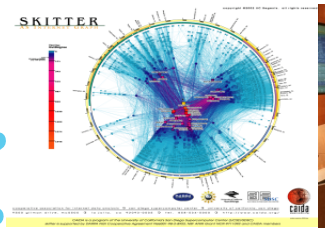
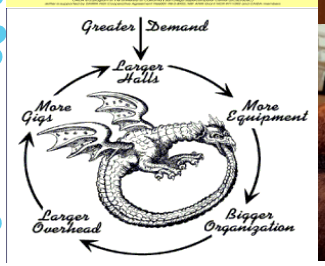
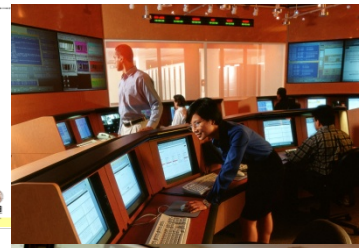
Operator's Security Toolkit Workshop – for Investigators







Operators Security Toolkit Slides & Papers

http://www.senki.org/sp-security/operators-security-toolkit/

Barry Raveendran Greene
bgreene@senki.org

Operator’s Security Toolkit – for Investigators

This workshop reviews the tools and techniques that Operators use to mitigate, remediate, and investigate ”activities” on the Internet.

The goal is to provide a understanding of how Operators think, operator, and interact with each other.

This understanding would better help “Law Enforcement” Investigators more effectively interact.

Agenda

- Understanding the “Operator’s World”
- How to Respond to DOS Attacks (Operator’s POV)
- Core Principles of Why the Internet Won
- Threat Actors – How Operators View Threats
- The Operator Security Toolkit
- Deep Dive Sessions
  - Remote Triggered Black Hole – the Foundation
  - Sink Holes
  - BGP Hijacking
  - Can Vendors ever Provide “Secure” Solutions?
  - DNS Security
- Pressing Questions

Why is this important?

- 1994 – SingNet – the first Commercial ISP in Singapore.
  - No SingNet Security Team
  - No Corporate Security Team
  - Landing in a know threat zone (Triads in Hong Kong)

- Advantage – Singapore's Attitude and a brand new Computer Misuse Act

SingNet's Original Security Plan

1. Designate one engineer/architect - Leona Leong - to be our "CISCO." Sent her to IETF to work with Barbra Frasier (CC-CERT) to work on the IETF Site Security Handbook.
2. Designated our Weekend Red Team/Blue Team ½ day exercises. We started with Alt2600 & Phrack Magazine.
3. We call the Singapore Police Team who does the "Computer Misuse Investigation."

Then things got interesting ….

1994 Singapore Computer Investigative Team

- When the 1994 Computer Misuse Act was passed, there was not foresight to pass a budget for the police investigators who would enforce the act.

- SingNet really needs the police for when they will get attacks. It is not a matter of “if,” it is always a matter of <u>when.</u>

- Think out of the box ……

SingTel's "Investment"

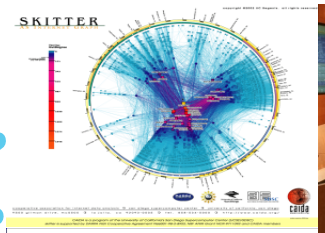
- In consultation with Singapore Telecom's Legal Team, there was no barrier to:
  - Granting SingTel badges for the Investigator for the SingNet Com Center
  - Set up two cubes for them with Computers, Printers, high walls, and 7x24 access to the Internet.
  - Access to any of the staff to help them learn everything they need to know about the Internet
  - Joined in several our Red Team/Blue Team exercises.

