

## **0** DDoS Protection

---

## **1** Security Report 2013

---

## **2** Mobile Data Protection

---

## **3** Threat Prevention

---

## **4** Tufin Security Suite

---



**Check Point®**

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

---

# Check Point DDoS Protector

Peter Kovalcik

SE Eastern Europe

[pkovalcik@checkpoint.com](mailto:pkovalcik@checkpoint.com)



**1**

## DDoS Trends

---

**2**

## Overview DDoS 2.0

---

**3**

## Check Point DDoS Protector

---

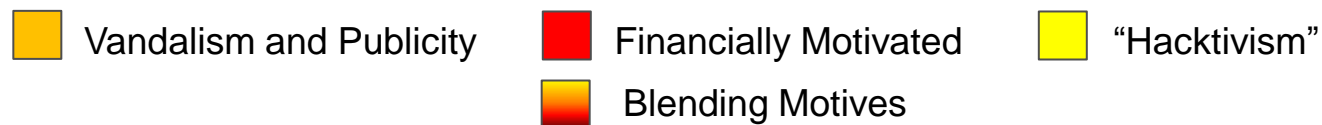
# What is an DoS Attack?

Denial-of-Service attack (DoS attack) an attempt to make a machine or network resource unavailable to its intended users.

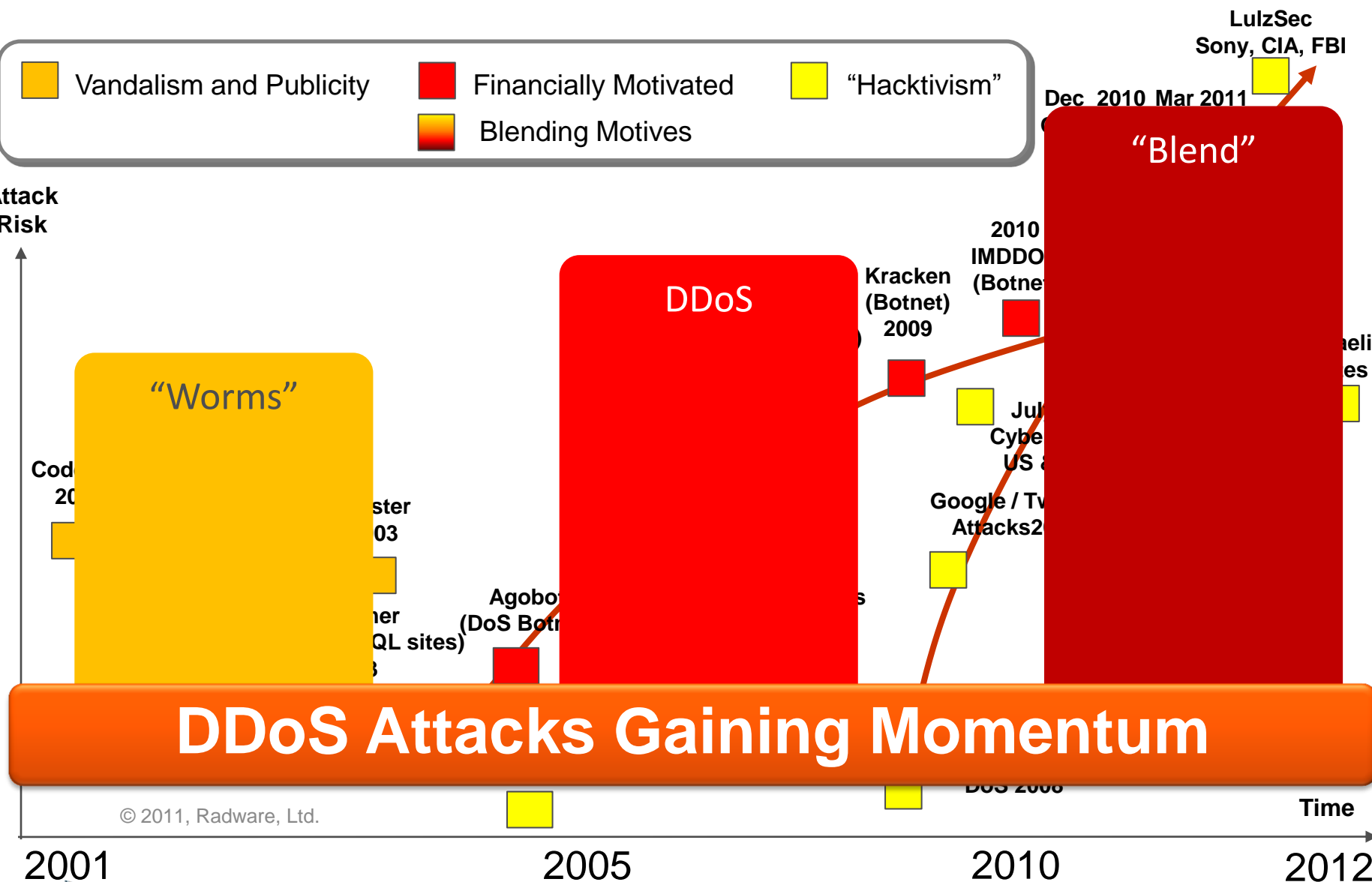
Distributed Denial-of-service attack (DDoS) is coordinated and simultaneously launched from multiple sources



# DDoS Timeline—Summary Graph



Attack Risk



© 2011, Radware, Ltd.

