Threading the Eye of the Storm

Effective Security Resiliency with Hybrid Distributed Denial of Service (DDoS) Protection

Tim Nolen <tim.nolen@netscout.com>

Senior Solutions Architect, CISSP, GPEN

Roland Dobbins <roland.dobbins@netscout.com>

Principal Engineer, ASERT

Photo courtesy of NOAA ESRL

Agenda

Background & Context

Attack Surface & Methodologies

Resiliency by Design

DDoS Mitigation Techniques

Conclusion

Background & Context

Distributed Denial of Service (DDoS)

/ˈdēˌdôs/

An attempt to **consume** finite **resources**, **exploit weaknesses** in software design or implementation, or **exploit lack** of infrastructure **capacity**

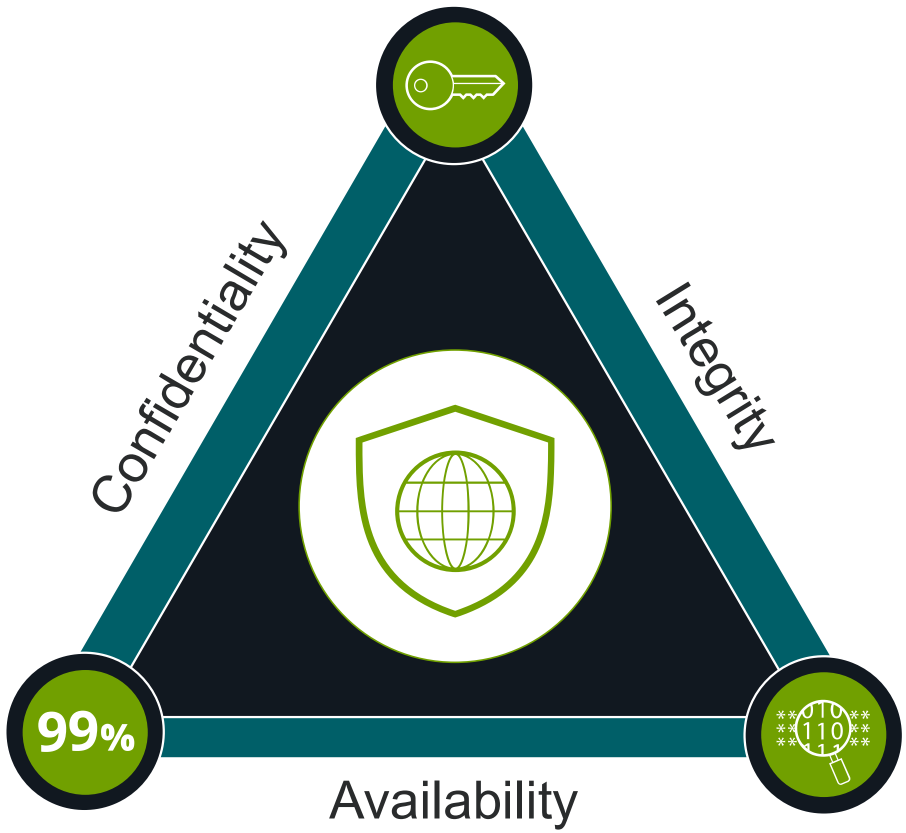
Targets the **availability** and utility of computing and network resources

Attacks are almost always **distributed** for even more significant effect (i.e., DDoS)

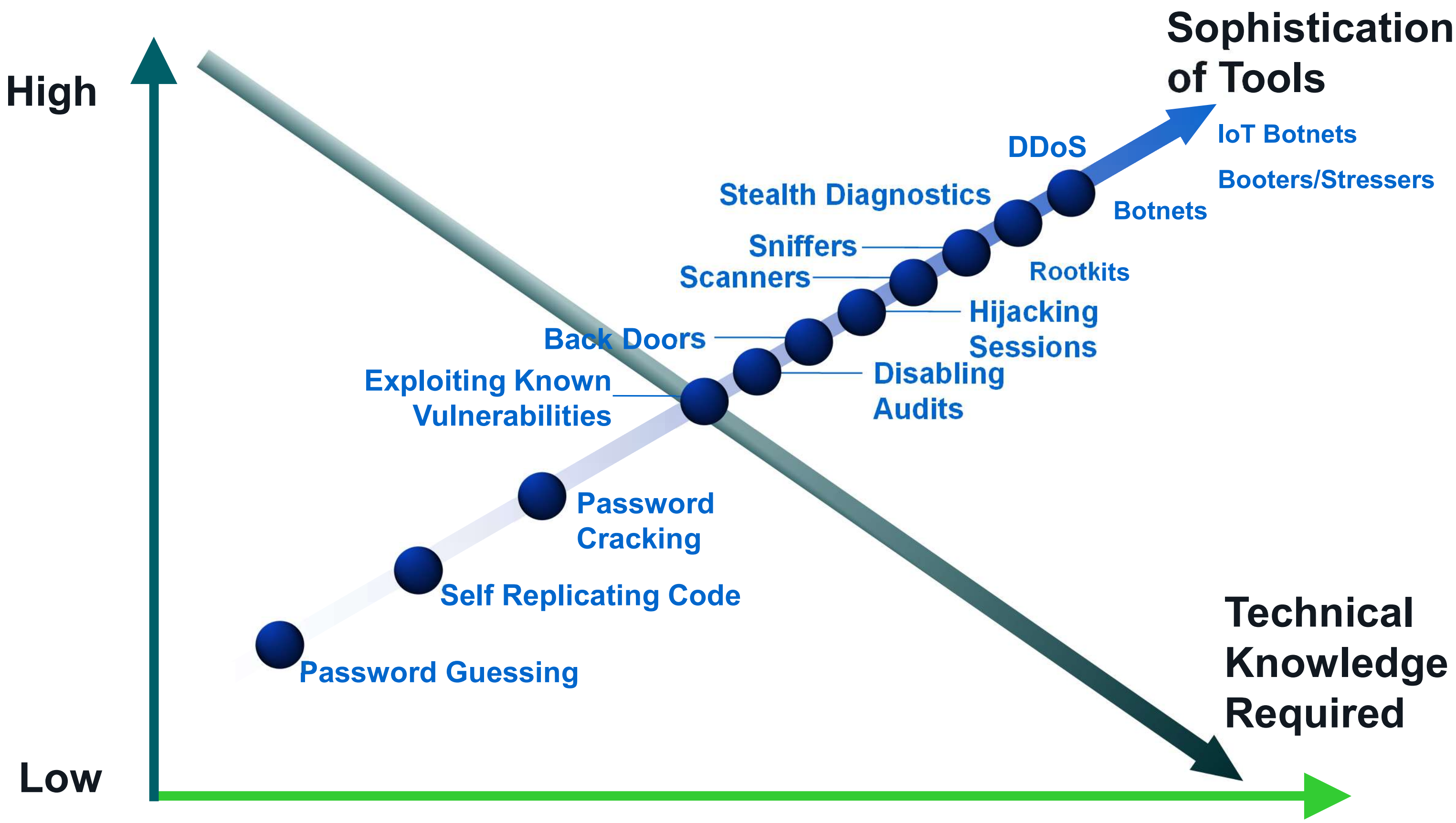
The **collateral damage** caused by an attack can be as bad, if not worse, than the attack itself

Remember the CIA Triad?

Availability, availability, availability



Evolution of Threats and Exploits



A (Highly) Condensed Timeline of DDoS Attacks

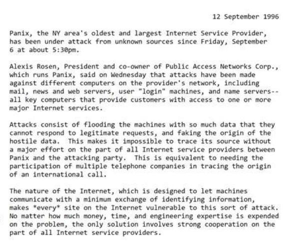
"There's always going to be idiots that do bad things with information. These are growing pains on the Net. We'll fix this and move on to the next one."
– Emmanuel Goldstein, 1996

The Morris Worm
First Internet worm
November 2, 1988

Eggdrop
IRC chat DoS
December 1993

ICMP (ping)
Popular DoS method
1992-1993

Panix
First SYN flood, takes out ISP
September 6, 1996



12 September 1996

Panix, the NY area's oldest and largest Internet Service Provider, has been under attack from unknown sources since Friday, September 6 at about 5:30pm.

Alexis Rosen, President and co-owner of Public Access Networks Corp., which runs Panix, said on Wednesday that attacks have been made against different computers on the provider's network, including mail, news and web servers, user "login" machines, and name servers--all key computers that provide customers with access to one or more major Internet services.

Attacks consist of flooding the machines with so much data that they cannot respond to legitimate requests, and faking the origin of the hostile data. This makes it impossible to trace its source without a major effort on the part of all Internet service providers between Panix and the attacking party. This is equivalent to needing the participation of multiple telephone companies in tracing the origin of an international call.

The nature of the Internet, which is designed to let machines communicate with a minimum exchange of identifying information, makes *every* site on the Internet vulnerable to this sort of attack. No matter how much money, time, and engineering expertise is expended on the problem, the only solution involves strong cooperation on the part of all Internet service providers.

###

Smurf
ICMP-based reflexive amplification attack
1997

fapi
CERT reports first DDoS botnet
1998

DDoS Extortion
Criminals extorting gambling/porn sites
1998

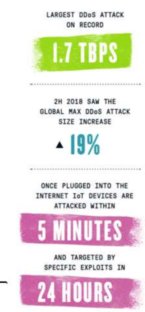
EHippies
Ideology driven DDoS, participatory botnet
1999

SQL Slammer
Cascading failure
2003

Mirai
Widely successful IoT botnet
2016

Krebs on Security
620Gbit/s
September 20, 2016

Terabit Era
1.7Tbps memcached reflection/amplification
March 5, 2018

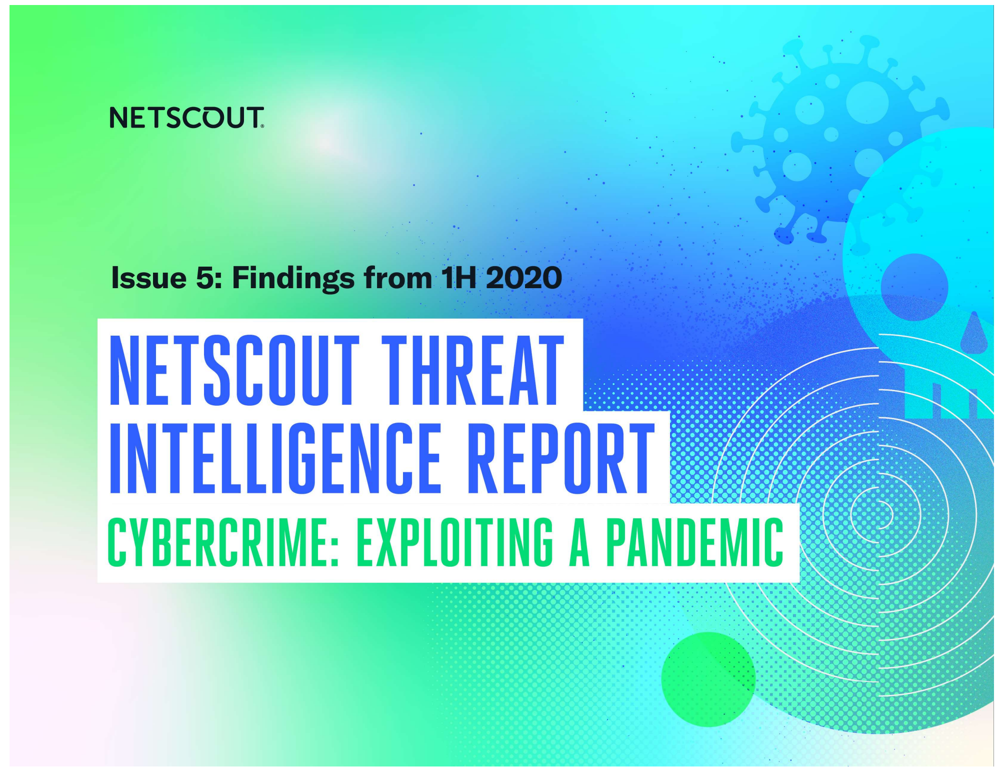


Lazarus Bear Armada
DDoS extortion v2
2020

Trends as of 1H 2020

Key Findings

- Pandemic Profiteers
  - 929,000 DDoS Attacks in May alone
  - 4.83 Million DDoS Attacks 1H 2020
- Hidden Impact of DDoS Traffic
  - 15% Increase YoY
  - 25% Increase during Pandemic
  - DDoS Attack Coefficient (DAC)
- Complex Multivector Attacks
  - 2,851% Increase since 2017 in 15+ vectors
  - 43% Decrease in single-vector YoY



https://www.netscout.com/threatreport

Global DDoS Attack Trends

Largest attack in 1H 2020 occurred in APAC region.

Despite the single attack, most attacks are under 100 Gbps.

However, attacks combine increased speed, shorter duration, and more vectors

Shorter duration + increased complexity = less time to respond to harder to mitigate attacks

Attack Size

1.12 TBPS Largest attack in 1H 2020

▲ **77%** Growth in max attack size in 1H 2020 from 1H 2019

Attack Duration

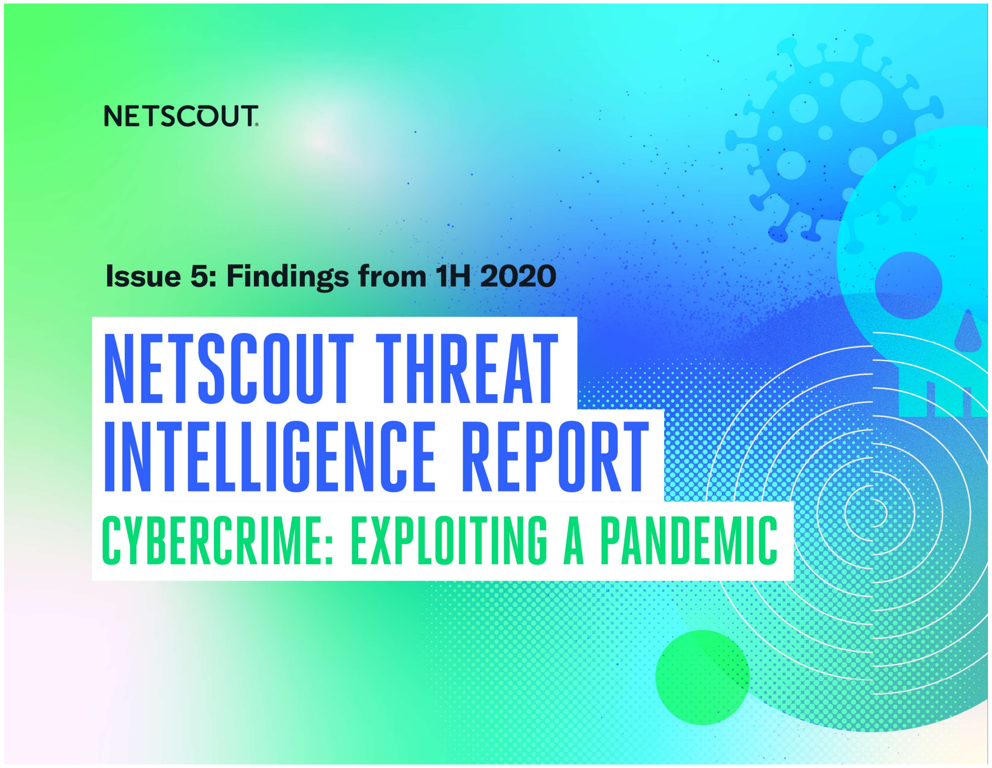
▼ **51%** Decrease in attack duration in 1H 2020 from 1H 2019

92% Of attacks were less than an hour

For More In-depth Coverage…

If you are looking for real-time data on global DDoS attacks, Cyber Threat Horizon is an invaluable (and free) tool.

https://www.netscout.com/horizon



https://www.netscout.com/threatreport

Attack Surface

Points of Impact

Service Provider/Internet Backbone:

Large pipes, highly connected infrastructure

Volumetric Attacks

Customer/Enterprise Edge:

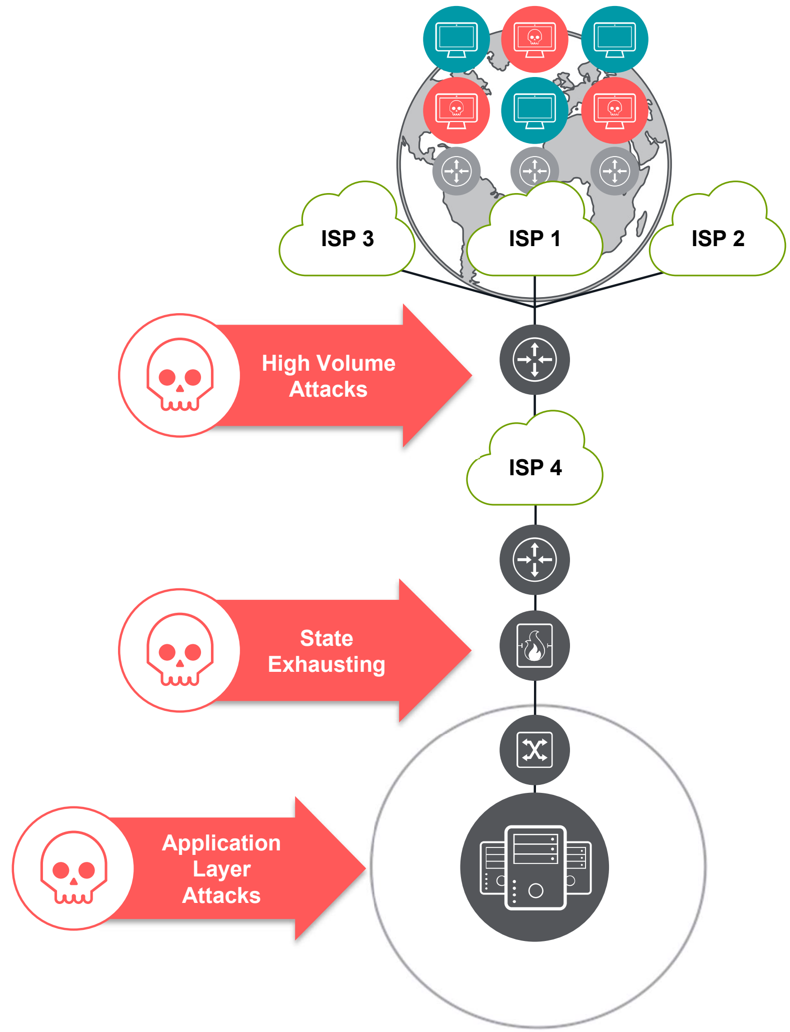
Edge routers, Firewalls, Load Balancers, VPN concentrators

Volumetric & State Exhaustion Attacks

Datacenter:

Web Servers, App Servers, DB, SIP, etc.

