DDoS attacks and rise of IoT botnets

RIPE 75 – Dubai , UAE

Khaled Fadda

Consulting Engineer , Arbor Networks – Middle East

kfadda@arbor.net

Things You Should Know About DDoS Attacks

- Its never been easier in history to launch a DDoS attack.
- DDoS attacks are increasing in size, frequency and complexity.
- DDoS attacks are used as smoke screens or forms of diversion during advanced threat campaigns.
- Of the Top 3 causes of unplanned outages, DDoS attacks are the most costly to an organization.

Did You Know?

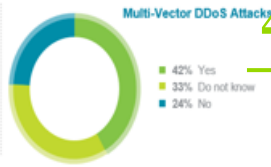
$5:$100sK

DDoS for Hire

For $5/hr anyone can launch a DDoS attack an cause $100sK in damage

400Gbps …DDoS attack size increasing [1]

74% …involved DDOS as a diversion[2]



42% …experienced multi-vectored attacks[1]

78% …Increase in demand for DDoS Protection services[1]

DDOS BACKGROUND

- What is a DDoS “ Distributed Denial Of Service” attack ?
  - An attempt to consume finite resources, exploit weaknesses in software design or implementations , or exploit lac of infrastructure .
  - Target the availability and utility of computing and network resources.
  - DDoS attacks effect availability! No Availability , no applications/services/data/internet ! NO revenue!
  - Attacks are almost always distributed for more significant effect.

AVAILABILITY IS HARD !

- **The Primary goal for DDoS defense is maintaining availability in the face of the attack.**
- Maintaining availability in the face of attack requires a combinations of skills, architecture, operational agility, analytical capabilities and mitigation capabilities.
- In Practice, most organizations never take availability into account when designing /speccing /building/deploying/testing/online apps/services/properties.
- In Practice, most organizations never make the logical connection between maintaining availability and business continuity.
- In practice, most organizations never stress-test their apps serves stacks in order to determine scalability/resiliency shortcomings and proceed to fix them.
- In practice, most organizations do not have plans for DDoS mitigation – or if they have a plan , they never rehearse it!

DDOS ATTACKS

- DDoS attacks can consist of just about anything
  - Large quantities of raw traffic designed to overwhelm a resource or infrastructure
  - Application specific traffic designed to overwhelm a particular service – sometimes stealthy in nature
  - Traffic formatted in such a way to disrupt a host from normal processing
  - Traffic reflected and/or amplified through legitimate hosts
  - Traffic from compromised sources or from spoofed IP addresses
  - Pulsed attacks – start/stop attacks
- DDoS attacks can be broken out by category

DDOS ATTACK CATEGORIES

Volumetric, Brute Force attacks

- **Traffic Floods**
  - Exhaust resources by creating high bps or pps volumes
  - Overwhelm the infrastructure – links, routers, switches, servers

Layer 4-7, Smart attacks

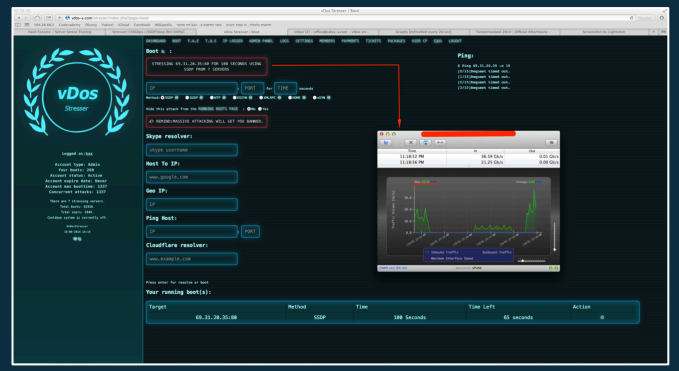
- **TCP resource exhaustion**
  - Exhaust resources in servers, load balancers, firewalls or routers
- **Application Layer**
  - Take out specific services or applications

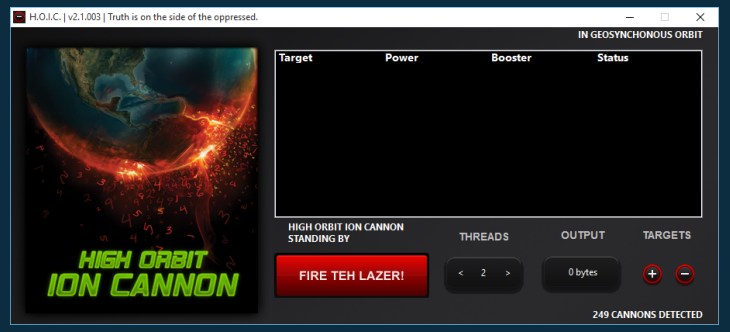
THE DDOS ATTACK SURFACE

- Any part of your network or services that is vulnerable to an attack
  - Network Interfaces
  - Infrastructure
  - Firewall/IPS
  - Servers
  - Protocols
  - Applications
  - Databases
- Attackers will find the weakness

The weaponization of DDoS

”Weaponize” : *Convert to use as a weapon / simplify use as weapon*



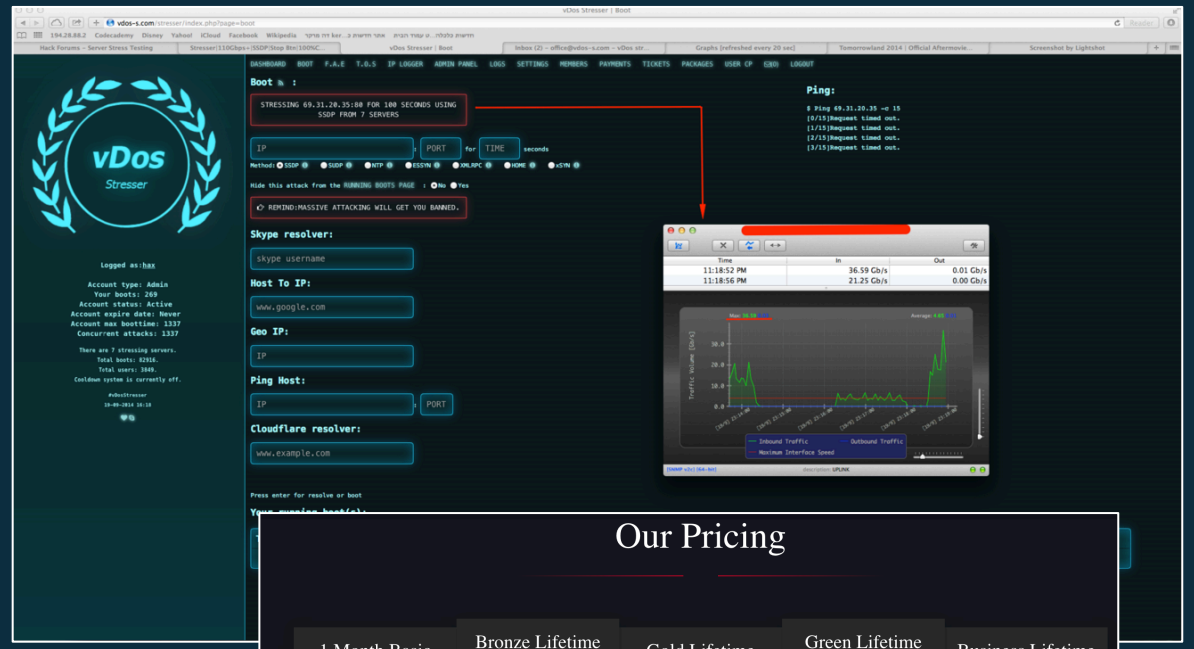


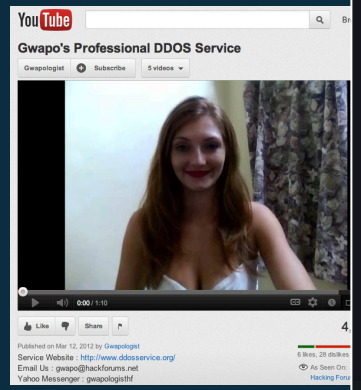
- Increased availability of “Stresser Tools”/”Booters” which perform highly distributed attacks using a combination of non-spoofed and spoofed amplification attacks. Often linked to bot-farms.

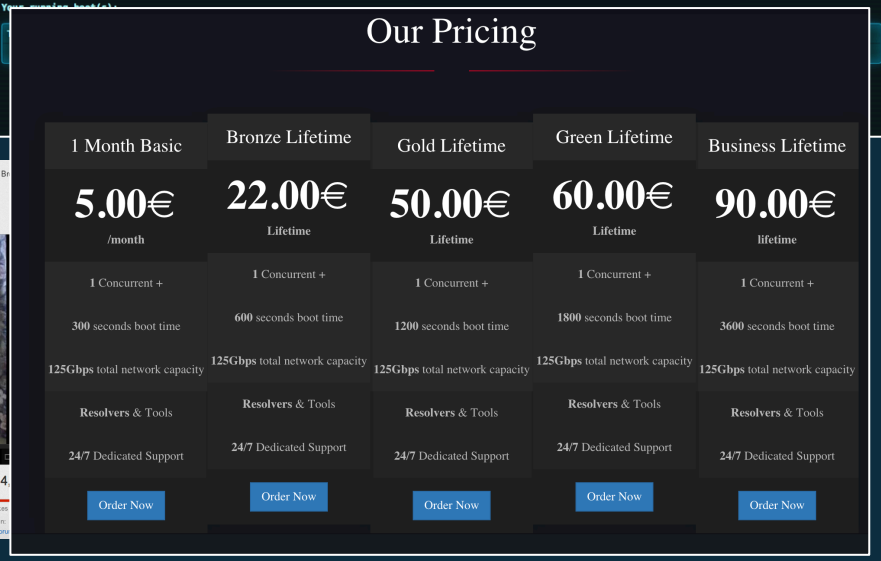
- Development of tools for use by voluntarily opt-in attackers:
  - Low Orbit Ion Cannon used to perform non-spoofed UDP/ICMP attacks
  - High Orbit Ion Cannon sends non-spoofed HTTP requests against multiple sites

ARBOR NETWORKS

DDoS tools for the masses



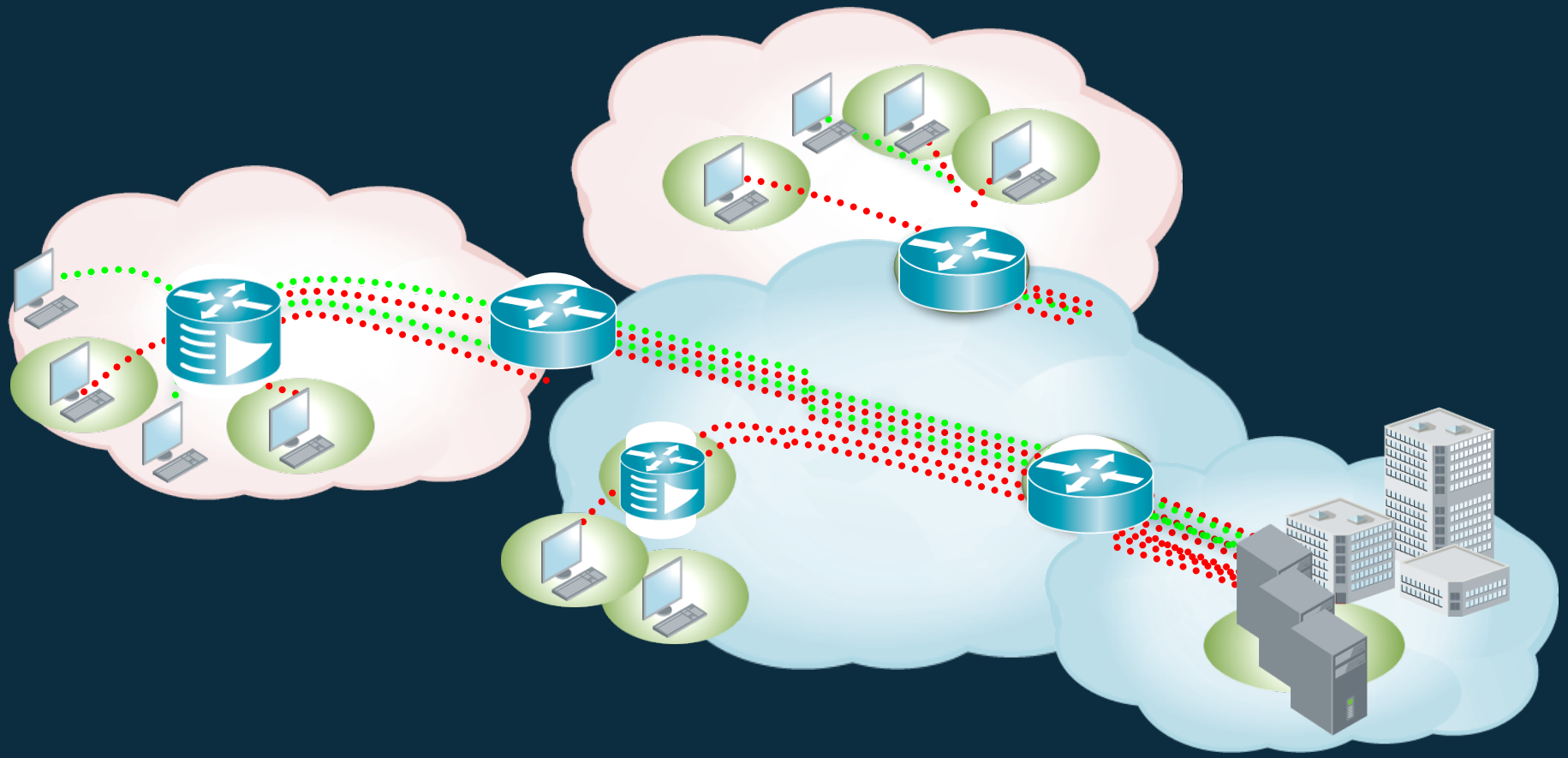




- Anyone which has the capability to click a button can now launch an DDoS attack.
- Cheap and simple to use:
  - VIP accounts!
  - Lifetime subscription!
  - 24x7 customer support!
- Primarily used by gamers attacking each other but recently we have been seeing them used to attack highly visible targets.

ARBOR NETWORKS

How a DDoS attack works?



During a **Distributed Denial of Service (DDoS) attack**, [compromised] hosts or **bots** coming from distributed sources overwhelm the target with [il]legitimate traffic so that the servers cannot respond to legitimate clients.

➔ **Critical services are no longer available!**

BOTS AND BOTNETS

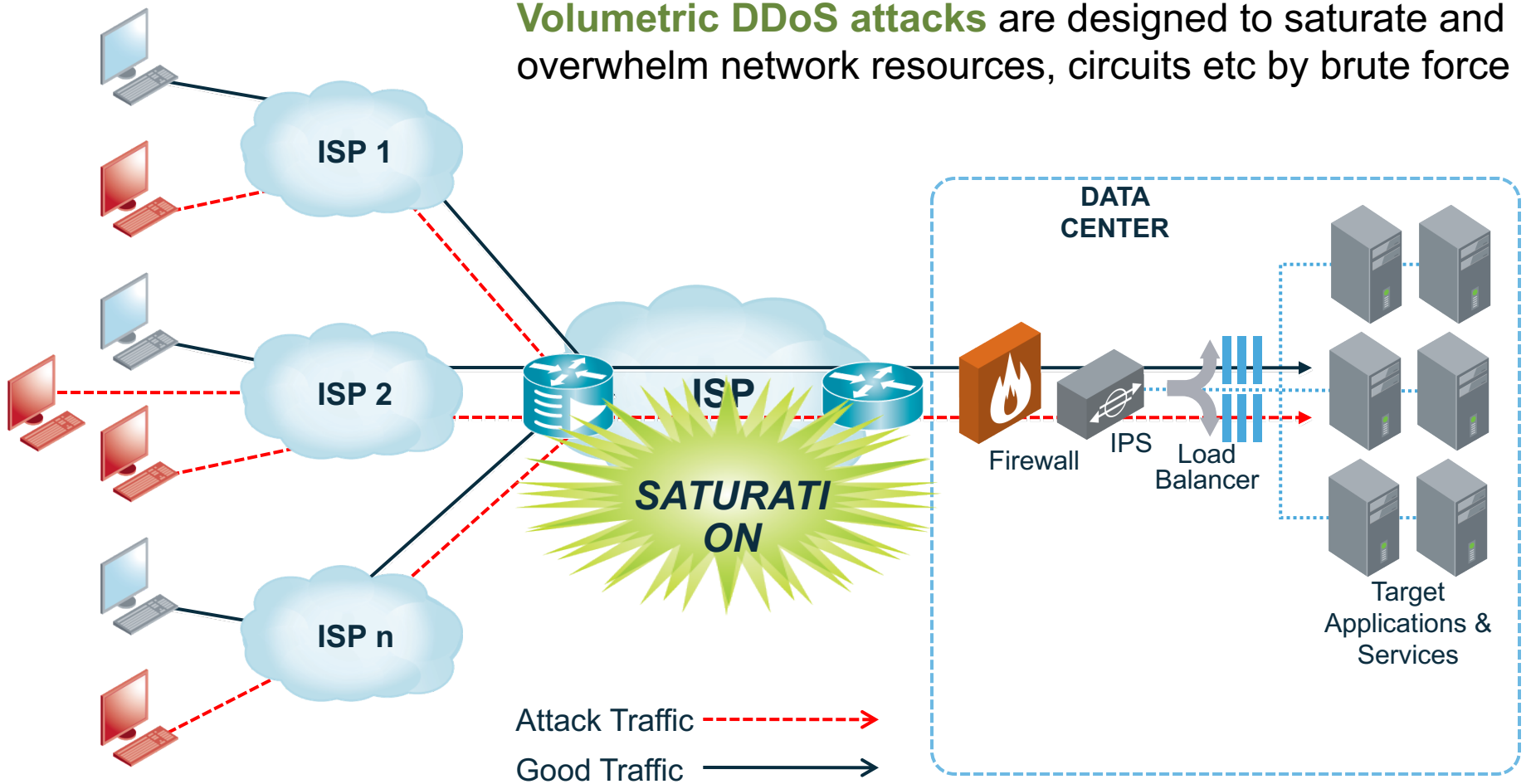
- Botnets can have 100,000s of Bots
- Why use Bots to attack a destination?
  - Cheap
  - Practically untraceable
  - No one tries to clean up the bots

same prices, and the average rate for taking a Web site offline is surprisingly affordable: about $5 to $10 per hour; $40 to $50 per day; $350-$400 a week; and

Cost of a botnet to take a website off-line is as little as **$50 per day**

DDoS Attacks: Volumetric

Volumetric DDoS attacks are designed to saturate and overwhelm network resources, circuits etc by brute force



HIGH BANDWIDTH VOLUMETRIC DDOS

Description

- Large volume of traffic in bps and/or pps.
- Traffic could be spoofed or not spoofed.

Affect on Network

- Network links become saturated.
- Software-based routers, switches, firewalls, ISPs get overwhelmed.

Affect on Services

- Legitimate users can't get to services.

