SEC-2103:

Taking Control of Your Network – Mitigating Attacks

Alvaro Retana (aretana@cisco.com)

Technical Leader, IP Routing Deployment and Architecture

Recuerde siempre:

- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.
- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.
- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.
- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

Agenda

- Introduction
- Preparation – Before an Attack
- Detecting and Classifying DoS Attacks
- Tracing DoS Attacks
- Reacting to DoS Attacks

    Reacting with the Data Plane

    Reacting with the Control Plane

    Using Discrete tools

Introduction

Reacting to Attacks

- 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!
- Choose your techniques wisely

All of this assumes you can Detect it

Cisco.com

- Reacting to attacks in a lot of ways depends on how you detect the attacks
- Time of reaction is often times a critical factor

  Once state full devices fail, the restoration path is usually a hard reboot

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

Routing DNA

You are Under Attack – Its usually too Late


```
TCP
Local Address        Remote Address       State
-------------------- -------------------- -------
*.*                  *.*                  IDLE
*.sunrpc             *.*                  LISTEN
*.ftp                *.*                  LISTEN
*.telnet             *.*                  LISTEN
*.finger             *.*                  LISTEN
target.telnet    10.10.10.11.41508        SYN_RCVD
target.telnet    10.10.10.12.41508        SYN_RCVD
target.telnet    10.10.10.13.41508        SYN_RCVD
target.telnet    10.10.10.14.41508        SYN_RCVD
target.telnet    10.10.10.10.41508        SYN_RCVD
target.telnet    10.10.10.15.41508        SYN_RCVD
target.telnet    10.10.10.16.41508        SYN_RCVD
target.telnet    10.10.10.17.41508        SYN_RCVD
target.telnet    10.10.10.18.41508        SYN_RCVD
target.telnet    10.10.10.19.41508        SYN_RCVD
target.telnet    10.10.10.20.41508        SYN_RCVD
*.*                  *.*                  IDLE
```

output from `netstat -an` on target host

Once the connection queue is full of waiting-to-be-completed connections, all SYN+RCVDs get FIFOed out!

Capacity as a Solution

- **To many sorts of attacks, a common solution is to add more capacity**
- **Not every problem gets solved this way**

  Think about collateral damage
- **Challenge is to solve all the problems in the most economically feasible way**

Preparation

Preparation

- **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
  - Understand performance characteristics

DETECTING AND CLASSIFYING DoS ATTACK

Network Baselines

Cisco.com

- Network baselines from a variety of sources
- Unexplained changes in link utilization

  Worms can generate a lot of traffic, sudden changes in link utilization can indicate a worm

- Unexplained changes in CPU utilization

  Worm scans can affect routers/switches resulting in increased CPU both process and interrupt switched

- Unexplained syslog entries
- These are examples

  Changes don’t always indicate an attack or worm!

  Need to know what’s normal to identify abnormal behavior

Ways to Detect and Classify DoS Attacks

- Customer call
- SNMP: Line/CPU overload, drops
- NetFlow: Counting flows
- ACLs with logging
- Cisco Anomaly Detector (formerly Riverhead)
- Backscatter
- Sniffers
- Third party partner products

Netflow: Detection and Classification

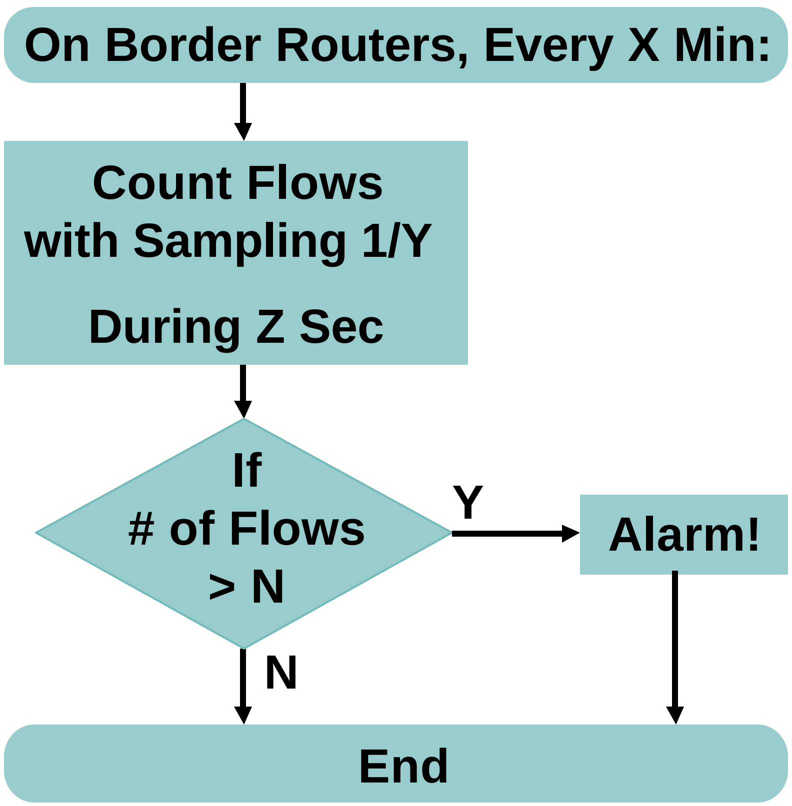
- **Netflow provides enough data to develop a baseline**
  - **What's normal --> what's abnormal**
- **Changes in Netflow indicative of changing traffic patterns**
  - **Might be DoS**
  - **SPAM and other mass mailers (e.g. a virus)**
- **Customers who use Netflow report very high rate of detection**
  - **Partner tools such as Arbor provide a lot of back-end intelligence**

Using Netflow

- **Real-time Netflow display**
  - **Show ip cache flow**
  - **Use inc command as needed**
  - **Look for relevant data**
- **Data analysis**
  - **Export data for external analysis**
  - **Find anomalies and changes → variation from "normal"**
  - **Scripts, Netflow tools, Arbor Networks**

Detecting DoS Attacks with NetFlow

BASIS: HAVE NETFLOW RUNNING ON THE NETWORK



DANTE Uses:
X=15 Min, Y=200,
Z=10 Sec, N=10

Values Are Empirical

Netflow: Real DoS Traffic

Potential DoS Attack (33 Flows) on Router1
Estimated: 660 Pkt/s   0.2112 Mbps
ASxxx Is: …
ASddd Is: …

Real Data Deleted in this Presentation

src_ip	dst_ip	in int	out int	src port	dest port	pkts	bytes	prot	src_as	dst_as
192.xx.xxx.69	194.yyy.yyy.2	29	49	1308	77	1	40	6	xxx	ddd
192.xx.xxx.222	194.yyy.yyy.2	29	49	1774	1243	1	40	6	xxx	ddd
192.xx.xxx.108	194.yyy.yyy.2	29	49	1869	1076	1	40	6	xxx	ddd
192.xx.xxx.159	194.yyy.yyy.2	29	49	1050	903	1	40	6	xxx	ddd
192.xx.xxx.54	194.yyy.yyy.2	29	49	2018	730	1	40	6	xxx	ddd
192.xx.xxx.136	194.yyy.yyy.2	29	49	1821	559	1	40	6	xxx	ddd
192.xx.xxx.216	194.yyy.yyy.2	29	49	1516	383	1	40	6	xxx	ddd
192.xx.xxx.111	194.yyy.yyy.2	29	49	1894	45	1	40	6	xxx	ddd
192.xx.xxx.29	194.yyy.yyy.2	29	49	1600	1209	1	40	6	xxx	ddd
192.xx.xxx.24	194.yyy.yyy.2	29	49	1120	1034	1	40	6	xxx	ddd
192.xx.xxx.39	194.yyy.yyy.2	29	49	1459	868	1	40	6	xxx	ddd
192.xx.xxx.249	194.yyy.yyy.2	29	49	1967	692	1	40	6	xxx	ddd
192.xx.xxx.57	194.yyy.yyy.2	29	49	1044	521	1	40	6	xxx	ddd
…	…	…	…	…	…	…	…	…	…	…

Classifying DoS with ACLs

- Requires ACLs to be in place (for detection)

  Extended IP access list 169

  permit icmp any any echo (2 matches)
  permit icmp any any echo-reply (21374 matches)
  permit udp any any eq echo
  permit udp any eq echo any
  permit tcp any any established (150 matches)
  permit tcp any any (15 matches)
  permit ip any any (45 matches)

Found:
- Attack type
- Interface

Looks Like Smurf Attack

- Watch performance impact
- Used on demand, not pro-active
- More used for checking than for detection
- Some ASIC based LCs do not show counters

Code Red Worm (Aug 2001)

Cisco.com

- Infects Microsoft IIS web servers
- Spread: Using real source, random destination
- Attack: accessing a specific server

217.33.138.14- - [07/Aug/2001:01:17:32 +0100] "GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u 6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00 %u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 400 328

Infected Host (Real IP!)

http get

Fill Buffer

Unicode Encoded Assembler Code

Code Red:
Detection of Infected Hosts

- **Spread: Infected host accesses random IP addresses (using real IP address)**
- **Examine Scatter: Every host likely to receive some “code red” HTTP requests!**
- **On an ISP’s network:**

  Route big chunks of unused space → analyser (sniffer, NetFlow, etc.)

  Analyzer receives lots of code red http connects

  Log IP sources: These hosts are infected!

SQL Slammer Worm (Jan 2003)

- **Very fast: Maximum spread after 10 min!**
- **No exploit, just spread (lucky!!)**
  - **Could have erased disks on all systems!**
- **Using true source, random destinations**
- **High pps load on the networks**
- **Scanning activity is a key indicator**
  - **How do we capture it? --> Sink Holes**

Backscatter Analysis

Cisco.com

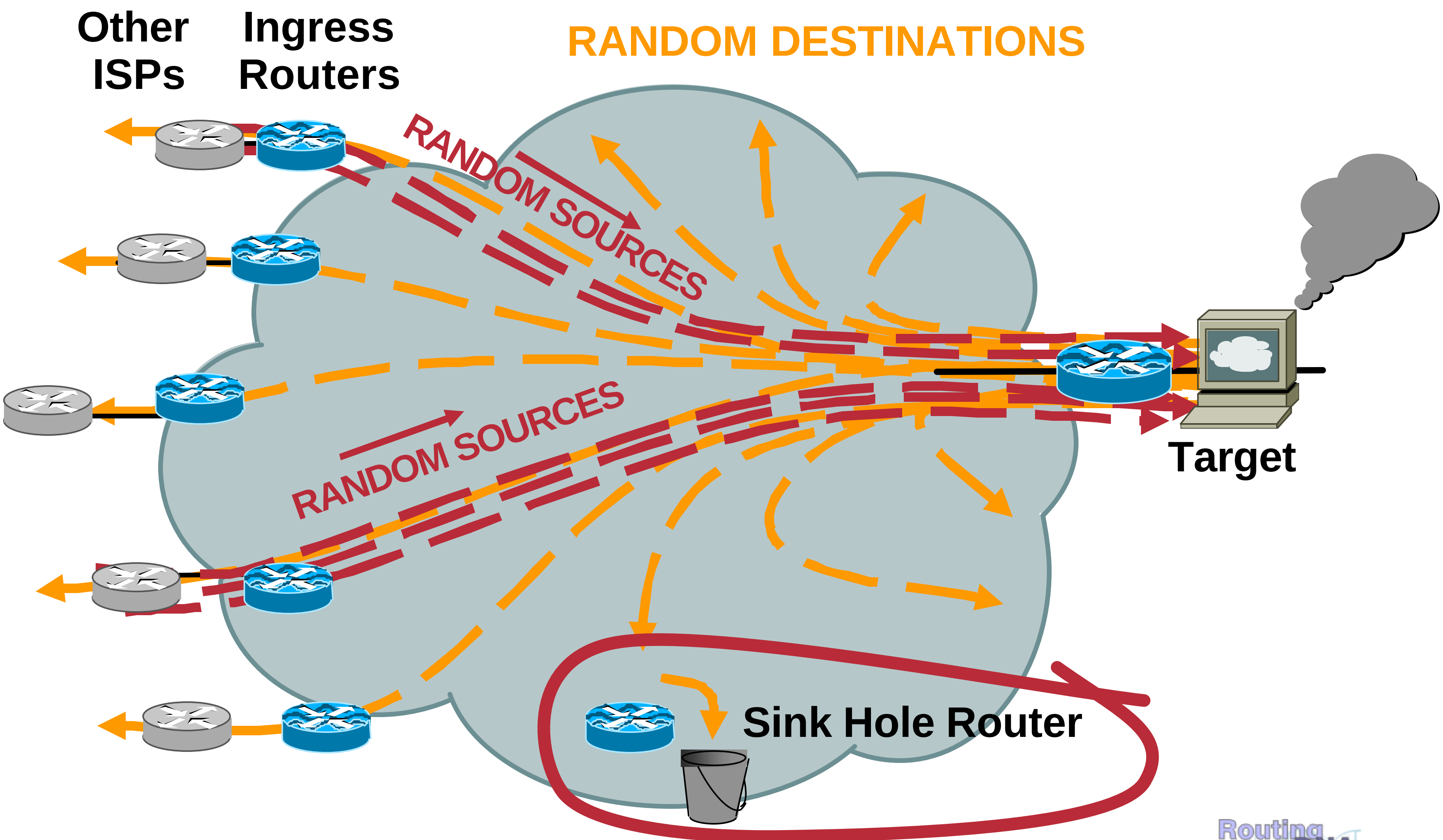
- Sink hole router: Statically announce unused address space (1/8, 2/8, 5/8, …)
  (see http://www.iana.org/assignments/ipv4-address-space)

  Note: Hackers know this trick: Use also unused space from your own ranges (aka DarkIP)

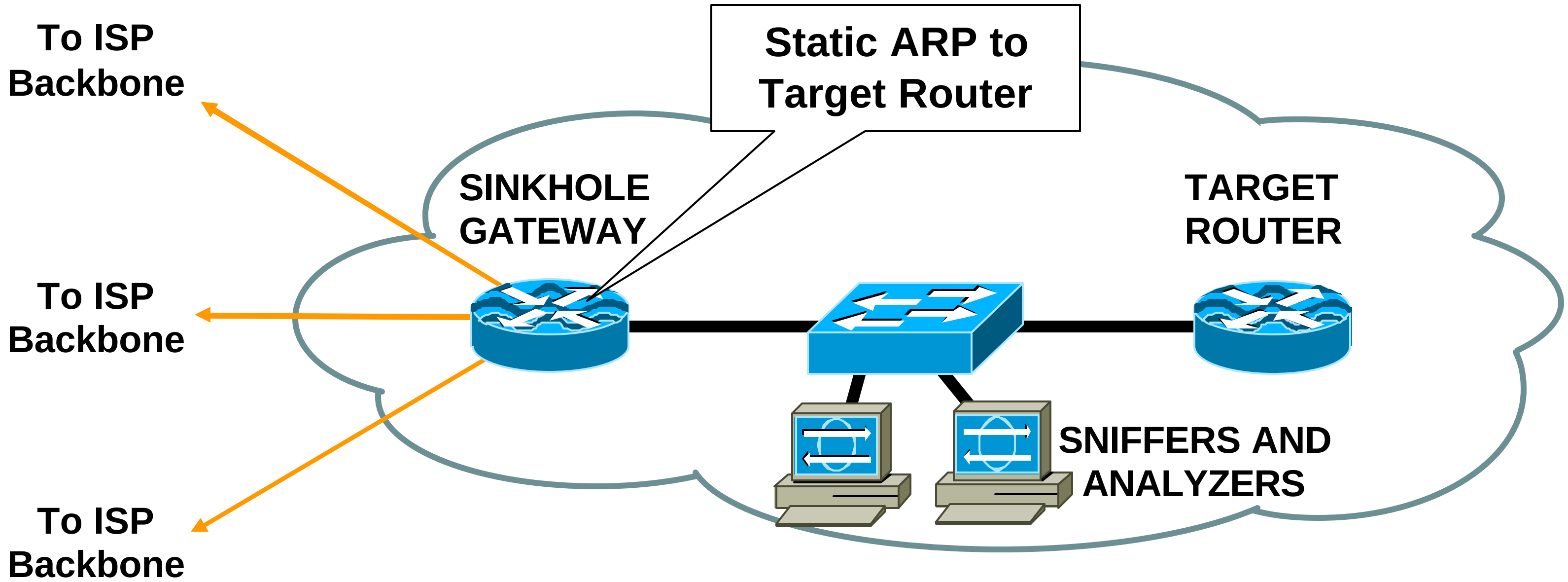
- Or, use default (if running full routing)
- Victim replies to random destinations
- → Some backscatter goes to sink hole router, where it can be analyzed

Backscatter Analysis

Cisco.com

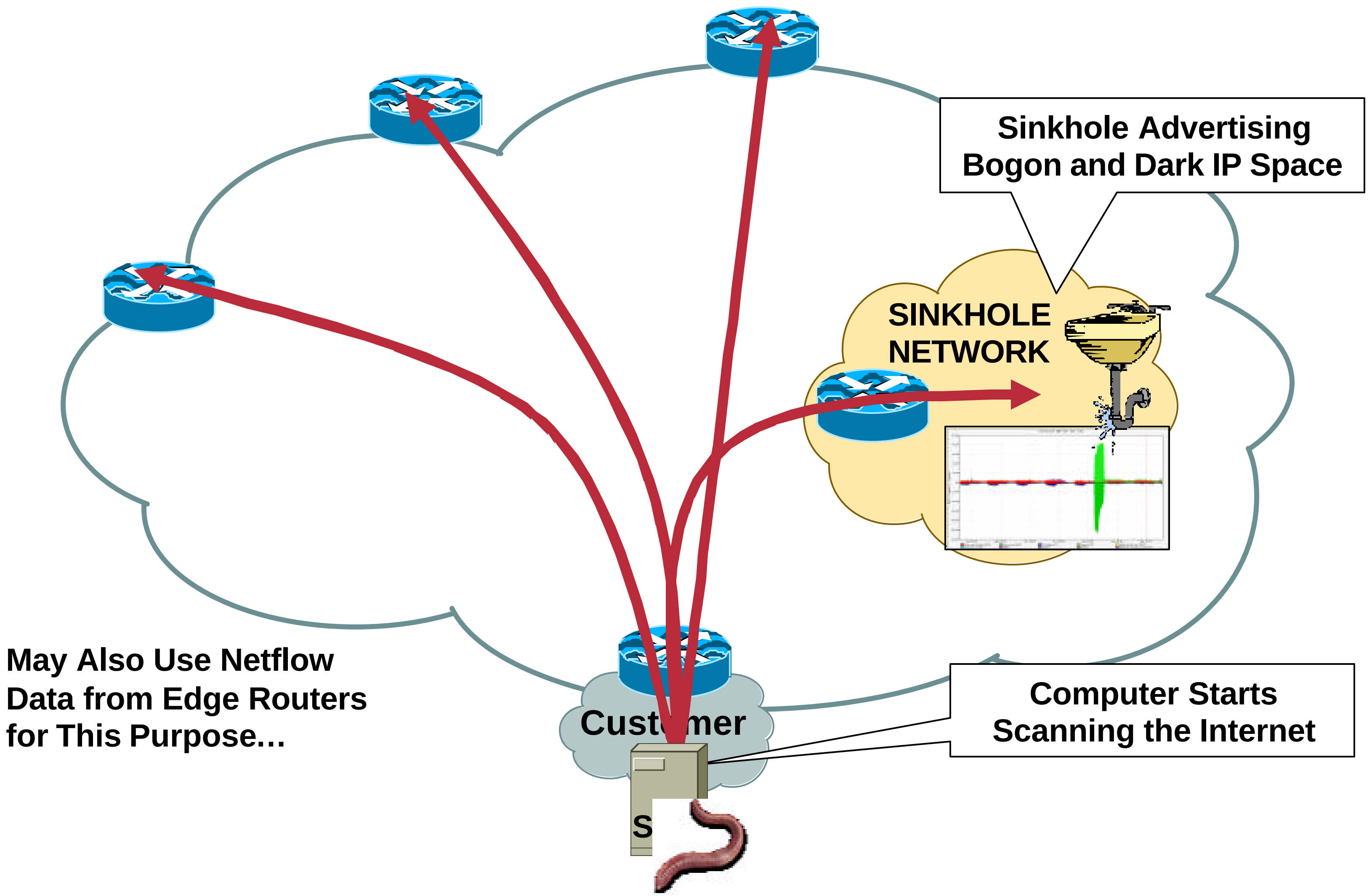


Sink Hole Architecture



- **Dedicated network component to attract traffic**
- **Can also be used "on demand": pull the DoS/DDoS attack to the sinkhole**
- **Sink Hole design can also incorporate Riverhead scrubbers**

Sinkholes: Worm Detection



TRACING DoS ATTACKS

Tracing DoS Attacks

- **If source prefix is not spoofed:**
  - → Routing table
  - → Internet Routing Registry (IRR)
  - → Direct site contact
- **If source prefix is spoofed:**
  - → Trace packet flow through the network
  - → Find upstream ISP
  - → Upstream needs to continue tracing