Volumetric, State, & Application Layer Attacks



Volumetric Attacks

“The numbers all go to 11…” – Nigel Tufnel

Description

Flood of traffic for one or more protocols and/or ports

Can be designed to look like normal traffic — often consists of brute-force garbage packets

Direct flooding or reflection/amplification attacks (more on this later)

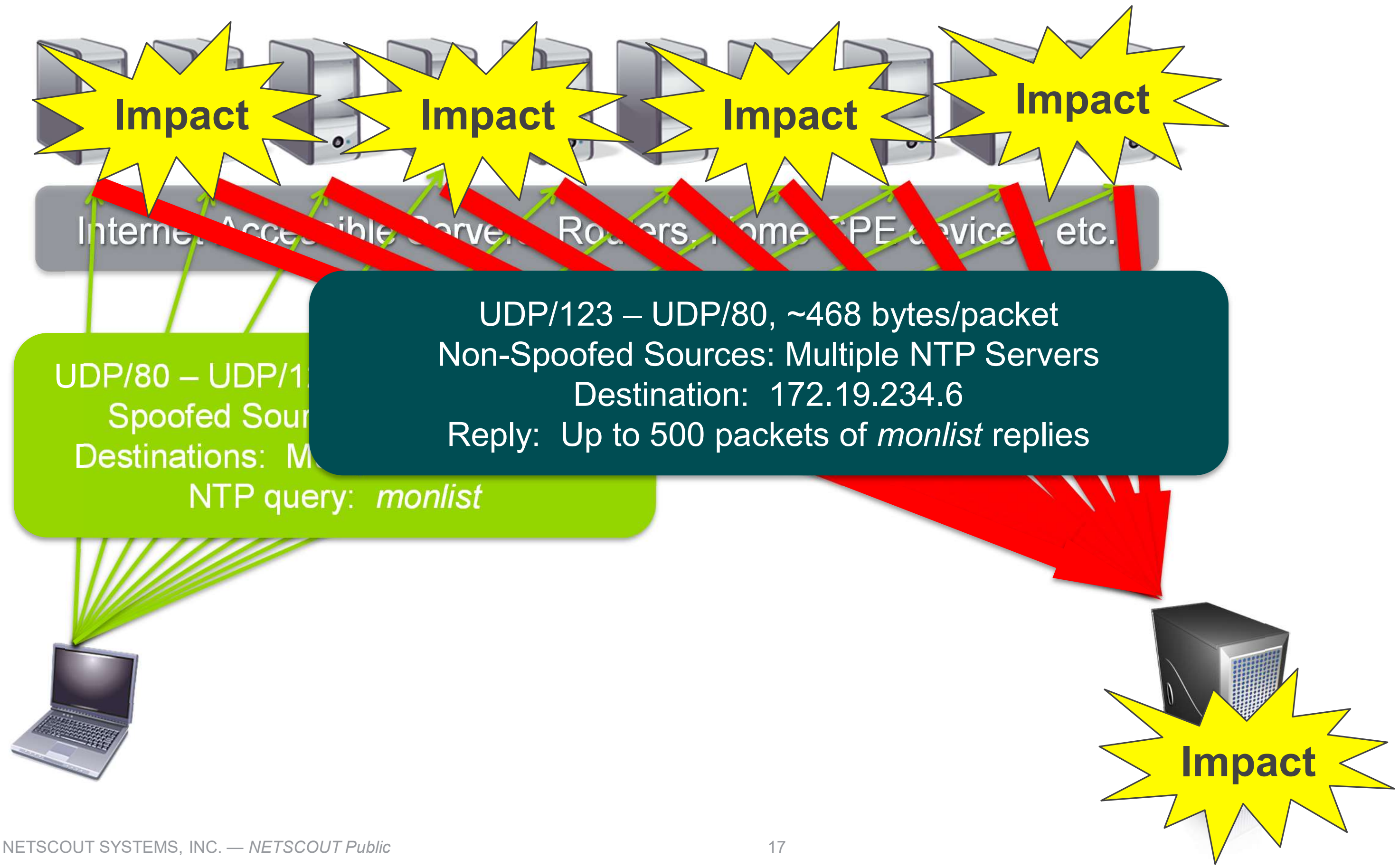
May be spoofed or non-spoofed

Common Vectors

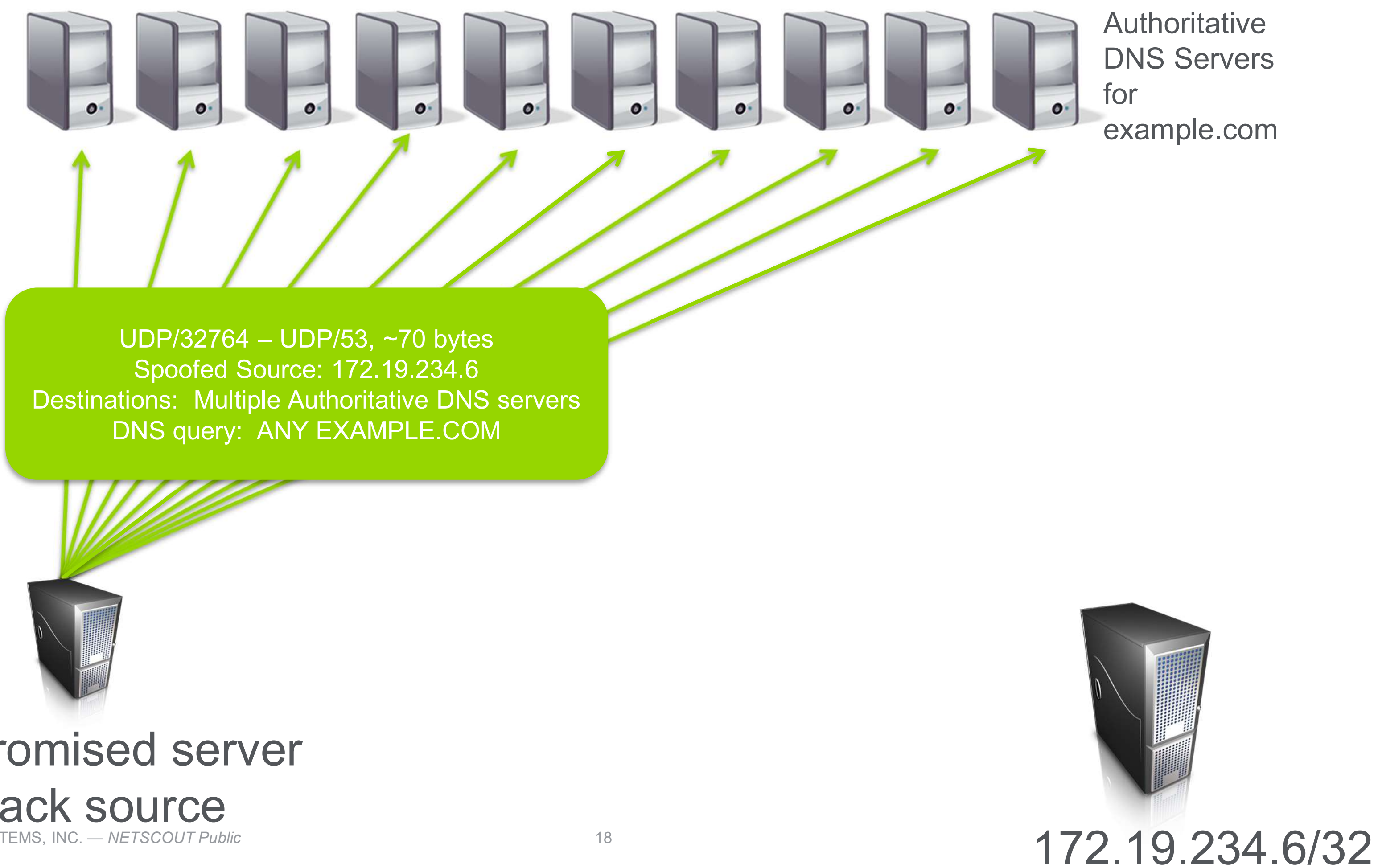
SYN-flood, RST-flood , UDP flood, non-initial fragments flood, GRE flood, ESP flood, UDP reflection/amplification, TCP reflection/amplification

Volumetric Attacks: Reflection/Amplification

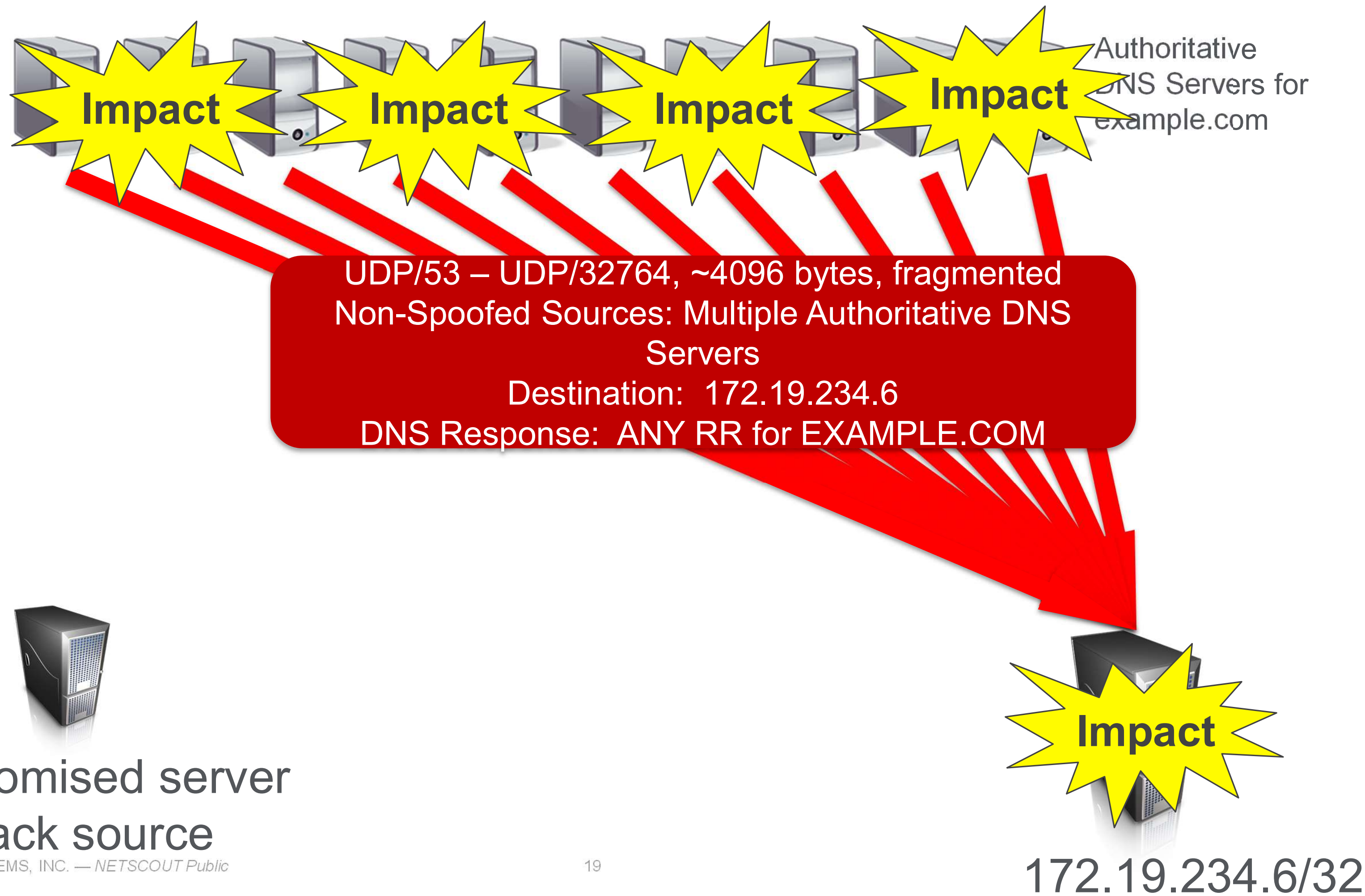
Mirror, mirror in the net…



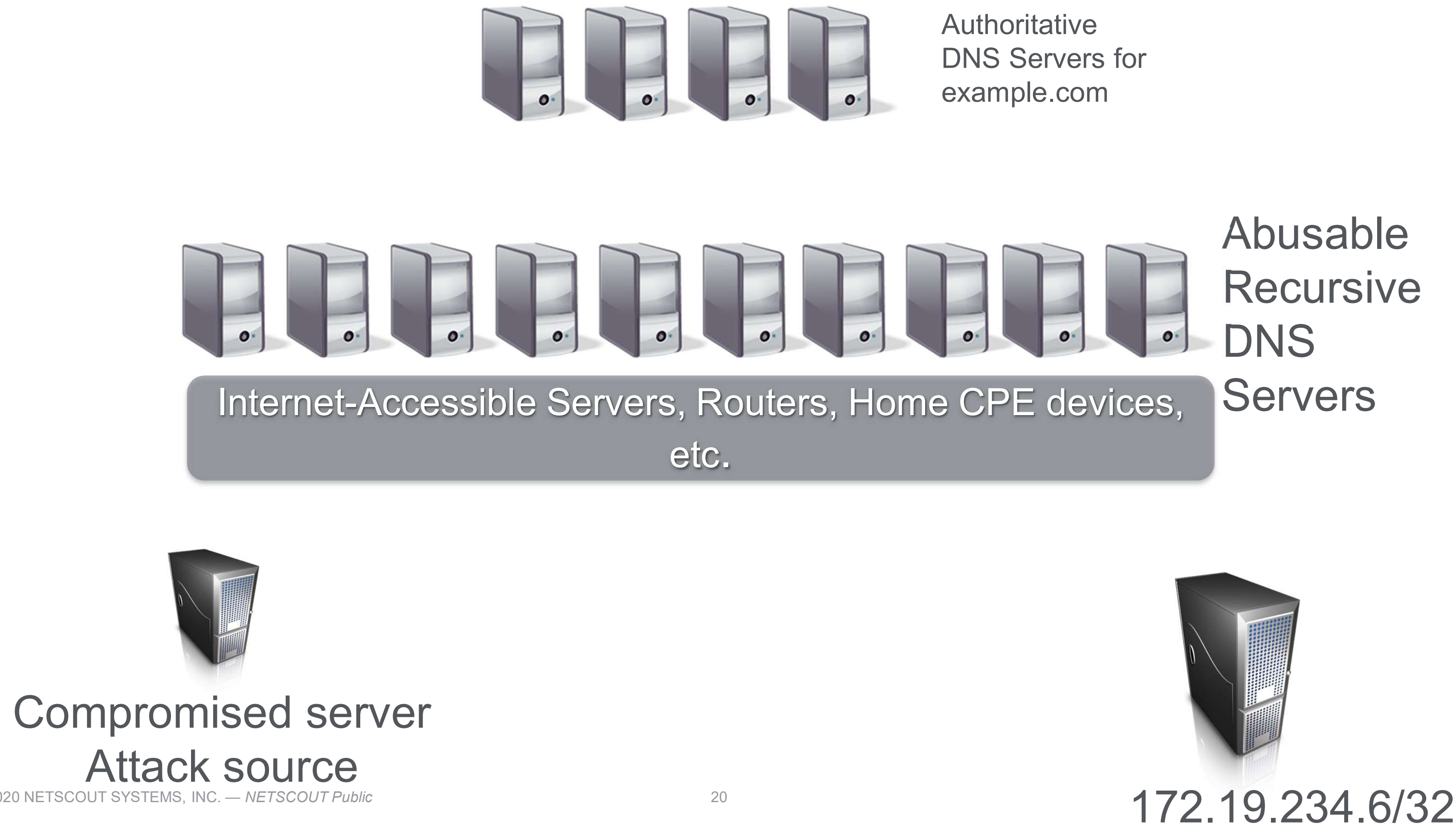
DNS Reflection/Amplification Attack Methodology #1



DNS Reflection/Amplification Attack Methodology #1

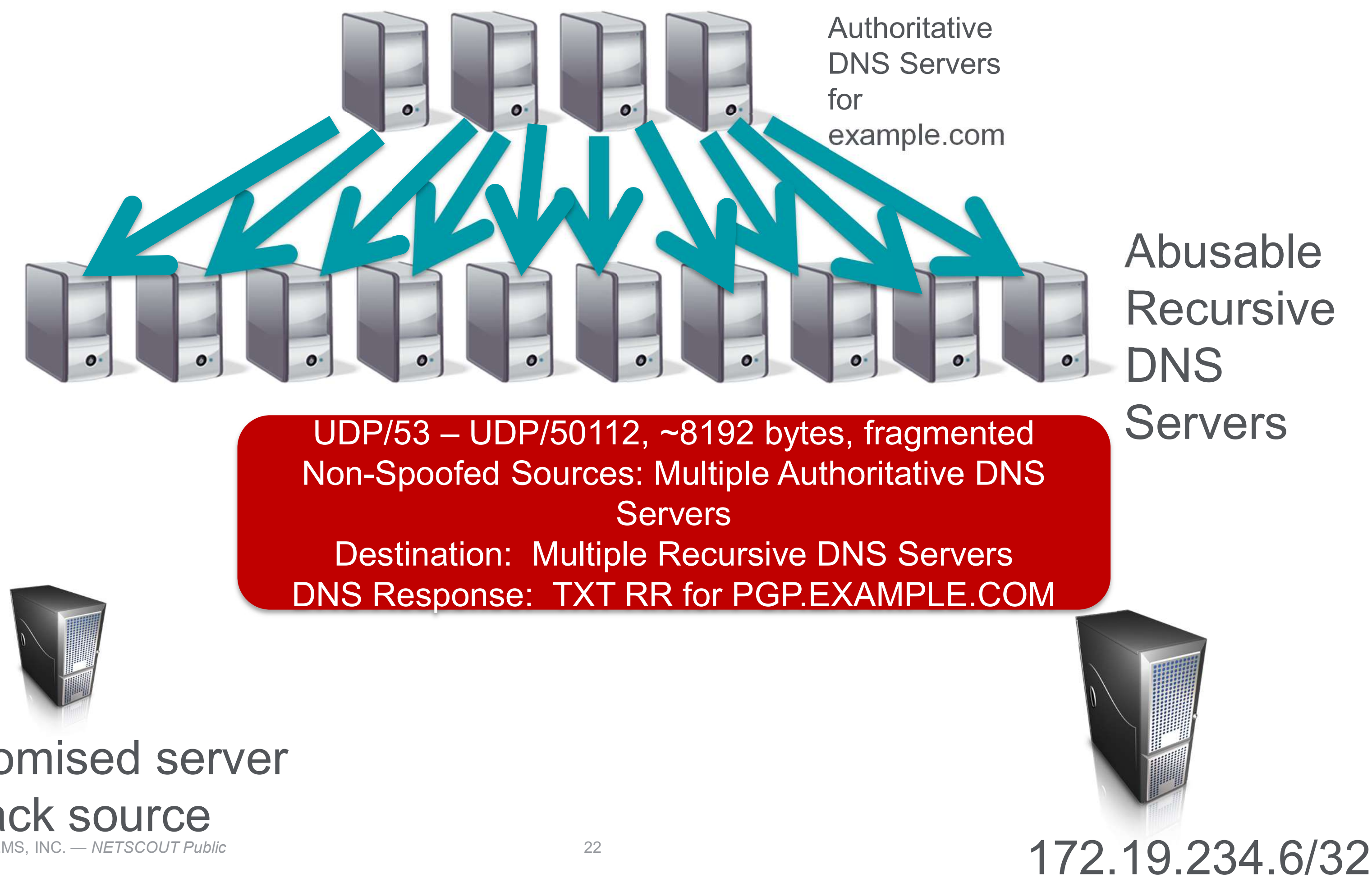


DNS Reflection/Amplification Attack Methodology #2

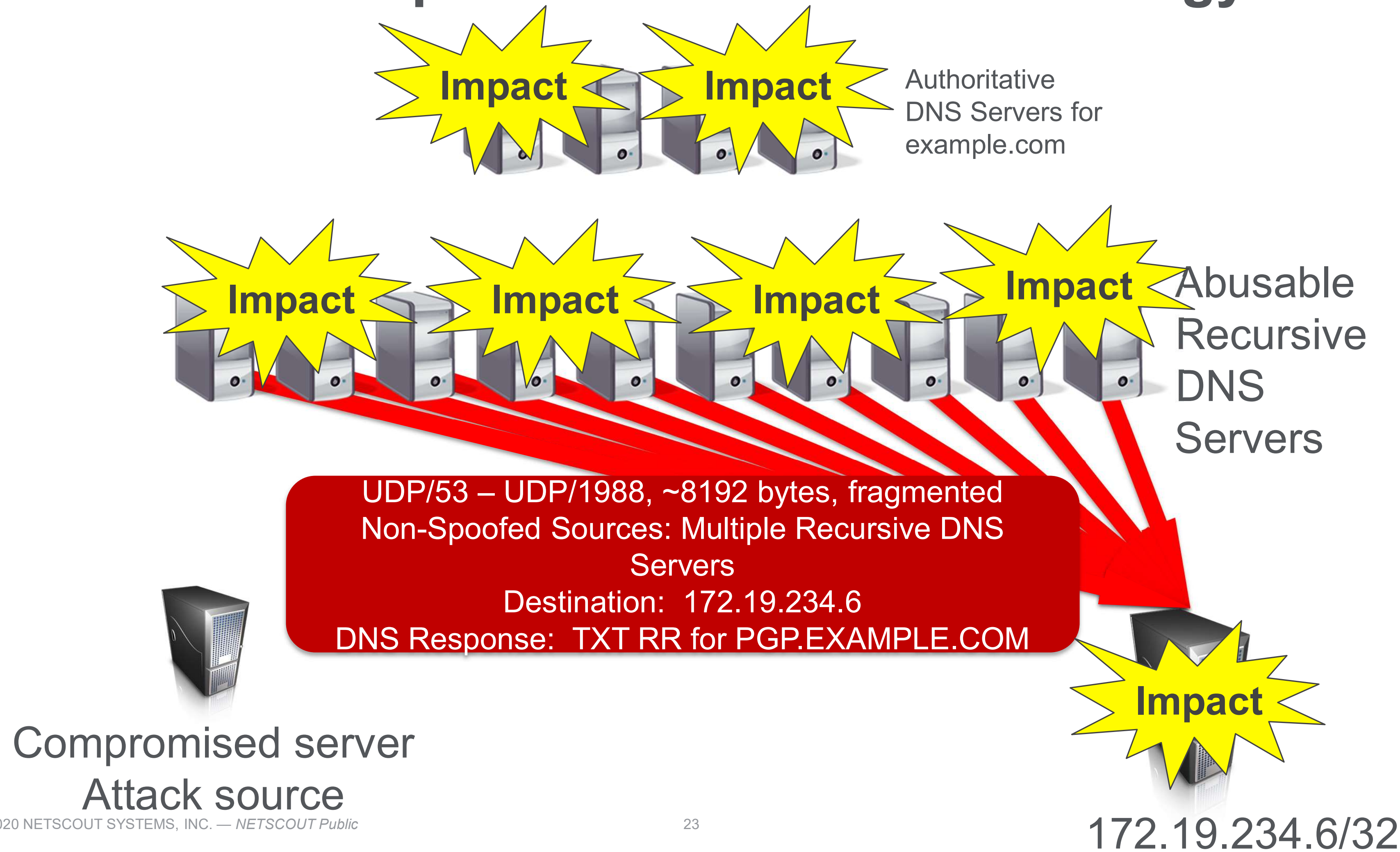


DNS Reflection/Amplification Attack Methodology #2

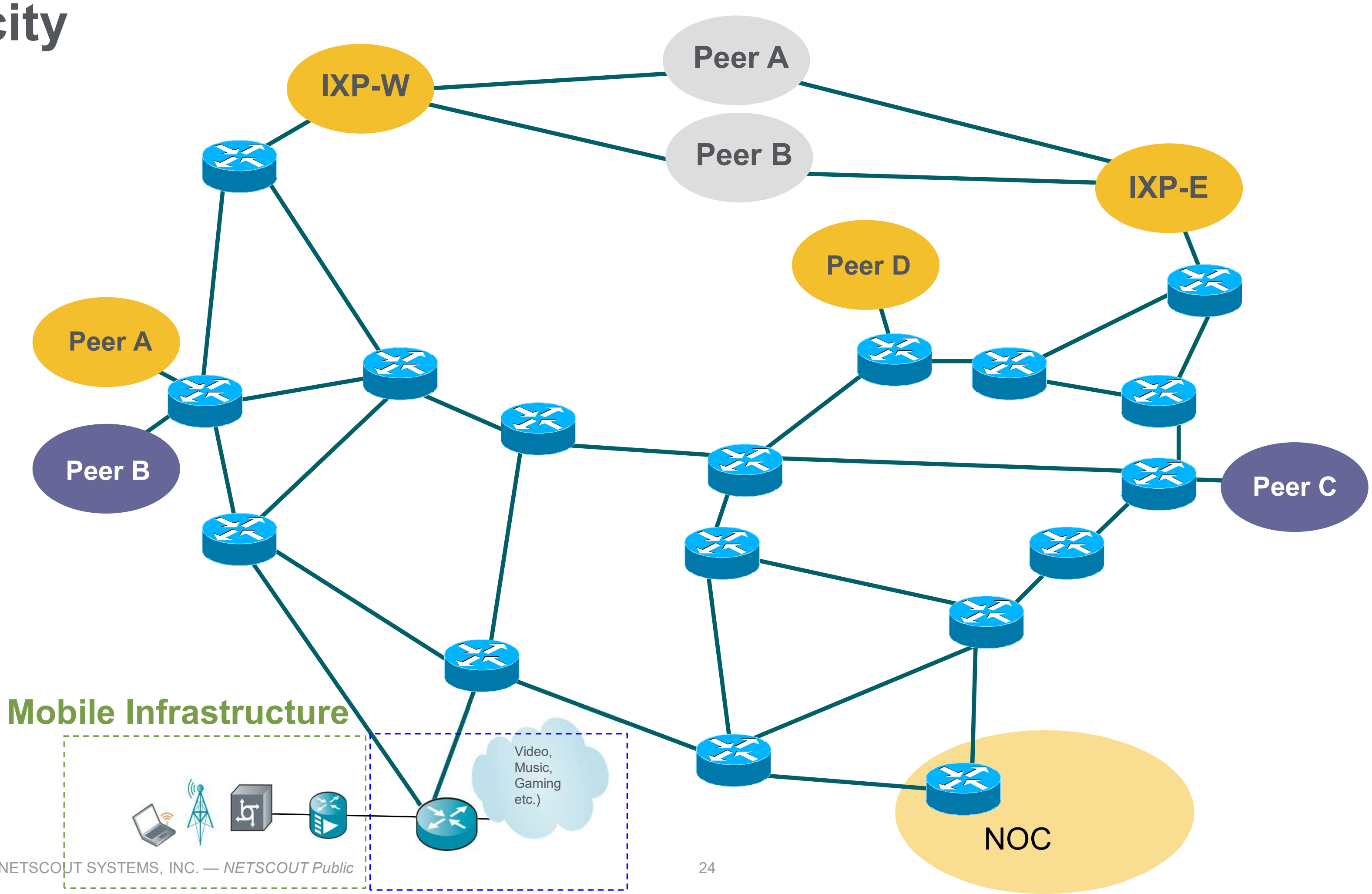
DNS Reflection/Amplification Attack Methodology #2



