Stallion

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

Check Point DDoS Protector Simple and Easy Mitigation

Jani Ekman – janie@checkpoint.com

Sales Engineer

DDoS Protector

1 **(D)DoS Attacks**

2 DDoS Protector

3 Behavioral DoS Protection

4 Summary

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

(D)DoS Attack Methods and Tools

Attacks can be partitioned into three dimensions

Network DoS Attack

Consuming bandwidth resources

Application flood DoS attacks

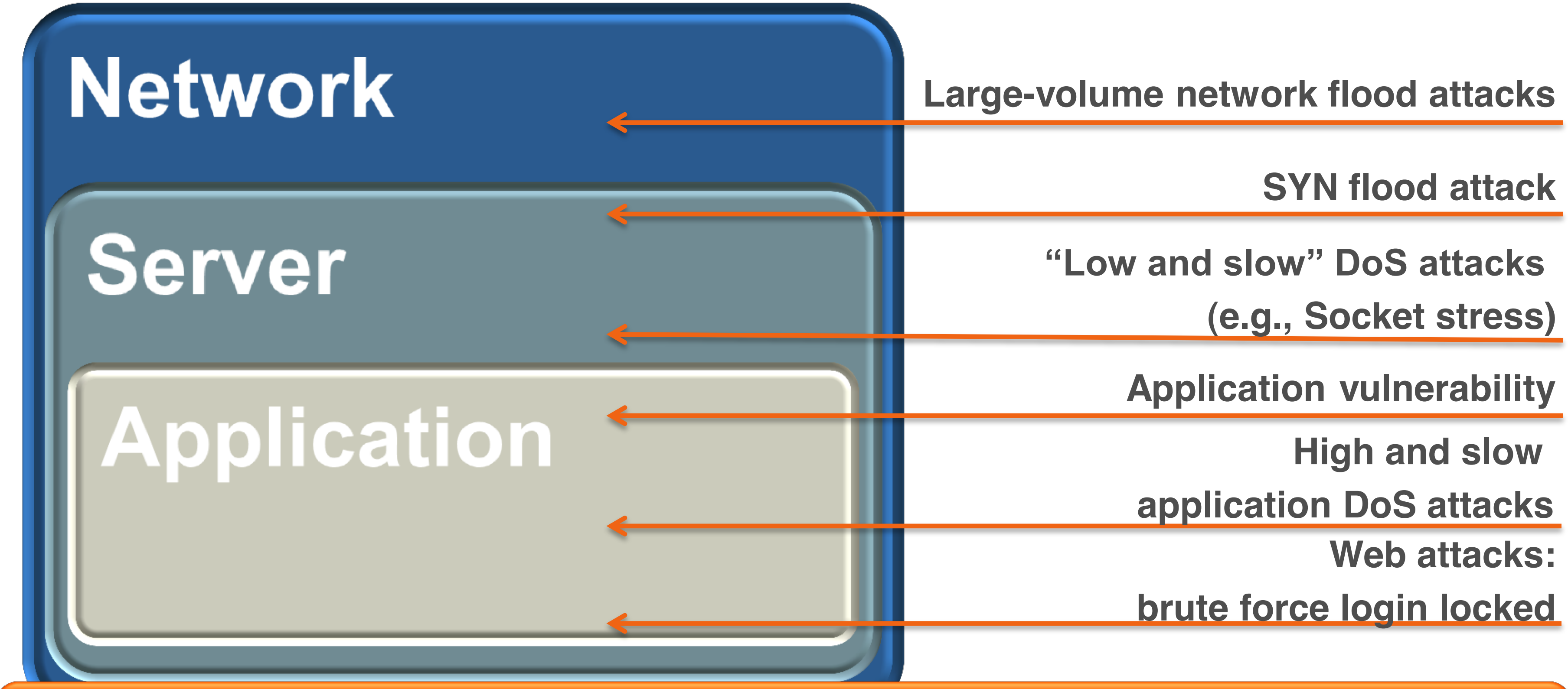
Target the application resources

Directed application DoS attacks

Exploit application implementation weaknesses

Attackers Use Multi-Layer DDoS

Simultaneous Attack Vectors



Network

Server

Application

Large-volume network flood attacks

SYN flood attack

“Low and slow” DoS attacks
(e.g., Socket stress)

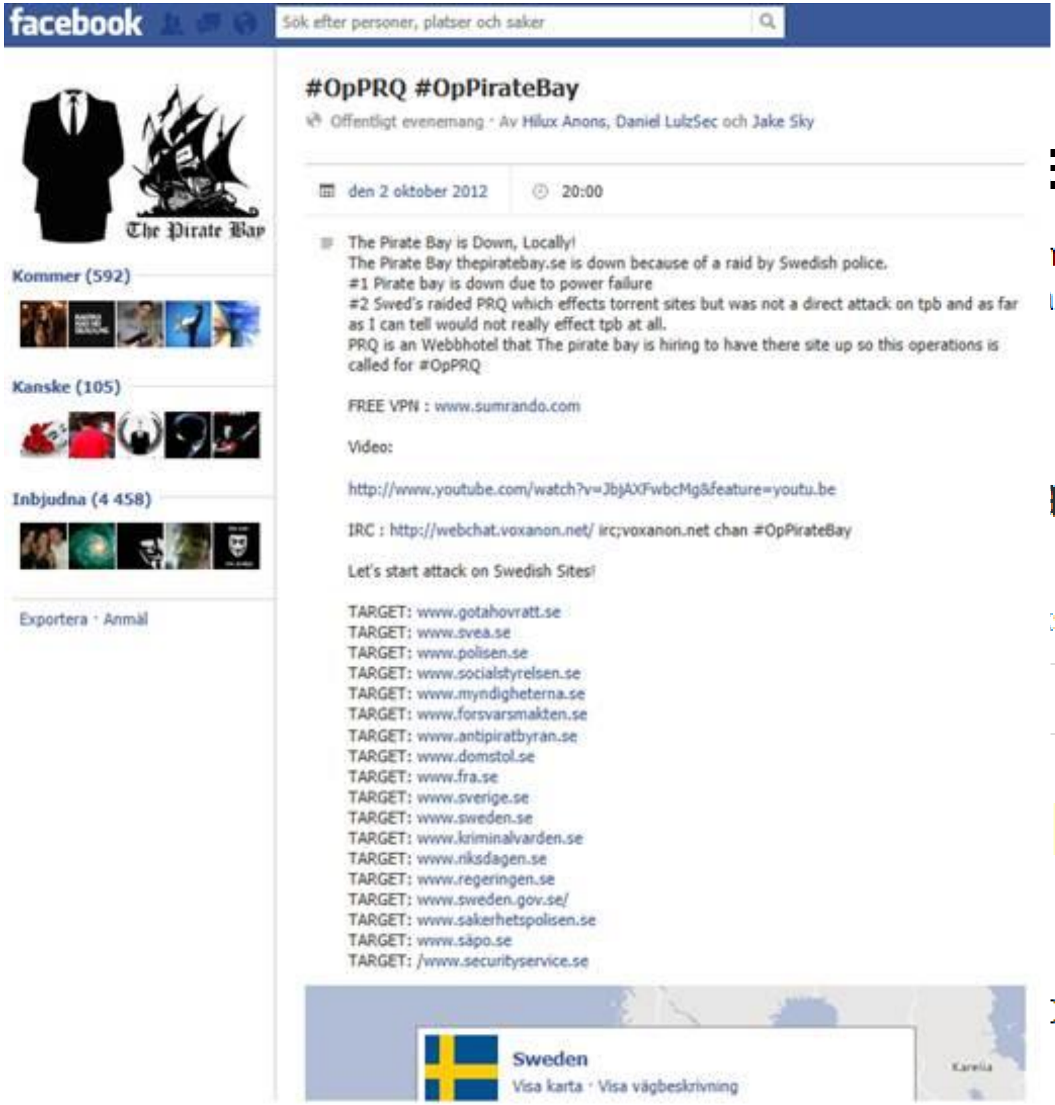
Application vulnerability

High and slow
application DoS attacks

Web attacks:
brute force login locked

1 successful attack vector = No service

Is there any attacks?



#OpPRQ #OpPirateBay

Offentligt evenemang · Av Hilux Anons, Daniel LulzSec och Jake Sky

den 2 oktober 2012 | 20:00

The Pirate Bay is Down, Locally!
The Pirate Bay thepiratebay.se is down because of a raid by Swedish police.
#1 Pirate bay is down due to power failure
#2 Swed's raided PRQ which effects torrent sites but was not a direct attack on tpb and as far as I can tell would not really effect tpb at all.
PRQ is an Webbhotel that The pirate bay is hiring to have there site up so this operations is called for #OpPRQ

FREE VPN : www.sumrando.com

Video:

http://www.youtube.com/watch?v=JbjAXFwbcMg&feature=youtu.be

IRC : http://webchat.voxanon.net/ irc;voxanon.net chan #OpPirateBay

Let's start attack on Swedish Sites!

TARGET: www.gotahovratt.se
TARGET: www.svea.se
TARGET: www.polisen.se
TARGET: www.socialstyrelsen.se
TARGET: www.myndigheterna.se
TARGET: www.forsvarsmakten.se
TARGET: www.antipiratbyran.se
TARGET: www.domstol.se
TARGET: www.fra.se
TARGET: www.sverige.se
TARGET: www.sweden.se
TARGET: www.kriminalvarden.se
TARGET: www.riksdagen.se
TARGET: www.regeringen.se
TARGET: www.sweden.gov.se/
TARGET: www.sakerhetspolisen.se
TARGET: www.säpo.se
TARGET: /www.securityservice.se

Sweden
Visa karta · Visa vägbeskrivning

es under attack

ne Sanoma media group on Tuesday. The sites
lly seen among attack targets, have suffered