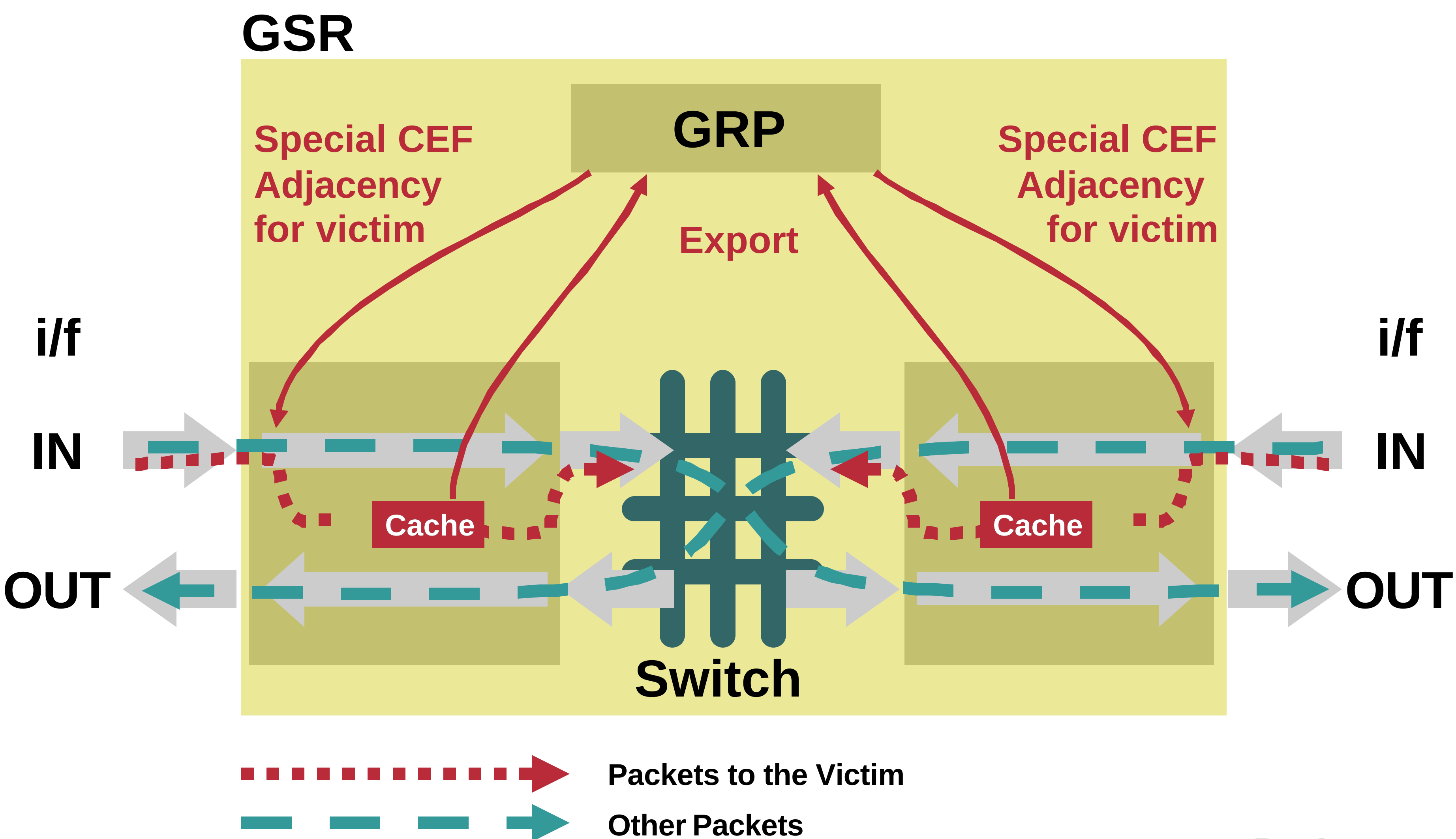
IP Source Tracker

- **Traditional way of tracking DoS: ACL or NetFlow**
  - **Limitation in performance and cross LC support**
- **Source Tracker:**
  - **Across LCs, low performance impact**

Line Card

- **Availability:**
  - **GSR E0,1,2,4: 12.0(21)S**
  - **GSR E3: 12.0(26)S**
  - **GSR E4+: 12.0(21)S (POS), (23)S (other)**
  - **7500: From 12.0(22)S**
  - **Other: 12.3(7)T**

IP Source Tracker



IP Source Tracker: Config

Cisco.com

Router# ip source-track <victim> — **Enable the Feature**

Router# show ip source-track 10.1.2.1 (also: … summary)

Address	SrcIF	Bytes	Pkts	Bytes/s	Pkts/s
10.1.2.1	Pos 1/0	2000	20	200	1

Protocol --------	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
ICMP	100	1	10	100	10	0	5

Victim (10.1.2.1)

Ingress Interface (Pos 1/0)

See: http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00800e9d38.html

Tracing Back with Netflow

Cisco.com

Routers Need Netflow Enabled

Victim

```
router1#sh ip cache flow | include <destination>
Se1     <source>    Et0      <destination>   11 0013 0007   159
.... (lots more flows to the same destination)
```

The flows come from serial 1

```
router1#sh ip cef se1
Prefix          Next Hop        Interface
0.0.0.0/0       10.10.10.2      Serial1
10.10.10.0/30   attached        Serial1
```

Find the upstream router on serial 1

Continue on this router

Show IP Cache Flow


```
router_A#sh ip cache flow
IP packet size distribution (85435 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2728 active, 1368 inactive, 85310 added
  463824 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics neve
Protocol         Total    Flo      Packets Bytes   ackets Active(Sec) Idle(Sec)
--------         Flows    /Sec     /Flow   /  kt   /Sec     /Flow     /Flow
TCP-X                      0.0         1  1440      0.0       0.0       9.5
TC                82580   11.2         1  1440     11.2       0.0      12.0
To                82582                            11.2       0.0      12.0

Sr            SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et            132.122.25.60   Se0/0          192.168.1.1     06 9AEE 0007     1
Et            139.57.220.28   Se0/0          192.168.1.1     06 708D 0007     1
Et            165.172.153.65  Se0/0          192.168.1.1     06 CB46 0007     1
```

Source Interface

Flow Info Summary

Flow Details

```
SrcIf
Et0/0
Et0/0
Et0/0
```

Tracing Back with ACLs

- **Create ACL:**

  access-list 101 permit ip any <target> log-input

- **Apply to interface for a few seconds:**

  interface xxx
  ip access-group 101 in
  (wait a few seconds)
  no ip access-group 101

- **Log shows interface the attack comes from**

14:17:21: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 105.12.73.84(0) (FastEthernet0/0 0006.d780.2380) -> 192.168.1.1(0), 1 packet

14:17:22: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 166.159.237.65(0) (FastEthernet0/0 0006.d780.2380) -> 192.168.1.1(0), 1 packet

mac Address

src Interface

Tracing Back Across an Internet Exchange Point (IXP) (or Any Other Shared Medium)

Cisco.com

- **NetFlow: Shows i/f only**
  - **Useless if IXP: Lots of routers behind…**
- **ACLs with log-input:**
  - **Shows also the MAC address of the router:**

1d00h: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 11.1.1.18 (Ethernet0 0001.96e6.7641) -> 10.1.2.1 (0/0), 169 packets

router#sh arp | include 0001.96e6.7641

Internet 12.1.1.99 152 0001.96e6.7641 ARPA Ethernet0

Originating Router

Routing DNA

Tip for Logging

- **Do not log to console**
  - **Slow connection (9.6 kbit/s)**
  - **Lots of logging → You lose the console**
- **Logging buffered**
  - **Avoids console overload**
  - **Automatically wraps**

Trace-Back in One Step: ICMP Backscatter

- **Border routers: Allow ICMP (rate limited)**
- **From sink hole router:**

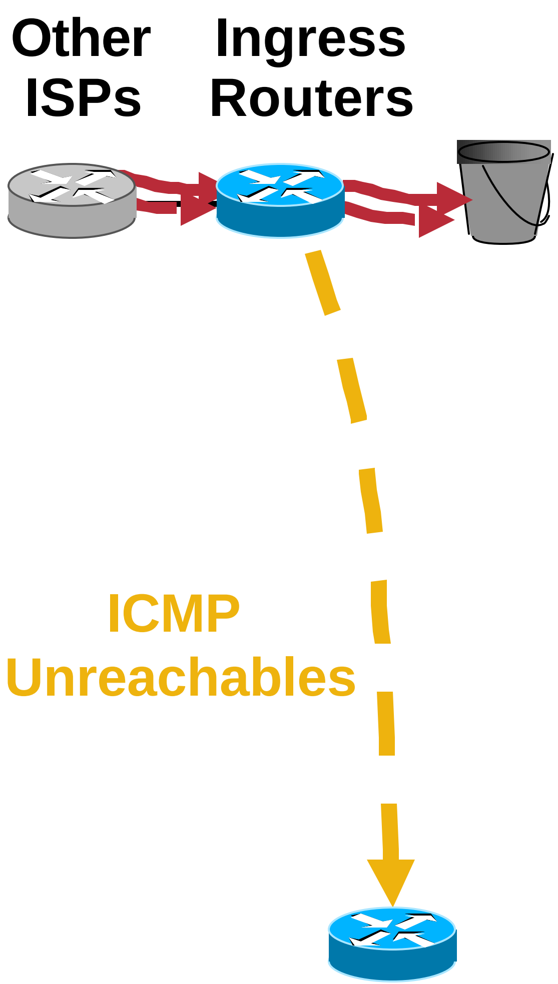
  iBGP update to all ingress routers:
  “drop all traffic to <victim>” (details later)

- **All ingress router drop traffic to <victim>**
- **And send ICMP unreachables to source!!**
- **For spoofed sources:**

  Sink hole router logs the ICMPs!

How to Detect Drops on a Router

Cisco.com

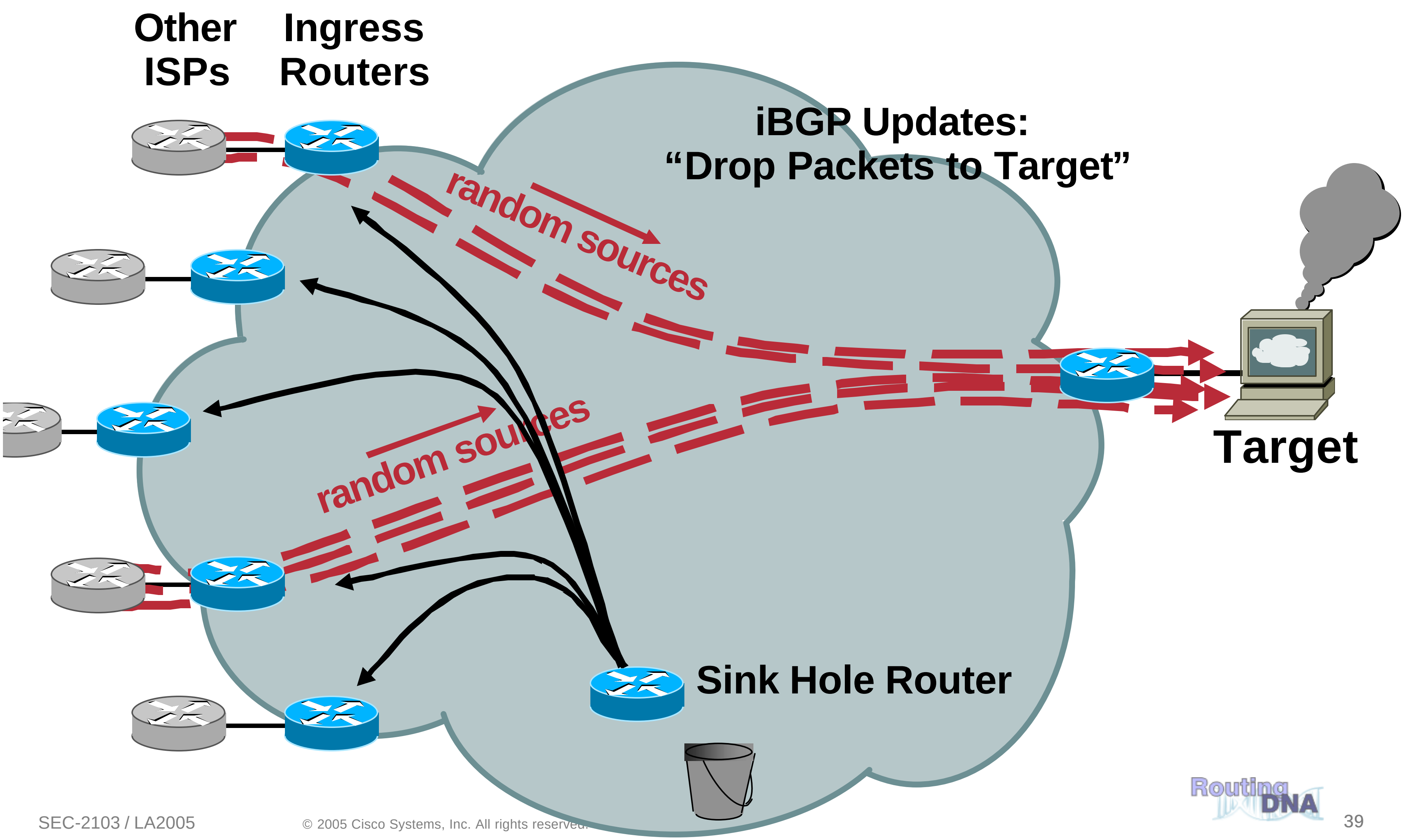


DROPS CAN BE SEEN:

- **Netflow: destination “null0”**
- **Interface “null0” counters (simple!)**
- **ICMP unreachables**

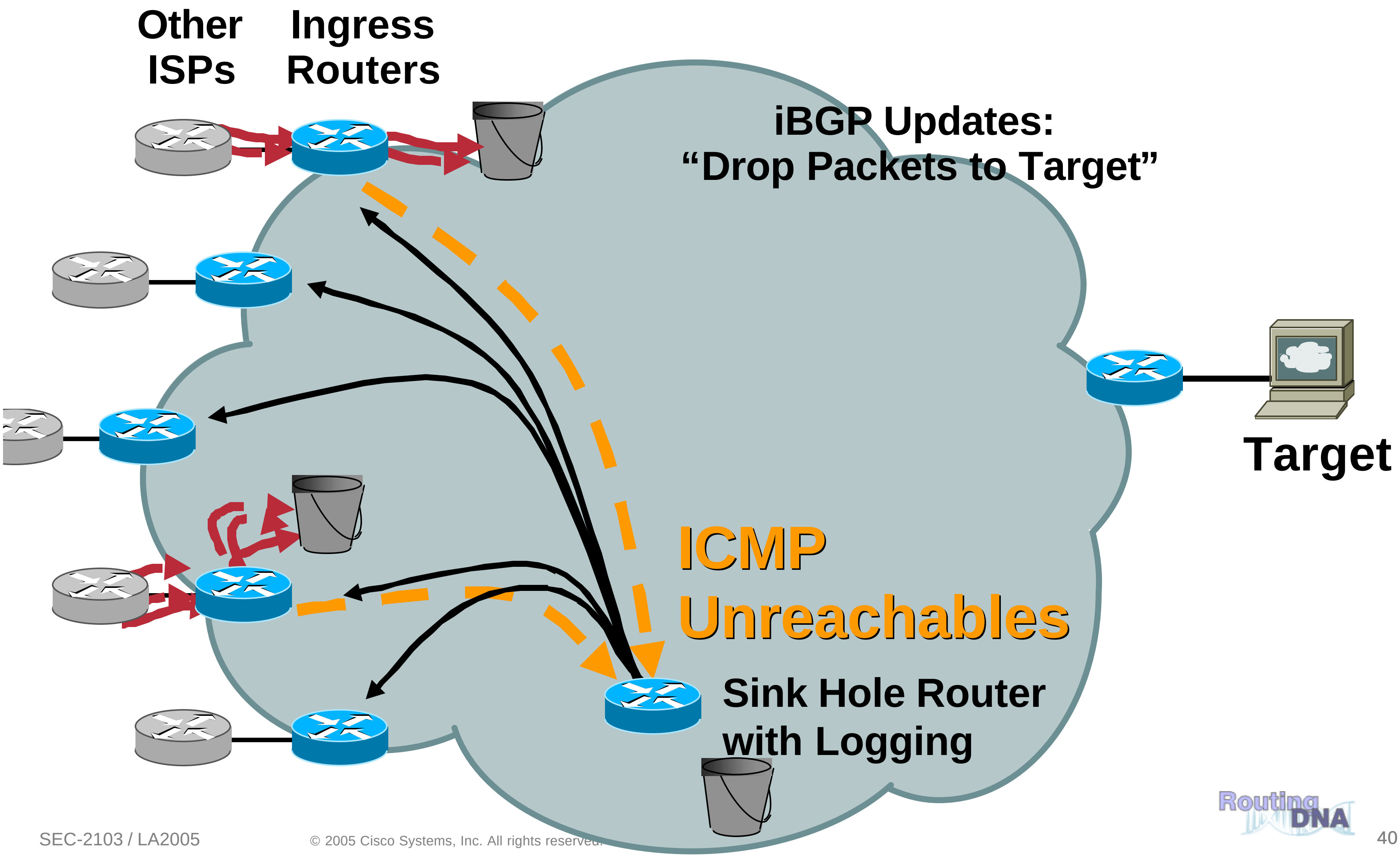
Routing DNA

Trace-Back in One Step: ICMP Backscatter



Trace-Back in One Step: ICMP Backscatter

Cisco.com



ICMP Backscatter

ON SINK HOLE ROUTER:

- **Static routes for 1/8,2/8,5/8 (will attract 3/256 of packets)**
- **Access-list 105 permit icmp any any log-input**
  Access-list 105 permit ip any any
- **Border router sends ICMP unreachable for deleted packets, to source**
- **If source is random, some will go to 1/8, 2/8, 5/8,…**

03:17:22: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.168.0.2 (Serial0/0 *HDLC*) -> 5.52.203.66 (0/0), 1 packet
03:17:38: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.168.0.2 (Serial0/0 *HDLC*) -> 1.167.111.47 (0/0), 1 packet
03:17:52: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.171.12.5 (Serial0/1 *HDLC*) -> 2.153.59.34 (0/0), 1 packet
…

Summary Tracing DoS Attacks

- **Non-spoofed: Technically trivial (IRR)**

  But: Potentially tracing 100's of sources…

- **Spoofed:**

  IP Source Tracker: router by router

  NetFlow:
  Automatic if analysis tools are installed
  Manually: Router by router

  ACLs:
  Has performance impact on some platforms
  Mostly manual: Router by router

  Backscatter technique:
  One step, fast, only for spoofed sources

Reacting with the Data Plane

RFC 2827/BCP 38 Ingress Packet Filtering

Packets Should Be Sourced from Valid, Allocated Address Space, Consistent with the Topology and Space Allocation

- **Our Goal here is to bound the problem and reduce the requirements for implementing security**

BCP 38: Consequences of No Action

- **No BCP 38 means that:**

  Devices can (wittingly or unwittingly) send traffic with spoofed and/or randomly changing source addresses out to the network

  Complicates traceback immensely

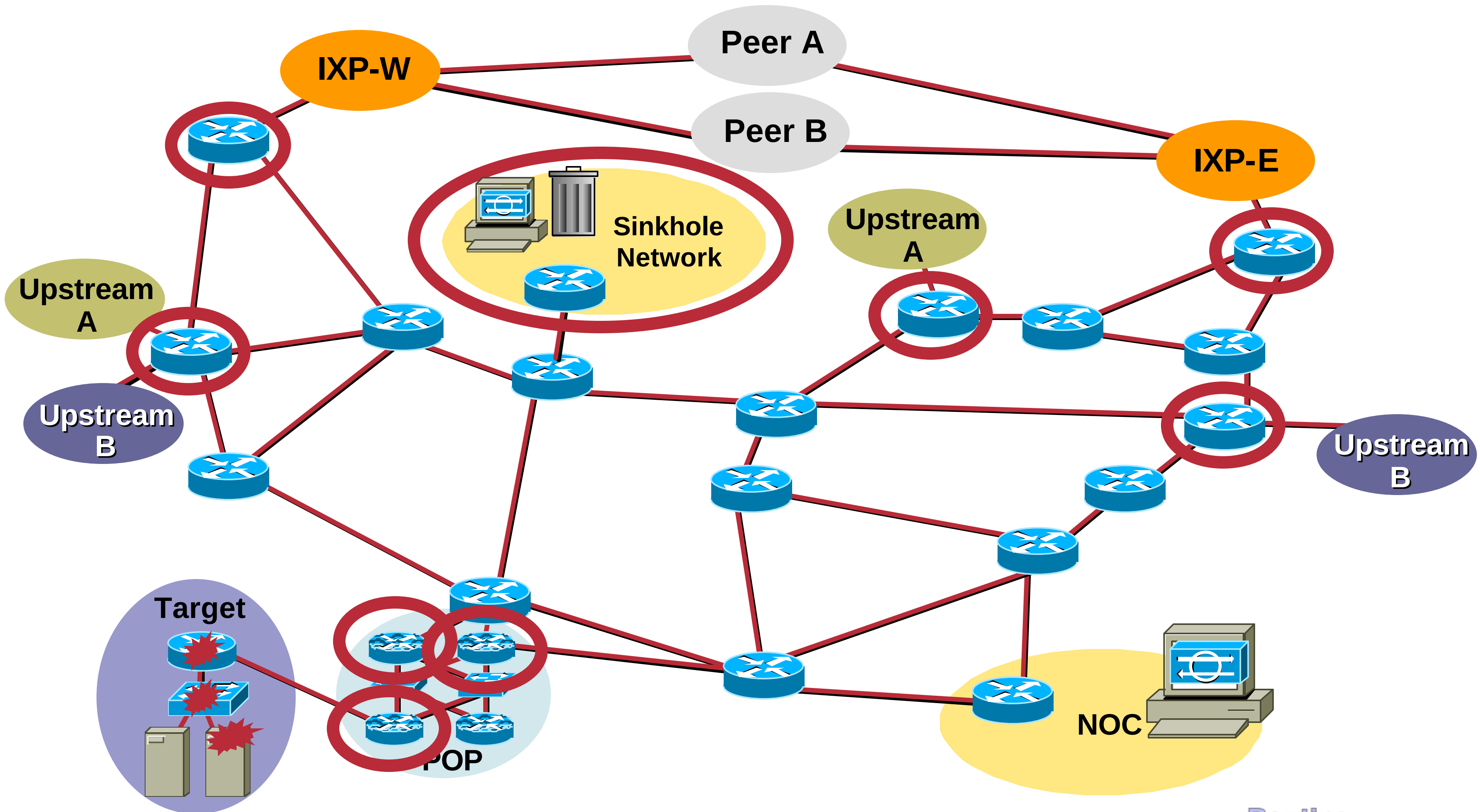
  Sending bogus traffic is NOT free!