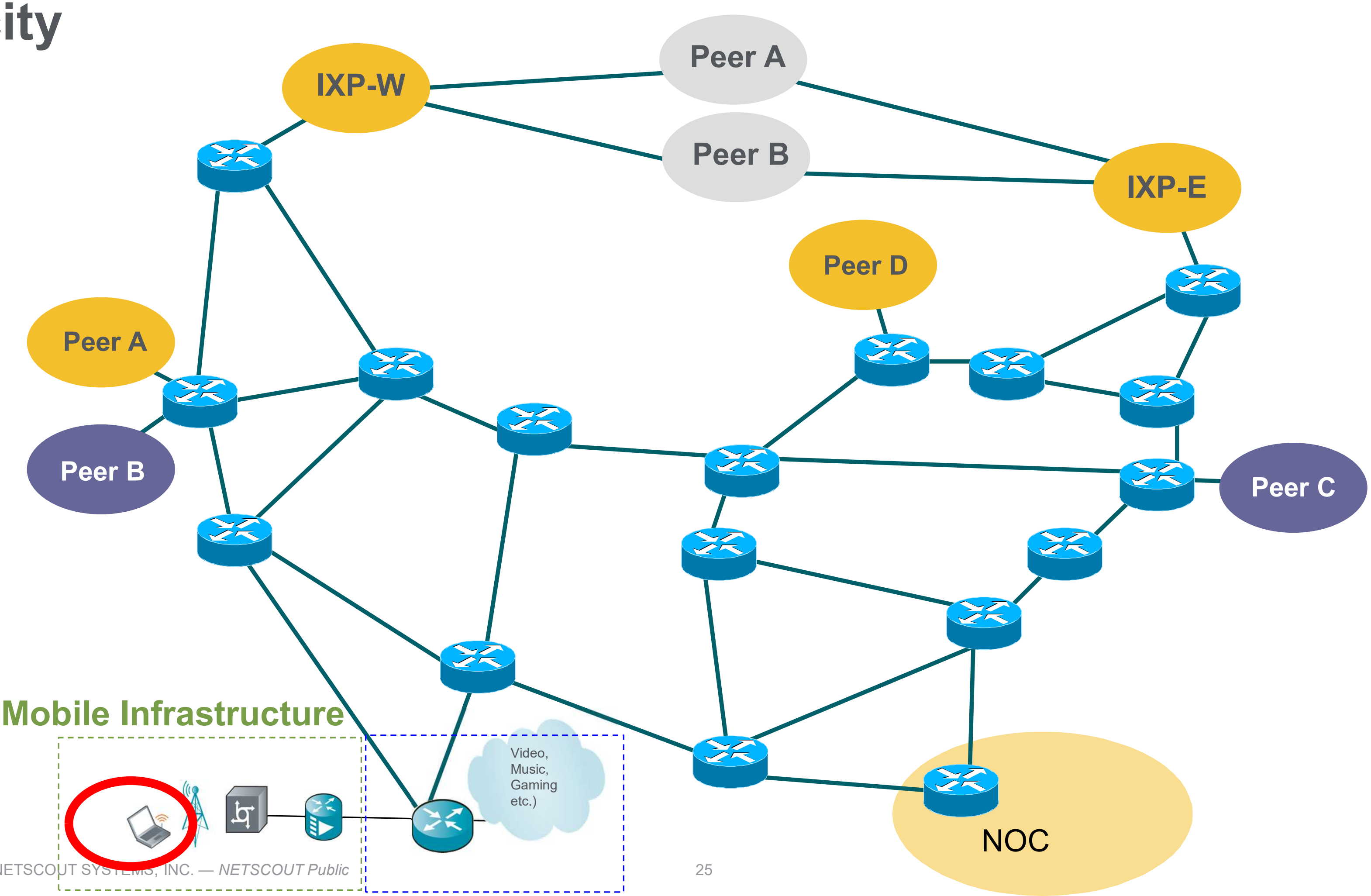
DNS Reflection/Amplification Attack Methodology #2



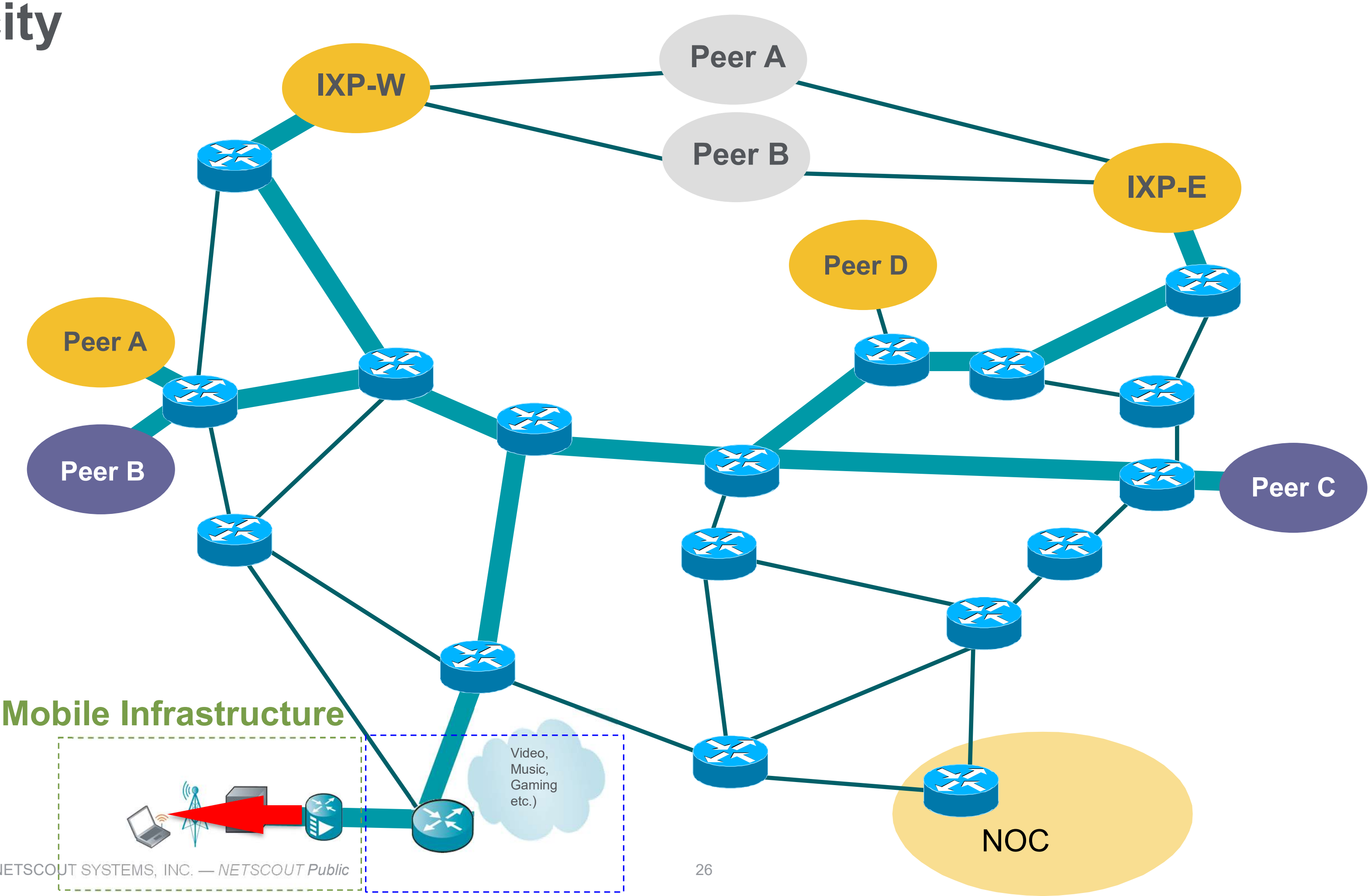
Effects of a Reflection/Amplification DDoS Attack on Network Capacity



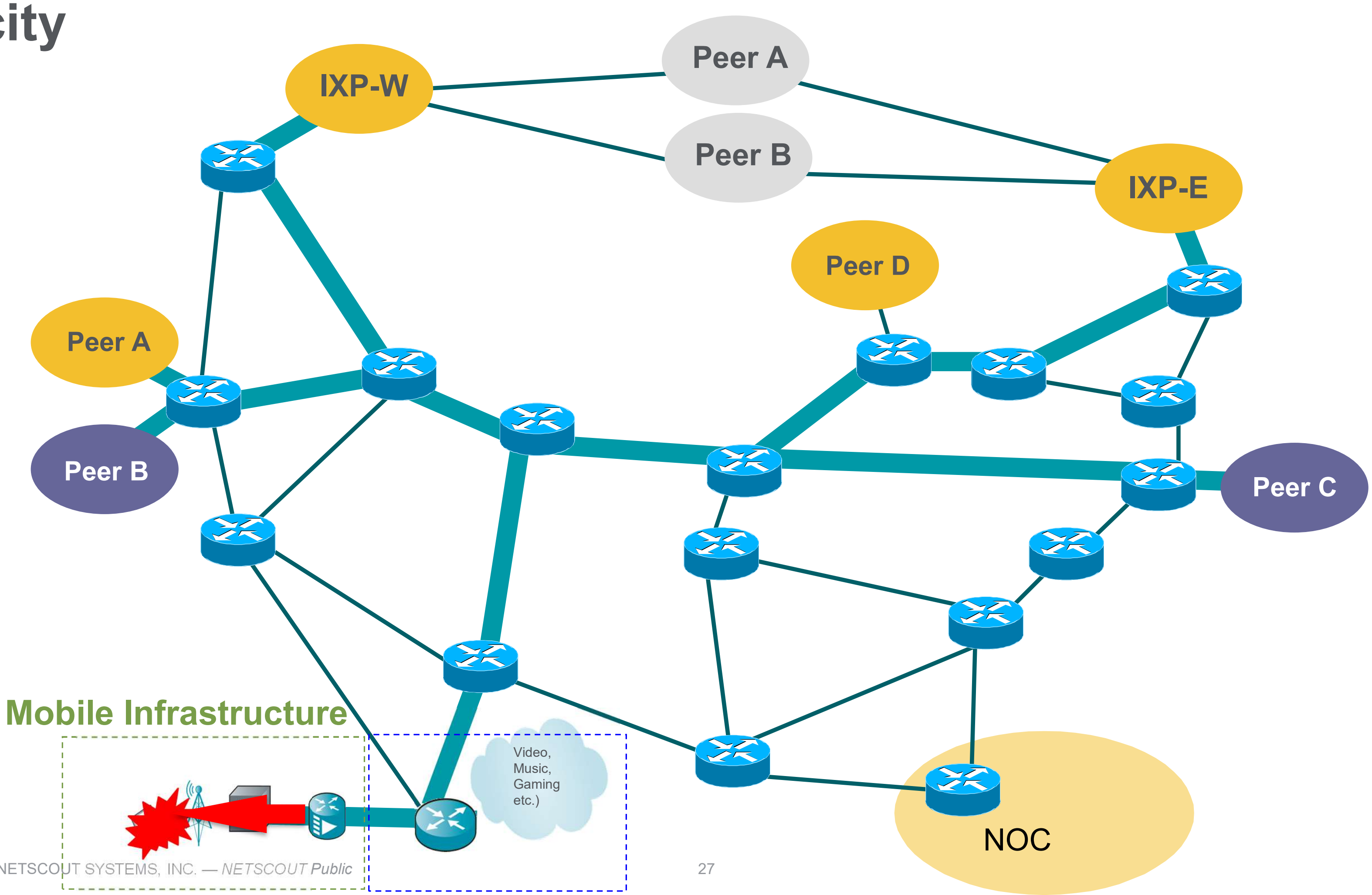
Effects of a Reflection/Amplification DDoS Attack on Network Capacity



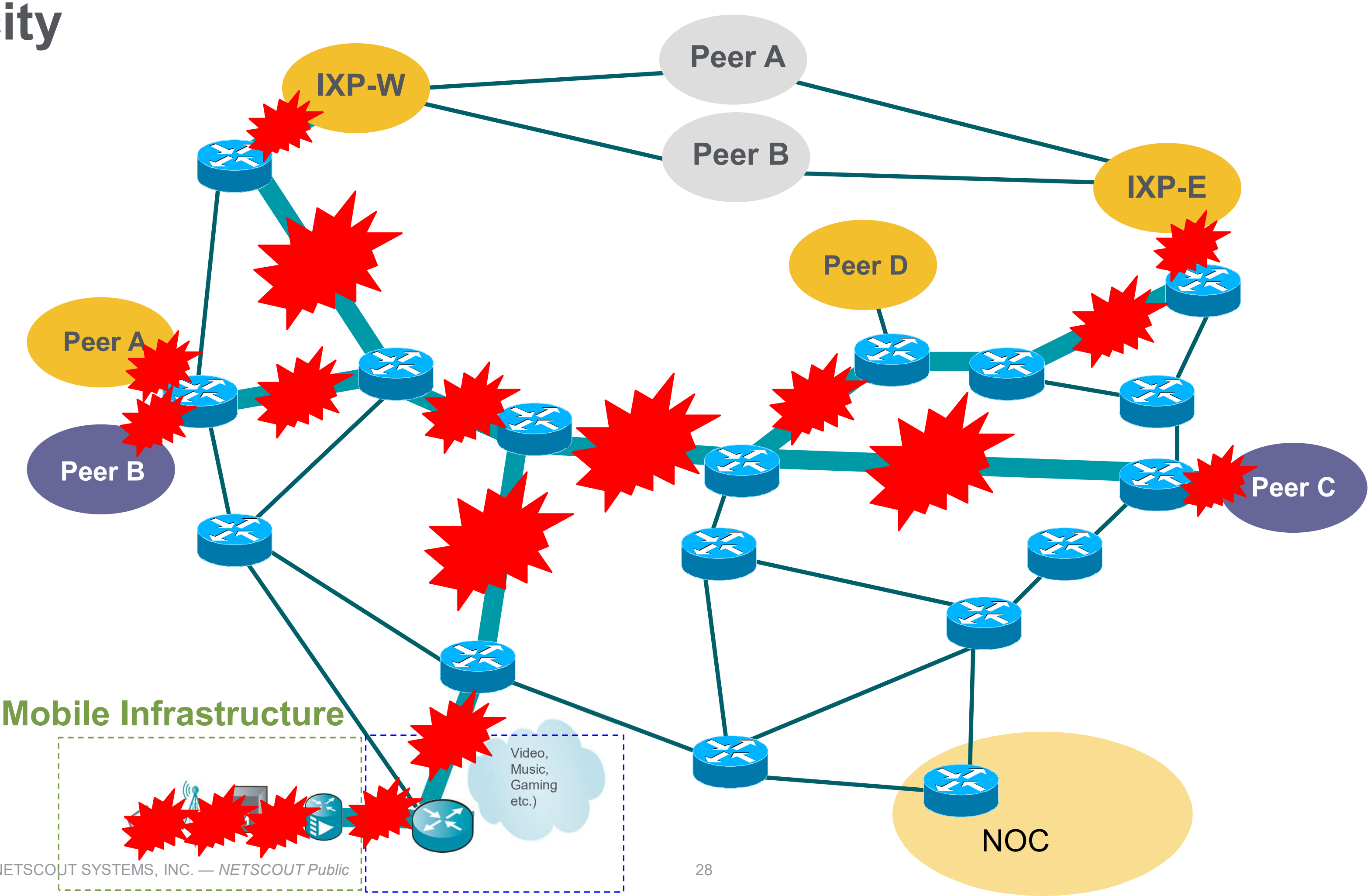
Effects of a Reflection/Amplification DDoS Attack on Network Capacity



Effects of a Reflection/Amplification DDoS Attack on Network Capacity



Effects of a Reflection/Amplification DDoS Attack on Network Capacity



TCP State-Exhaustion Attacks

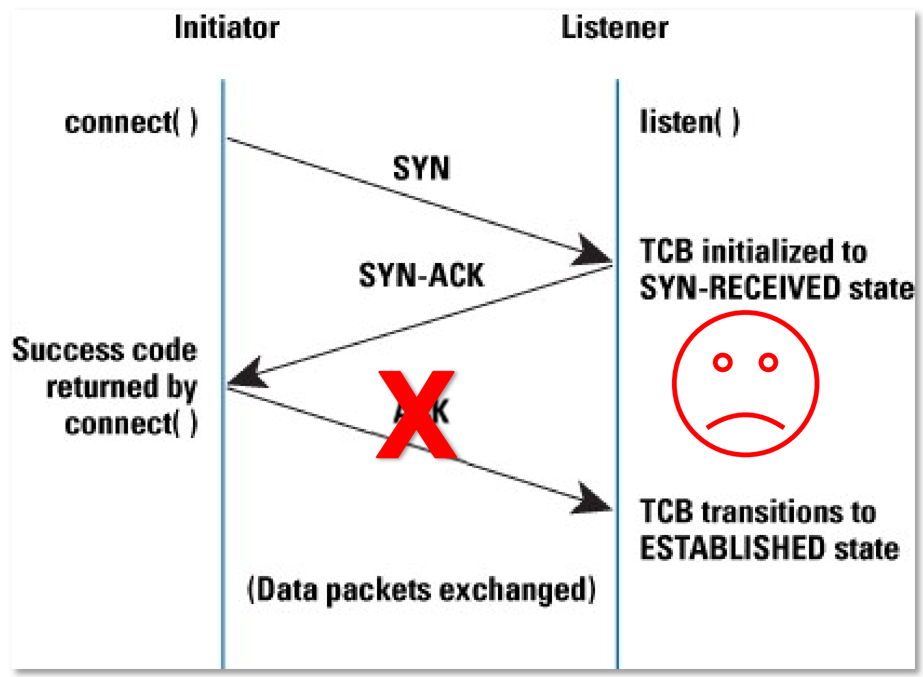
Why not use ALL the flags?

