

# 1<sup>st</sup> Slovenian Network Operators Group

## Corero Network Security

Peter Cutler, Systems Engineer EMEA



# Hello

**Peter Cutler, Corero Systems Engineer**

BEng (Hons)

**Skype: petercutler\_s**

**[peter.cutler@corero.com](mailto:peter.cutler@corero.com)**

**+44 7824 996 520**



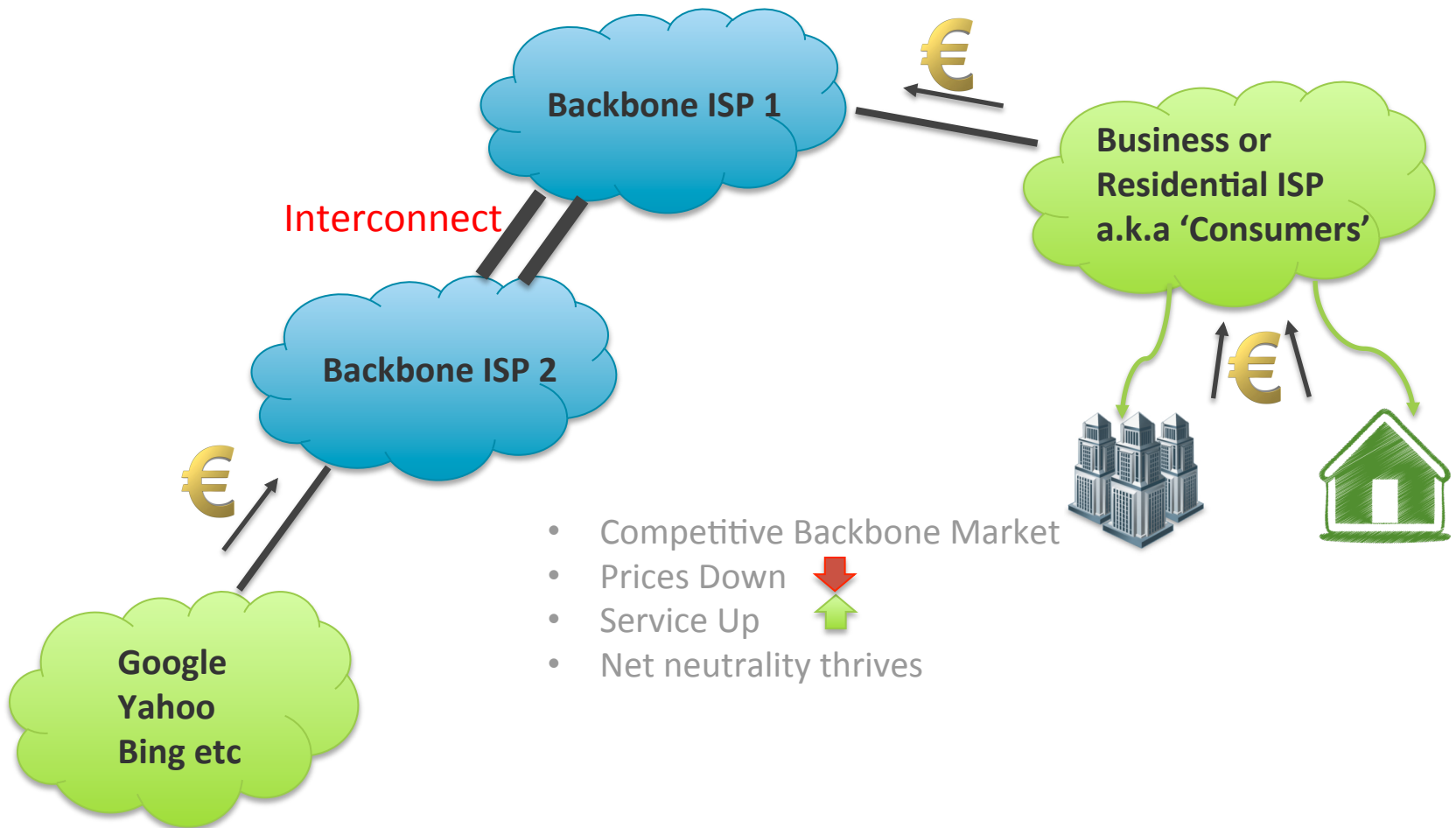
# Unique Slovenian Legislation




*...confirms the open and neutral character of the Internet and prohibits discrimination of Internet traffic on the basis of the services provided through it"*

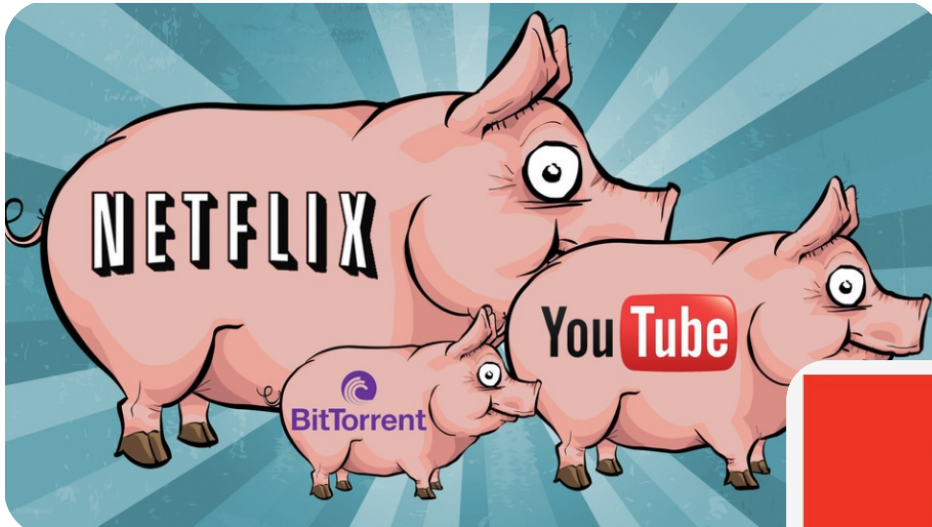
*ISPs will be prevented from restricting, delaying or slowing Internet traffic except in the case they have to solve congestion, **preserve security** or address spam...*

# 'Classic Internet Operation Model'

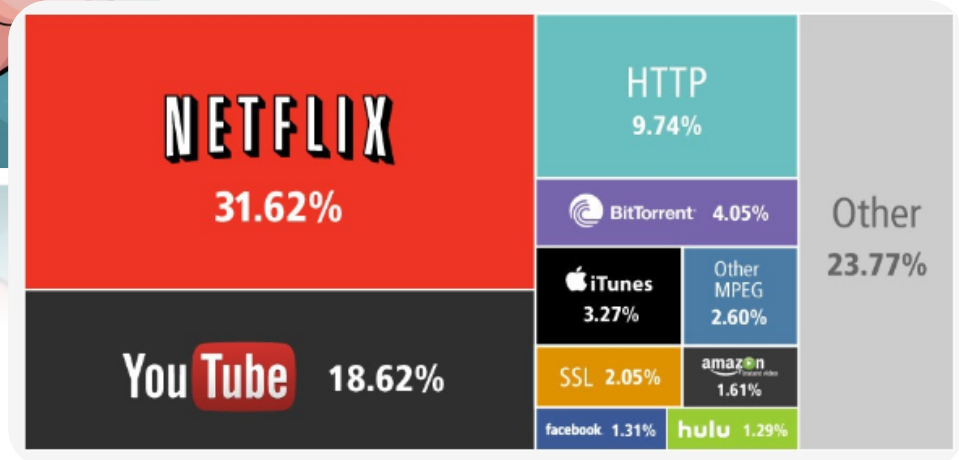


- Competitive Backbone Market
- Prices Down 
- Service Up 
- Net neutrality thrives

# North American Downstream Internet Traffic



Source: Mashable 2014



Source: Statista 2014

# Potential reasons for impact to Net Neutrality

- US-Specific Consolidated Operating Model  
e.g. Verizon purchasing MCI (Consumer /Backbone now one)
- Operating and Business Models to differentiate...