BCP 38 Packet Filtering Principles

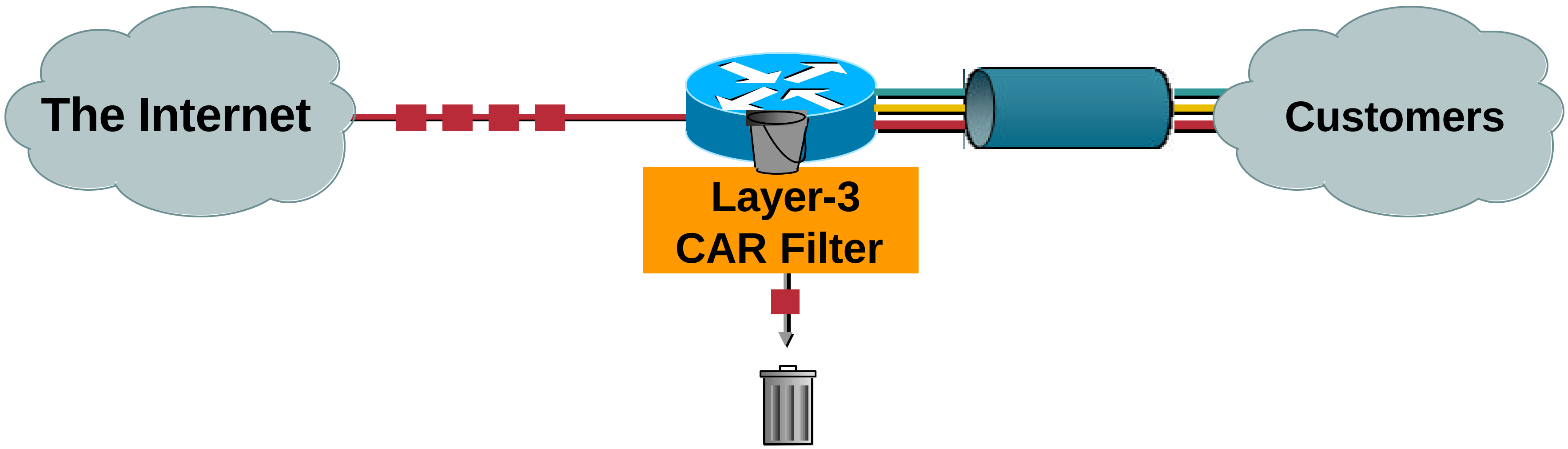
- Filter as close to the edge as possible
- Filter as precisely as possible
- Filter both source and destination where possible

Where to React?

Cisco.com



Reacting to an Attack with CAR



- Layer-3 input and output rate limits—specifically input rate limits
- Security filters use the input rate limit to drop packets before there are forwarded through the network
- Aggregate and granular limits
  - Port, MAC address, IP address, application, precedence, QOS_ID
- Excess burst policies

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

ACLs: Deployment Considerations

- How does the ACL load into the router? Does it interrupt packet flow?
- How many ACEs can be supported in hardware? In software?
- How does ACL depth impact performance?
- How do multiple concurrent features affect performance?

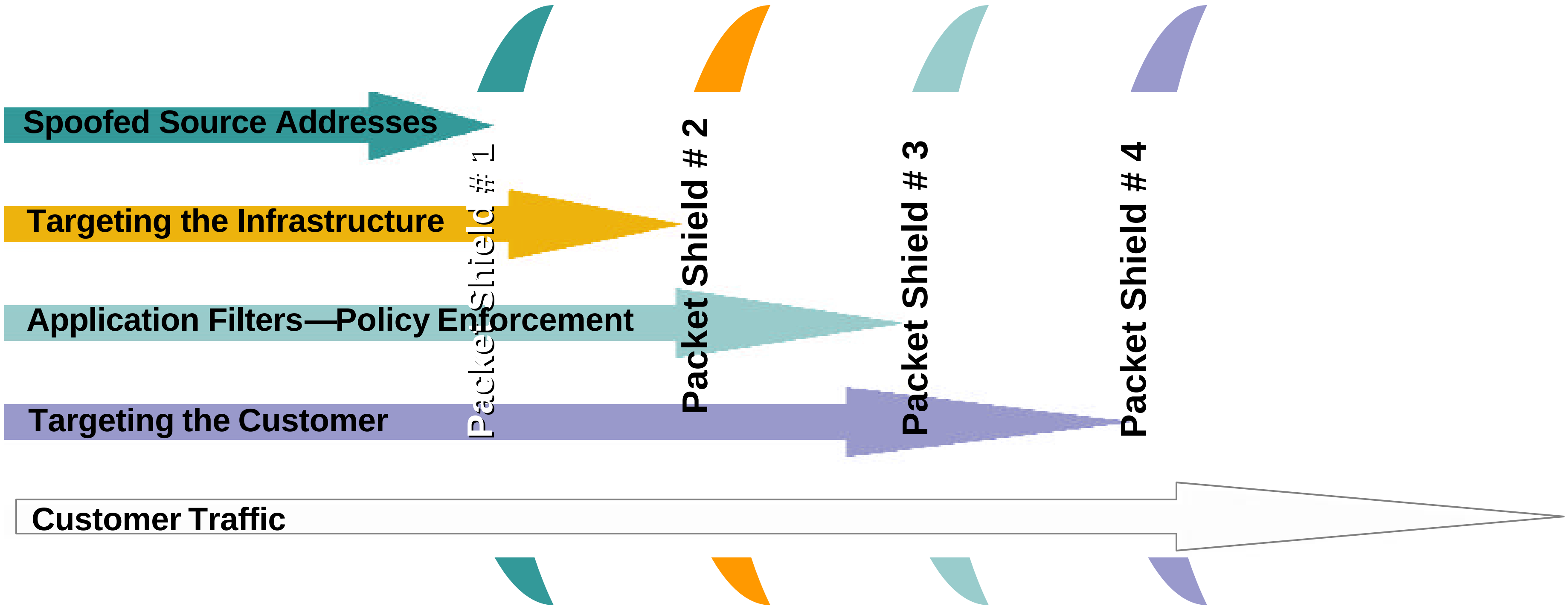
Filtering Fragments

- **Fragments can be explicitly denied**
- **Fragment handling is enabled via fragments keyword**
- **Default permit behavior → permit fragments that match ACE L3 entries**
- **Denies fragments and classifies fragment by protocol:**

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
```

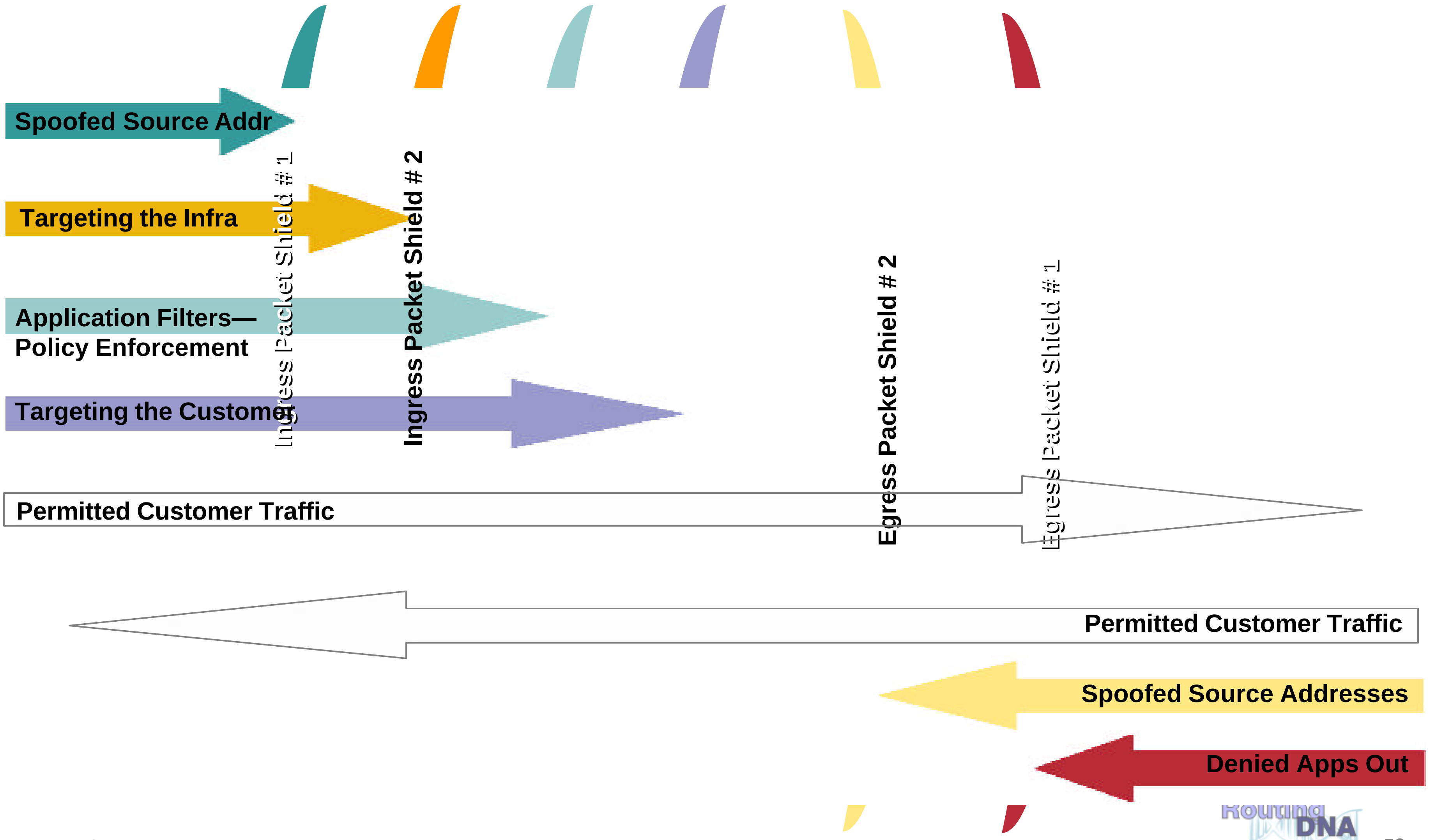
Packet Filtering Viewed Horizontally

Cisco.com



Packet Filtering
Remember to Filter the Return Path

Cisco.com



ACL Construction

- **Most common problems**
  - **Poorly-constructed ACLs**
  - **Ordering matters**
- **Scaling and maintainability issues with ACLs are commonplace**
- **Make your ACLs as modular and simple as possible**

ACL Categories: Hybrid Philosophy

Cisco.com

- **Hybrid permit/deny**
  - **Anti-spoofing**
  - **Anti-bogon (source)**
  - **Infrastructure**
  - **Explicit deny specific L3**
  - **Explicit deny specific L4**
  - **Incident reaction**
  - **Explicit permit L3 (good traffic)**
  - **Explicit permit L4 (good traffic)**
  - **Explicit deny everything else (auditing)**

ACL Summary

- ACLs are widely deployed as a primary containment tool
- Prerequisites: identification and classification—need to know what to filter
- Apply as specific an ACL as possible
- ACLs are good for static attacks, not as effective for rapidly changing attack profiles
- Understand ACL performance limitations before an attack occurs
- Operational efficiencies are important – scripped

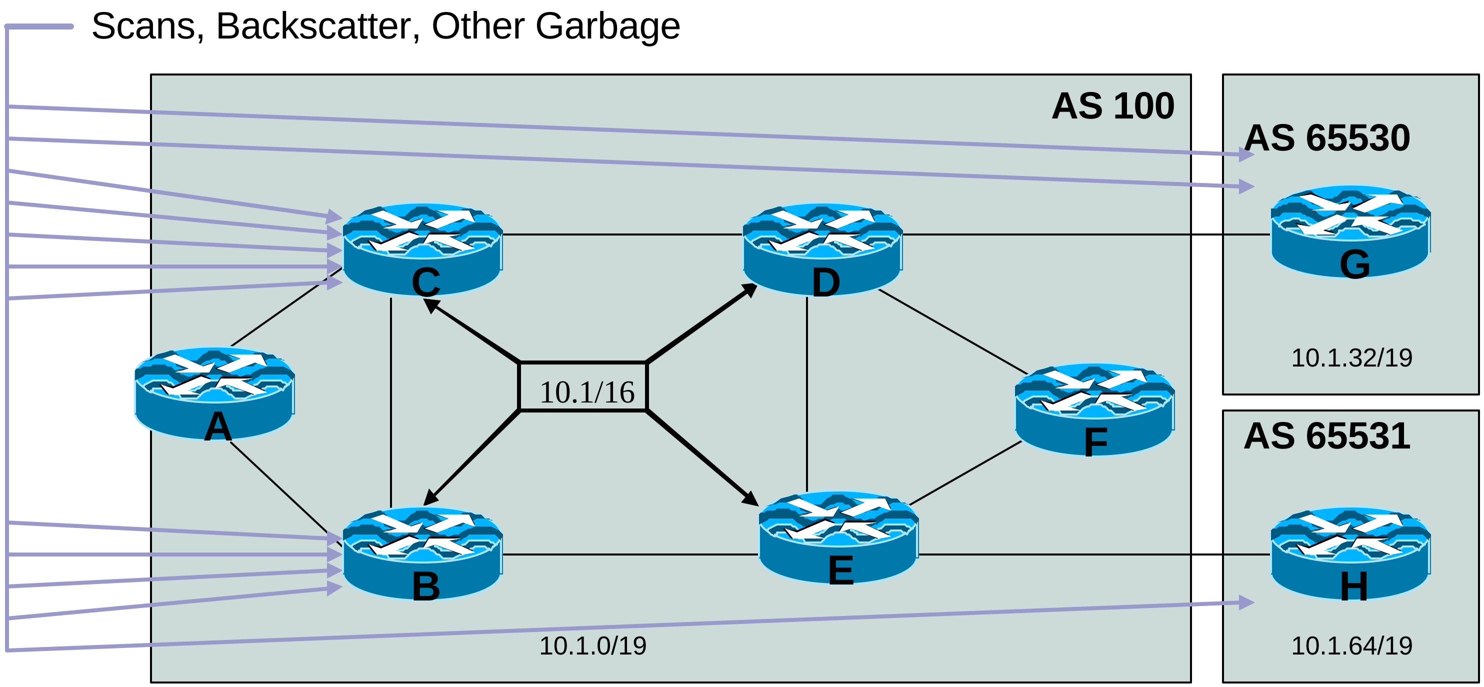
The Pros and Cons of ACLs

- **ACLs key strengths:**
  - Detailed packet filtering (ports, protocols, ranges, fragments, etc.)
  - Relatively static filtering environment
  - Clear filtering policy
- **ACLs can have issues when faced with:**
  - Dynamic attack profiles (different sources, different entry points, etc.)
  - Frequent changes
  - Quick, simultaneous deployment on a multitude of devices
  - Operationally hard to remove
- **Because of these weaknesses another tool was developed- using the Control Plane to signal the action**

Reacting with the Control Plane

Routers Drop Data, Often!

Cisco.com



- **An AS collects all the garbage (backscatter, scans, etc..) destined for 10.1/19, 10.1.96/19 & 10.1.128/17 addresses**
- **Routers who source those aggregates drop the data to unreachable parts of the networks, and are required to process data, send ICMP unreachables, etc..**

Routing DNA

Black Hole Filtering

- Blackhole Filtering or Blackhole Routing forwards a packet to a router's bit bucket
  - 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

Cisco.com

- We will 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
- This provides a tool that can be used to respond to security related events and forms a foundation for other remote triggered uses
- Often referred to as RTBH

Remote Triggered Black Hole (RTBH)

- Configure all edge routers with static route to Null0 (must use "reserved" network)

  ip route 192.0.2.1 255.255.255.255 Null0

- Configure trigger router

  Part of iBGP mesh

  Dedicated router recommended

- Activate black hole

  Redistribute host route for victim into BGP with next-hop set to 192.0.2.1

  Route is propagated using BGP to all BGP speaker and installed on routers with 192.0.2.1 route

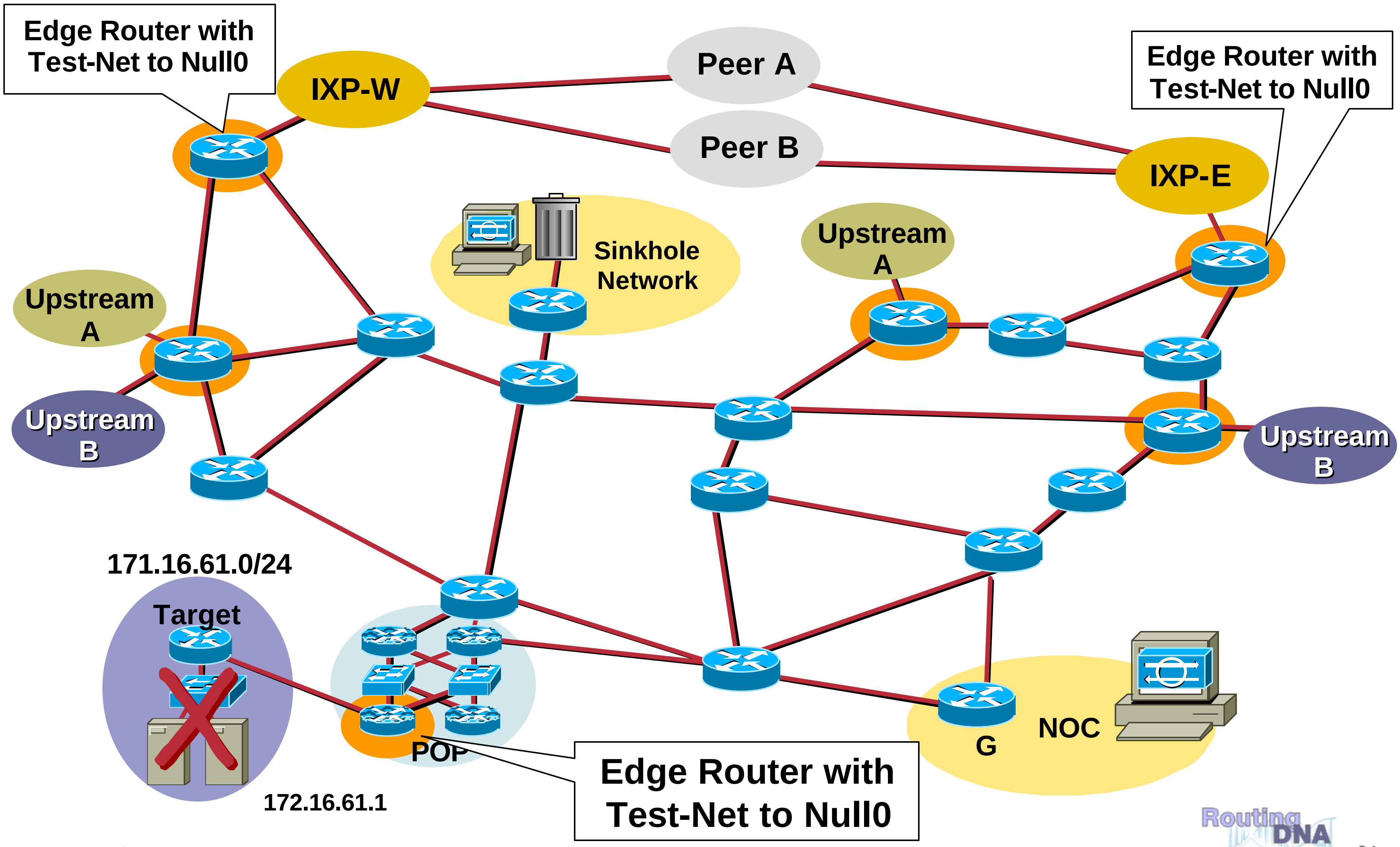
  All traffic to victim now sent to Null0

Step 1: Prepare all the Routers w/Trigger

- **Select a small block that will not be used for anything other than black hole filtering; test Net (192.0.2.0/24) is optimal since it should not be in use**
- **Put a static route with Test Net—192.0.2.0/24 to Null 0 on every edge router on the network**

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Step 1: Prepare All the Routers w/Trigger



Step 2: Prepare the Trigger Router

- **The trigger router is the device that will inject the iBGP announcement into the ISP's Network**
  - **Should be part of the iBGP mesh—but does not have to accept routes**
  - **Can be a separate router (recommended)**
  - **Can be a production router**
  - **Can be a workstation with Zebra/Quagga (interface with Perl scripts and other tools)**

Trigger Router’s Config

Cisco.com

Redistribute Static with a route-map

Match Static Route Tag

Set Next-Hop to the Trigger

Set Local-Pref