Description

- Overwhelm a certain aspect of the TCP connection process to keep the host from being able to respond to legitimate connections
- Generally floods at large packet rates
- Source addresses may be spoofed or non-spoofed

Common attack vectors

- TCP SYN, TCP FIN, TCP RST, TCP Flags



Final ACK not sent leaves TCP connection half open tying up Transmission Control Block (TCB)

Application-Layer Attacks

Description

Attacks designed to overwhelm components of specific applications

Commonly seen against HTTP, DNS and SIP in particular

May be stealthy by mixing with a much higher traffic volume on the same protocol/port

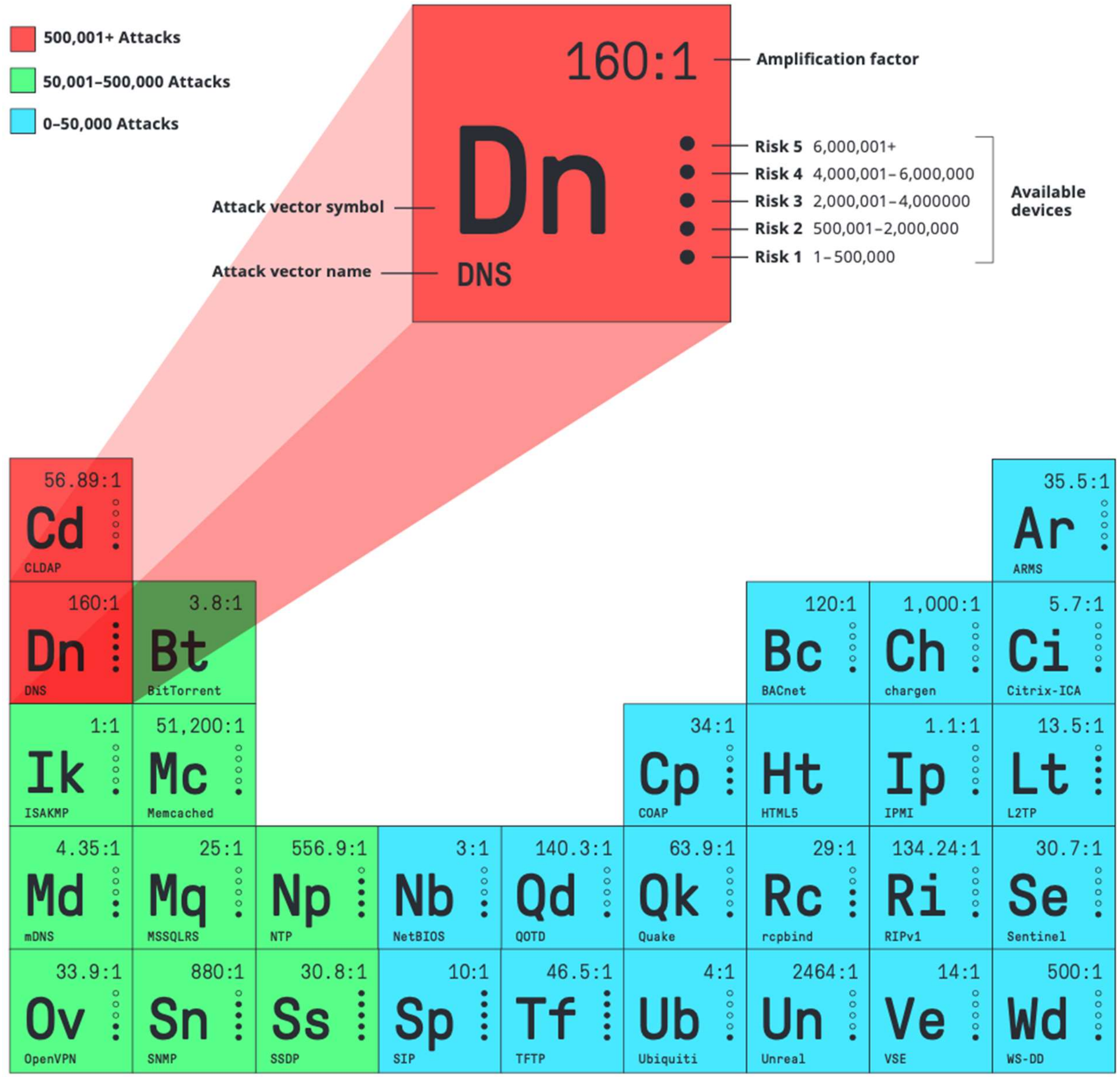
Common Attack Vectors

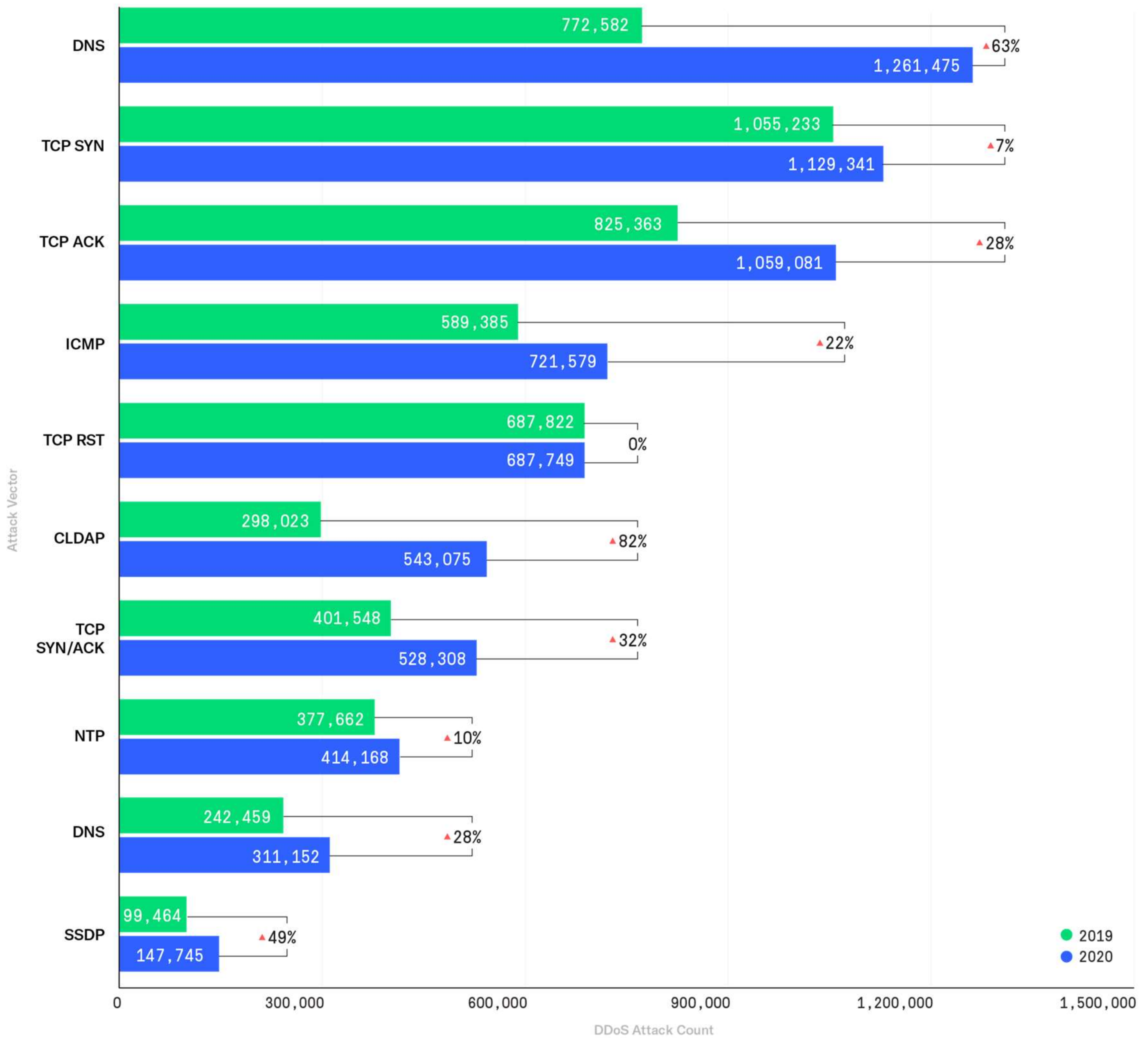
HTTP GET floods, HTTP/S TLS Negotiation floods, SIP Invite floods, DNS non-existent query attacks (‘DNS Water Torture’, et. al.)

Periodic Table of DDoS Attack Vectors

DNS and CLDAP topped the charts in 1H 2020 for the most UDP Reflection/Amplification attacks.

DNS, SIP, SSDP, and TFTP all surpass 6,000,000+ available reflectors/amplifiers available to attackers.





Top DDoS Attack Vectors

DNS Reflection/Amplification attacks took #1 spot in the 1H 2020, representing a 63% increase over 1H 2019. Additionally, non-reflective DNS attacks also made its way into the top ten for 1H 2020

All TCP-based attacks increased in usage in 1H 2020.

Some TCP SYN, and ICMP attacks may be sympathetic to websites and services going offline from attacks.

DNS Query-Flooding

But I didn't ask for that

Description

Attackers send valid but (usually) spoofed DNS request packets at a very high packet rate and from a very large group of source IP addresses.

Generally floods at large packet rates

Source addresses may be spoofed

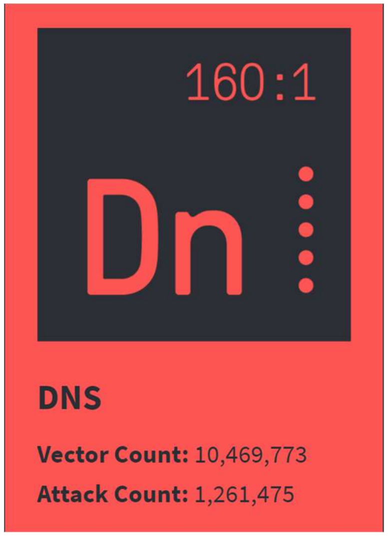
Requested records may be large

Requested records may not exist

Common attack variants

Large-record queries, non-existent record queries (including 'DNS

Water Torture'), may be collateral impact of DNS reflection/amplification

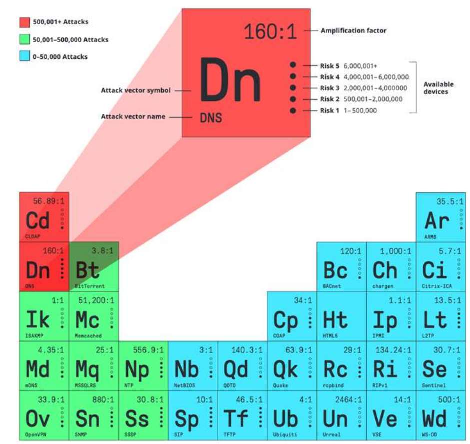


UDP Reflection/Amplification Attacks

Connection? What connection…

Description

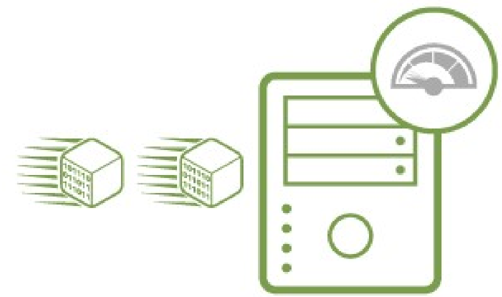
Attacker has the ability (often via booters/stressers) to spoof queries from the target's IP address(es) — abusable services on the Internet act as reflectors/amplifiers, amplification factors of 1000:1 or more, in some cases.



Common reflection/amplification attack vectors

DNS, CLDAP, ntp, SSDP, SNMP, chargen, WS-DD, ARMS, VSE, mDNS, memcached, RIPv1, rpcbind, MSSQL, L2TP, CoAP,

tftp, et. al.



2.3 Tbps CLDAP attack on AWS took place in February 2020

TCP Reflection/Amplification Attacks

Description

Attacker has the ability (often via booters/stressers) to spoof the IP address of the target, generates SYN-packets destined for TCP-based services in order to generate SYN/ACK-floods towards the target. Exploits the nature of the TCP 3-way handshake.

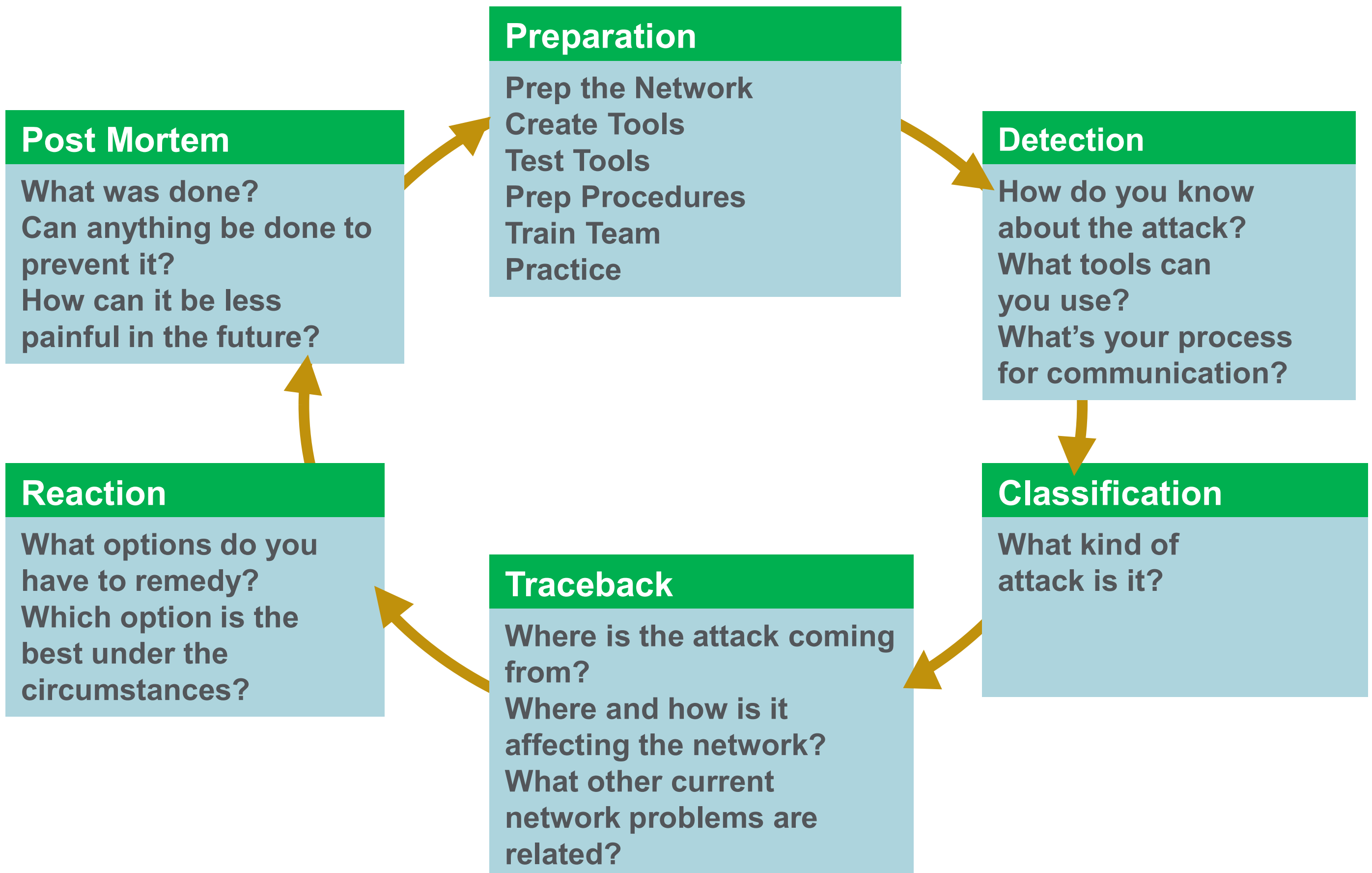
Common attack vectors

Web servers, application servers, anything TCP-based; attackers often leverage well-known cloud services to complicate mitigation efforts.

NETSCOUT

Resiliency by Design

Six Phases of Incident Response



Preparation

Develop and Deploy a Solid Security Foundation

Includes technical and non-technical components

Encompasses best practices

The hardest yet most important phase

Without adequate preparation, you are destined to fail

The midst of a large attack is not the time to be implementing foundational best practices and processes

Preparation

- Know the enemy
  - Understand what drives the miscreants
  - Understand their techniques
- Create the security team and plan
  - Who handles security during an event; is it the security folks; the networking folks
  - A good operational security professional needs to be a cross between the two: silos are useless
- Harden the devices
- Prepare the tools
  - Network telemetry
  - Reaction tools

Preparation

Establish upstream/downstream contacts

- Understand their capabilities
- Establish a relationship and contact procedures
- An attack is no time to figure out how to contact an upstream or understand how they could potentially assist you

Infrastructure security

- All of the techniques talked about today also assume that the infrastructure is available to route and forward packets!

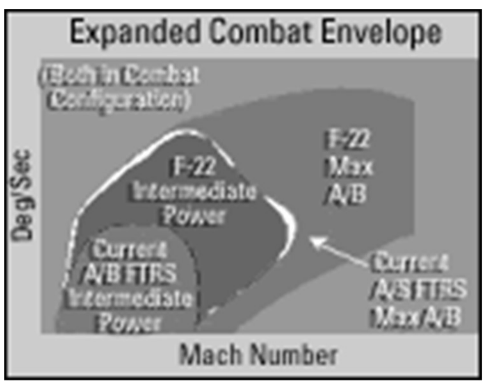
Are You Pushing the Envelope?

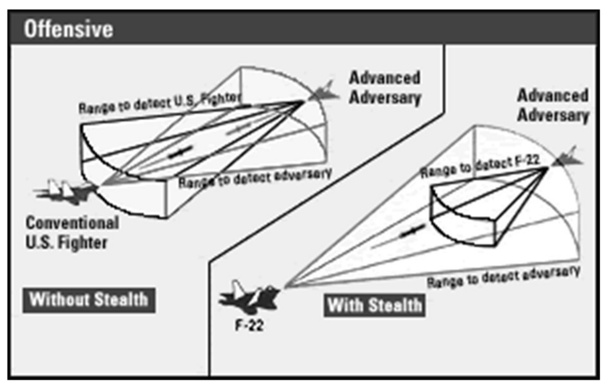
Know Your Equipment and Infrastructure

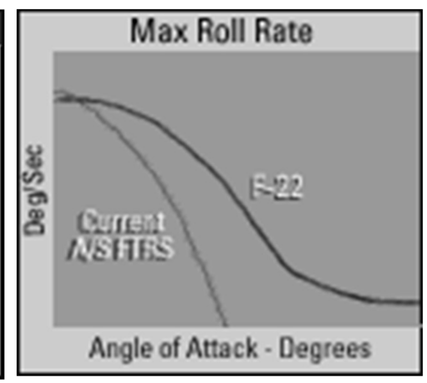
Know the performance envelope of all your equipment (routers, switches, security devices, servers, etc.). You need to know what your equipment is *really* capable of doing.

Know the capabilities of your network. If possible, test it. Surprises are not amusing during a security incident.

Understand PPS vs. BPS, and how enabling various features impacts performance.







Are You Pushing the Envelope? Get Real!

Operator, “I tried to push my aircraft to 20,000 feet and it stalled.”

Vendor, “But the aircraft was only designed for a 15,000 foot ceiling.”

Operator, “I need it to go to 20,000 feet, so you should make that happen.”

Vendor, “But that is not going to happen; 15,000 feet is its ceiling. You knew that when you bought it.”

Operator, “Your equipment sucks if you cannot exceed you design specs.”

Detection, Classification, and Traceback

All of this assumes you can detect and understand the attack

Detection — understanding that something potentially bad is happening

Classification — understanding what's happening, how much of it is happening, and how serious it is

Traceback — understanding where it's happening on the network; where is the attack traffic ingressing & egressing the network?

Reacting to attacks depends, in a lot of ways, on how you detect the attacks

Time of reaction is often a critical factor

- Once stateful devices fail, the restoration path is usually a hard reboot

Reaction

Many varying reaction mechanisms

No one tool or technique is applicable in all circumstances

- Think ‘toolkit’
- Automate where possible
- Don’t forget about the operational costs

It is critical to identify and classify an attack so you can choose the most appropriate mitigation tool

- Every problem does not call for a hammer solution, simplicity is key
- Some ‘solutions’ actually make the problem worse!

Postmortem - Analyzing What Just Happened

What Can Be Done to Build Resistance to the Attack Happening Again?

The step everyone forgets, or doesn’t make time to conduct

What can you do to make it faster, easier, less painful in the future?

Complete the loop!