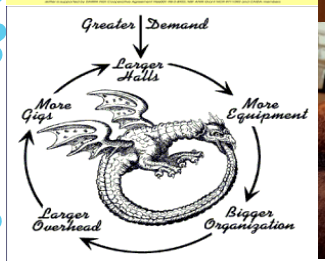
Investment Payoff

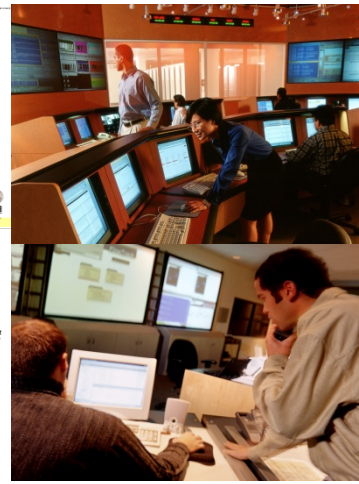
- Two months later we identified a break into our E-mail systems. Working together with the Singapore Police – caught, arrested, and taken to court.
- LKY “Spoofed Lectures” to Taiwan on USENET (the original Social Media). Caught, Arrested, and taken to court.

- Maintained a health relationship until 1997 (when Leong and Barry left).

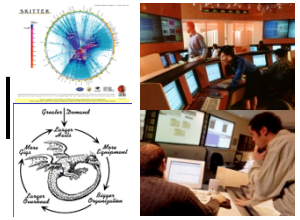
Private to Private Collaboration







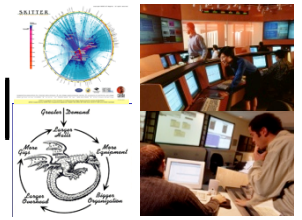
NSP-SEC



NSP-SEC was created by several ISP/SP Security Engineers as a means to meet the following objectives:

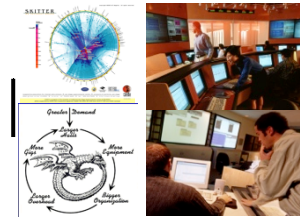
1. Provide a means for ISP/SP Security Engineers to find their colleagues.
2. Create a potential forum for ISP/SP Security Engineers to work on DOS attacks, Incidents, and other activities.

Finding their Colleagues was the Key



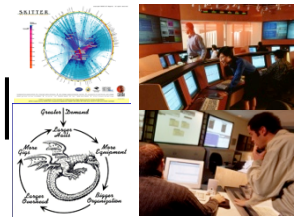
- We know that:
  - two engineers working together to mitigate an incident is more effective than one engineer working alone.
  - incident mitigation is faster if engineers can communicate with each other during an incident.
- NSP-SEC provides that means to find colleagues and perhaps – work on the incidents.
  - It is not the exclusive mode of collaboration. “Point to Point” collaboration outside of NSP-SEC does happen and is strongly promoted.

NSP-SEC – The Details



- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- NSP-SEC “hides in plane sight – where anyone interested can find, but not be privy to need to know consultation/actions
  - http://puck.nether.net/mailman/listinfo/nsp-security

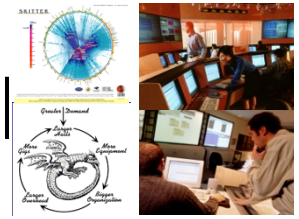
NSP-SEC Membership Requirements



Membership in nsp-sec is restricted to those actively involved in mitigation of NSP Security incidents. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP Security incidents. That means no press and (hopefully) none of the "bad guys.“

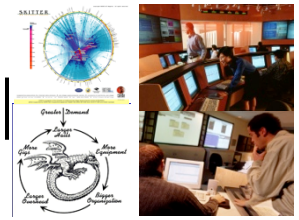
http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC Membership Requirements



- Being a “Security Guru” does not qualify for NSP-SEC Membership.
- Being “from the *Government*” does not qualify for NSP-SEC Membership.
- You need to be someone who *touches* a router in a ISP/SP backbone, can tell someone to *touch* a router, offer some *service* to the forum, or develop BCPs for the community.
- NO LURKERS! If you do not contribute, you get punted off.