Volume and  
Bandwidth delivered



Security Delivered



# Denial of Service

February 11, 2014  
**CloudFlare spots 'largest ever DDoS attack'**  
Content delivery network CloudFlare says that one of its clients was hit by one of the biggest distributed denial of service (DDoS) attacks ever seen on European networks.

CloudFlare  
400Gbps  
DDoS  
Which  
attack was close to  
larger than last year's  
Spamhaus,  
Confédération Eidgenössische  
Confederazione Svizzera  
Confederaziun svizra



NEWS  
**NTP-based DDoS  
Cloudflare**

Warwick Ashford  
Wednesday 12 February 2014  
08:57

Security firm Cloudflare says it has spotted and blocked a distributed denial of service (DDoS) attack that exploited a vulnerability in the infrastructure of the target. The firm said the target was unclear, but the attack was the biggest of its kind, measuring about 400Gbps, about 100Gbps greater than the previous record attack on Spamhaus.

**W TechWeek**  
europe  
Enhancing business with technology - in association with eWeek.com

HOME | GALLERIES | SECURITY | CLOUD | SERVERS | VIDEO | QUIZ | POLLS | MOBILE | GREEN | BIG DATA  
NEWS | OPINION | IT LIFE | WHITE PAPERS | WEBCASTS | SMB | IT JOBS | TECH CLUB | AWARDS

**Wearable Conference & Hackfest**  
Technology Conference and Expo

On January 17, 2014 by Max Sinikale  
The number of threats facing individuals and businesses online has grown 14 percent in a single year, according to the Annual Security Report published by Cisco.

This emerging type of DDoS attack...  
servers with huge amounts of...  
exploiting weaknesses in...  
chronise comput...  
Protocol (...

Gefahren im Internet | Kontakt | Glossar | Häufige Fragen | Hilfe

Checklisten und Anleitungen  
Demonstrationen und  
Lernprogramme

Sensibilisierung  
Meldeformular

Newsletter  
News abonnieren

Inhalt  
RSS Feed

Startseite > Dienstleistungen > Newsletter > DDoS-Angriffe - Mas...  
Über MELANI

**DDoS-Angriffe - Massive Zunahme auch in der Schweiz - 17.  
Halbjahresbericht MELANI**

Der grösste DDoS-Angriff in der Geschichte des Internets, E-Banking-Angriffe mit  
Smartphone-Trojanern und zahlreiche gezielte Spionageangriffe bilden inhaltlichen die  
Schwerpunkte des heute publizierten 17. Halbjahresberichts der Melde- und Analysestelle  
Informationssicherung (MELANI). Zusätzlich veröffentlicht MELANI heute  
Sicherheitsempfehlungen zu industriellen Kontrollsystemen sowie zu Content  
Management Systemen.

**inside-it.ch**

Technologie-Partner | RSS Feeds | Impressum | Huron AG

HOME | ARCHIV | ictjobs.ch | OSS DIRECTORY | N

Kommentar schreiben | Artikel Drucken | In PDF umwandeln | Artikel verschicke

Donnerstag, 10.01.2013

**Erste DDoS-Attacken auf Schweizer Nameserver**

Schweizer Nameserver werden seit heute mit DDoS angegriffen. Die  
Angreifer waren jedoch erfolglos.

Seit heute Morgen um 04.00 Uhr werden alle Schweizer Nameserver  
systematisch missbraucht, um andere Webseiten lahm zu legen. Laut der  
Stiftung Switch handle es sich dabei um "Distributed Denial of Service"  
(DDoS)-Angriffe. Mit DDoS-Attacken versucht der Angreifende eine

**Massive Internetattacke  
beeinträchtigt weltweiten  
Datenverkehr**

Es ist die schwerste bislang bekannte Attacke - und beeinträchtigt  
den Datenverkehr weltweit: Mit 75 Gigabit pro Sekunde haben  
Unbekannte einen Schweizer Dienstleister für Spam-Filter  
angegriffen.

**Keeping the Doors Open  
and Lights On**

As more and more enterprises move mission-critical services online and require continuous uptime to perform business transactions, the threat landscape has changed. Although distributed denial-of-service (DDoS) attacks are not new, they are more effective today than ever before. DDoS prevention solutions offer protection against the different categories of DDoS attack, and many vendors have entered the market in recent years. In 2014, NSS Labs will begin testing DDoS vendors, and this week we published our [methodology](#) along with an analyst brief on why DDoS attacks can be difficult to protect against.

Read the new [brief](#) and blog [Ha Ha You're Dead \(The Effects of DDoS Attacks\)](#) to learn more!

NSS subscribers have full access to this report and all NSS research, so visit [www.nsslabs.com](#) today to learn more about becoming a client!

Best regards,

**NSS** LABS

About NSS Labs

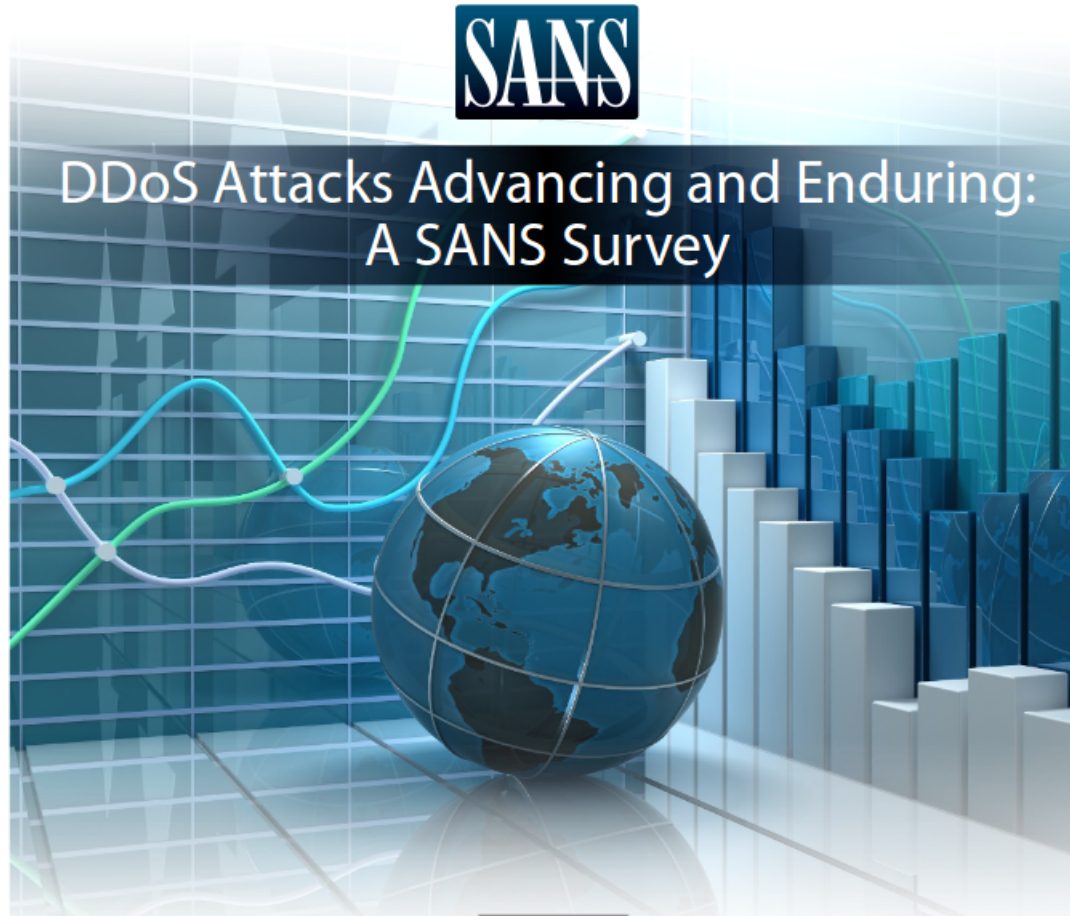
NSS Labs, Inc. is the world's leading information security research and advisory company, with unparalleled expertise in the complex aspects of information security across a wide range of technologies. Unique to the IT industry, NSS is the only research analyst firm backed by a testing laboratory rather than relying on surveys and questionnaires to advise clients. Products are tested and rated for their effectiveness, performance, manageability and cost of ownership. So when NSS makes a recommendation, it is based upon analysis of the facts.