Resiliency by Design

Multilayer DDoS Mitigation

Cloud Mitigation:

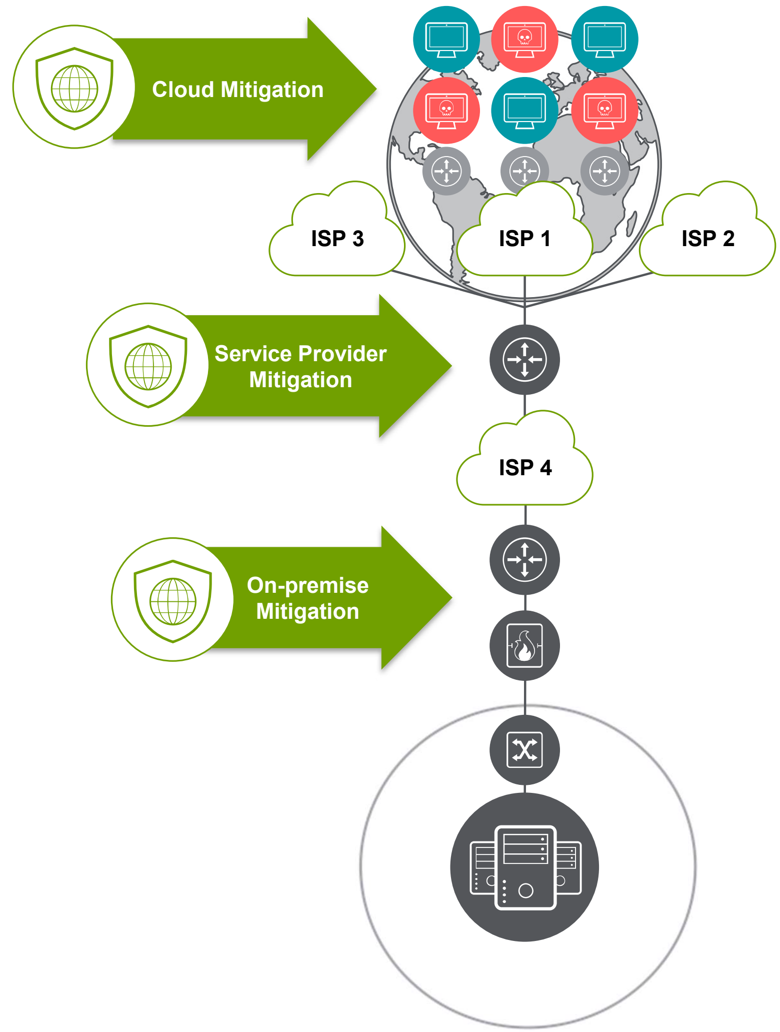
Carrier agnostic, works across multi-provider environments

Service Provider Mitigation:

Upstream transit providers

On-premise Mitigation

Can be standalone, or in conjunction with cloud or service provider upstream mitigation



Network Availability: Protect The Infrastructure

Security is the heart of internetworking's future; we have moved from an Internet of implicit trust to an Internet of pervasive distrust

No packet can be trusted; all packets must earn that trust through a network device's ability to inspect and enforce policy

Protecting the infrastructure is the most fundamental security requirement

Infrastructure protection should be included in all high availability designs

A secure infrastructure forms the foundation for continuous service delivery

Network Infrastructure Security Best Current Practices (BCPs)

Many organizations publish guides to best practices around router/switch security

These include:

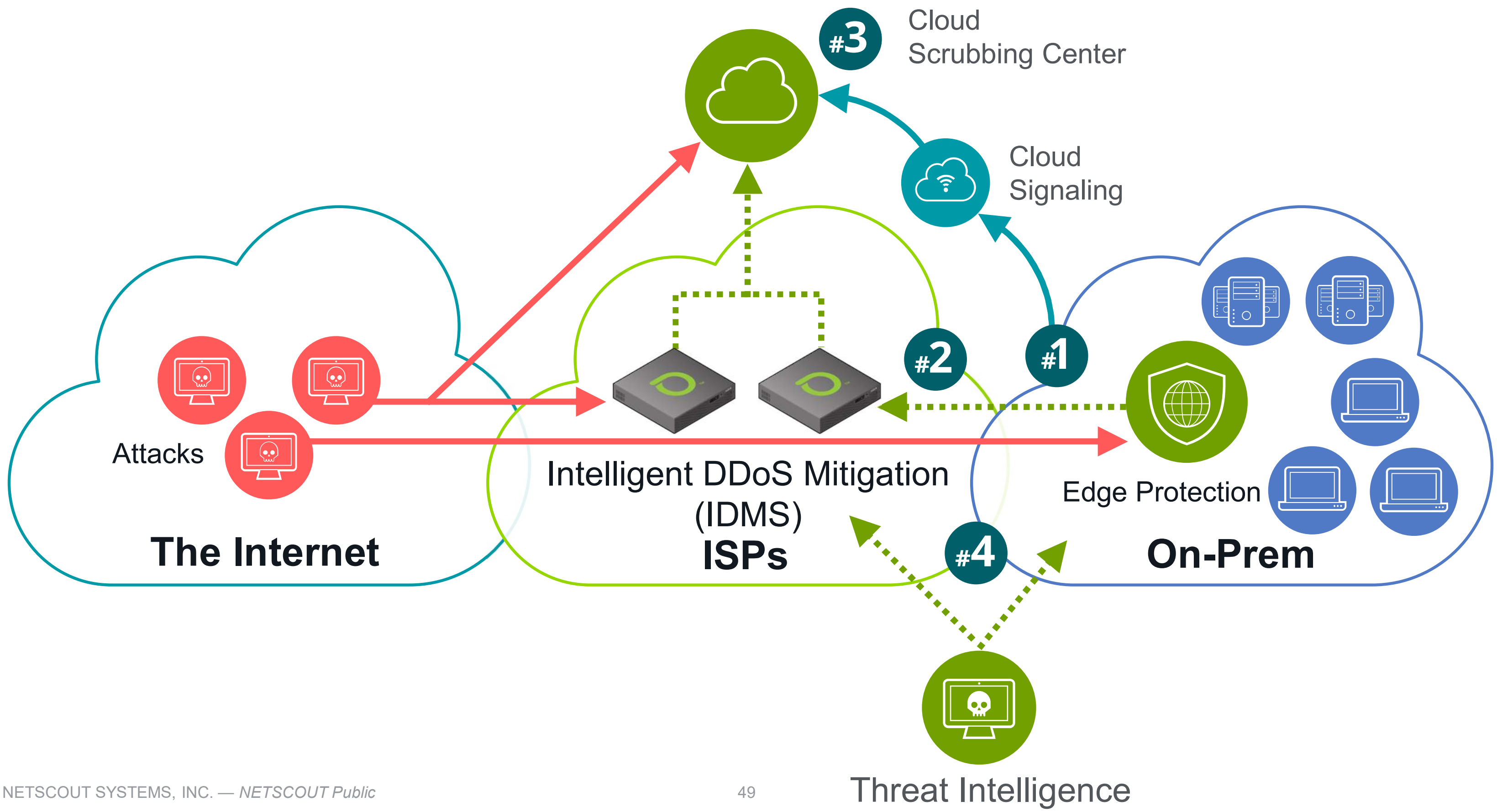
- https://www.manrs.org/
- http://www.first.org/resources/guides/
- http://www.sans.org/resources/policies/
- http://www.ietf.org/html.charters/opsec-charter.html

These guides do a good job of documenting best practices, especially in what we are referring to as traditional methods for router hardening

Network self-protection mechanisms must be implemented in order to withstand DDoS attacks.

Multi-Layer DDoS Protection

Defense is like an onion…



The Importance Of Detection And Classification

In order to operate and ensure availability of the network, we must have the ability to detect undesirable network traffic and to classify it appropriately

We cannot contain/mitigate what we cannot detect!

- All the mitigation technology in the world isn't helpful if we've no visibility into threats to network availability

Detection and classification must be part of the network architecture and operational security practice

- Otherwise, we're left scrambling to figure out what's happening—or even if anything is happening at all—instead of what we're going to do about it

In order to detect the abnormal, and possibly malicious, we have to know what's normal—we must establish a baseline of network activity, traffic patterns, etc.

Classification is key—it provides the context for further action

OPEX and CAPEX expended to gain network visibility pays big dividends - it is a force multiplier which allows overworked staff to plan, troubleshoot, and secure the network, and the hosts and networks which depend on the network

Use flow telemetry (NetFlow, etc.) to detect/classify/traceback DDoS at scale across the network; use packet capture to see specifics, when necessary; use DNS to understand network behaviors, at scale.

What Is Meant by ‘Telemetry’?

Te·lem·e·try—n.

The science and technology of automatic measurement and transmission of data by wire, radio, or other means from remote sources, as from space vehicles, to receiving stations for recording and analysis.

Source *The American Heritage® Dictionary of the English Language, Fourth Edition*

Network Telemetry

Network telemetry offers extensive and useful detection capabilities

This telemetry is often coupled with dedicated analysis systems to collect, trend, and correlate observed activity

There are several forms of telemetry available from routers, switches, and other network devices — flow telemetry (NetFlow, et. al.) & packet capture chief among them.

DNS is a rich source of behavioral telemetry, as well.

There are a number of open source and commercial tools available which greatly enhance the utility of network telemetry

Getting started with network telemetry is both inexpensive and relatively easy

Network Telemetry — Time Synchronization

When dealing with network telemetry, it is important that dates and times are both accurate and synchronized

Enabling Network Time Protocol (NTP) is the common method of time synchronization — it is supported by routers, switches, firewalls, hosts, and other network-attached devices

Without time synchronization, it's very difficult to correlate different sources of telemetry

More information on NTP can be found at http://www.ntp.org

Network Telemetry — OOB Management

In-Band access to network infrastructure, hosts, etc., works very well — until there' s a problem on
the network

In order to maximize reachability of and control over the network even during disruptive events, it is necessary to build an isolated Out-of-Band (OOB) management network (sometimes called a Data Communications Network, or DCN)

Many devices such as routers and switches have serial console ports; others have Ethernet management interfaces

Transmitting network telemetry over the OOB network minimizes the chance for disruption of the very information which gives us visibility into the network

Network Telemetry — Antispoofing/Source Address Validation (SAV)

There are many mechanisms available in modern network infrastructure devices to disallow spoofed traffic from transiting the network - Unicast Reverse Path Forward (uRPF), DHCP Snooping with IP Source Guard, Cable IP Source Verify, etc.

Spoofed traffic is by definition invalid traffic - there is no reason to allow spoofed traffic to ingress and transit your network. Disallowing spoofed traffic is a basic step in improving network resiliency

By eliminating spoofed traffic, we remove clutter from the ‘data horizon’ generated by analyzing network telemetry

This greatly reduces the traceback problem - with antispooing measures in place, we know that purported source IPs originating from network edges under our control are valid, and we eliminate falsely-sourced traffic from the peering edge

DDoS Mitigation Techniques

DDoS Reaction/Mitigation Mechanisms

ACLs
- Drops traffic with layer-3/-4 granularity
- Can be difficult to deploy manually during an attack (see flowspec below)

Blackhole (null-routing using BGP)
- Drops traffic with layer-3 granularity on routers, layer-3 switches
- Uses a BGP announcement with a new BGP nex-thop to redirect the traffic
- D/RTBH drops traffic to destination (completing the attack!), S/RTBH can drop based on source IPs

Flow Specification (flowspec)
- Uses a multi-protocol BGP (mBGP) announcement to push ACLs to flowspec-enabled routers
- Drop or rate-limit traffic that matches a layer-3/-4 flowspec filter (an ACL)

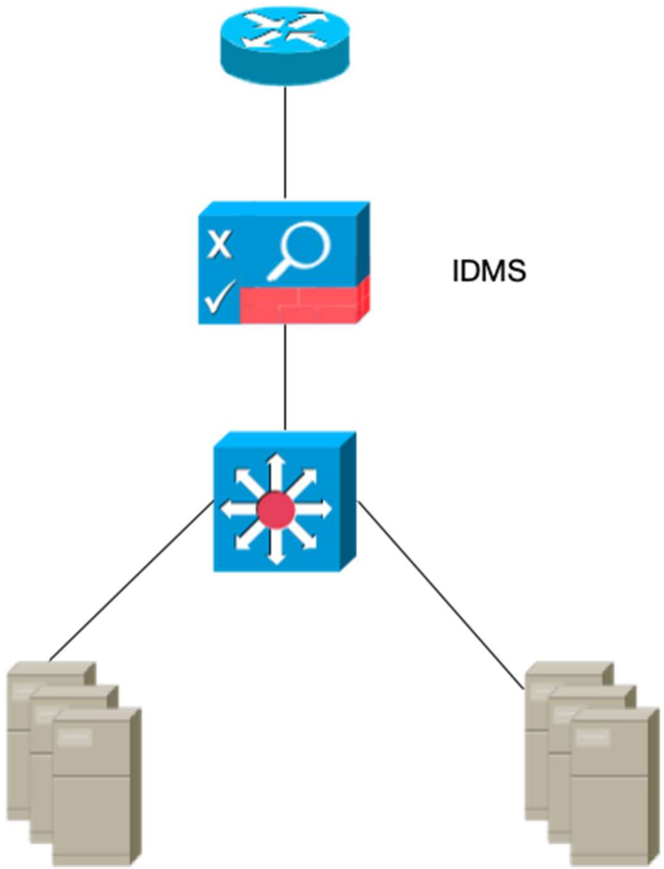
Intelligent DDoS Mitigation System (IDMS)
- Diverts traffic destined for the target into a mitigation center via BGP announcements
- Attack traffic dropped, legitimate traffic re-injected via GRE, VRF, direct mitigation peering
- Can mitigate layer-3 – layer-7 attacks
- Provides detailed mitigation feedback & statistics
- Horizontally scalable in mitigation clusters, multiple BGP-anycasted clusters

Mitigation Mechanism: IDMS

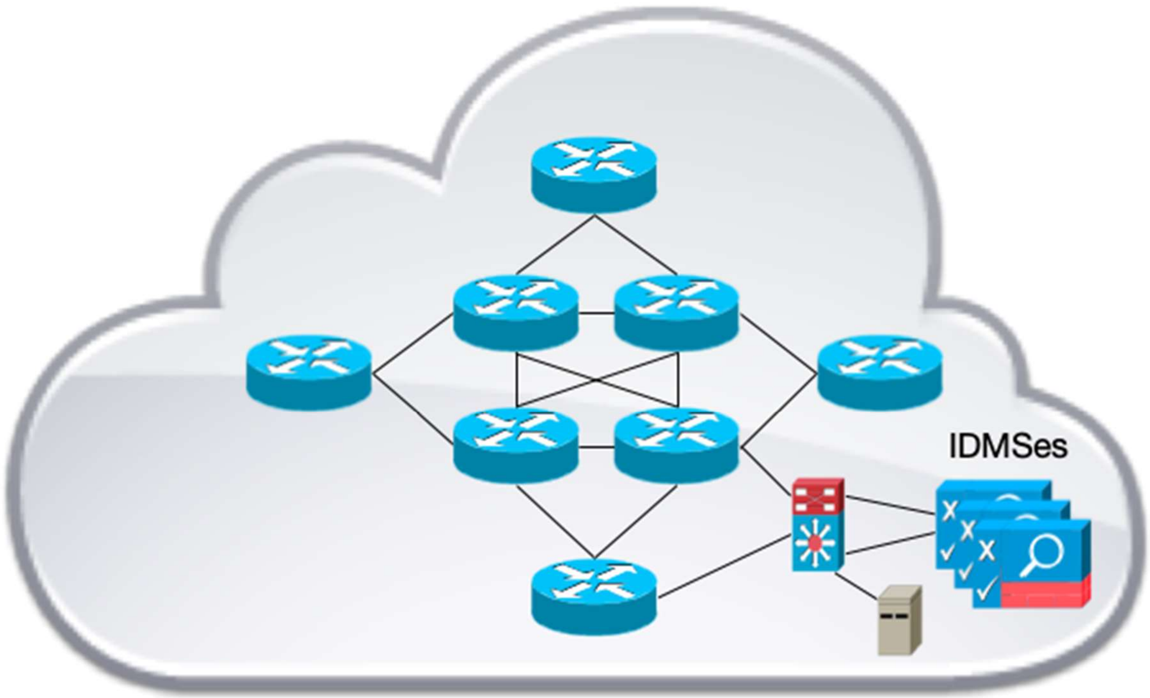
Ease of Implementation	Complex
Ease of Usage	Easy
Impact on Infrastructure	Medium

- Intelligent DDoS Mitigation System
- Surgically drop traffic
  - Use various countermeasures to target and remove as much of the attack traffic as possible
  - Allow the network to continue operating
- Deployment methods
  - Inline (mainly on-prem)
  - On-demand BGP diversion and re-injection
  - ‘Nailed up’ BGP diversion and re-injection
  - DNS diversion (often used whilst provisioning BGP)
- Apply various countermeasures (defense mechanisms) to target and remove attack traffic to allow servers/services/applications to continue operating, even in the face of attack
  - Different countermeasures are designed to protect different types of services, mitigate different types of attacks
  - IDMS countermeasures provide defense in depth mitigation
  - The main organizing principle of countermeasure provisioning is “What is being protected?”
  - Attack vector-specific countermeasures may also be employed during a mitigation

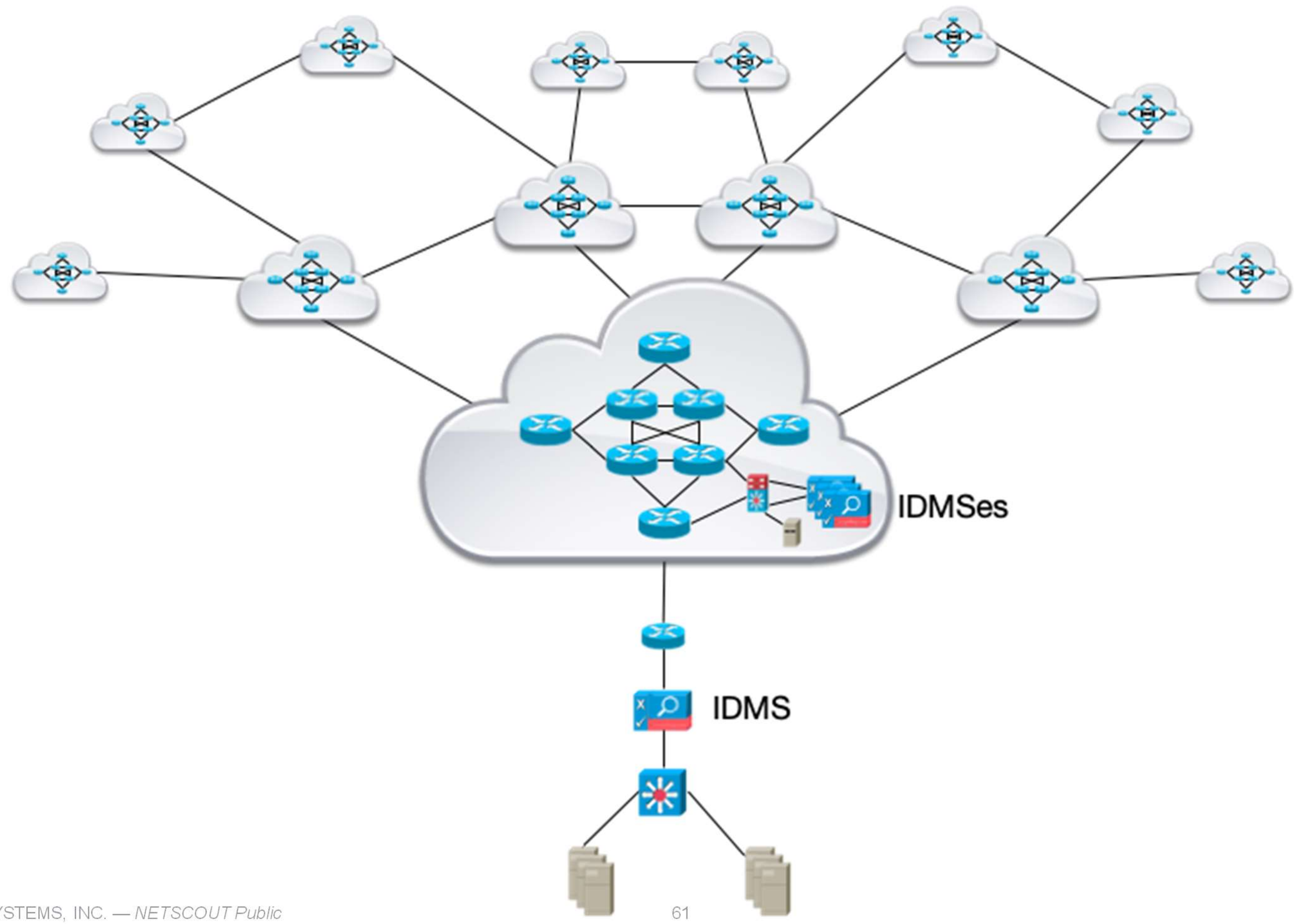
On-Premise IDMS Deployment



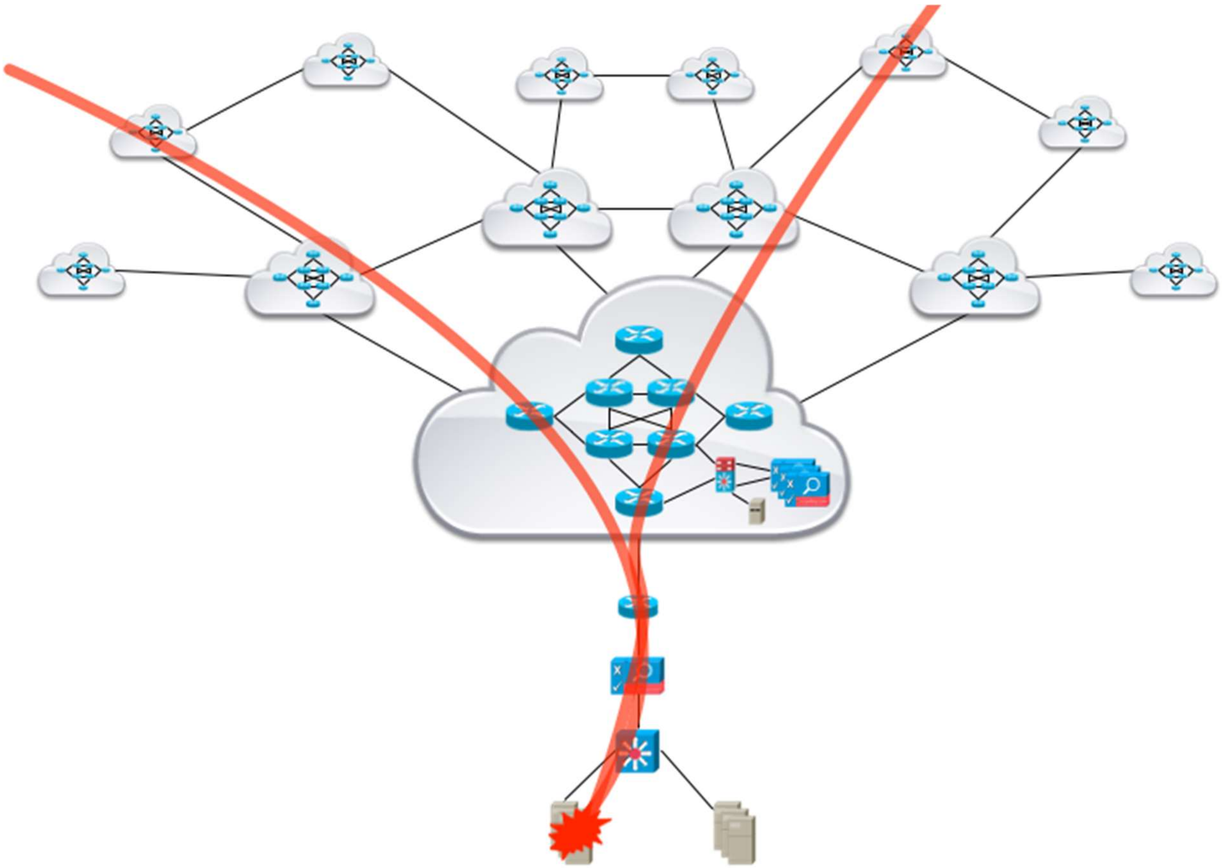
Upstream IDMS Deployment (Mitigation Center)