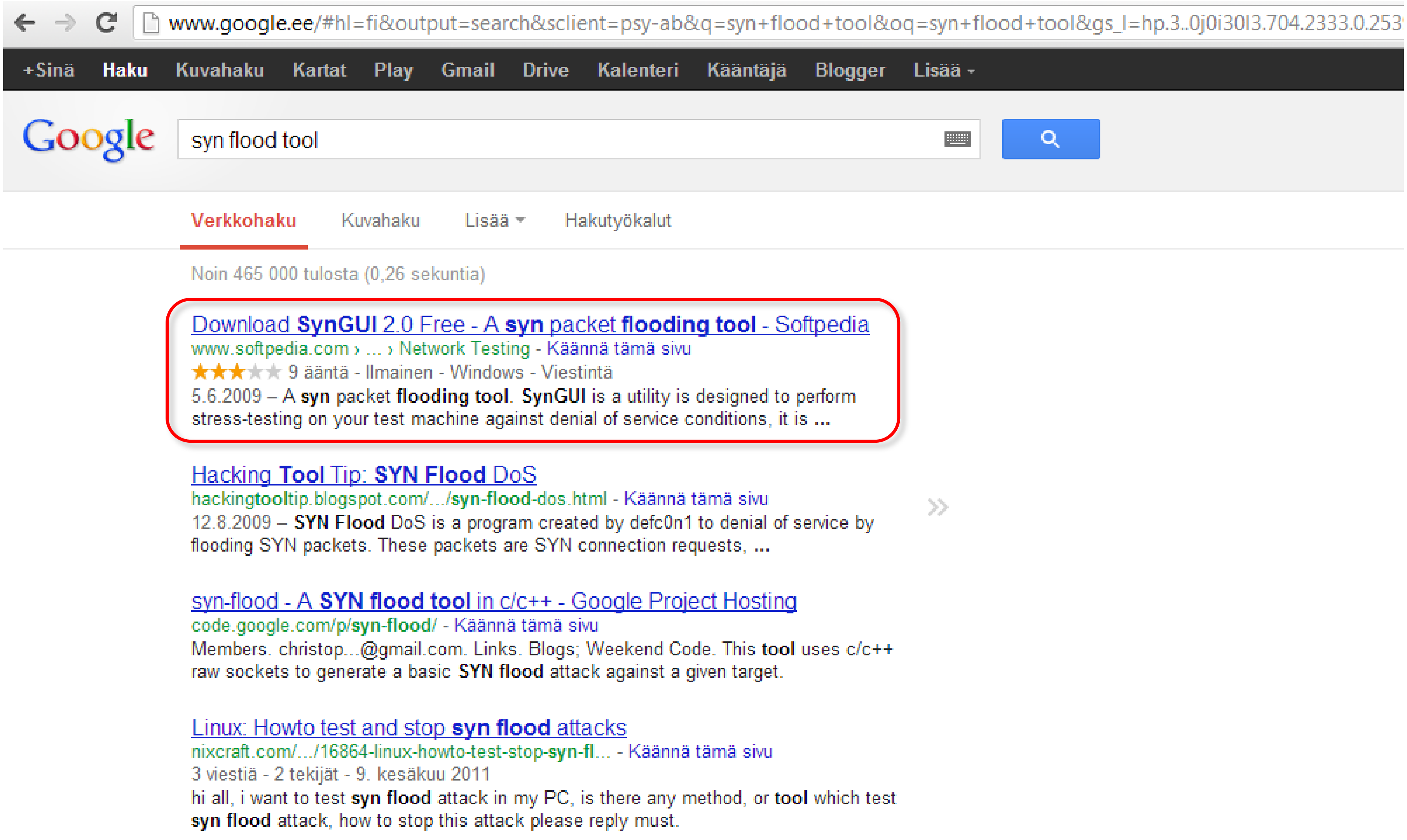
ı; Russia

s bring ...

l of service

Company Yle were the target of a denial

Is there any tools available?



www.google.ee/#hl=fi&output=search&sclient=psy-ab&q=syn+flood+tool&oq=syn+flood+tool&gs_l=hp.3..0j0i30l3.704.2333.0.253

syn flood tool

Noin 465 000 tulosta (0,26 sekuntia)

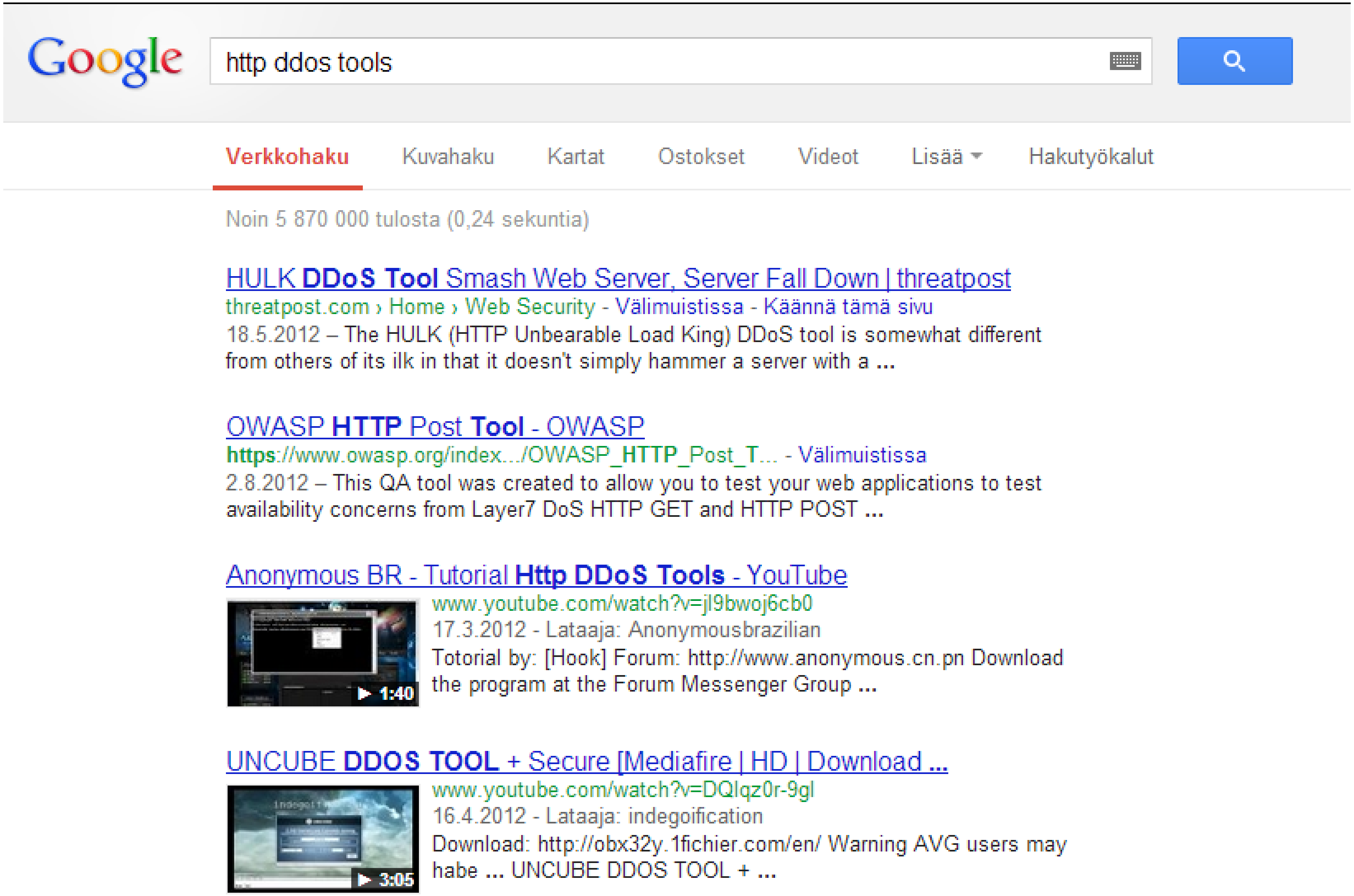
Download **SynGUI** 2.0 Free - A **syn** packet **flooding tool** - Softpedia
www.softpedia.com › ... › Network Testing - Käännä tämä sivu
★★★☆☆ 9 ääntä - Ilmainen - Windows - Viestintä
5.6.2009 – A **syn** packet **flooding tool**. **SynGUI** is a utility is designed to perform stress-testing on your test machine against denial of service conditions, it is ...

Hacking **Tool** Tip: **SYN Flood** DoS
hacking**tool**tip.blogspot.com/.../**syn-flood**-dos.html - Käännä tämä sivu
12.8.2009 – **SYN Flood** DoS is a program created by defc0n1 to denial of service by flooding SYN packets. These packets are SYN connection requests, ...

syn-flood - A **SYN flood tool** in c/c++ - Google Project Hosting
code.google.com/p/**syn-flood**/ - Käännä tämä sivu
Members. christop...@gmail.com. Links. Blogs; Weekend Code. This **tool** uses c/c++ raw sockets to generate a basic **SYN flood** attack against a given target.

Linux: Howto test and stop **syn flood** attacks
nixcraft.com/.../16864-linux-howto-test-stop-**syn-fl**... - Käännä tämä sivu
3 viestiä - 2 tekijät - 9. kesäkuu 2011
hi all, i want to test **syn flood** attack in my PC, is there any method, or **tool** which test **syn flood** attack, how to stop this attack please reply must.

Going for layer 7



http ddos tools

Noin 5 870 000 tulosta (0,24 sekuntia)

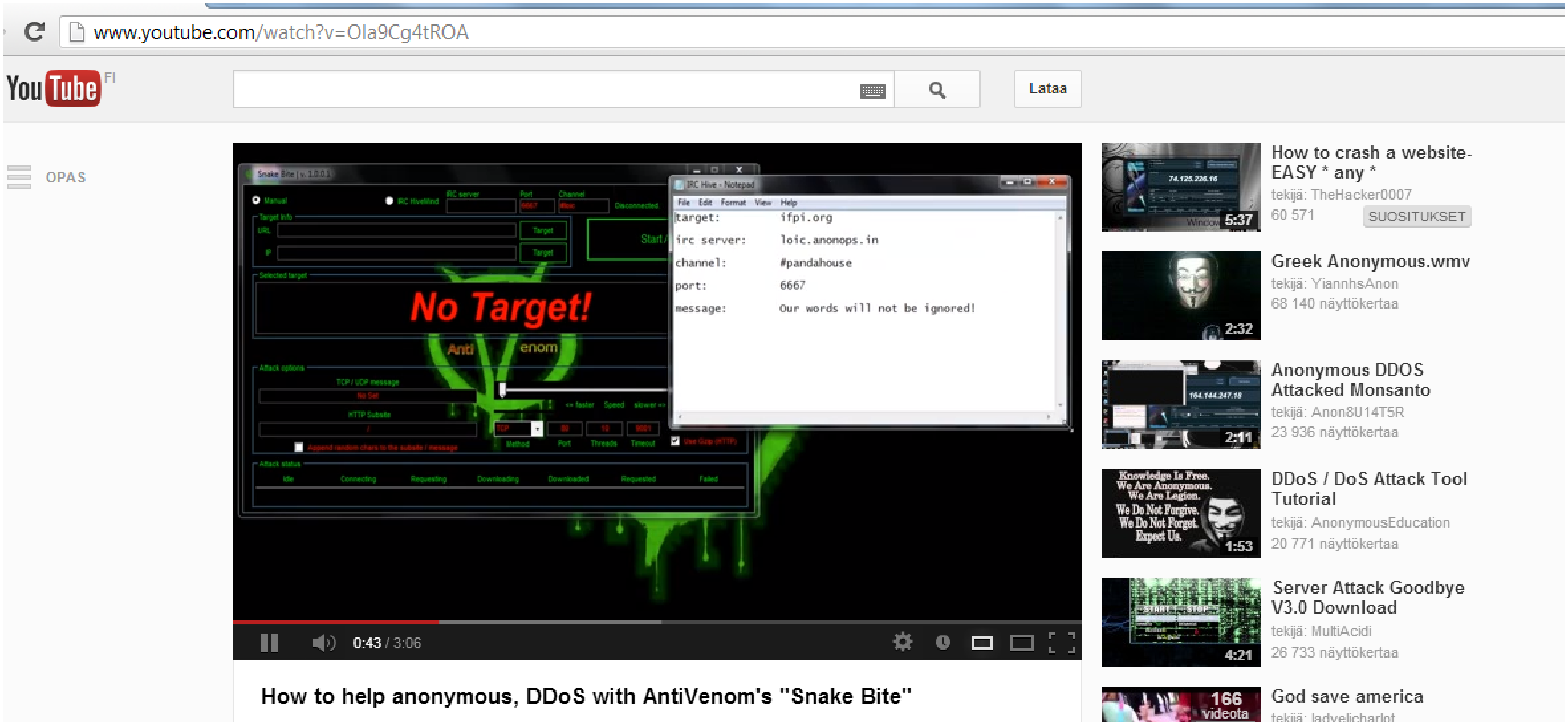
HULK DDoS Tool Smash Web Server, Server Fall Down | threatpost
threatpost.com › Home › Web Security - Välimuistissa - Käännä tämä sivu
18.5.2012 – The HULK (HTTP Unbearable Load King) DDoS tool is somewhat different from others of its ilk in that it doesn't simply hammer a server with a **...**

OWASP **HTTP** Post **Tool** - OWASP
https://www.owasp.org/index.../OWASP_**HTTP**_Post_T... - Välimuistissa
2.8.2012 – This QA tool was created to allow you to test your web applications to test availability concerns from Layer7 DoS HTTP GET and HTTP POST **...**

Anonymous BR - Tutorial **Http DDoS Tools** - YouTube
www.youtube.com/watch?v=jI9bwoj6cb0
17.3.2012 - Lataaja: Anonymousbrazilian
Totorial by: [Hook] Forum: http://www.anonymous.cn.pn Download the program at the Forum Messenger Group **...**

UNCUBE **DDOS TOOL** + Secure [Mediafire | HD | Download **...**
www.youtube.com/watch?v=DQIqz0r-9gl
16.4.2012 - Lataaja: indegoification
Download: http://obx32y.1fichier.com/en/ Warning AVG users may habe **...** UNCUBE DDOS TOOL + **...**

It's easy to learn and use!