At NSS, we make security a science.



**corero**  
FIRST LINE OF DEFENSE

# SANS Institute: [DDoS Survey](#) Feb 2014

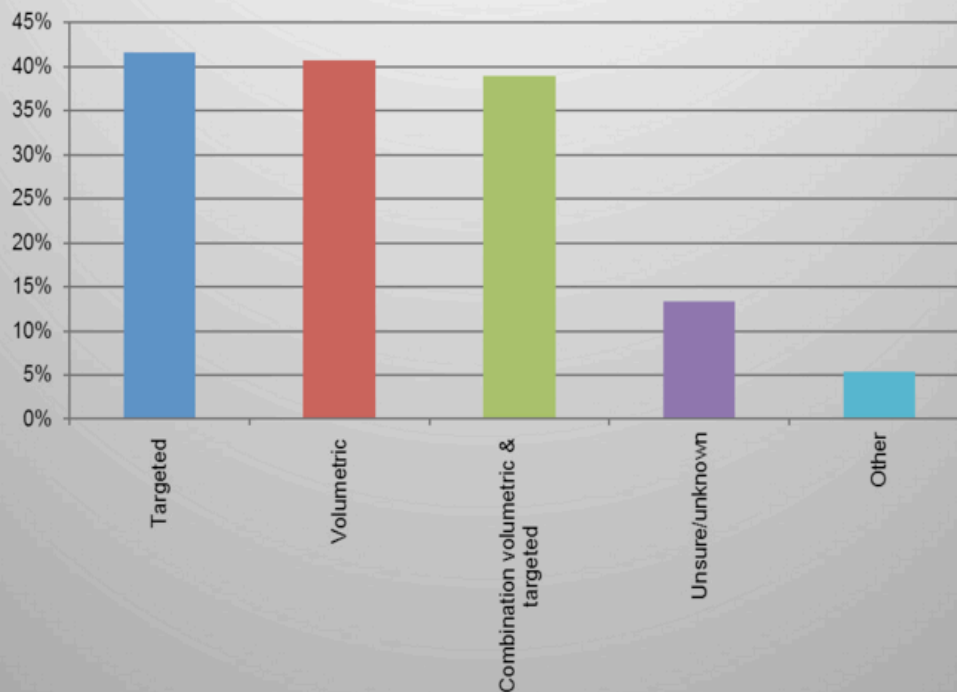


[Corero.com](#) > [Resources](#) > [Reports](#)



# DDoS Attack Types

What type(s) of attack(s) did you experience? Select all that apply.

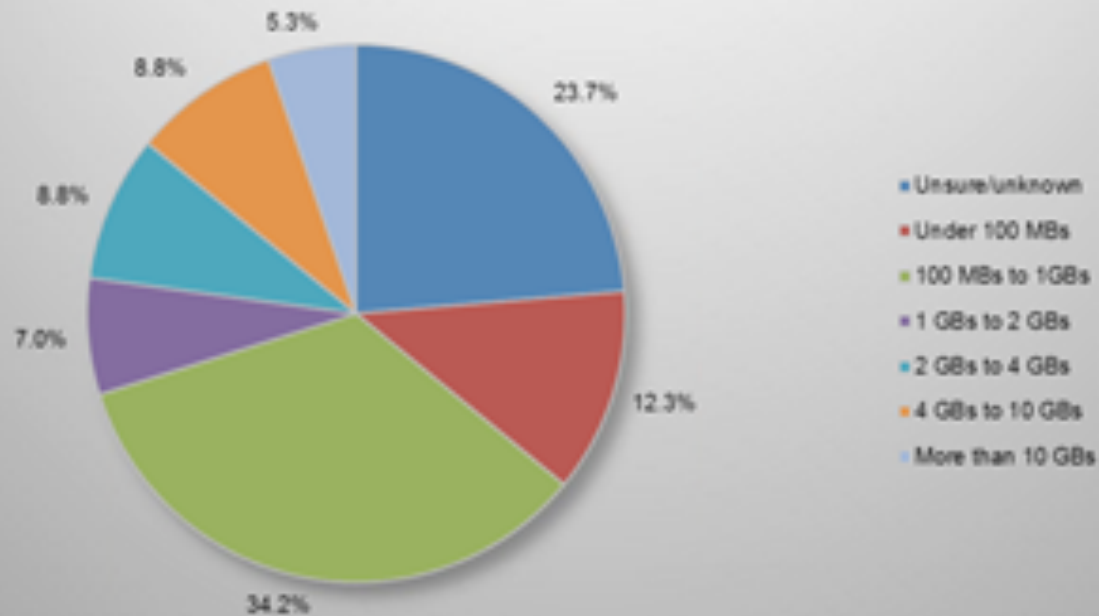


© 2014 The SANS™ Institute – [www.sans.org](http://www.sans.org)

12

# DDoS Attack Data Rates

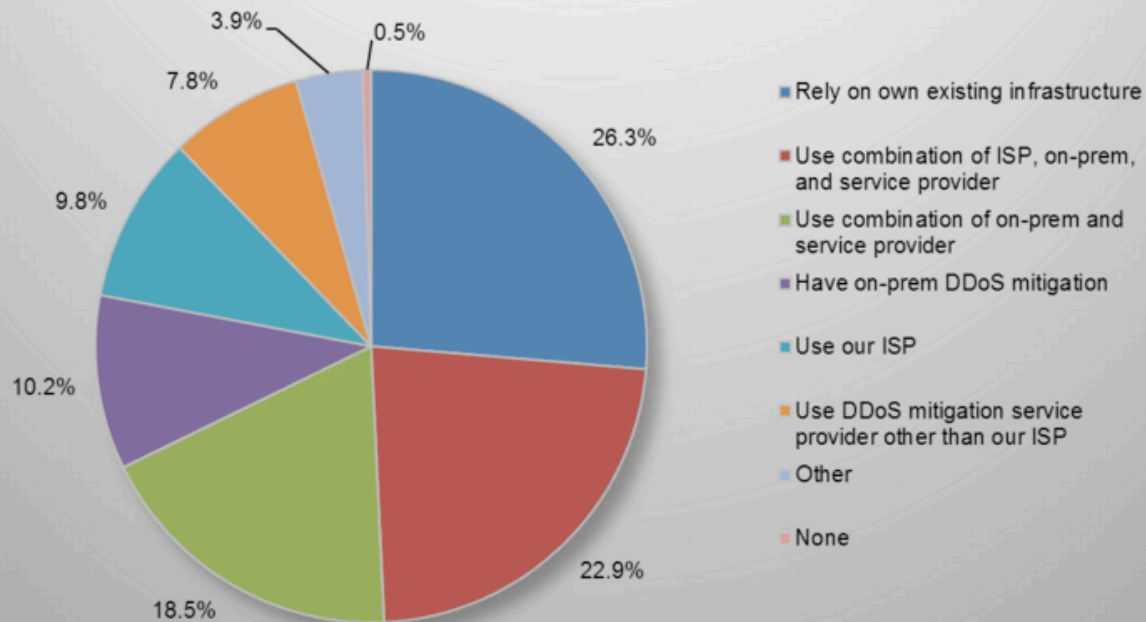
On average, what was the bandwidth of the attacks?