2001

2005

2010

2012



softwareblades™

lidovky.cz

iDNES.cz



www  
zive

Novinky.cz





## Attacks can be partitioned into three dimensions



**Network DoS  
Attack**

Consuming  
bandwidth  
resources



**Application flood  
DoS attacks**

Target the  
application  
resources

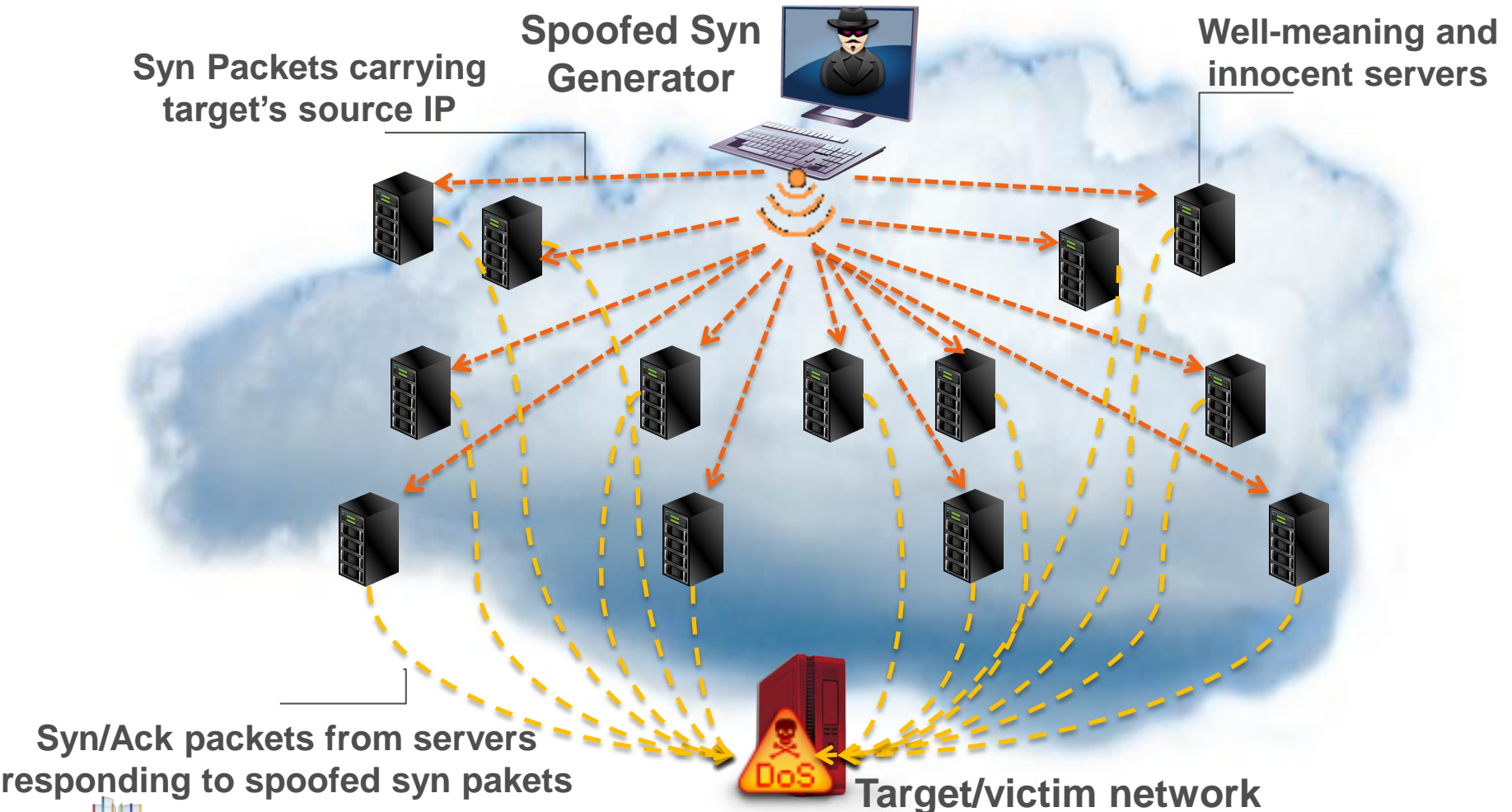


**Directed application  
DoS attacks**

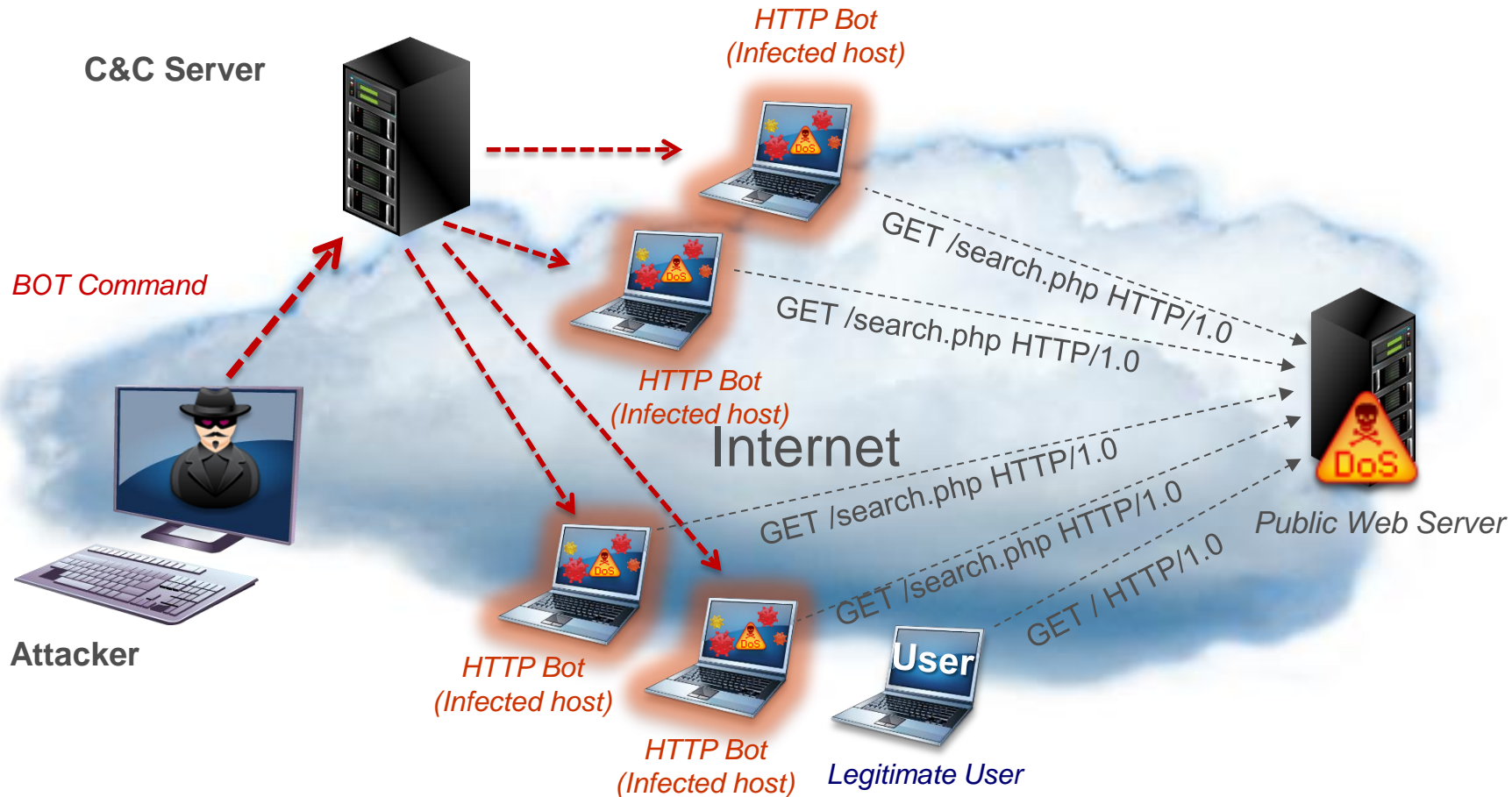
Exploit application  
implementation  
weaknesses