```
router bgp 65535
.
redistribute static route-map static-to-bgp
.
!
route-map static-to-bgp permit 10
match tag 66
set ip next-hop 192.0.2.1
set local-preference 200
set community no-export
set origin igp
!
Route-map static-to-bgp permit 20
```

Step 3: Activate the Black Hole

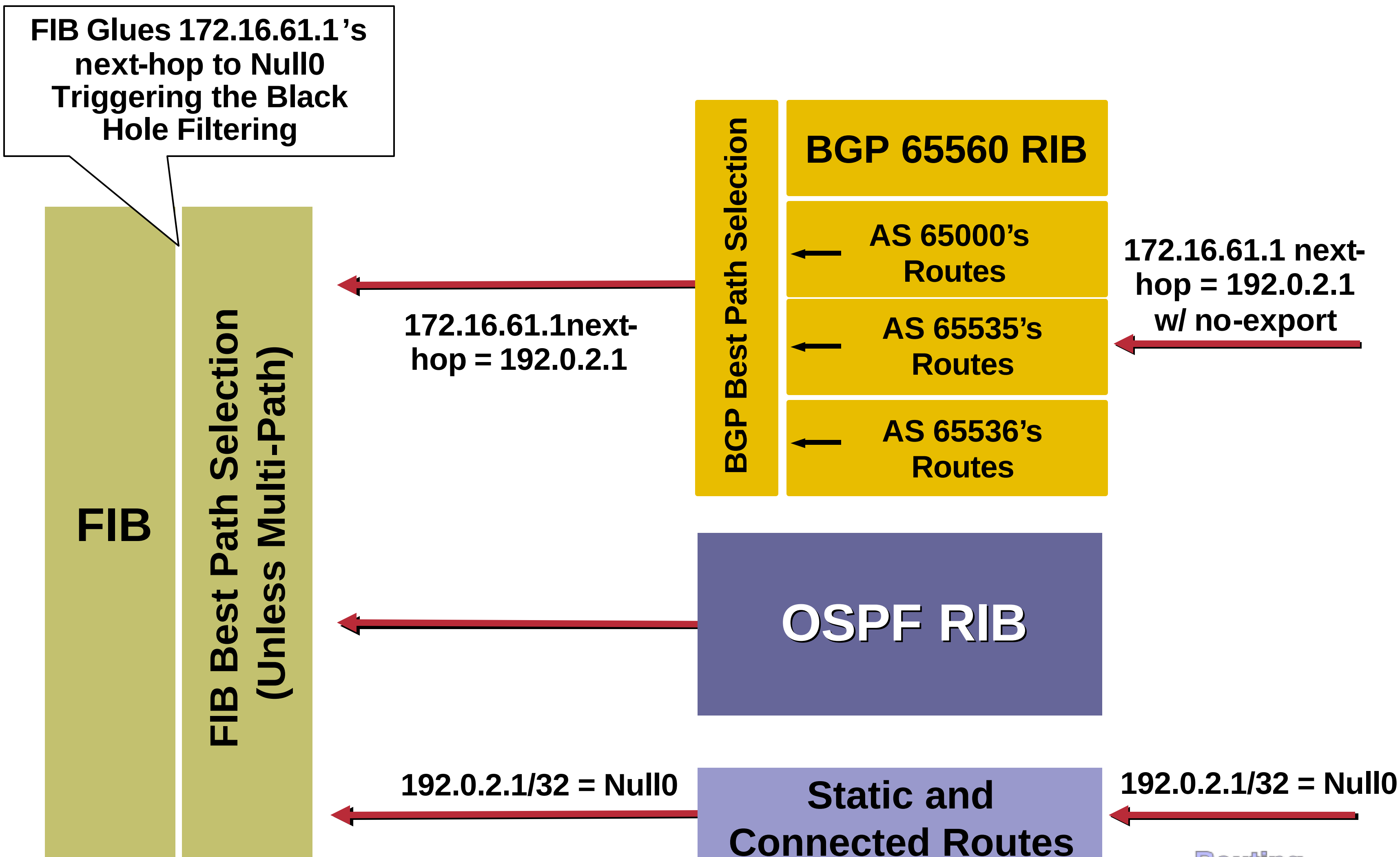
- **Add a static route to the destination to be blackholed; the static is added with the "tag 66" to keep it separate from other statics on the router**