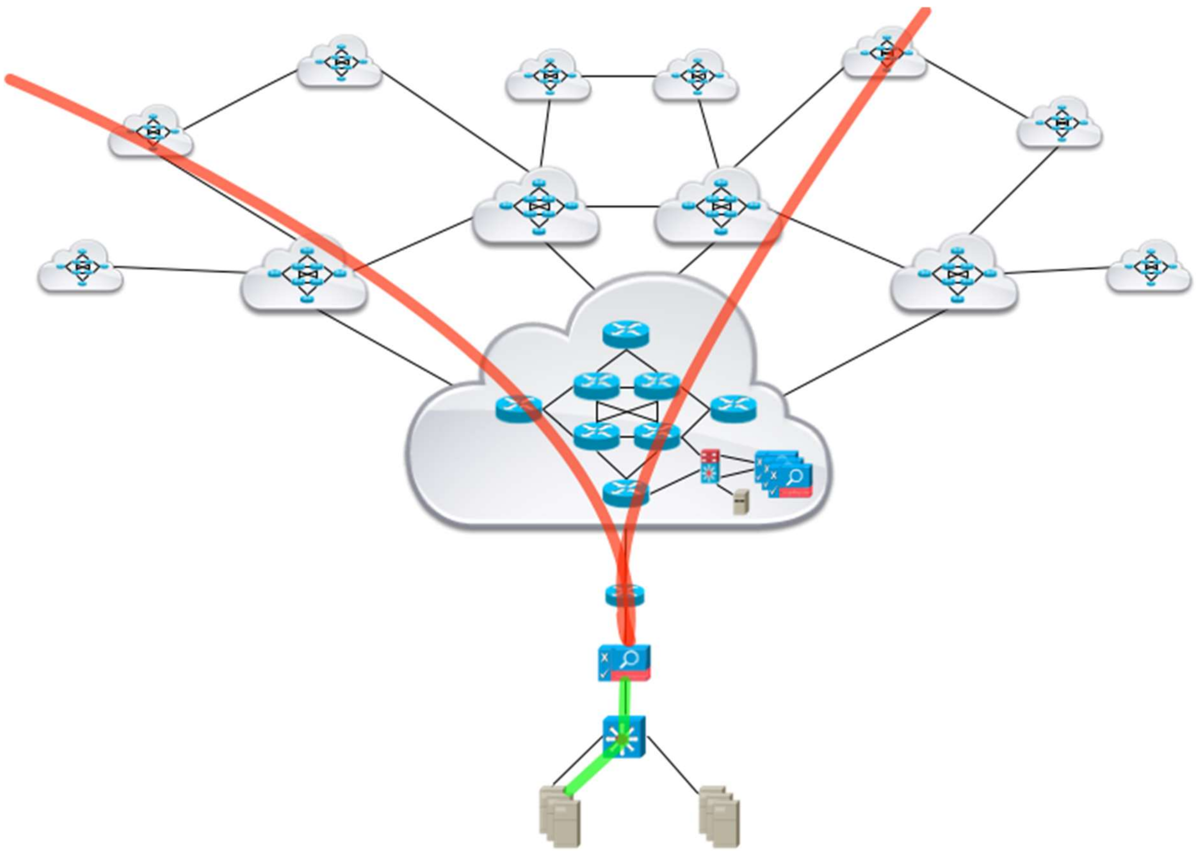
Hybrid IDMS Deployment



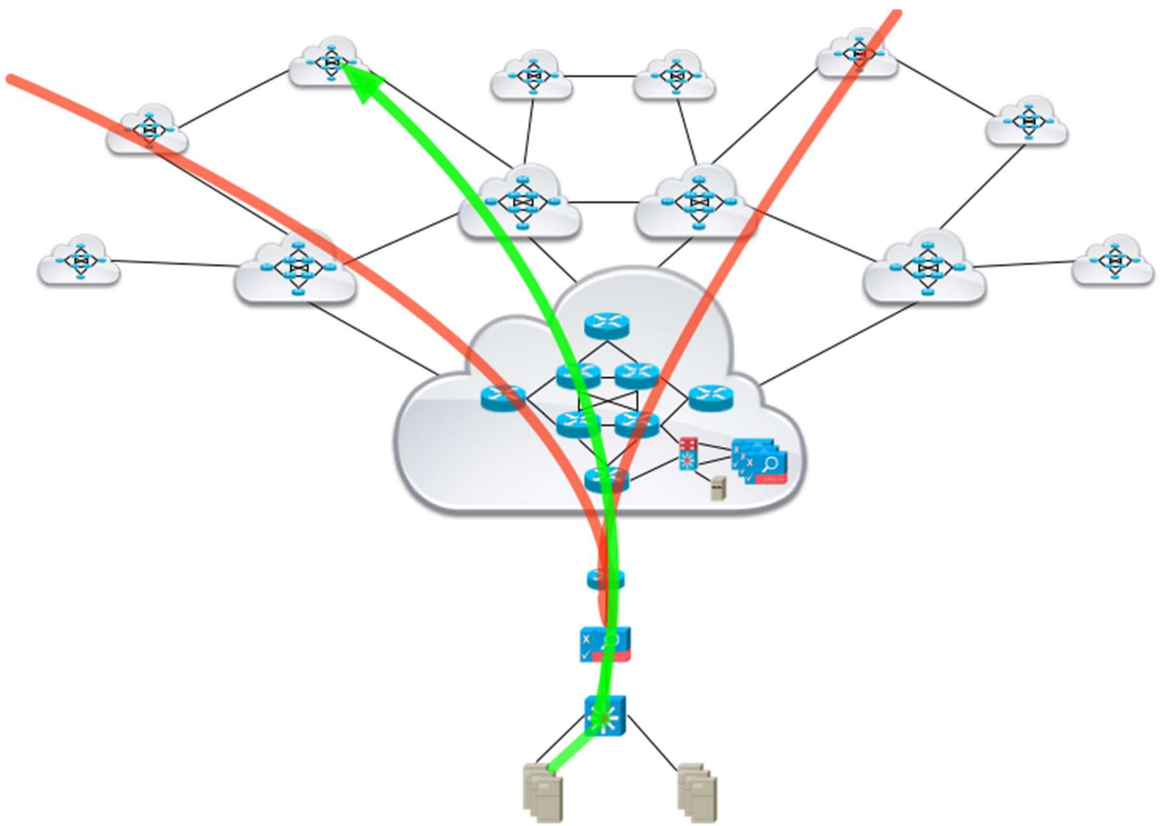
Initial DDoS Attack



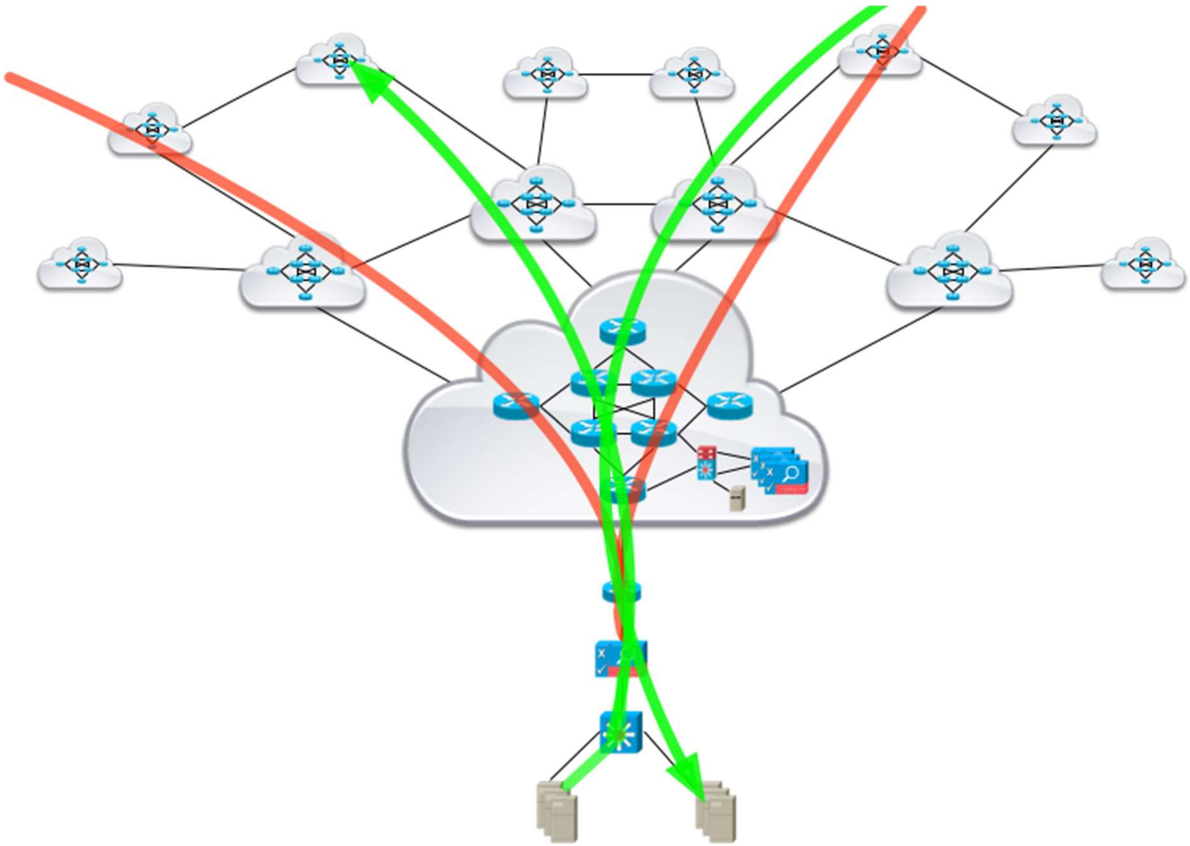
On-Premise IDMS Sucessfully Mitigates



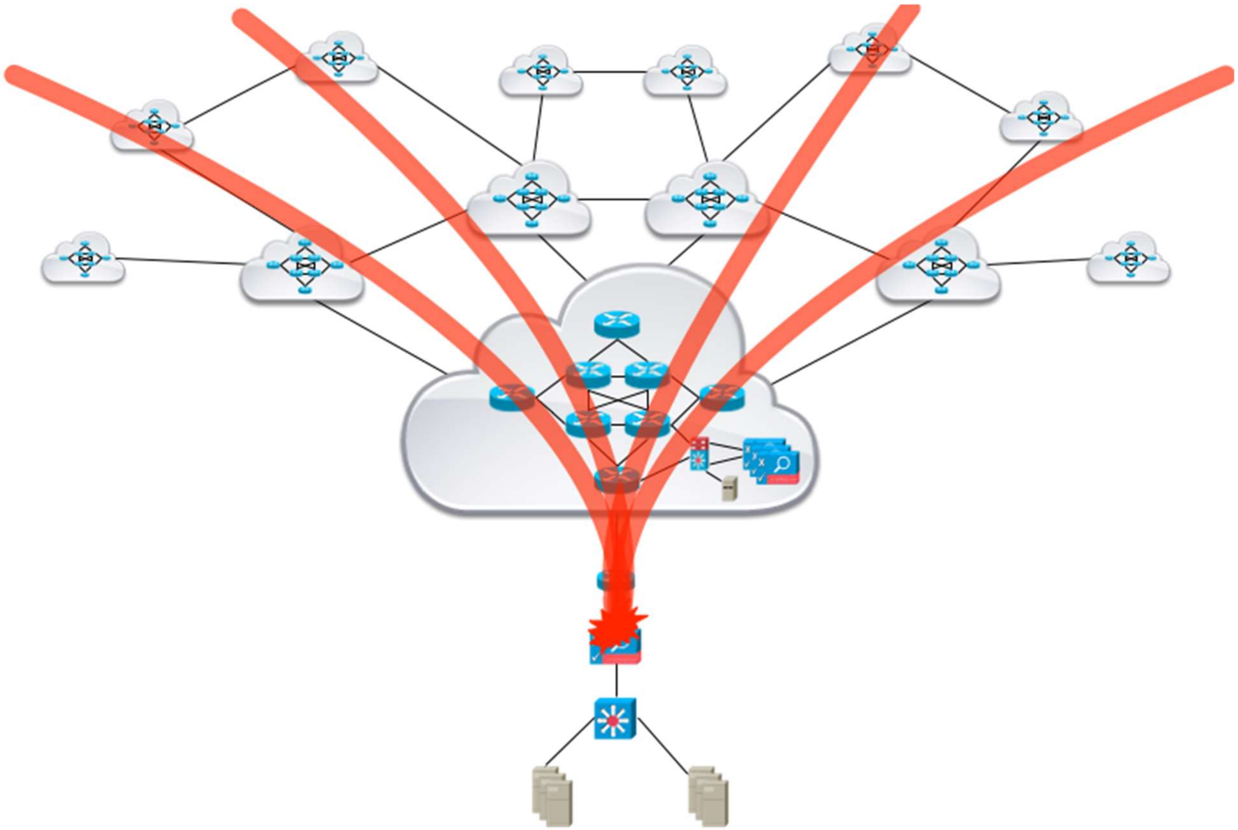
Outbound Server Responses to Legitimate Traffic Continue



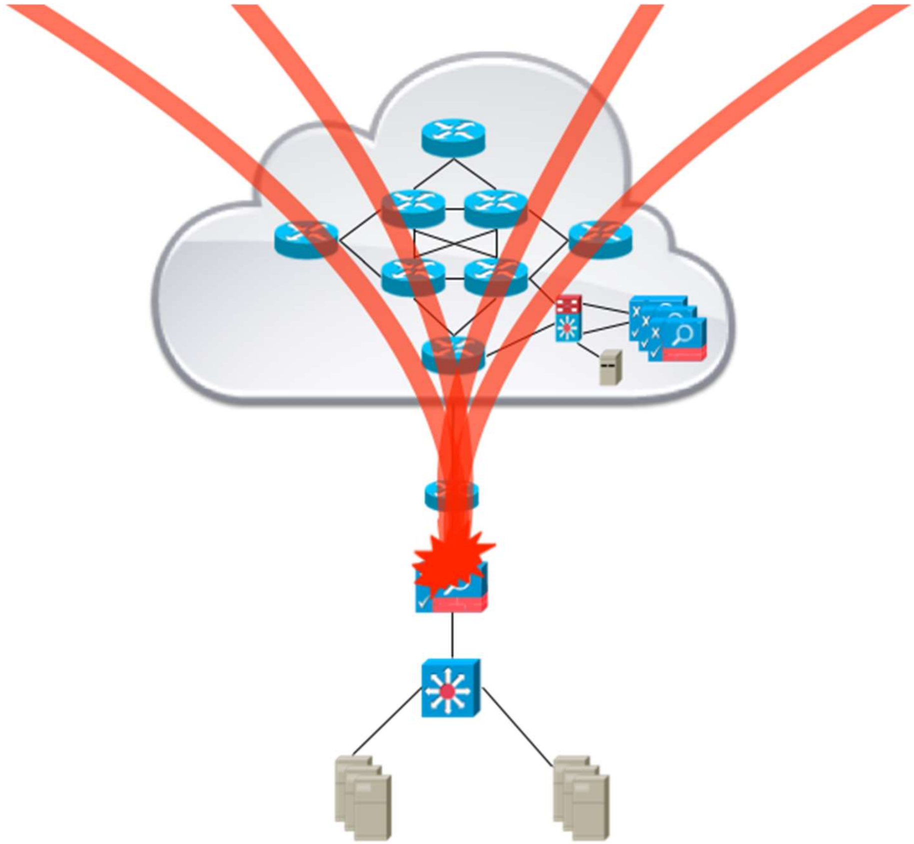
Traffic to Non-Targeted Servers Unimpeded



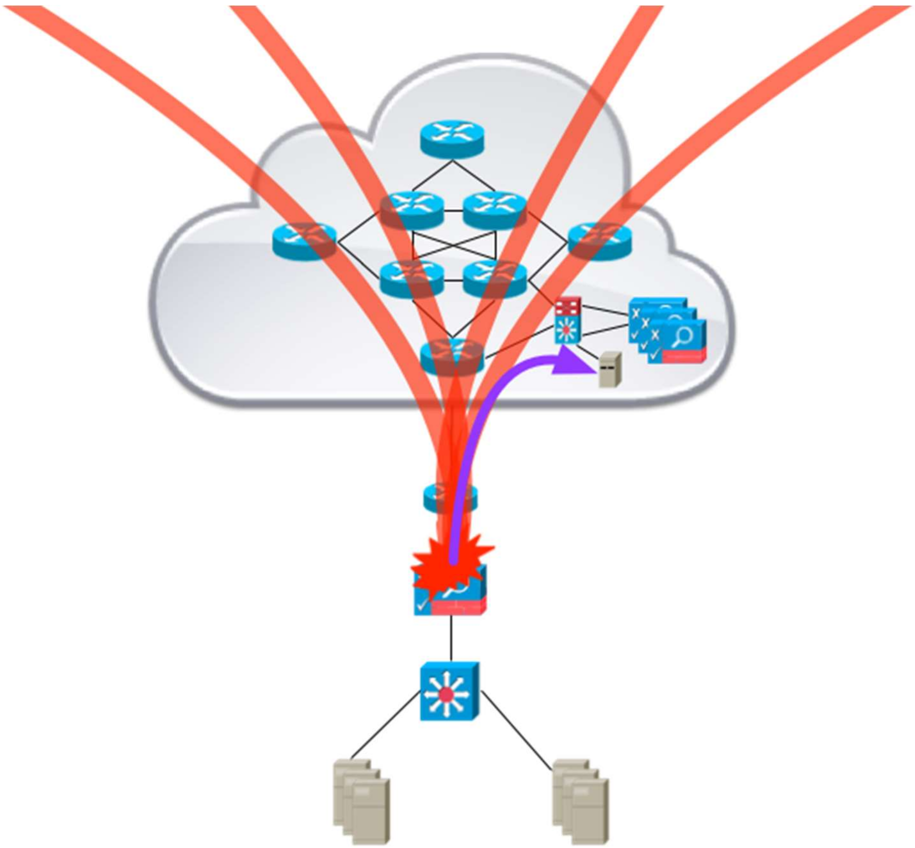
Attack Traffic Increases, On-Premise Mitigation Capacity Exceeded



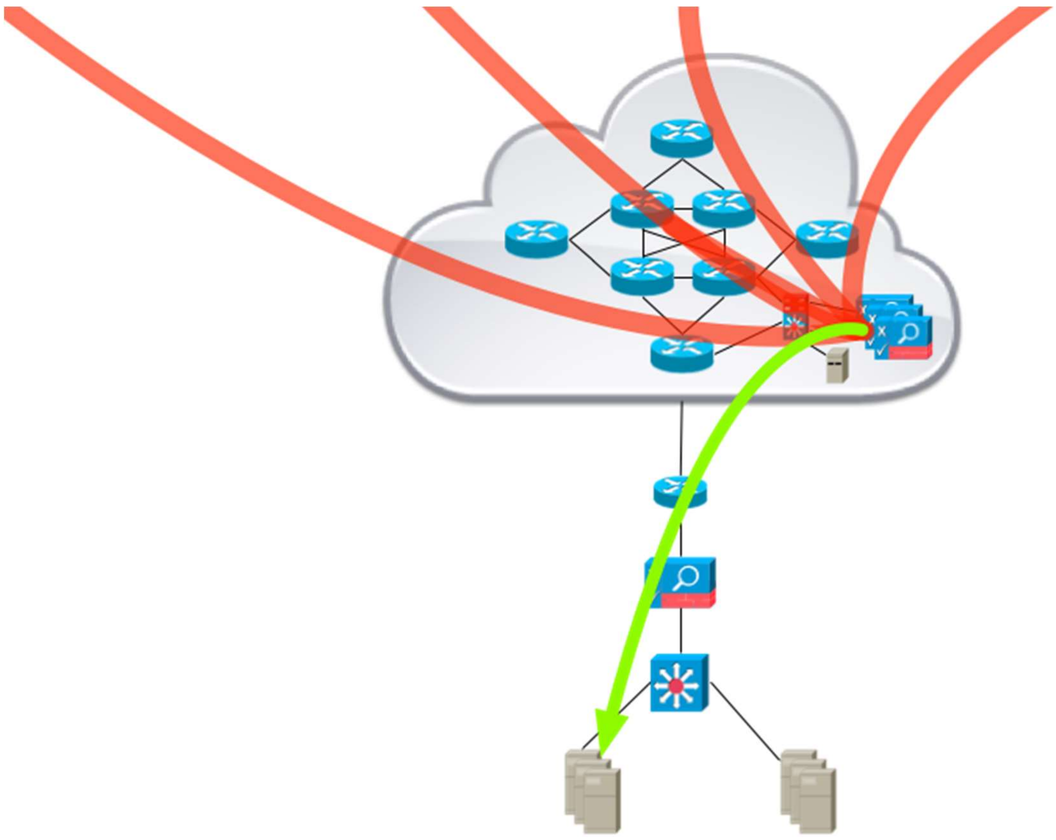
Attack Traffic Increases, On-Premise Mitigation Capacity Exceeded



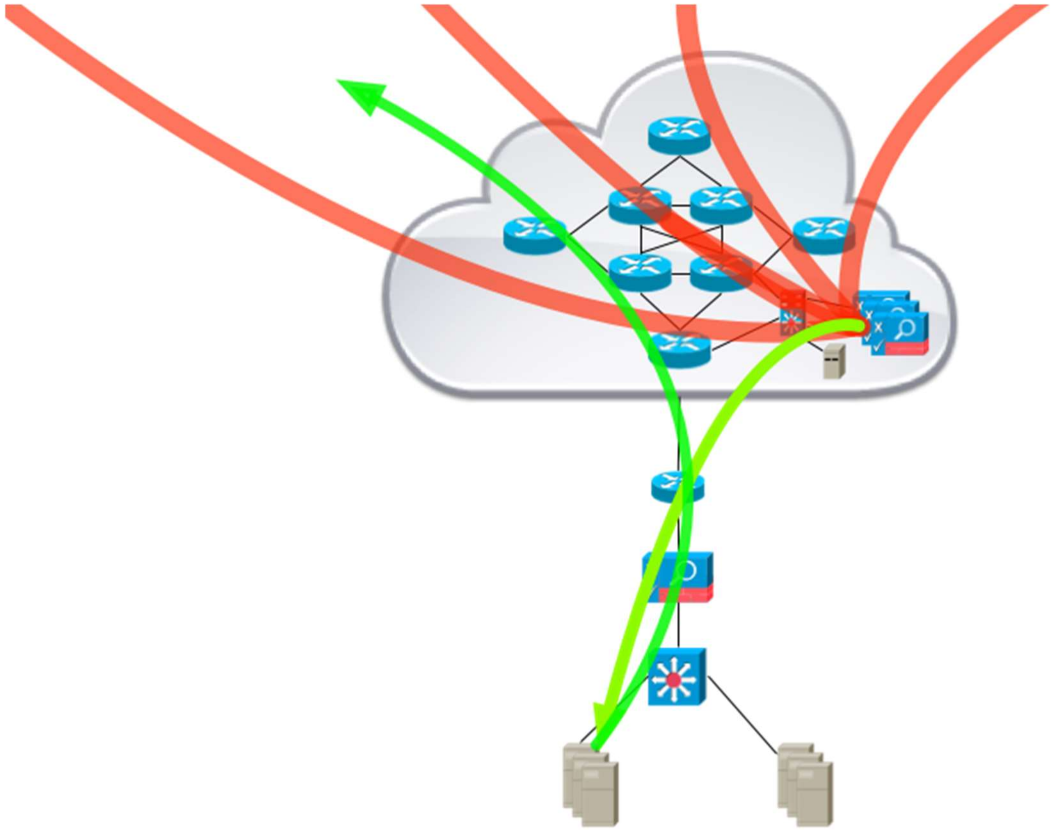
IDMS Signals Upstream Mitigation Provider