## Network Flood DoS Attack



## Application DDoS flood attacks



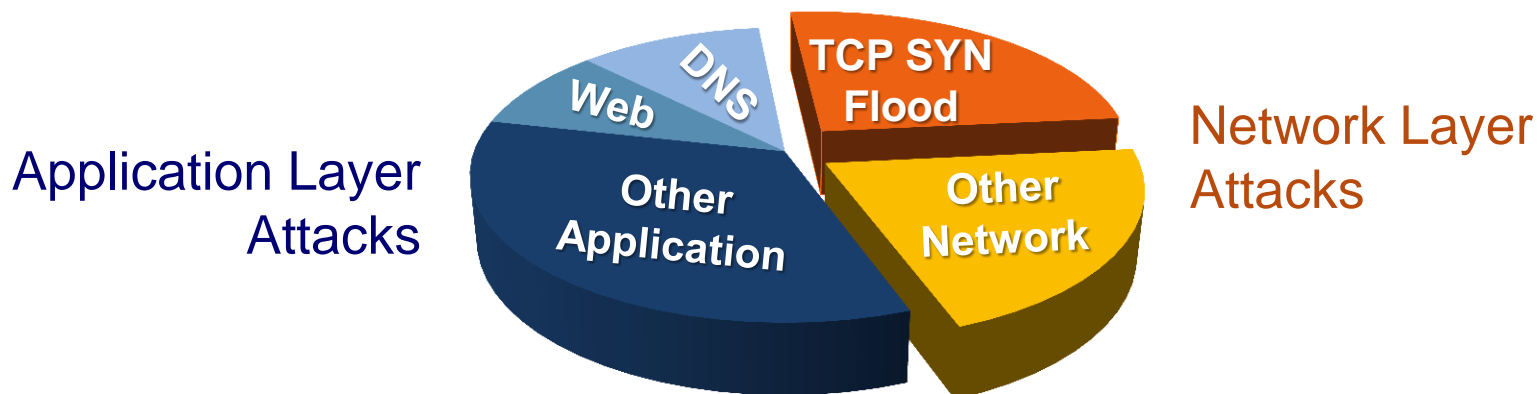
## Directed attacks (Low & Slow Attack)



```
GET / HTTP/1.1 CRLF
Host: www.example.com CRLF
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322;
.NET CLR 2.0.50313; .NET CLR 3. 0.4506.2152;
.NET CLR 3.5.30729; MSOffice 12) CRLF
Content-Length: 42 CRLF
.....
```

**The request is missing the final CRLF that tells the destination web server that the request has completed**

# DDoS Attack by Types



**More attacks are targeted at the application layer**

1

DDoS Trends

---

2

**Overview DDoS 2.0**

---

3

Check Point DDoS Protector

---

# DDoS Tool Anyone Can Use

## Example HOIC Attack Request #1

```
// E
GET / HTTP/1.0
Accept: */*
Accept-Language: en
Referer: http://www.hoic_target_site.com/
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1; .NET CLR 1.1
If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT
```

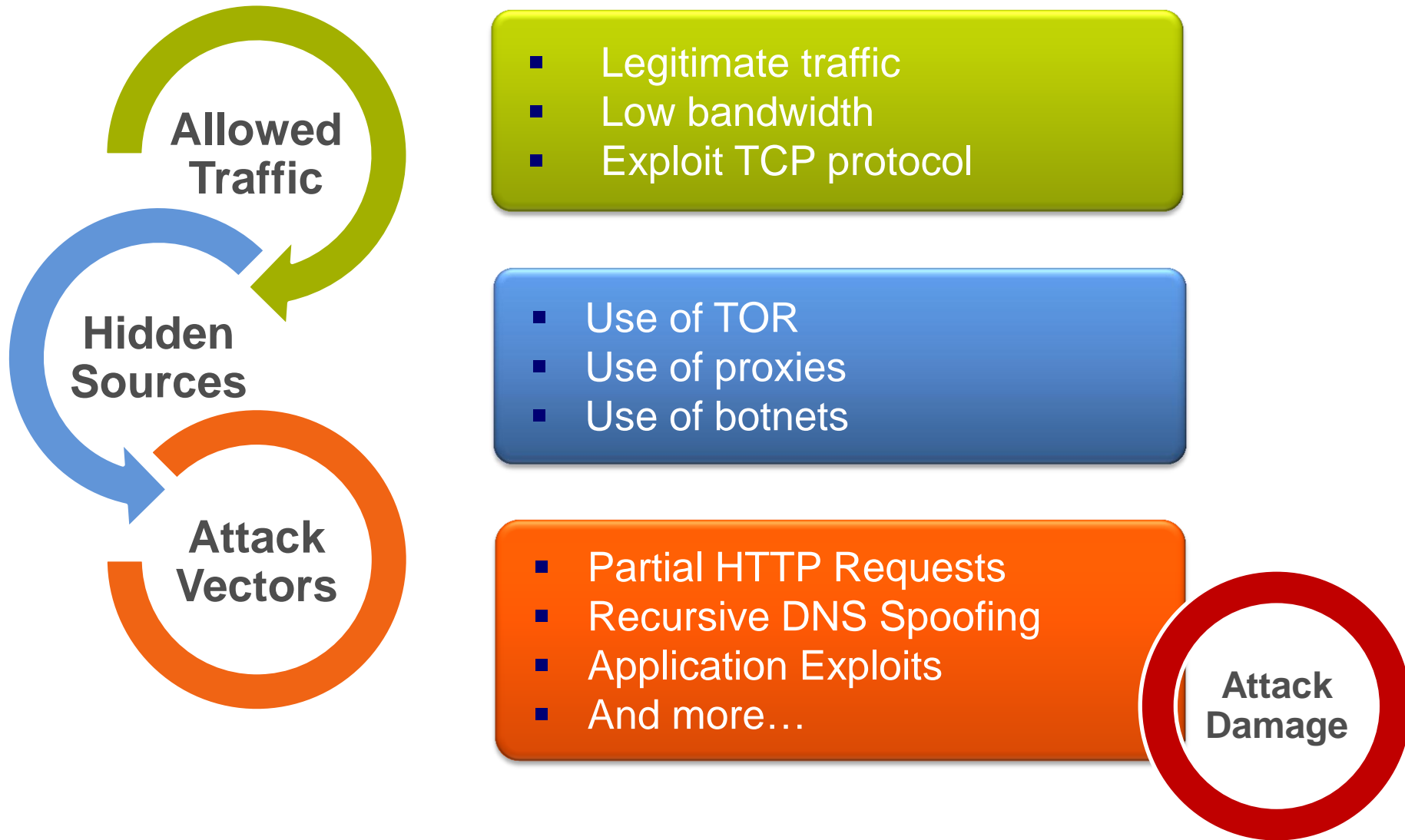
## Example HOIC Attack Request #2

```
// ge
GET / HTTP/1.0
Heade Accept: */*
// ge Accept-Language: en
Heade Referer: http://www.yahoo.com/
// Ge User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534
Heade If-Modified-Since: Tue, 18 Aug 2003 12:54:49 GMT
Host: www.hoic_target_site.com
```

- Simple Interface
- Focused Payload
- Script - Killer Attacks
- Simple Scripting
- Randomize Attacks
- Difficult Detection



# Layer 7 DoS Attacks





Allowed  
Traffic

## Services need to allow traffic

### Legitimate Traffic

- Use proper ports (Port 80)
- Use correct services (HTTP)
- Use allowed applications (media streaming)

### Low Bandwidth

- Few packets from attacker
  - Results in many packets from target
- Attacker: Get HTTP/1.0 (example)
  - Target: Sends megabytes of data

### Exploit TCP/IP Protocol

- Flag to fragment packets
- Set maximum packet size to 100 bytes
- Send keep-alive to hold connection open