Common Names

- Packet flood, UDP flood, TCP flood

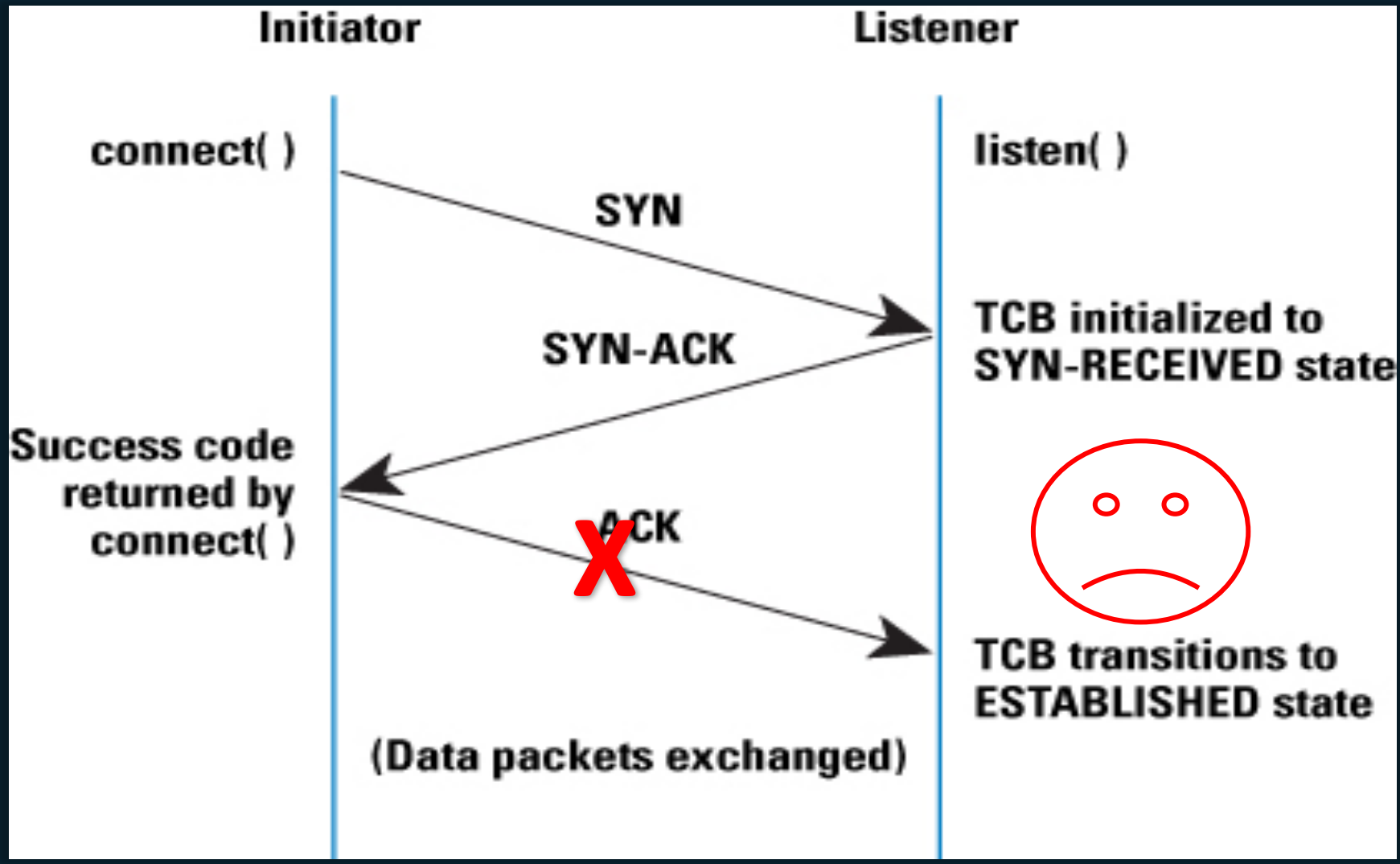
UDP Flood Attacks

- UDP is stateless, making it a common tool for flood attacks
  - Generation of UDP packets is easy
  - Stateless implies spoofing source IP addresses is possible
  - BPS and PPS: packet sizes may range from 60 to 1500 bytes
    - High volume of small packets can cause forwarding issues for routers and firewalls and other inline devices
    - 1Mpps @ 60bytes = 458Mbps
    - 1Mpps @ 1400bytes = 10Gbps
- UDP Floods do not generally impact services (unless DNS) but do impact the infrastructure causing collateral damage
  - UDP Floods can cause jitter and latency, impacting other services like VoIP

SYN Flood Attacks

- SYN flood attacks attempt to exhaust the server side resources for TCP connections
- Source(s) continuously send packets with just the SYN bit set
- Victim (Server) must open a connection and send a SYN-ACK back to the source
- Connection is kept open
  - Source ACK's and then data is exchanged
  - Source terminates connection
  - Server times out the connection
- SYN packets are typically small in size

TCP Stack Attack – Syn Flood Attack



Reflection Attacks

Description

- Attackers spoof IP address of victim as source and send queries to open proxies or resolvers that then send “answers” to the victim.
- Answers may be amplified if the response is bigger.

Affect on Network

- Network links become saturated.
- Software-based routers, switches, firewalls, ISPs get overwhelmed.

Affect on Services

- Legitimate users can’t get to services.

Common Names

- DNS Reflection, NTP Reflection/Amplification

Components of a Reflection/Amplification DDoS Attack

Amplification

- Attacker makes a relatively small request that generates a significantly-larger response/reply. This is true of most (not all) server responses.

Reflection

- Attacker sends spoofed requests to a large number of Internet connected devices, which reply to the requests. Using IP address spoofing, the ‘source’ address is set to the actual target of the attack, where all replies are sent. Many services can be exploited to act as reflectors.

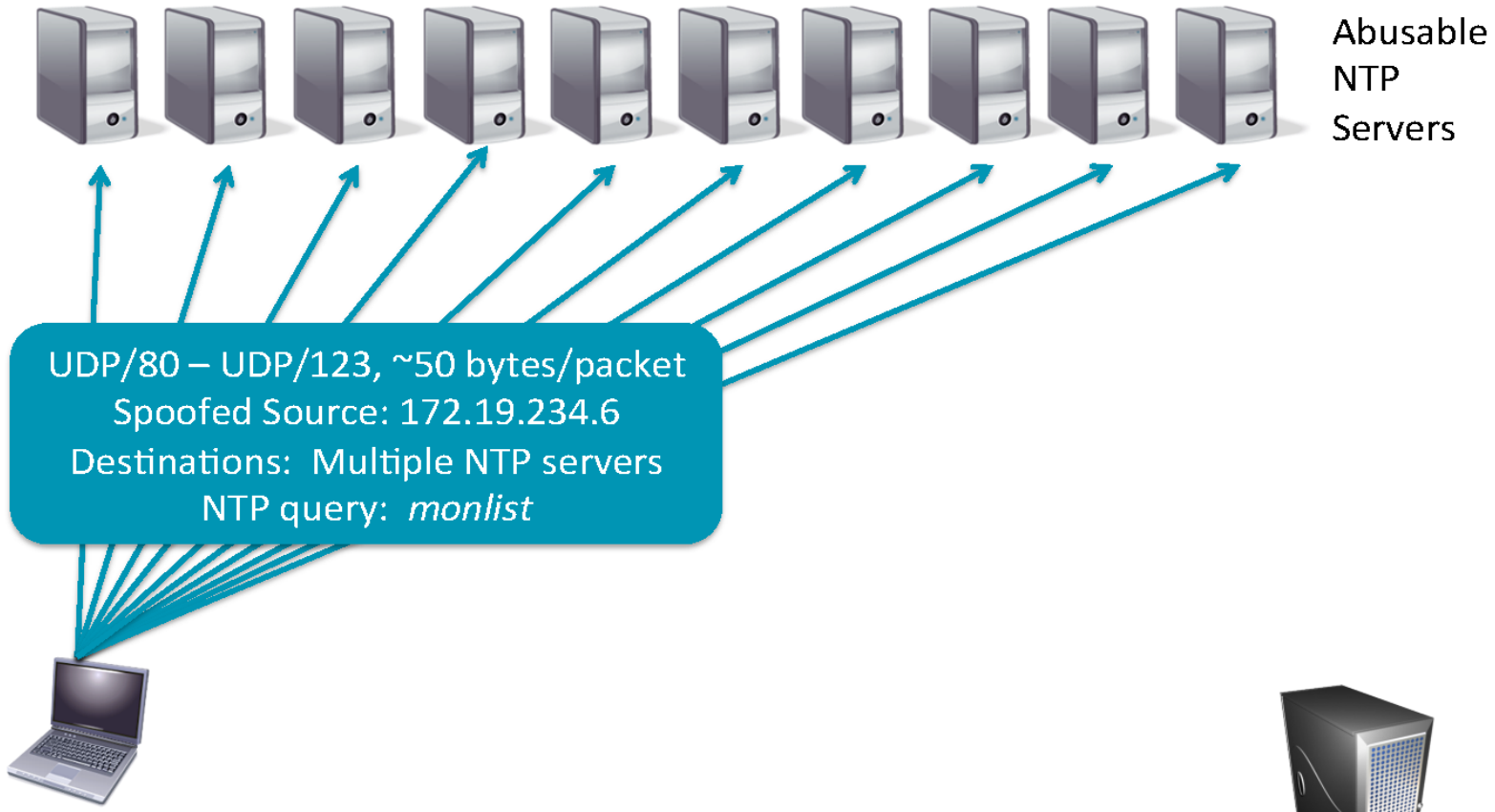
NTP Reflection/Amplification Attack Methodology

Abusable NTP Servers

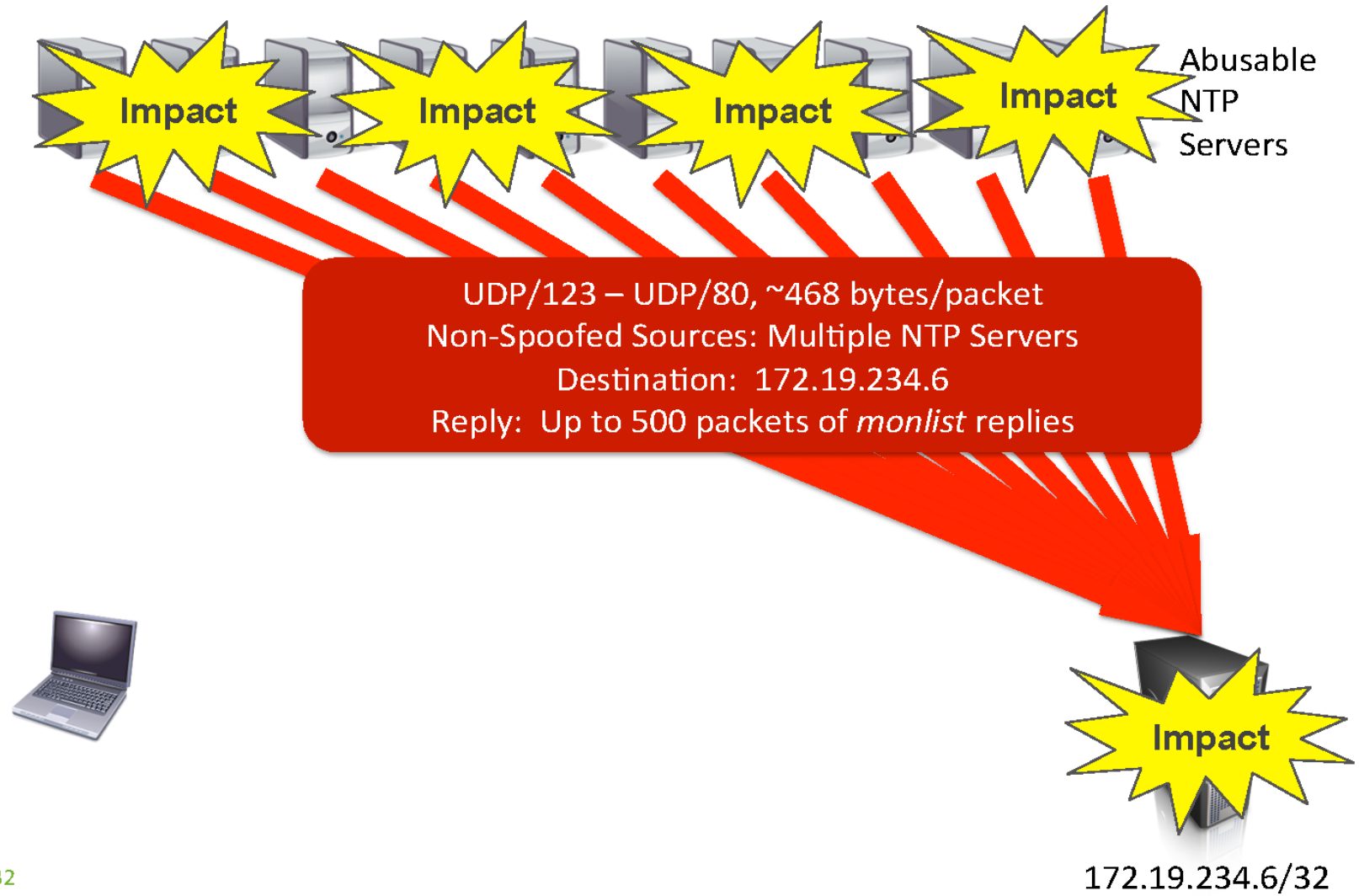
Internet-Accessible Servers, Routers, Home CPE devices, etc.

172.19.234.6/32

NTP Reflection/Amplification Attack Methodology



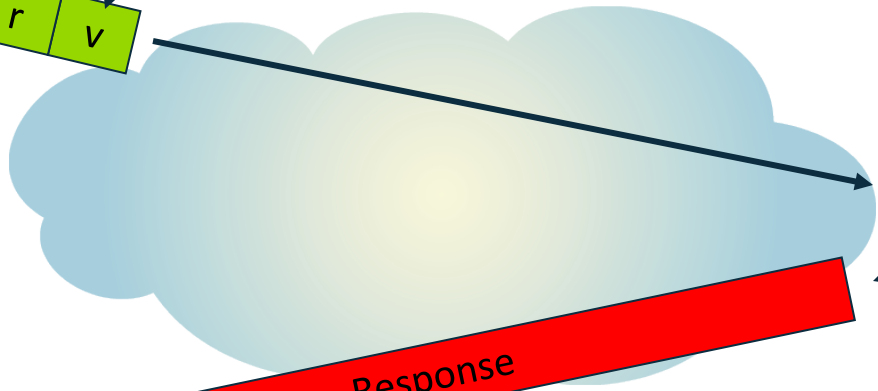
NTP Reflection/Amplification Attack Methodology

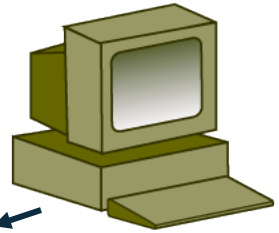


DNS Amplification Attack: UDP Flood

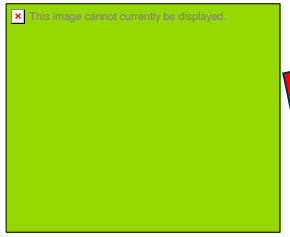
Source IP of Victim (v) spoofed when query sent to resolver (r), resolver receives, responds to v. 55-byte query elicits 4200-byte response

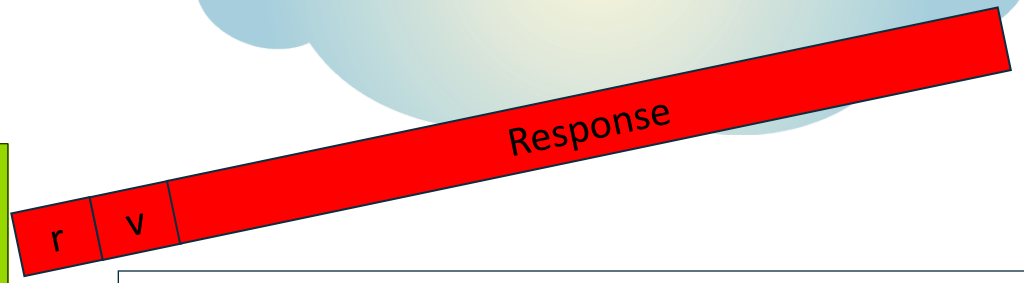
Attacker - a





Resolver - r

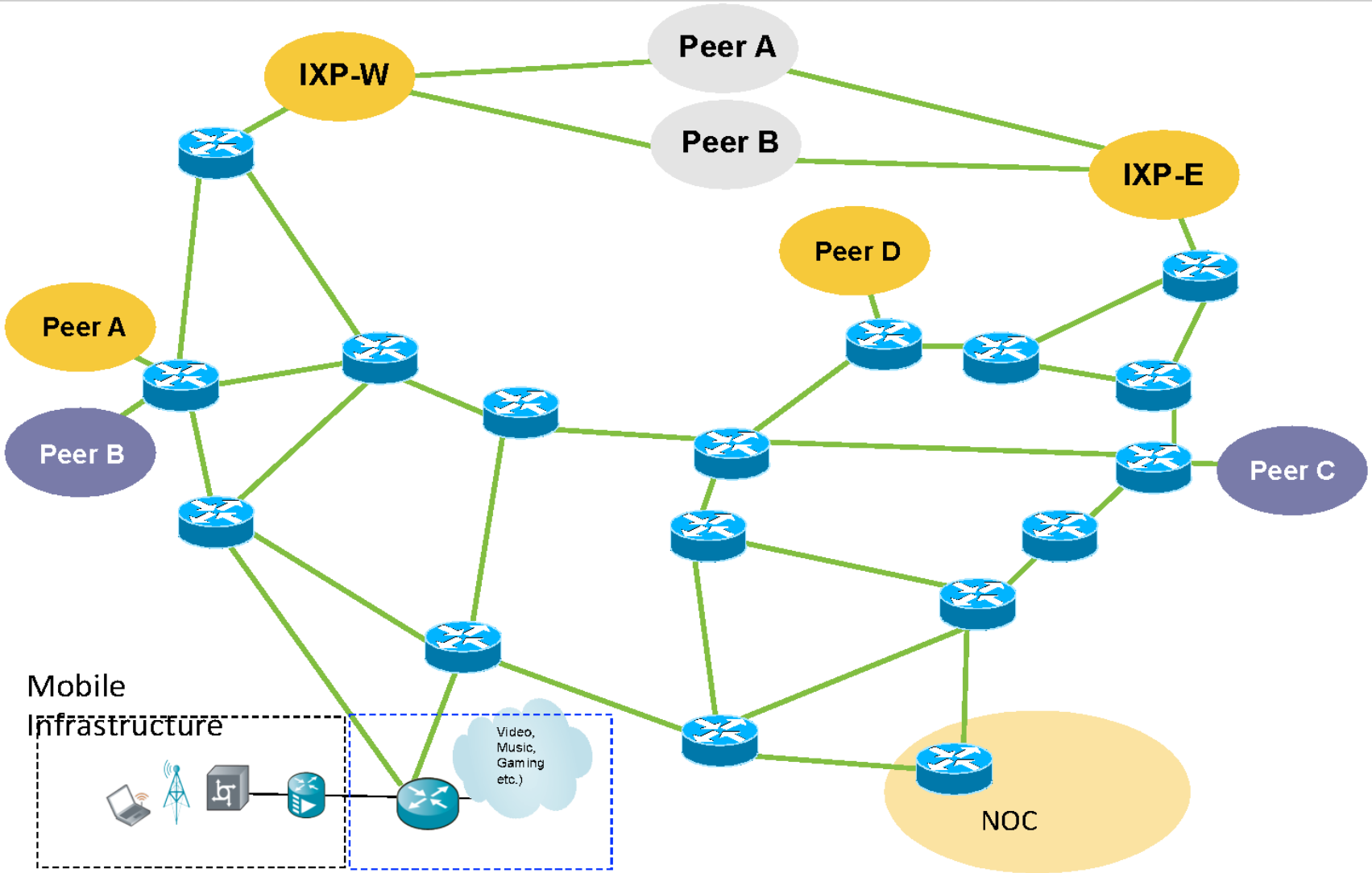




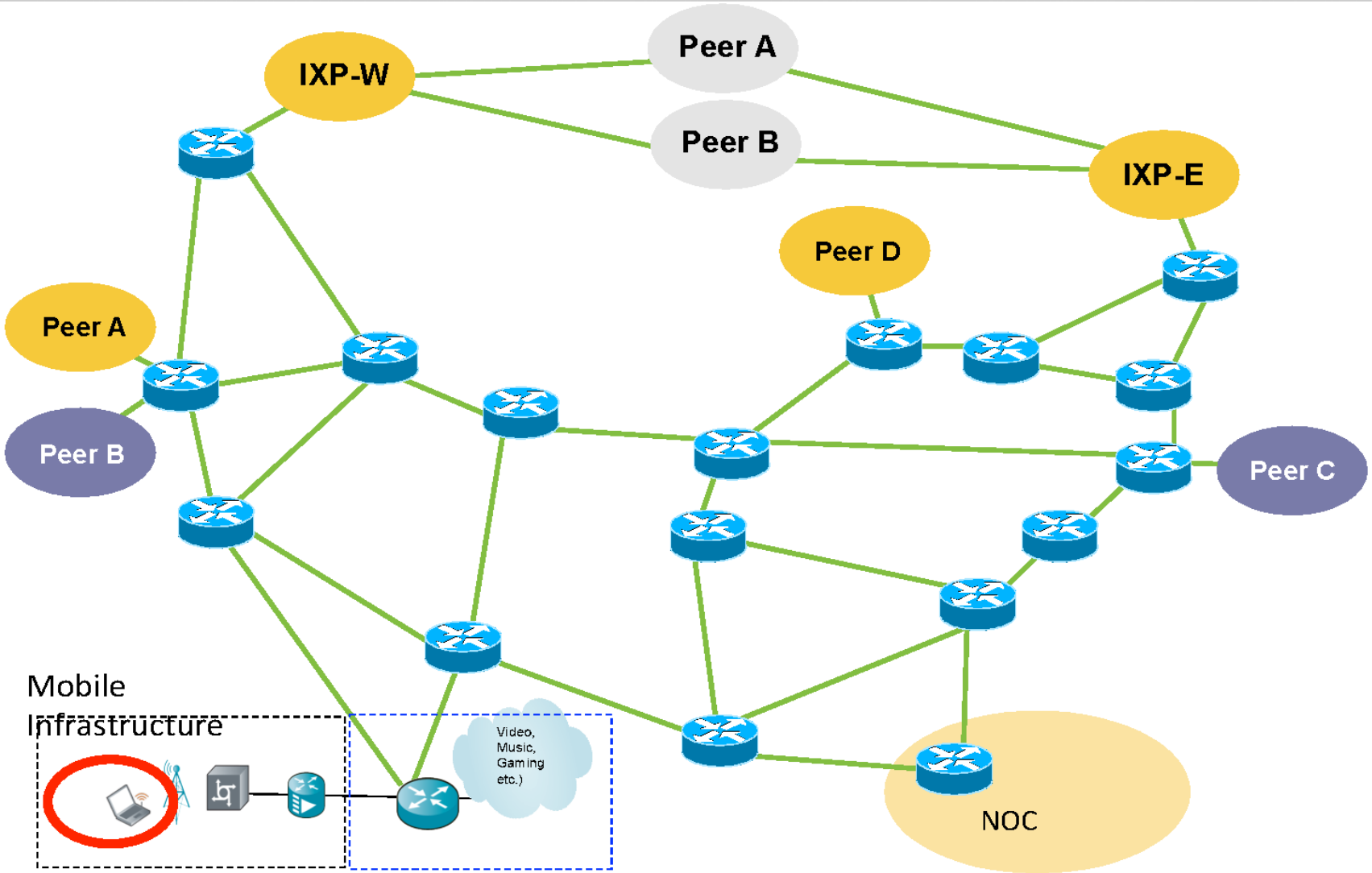
Victim - v

A botnet with as few as 20 DSL-connect homes (1 Mbps upstream each) can generate 1.5 Gbps of attack traffic with DNS reflective amplification attack vectors such as those employed for root server attacks in early 2006 (1:76 amplification factor). Most enterprises have little more than 155 Mbps Internet connectivity.

