Attacked Subnets" portlet displays the following data:

Subnet Id	IP address/Mask	SPP	Direction	Drops
1	192.168.235.101/32	SPP-Web	Inbound	273159137988
0	-	SPP-0	Inbound	250513740
1	192.168.235.101/32	SPP-Web	Outbound	119207461
0	-	SPP-0	Outbound	2

The "Top Attackers" portlet displays the following data:

IP	SPP	Direction	Drops	Events
172.16.1.2	SPP-Web	Outbound	116271355	202
172.16.1.1	SPP-Web	Inbound	5554704	140
172.16.1.20	SPP-Web	Outbound	2221861	9
192.168.235.101	SPP-Web	Outbound	1483363	12
192.168.235.99	SPP-Web	Inbound	3469	12

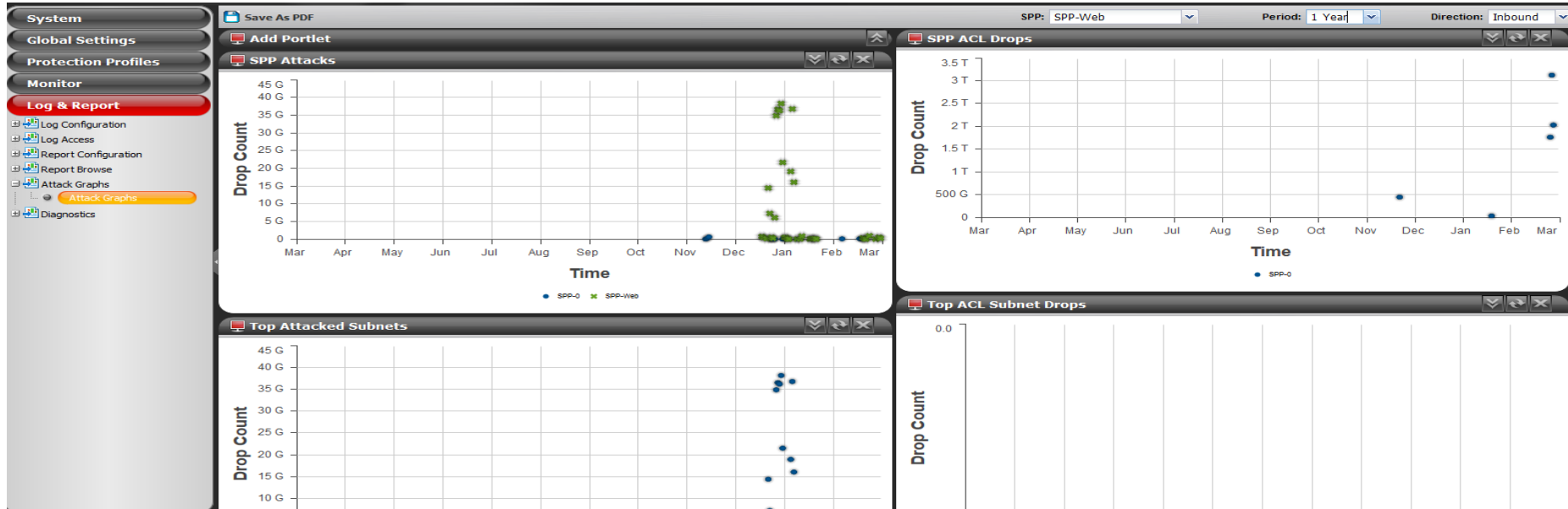
The "Top ACL Subnet Drops" portlet displays the message: "There are no records to display".

The "Top Attacked TCP Ports" portlet displays the following data:

Port	SPP	Direction	Drops	Events
------	-----	-----------	-------	--------

Local Logs - Graphs

- Attack Graphs



Local Logs - Snapshot Diagnostics

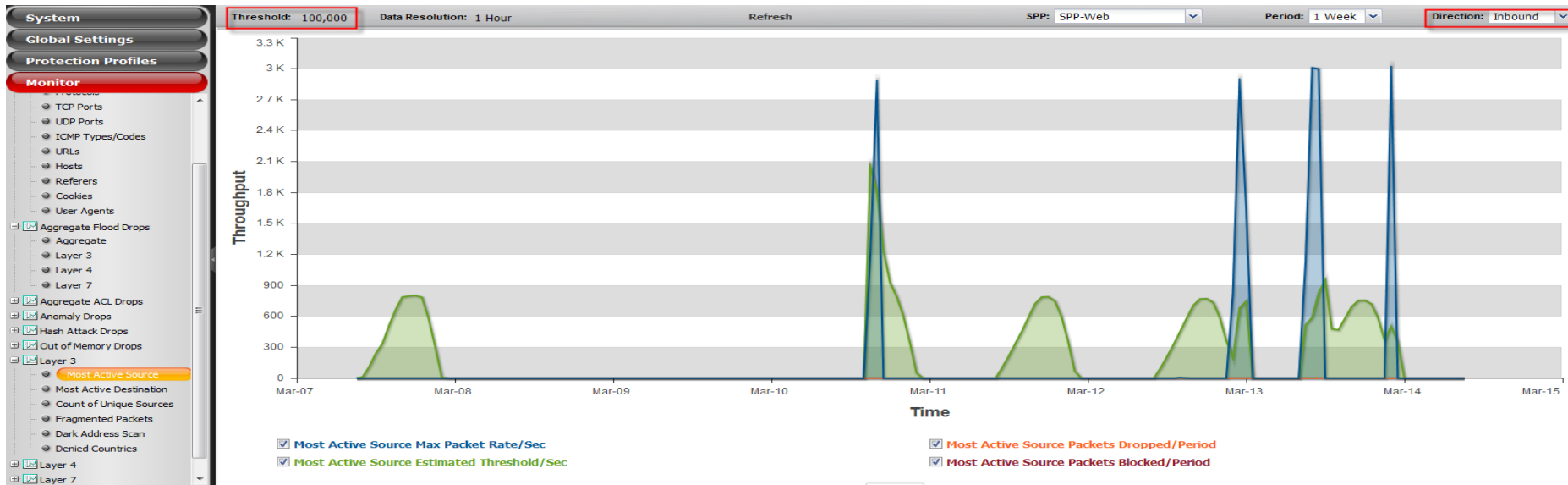
• Diagnostics

System		SPP: SPP-0				
Global Settings						
Protection Profiles						
Monitor						
Log & Report						
Log Configuration						
Log Access						
Report Configuration						
Report Browse						
Attack Graphs						
Diagnostics						
Sessions						
Sources						

Source Diagnostics						
Due to inherent ephemeral nature of high speed traffic, the data in the Source Diagnostics is not always accurate and timely. Use due caution and judgment.						
Filter Settings	Proxy IP	Apply flag: <input type="radio"/> Allowed <input type="radio"/> Blocked <input type="radio"/> Denied <input checked="" type="radio"/> None			Submit	Refresh Data
#	SPP	Source IP Address	Direction	Connections Per Source	Drop Count	
1	SPP-0	10.0.0.2	Inbound	100	0	
2	SPP-0	67.158.188.219	Inbound	-	1	
3	SPP-0	115.89.233.16	Inbound	-	1	
4	SPP-0	12.80.137.220	Inbound	-	1	
5	SPP-0	213.151.84.9	Inbound	-	1	
6	SPP-0	57.248.59.225	Inbound	-	1	
7	SPP-0	89.89.119.216	Inbound	-	1	
8	SPP-0	107.130.200.72	Inbound	-	1	
9	SPP-0	207.143.81.106	Inbound	-	1	
10	SPP-0	19.177.183.247	Inbound	-	1	
11	SPP-0	14.166.103.49	Inbound	-	1	
12	SPP-0	110.178.31.228	Inbound	-	1	
13	SPP-0	10.98.120.168	Inbound	-	1	
14	SPP-0	119.179.87.167	Inbound	-	1	
15	SPP-0	140.105.93.237	Inbound	-	1	
16	SPP-0	236.16.115.242	Inbound	-	1	
17	SPP-0	106.14.110.18	Inbound	-	1	
18	SPP-0	5.194.31.23	Inbound	-	1	
19	SPP-0	153.121.37.81	Inbound	-	1	
20	SPP-0	197.231.183.26	Inbound	-	1	
21	SPP-0	173.251.31.9	Inbound	-	1	