```
ip route 172.16.61.1 255.255.255.255 Null0 Tag 66
```

- **BGP advertisement goes out to all BGP speaking routers**
- **Routers received BGP update, and "glue" it to the existing static route; due to recursion, the next-hop is now Null0**

Step 3: Activate the Black Hole

Cisco.com



Step 3: Activate the Black Hole

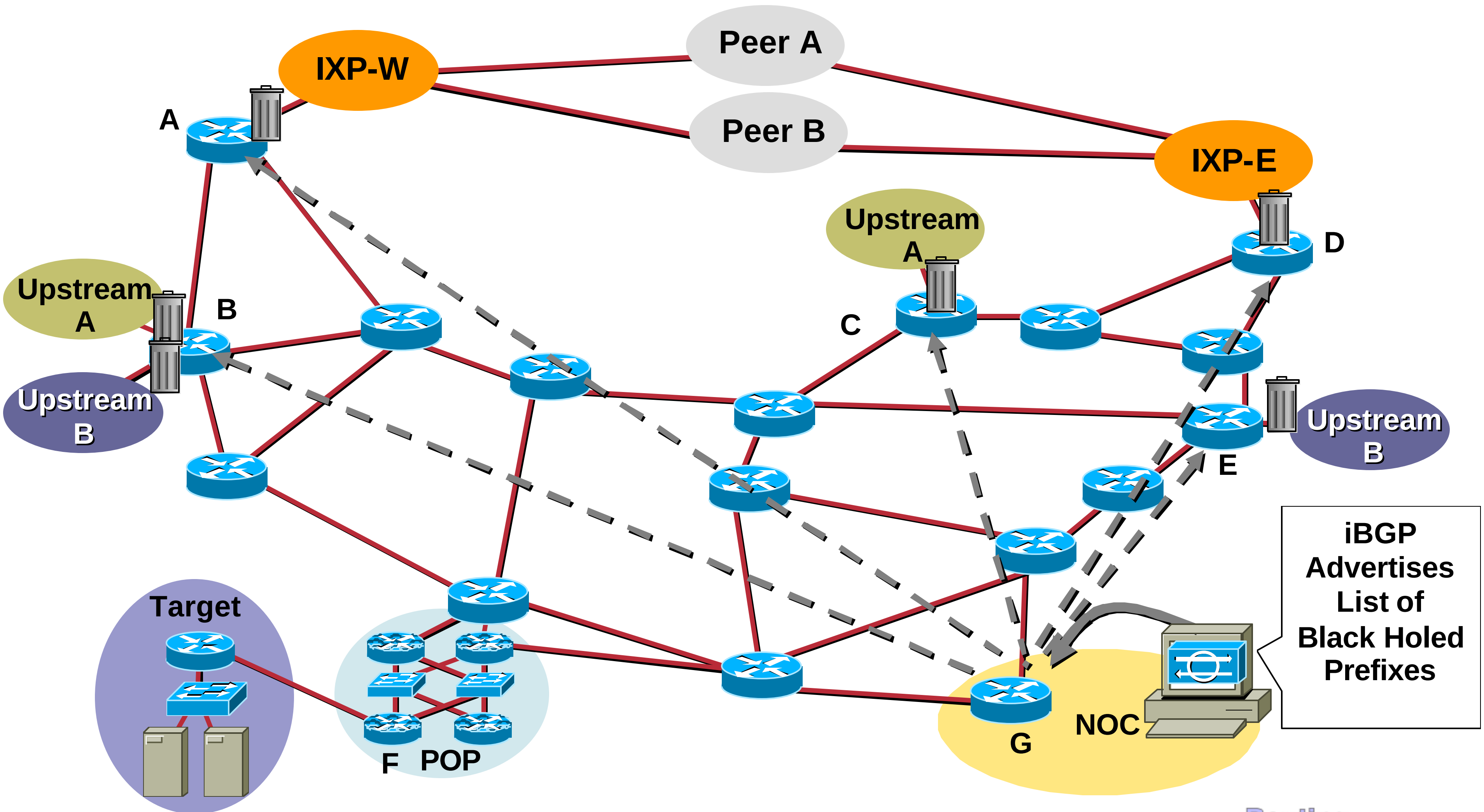
BGP Sent—172.16.61.1 Next-Hop = 192.0.2.1

Static Route in Edge Router—192.0.2.1 = Null0

172.16.61.1= 192.0.2.1 = Null0

Next-Hop of 172.16.61.1
Is Now Equal to Null0

Step 3: Activate the Black Hole



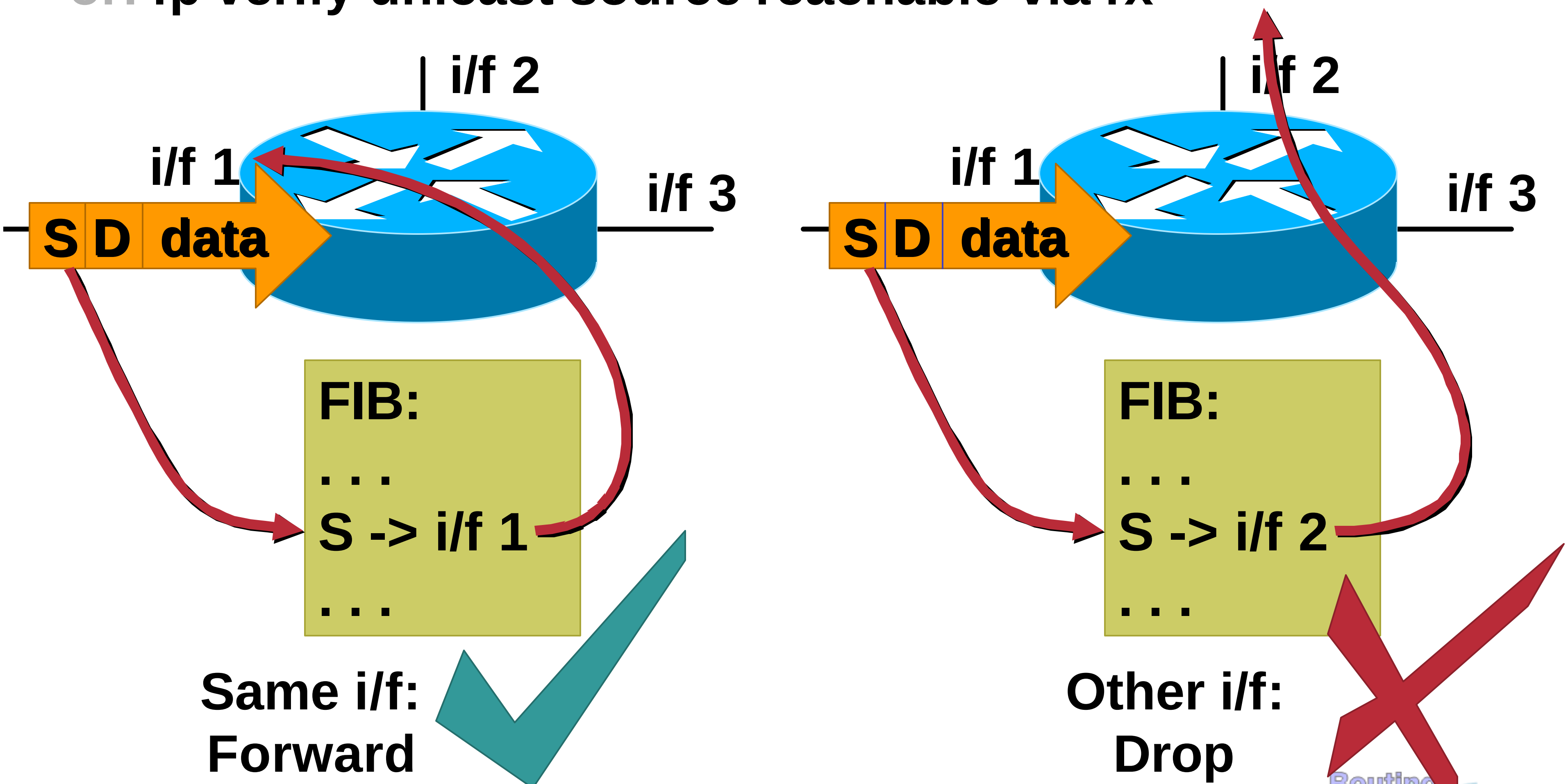
RTBH: Triggered Source Drops

- **Dropping on destination is very important**
  - **Dropping on source if often what we really need**
- **Reacting using source address provides some interesting options:**
  - **Stop the attack without taking the destination offline**
  - **Filter command and control servers**
  - **Filter (contain) infected end stations**
- **Must be rapid and scalable**
  - **Leverage pervasive BGP again**

Strict uRPF Check (Unicast Reverse Path Forwarding)

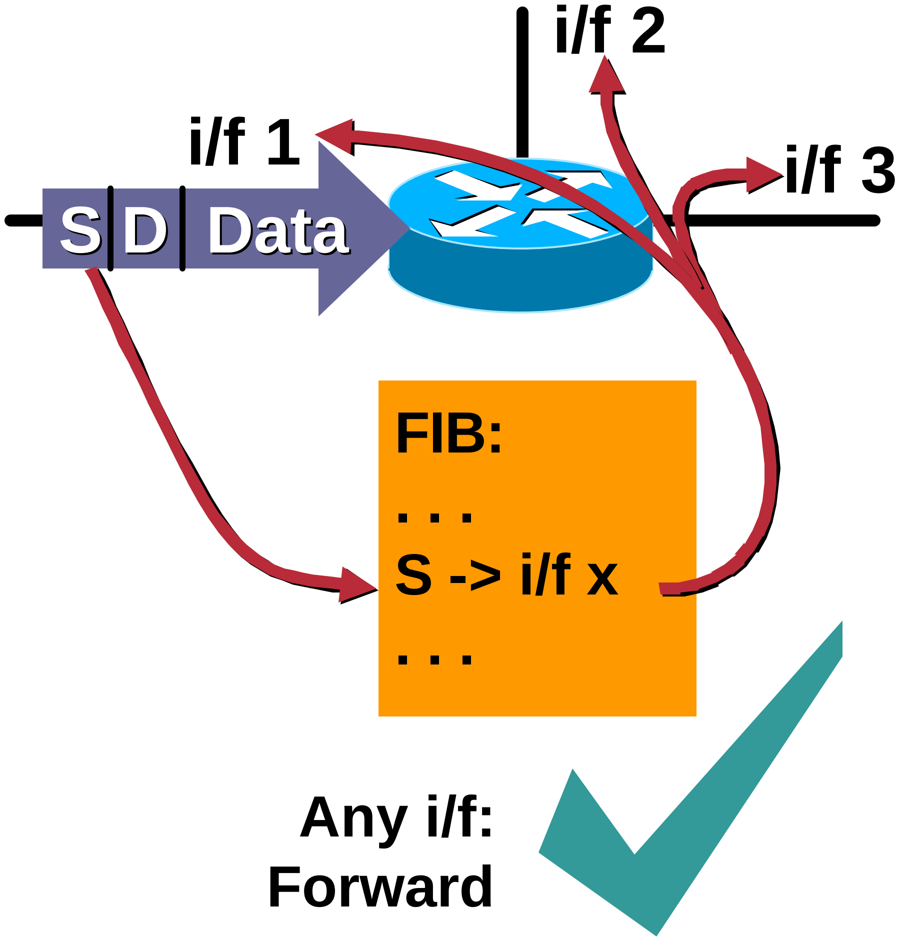
router(config-if)# **ip verify unicast reverse-path**

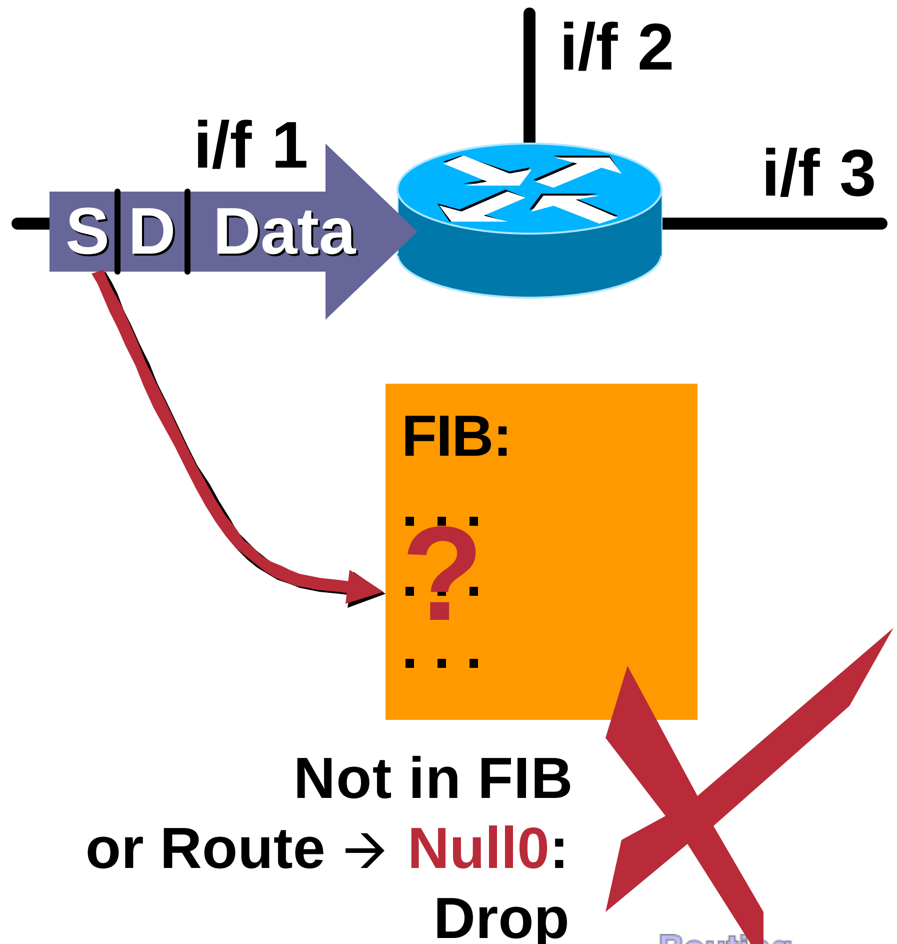
or: **ip verify unicast source reachable-via rx**



Quick Review: Loose uRPF Check

router(config-if)# ip verify unicast source reachable-via any





Source-Based Remote Triggered Black Hole Filtering

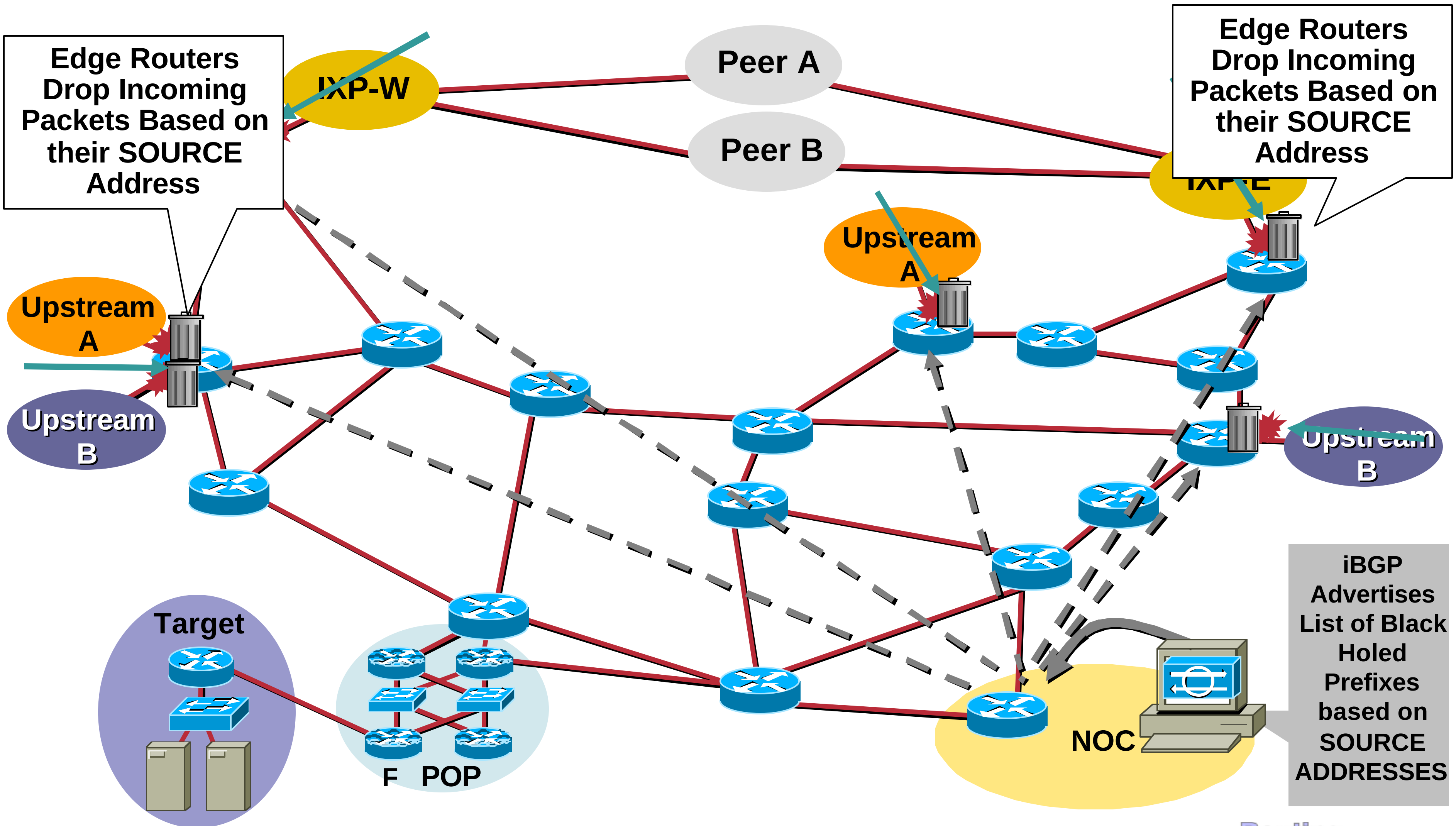
- **Uses the same architecture as destination-based filtering + Unicast RPF**
  - **Edge routers must have static in place**
  - **They also require Unicast RPF**
  - **BGP trigger sets next hop—in this case the "victim" is the source we want to drop**

Source-Based Remote Triggered Black Hole Filtering

- **What do we have?**
  - **Black Hole Filtering—If the destination address equals Null0 we drop the packet**
  - **Remote 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 drop for any packet coming into the network whose source or destination equals Null0!**

Customer Is DOSed: After Packet Drops Pushed to the Edge

Cisco.com



Source Dropping Caution

- **Caution you will drop all packets with that source.**
- **Remember spoofing**

Community-Based Trigger

- **BGP community-based triggering allow for more fined tuned control over where you drop the packets**
- **Three parts to the trigger:**
  - **Static routes to Null0 on all the routers**
  - **Trigger router sets the community**
  - **Reaction routers (on the edge) matches community and sets the next-hop to the static route to Null0**

Why Community-Based Triggering?

Cisco.com

- **Allows for more control on the attack reaction**
  - Trigger community #1 can be for all routers in the network
  - Trigger community #2 can be for all peering routers; no customer routers—allows for customers to talk to the DOSed customer within your AS
  - Trigger community #3 can be for all customers; used to push a inter-AS traceback to the edge of your network
  - Trigger communities per ISP Peer can be used to only black hole on one ISP Peer's connection; allows for the DOSed customer to have partial service

(Source-Based) RTBH

- **Advantages:**

  No ACL update

  No change to the router's configuration