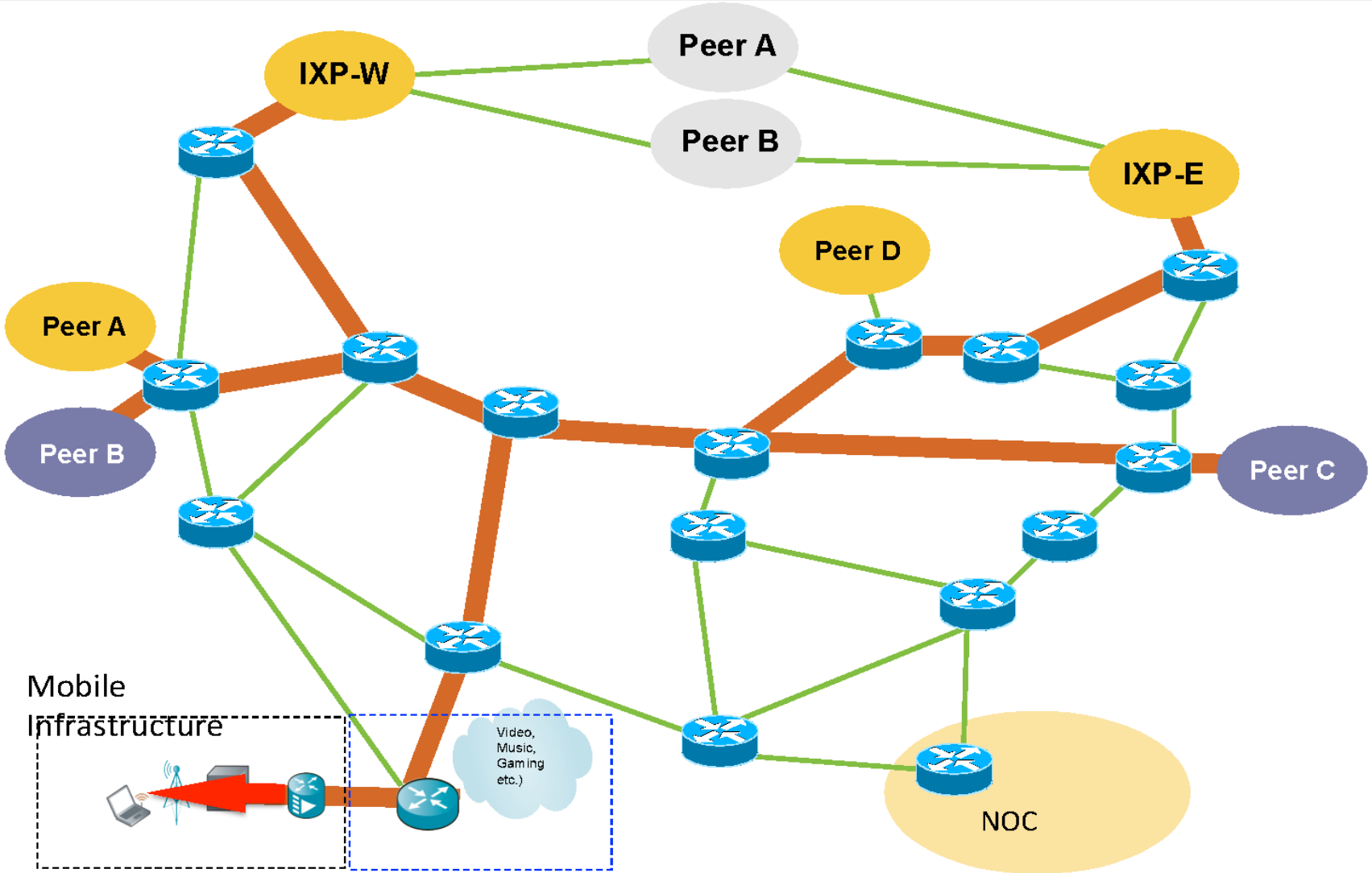
Effects of a 300gb/sec Reflection/Amplification DDoS Attack on Network Capacity



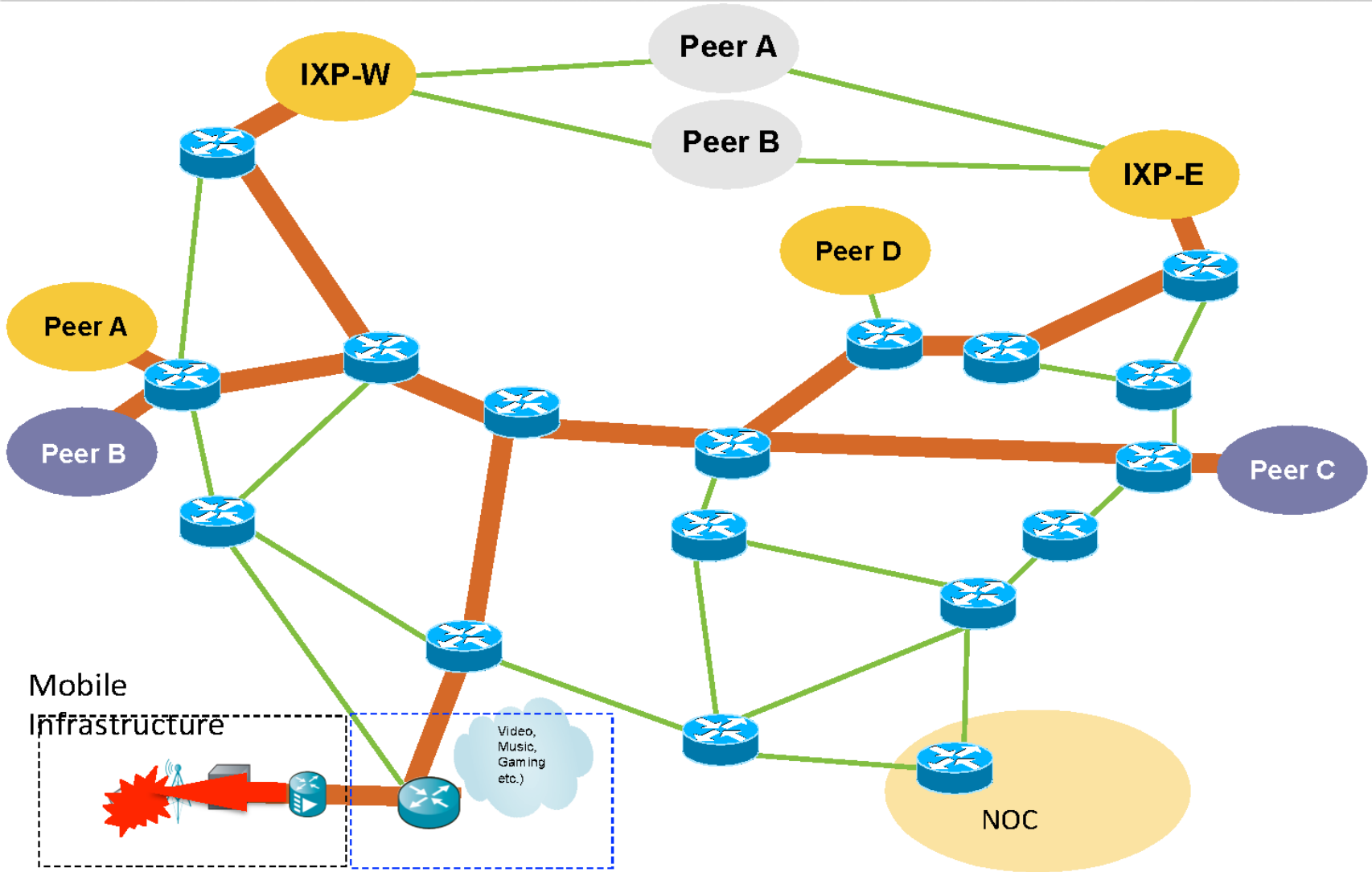
Effects of a 300gb/sec Reflection/Amplification DDoS Attack on Network Capacity



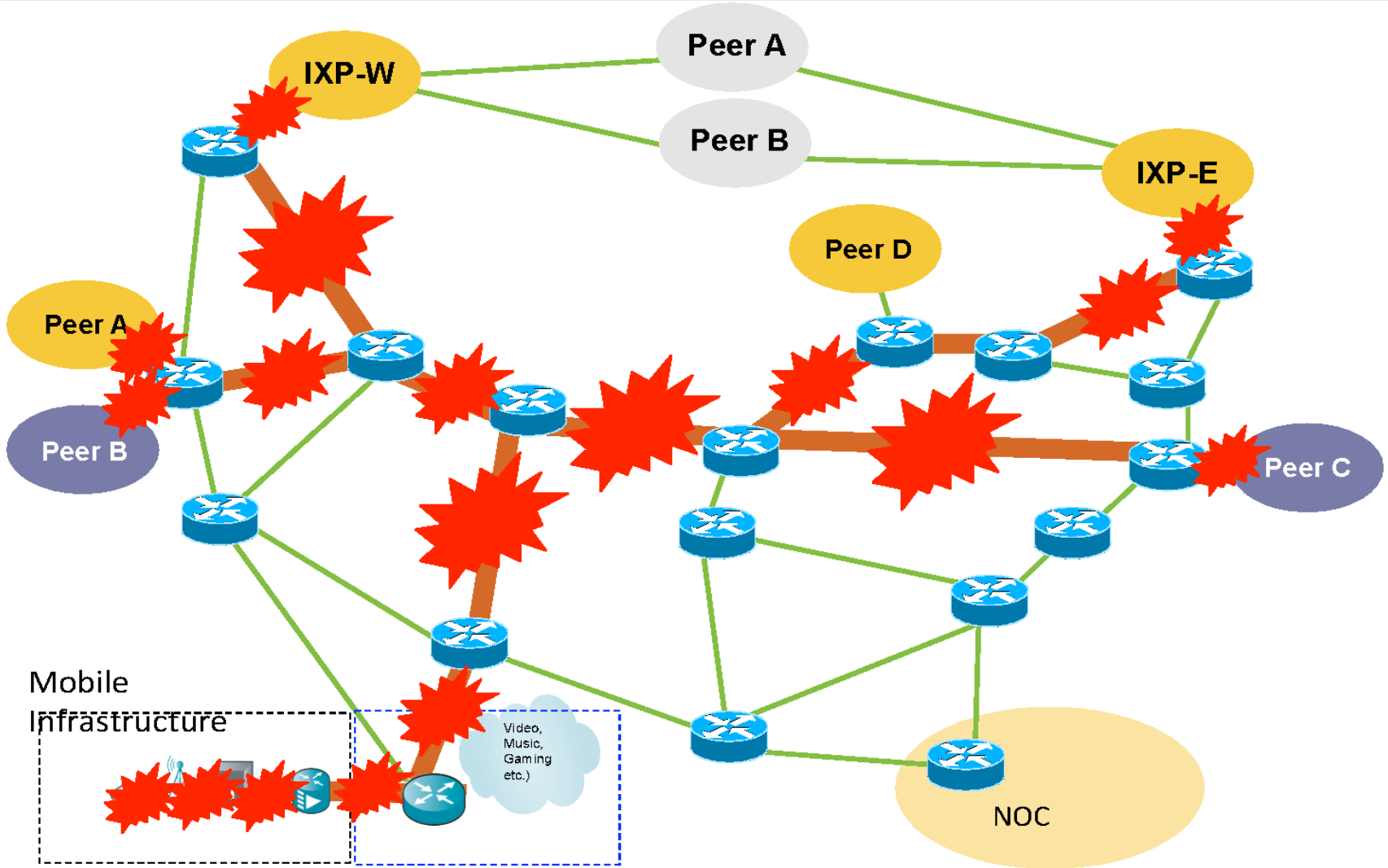
Effects of a 300gb/sec Reflection/Amplification DDoS Attack on Network Capacity



Effects of a 300gb/sec Reflection/Amplification DDoS Attack on Network Capacity



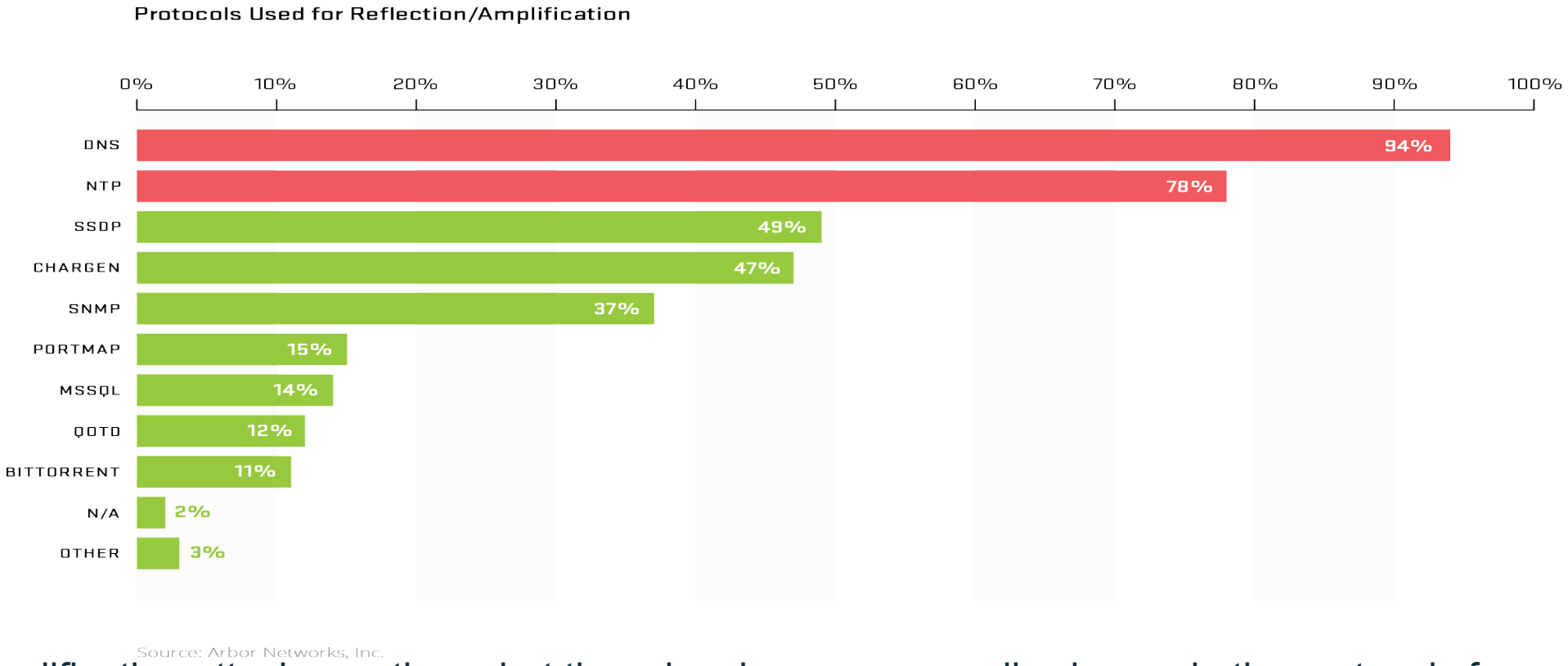
Effects of a 300gb/sec Reflection/Amplification DDoS Attack on Network Capacity



Five Common Reflection/Amplification Vectors

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

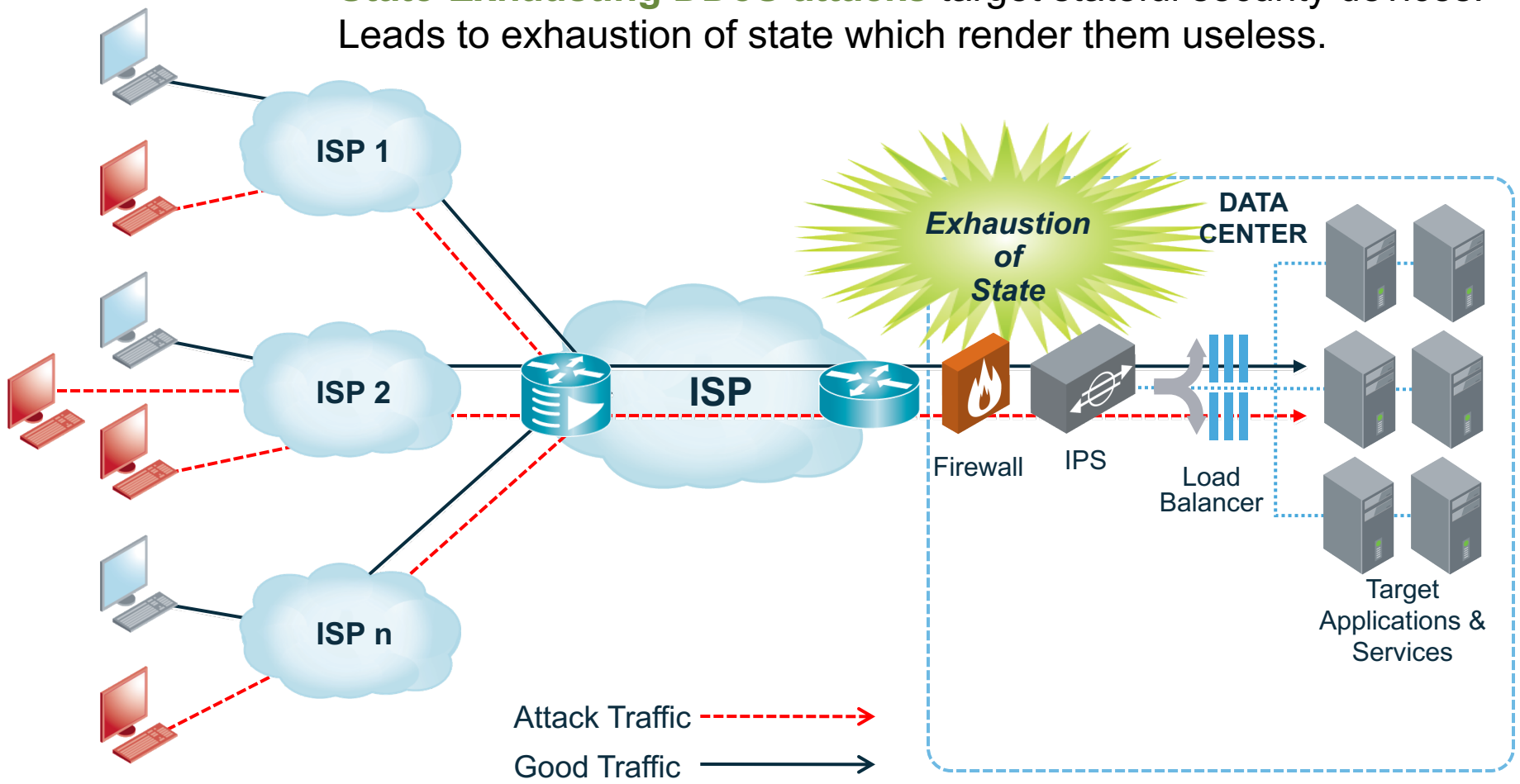
Scale: Driving Factors, Reflection Amplification



- Reflection Amplification attacks continue, but there has been some cyclic change in the protocols favored by attackers.
- Strong growth in the use of DNS (again) through 2016
- Largest monitored attack of 498.3Gbs, a 97% jump from last year
  - DNS and NTP attacks over 400Gbps, Chargen over 200Gbps

DDoS Attacks: State-Exhausting

State-Exhausting DDoS attacks target stateful security devices.
Leads to exhaustion of state which render them useless.