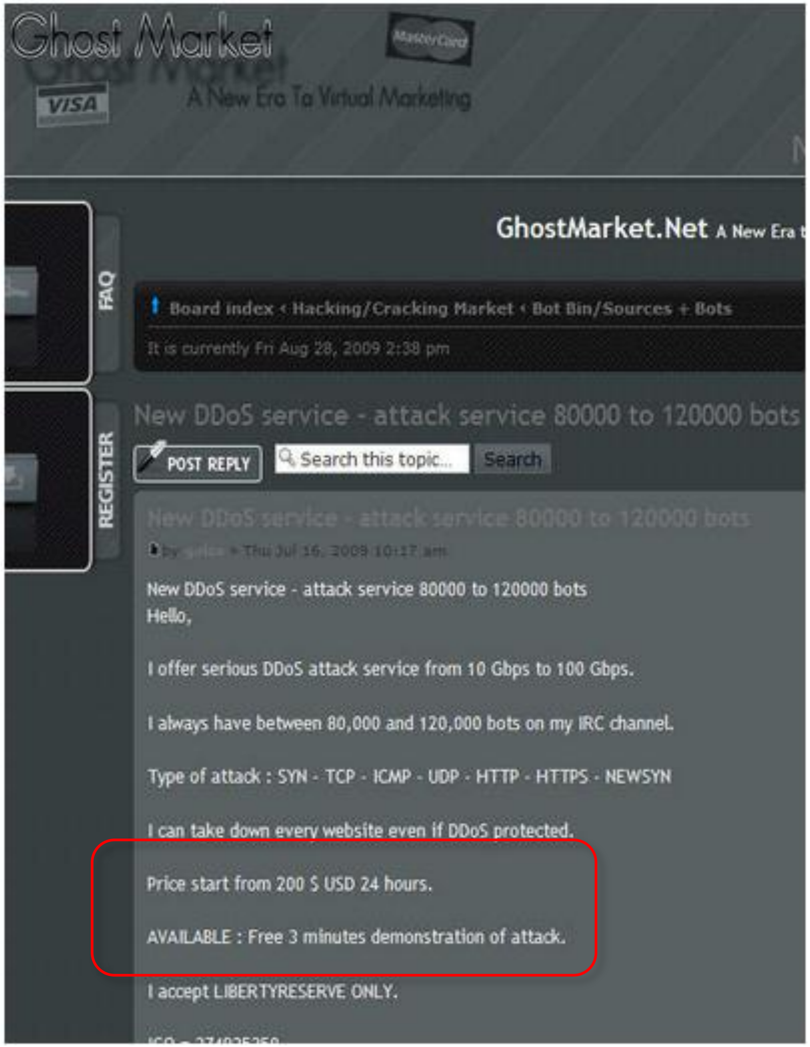
www.youtube.com/watch?v=Ola9Cg4tROA

```
target:       ifpi.org
irc server:   loic.anonops.in
channel:      #pandahouse
port:         6667
message:      Our words will not be ignored!
```

How to help anonymous, DDoS with AntiVenom's "Snake Bite"

- How to crash a website-EASY * any * — tekijä: TheHacker0007 — 60 571 — 5:37 — SUOSITUKSET
- Greek Anonymous.wmv — tekijä: YiannhsAnon — 68 140 näyttökertaa — 2:32
- Anonymous DDOS Attacked Monsanto — tekijä: Anon8U14T5R — 23 936 näyttökertaa — 2:11
- DDoS / DoS Attack Tool Tutorial — tekijä: AnonymousEducation — 20 771 näyttökertaa — 1:53
- Server Attack Goodbye V3.0 Download — tekijä: MultiAcidi — 26 733 näyttökertaa — 4:21
- God save america — tekijä: ladyelicharlot — 166 videota

Don’t do it Your self – rent it.



GhostMarket.Net A New Era t

Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots

It is currently Fri Aug 28, 2009 2:38 pm

New DDoS service - attack service 80000 to 120000 bots

New DDoS service - attack service 80000 to 120000 bots

by [illegible] » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

I can take down every website even if DDoS protected.

Price start from 200 $ USD 24 hours.

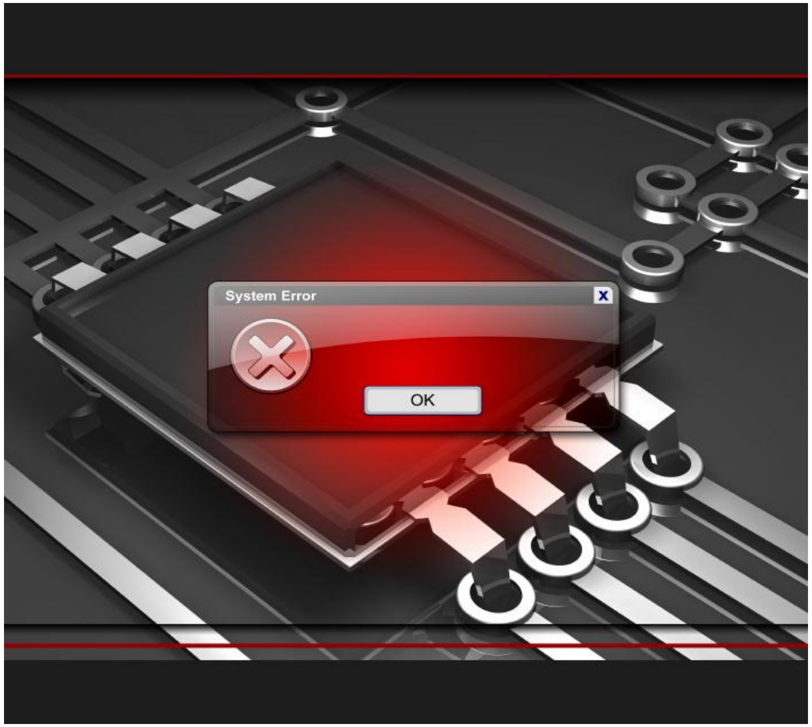
AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

Traditional Firewalls Not Sufficient

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



Introducing Check Point
Check Point DDoS Protector™

Block Denial of Service Attacks within seconds!