© 2014 The SANS™ Institute – [www.sans.org](http://www.sans.org)

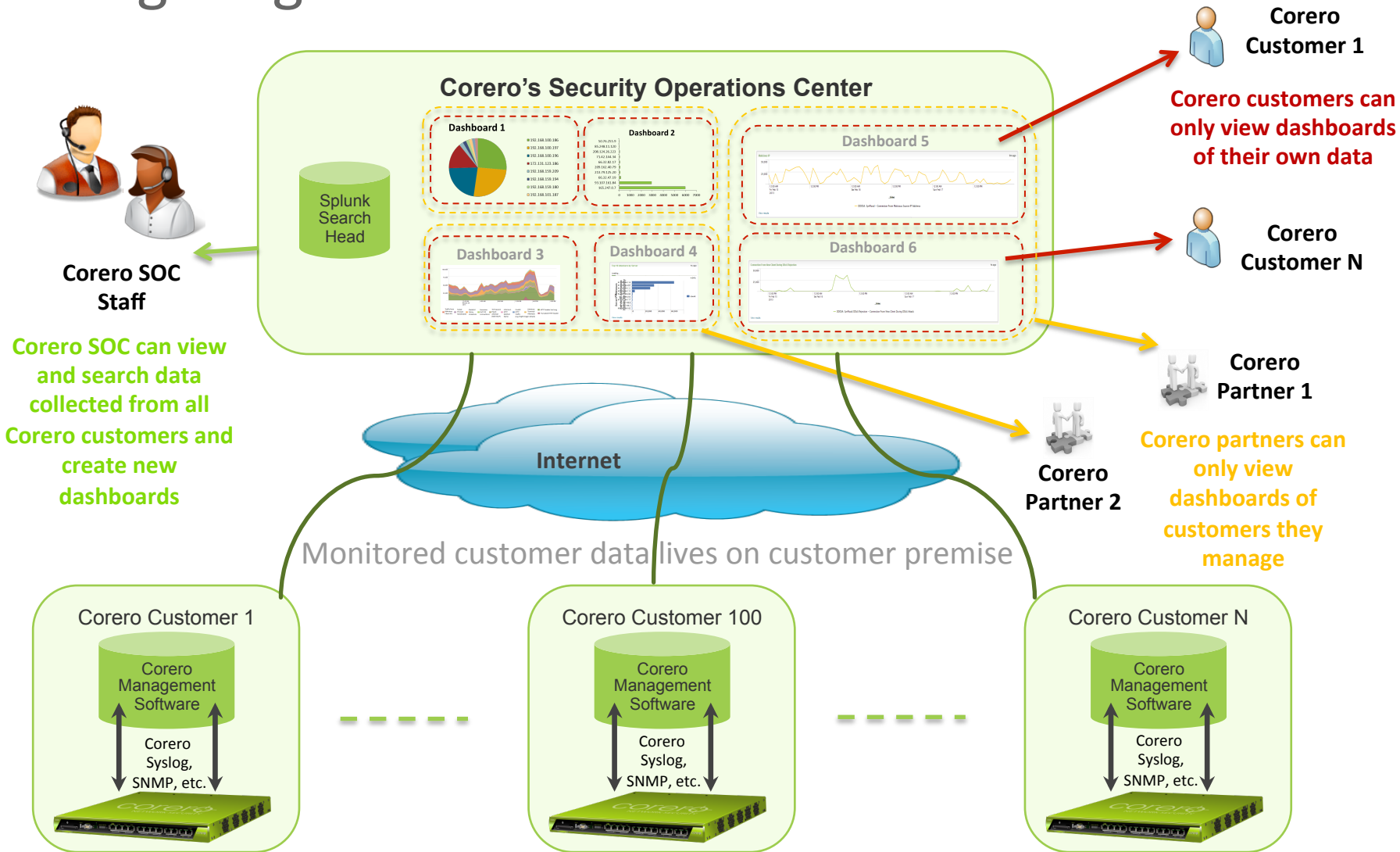
# DDoS Mitigation Architecture

How are your Denial of Service mitigation capabilities deployed?



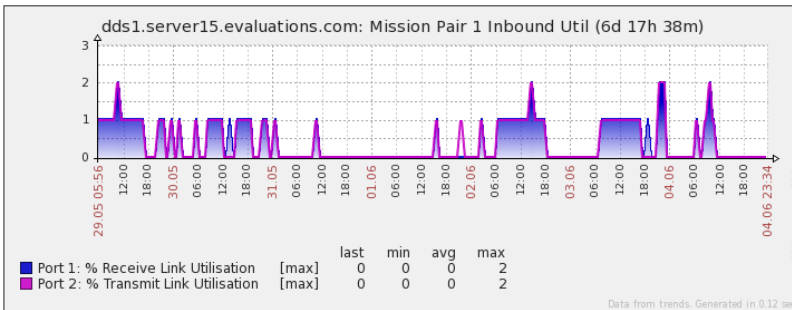
© 2014 The SANS™ Institute – [www.sans.org](http://www.sans.org)

# Mitigating 'the Attack'



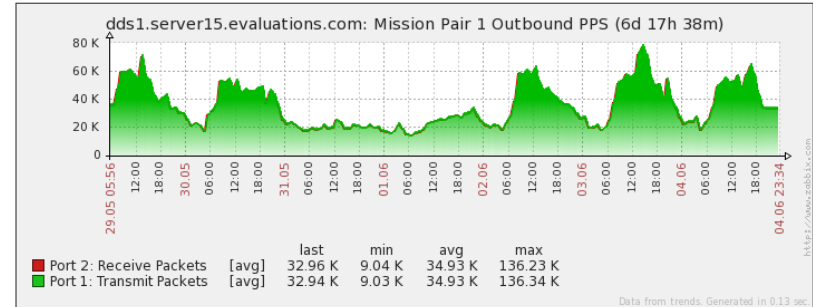
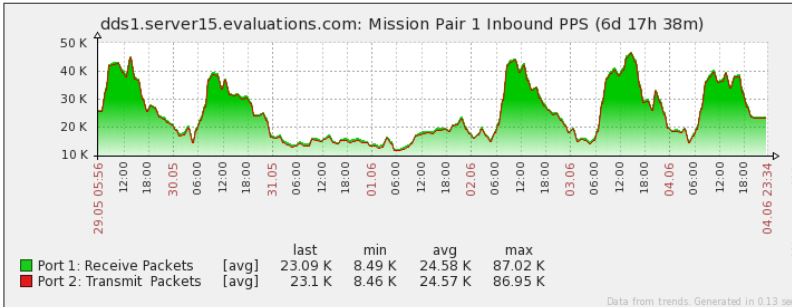
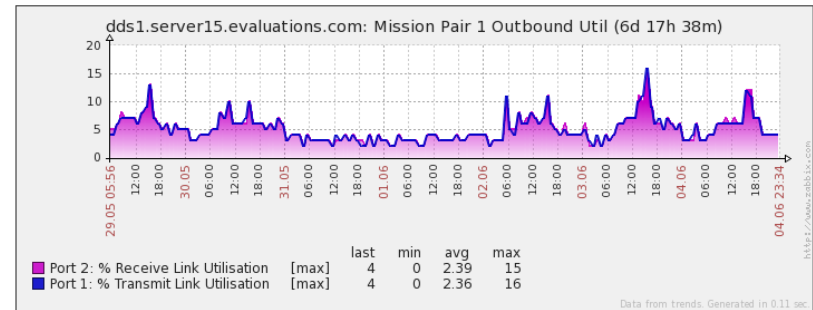
Timestamp dds1.server15.evaluations.com: Port 1: Speed

04 Jun 2014 22:26:04 FDX\_10000



Timestamp dds1.server15.evaluations.com: Port 2: Speed

04 Jun 2014 22:26:04 FDX\_10000



Activities VirtualBox Fri 13 Jun, 08:50 eni peter

Windows 7 [Running] - Oracle VM VirtualBox

Machine View Devices Help

www.evaluations.com/host\_screen.php?hostid=30030000000010981&screenid=3003000000000089&sid=5ac3d785757fd2a8

Corero Evaluations Corero Network Securi...