Protocol Attacks

Description

- Attacks that exploit vulnerable parts of protocols such as TCP 3-way handshake. They are often crafted to overwhelm protocol state of devices

Affect on Network

- State table on servers, load balancers, IPS and firewalls fill up and they will no longer pass traffic

Affect on Services

- Legitimate users can’t get to services.

Common Names

- SYN flood, RST flood, FIN flood

Connection Based Attacks

Description

- Attackers create many connections to the service sending no traffic or infrequent traffic. Sometimes the attacker may send incomplete requests to the services.

Affect on Network

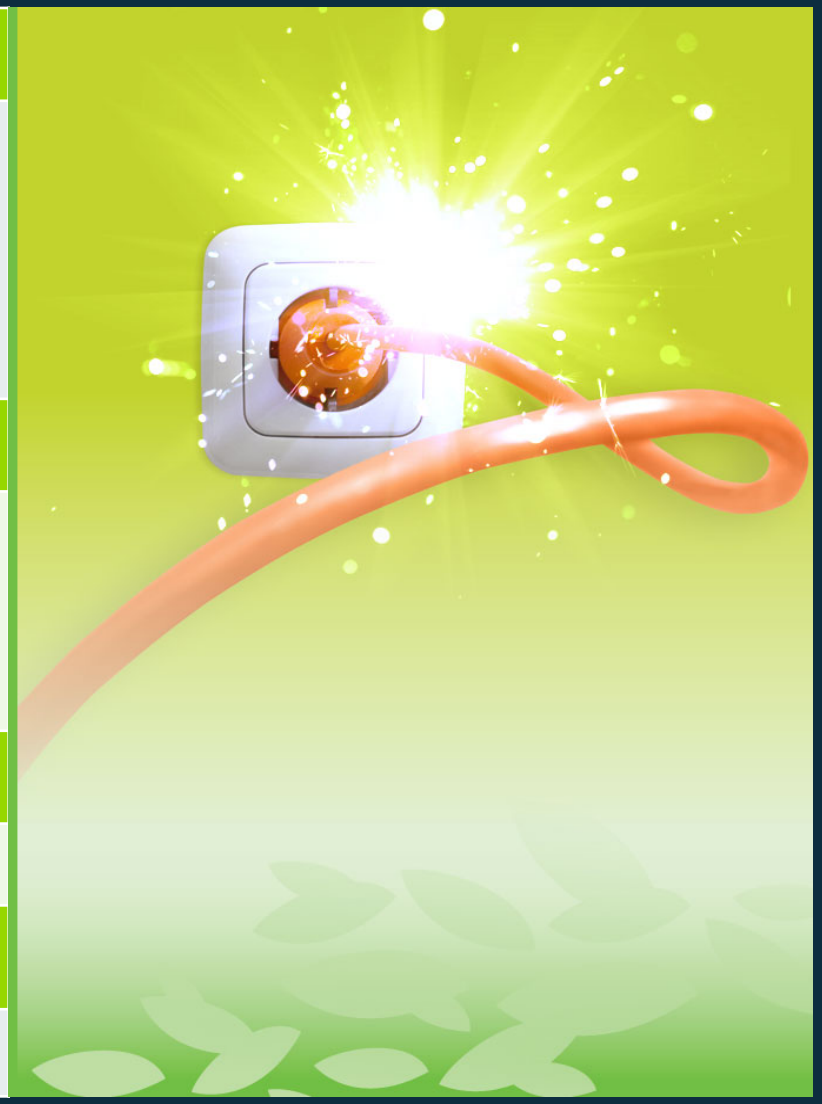
- Available connections to the service are exhausted. State tables of FW, IPS, load balancers could also get overwhelmed.

Affect on Services

- Legitimate users can’t get to services.

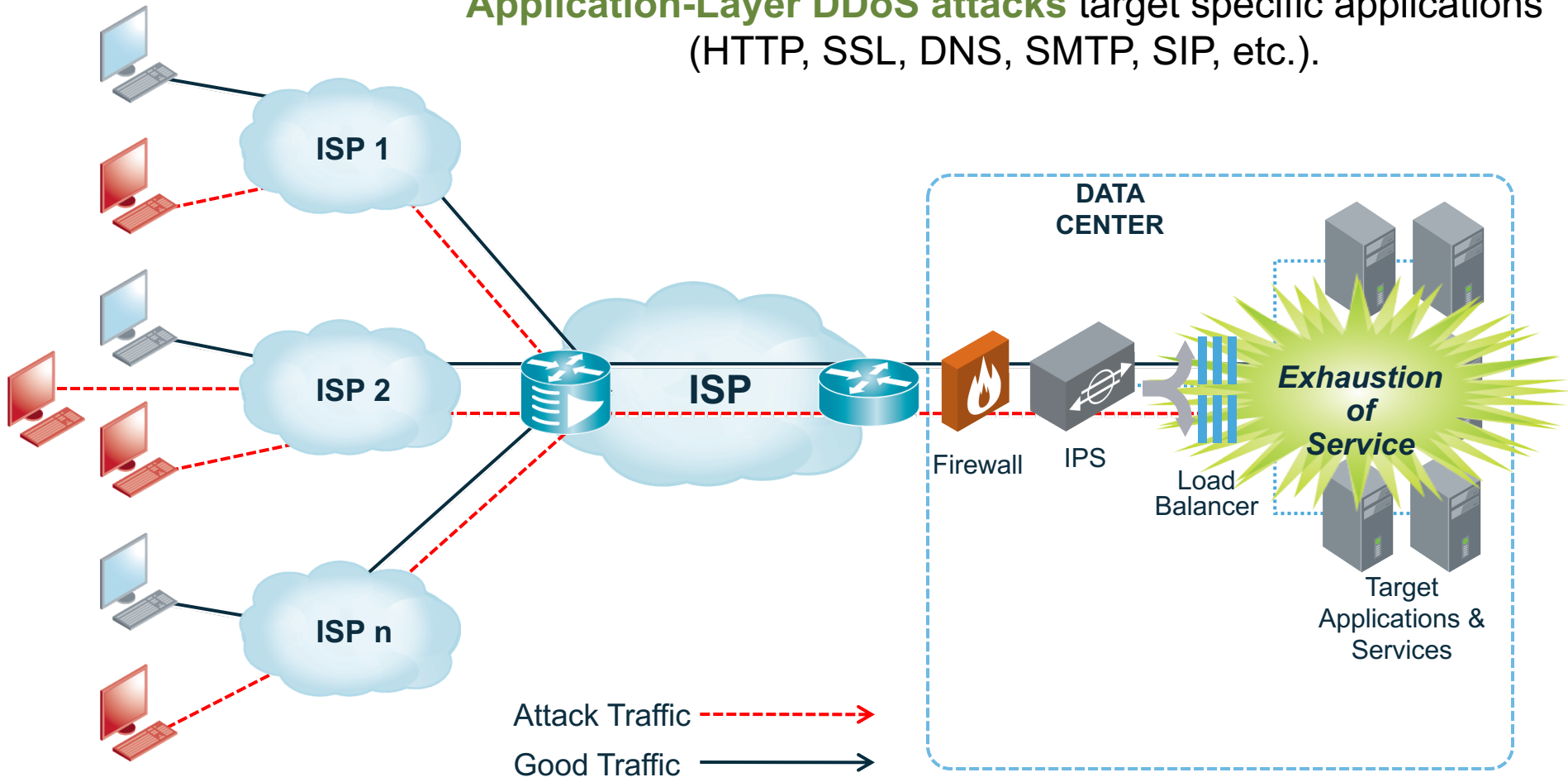
Common Names

- Sockstress



DDoS Attacks: Application Layer

Application-Layer DDoS attacks target specific applications (HTTP, SSL, DNS, SMTP, SIP, etc.).



Application-Layer Attacks

Description

- Attacks that target a vulnerability at the application layer.
- Can range from application floods to slow stealthy attacks that target a particular weakness.

Affect on Network

- Limited network effect as the traffic rates can be very low.
- They sometimes cause congestion between services and storage databases.

Affect on Services

- Services become unresponsive or go down altogether.

Common Names

- URL floods, R U Dead Yet (RUDY), Slowloris, LOIC, HOIC, DNS dictionary attacks

Application Attacks to Web Servers

- Get Floods
  - Brute force use the server's processing capacity – typically done using a Botnet
  - Ex: Siege
- Slow GET
  - Creates TCP sessions that never close and hold server resources (TCP table space, process table, memory)
  - Ex: Slowloris
- Slow POST
  - Similar to Slow GET, focused on pages which have forms to be completed (can't be cached by CDNs)
  - Ex: RUDY

Slowloris – Slow HTTP GET DDoS

- HTTP DDoS attack tool
- Allows a single machine to take down a web server with minimal bandwidth and side effects on unrelated services and ports
- Designed to hold open as many connections as possible to the HTTP server.
- Exploits design flaws in the HTTP protocol

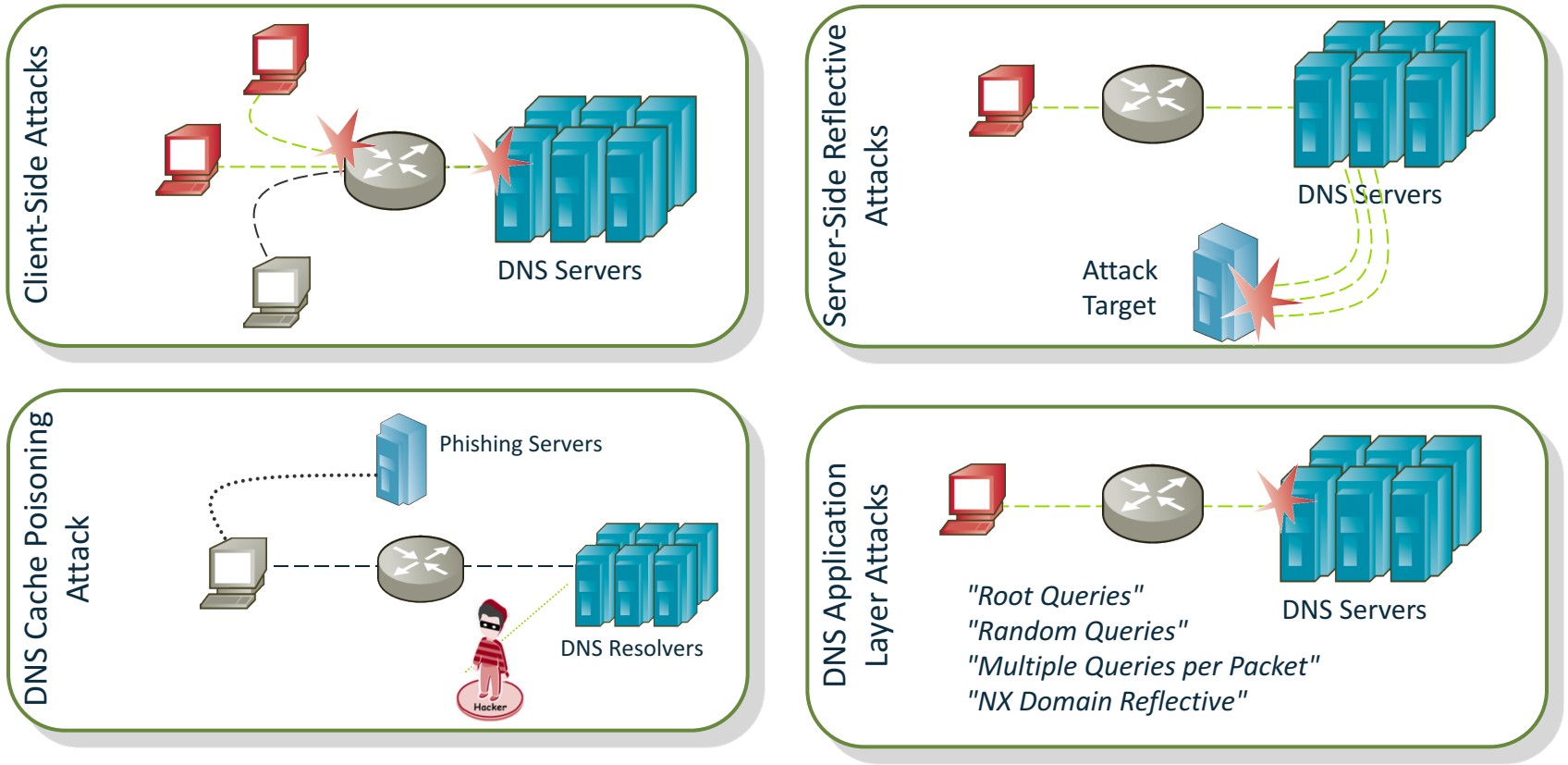
Slowloris – Slow HTTP GET DDoS

- Slowloris abuses handling of HTTP request headers sssloooowly…
- Each Slowloris process opens several connections to the target web server and sends a partial request: one not ending with a “/n” line
- This tells the web server to hold on: the rest of the get request is on its way…
- periodically, each slowloris process will send subsequent HTTP headers, but never completing the request.
- Affected servers will keep these connections open, filling their maximum concurrent connection pool, eventually denying additional connection attempts from clients.
- Slowloris has high impact and relatively low bandwidth usage

R.U.D.Y – Slow HTTP POST DDoS

- Uses HTTP POST requests
- The HTTP Header portion is complete and sent in full to the web server.
- R.U.D.Y.
  - Abuses HTTP web form fields
  - Iteratively injects one custom byte into a web application post field and goes to sleep
  - Application threads become zombies awaiting ends of posts… until death lurks upon the website

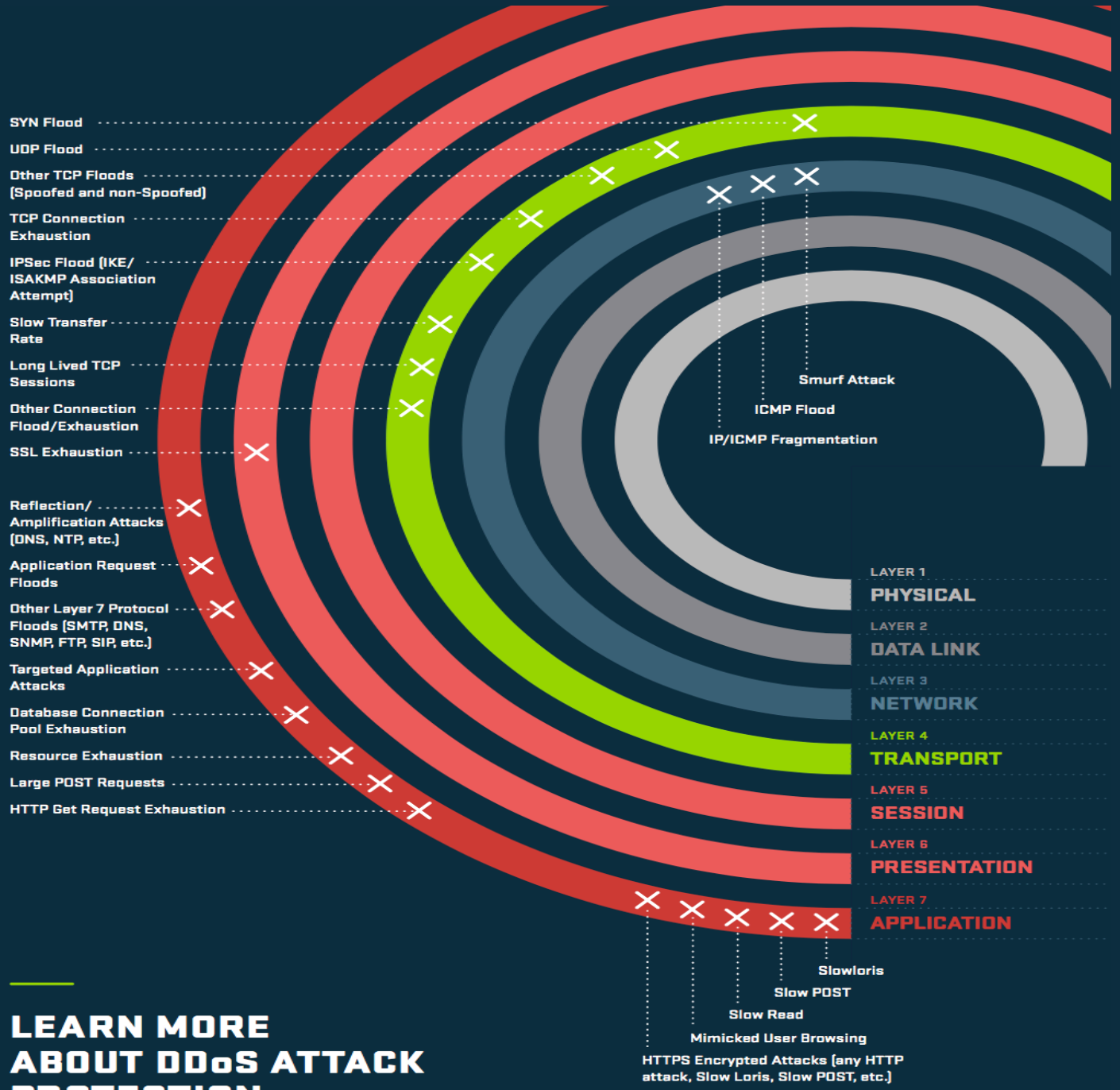
Common DNS Attacks



- Multiple threat vectors against DNS whose impacts include loss of service availability, reduced customer satisfaction, and hurt profitability