Product Information

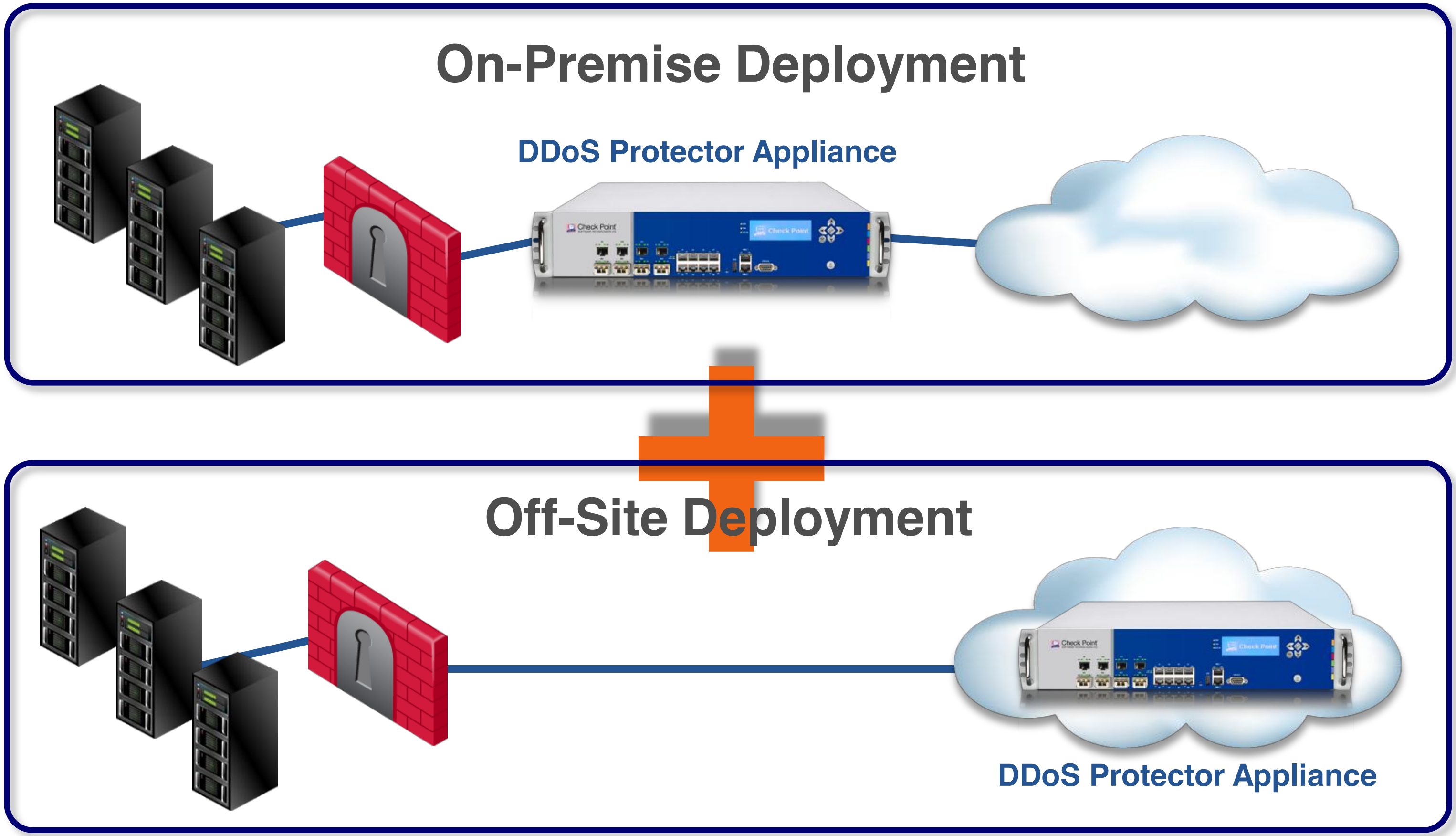
DP x06 Series

DP x412 Series

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						

Where to Protect Against DDoS

Scenarios: 1 2 3



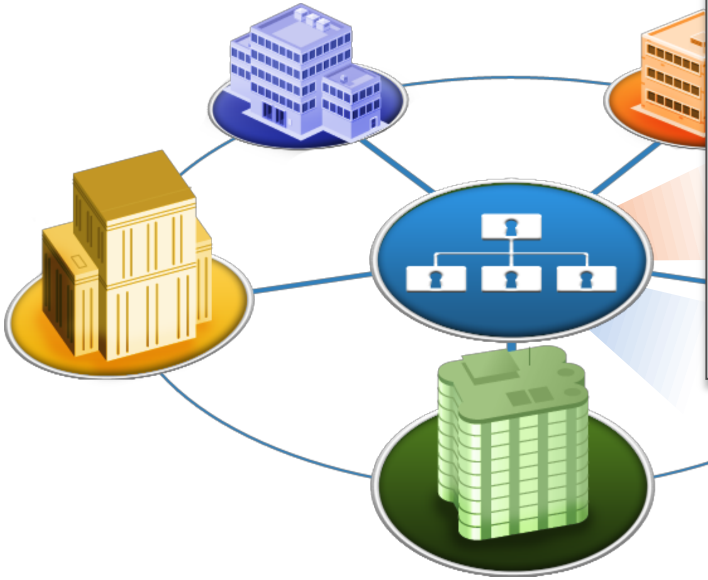
On-Premise Deployment

DDoS Protector Appliance

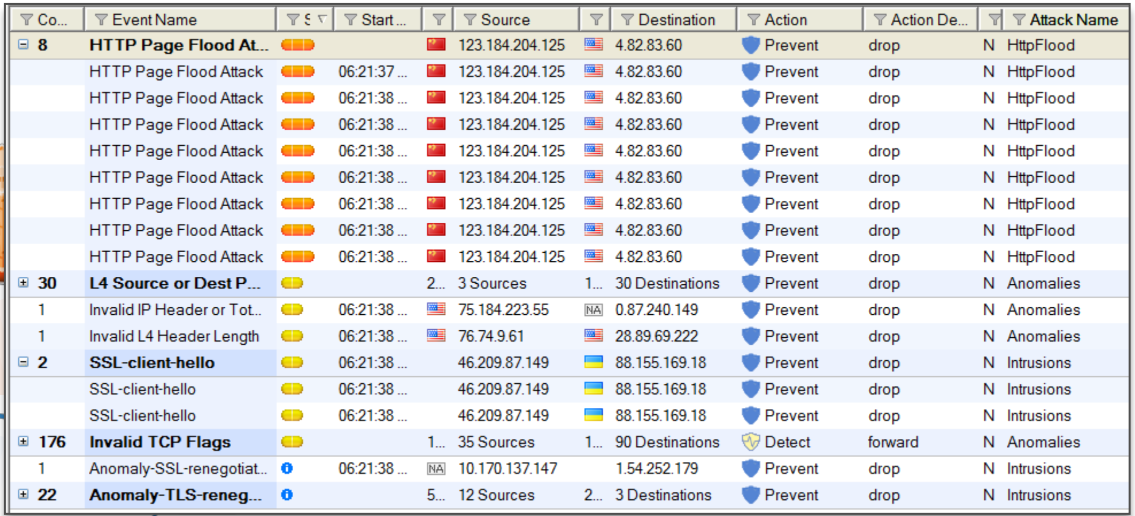
Off-Site Deployment

DDoS Protector Appliance

Integrated Security Management

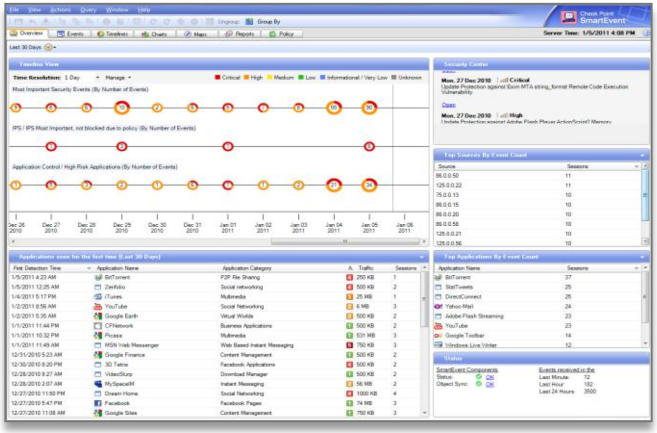


Unified Logs and Monitoring



Co...	Event Name	S	Start ...	Source	Destination	Action	Action De...		Attack Name
⊟ 8	**HTTP Page Flood At...**	🟧		123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:37 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
	HTTP Page Flood Attack	🟧	06:21:38 ...	123.184.204.125	4.82.83.60	Prevent	drop	N	HttpFlood
⊞ 30	**L4 Source or Dest P...**	🟨		2... 3 Sources	1... 30 Destinations	Prevent	drop	N	Anomalies
1	Invalid IP Header or Tot...	🟨	06:21:38 ...	75.184.223.55	NA 0.87.240.149	Prevent	drop	N	Anomalies
1	Invalid L4 Header Length	🟨	06:21:38 ...	76.74.9.61	28.89.69.222	Prevent	drop	N	Anomalies
⊟ 2	**SSL-client-hello**	🟨	06:21:38 ...	46.209.87.149	88.155.169.18	Prevent	drop	N	Intrusions
	SSL-client-hello	🟨	06:21:38 ...	46.209.87.149	88.155.169.18	Prevent	drop	N	Intrusions
	SSL-client-hello	🟨	06:21:38 ...	46.209.87.149	88.155.169.18	Prevent	drop	N	Intrusions
⊞ 176	**Invalid TCP Flags**	🟨		1... 35 Sources	1... 90 Destinations	Detect	forward	N	Anomalies
1	Anomaly-SSL-renegotiat...	ⓘ	06:21:38 ...	NA 10.170.137.147	1.54.252.179	Prevent	drop	N	Intrusions
⊞ 22	**Anomaly-TLS-reneg...**	ⓘ		5... 12 Sources	2... 3 Destinations	Prevent	drop	N	Intrusions

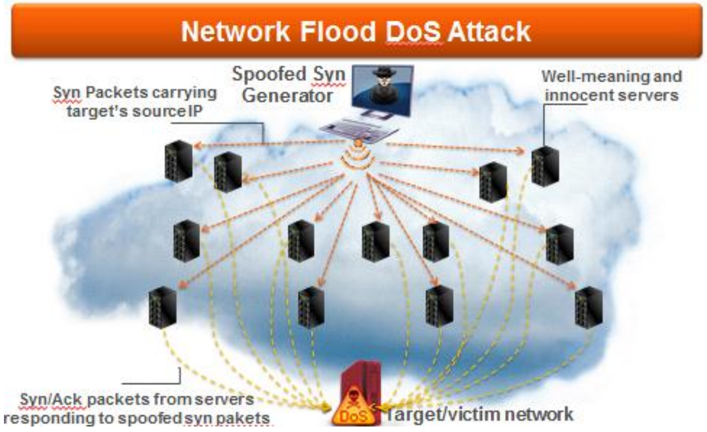
…and Unified Reporting

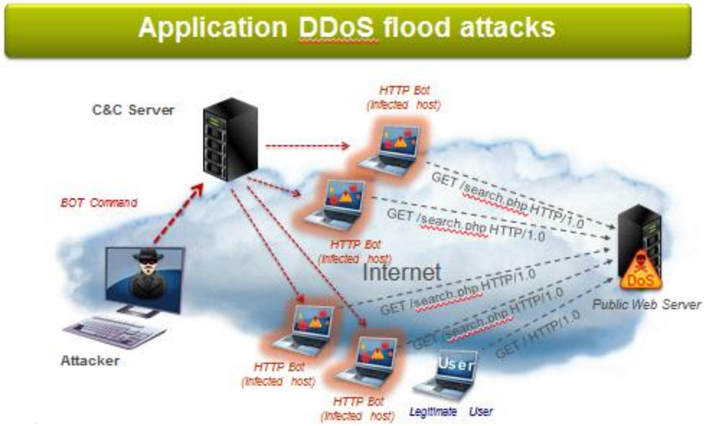


Leverage SmartView Tracker, SmartLog and SmartEvent for historic and real-time security status

DDoS Protector Logs

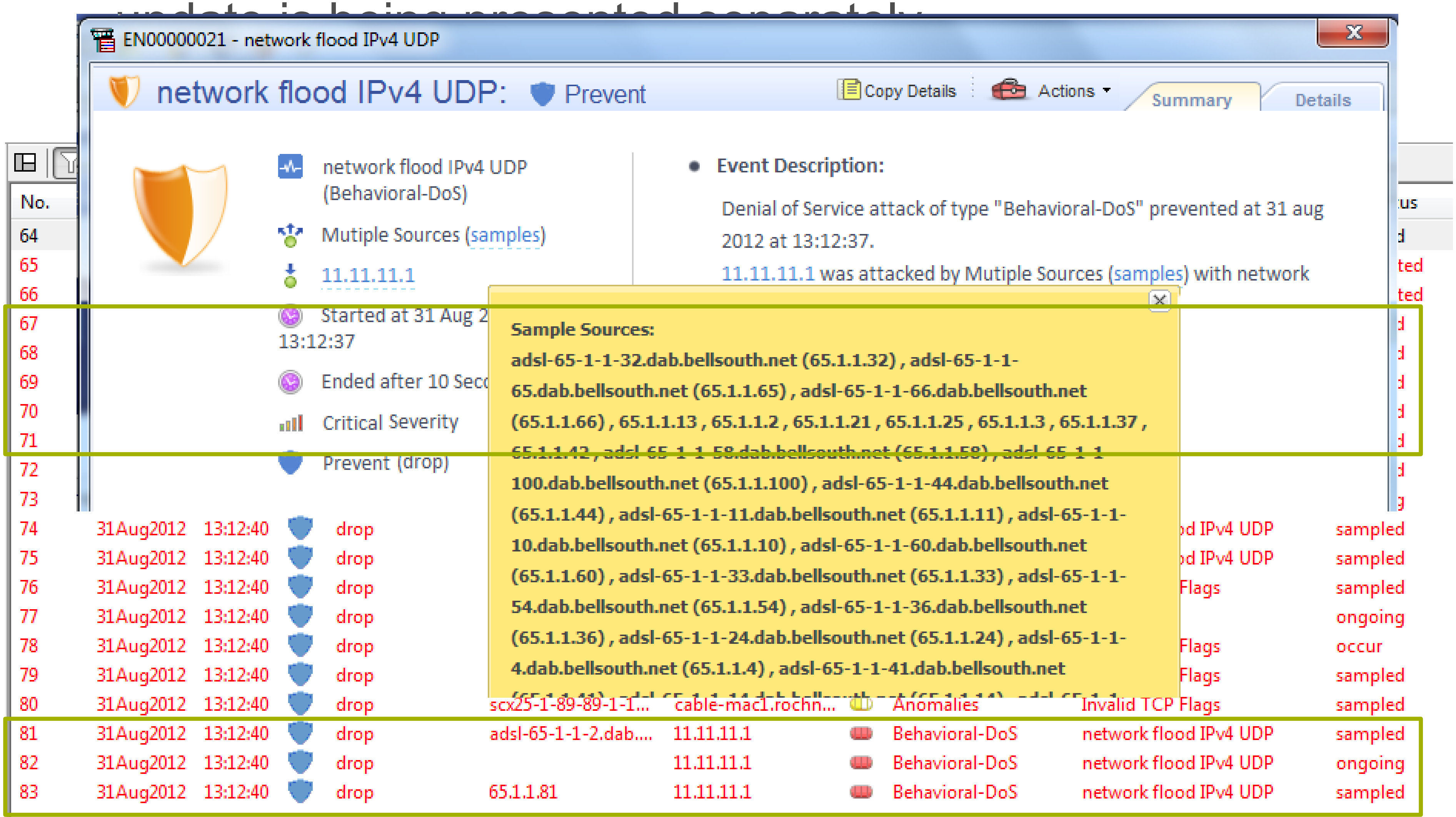
- For attacks with multiple sources / destinations.
  - the DDoS Protector appliance sends several logs to describe the attack
  - With status: **start**, **ongoing**, **completed**
  - And other logs with samples for source / destination (with status: **sampled**).