### dds1.server15.evaluations.com: Flows: Total Usage (3d 14h 6m)

Flows: Total Usage [all] last 33.73 K min 8.51 K avg 25.42 K max 42.94 K

Data from trends. Generated in 0.13 sec.

### dds1.server15.evaluations.com: Flows: Used TCP (3d 14h 6m)

Flows: Used TCP [all] last 21 K min 3.08 K avg 15.31 K max 28.46 K

Data from trends. Generated in 0.11 sec.

### dds1.server15.evaluations.com: Flows: Used UDP (3d 14h 6m)

Flows: Used UDP [all] last 12.47 K min 4.56 K avg 9.85 K max 16.76 K

Data from trends. Generated in 0.09 sec.

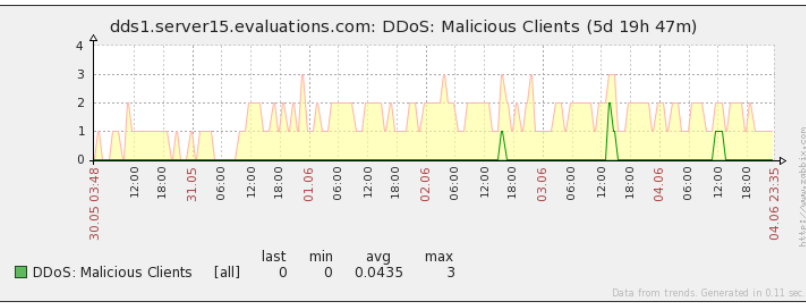
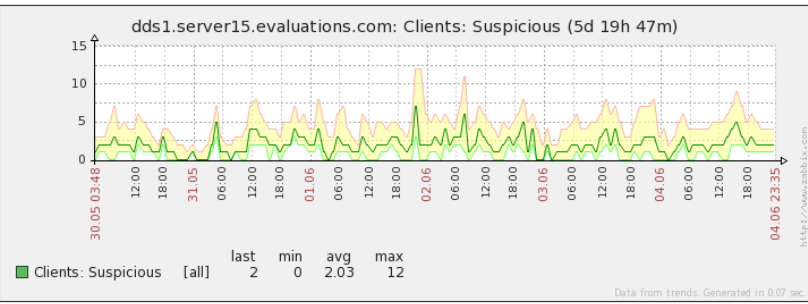
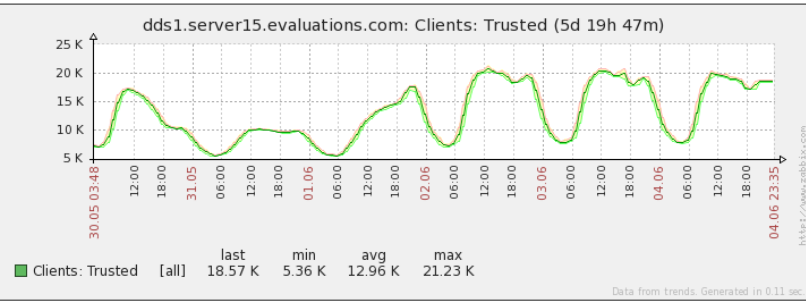
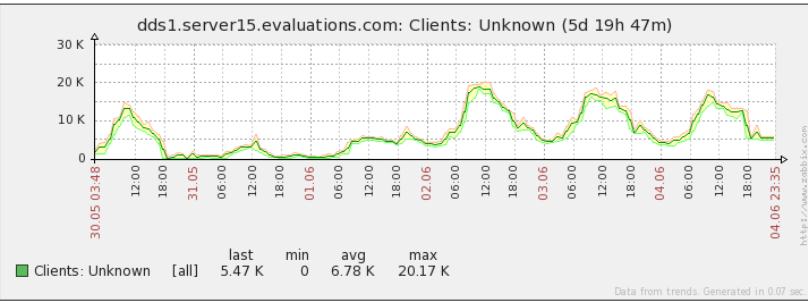
### dds1.server15.evaluations.com: IP: Used Other (3d 14h 6m)

### dds1.server15.evaluations.com: Flows: Aged (3d 14h 6m)

Right Ctrl

■ Rate Based: Client Rate Limiting [all] last 0 pps min 0 pps avg 0 pps max 0 pps  
Data from trends. Generated in 0.10 sec

■ Rate Based: Connection Limiting [all] last 0 pps min 0 pps avg 0 pps max 0 pps  
Data from trends. Generated in 0.09 sec



VM VirtualBox

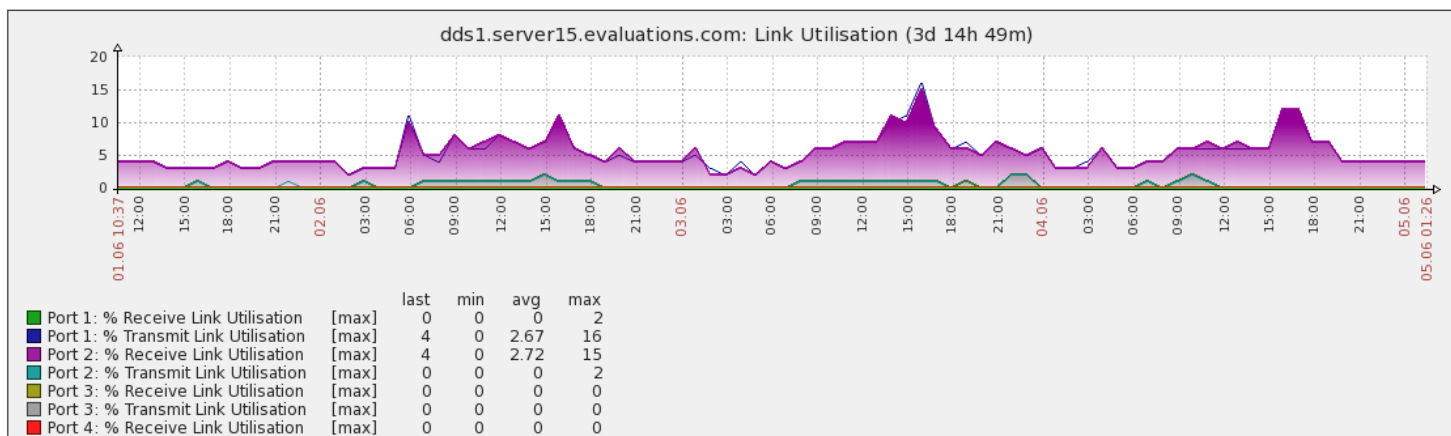
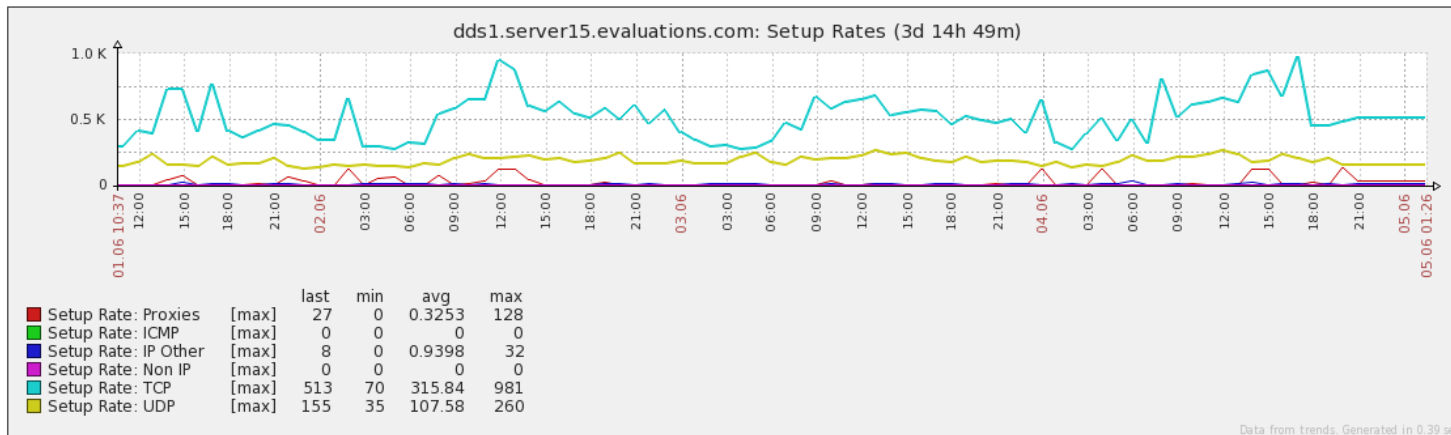
P