DDoS Attack Types

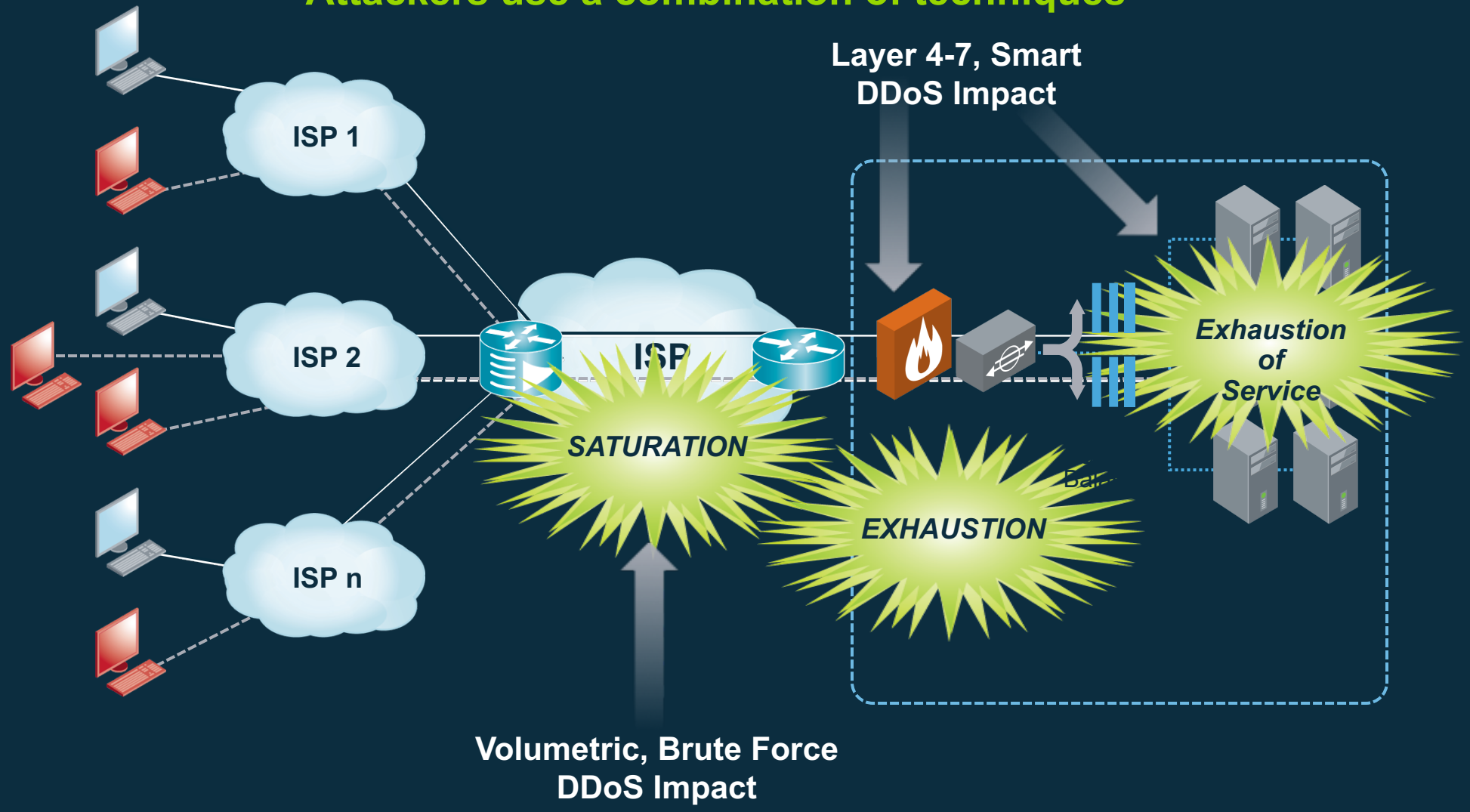
ACROSS NETWORK LAYERS OF THE OSI MODEL



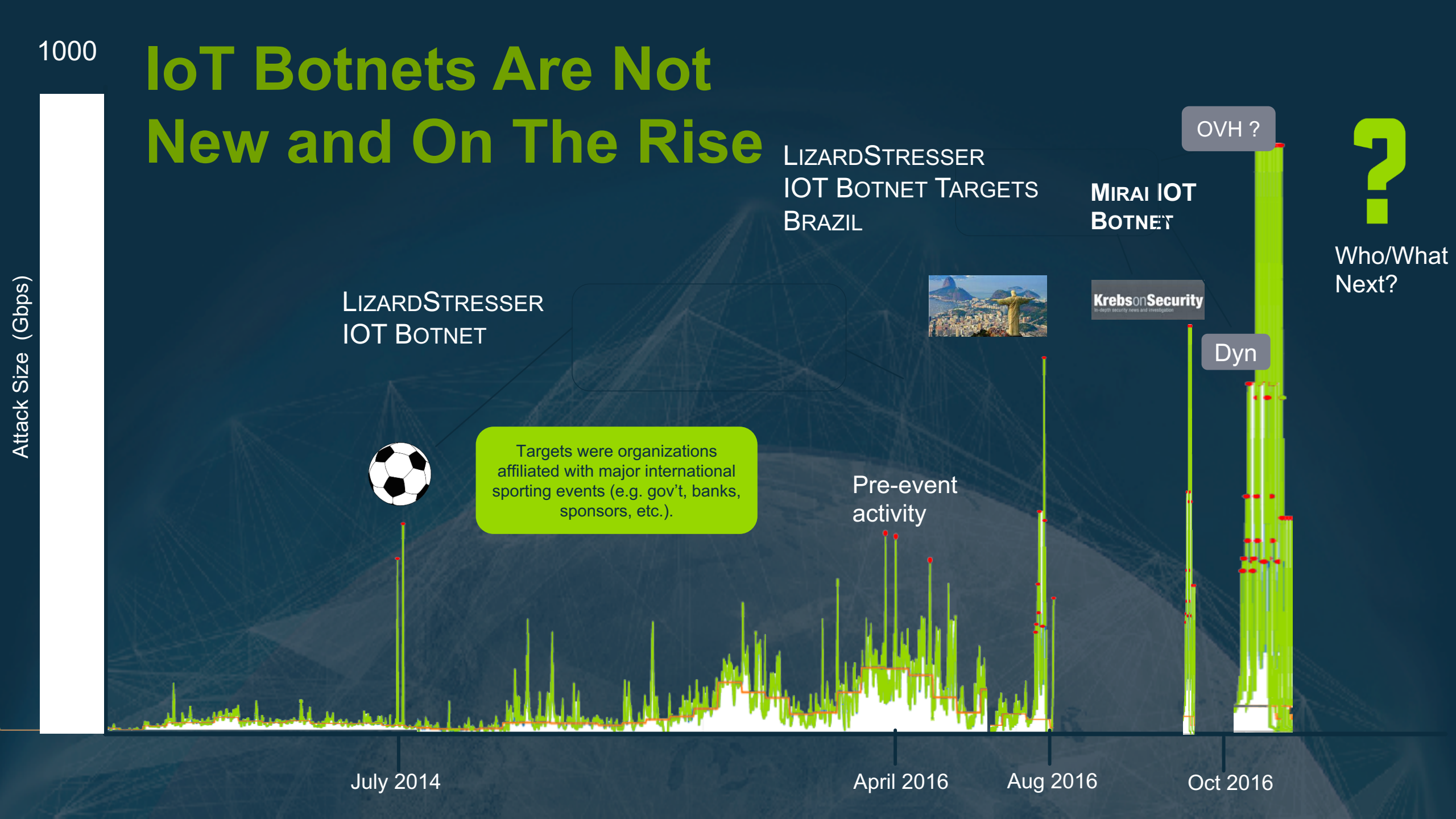
LEARN MORE ABOUT DDoS ATTACK PROTECTION

The Evolving DDoS Threat

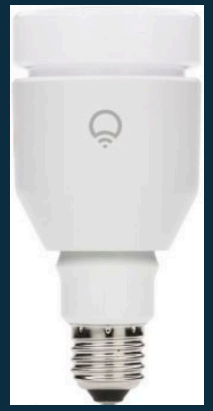
Attackers use a combination of techniques



IoT Botnets Are Not New and On The Rise



INTERNET OF THINGS (IoT)

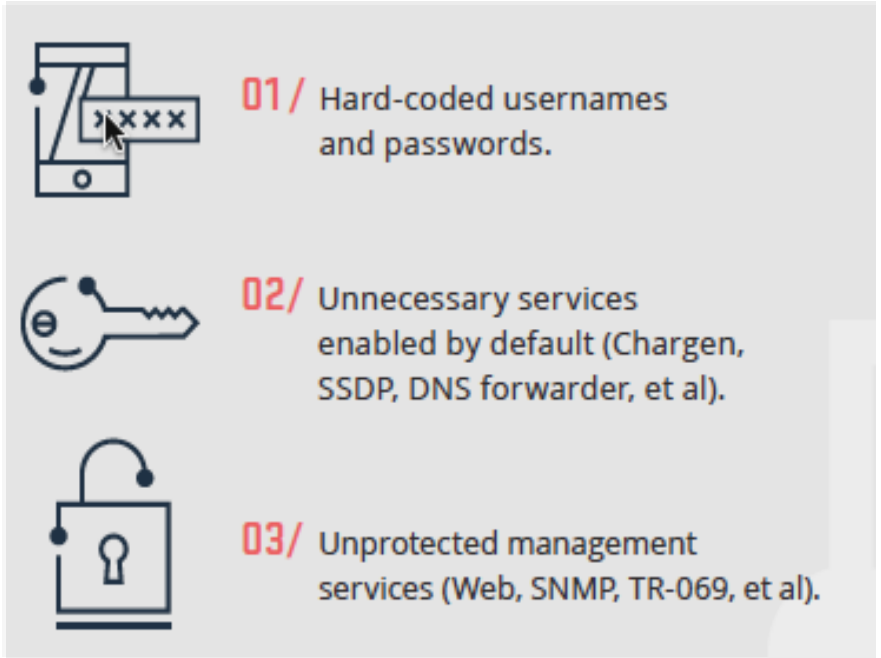


ARBOR NETWORKS

Scale: Driving Factors, IoT

The Problem

- Almost every piece of technology we buy is ‘connected’
- Devices are designed to be easy to deploy and use, often resulting in limited security capabilities
- Software is very rarely upgraded. Some manufacturers don’t provide updates, or the ability to install updates



The Result

- First high-profile attack using IoT devices Christmas 2013, using CPE and webcams
- In 2016 Botnet owners started to recruit IoT devices en mass
- Attacks of 540Gbps against the Olympics, 620Gbps against Krebs, Dyn etc..

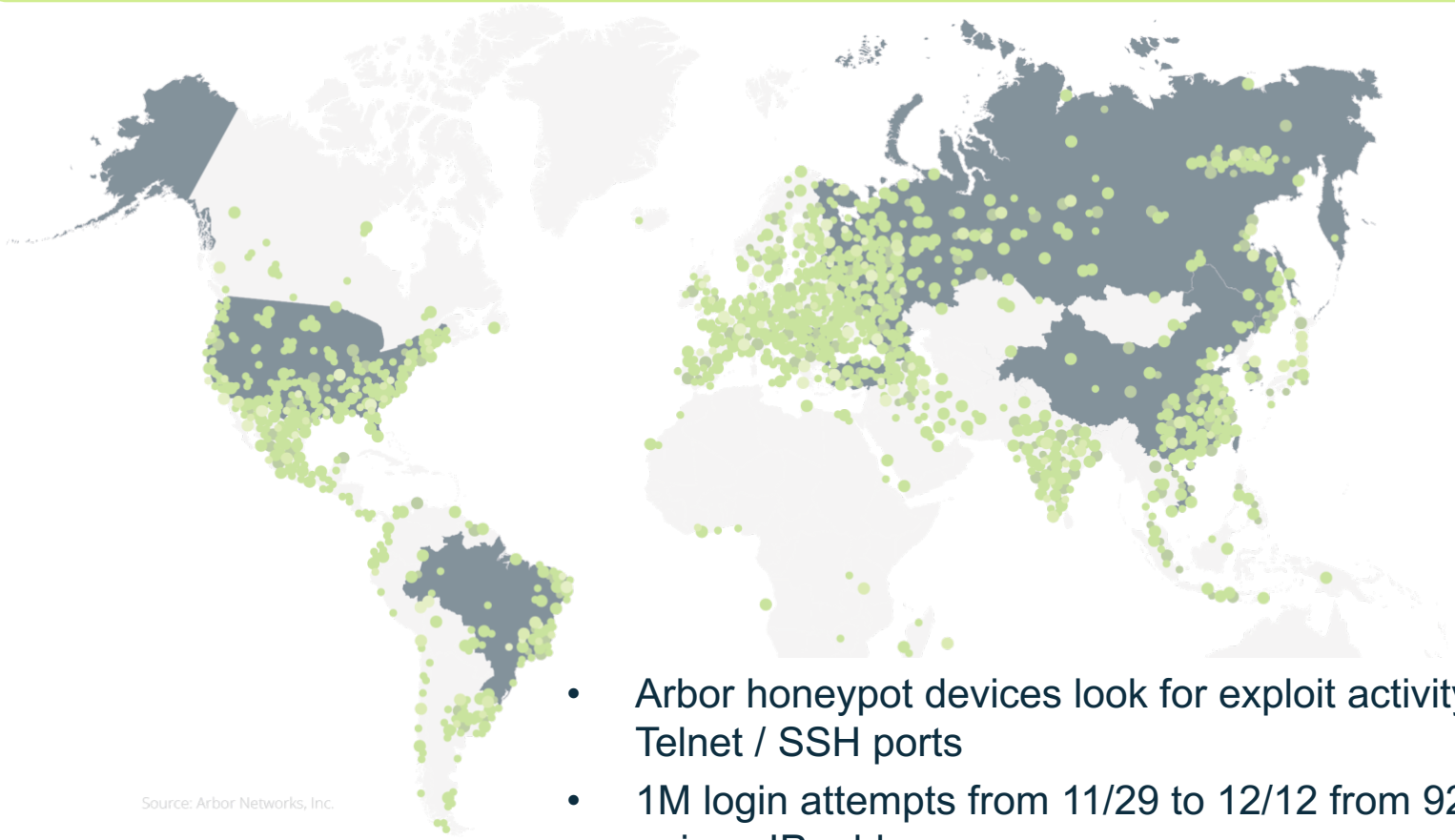
DEFAULT CREDENTIALS FOR IOT DEVICES

https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.pdf

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/

Scale: Driving Factors, Mirai

Mirai is designed to infect and control IoT devices and contains the code necessary to manage and build large-scale botnets

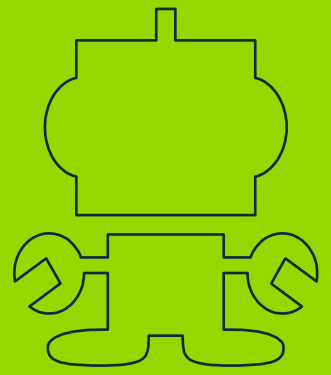


- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than 1 attempt per minute in some regions

Mirai is NOT Just a DNS Attack

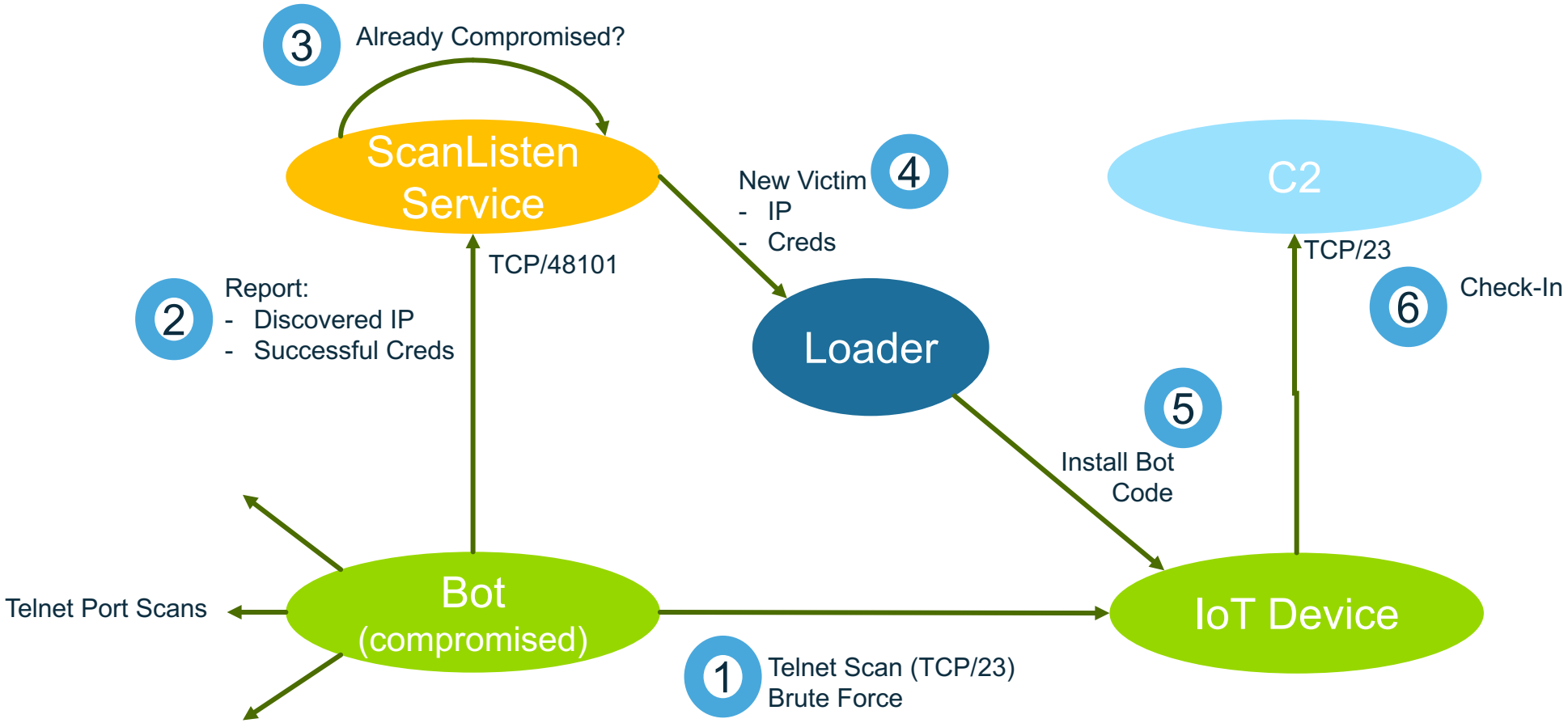
Attack Vectors:

- SYN-flooding
- ACK-flooding
- UDP flooding
- Valve Source Engine (VSE) query-flooding
- GRE-flooding
- Pseudo-random DNS label-prepending attacks (also known as DNS ‘Water Torture’ attacks)
- HTTP GET, POST and HEAD attacks.

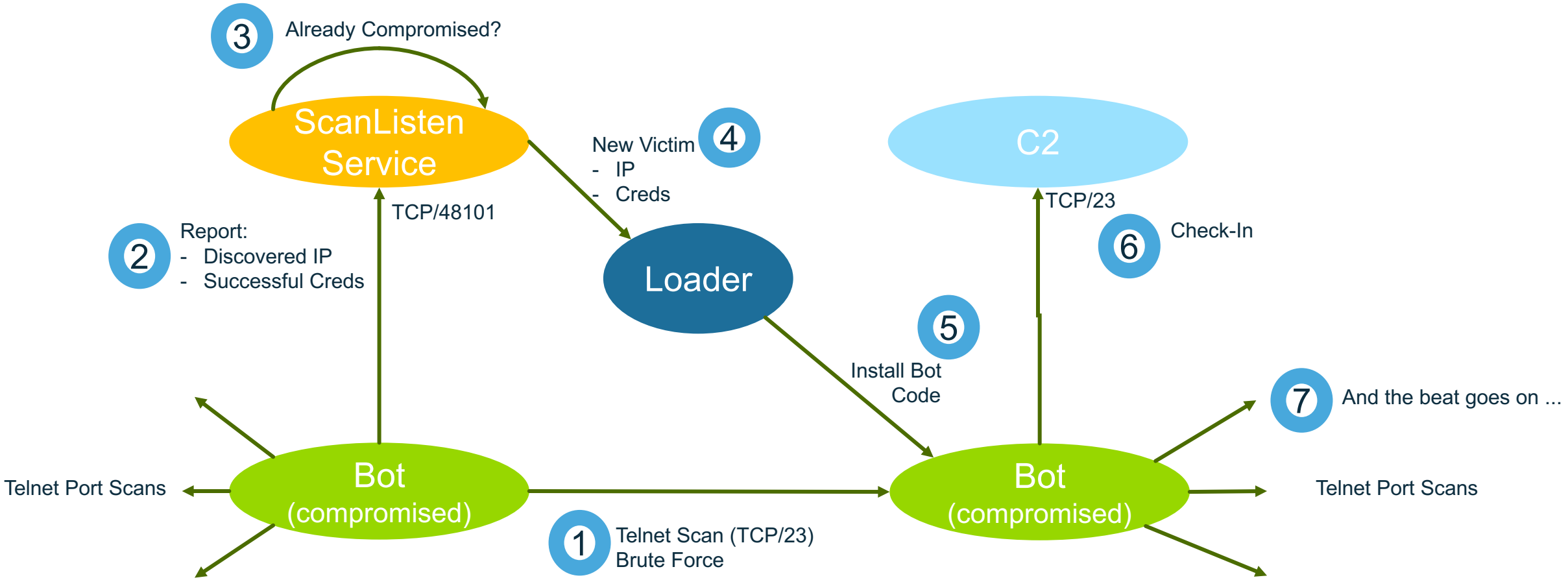


The Mirai Botnet is capable of launching complex multi-vector attacks.