Local Logs - Internal Graphs

- Monitor Graphs



REST API



- REST API



cURL client
GET, POST, PUT, DELETE

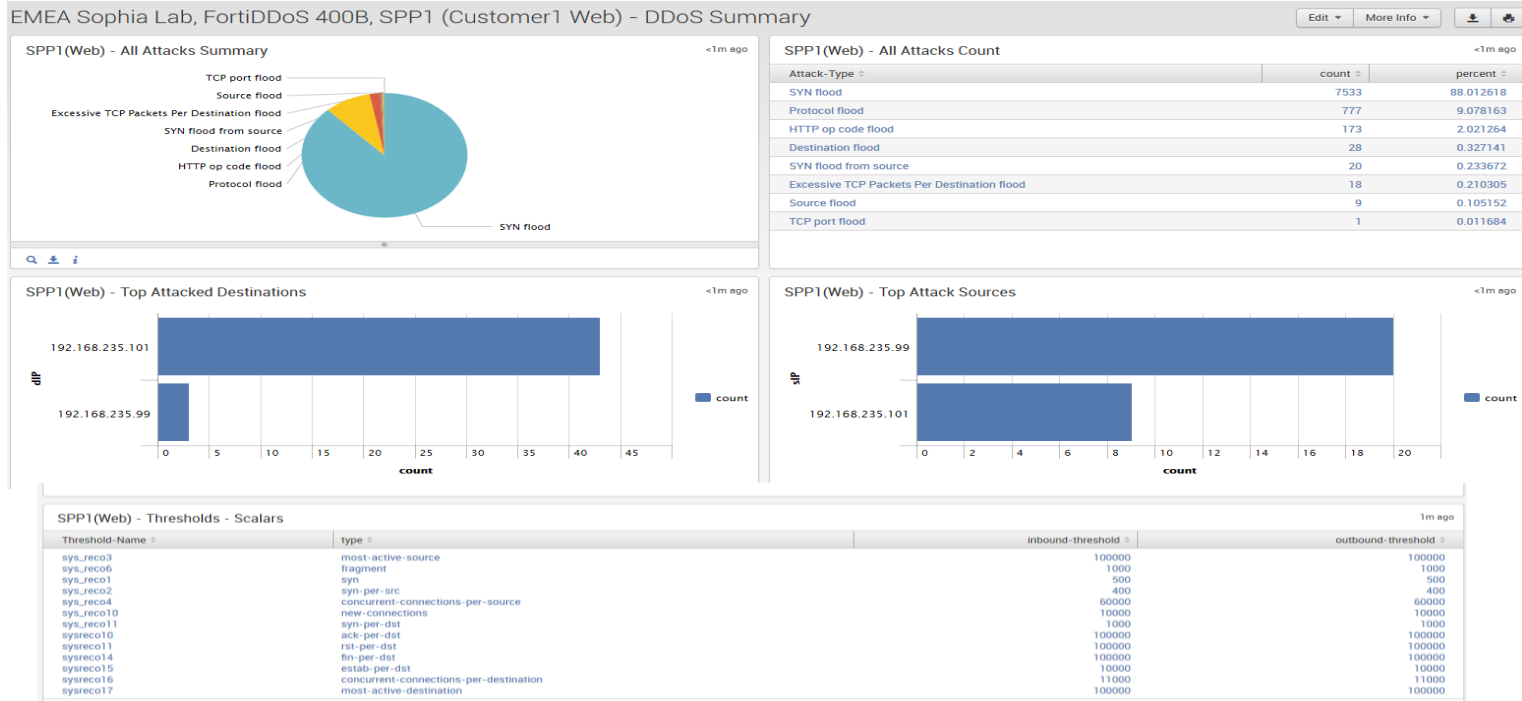


GET Example **curl -u admin: http://192.168.234.77/api/v1/spp/SPP-Web/ddos_spp_threshold_scalar/**

```
{"query": "full", "success": true, "message": "data generated", "data": [{"mkey": "sys_reco3", "type": "most-active-source", "inbound-threshold": "100000", "outbound-threshold": "100000"}, {"mkey": "sys_reco6", "type": "fragment", "inbound-threshold": "1000", "outbound-threshold": "1000"}, {"mkey": "sys_reco1", "type": "syn", "inbound-threshold": "500", "outbound-threshold": "500"}, {"mkey": "sys_reco2", "type": "syn-per-src", "inbound-threshold": "400", "outbound-threshold": "400"}, {"mkey": "sys_reco4", "type": "concurrent-connections-per-source", "inbound-threshold": "60000", "outbound-threshold": "60000"}, {"mkey": "sys_reco10", "type": "new-connections", "inbound-threshold": "10000", "outbound-threshold": "10000"}, {"mkey": "sys_reco11", "type": "syn-per-dst", "inbound-threshold": "1000", "outbound-threshold": "1000"}, {"mkey": "sysreco10", "type": "ack-per-dst", "inbound-threshold": "100000", "outbound-threshold": "100000"}, {"mkey": "sysreco11", "type": "rst-per-dst", "inbound-threshold": "100000", "outbound-threshold": "100000"}, {"mkey": "sysreco14", "type": "fin-per-dst", "inbound-threshold": "100000", "outbound-threshold": "100000"}, {"mkey": "sysreco15", "type": "estab-per-dst", "inbound-threshold": "10000", "outbound-threshold": "10000"}, {"mkey": "sysreco16", "type": "concurrent-connections-per-destination", "inbound-threshold": "1000", "outbound-threshold": "1000"}, {"mkey": "sysreco17", "type": "most-active-destination", "inbound-threshold": "100000", "outbound-threshold": "100000"}]}
```