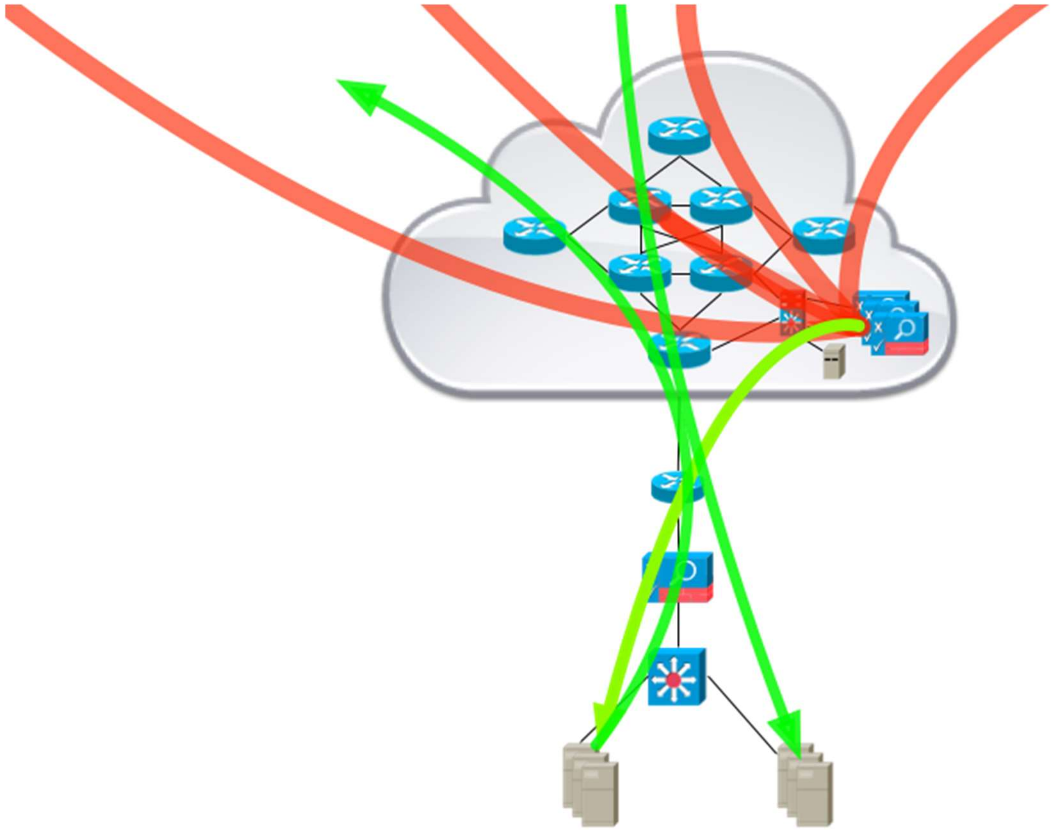
Upstream Mitigation Diverts Traffic to Targeted Servers, Drops Attack Traffic, Re-Injects Good Traffic



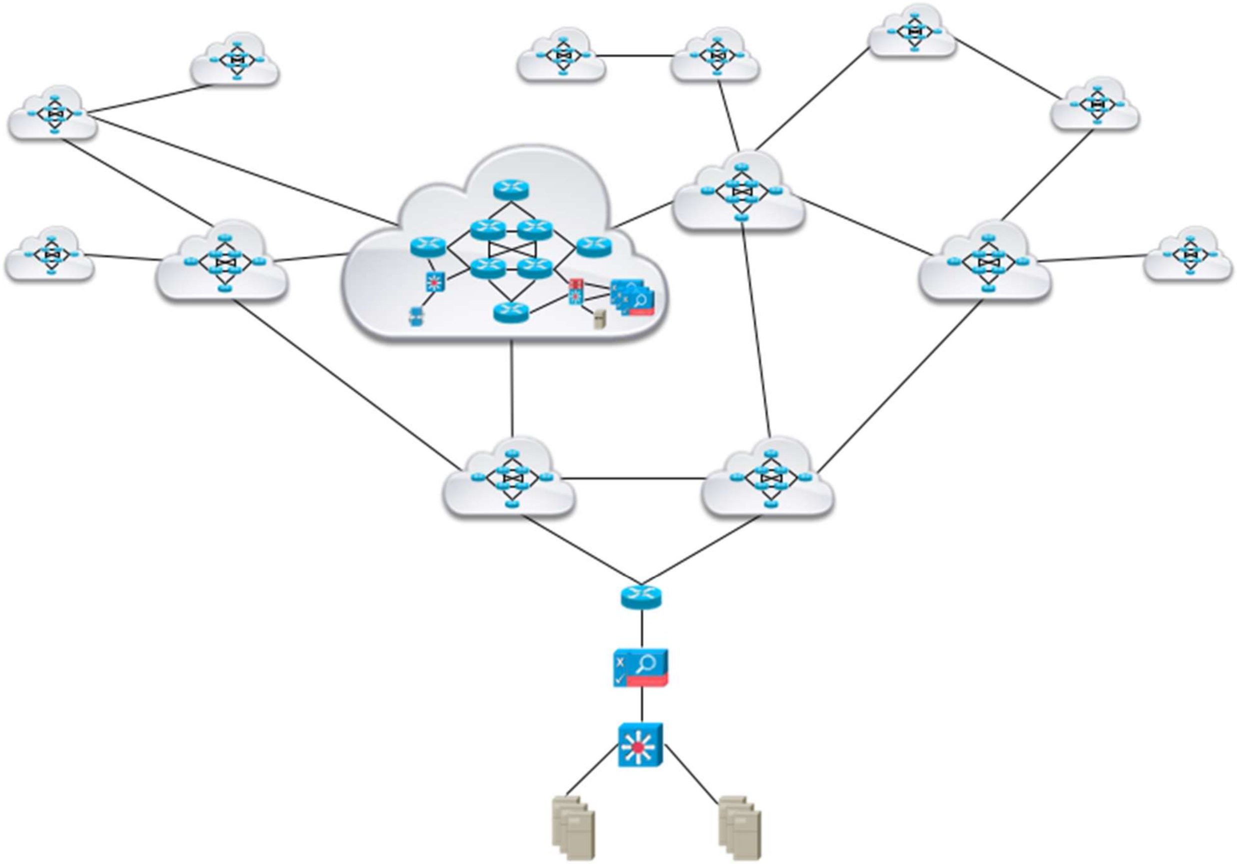
Server Responses to Legitimate Requests Follow ‘Natural’ BGP Routing



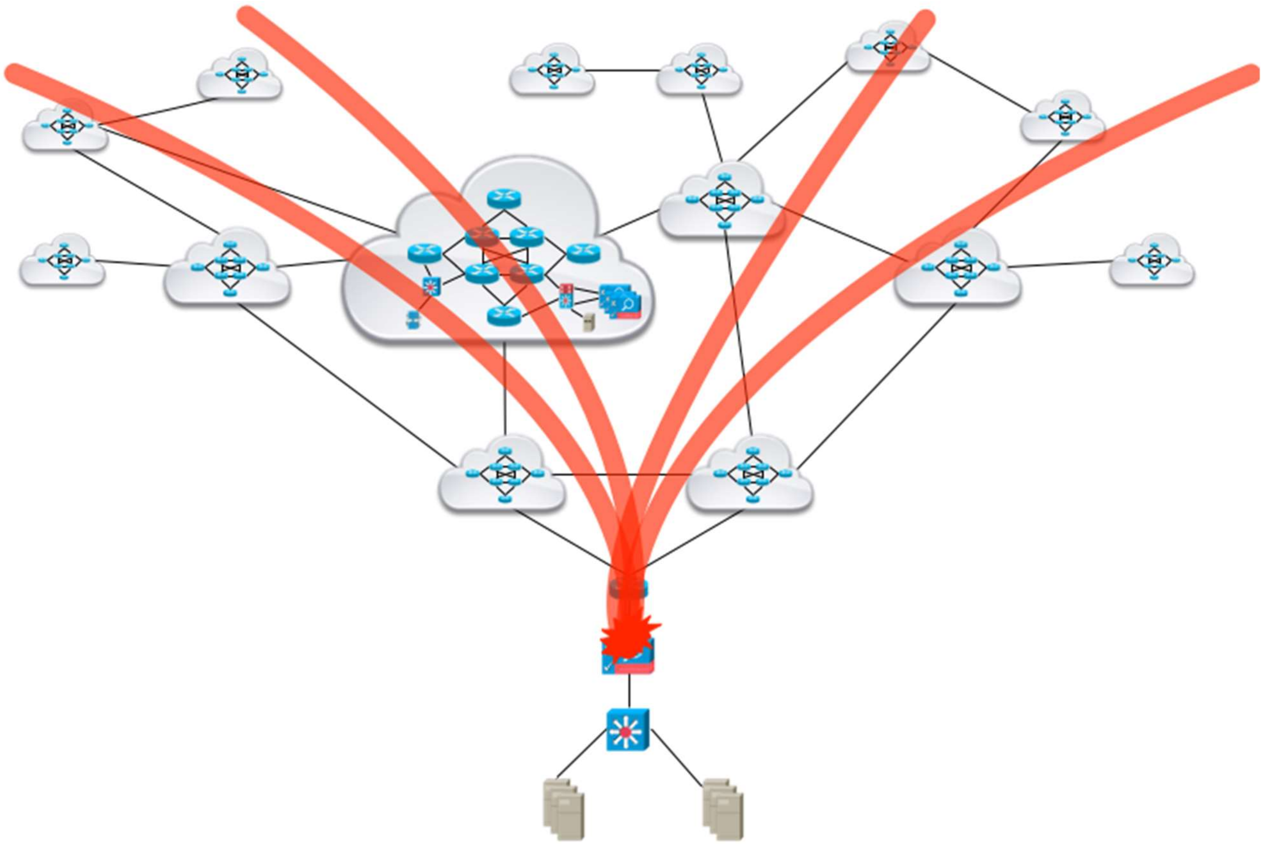
Traffic Directed Towards Non-Targeted Servers Not Diverted



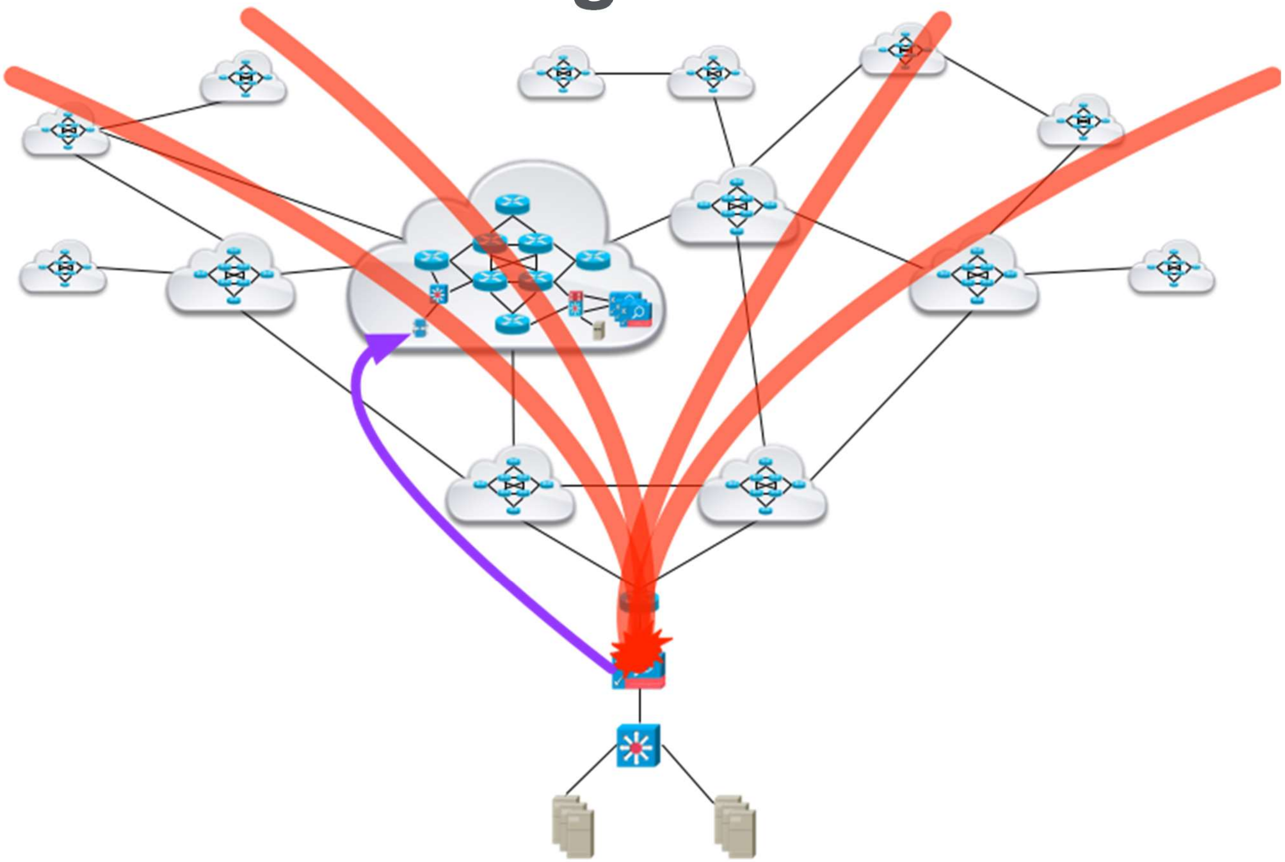
Hybrid Deployment Model with Cloud Mitigation Provider



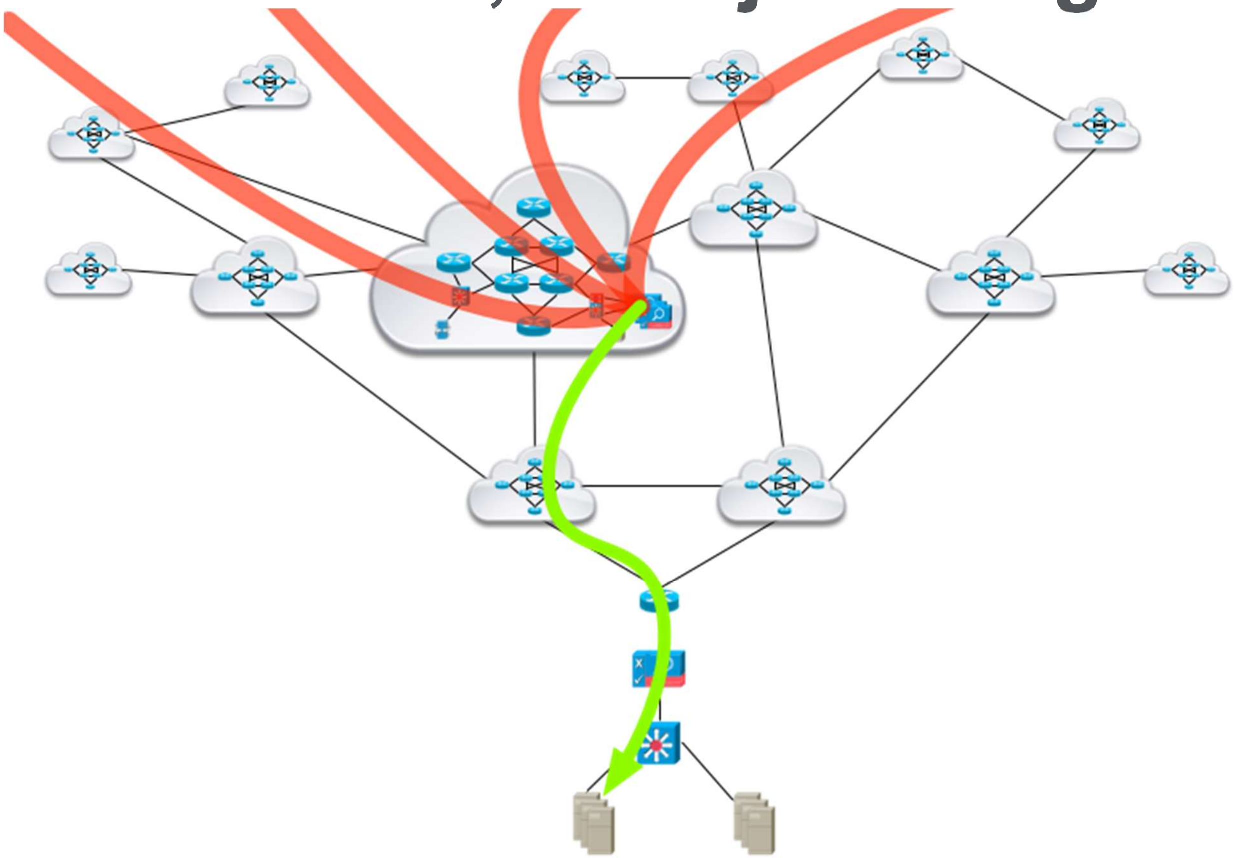
DDoS Attack Traffic Fills Transit Links of Targeted Network



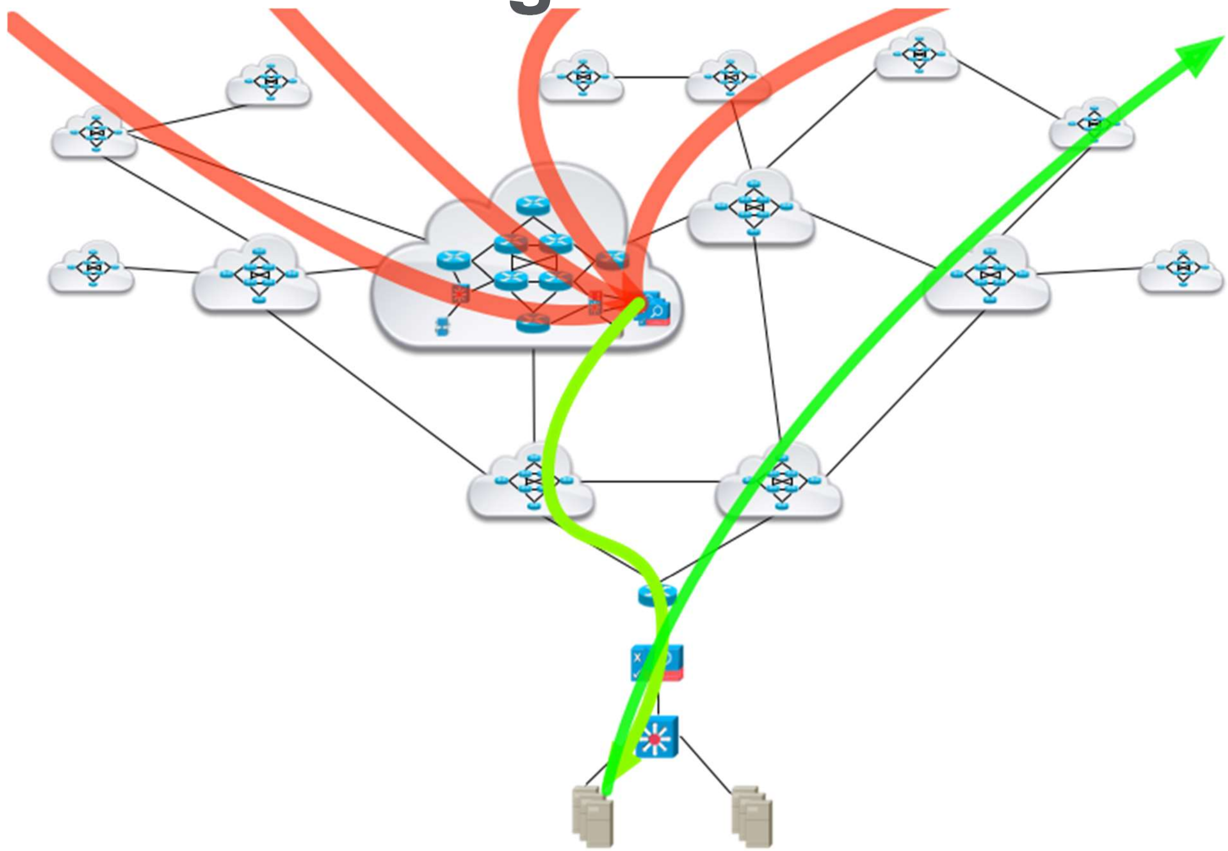
On-Premise IDMS Signals Cloud Mitigation Provider to Initiate Mitigation