+

een.php?hostid=30030000000010981&screenid=3003000000000097&sid=5ac3d785757fd2a8

Google

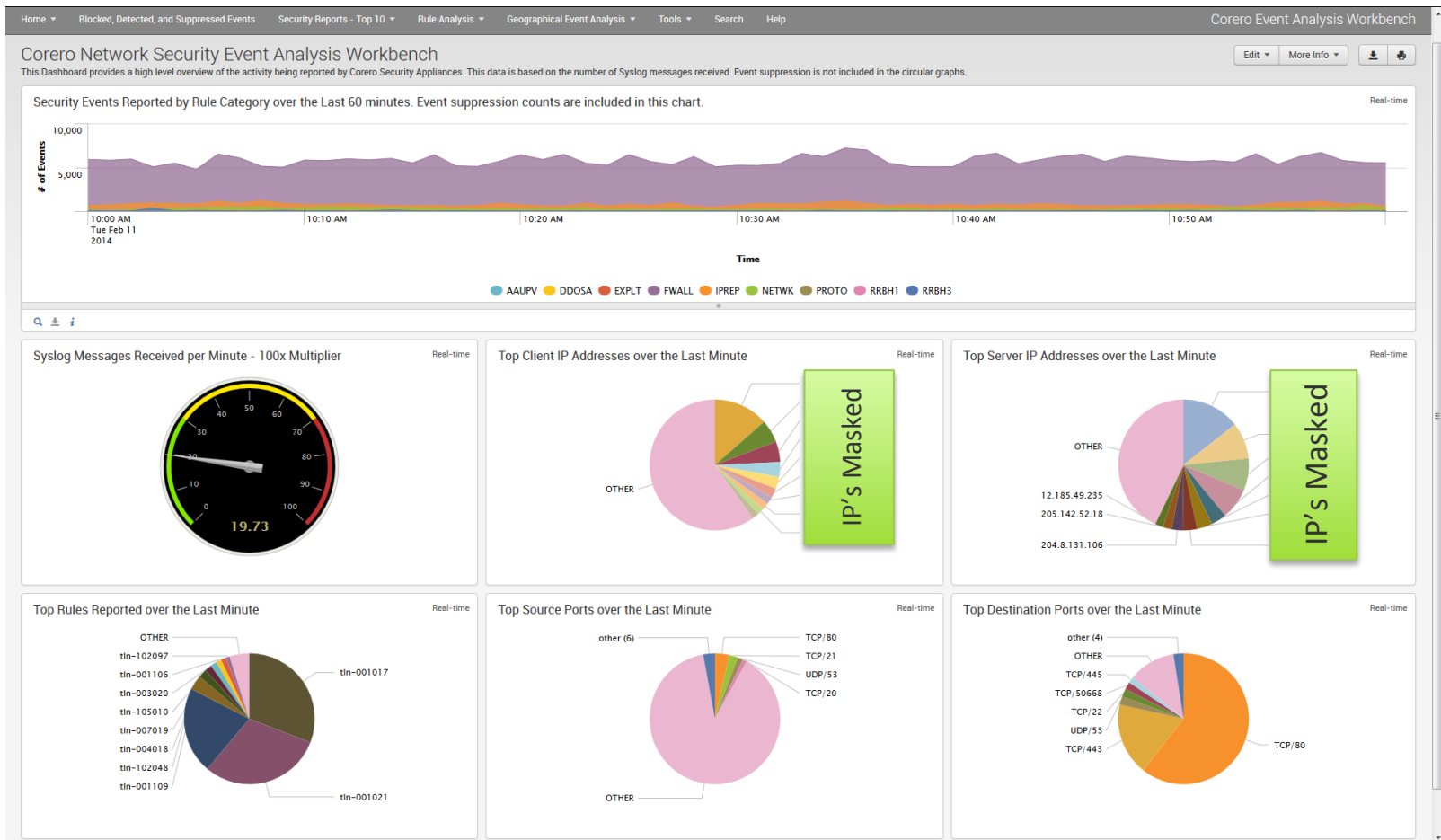
rk Securi...