Hidden  
Sources

## Difficult to Block by IP

### Use of TOR

- Hides attacker's IP address
- Creates multiple source IP addresses
- Randomly routed around the world

### Use of Proxies

- Public web proxies
- Email relays (Anonymizer)
- Recursive DNS query—DNS server makes request on behalf of client

### Use of Botnet

- Amplifies attack
- Attack from many locations
- Can rent as needed

## Attack Vectors

### More Disruptive with Fewer Packets

#### Partial HTTP Requests

1. Start HTTP(S) Get
2. Set fragment flag to slow server reply
3. Keep connection alive
4. Never complete request

#### Recursive DNS Spoofing

1. Spoof recursive DNS queries aimed at target (send to many public DNS servers)
2. Public DNS servers forward queries to target
3. Target replies many bytes to bad IP addresses

#### Application Exploits

1. Wildcard search with hidden function/bug
2. Outputs large amounts of data (Gigabytes)
3. Set fragment flag to slow server reply
4. Attempt to send all data to "clients"



**Attack  
Damage**

## Crashes Servers and Services

### Partial HTTP Requests

- Server unable to make new connections
- Server will run low on memory
- All server responses slow
- Server and services might crash

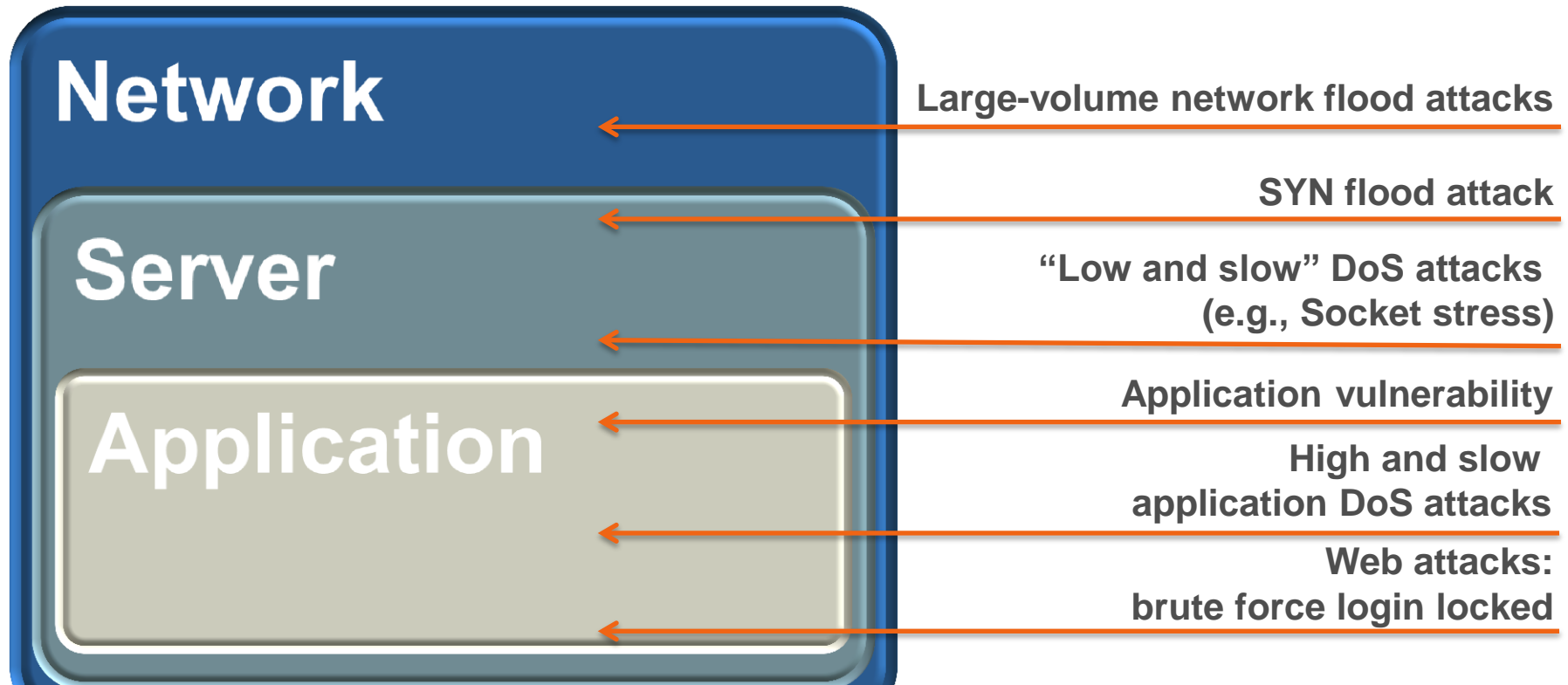
### Recursive DNS Spoofing

- Target DNS servers will be very busy
- Will disrupt domain name resolution
- Will have browsing and email issues

### Application Exploits

- Services can crash
- Processor 100% utilized
- Disk 100% utilized
- All server responses slow