  Drops happen in the forwarding path

  Frequent changes when attacks are dynamic (for multiple attacks on multiple customers)

- **Limitations:**

  Source detection and enumeration

  attack termination detection (reporting)

  Resource utilization: finite resources

  Effects all traffic, on all triggered interfaces, regardless of actual intent

Using Dedicated Security Tools

Given Everything Said, What Remains

- **Raise the bar! Stop ONLY bad traffic**
- **In asymmetric environments, especially across peers, packet spoofing is still problematic**
- **Detection of exactly who is attacking is problematic**
- **Doing all this in the core requires specialized hardware, which has scaling and availability problems**

Network IDS/IPS
Terminology

Cisco.com

- **False Positives: System mistakenly reports certain benign activity as malicious; also called false alarms**
- **False Negatives: System does not detect and report actual malicious activity**

- **For many, false positives are the bane of IDS technology**
- **Additionally, you require a signature in order to stop the attack**
- **To reduce the rate of false positives**
  - **Use false positive reduction technologies, such as CTR (Cisco Threat Response)**
  - **Spend time TUNING for your environment**

Firewalls

Modern Stateful Firewall: The Security Keystone

What It Is:

- Sometimes called a hybrid
- Combines features of other firewall approaches such as…
  - Access Control Lists
  - Application specific proxies/inspections
  - Stateful Inspection
- Plus features of other devices…
  - Web (HTTP) cache
  - Specialized servers
    - SSH, SOCKS, NTP
  - Most include VPN, some include IDS

Pros and Cons

- Pro: Maintains most of the speed advantage of a simple stateful firewall
- Pro: Application Layer Gateway services provide application security while resolving the NAT issue
- Con: Does not provide complete session termination, as would a full proxy
- Con: Actively tracks the state of incoming connections – a DoS issue.

Formal Requirements for a Core Security Device

Cisco.com

- **Need to avoid state**
  - **Constant state tracking leaves us vulnerable to DDoS attacks**
- **Doesn't rely on signatures**
  - **If I get an attack that there is no signature I cannot block it**
  - **Possibly can use signature like filters however after the fact**
- **Doesn't have to be Inline when it isn't needed**
- **Scales easily**
- **Doesn't require traffic symmetry**
  - **The Internet is a very asymmetrical place!**

Routing DNA

Core Design Philosophies

- **Scale by using traffic shunting**
- **Core packet scrubbing requirements**

  1) Validate incoming traffic to make sure it comes from the source IP's that are in the SRC IP field of the packet

  2) Evaluate these validated sources against a baseline and then recommend either further processing or dropping for sources that mis-behave

- **Don't need to stop every bad packet – instead, focus on not stopping any good packets!**
  - **Pad thresholds to reduce likelihood of false positives**
  - **Have very high defaults so in a non-leaned environment you won't block good traffic**

Packet Scrubbing Issues

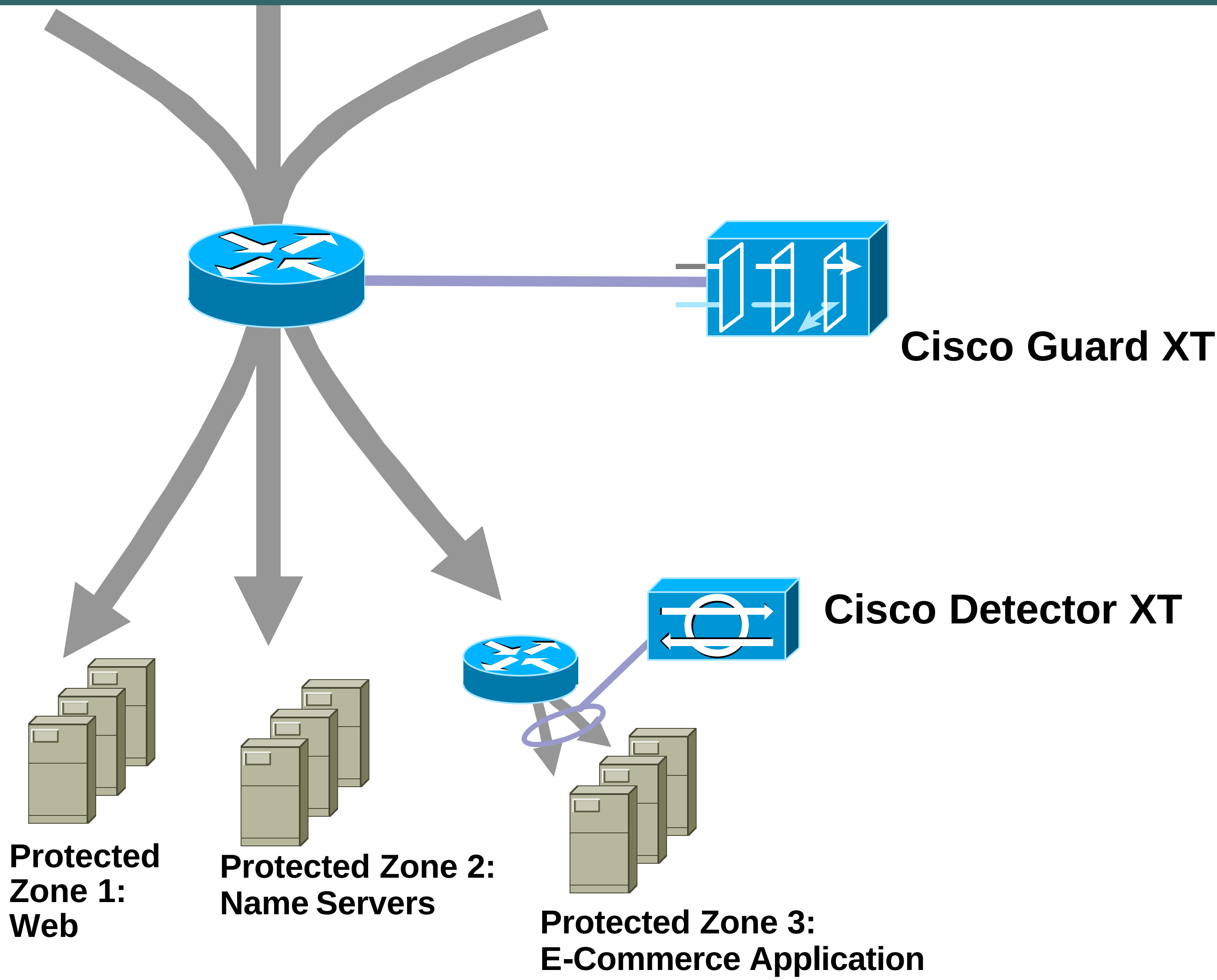
Shunting the Packets

Scrubbing the Packets

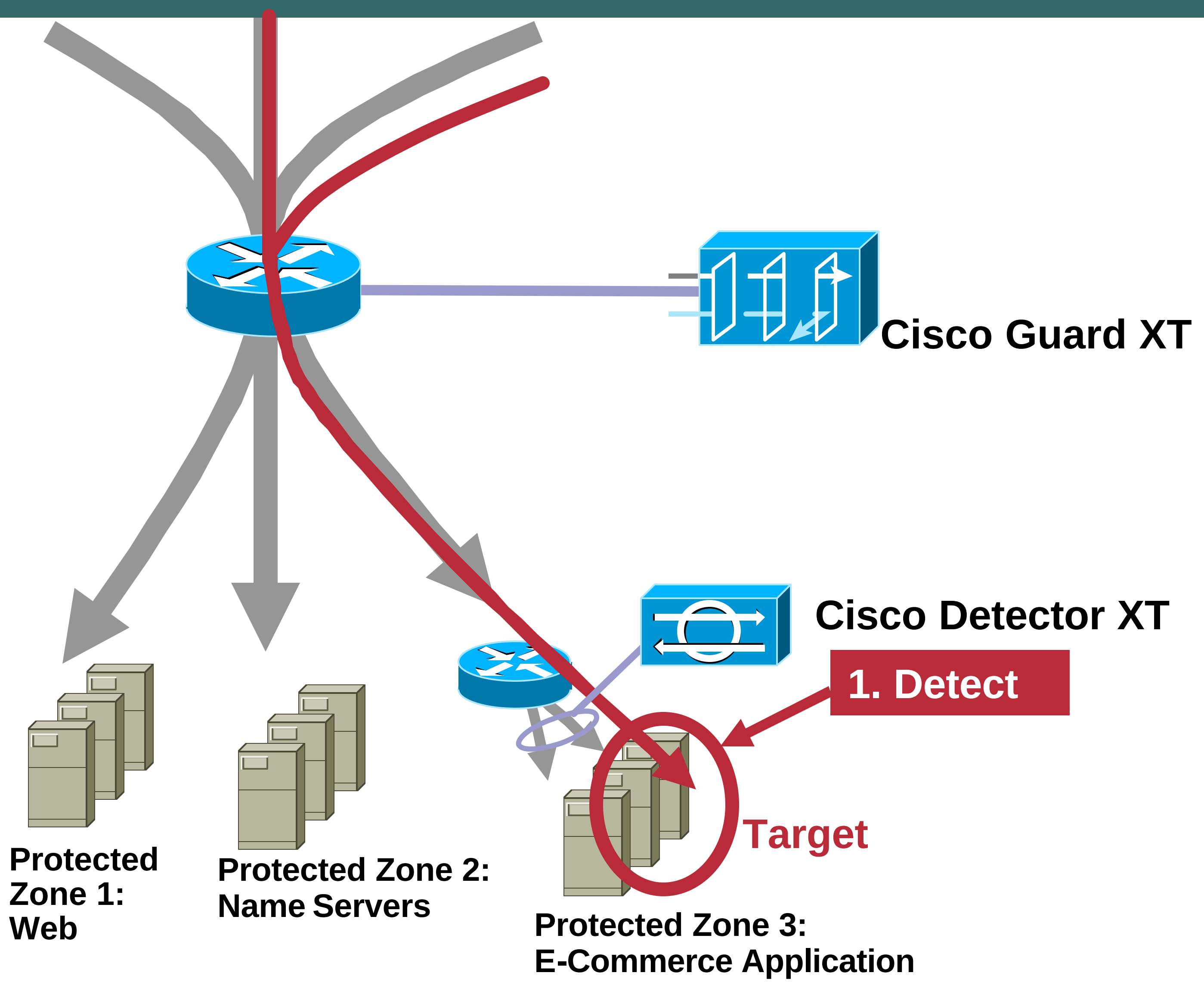