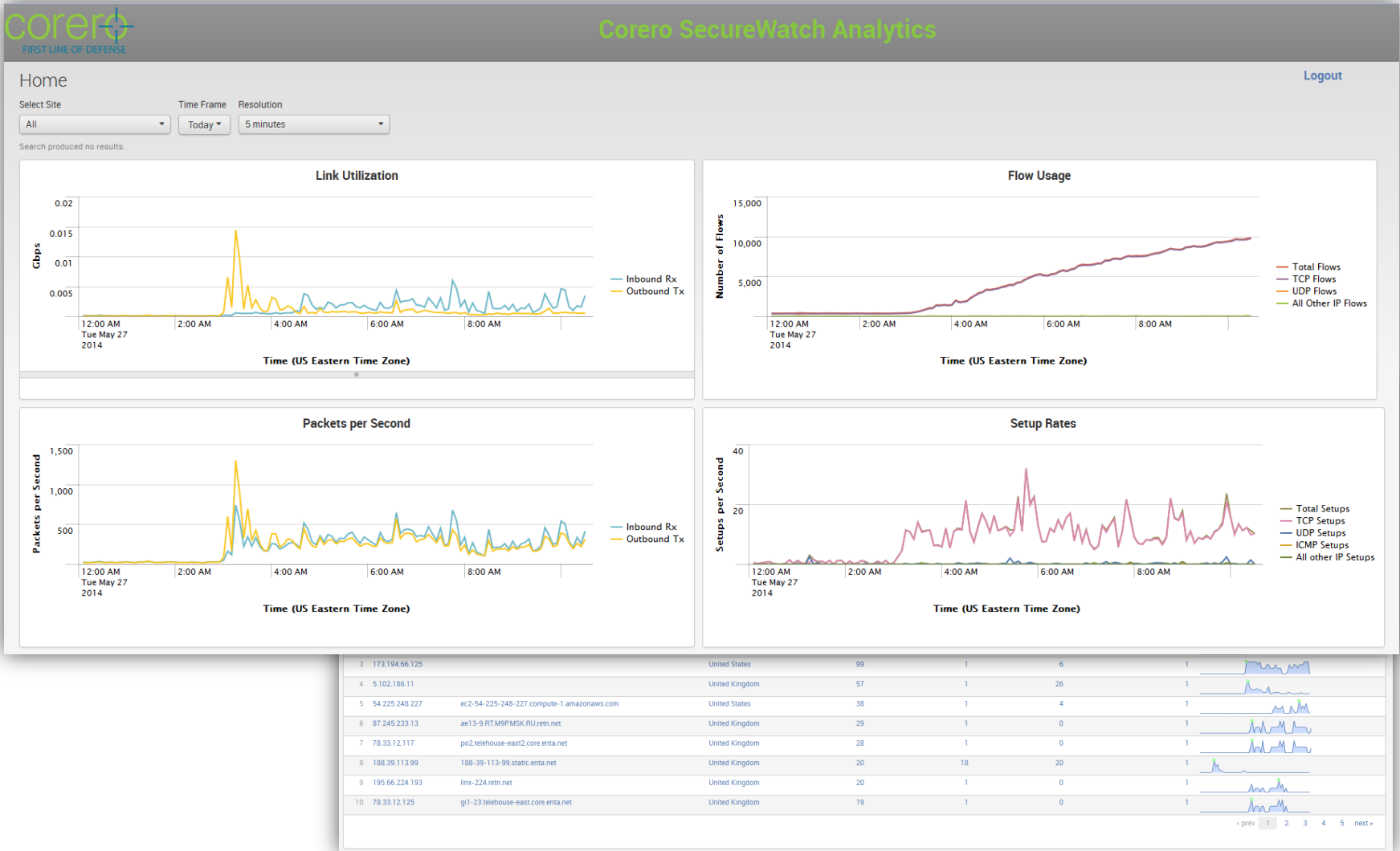


# Security Event Reporting

## Answer who is attacking what...

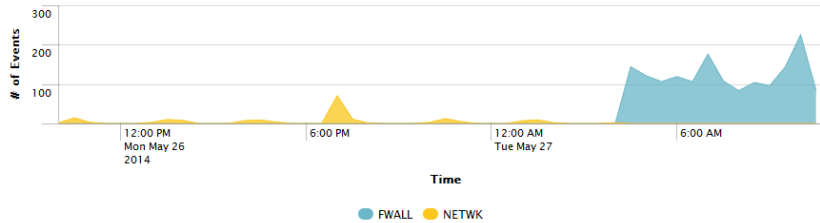


# ..with additional network metrics...

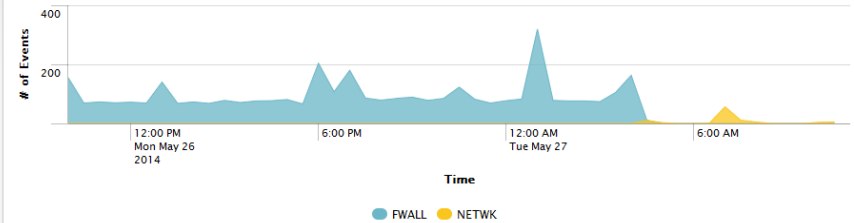


# ..Application Protocol Analysis ...

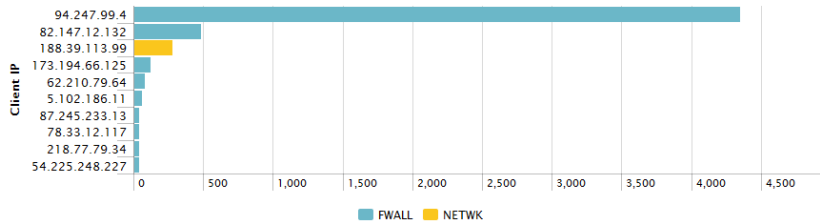
Security Events Reported for Inbound Blocked Traffic by Rule Category



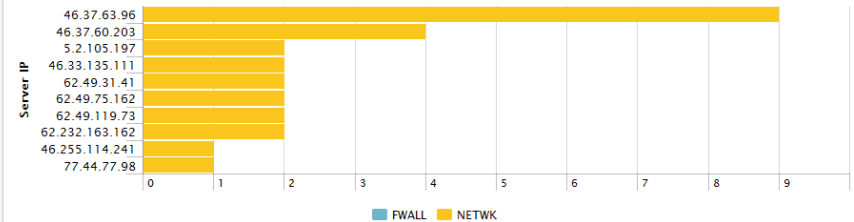
Security Events Reported for Outbound Blocked Traffic by Rule Category



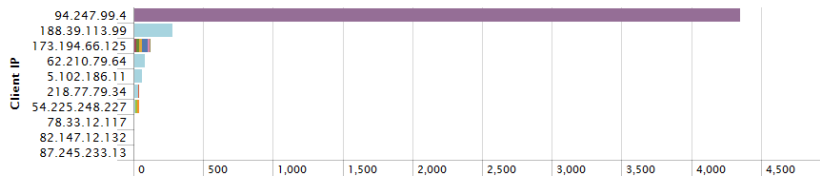
Top 10 Client IP Addresses that were Blocked by Rule Category



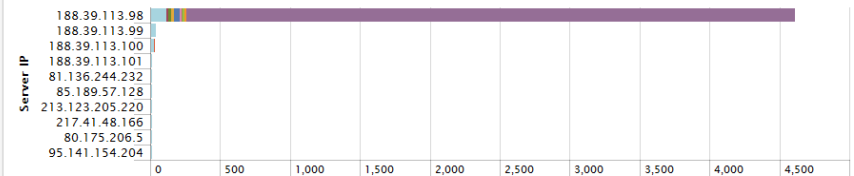
Top 10 Server IP Addresses that were Blocked by Rule Category



Top 10 Client IP Addresses that were Blocked by Protocol



Top 10 Server IP Addresses that were Blocked by Protocol





# SecureWatch – Top 3 Network Operator Relevant ‘Security Events’

~~Number 4: ‘SYN Flood’:~~

**SO 2012!**

## Number 3: Open DNS Resolvers

**SO 2013!**

**Victims are multiple:**

- Client performing lookup for the spoofed source (Real Victim!)
- Root name servers being queried.
- Backbone providers.

## Number 2: NTP

Amplification factor = ☺

UDP/123

Asking the Question:

```
Ntpdc -n -c monlist <Address>
```

Use nmap to scan for reflectors

```
nmap -sU -A -PN -n -pU:19,53,123,161 --script=ntp-monlist,dns-  
recursion,snmp-sysdescr <target>
```