Mirai – Propagation, Command and Control



Mirai – Propagation, Command and Control



THE MIRAI BOTNET

✓**Predominantly Webcam IoT devices**

- Approximately 500,000 devices worldwide
- High concentrations in China, Hong Kong, Macau, Vietnam, Taiwan, South Kora, Thailand, Indonesia, Brazil, and Spain

✓**Segmented Control**

✓**Multi-Vector Attack Support:**

```
34  #define ATK_VEC_UDP          0  /* Straight up UDP flood */
35  #define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
36  #define ATK_VEC_DNS          2  /* DNS water torture */
37  #define ATK_VEC_SYN          3  /* SYN flood with options */
38  #define ATK_VEC_ACK          4  /* ACK flood */
39  #define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
40  #define ATK_VEC_GREIP        6  /* GRE IP flood */
41  #define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
42  //#define ATK_VEC_PROXY        8  /* Proxy knockback connection */
43  #define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
44  #define ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

✓**Krebs, OVH, Dyn, and Liberia**

- Does not imply it was the same adversaries!!!

ARBOR NETWORKS

Mirai source code development

```
#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP       10 /* HTTP layer 7 flood */

#define ATK_OPT_PAYLOAD_SIZE    0   // What should the size of the packet data be?
#define ATK_OPT_PAYLOAD_RAND    1   // Should we randomize the packet data contents?
#define ATK_OPT_IP_TOS          2   // tos field in IP header
#define ATK_OPT_IP_IDENT        3   // ident field in IP header
#define ATK_OPT_IP_TTL          4   // ttl field in IP header
#define ATK_OPT_IP_DF           5   // Dont-Fragment bit set
#define ATK_OPT_SPORT           6   // Should we force a source port? (0 = random)
#define ATK_OPT_DPORT           7   // Should we force a dest port? (0 = random)
#define ATK_OPT_DOMAIN          8   // Domain name for DNS attack
#define ATK_OPT_DNS_HDR_ID      9   // Domain name header ID
//#define ATK_OPT_TCPCC          10  // TCP congestion control
#define ATK_OPT_URG             11  // TCP URG header flag
#define ATK_OPT_ACK             12  // TCP ACK header flag
#define ATK_OPT_PSH             13  // TCP PSH header flag
#define ATK_OPT_RST             14  // TCP RST header flag
#define ATK_OPT_SYN             15  // TCP SYN header flag
#define ATK_OPT_FIN             16  // TCP FIN header flag
#define ATK_OPT_SEQRND          17  // Should we force the sequence number? (TCP only)
#define ATK_OPT_ACKRND          18  // Should we force the ack number? (TCP only)
#define ATK_OPT_GRE_CONSTIP     19  // Should the encapsulated destination address be the same as the target?
#define ATK_OPT_METHOD              20      // Method for HTTP flood
#define ATK_OPT_POST_DATA           21      // Any data to be posted with HTTP flood
#define ATK_OPT_PATH            22  // The path for the HTTP flood
#define ATK_OPT_HTTPS           23  // Is this URL SSL/HTTPS?
#define ATK_OPT_CONNS           24  // Number of sockets to use
#define ATK_OPT_SOURCE          25  // Source IP
```

```
#define HTTP_CONN_INIT          0 // Inital state
#define HTTP_CONN_RESTART       1 // Scheduled to restart connection next spin
#define HTTP_CONN_CONNECTING    2 // Waiting for it to connect
#define HTTP_CONN_HTTPS_STUFF   3 // Handle any needed HTTPS stuff such as negotiation
#define HTTP_CONN_SEND          4 // Sending HTTP request
#define HTTP_CONN_SEND_HEADERS  5 // Send HTTP headers
#define HTTP_CONN_RECV_HEADER   6 // Get HTTP headers and check for things like location or cookies etc
#define HTTP_CONN_RECV_BODY     7 // Get HTTP body and check for cf iaua mode
#define HTTP_CONN_SEND_JUNK             8 // Send as much data as possible
#define HTTP_CONN_SNDBUF_WAIT   9 // Wait for socket to be available to be written to
#define HTTP_CONN_QUEUE_RESTART 10 // restart the connection/send new request BUT FIRST read any other available data.
#define HTTP_CONN_CLOSED        11 // Close connection and move on

#define HTTP_RDBUF_SIZE         1024
#define HTTP_HACK_DRAIN         64
#define HTTP_PATH_MAX           256
#define HTTP_DOMAIN_MAX         128
#define HTTP_COOKIE_MAX         5   // no more then 5 tracked cookies
#define HTTP_COOKIE_LEN_MAX     128 // max cookie len
#define HTTP_POST_MAX           512 // max post data len