Network Flood DoS Attack
Spoofed Syn Generator
Syn Packets carrying target's source IP
Well-meaning and innocent servers
Syn/Ack packets from servers responding to spoofed syn pakets
DoS
Target/victim network



DDoS Protector Integration

- In SmartView Tracker and SmartLog, each log and log update is being presented separately



EN00000021 - network flood IPv4 UDP
network flood IPv4 UDP: Prevent
Copy Details
Actions
Summary
Details

network flood IPv4 UDP (Behavioral-DoS)

Mutiple Sources (samples)

11.11.11.1

Started at 31 Aug 2 13:12:37

Ended after 10 Secc

Critical Severity

Prevent (drop)

Event Description:

Denial of Service attack of type "Behavioral-DoS" prevented at 31 aug 2012 at 13:12:37.

11.11.11.1 was attacked by Mutiple Sources (samples) with network

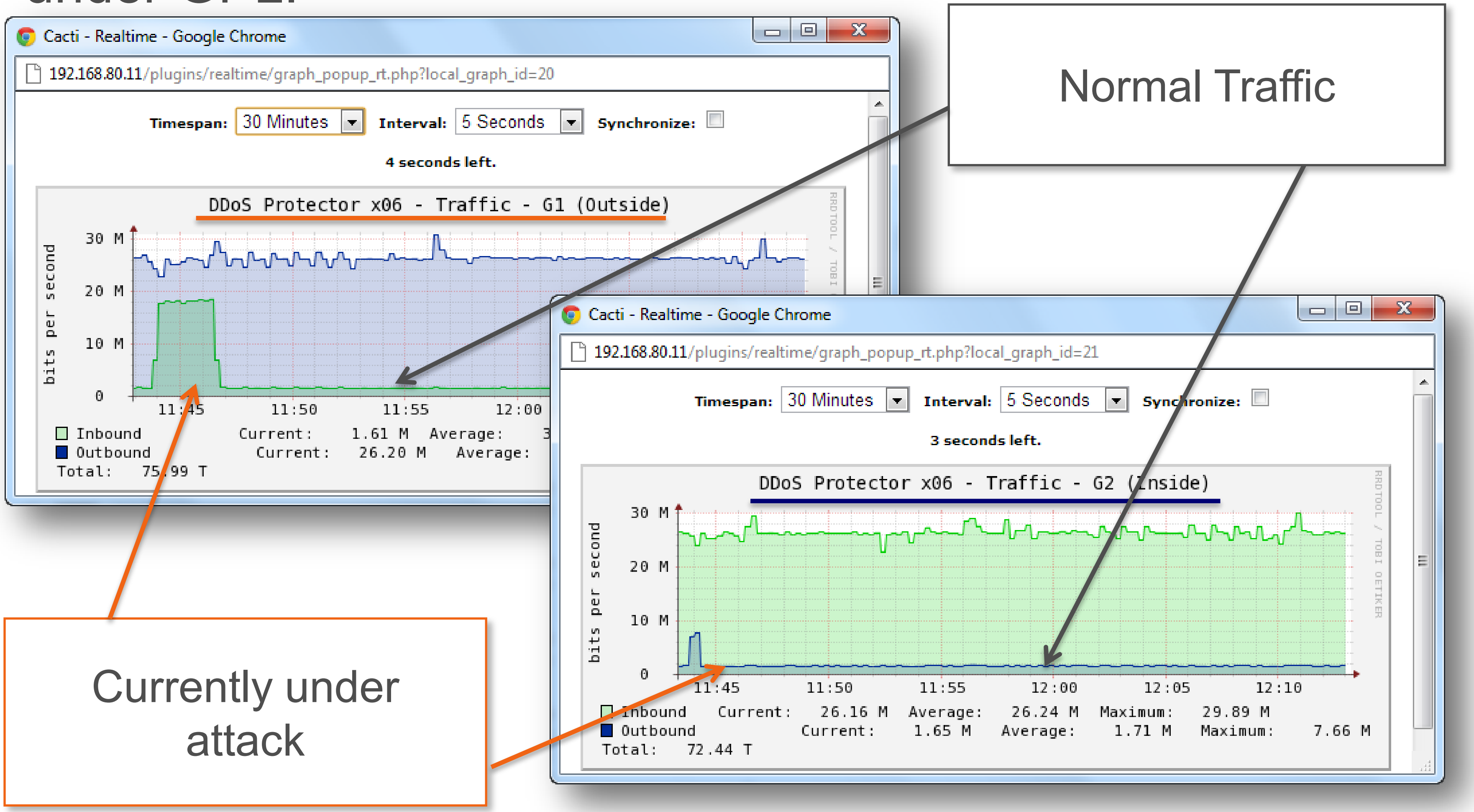
Sample Sources:

adsl-65-1-1-32.dab.bellsouth.net (65.1.1.32) , adsl-65-1-1-65.dab.bellsouth.net (65.1.1.65) , adsl-65-1-1-66.dab.bellsouth.net (65.1.1.66) , 65.1.1.13 , 65.1.1.2 , 65.1.1.21 , 65.1.1.25 , 65.1.1.3 , 65.1.1.37 , 65.1.1.42 , adsl-65-1-1-58.dab.bellsouth.net (65.1.1.58) , adsl-65-1-1-100.dab.bellsouth.net (65.1.1.100) , adsl-65-1-1-44.dab.bellsouth.net (65.1.1.44) , adsl-65-1-1-11.dab.bellsouth.net (65.1.1.11) , adsl-65-1-1-10.dab.bellsouth.net (65.1.1.10) , adsl-65-1-1-60.dab.bellsouth.net (65.1.1.60) , adsl-65-1-1-33.dab.bellsouth.net (65.1.1.33) , adsl-65-1-1-54.dab.bellsouth.net (65.1.1.54) , adsl-65-1-1-36.dab.bellsouth.net (65.1.1.36) , adsl-65-1-1-24.dab.bellsouth.net (65.1.1.24) , adsl-65-1-1-4.dab.bellsouth.net (65.1.1.4) , adsl-65-1-1-41.dab.bellsouth.net (65.1.1.41) , adsl-65-1-1-14.dab.bellsouth.net (65.1.1.14) , adsl-65-1-1-

No.									us
64									d
65									ted
66									ted
67									d
68									d
69									d
70									d
71									d
72									d
73									g
74	31Aug2012	13:12:40	drop					d IPv4 UDP	sampled
75	31Aug2012	13:12:40	drop					d IPv4 UDP	sampled
76	31Aug2012	13:12:40	drop					Flags	sampled
77	31Aug2012	13:12:40	drop						ongoing
78	31Aug2012	13:12:40	drop					Flags	occur
79	31Aug2012	13:12:40	drop					Flags	sampled
80	31Aug2012	13:12:40	drop	scx25-1-89-89-1-1...	cable-mac1.rochn...	Anomalies		Invalid TCP Flags	sampled
81	31Aug2012	13:12:40	drop	adsl-65-1-1-2.dab....	11.11.11.1	Behavioral-DoS		network flood IPv4 UDP	sampled
82	31Aug2012	13:12:40	drop		11.11.11.1	Behavioral-DoS		network flood IPv4 UDP	ongoing
83	31Aug2012	13:12:40	drop	65.1.1.81	11.11.11.1	Behavioral-DoS		network flood IPv4 UDP	sampled

Real time monitoring with SNMP

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



Cacti - Realtime - Google Chrome

192.168.80.11/plugins/realtime/graph_popup_rt.php?local_graph_id=20

Timespan: 30 Minutes Interval: 5 Seconds Synchronize: □

4 seconds left.

DDoS Protector x06 - Traffic - G1 (Outside)

```
Inbound     Current:    1.61 M   Average:   3
Outbound    Current:   26.20 M   Average:
Total:    75.99 T
```

Cacti - Realtime - Google Chrome

192.168.80.11/plugins/realtime/graph_popup_rt.php?local_graph_id=21

Timespan: 30 Minutes Interval: 5 Seconds Synchronize: □

3 seconds left.

DDoS Protector x06 - Traffic - G2 (Inside)

```
Inbound    Current:   26.16 M   Average:   26.24 M   Maximum:   29.89 M
Outbound            Current:    1.65 M   Average:    1.71 M   Maximum:    7.66 M
Total:    72.44 T
```