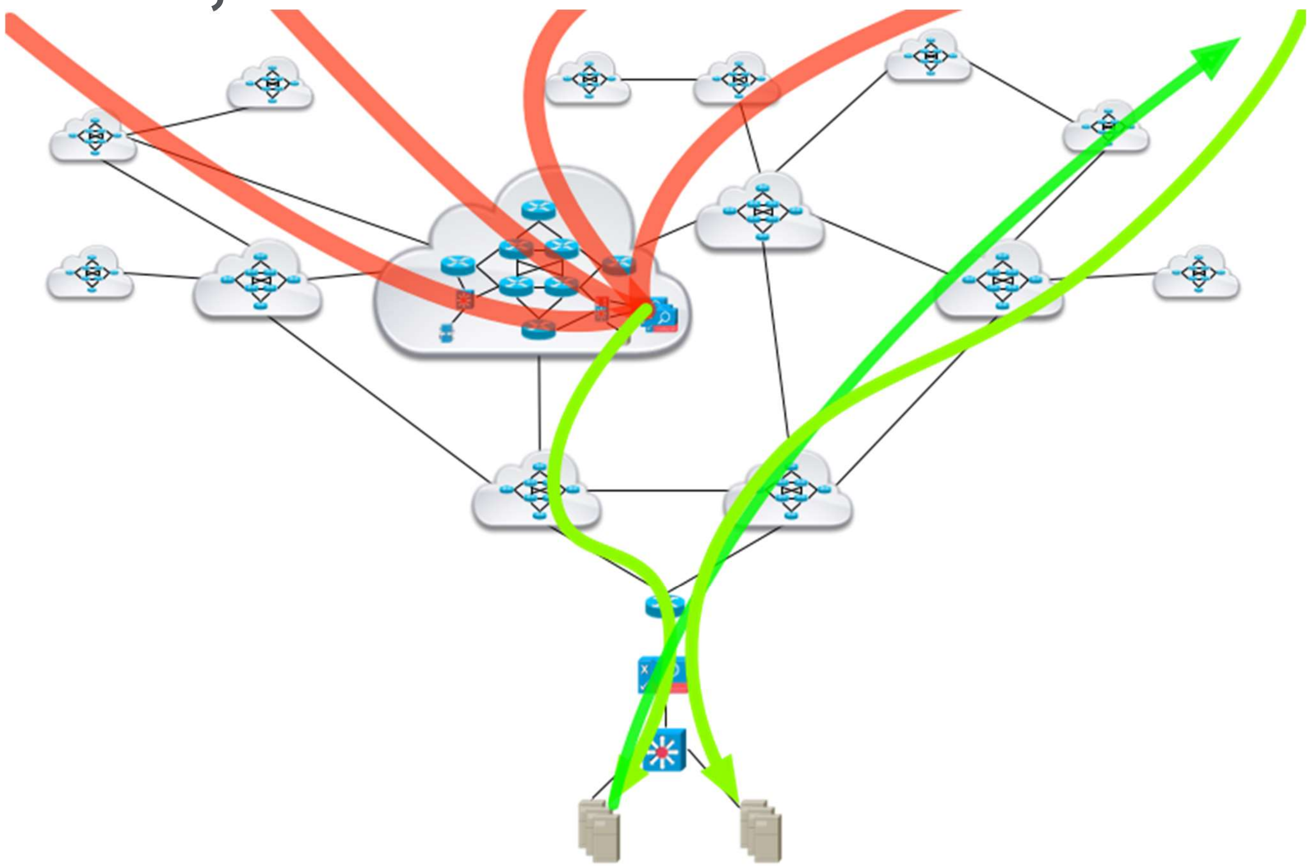
Cloud Mitigation Provider Initiates Diversion, Drops Attack Traffic, Re-injects Legitimate Traffic



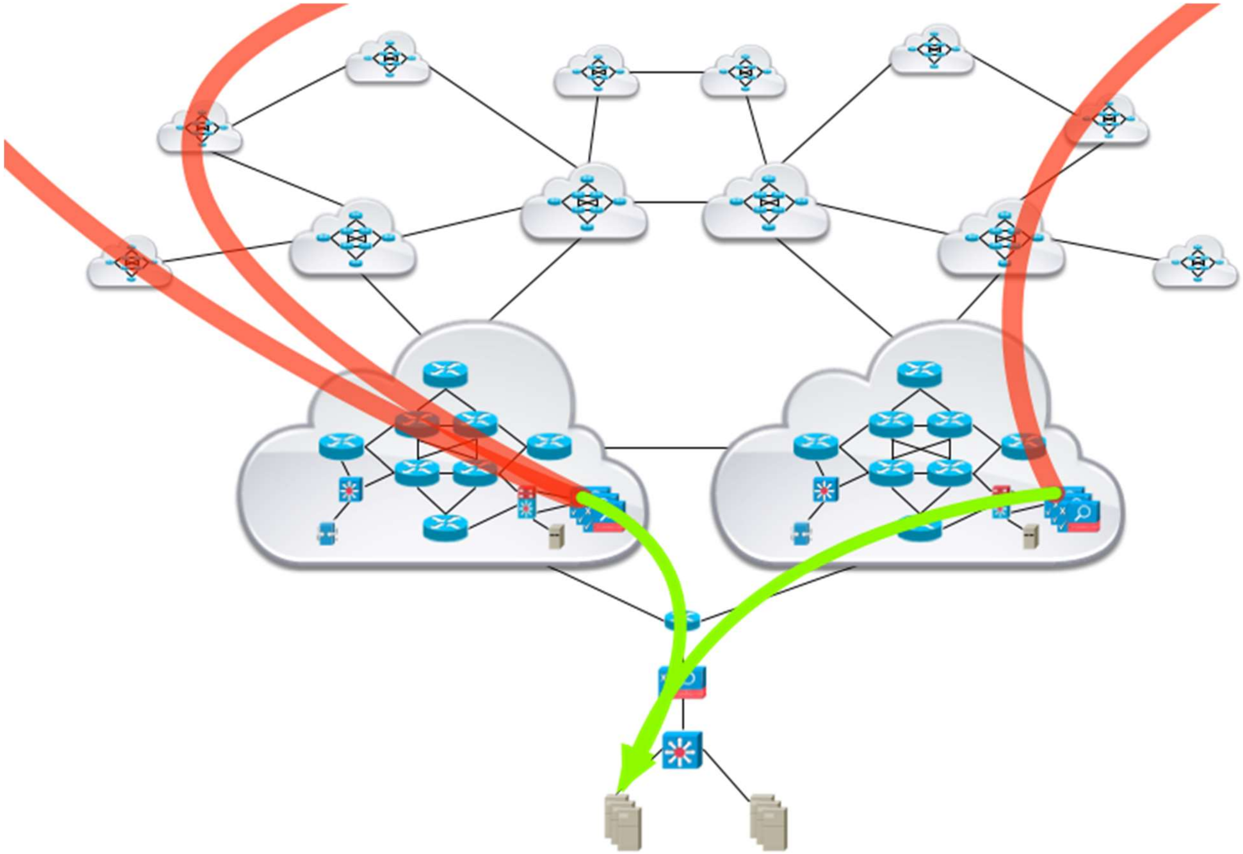
Server Responses to Legitimate Requests Follow 'Natural' BGP Routing



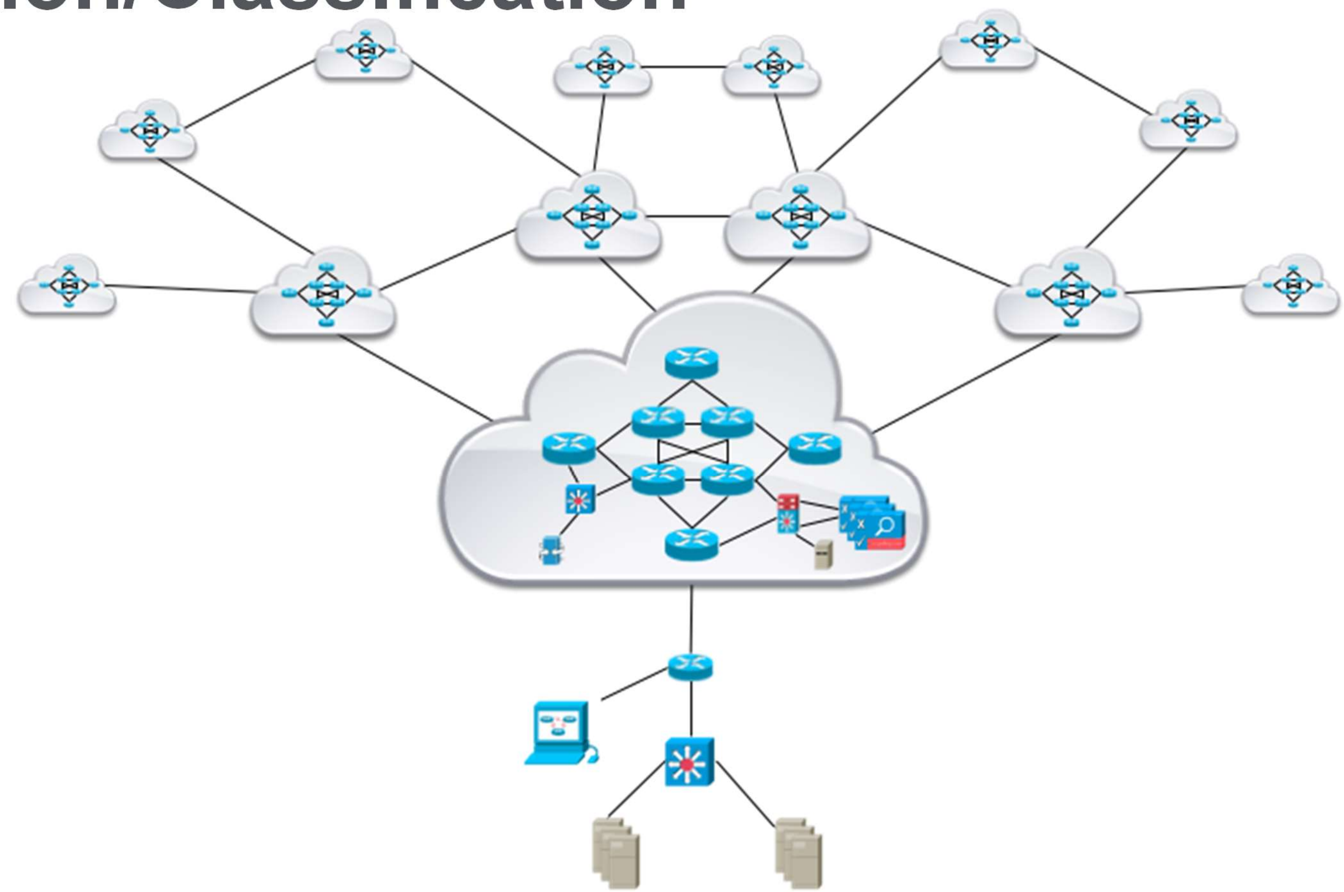
Inbound Traffic to Non-Targeted Server Farms Not Diverted, Follows 'Natural' BGP Routing



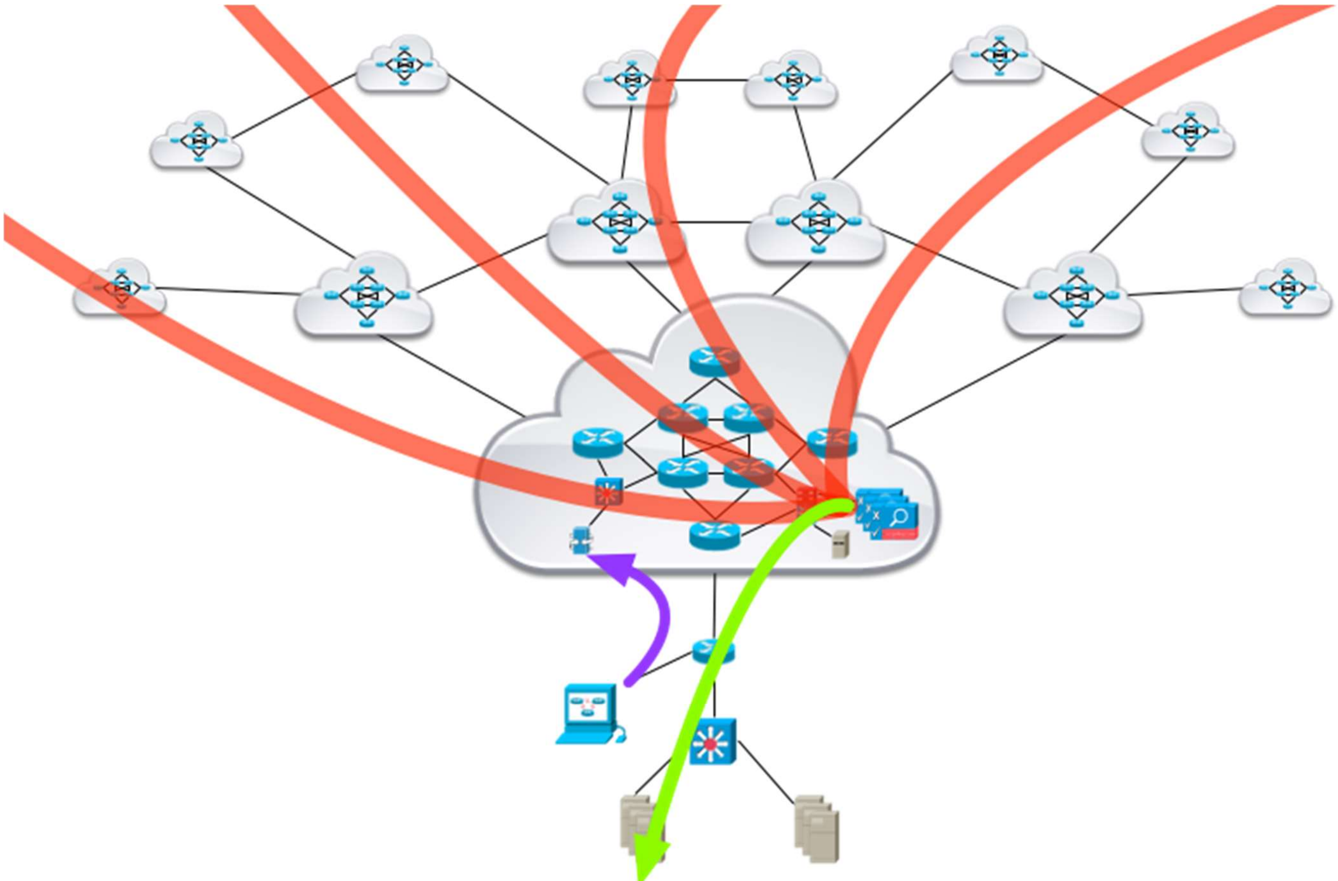
Hybrid Deployment with Multiple Upstream Transit Providers



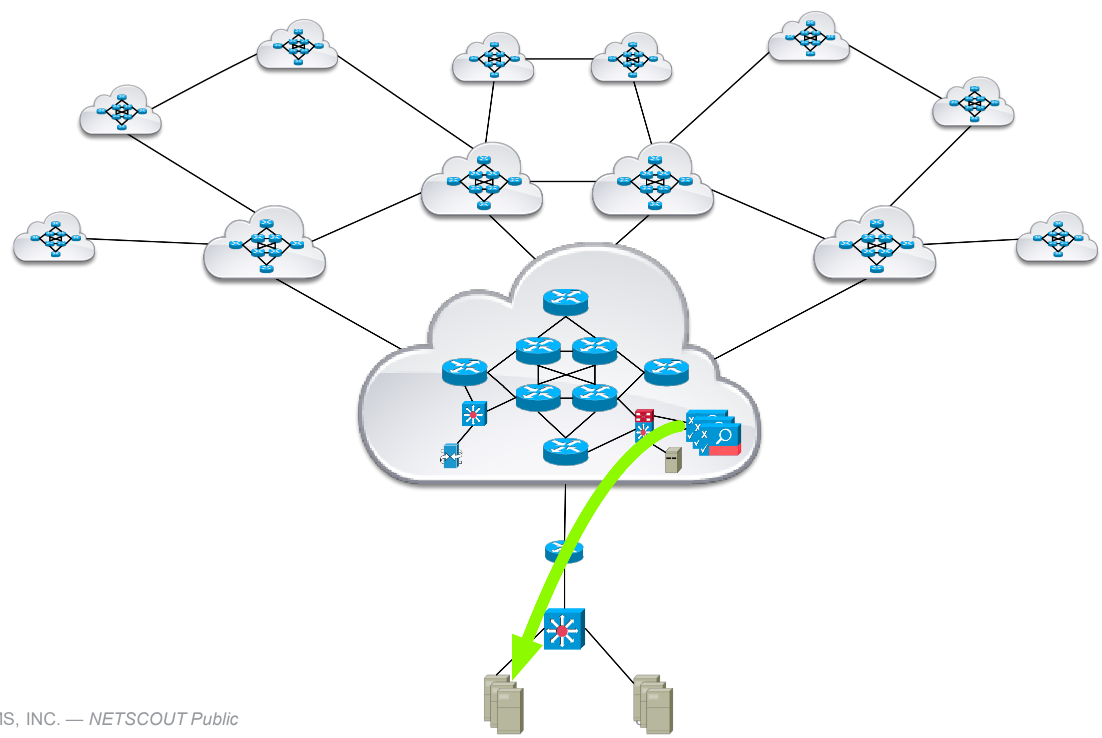
Upstream Deployment with On-Premise Detection/Classification



On-Premise Detection Triggers Upstream Mitigation



Upstream Detection/Classification/Traceback & Mitigation, No On-Premise Components



Conclusions & Next Steps

Common Perception of Internet Security Posture

Actual State of Internet Security Posture

Implications & Consequences

Network Operators

Their own first, best customers

Network operators must ensure that their own network infrastructure, DNS, servers/services/applications can maintain availability in the face of attack.

This is vital – end-user/-customer services depend upon the availability of the network operator's infrastructure and properties.

Ensure that all best current practices (BCPs) are implemented for network infrastructure, servers/services/applications, DNS, etc.

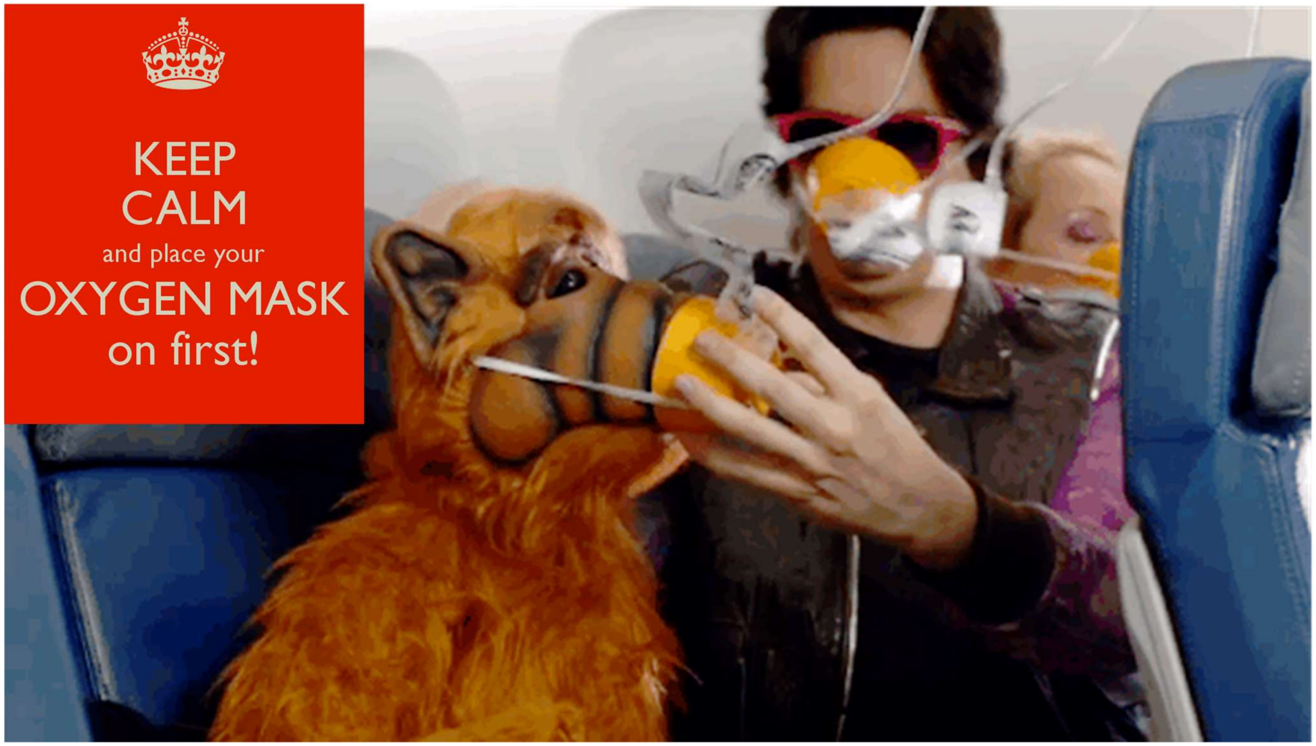
Ensure source-address validation (SAV) for ingress and egress traffic is performed at network edges in a situationally-appropriate manner.

Make use of flow telemetry, packet capture, & DNS for detection/classification/traceback.

Implement S/RTBH, flowspec, and IDMS in order to mitigate DDoS attacks at scale.

Participate in the global operational security community; build/maintain relationships with peers, customers, vendors.

You Must Defend Yourselves So That You Can Defend Your Users & Customers!



And, Most Importantly of All . . .

For More In-depth Coverage…

NETSCOUT 1H2020 Threat Intelligence Report:

https://www.netscout.com/threatreport

NETSCOUT ASERT blog:

https://www.netscout.com/asert

Roland Dobbins' public presentation folder:

https://app.box.com/s/4h2l6f4m8is6jnwk28cg

NETSCOUT

| REFERENCE GUIDE |

Effective DDoS Protection at Scale:

Best Practices and a Reference Architecture for Service Providers

Thank You!

Tim Nolen <tim.nolen@netscout.com>

Senior Solutions Architect, CISSP, GPEN

Roland Dobbins <roland.dobbins@netscout.com>

Principal Engineer, ASERT

netscout.com

Photo courtesy of NOAA ESRL

NETSCOUT®

Guardians of the Connected World