#define HTTP_PROT_DOSARREST     1 // Server: DOSarrest
#define HTTP_PROT_CLOUDFLARE    2 // Server: cloudflare-nginx
```

Time to Re-Assess Risk of DDoS Attack?

1. Do I know the latest DDoS attack trends?
2. Do I know the best practices in DDoS attack mitigation?
3. Do I know the real impact of a DDoS attack to my business?

LATEST DDOS ATTACK TRENDS

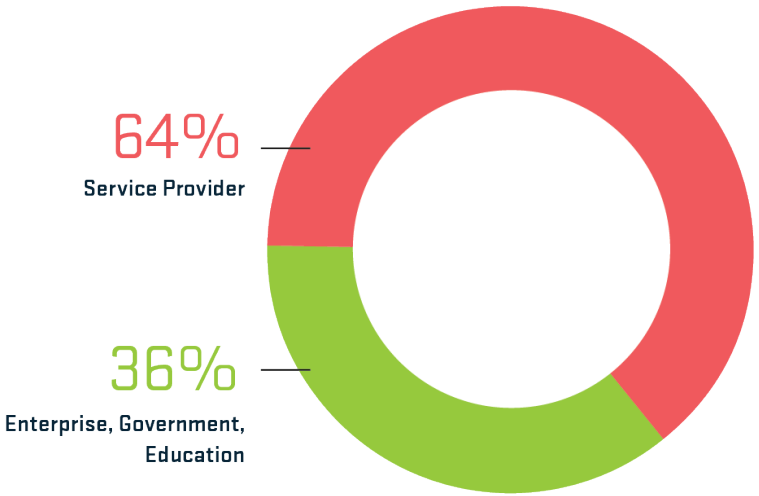
ARBOR NETWORKS

Overview

Arbor Networks' 12th annual Worldwide Infrastructure Security Report (WISR)

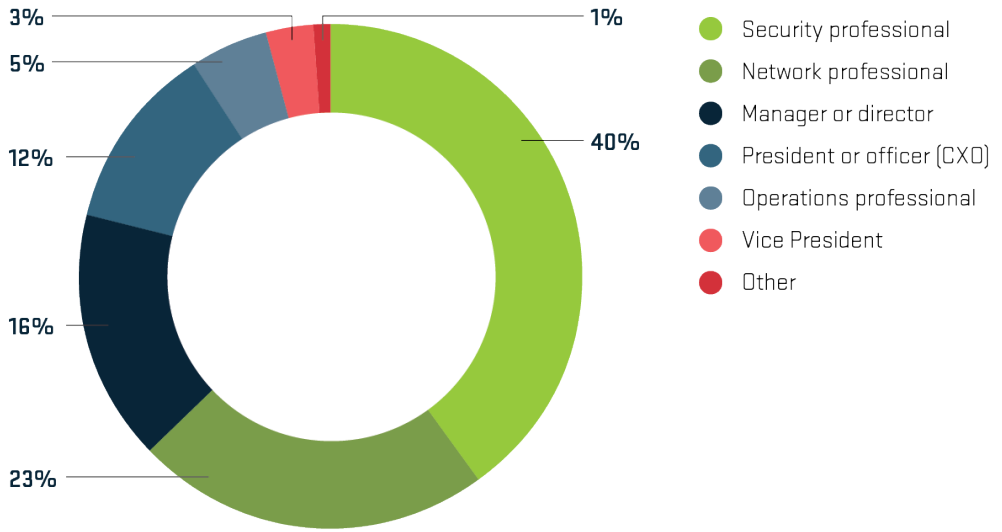
The WISR documents the collective experiences, observations and concerns of the operational security community in 2016 plus forecasts for the coming year

Respondent Classification



Source: Arbor Networks, Inc.

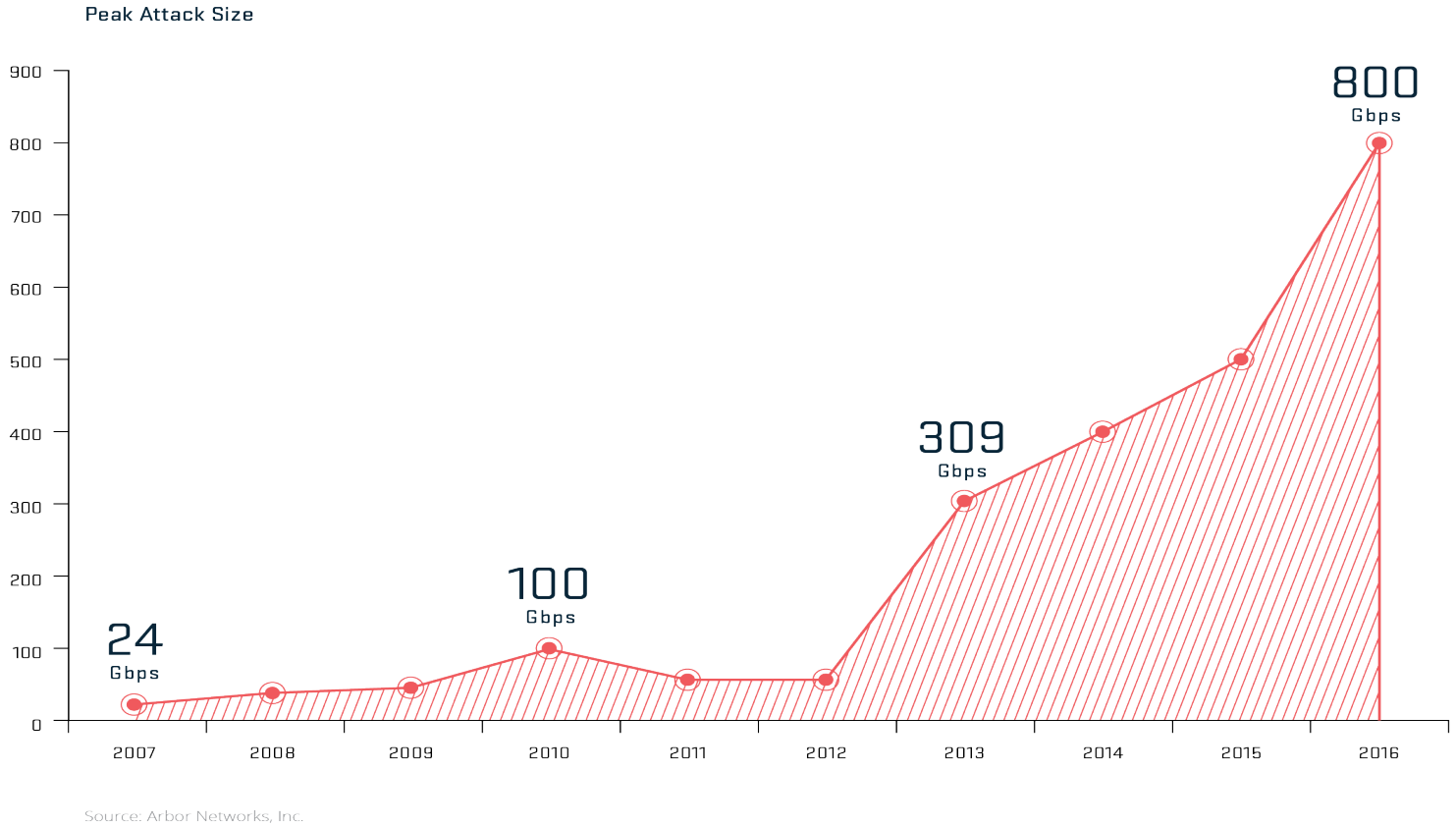
Respondent's Role in the Organization



Source: Arbor Networks, Inc.

Key Points

Scale : Volumetric Attacks Increase

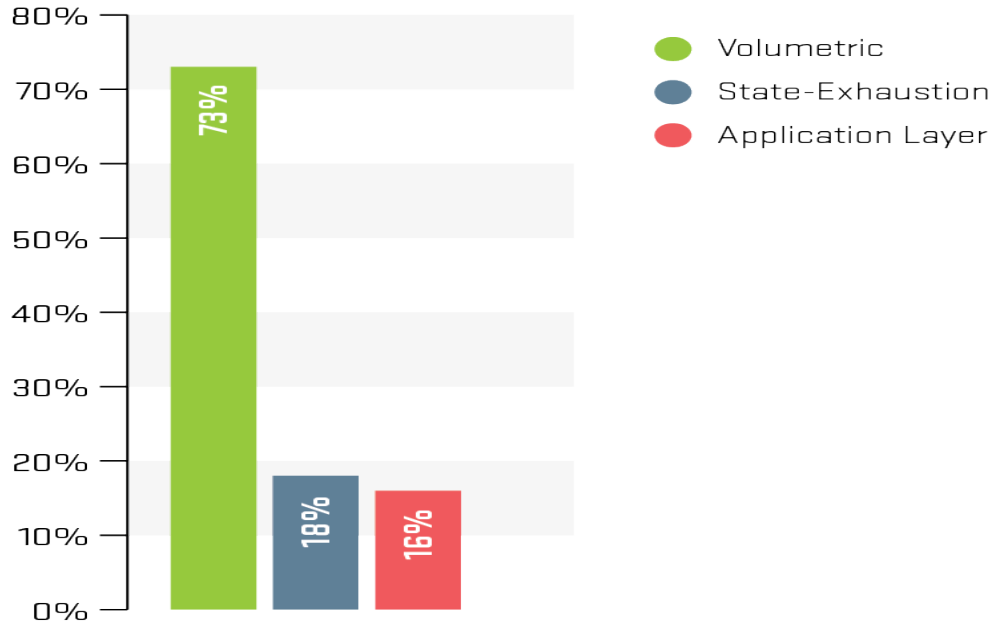


Source: Arbor Networks, Inc.

- Largest attack reported was 800 Gbps with other respondents reporting attacks of 600 Gbps, 550 Gbps, and 500 Gbps
- One third of respondents report peak attacks over 100Gbps
- 41% of EGE respondents and 61% of data-center operators reported attacks exceeding their total Internet capacity

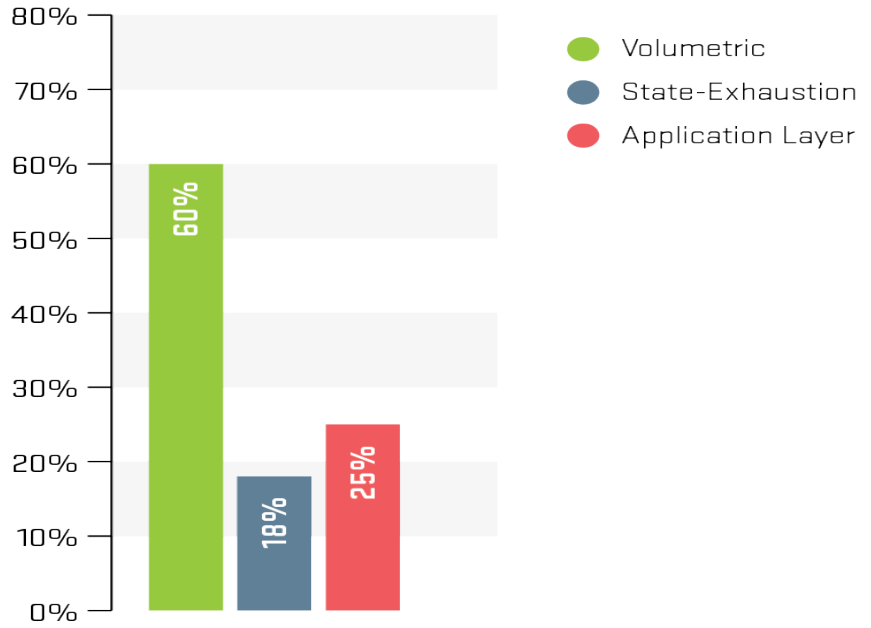
Complexity : Attack Types

SP **DDoS Attack Types**



Source: Arbor Networks, Inc.

EGE **Attack Category Breakout**

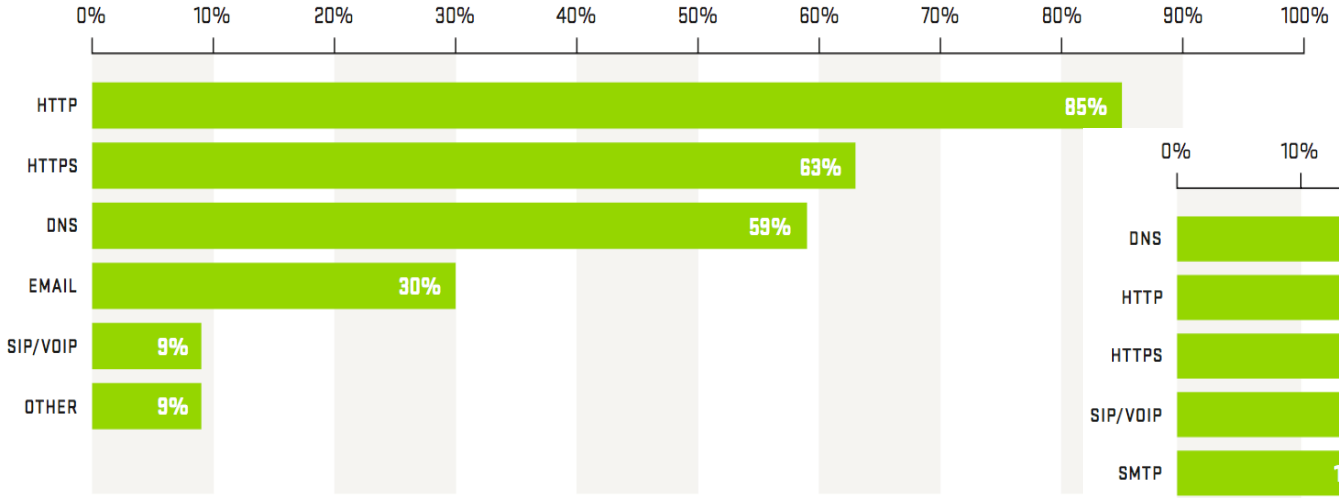


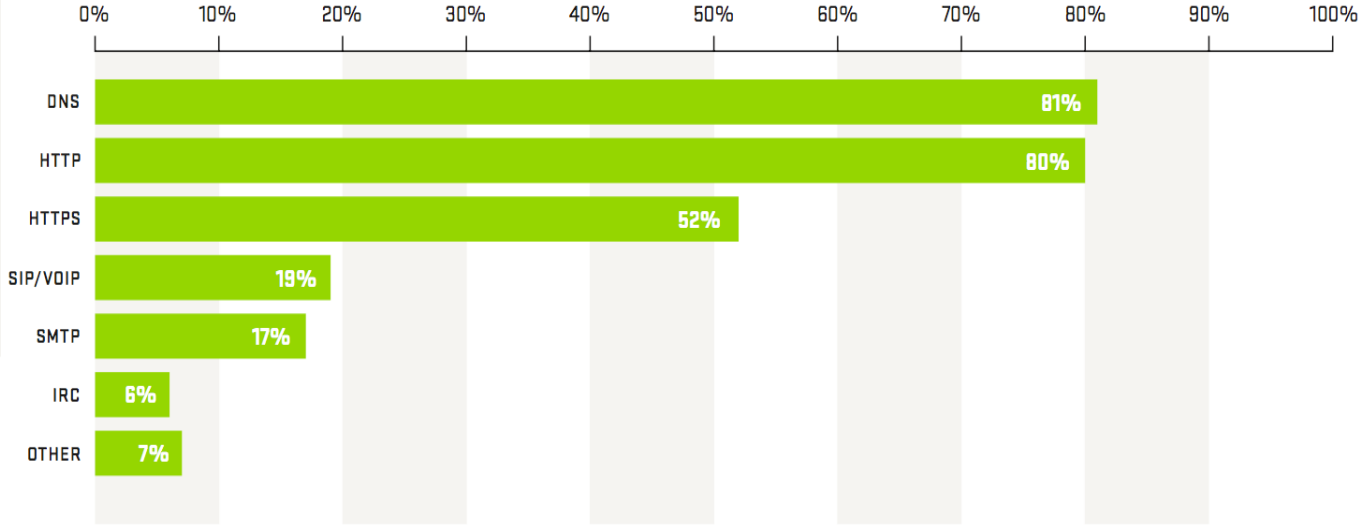
Source: Arbor Networks, Inc.

- Volumetric attacks still represent the majority of activity for both SP and EGE respondents
- 95% of SP report applications layer attacks, 93% last year, 90% in 2014
- 67% of SP report multi-vector attacks, 56% last year, 32% in 2014

Complexity : Targeted Services

EGE Service Targets



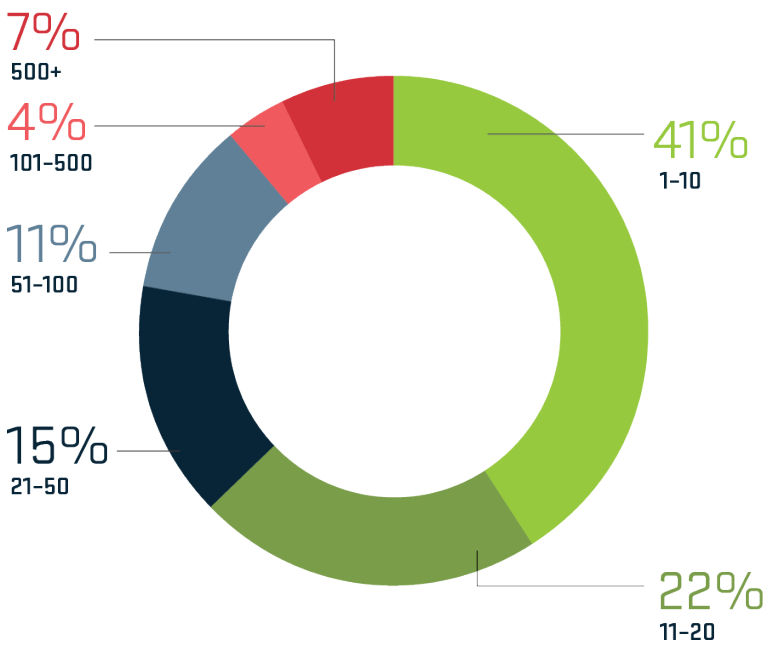


SP Service Targets

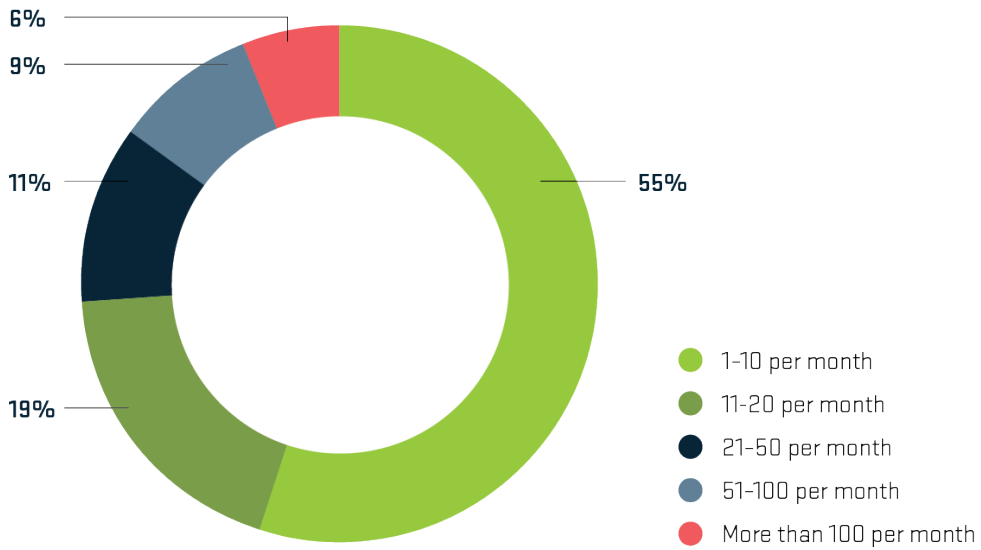
- DNS and HTTP the most common services targeted by application later attacks
- Majority of SP and EGE respondents also see attacks targeting HTTPS
- 57% of EGE respondents see attacks targeting the application behind HTTPS
  - Much higher than the 22% seen by SPs
  - Cipher suites that prevent traffic inspection are a key problem

Frequency : Up Across the Board

Data-Center Attack Frequency



EGE Attack Frequency

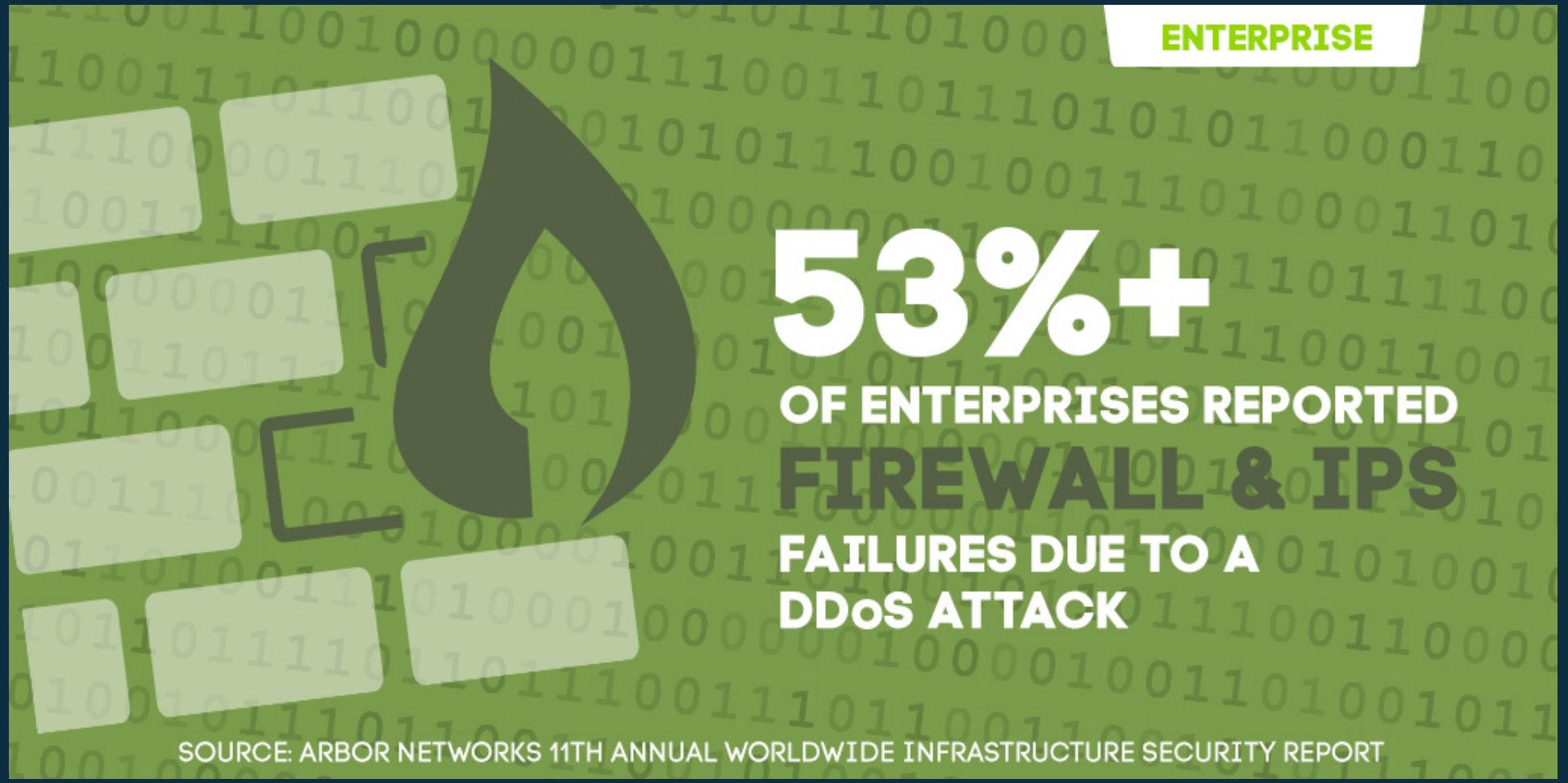


Source: Arbor Networks, Inc.

- 53% of SPs see more than 51 attacks per month, up from 44%
- 21% of data-centers see more than 50 attacks per month, up from 8%
- 45% of EGE see more than 10 attacks per month, up from 28%
- ATLAS is tracking 135,000 Volumetric attacks per week.

DDOS ATTACK MITIGATION

FIREWALLS AND INTRUSION PROTECTION/DETECTION SYSTEMS (IDS/IPS)



Reacting to a DDoS Attack

- ACL
- Black Hole Filtering (S/RTBH)
- On-premise IDM solutions (DDoS solutions).
- Layered-DDoS Attack Surgical mitigation solution.

Reacting to an Attack with ACLs

- Traditional method for stopping attacks
- Scaling issues encountered:
  - Operational difficulties
  - Changes on the fly
  - Multiple ACLs per interface
  - Performance concerns

Black Hole Filtering (S/RTBH)

- Black hole filtering or black hole routing forwards a packet to a router's
  - Also known as "route to Null0"
- Works only on destination addresses, since it is really part of the forwarding logic