Traffic Shunts

- Intercept and shunt traffic to the mitigation device – the ‘scrubber’
- Return good traffic back to the customer
- Need to avoid Forwarding loops – means some sort of tunneling

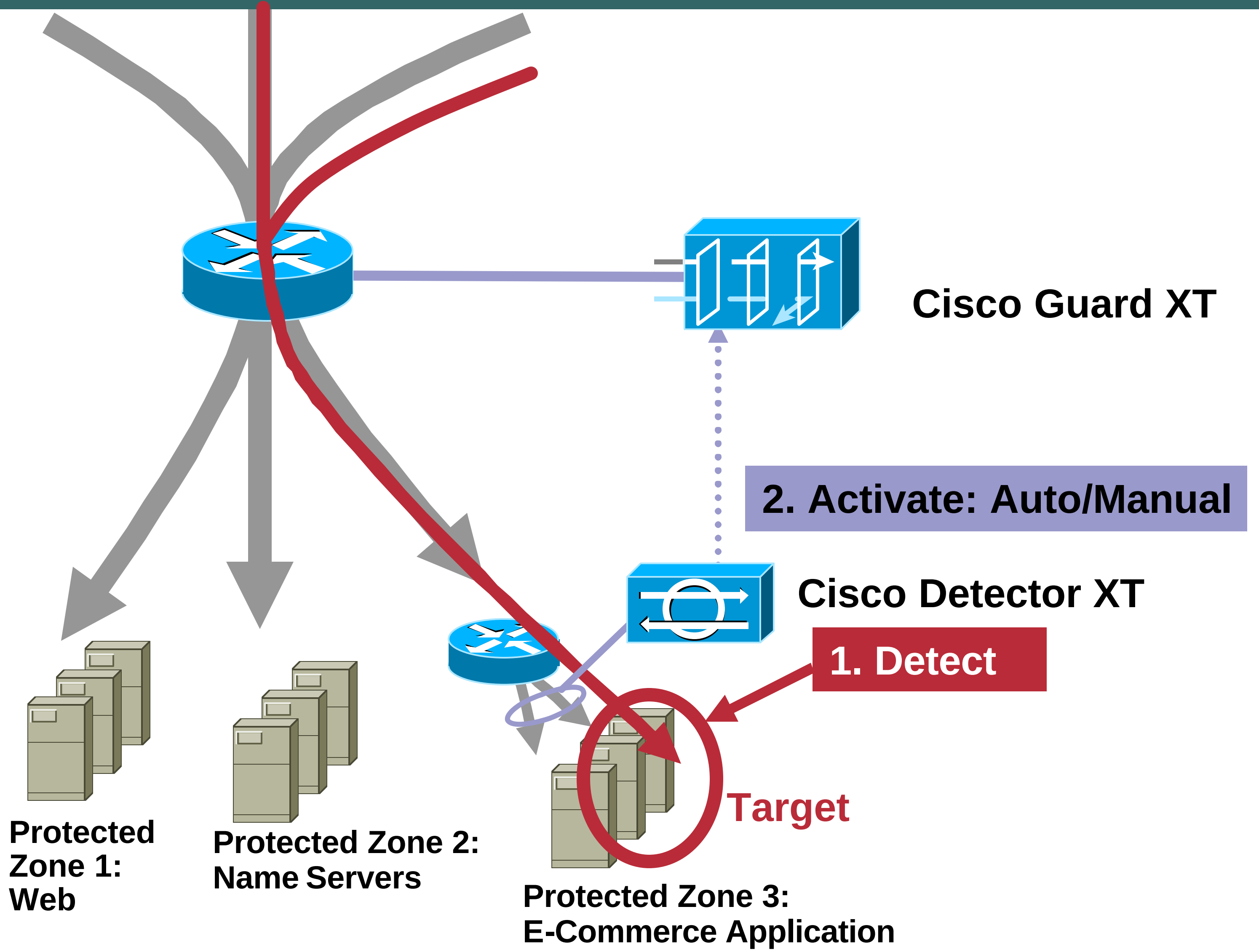
Cisco DDoS Solution: Diversion



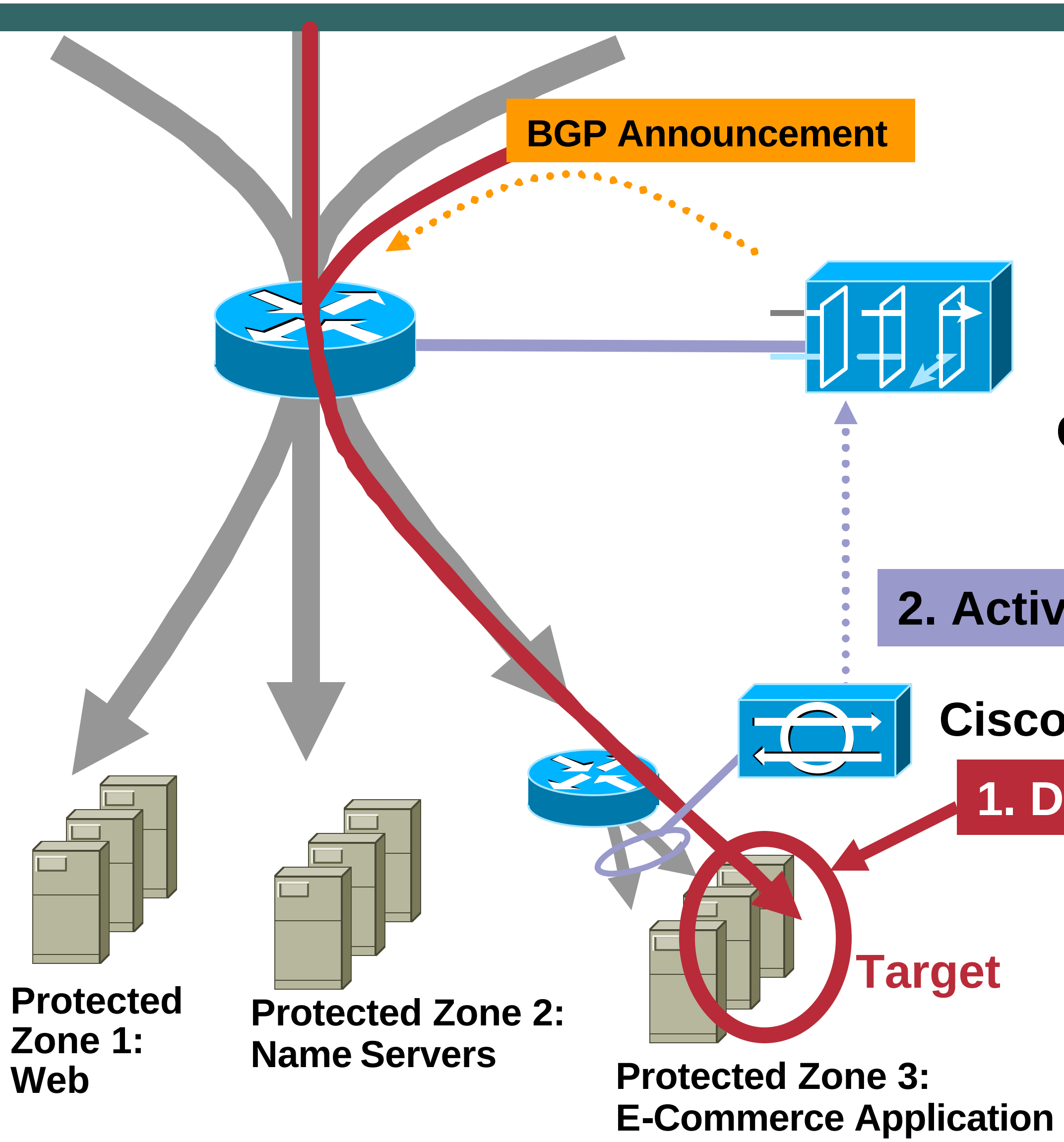
Cisco DDoS Solution: Diversion



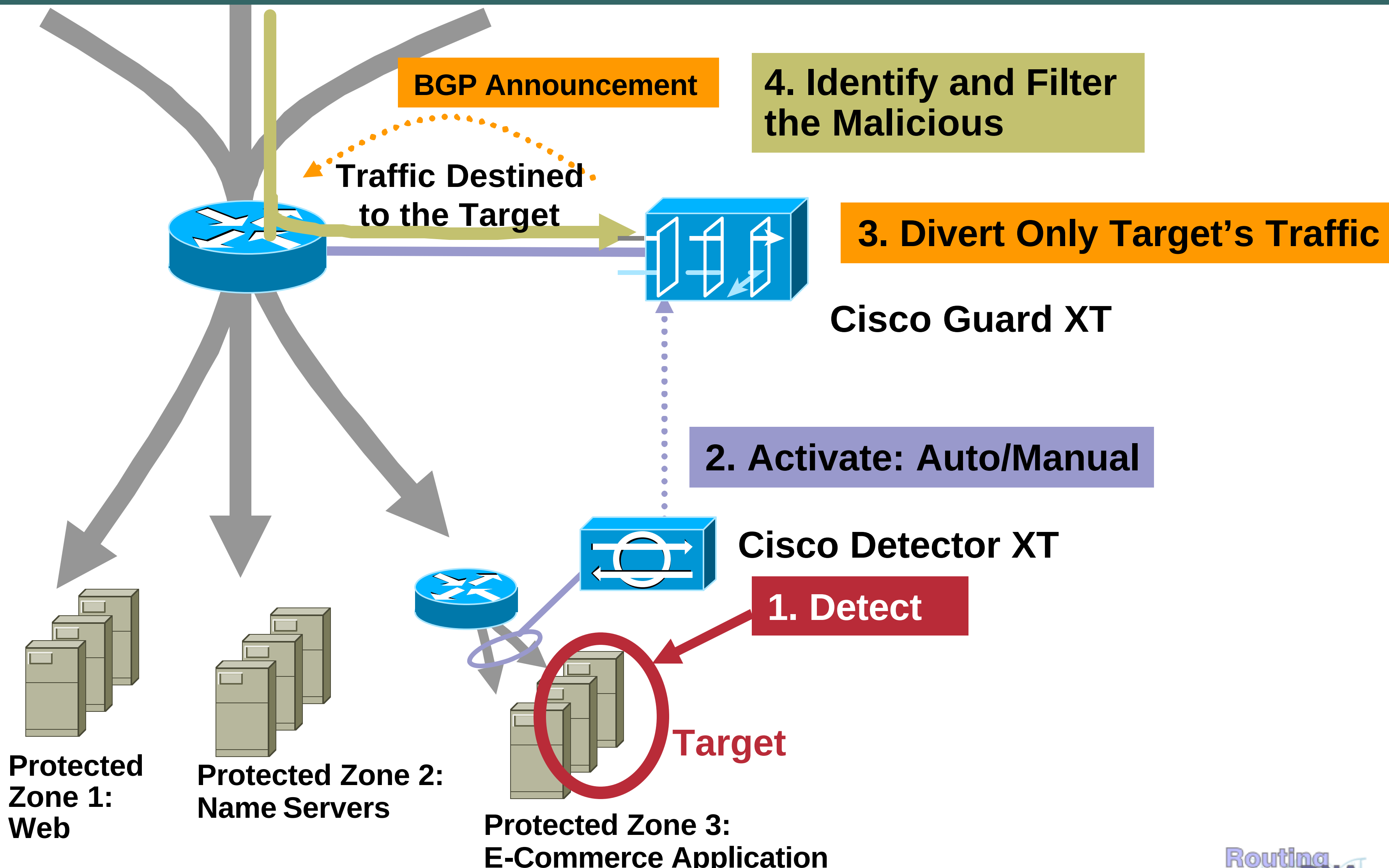
Cisco DDoS Solution: Diversion



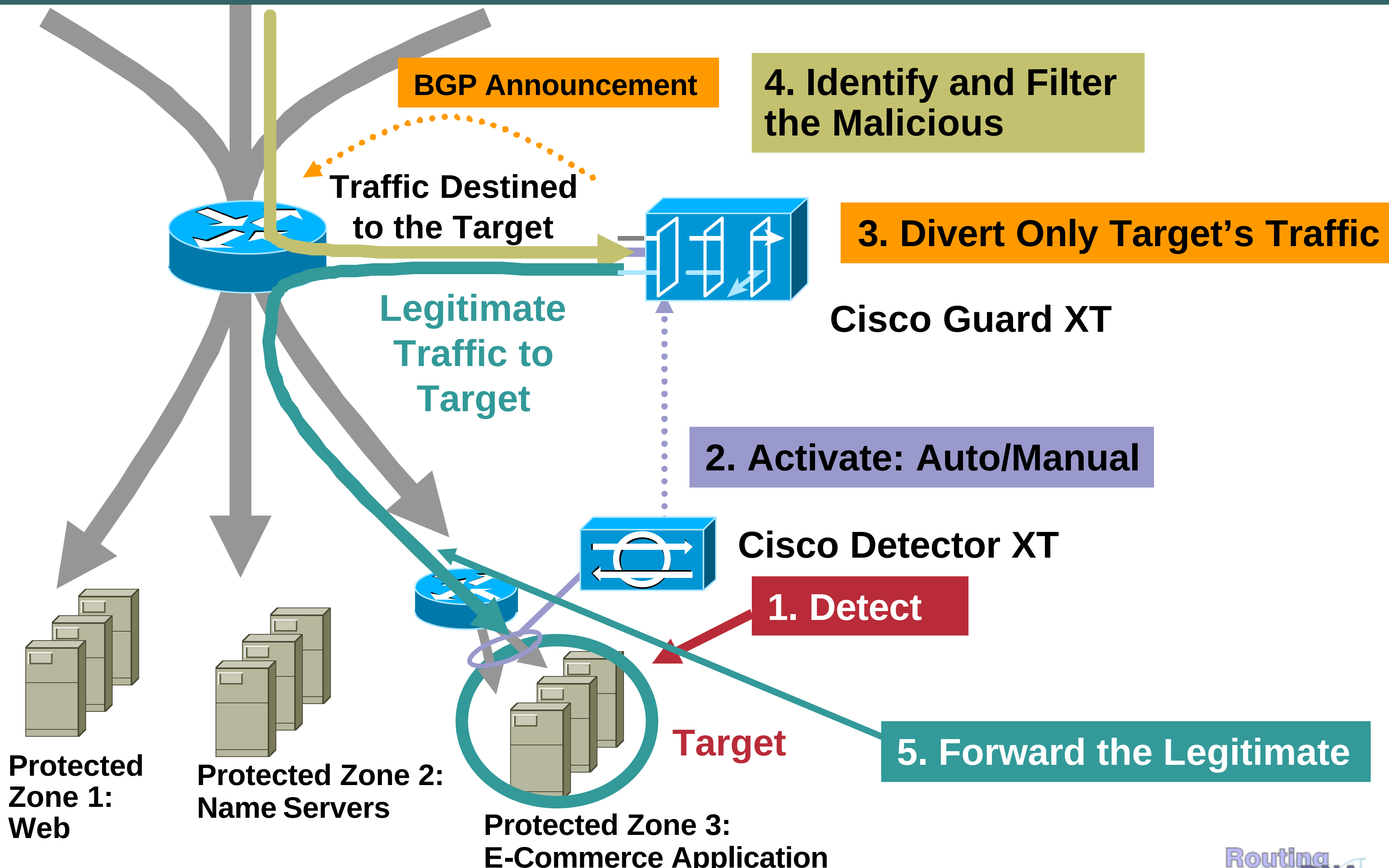
Cisco DDoS Solution: Diversion



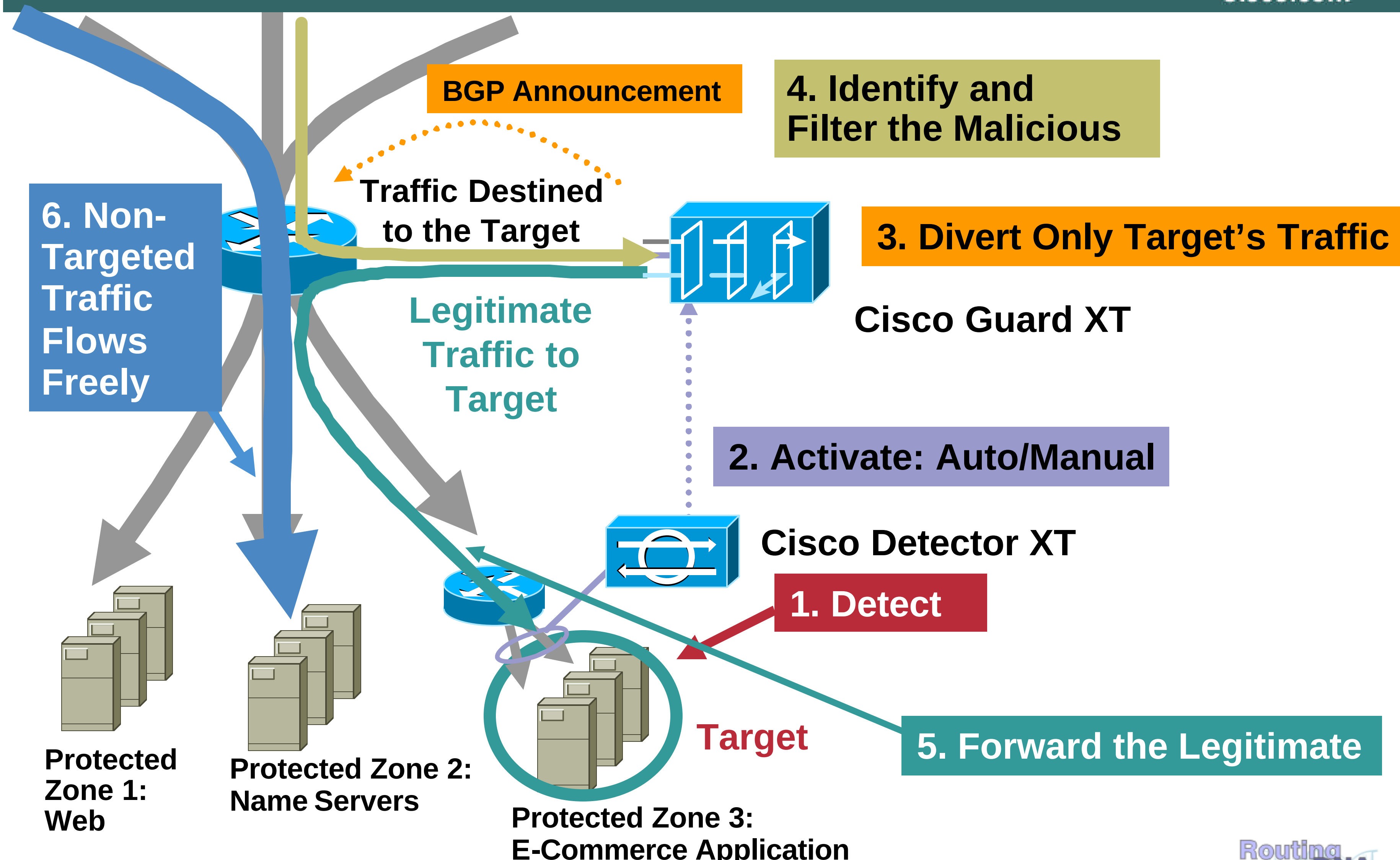
Cisco DDoS Solution: Diversion



Cisco DDoS Solution: Diversion



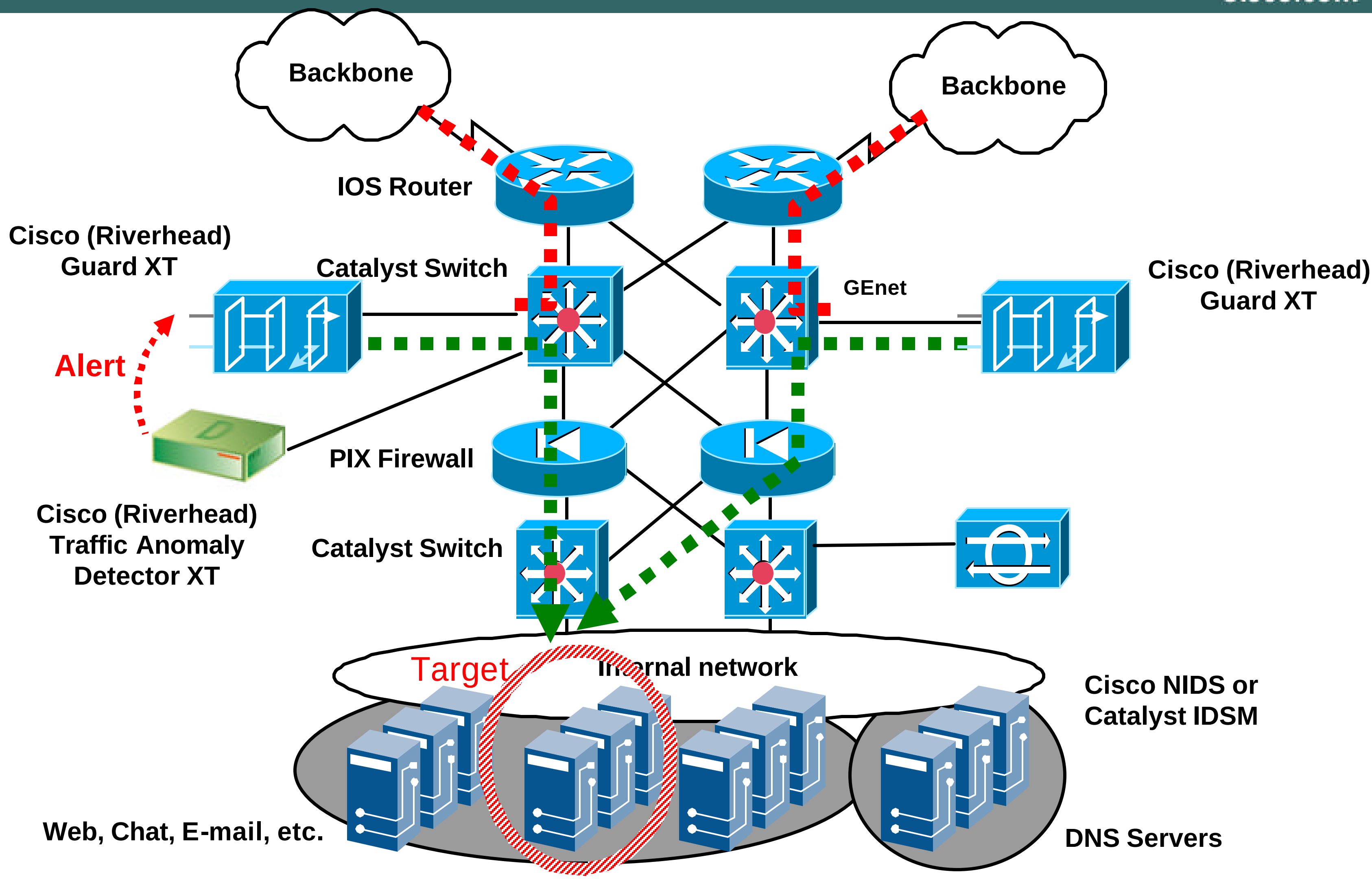
Cisco DDoS Solution: Diversion



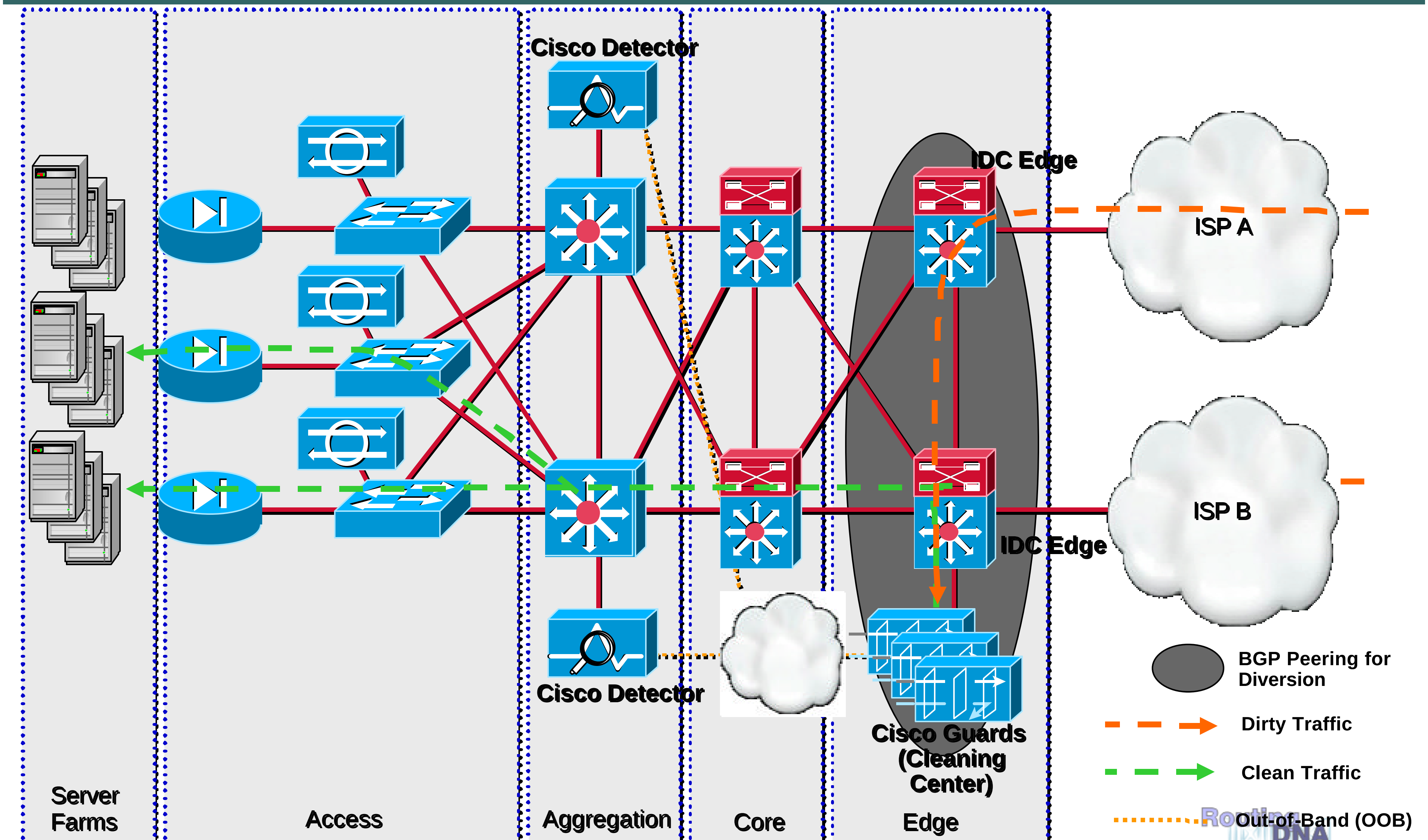
Shunts in the Datacenter

- **All Devices on the Same Subnet**
  - Either Guard driven or configured in router
  - May use remote triggered shunt trick
  - → All traffic in core to target goes to the Guard
- **Optionally, You can use VLANs to avoid loops**
  - Bypassing the “modified” router is trivial with vlans and .1Q trunking

Hosting/SP Data Center



Shunts in the Data Center

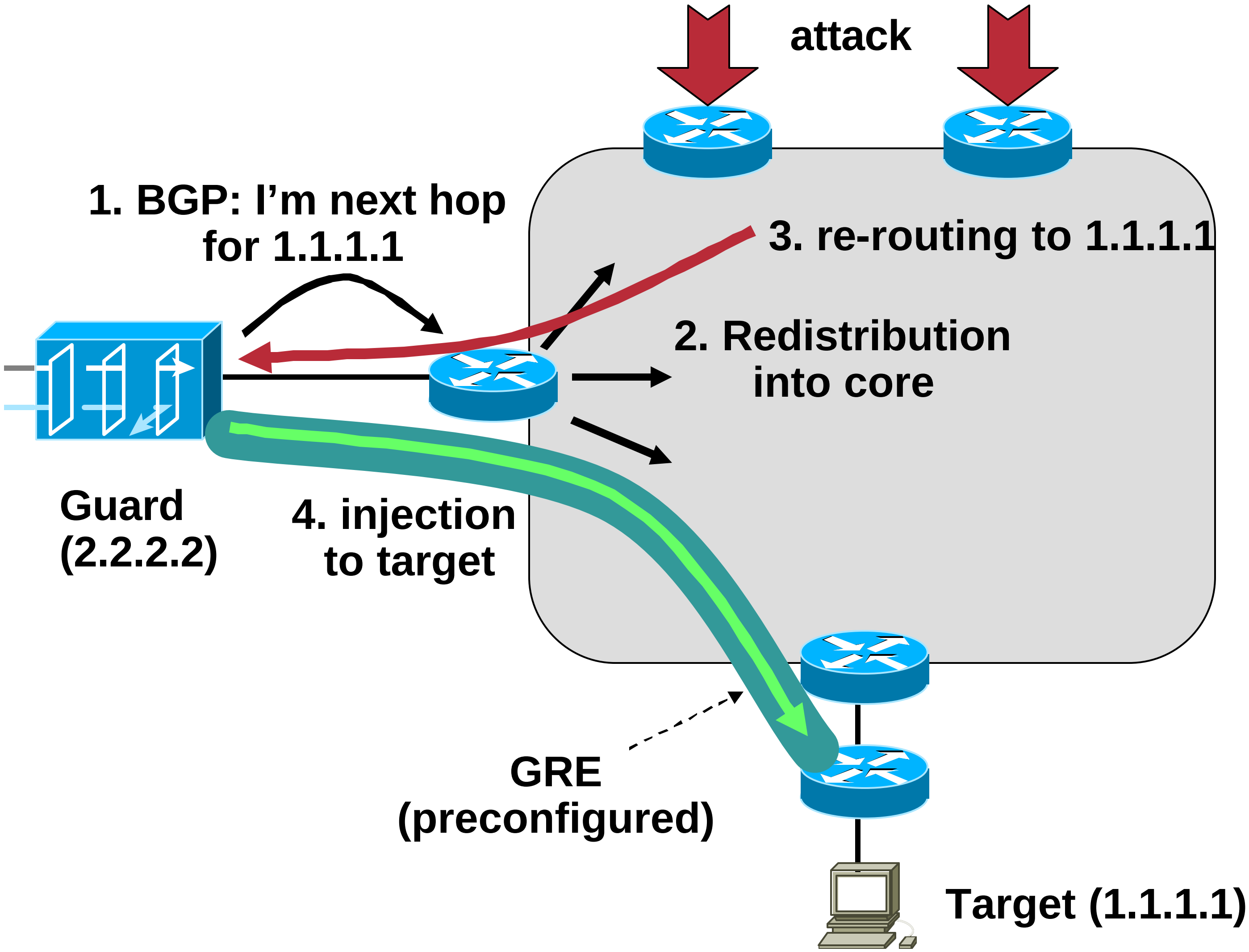


Shunts in the IP Core: GRE Injection

Cisco.com

- **Core routes target IP to the Guard**
  - Either Guard driven or configured in router
  - May use remote triggered shunt trick
  - → All traffic in core to target goes to the Guard
- **Injection into GRE tunnel**
  - Bypassing the "modified" core routing
  - GRE starts on Guard, terminates on CPE, which has "clean" routing to target

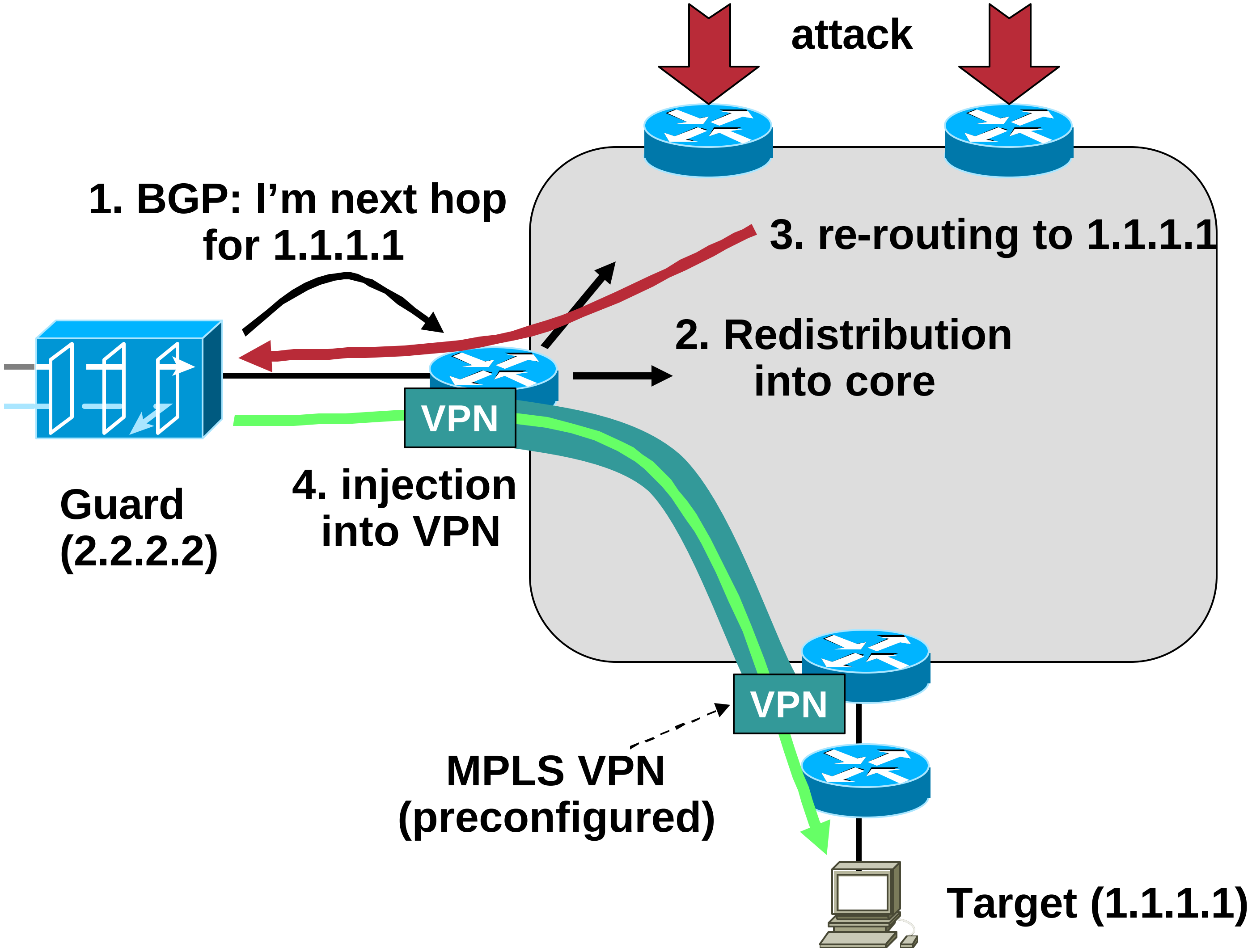
Shunts in the IP Core: GRE Injection



Shunts with MPLS VPNs

- **Easy to deploy:**
  - **Core remains untouched, injection VPN pre-configured**
  - **VPN invisible to core**
- **No performance impact**
- **No need to touch CPE**
- **But: MPLS VPN required on core**

MPLS VPN Shunt

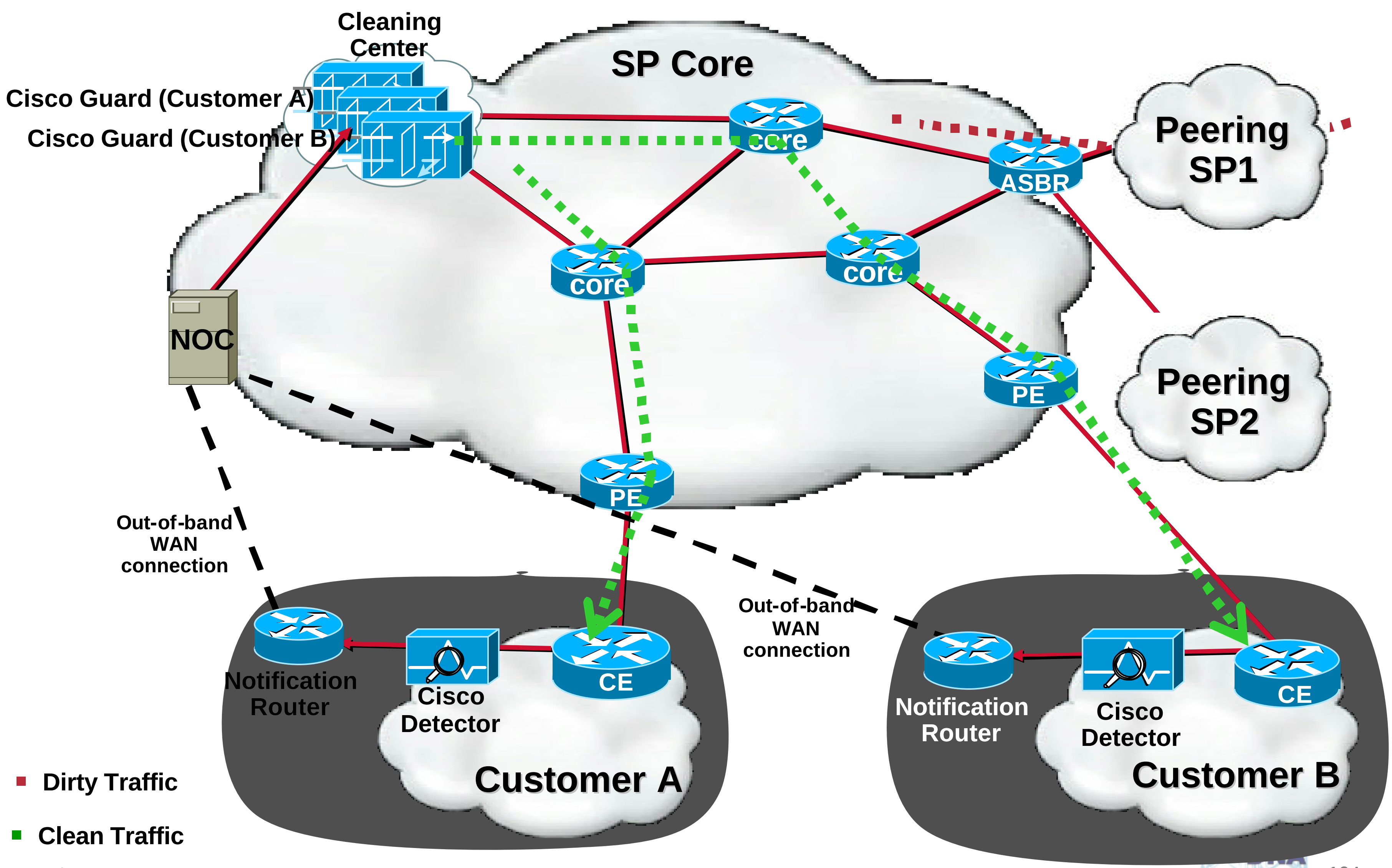


Packet Scrubbing issues

Shunting the Packets

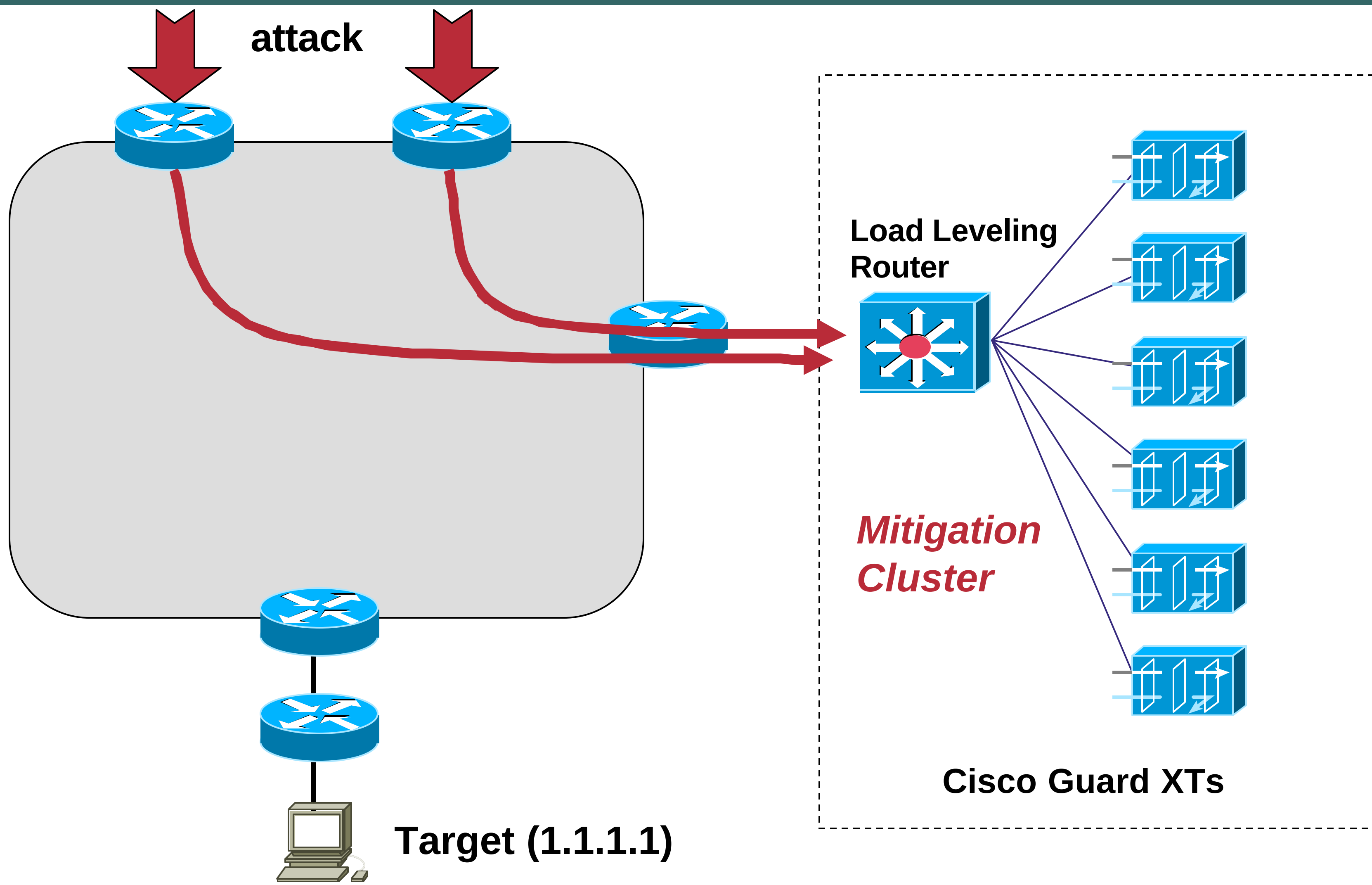
Scrubbing the Packets

Packet Scrubbing in the Core: The Cleaning Center



Scaling a Scrubbing Center: Clustering Topology

Cisco.com



Backbone Option – Scrubbing Centers

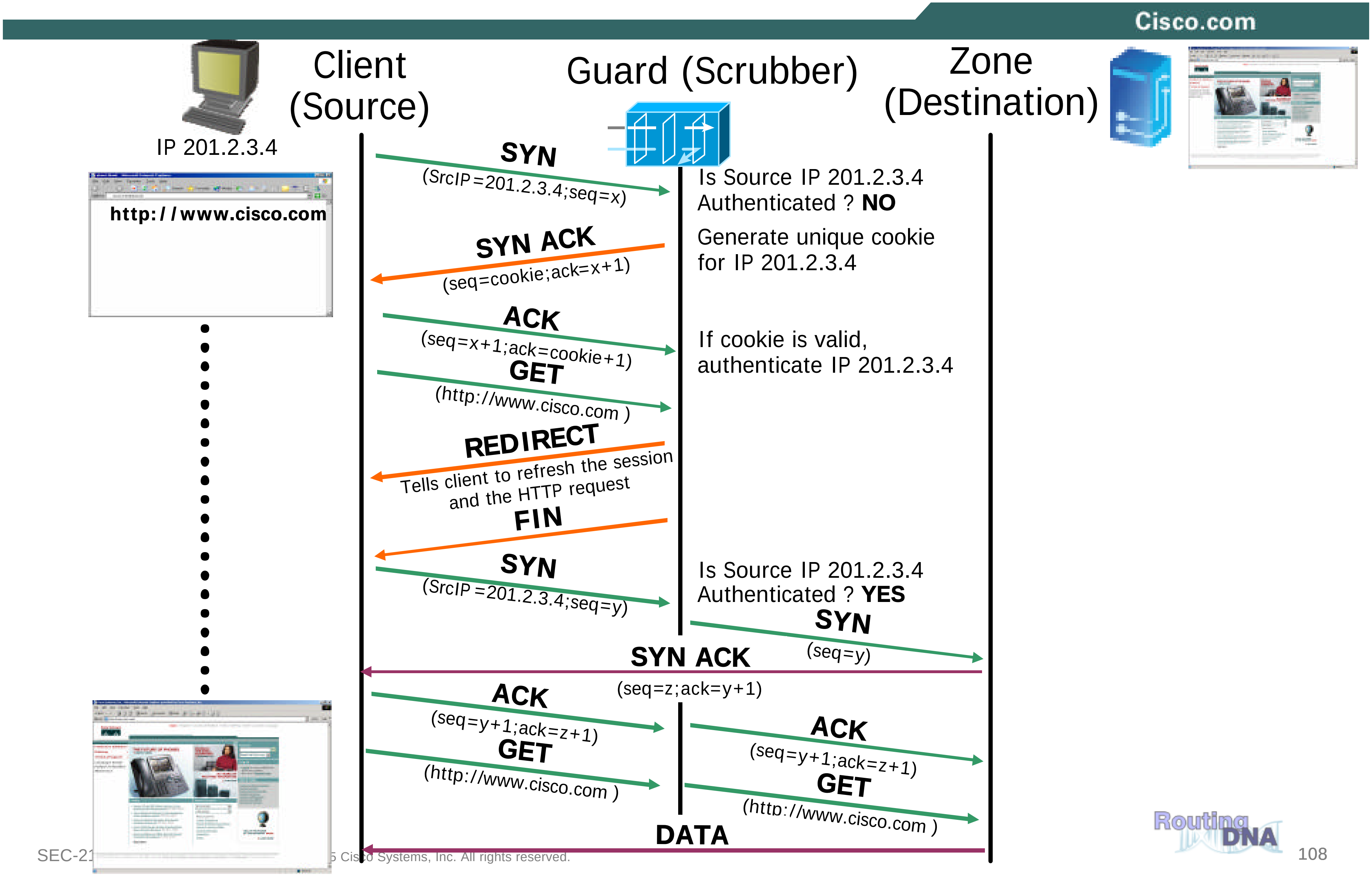
- **Question is how many**
  - **Most national providers have decided to start with two**
  - **Giographic redundancy**
  - **Adequate incoming bandwidth in key locations**
  - **Limit the backhaul of traffic across expensive links**
- **Once you decide on where, then the hard part is how many**

Packet Spoofing

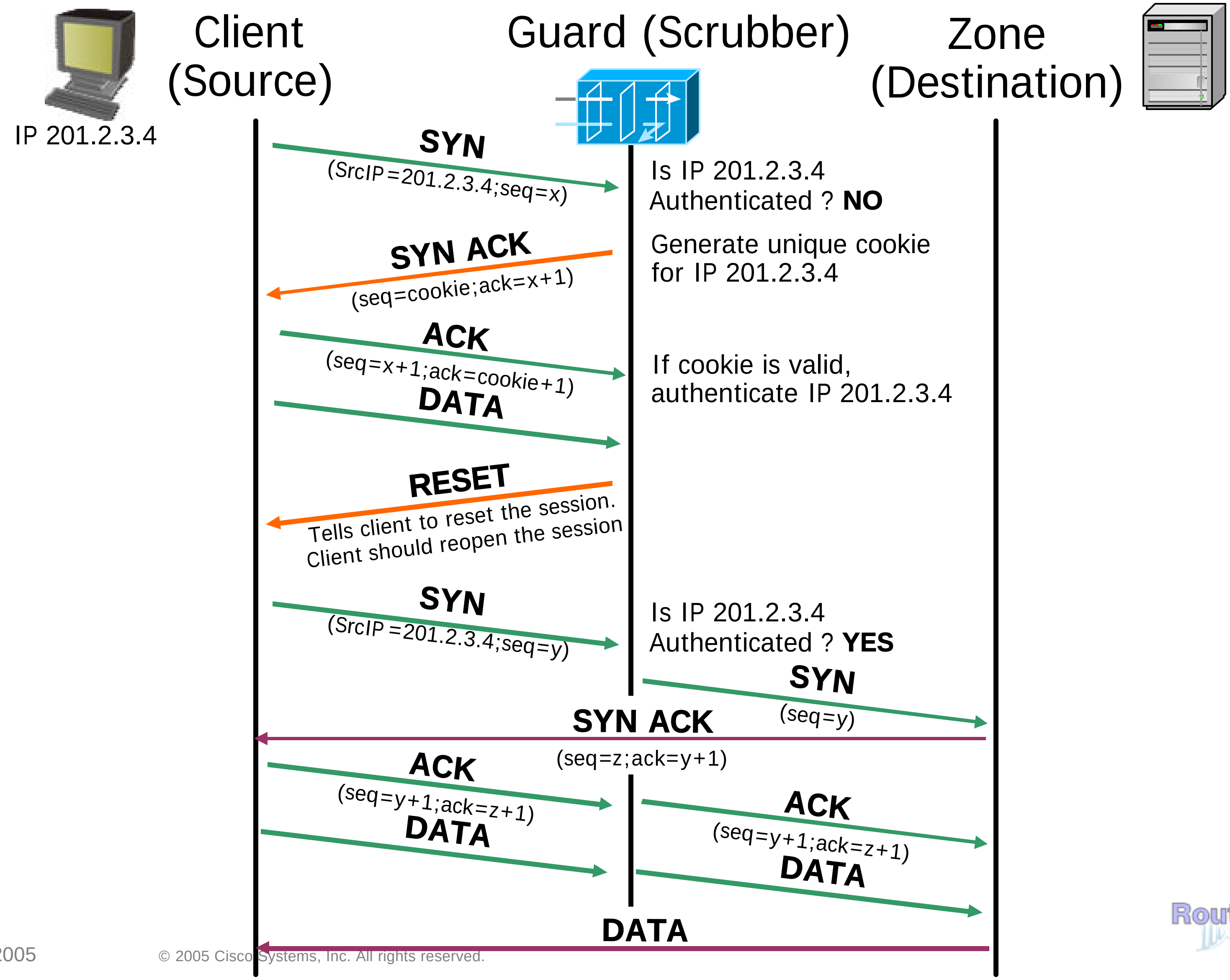
- **What can be spoofed?**
  - **Any field in an packet header! (well almost)**
  - **Spoofing most often happens in combinations with several fields being spoofed.**
- **Spoofing is used to:**
  - **Hide the source so the attacker or resource is not revealed.**
  - **Bypass Security – masquerading as valid packets.**
  - **Spoofing the real target – getting others to take out the target.**

IP				TCP				HTTP				
DST	SRC	Prtcl	CRC	Port	Port	SYN	FIN	SSL	GET	URL	CGI	www.victim.com….

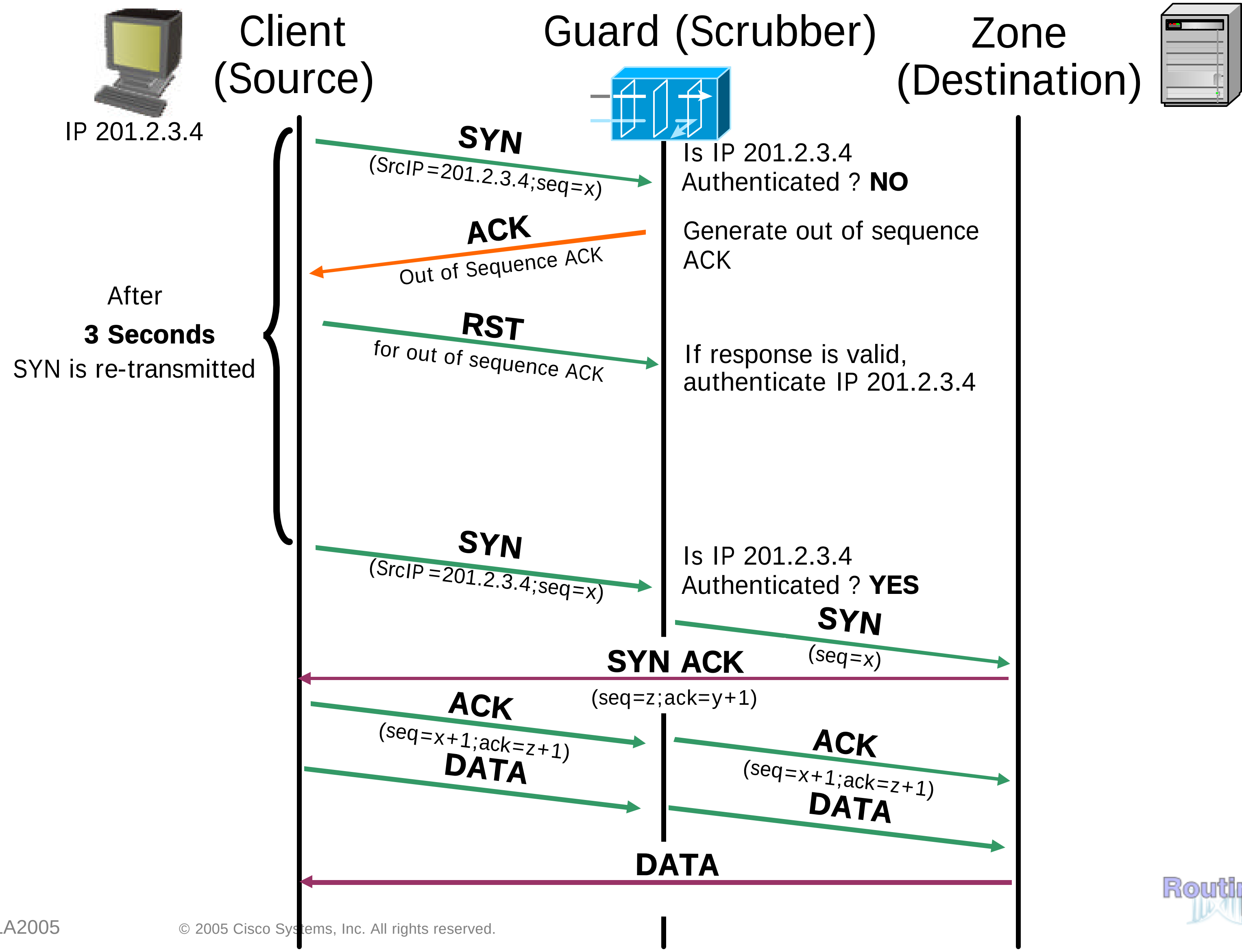
Basic/Redirect for HTTP Services



Basic/Reset for other TCP Services



Basic/Safe-Reset for Rst Sensitive TCP Services



Baseline & Learning

- Templates provide "universal" default values