3rd Party Logging Integration

• SYSLOG, SNMP and REST API allow for easy integration into 3rd Party Management, Logging and Reporting Systems





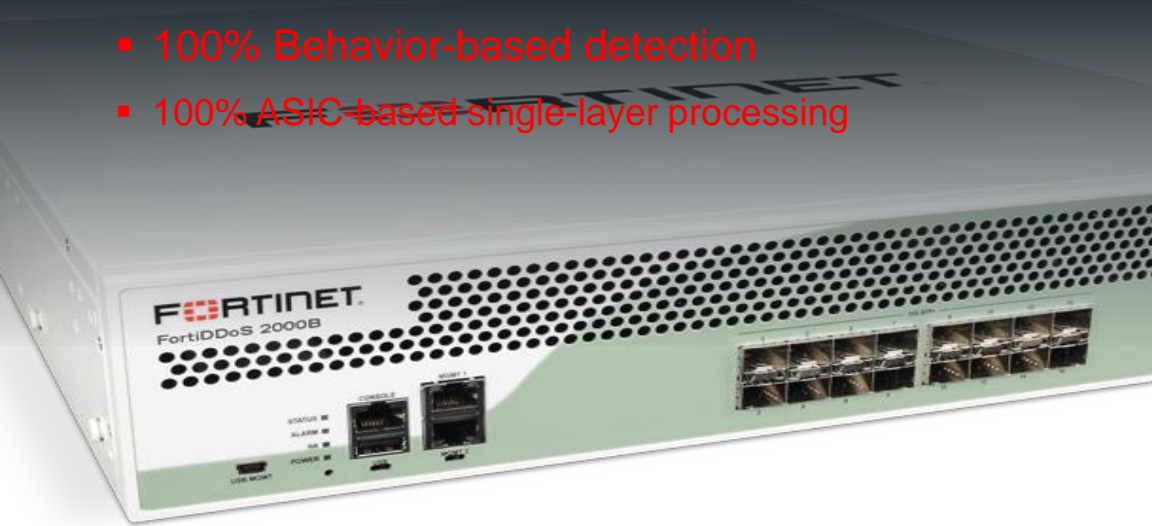
Platforms



April 3, 2015

FortiDDoS – DDoS Attack Mitigation Appliances

- All new FortiDDoS B-Series
- 5 models with 2-37.8 Gbps bi-directional throughput
- Up to 20x 10GE SFP+ ports (4 bypass)
- 100% Behavior-based detection
- 100% ASIC-based single-layer processing



- Up to 6x FortiASIC-TP2 processors
- <50 microsecond latency
- <2 second DDoS mitigation response time
- Adaptive line rating
- Automatic learning process
- IP Reputation scoring
- Geo-location ACLs
- Continuous threat evaluation
- Full CLI and easy to use GUI
- RESTful API
- Advanced analysis and reporting

FortiDDoS B-Series



FortiDDoS-200B

- 4x GE LAN/8x GE WAN
- 2 Gbps bi directional
- 1 M Connections
- 100 K/sec setup/teardown
- 1x FortiASIC-TP2



FortiDDoS-400B

- 8x GE LAN/8x GE WAN
- 6.1 Gbps bi directional
- 1 M Connections
- 100 K/sec setup/teardown
- 1x FortiASIC-TP2



FortiDDoS-800B

- 8x GE LAN/8x GE WAN
- 13.2 Gbps bi directional
- 2 M Connections
- 200 K/sec setup/teardown
- 2x FortiASIC-TP2



HIGH END



FortiDDoS-1000B

- 8x 10GE LAN/8x 10GE WAN
- 18.4 Gbps bi directional
- 3 M Connections
- 300 K/sec setup/teardown
- 3x FortiASIC-TP2



FortiDDoS-2000B

- 8x 10GE LAN/8x 10GE WAN
- 4x 10GE LAN/WAN bypass
- 37 Gbps bi directional
- 6 M Connections
- 600 K/sec setup/teardown
- 6x FortiASIC-TP2

MID-RANGE

TARGET SEGMENTS/VERTICALS

- Financial Services
- Government
- Enterprise/Internet Datacenters
- Web Hosting Providers
- MSPs

FORTINET®