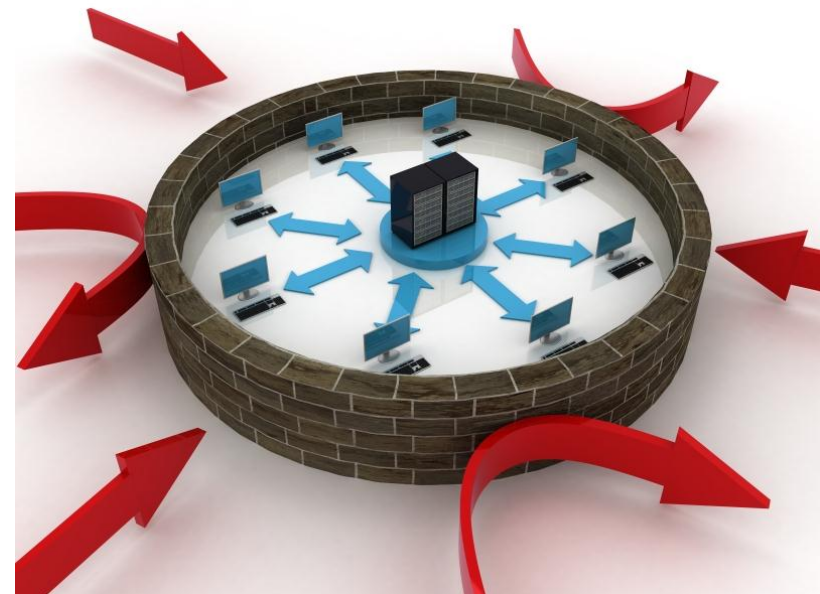
## Simultaneous Attack Vectors



1 successful attack vector = No service

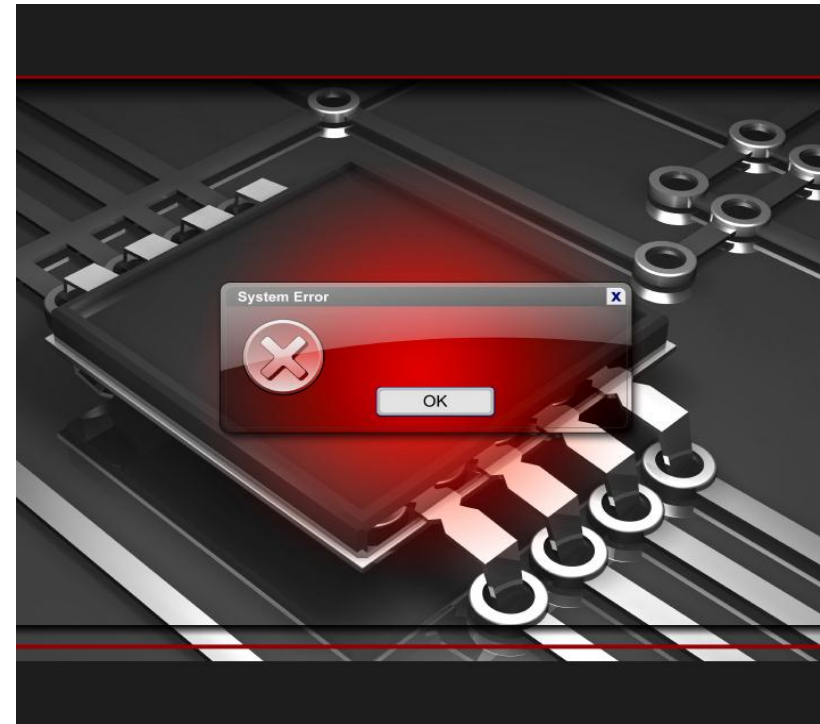
## Attackers Take Advantage of Traditional Security

- Routers may be affected before firewalls
- Firewalls track state of network connections (Can be bottleneck)
- Firewalls allow legitimate traffic (e.g. port 80 to web server)
- IPS allows legitimate request (e.g. get http/1.0\r\n)
- Application Control allows legitimate services (DNS or HTTPS)



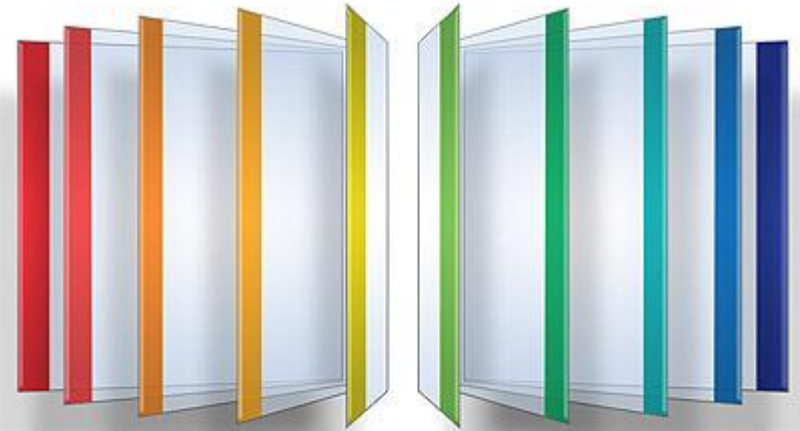
## Not Designed for Network and Application DDoS Protection

- Basic rate based flood protection affects all traffic (Real users and attack traffic)
- Lacks Comprehensive Layer 7 DDoS protection
  - Poor detection of sly attacks
  - No filters to block attacks and allow real traffic
  - Administrators cannot create custom signatures



# What Software Blades Can Do

- Firewall configurations: network access control
  - Aggressive aging: protection against connection-consuming attacks
  - Network quota: limit number of connections by source IP
  - ICMP/UDP perimeter, initial drop rules: drop early in policy
  - Lower Stateful Inspection timers: defense against slow attack
- IPS configurations: proactive intrusion prevention
  - Geo protection: Rules to block by country and direction of traffic
  - Worm catcher signature: block known worms (HTTP and CIFS)
  - TCP window size enforcement: small TCP window and flood
  - SYN flood protection: cookie-based validation
  - HTTP flooding: rate-based blocking
- SmartEvent and SmartLog: improved visibility and forensics



**1**

DDoS Trends

---

**2**

Overview DDoS 2.0

---

**3**

**Check Point DDoS Protector**

---



# Introducing Check Point **Check Point DDoS Protector™**



**Block Denial of Service Attacks within seconds!**

# Check Point DDoS Protector

**Customized  
multi-layered  
DDoS  
protection**

**Fast  
response  
time—protect  
within  
seconds**

**Flexible  
deployment  
options**

**Integrated  
with Check  
Point security  
management**



# DDoS Protector Product Line



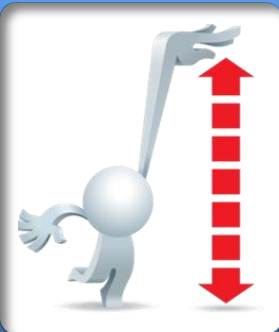
## Enterprise Grade

- Up to 3 Gbps throughput
- 2M concurrent sessions
- 1 Mpps max. DDoS flood attack rate



## Datacenter Grade

- Up to 12 Gbps throughput
- 4M concurrent sessions
- 10 Mpps max. DDoS flood attack rate



- 7 models to choose from
- 1GbE copper and 10GbE fiber connections
- Low latency