  Provision closest template

- The purpose of learning is to note an anomaly from a baseline

- The strength of an Anomaly Detection (AD) system is dependant on two factors:

  First the robustness of the language used to

  Second, the quality of the baseline itself vs. the application required

- This is primarily about per source behavior!

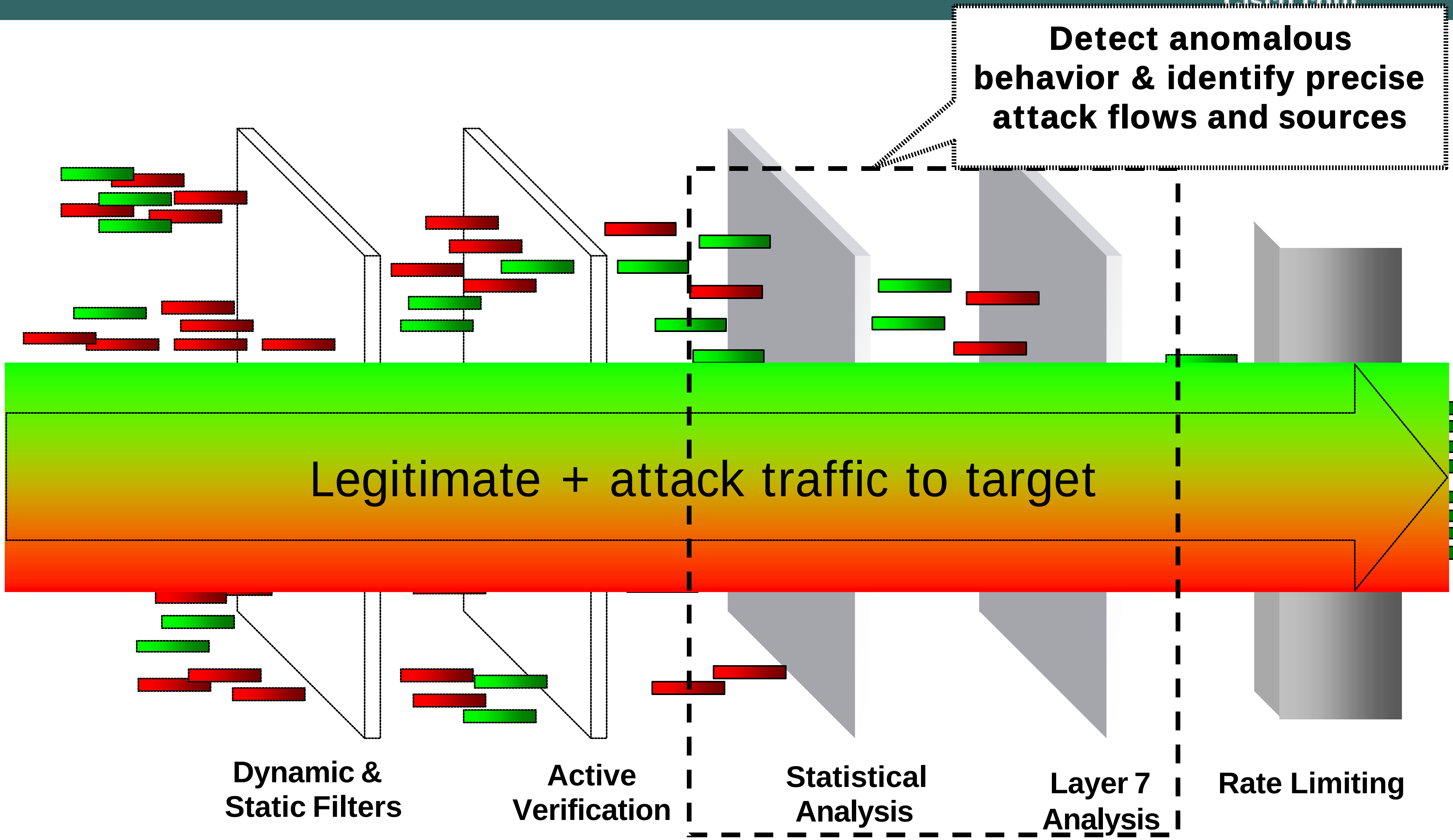
Anomaly Detection Overview

- **Extensive profiling**
  - Hundreds of anomaly sensors/victim
  - For global, proxies, discovered top sources, typical source,…
- **Auto discovery and profiling of services**
  - Automatically detects HTTP proxies and maintains specific profiles
  - Learns individual profiles for top sources, separate from composite profile
- **Depth of profiles**
  - PPS rates
  - Ratios eg SYNs to FINs
  - Connection counts by status
  - Protocol validity eg DNS queries

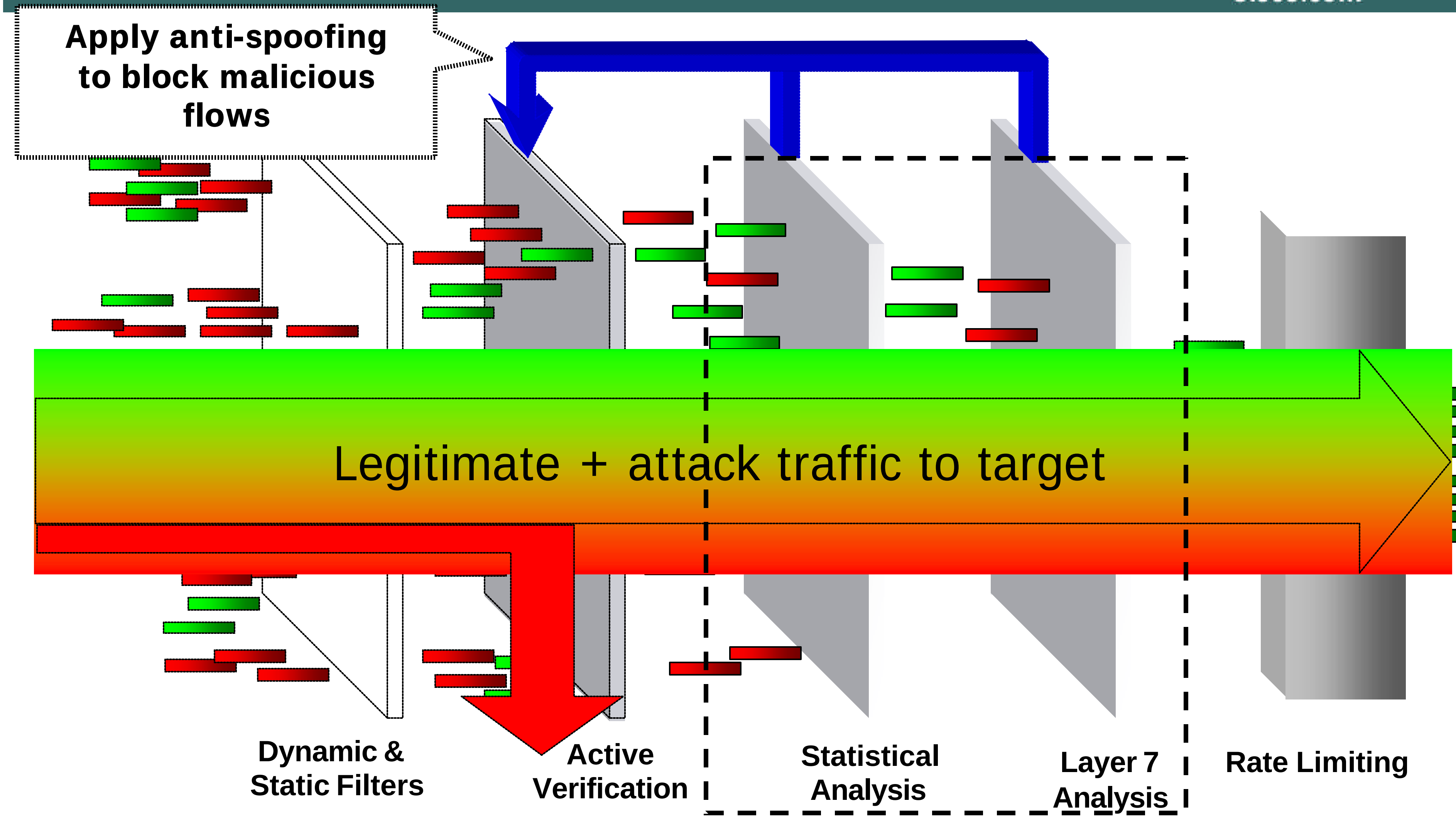
Putting all this Together to Stop DDoS

- **The core functional components of an anti-ddos packet scrubber:**
    - **Destination Detection**
    - **Source Verification (via anti-spoofing)**
    - **Source Detection (via anomalies)**
    - **Source Blocking / Filtering**
    - **Attack Termination Detection**

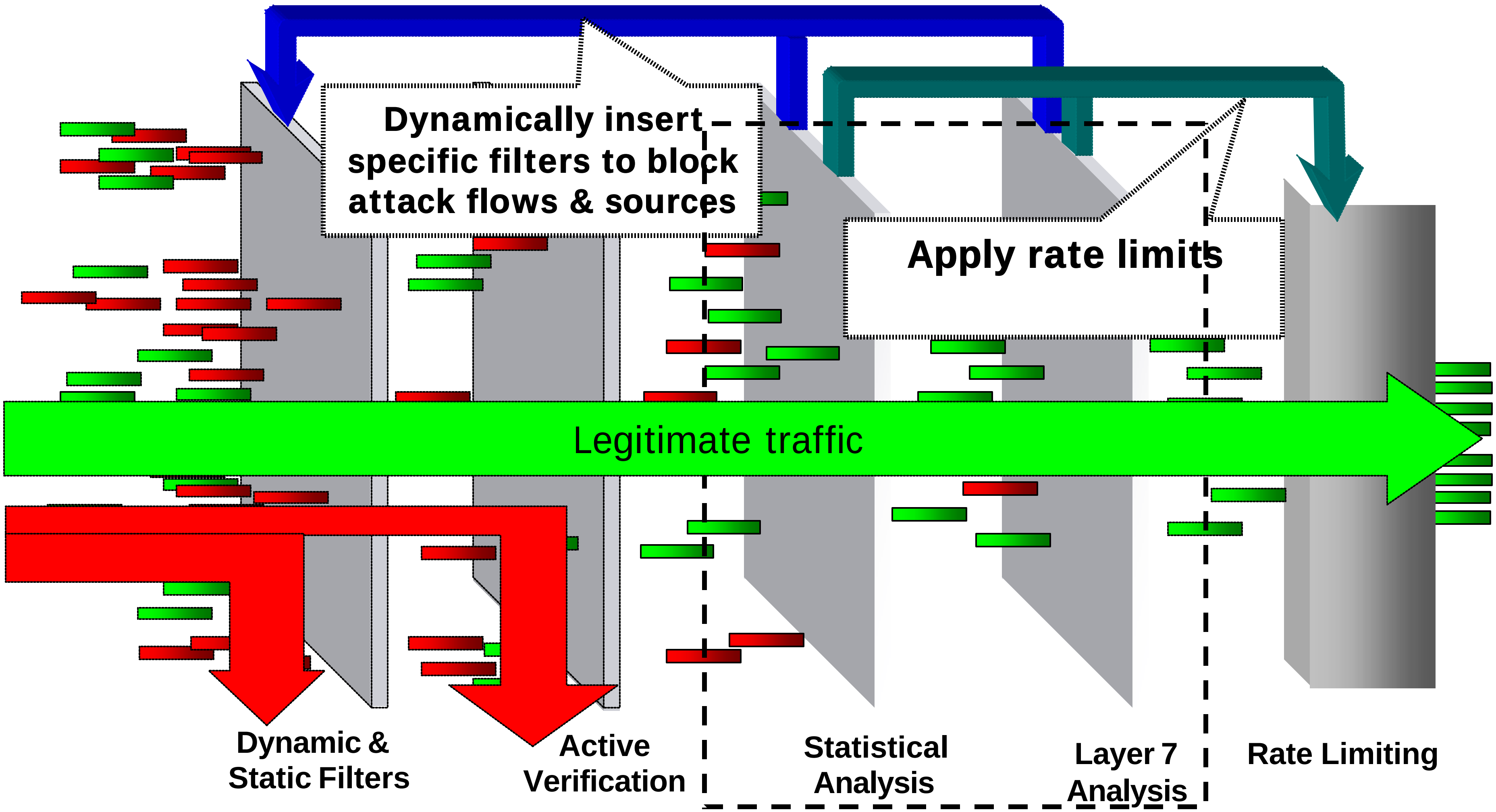
Multi-Verification Process (MVP)
Integrated Defenses in the Guard XT



Multi-Verification Process (MVP)
Integrated Defenses in the Guard XT



Multi-Verification Process (MVP)
Integrated Defenses in the Guard XT



Packet Scrubbing via Shunts

- **Advantages:**
  - Not on critical Path during normal operation
  - Anomaly based detection with base lining
  - Optimized for high performance blocking
  - Is resistant to state limitations of most other devices
- **Limitations:**
  - Not designed to stop single packet attacks
  - Enherent is an assumption of a ‘destination’ being protected
  - Resource utilization: finite resources in the scrubber complex
  - Requires up-front network engineering to implement

What We Can Do Now

- Detect DoS Attacks (SNMP, NetFlow, ACL)
- Trace back random packet floods (NetFlow, ACLs, IP source tracker)
- Shun a source (uRPF, ACL)
- Shun a destination (routing, ACL)
- Limit attacking traffic (CAR, PIRC)
- Remote trigger via iBGP
- Use BGP for security in general

Recommendations for ISPs

- **Preventative measures: ACLs, uRPF, CAR…**
  - See ISP Essentials
- **Monitor your routers and alarm on:**
  - CPU, line load, memory…
- **Use NetFlow plus collector s/w:**
  - Usage statistics, DoS detection, DoS tracing through the network
- **Be prepared:**
  - Technically: Understand the routers
  - Operationally: Have procedures in place, know your upstream/downstream contacts, have a CERT

What Will the Future Bring?

- More PCs always online (DSL, Cable)
  - The vulnerabilities are here!
  - Need quarantine and containment solutions
- More vulnerabilities and zombies?
- Better integration of detection and reaction
- Improved distinction of “good” from “bad” packets
- Increased infrastructure attacks
- More and more DoS: it pays well

Complete Your Online Session Evaluation!

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session ID: SEC-2103:

Taking Control of Your Network – Mitigating Attacks

CISCO SYSTEMS