- Forwarding ASICs are designed to work with routes to Null0—dropping the packet with minimal to no performance impact
- Used for years as a means to 'blackhole' unwanted packets

Remotely Triggered Black Hole Filtering

- Use BGP to trigger a network-wide response to an attack
- A simple static route and BGP will enable a network-wide destination address black hole as fast as iBGP can update the network (msecs)
- This provides a tool that can be used to respond to security-related events and forms a foundation for other remotely triggered uses
- Often referred to as RTBH

Source-Based Remotely-Triggered Black Hole Filtering (S/RTBH)

- Uses the same architecture as destination-based filtering and Unicast RPF
- Edge routers must have static in place
- They also require Unicast RPF
- BGP trigger sets next-hop—in this case the “victim” is the source we want to drop

Source-Based Remotely Triggered Black Hole Filtering

- What do we have?
  - Black Hole Filtering—if the destination address equals Null0, we drop the packet
  - Remotely Triggered—trigger a prefix to equal Null0 on routers across the network at iBGP speeds
  - uRPF Loose Check—if the source address equals Null0, we drop the packet
- Put them together and we have a tool to trigger a drop for any packet coming into the network whose source or destination equals Null0

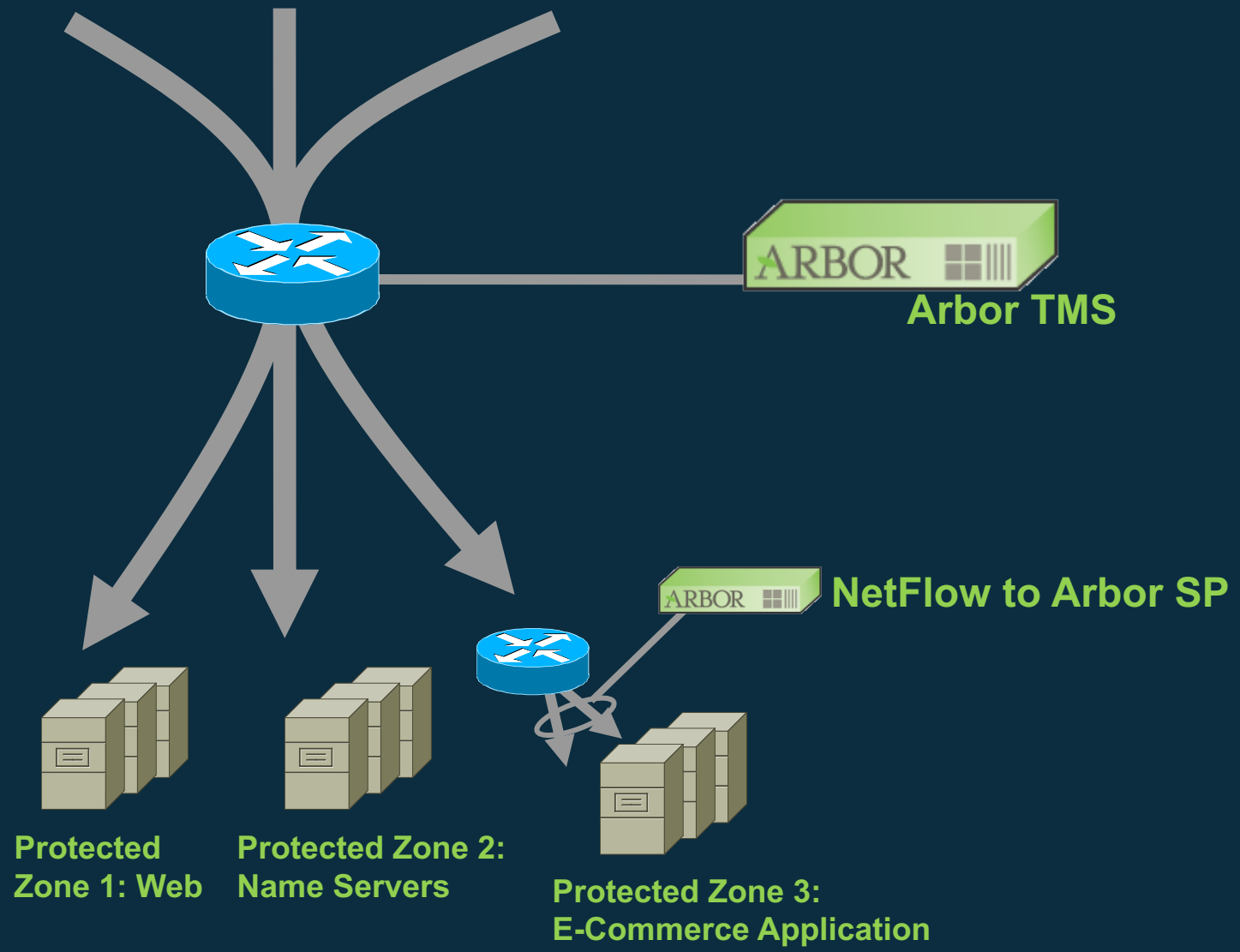
Source-Dropping Caution

- Caution: you will drop all packets with that source and/or destination
- Remember spoofing!
  - Don’t let the attacker spoof the true target and trick you into black holing it for them
  - Whitelist important sites which should never be blocked (i.e., root & TLD nameservers, etc.) via prefix-lists

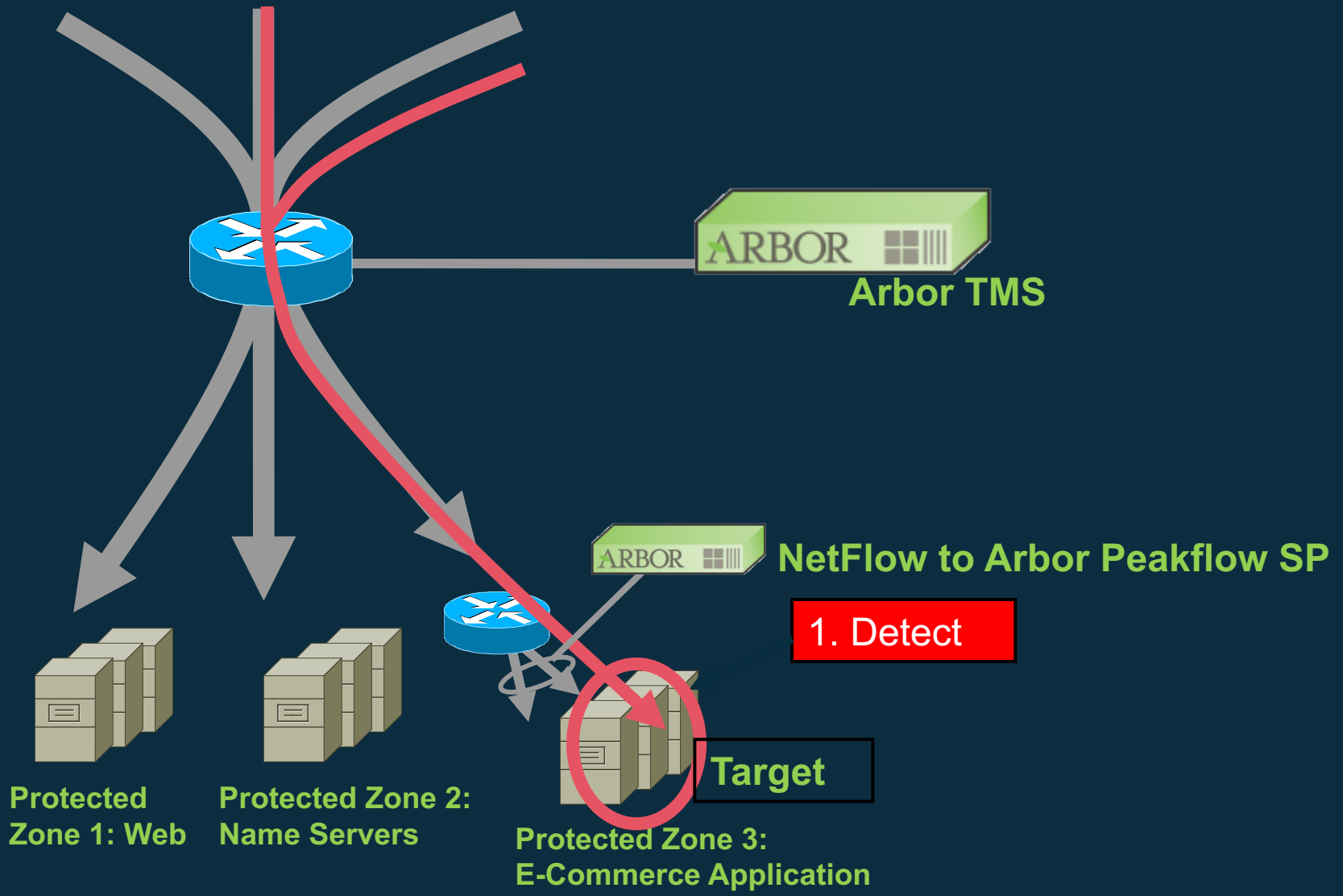
IDM (Intrusion detection) solutions

- DDoS attacks consist of undesirable traffic mixed in with some amount of desirable traffic
  - Undesirable traffic may come in large quantities or it could come shaped in a way designed to disrupt normal processing
- The IDM (E.x Arbor TMS) allows desirable traffic through while lowering the impact of undesirable traffic
- The TMS uses various countermeasures – defense mechanisms – to target and remove the most egregious attack traffic to allow the network to continue operating
  - Different countermeasures are designed to stop different types of attack traffic
  - The countermeasures as a whole provide defense in depth mitigation

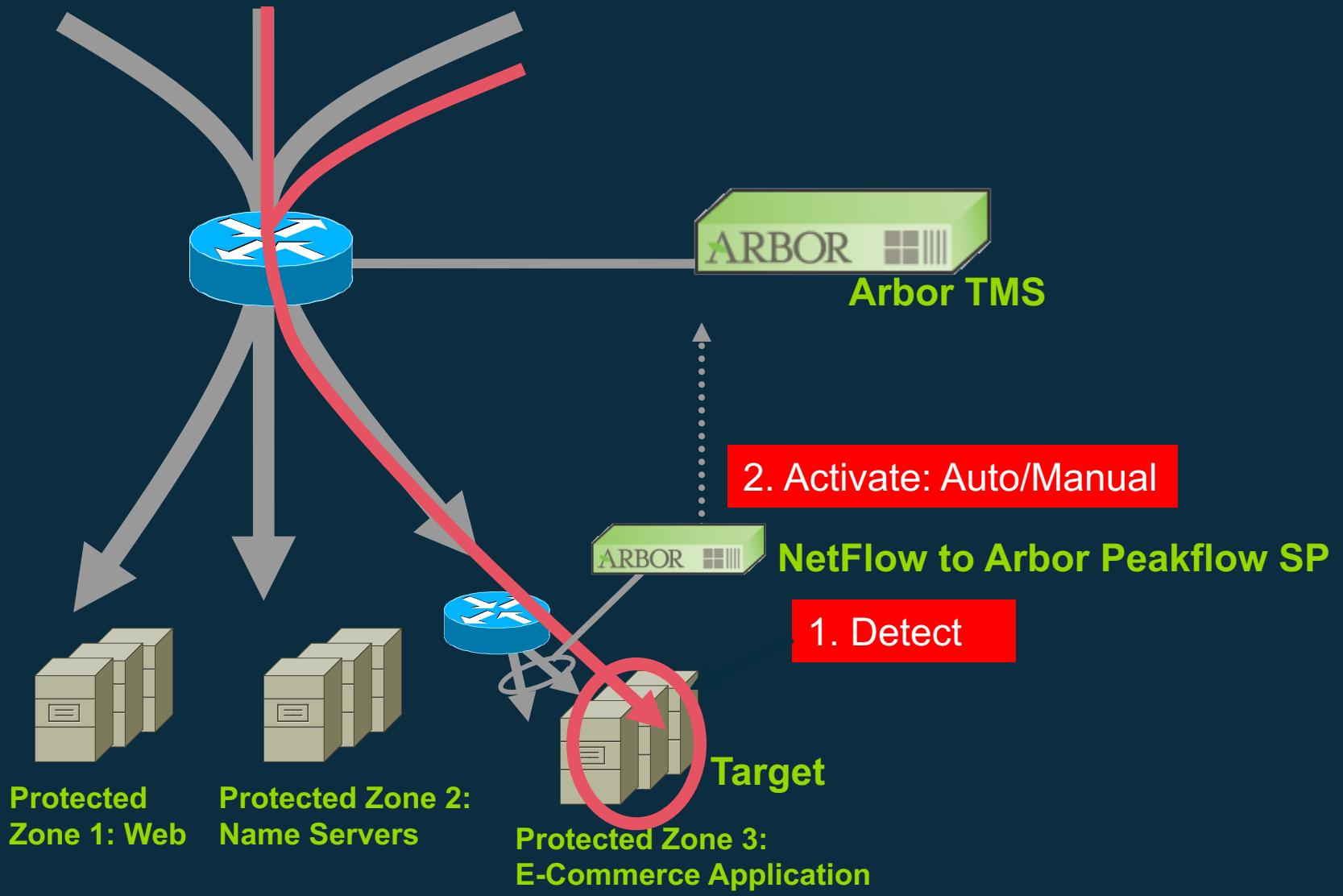
Arbor DDoS Solution: Diversion/Offramping



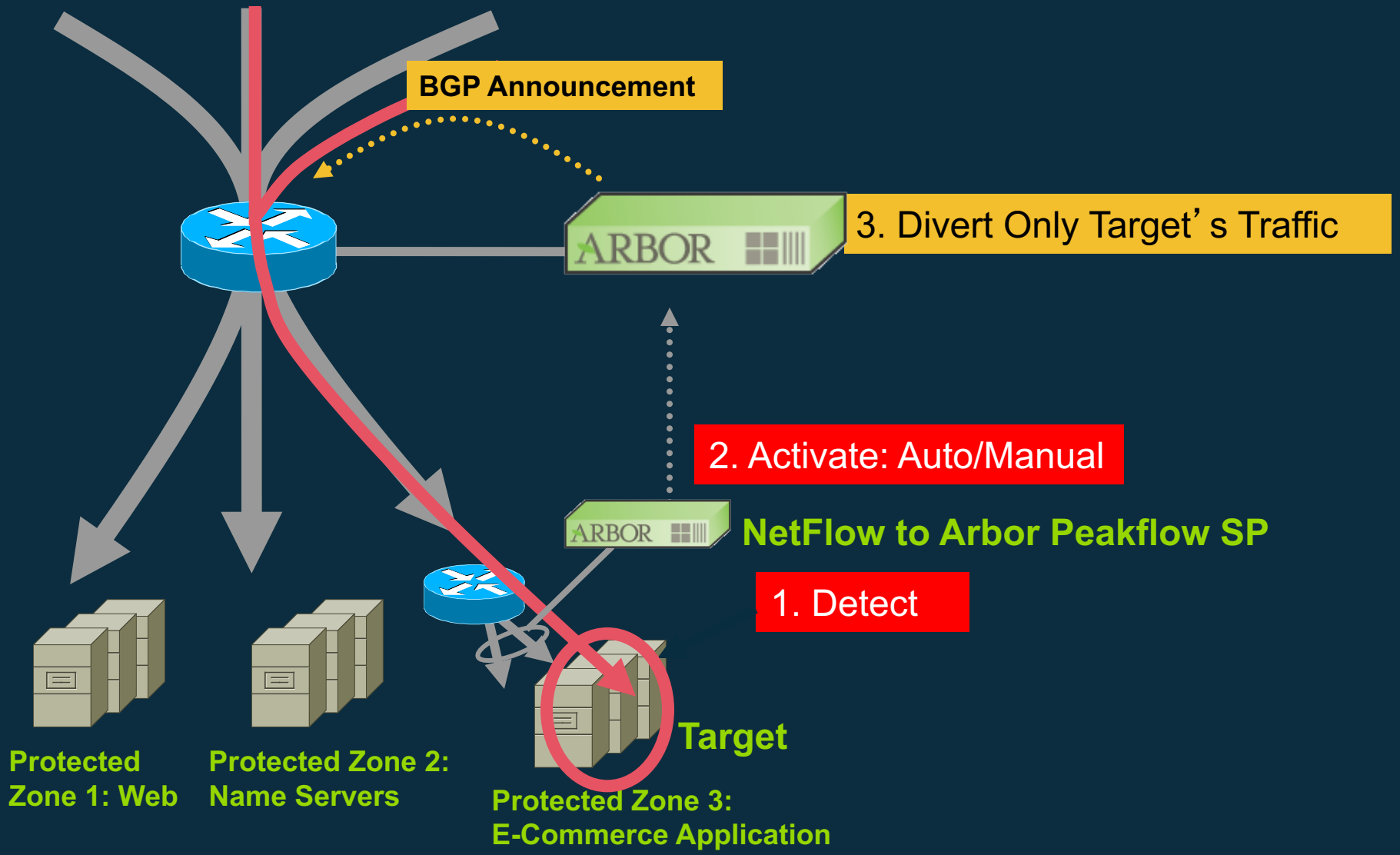
Arbor DDoS Solution: Diversion/Offramping



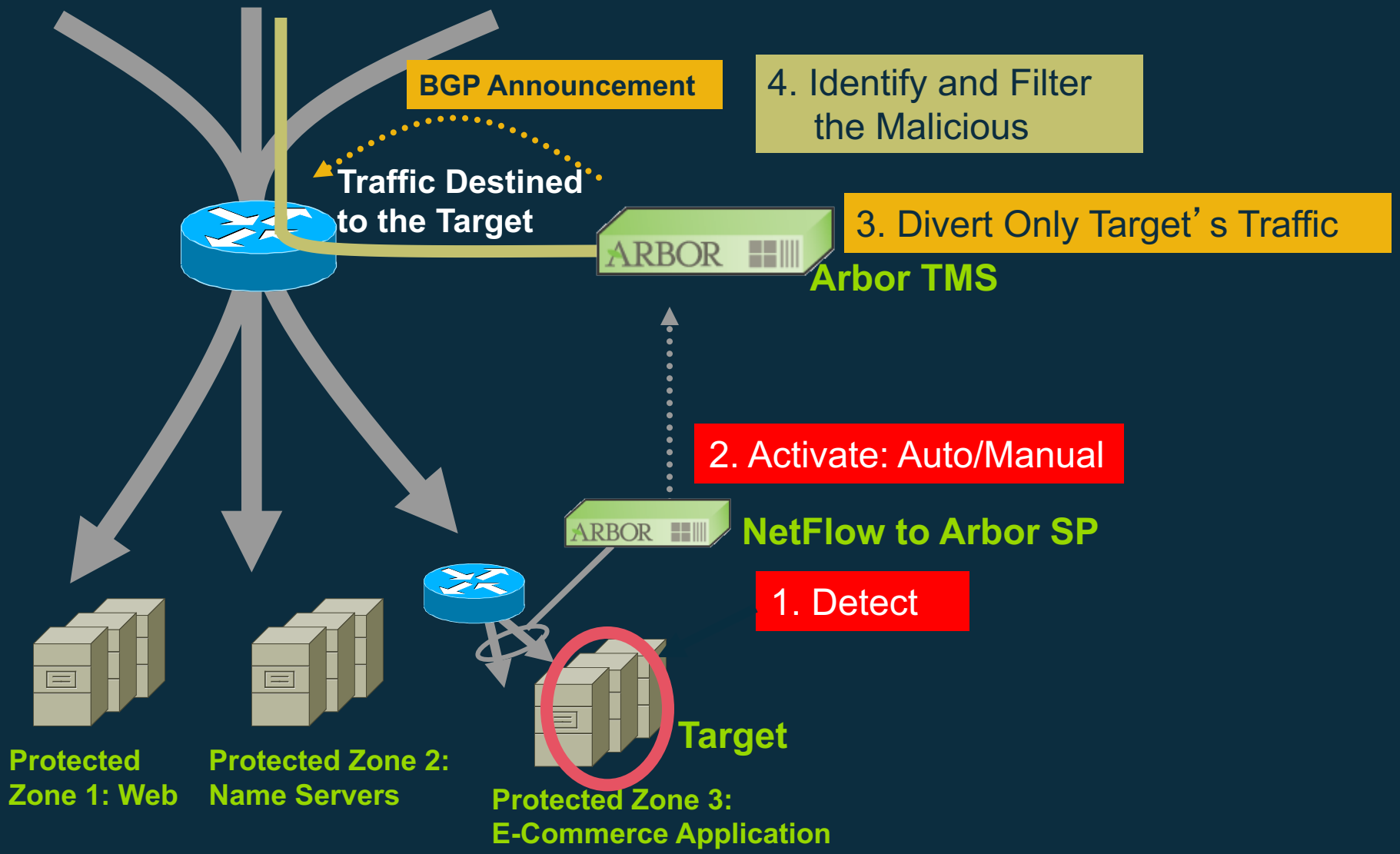
Arbor DDoS Solution: Diversion/Offramping



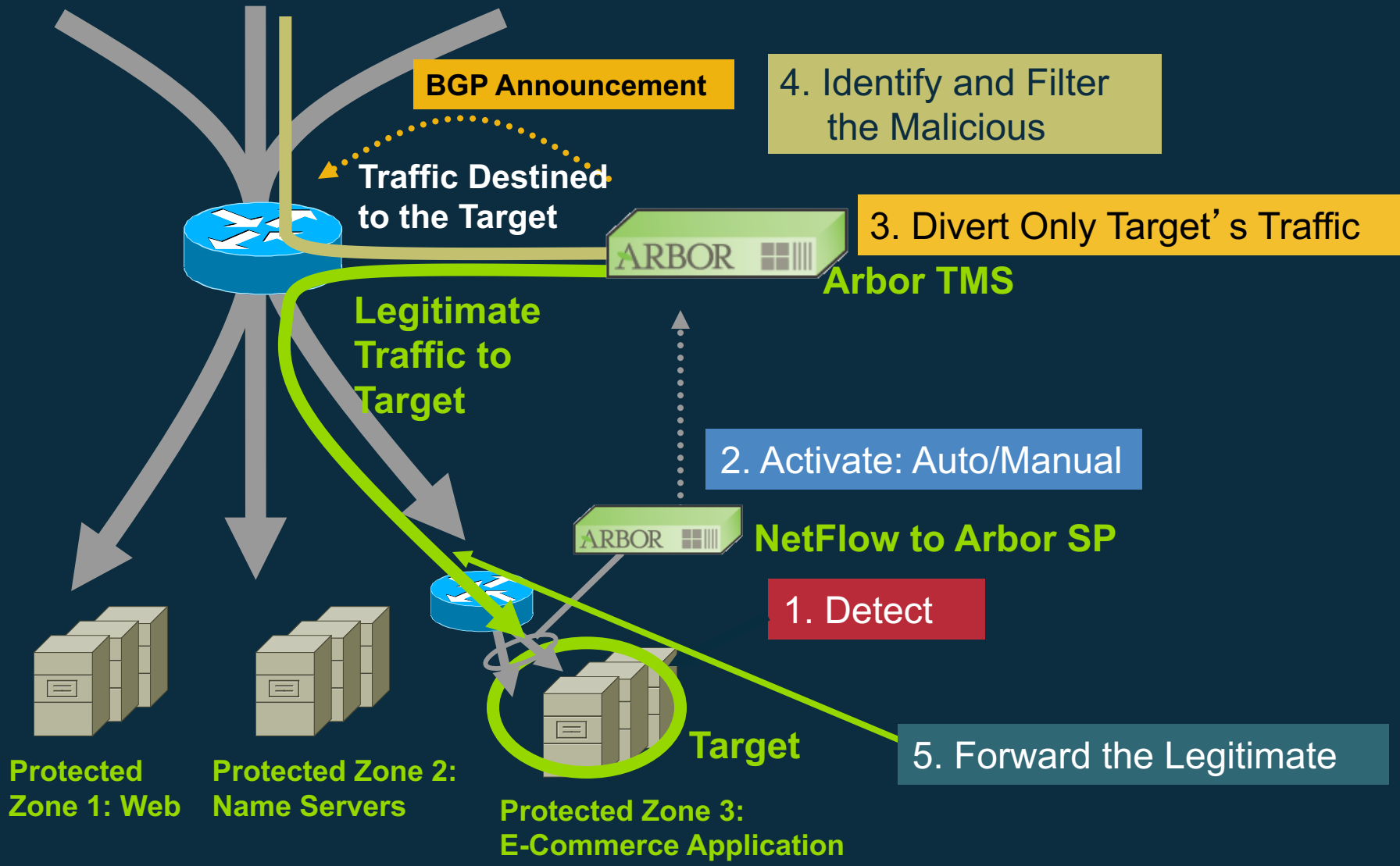
Arbor DDoS Solution: Diversion/Offramping



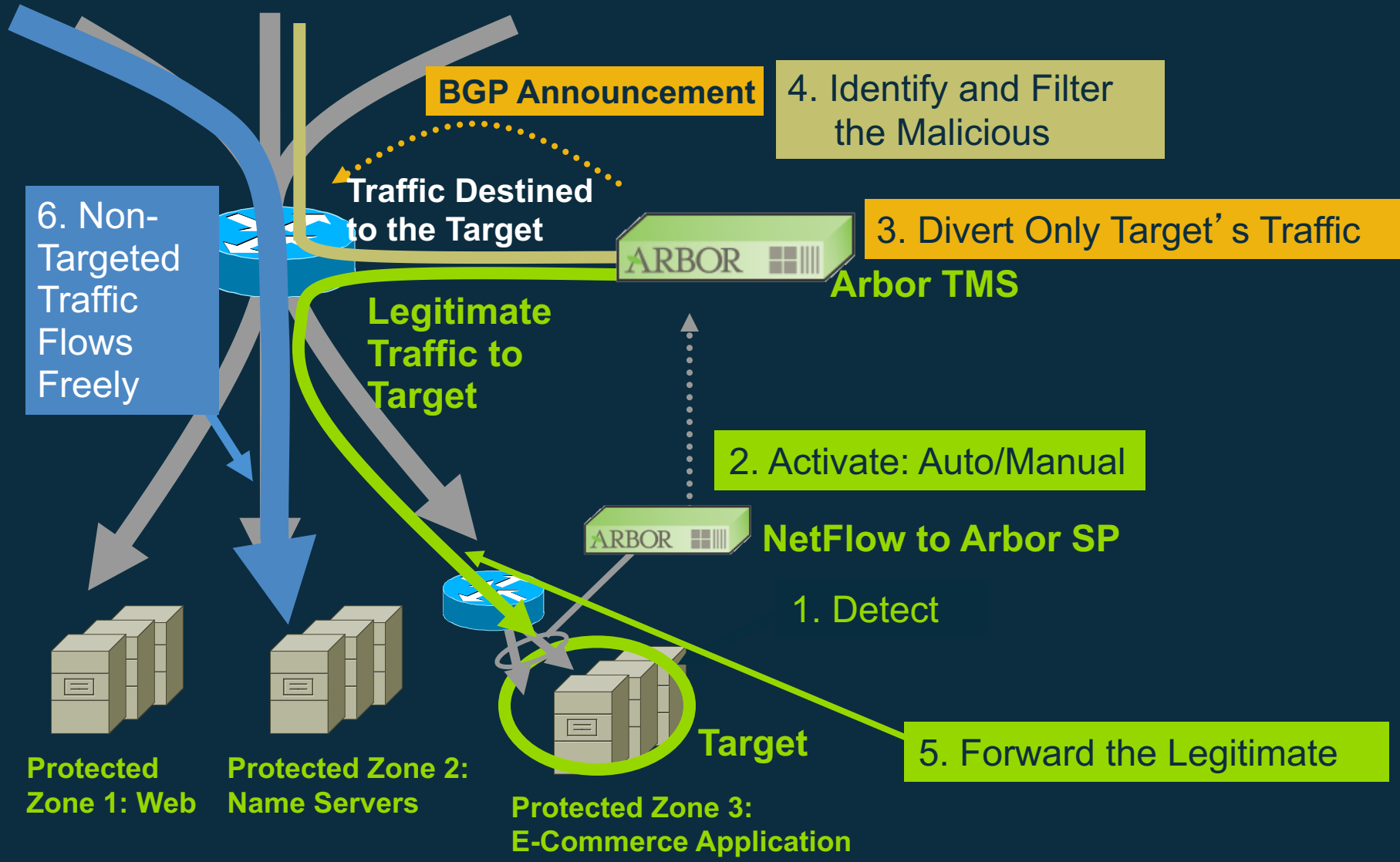
Arbor DDoS Solution: Diversion/Offramping



Arbor DDoS Solution: Diversion/Offramping

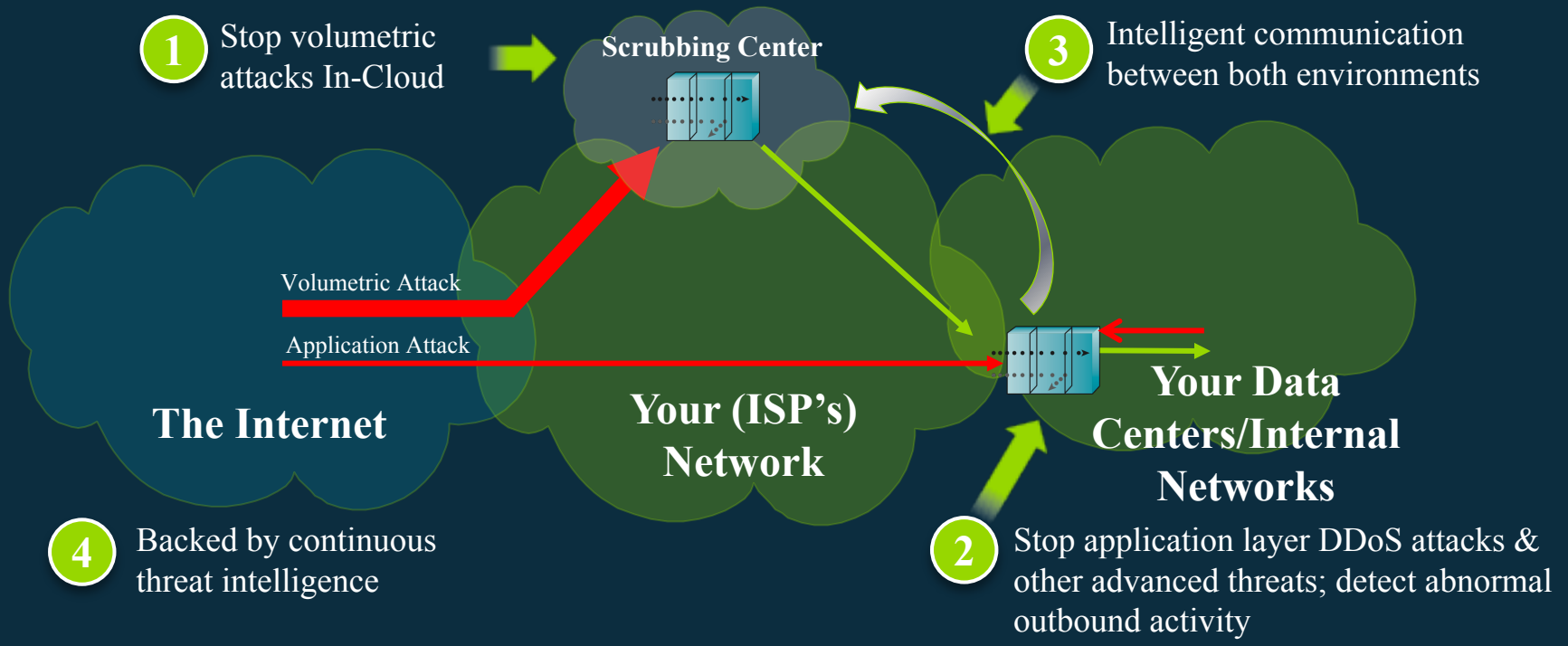


Arbor DDoS Solution: Diversion/Offramping



LAYERED DDoS ATTACK PROTECTION

Layered DDoS Attack Protection



Backed by Continuous Threat Intelligence

A Recommended Industry Best Practice:

FORRESTER® IDC FROST & SULLIVAN Infonetics RESEARCH Securosis ovum

ARBOR® NETWORKS

Q&A / THANK YOU

Contact Information:

Khaled Fadda, Consulting Engineer – Middle East

kfadda@arbor.net