Normal Traffic

Currently under attack

DDos Protector

1 (D)DoS Attacks

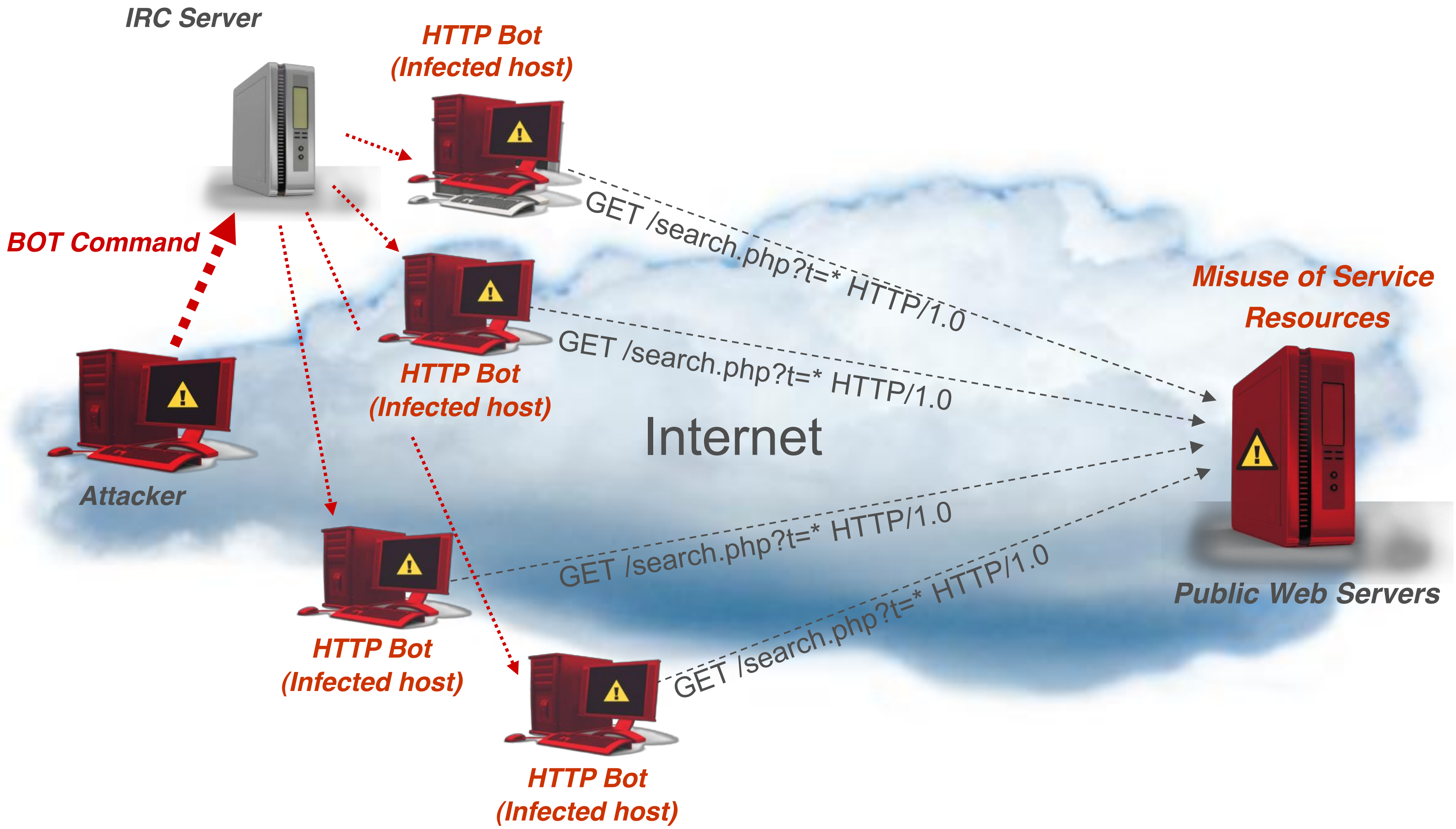
2 DDoS Protector

3 **Behavioral DoS Protection**

4 Summary

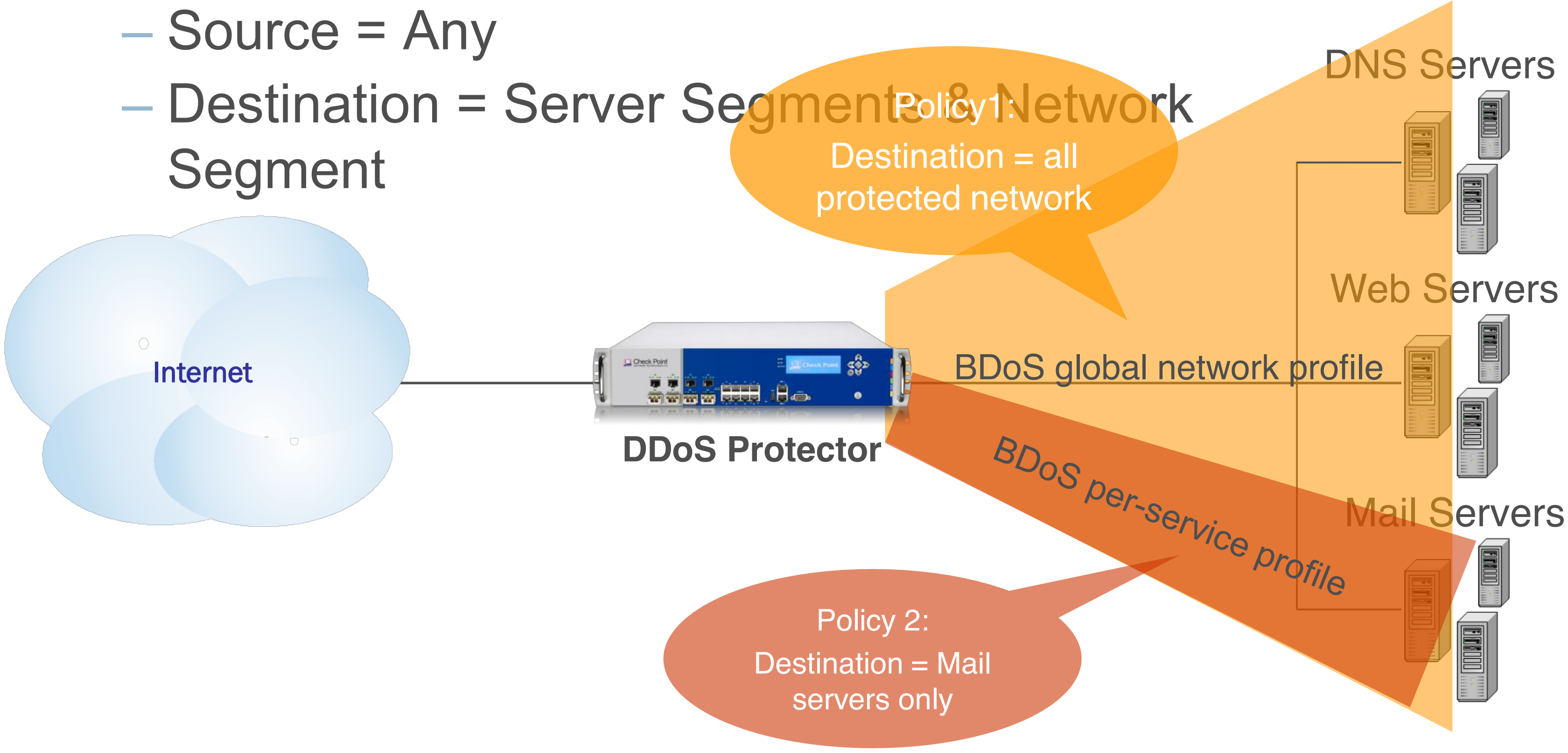
HTTP Flood Scenarios

Typical Distributed Attack



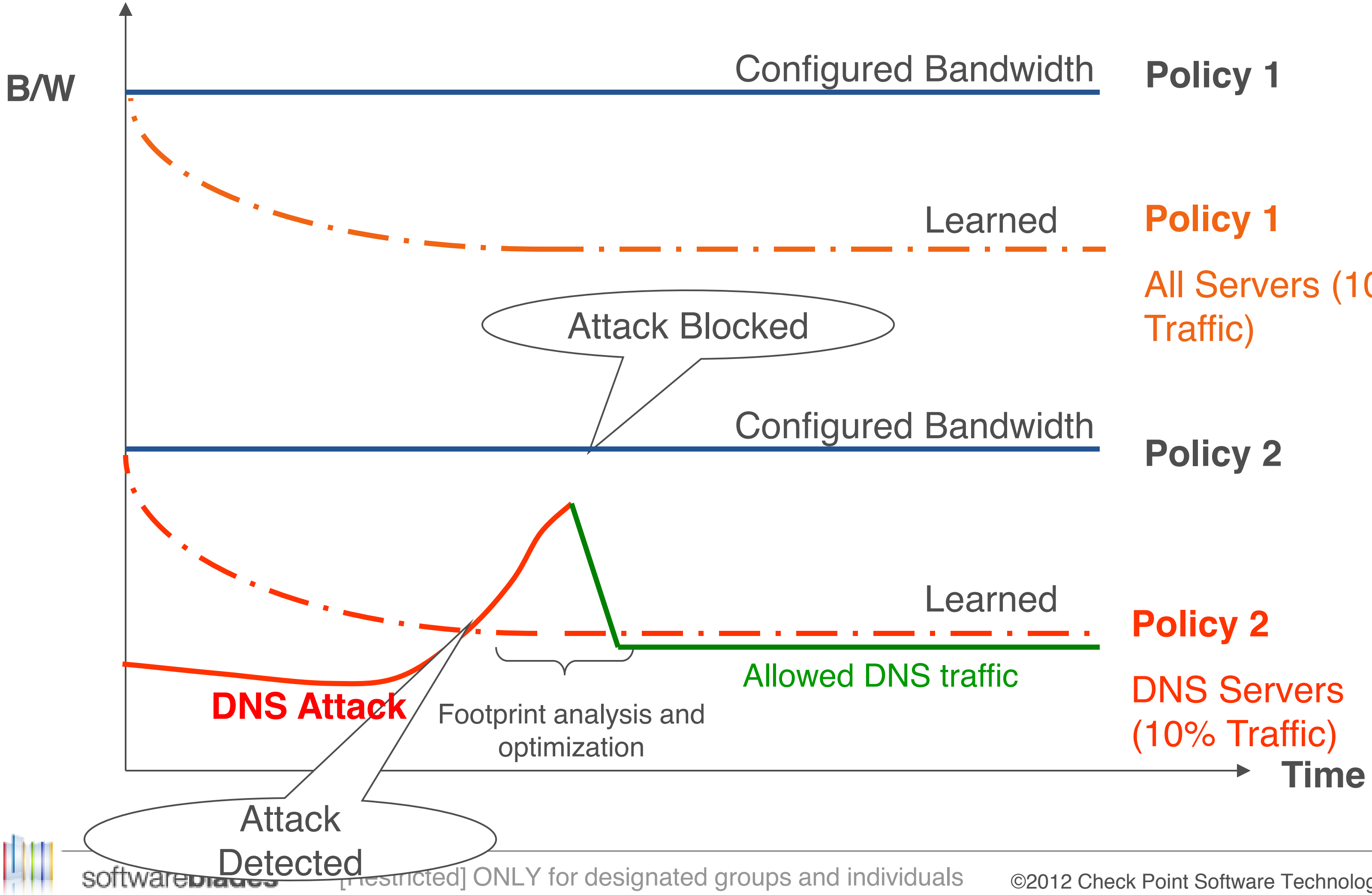
Setting BDoS Network Policy

- Protect Network & Servers from DDoS
- Policies are set with:
  - Source = Any
  - Destination = Server Segments & Network Segment