# DDoS Attack Information

## Network Flood



High volume of  
packets

## Server Flood



High rate of  
new sessions

## Application



Web / DNS  
connection-  
based attacks

## Low & Slow Attacks



Advanced  
attack  
techniques

# Multi-Layer DDoS Protection

**Network Flood**

**Server Flood**

**Application**

**Low & Slow  
Attacks**



**Behavioral  
network  
analysis**

**Automatic and  
pre-defined  
signatures**

**Behavioral  
HTTP and  
DNS**

**Granular  
custom filters**

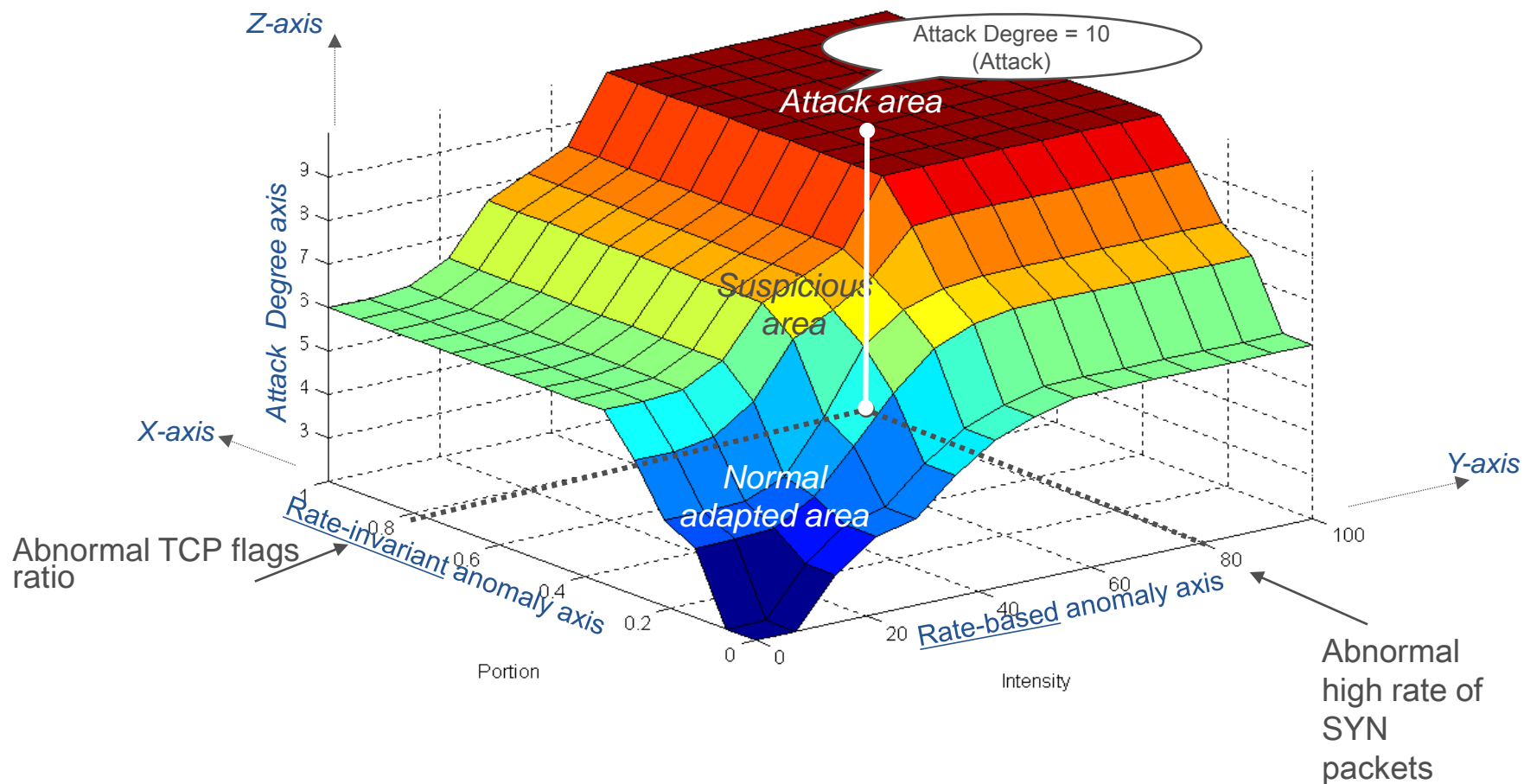
Stateless and  
behavioral  
engines

Protections  
against misuse  
of resources

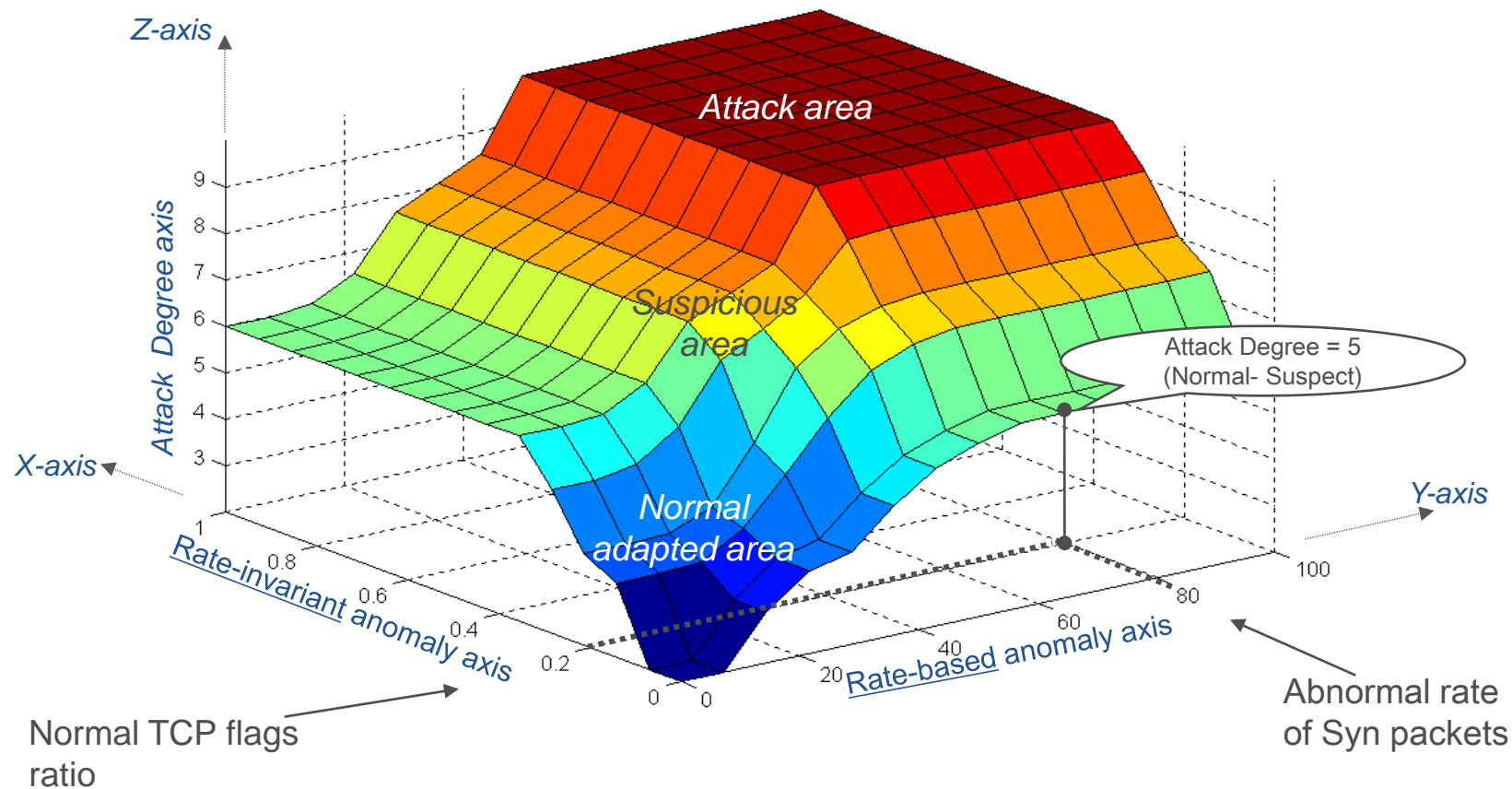
Challenge /  
response  
mitigation  
methods