**So  
November  
2013!**



# Number 1: SNMPv2..wait, what?

Amplification factor = 😊

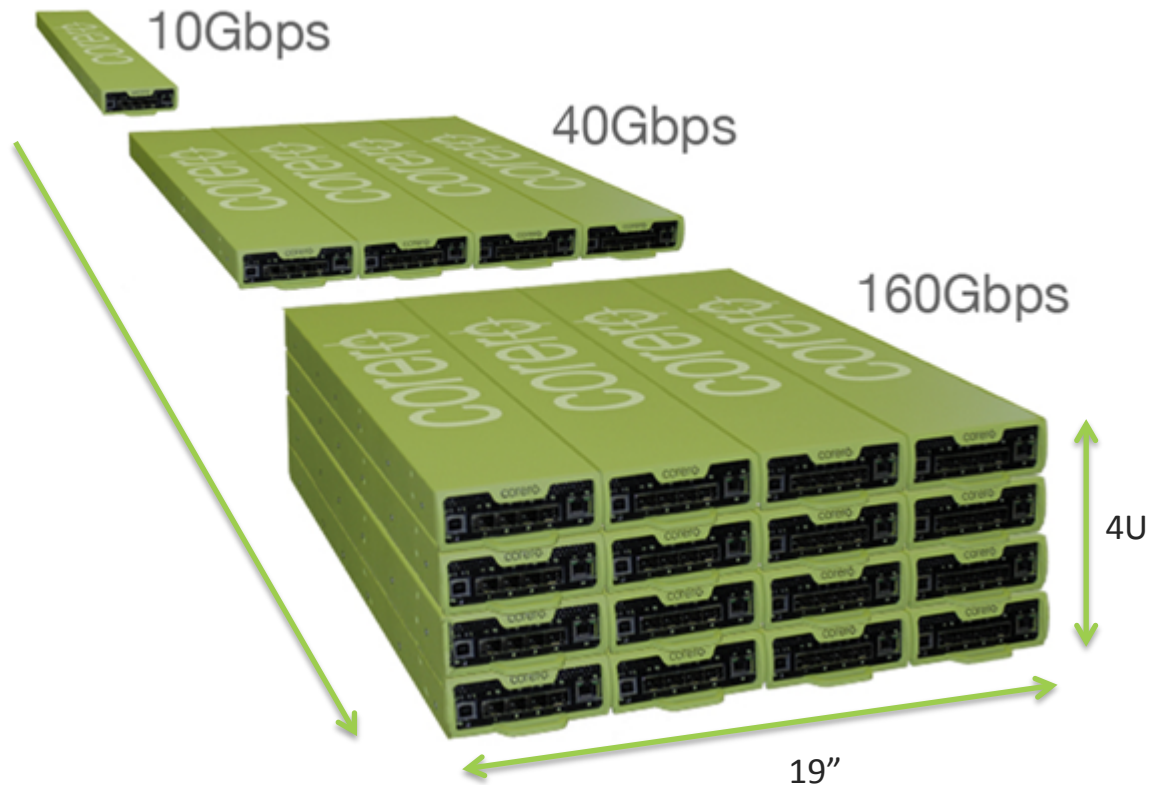
UDP/161

- SNMP Polling enabled.
- Queries sent that match the community string. Guess? 'Public' or 'Private'?..'noAuth' for SNMPv3..
- Botnet sends 'GetBulkRequest' or 'Get' query
- Spoof the source (Easy with UDP transport)
- For IPv4:
  - Question: 60 - 102bytes
  - response: 423 – 1560bytes

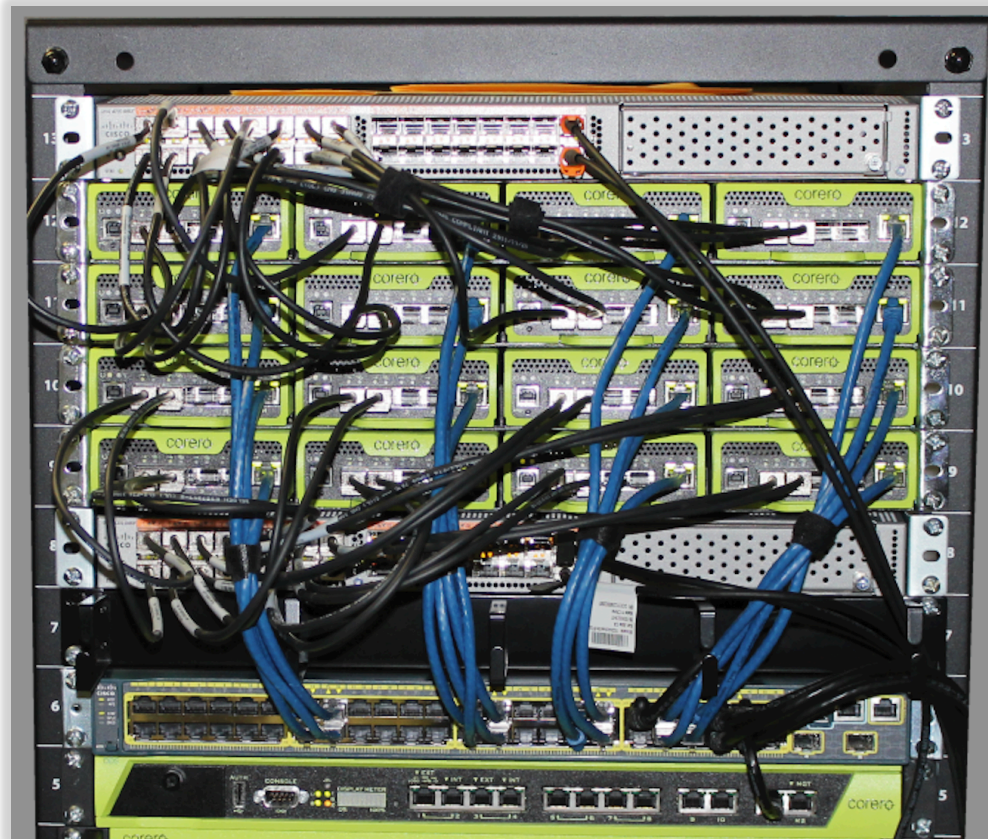
# SmartWall TDS – Power in a Small Package

- Scalable Deployment
- Increments of 10 Gbps, 30M PPS

¼ rack width



# SmartWall TDS – Power in a Small Package

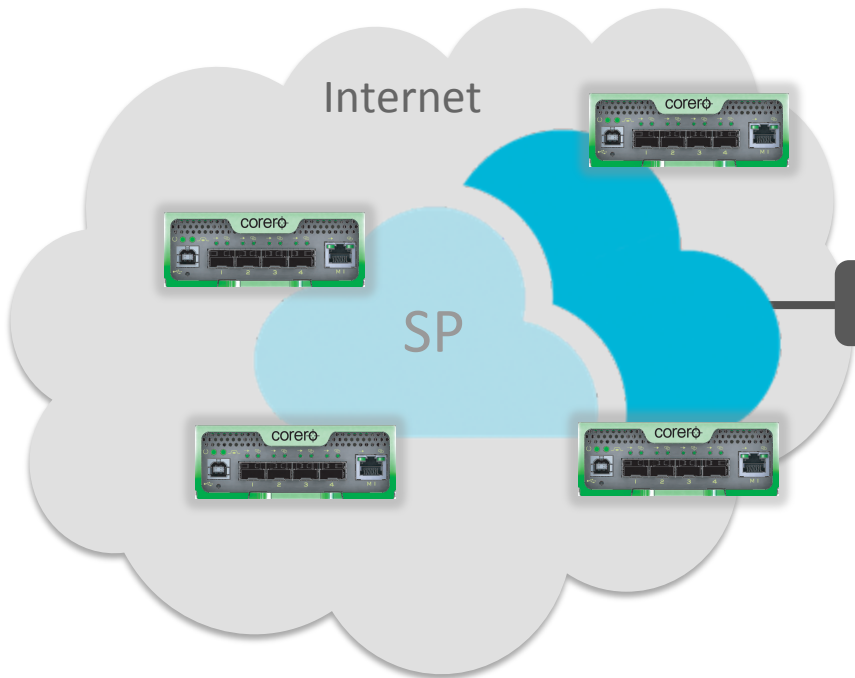


- ← ■ Nexus 5000
  - 8 way LACP
- ← ■ 80G (8x10G) NTD
- ← ■ 80G (8x10G) NTD
- ← ■ Nexus 5000
  - 8 way LACP
- ← ■ 1G Management Network



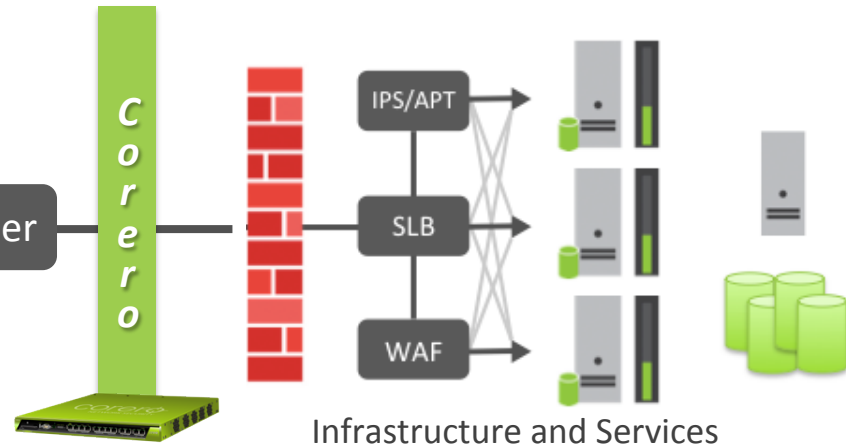
# Corero's Portfolio

## SmartWall Threat Defense System



In the Cloud

## First Line of Defense



Corero

On Premises



# Thank you

[Peter.cutler@corero.com](mailto:Peter.cutler@corero.com)

Twitter: Bleuhat