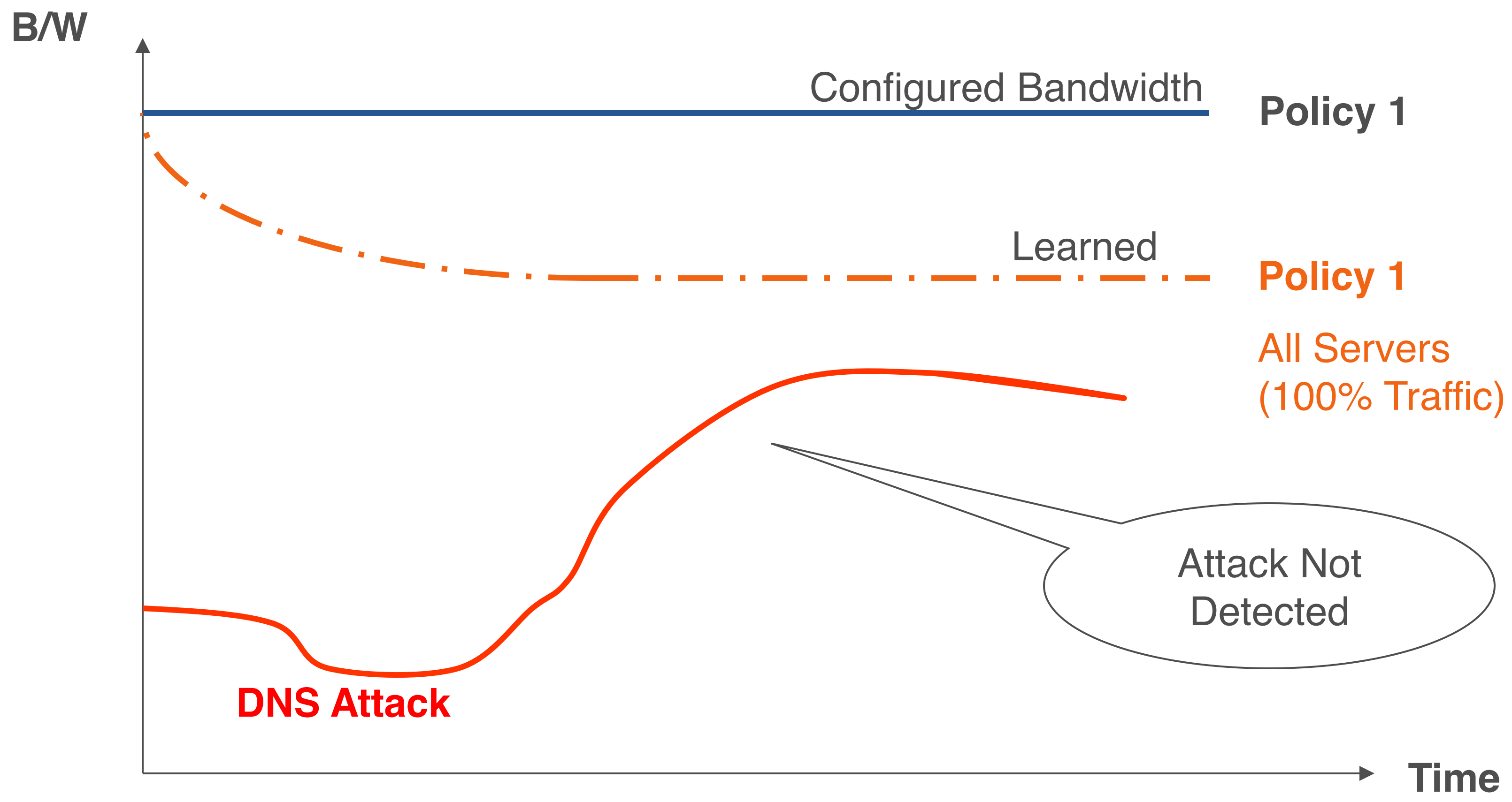
Setting BDoS Network Policy

Attack Mitigation per Network Policy



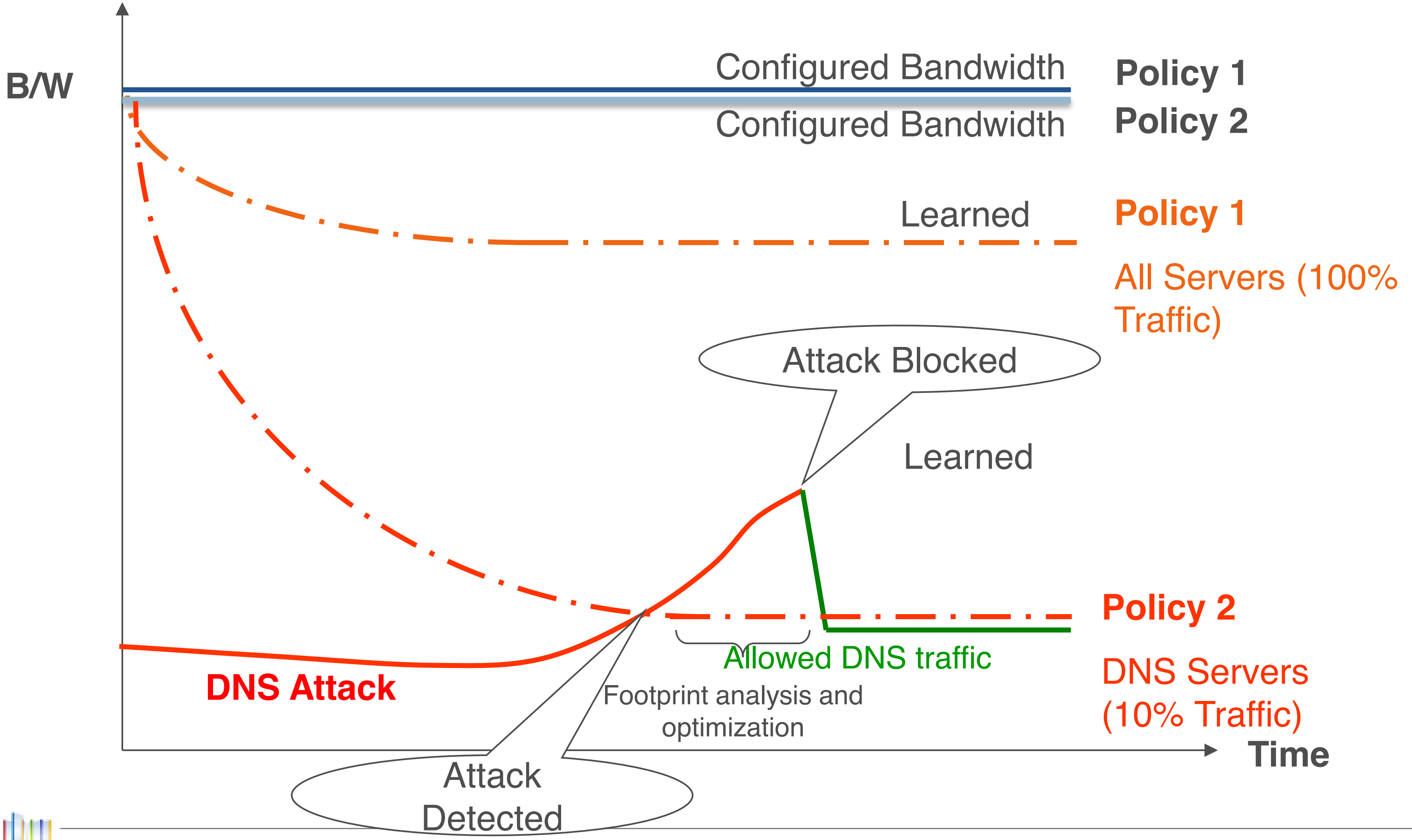
Setting BDoS Network Policy

Global Policy: Low Attack Detection Sensitivity



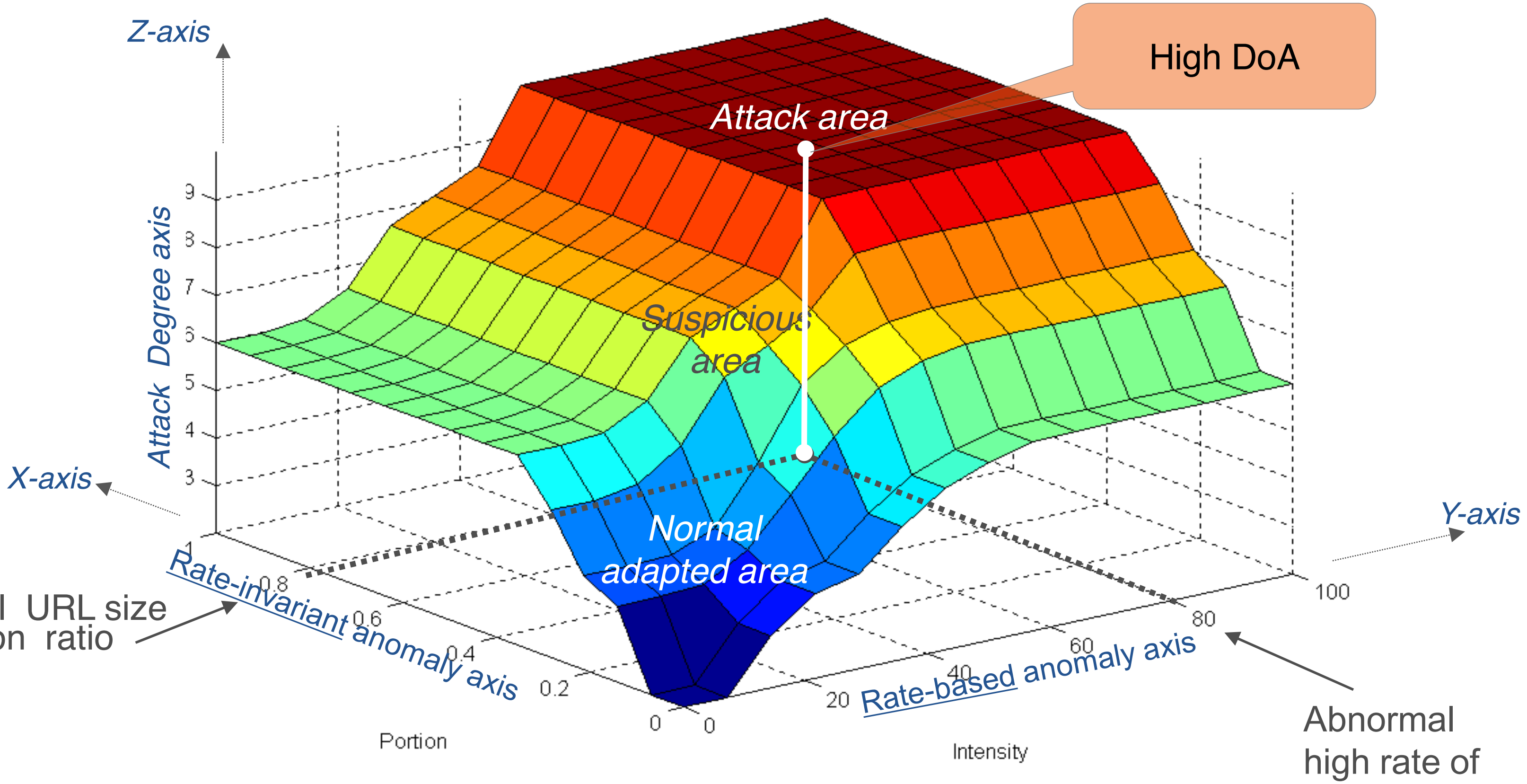
Setting BDoS Network Policy

Unknown bandwidth per policy



Adaptive Decision Engine

HTTP Flood



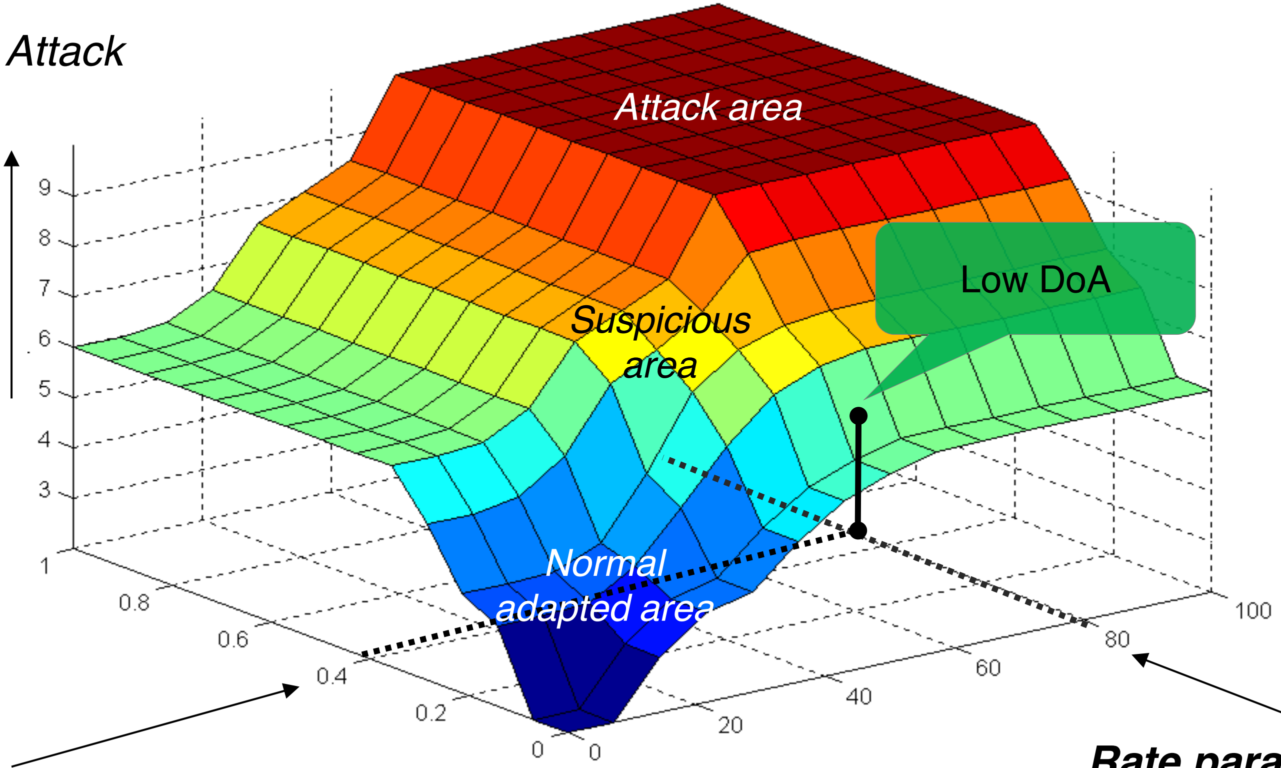
Abnormal URL size distribution ratio

Abnormal high rate of HTTP GET requests

Adaptive Detection Engine

Flash crowd scenario

Degree of Attack (DoA)