Create filters that  
block attacks  
and allow users

## SYN flood

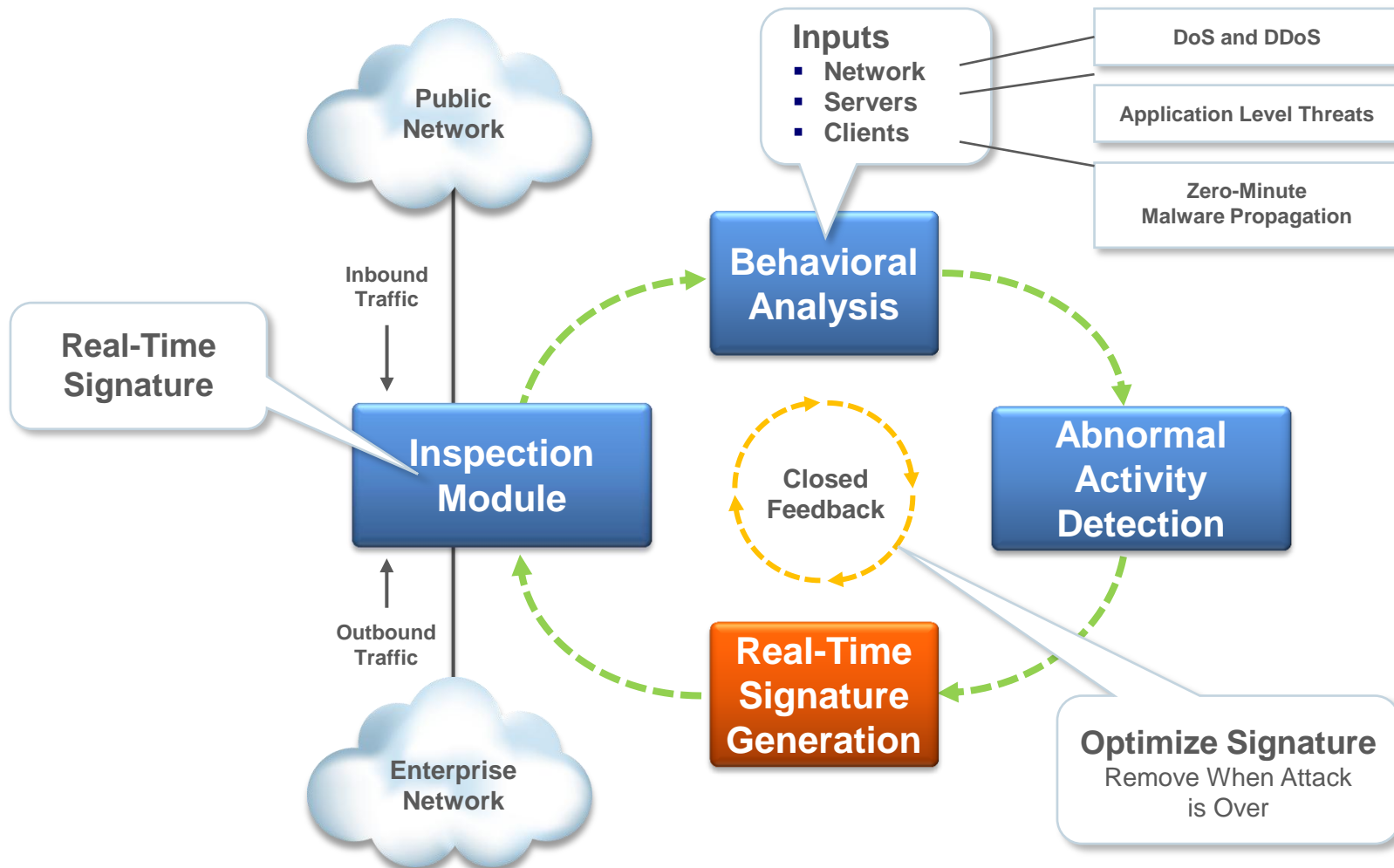


## Flash crowd





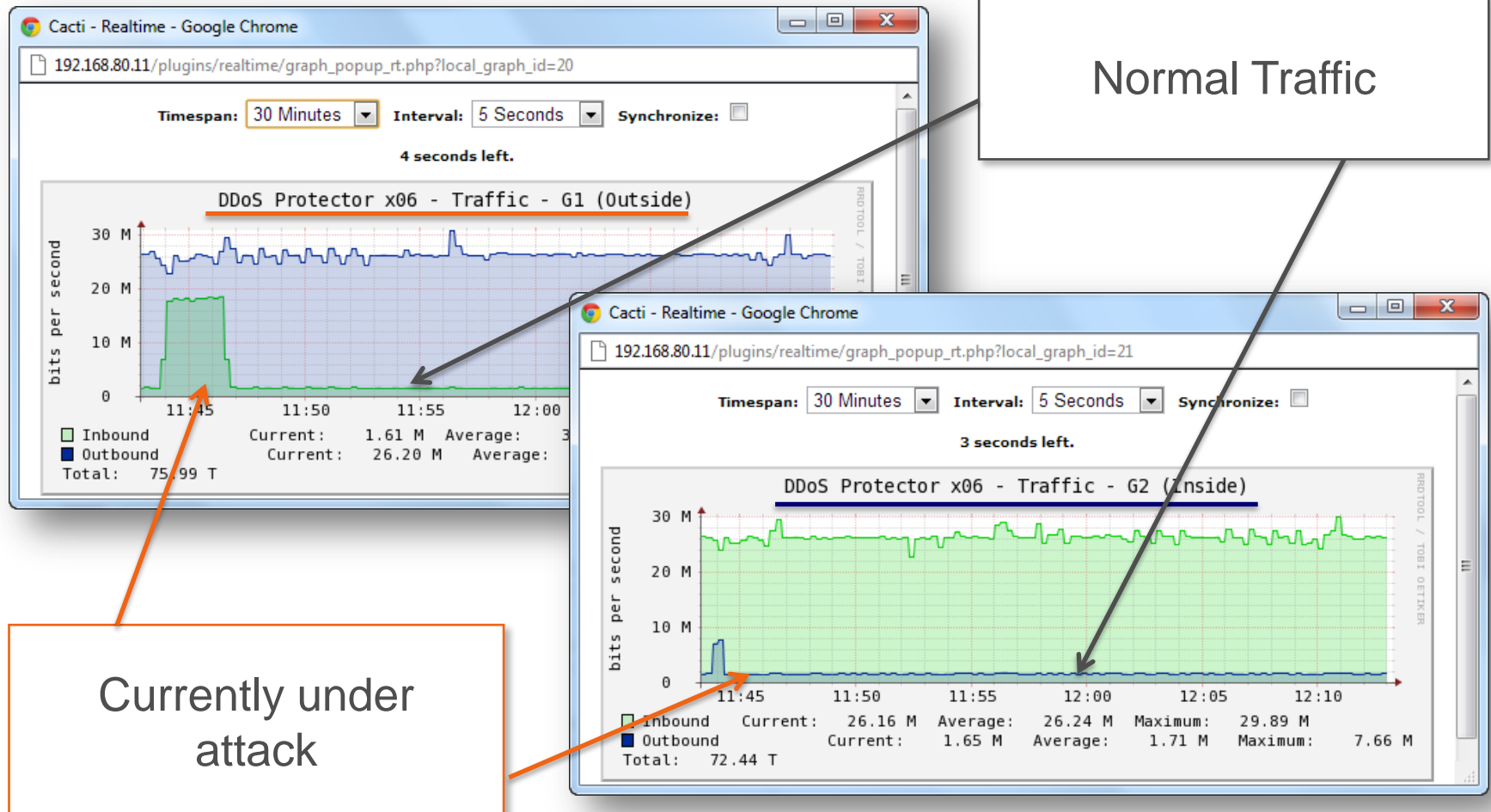
## Protect Applications and Services Automatically





# Real time monitoring with SNMP

- This realtime monitoring is achieved with CactiEZ delivered under GPL.