***Rate-invariant** input parameter*

(***Normal*** URL size distribution ratio)

***Rate parameter** input*

(**Abnormal** high rate of HTTP GET requests)

Adaptive Detection Engine

Resistance to False Positive

Case: Flash Crowd Access

Beha

✓ Bas

(or p

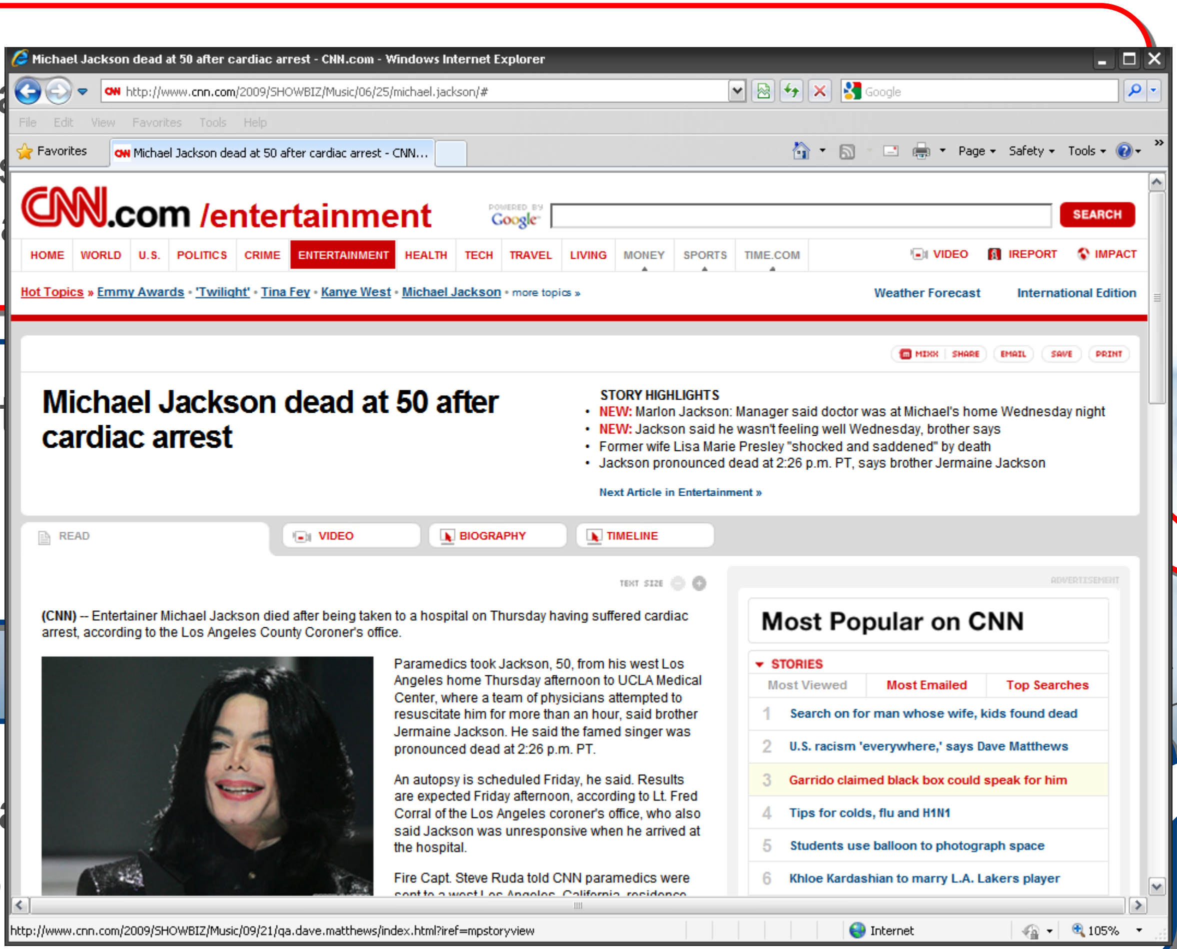
Legi

✓ No

✓ No

Beha

✓ No



Michael Jackson dead at 50 after cardiac arrest - CNN.com - Windows Internet Explorer
http://www.cnn.com/2009/SHOWBIZ/Music/06/25/michael.jackson/#
Google
File Edit View Favorites Tools Help
Favorites
Michael Jackson dead at 50 after cardiac arrest - CNN...
Page Safety Tools
CNN.com /entertainment
POWERED BY Google
SEARCH
HOME WORLD U.S. POLITICS CRIME ENTERTAINMENT HEALTH TECH TRAVEL LIVING MONEY SPORTS TIME.COM
VIDEO IREPORT IMPACT
Hot Topics » Emmy Awards • 'Twilight' • Tina Fey • Kanye West • Michael Jackson • more topics »
Weather Forecast International Edition
MIXX SHARE EMAIL SAVE PRINT

Michael Jackson dead at 50 after cardiac arrest

STORY HIGHLIGHTS

- NEW: Marlon Jackson: Manager said doctor was at Michael's home Wednesday night
- NEW: Jackson said he wasn't feeling well Wednesday, brother says
- Former wife Lisa Marie Presley "shocked and saddened" by death
- Jackson pronounced dead at 2:26 p.m. PT, says brother Jermaine Jackson

Next Article in Entertainment »

(CNN) -- Entertainer Michael Jackson died after being taken to a hospital on Thursday having suffered cardiac arrest, according to the Los Angeles County Coroner's office.

Paramedics took Jackson, 50, from his west Los Angeles home Thursday afternoon to UCLA Medical Center, where a team of physicians attempted to resuscitate him for more than an hour, said brother Jermaine Jackson. He said the famed singer was pronounced dead at 2:26 p.m. PT.

An autopsy is scheduled Friday, he said. Results are expected Friday afternoon, according to Lt. Fred Corral of the Los Angeles coroner's office, who also said Jackson was unresponsive when he arrived at the hospital.

Fire Capt. Steve Ruda told CNN paramedics were sent to a west Los Angeles, California, residence

Most Popular on CNN

STORIES

Most Viewed | Most Emailed | Top Searches

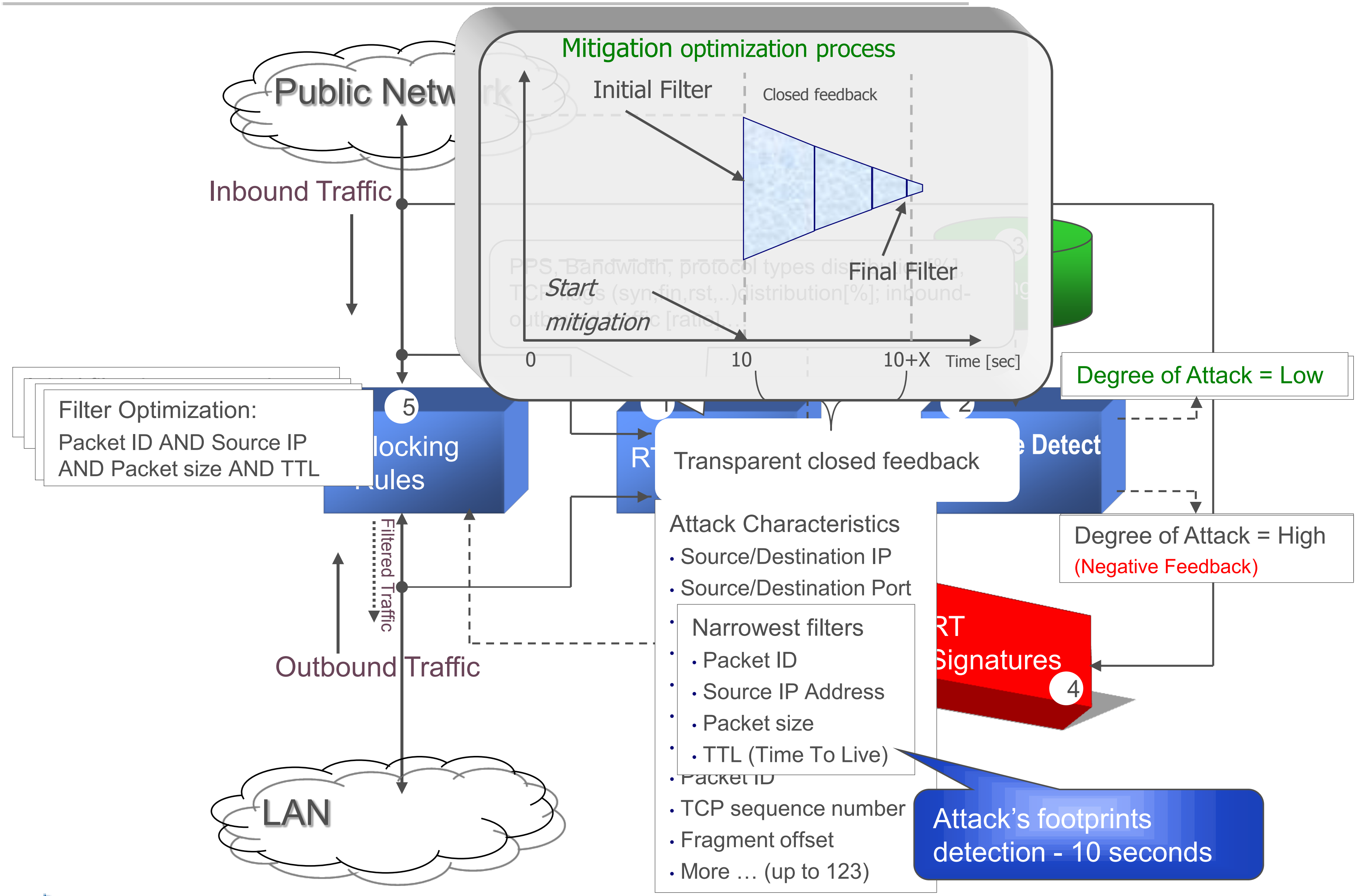
1 Search on for man whose wife, kids found dead
2 U.S. racism 'everywhere,' says Dave Matthews
3 Garrido claimed black box could speak for him
4 Tips for colds, flu and H1N1
5 Students use balloon to photograph space
6 Khloe Kardashian to marry L.A. Lakers player

http://www.cnn.com/2009/SHOWBIZ/Music/09/21/qa.dave.matthews/index.html?iref=mpstoryview
Internet
105%

Public Web Servers

Legitimate User

Statistical Analysis / Adaptive Detection



Filter Optimization:
Packet ID AND Source IP AND Packet size AND TTL

Transparent closed feedback

Degree of Attack = Low

Degree of Attack = High
(Negative Feedback)

Attack Characteristics
- Source/Destination IP
- Source/Destination Port
- Packet ID
- TCP sequence number
- Fragment offset
- More … (up to 123)

Narrowest filters
- Packet ID
- Source IP Address
- Packet size
- TTL (Time To Live)

Attack's footprints detection - 10 seconds

Flexible Deployment Options

Ready to Protect in Minutes

Fits to Existing Network Topology

Learning Mode Deployment

Low Maintenance and Support

Emergency Response and Support

Emergency Response Team

- Help from security experts when under DoS attacks
- Leverage experience gathered from real-life attacks

Check Point customer support

- World-class support infrastructure
- Always-on support 7x24
- Flexible service options

Summary

Blocks DDoS Attacks Within Seconds

Customized multi-layered DDoS protection

Ready to protect in minutes

Integrated with Check Point Security Management