**Ready to Protect in Minutes**

**Fits to Existing Network Topology**

**Optional Learning Mode Deployment**

**Low Maintenance and Support**



## Scenarios:

1

2

3

**Transparent network device easily fits into existing network topology (layer 2 bridge)**



**Off-Site Deployment**



**DDoS Security Appliance**

# Simple Deployment



1. Plug it in...
2. Let it learn...
3. Protected by signatures



No network  
address changes  
(Layer 2 bridge)



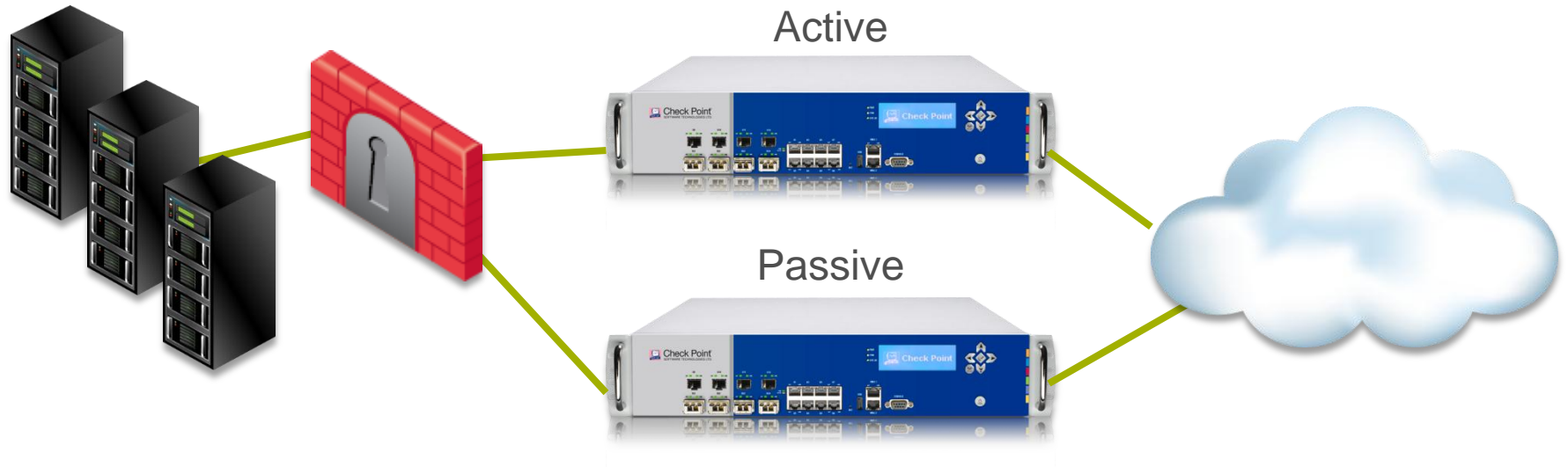
Baseline good  
network and  
application  
behavior



Signatures are  
ready to protect

**Ready to protect any size network in minutes**

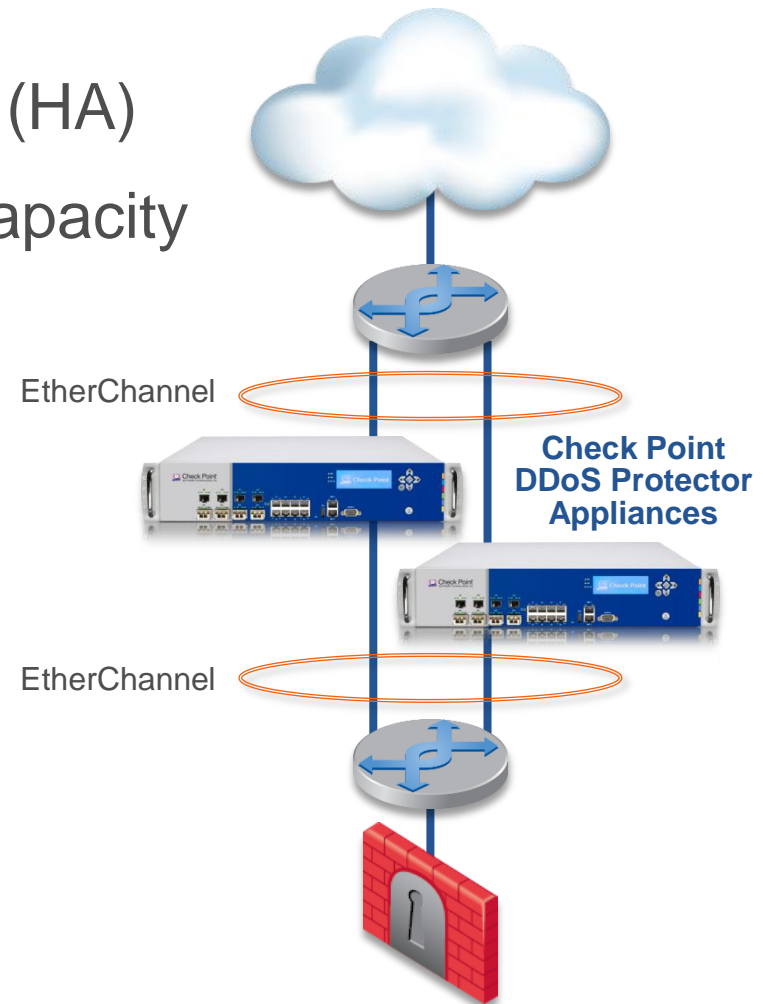
# High-Availability DDoS Protector



- High availability (HA): 2 compatible devices in a two-node cluster
- Compatibility: Same platform, software version, software license, throughput license, and signatures
- Device identification: Primary device is active and secondary device is passive
- When placed in HA: Primary device transfers configuration objects to secondary device
- When updated: Primary device immediately transfers changes to secondary device

## EtherChannel Solution for Additional Capacity

- Not active-active High Availability (HA)
- Each additional appliance adds capacity
- Appliances can have different
  - Software version
  - Software license
  - Throughput license
  - Signatures





## Inspect Traffic Within Tunnels

- L2TP (Layer 2 Tunneling Protocol)
- GRE (Generic Routing Encapsulation)
- GTP (GPRS Tunneling Protocol)
- MPLS (Multi-Protocol Label Switching)
- 802.1q VLAN tagging



# Product Information

							
Model	DP 506	DP 1006	DP 2006	DP 3006	DP 4412	DP 8412	DP 12412
Capacity	0.5Gbps	1Gbps	2Gbps	3Gbps	4GBps	8Gbps	12Gbps
Max Concurrent Sessions	2 Million				4 Million		
Max DDoS Flood Attack Protection Rate	1 Million packets per second				10 Million packets per second		
Latency	<60 micro seconds						
Real-time signatures	Detect and protect against attacks in less than 18 seconds						



## Blocks DDoS Attacks Within Seconds

**Customized  
multi-layered  
DDoS protection**

**Ready to protect  
in minutes**

**Integrated with  
Check Point  
Security  
Management**





**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet.

---

**Thank You**