NSP-SEC: Daily DDOS Mitigation Work

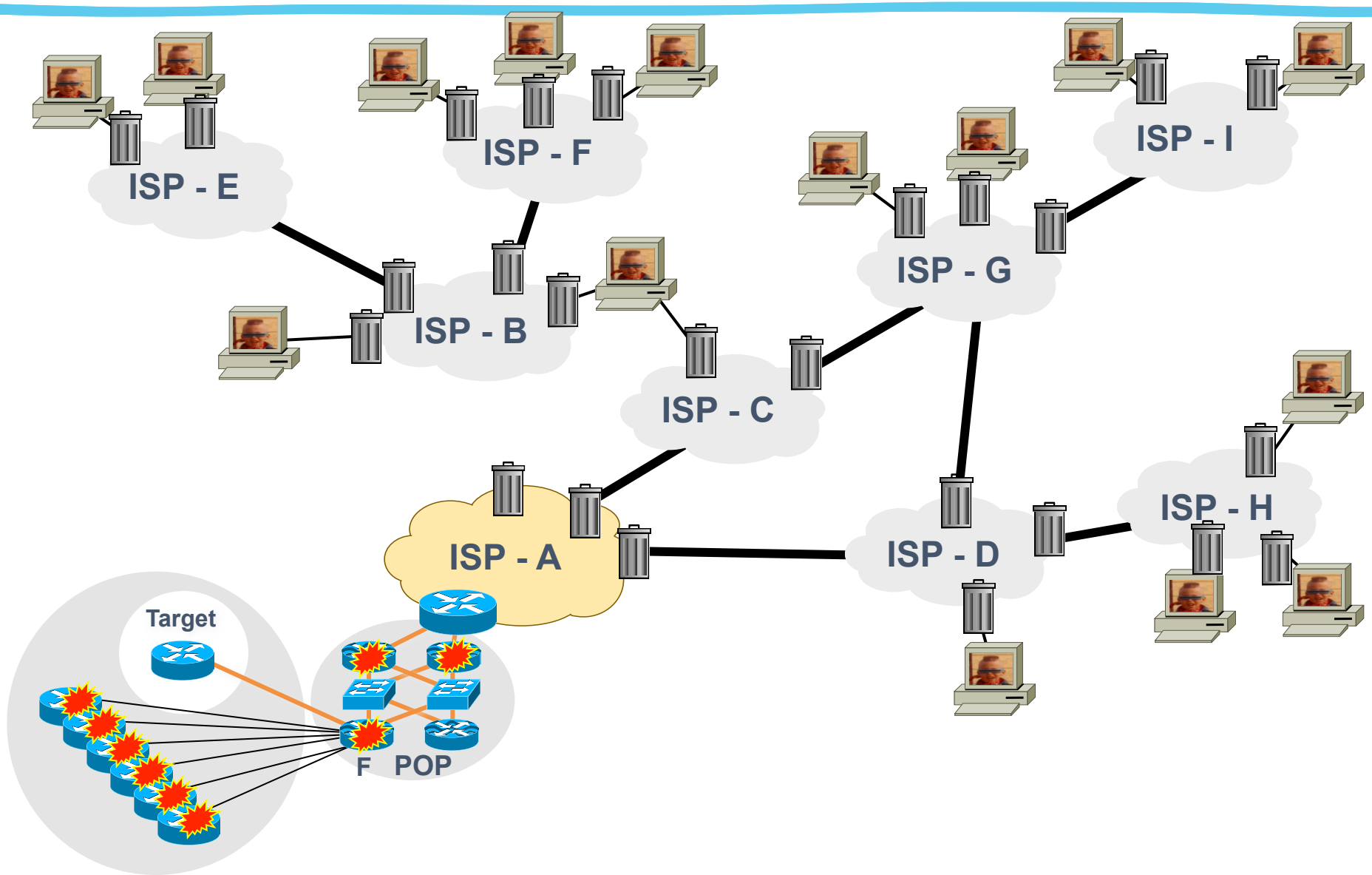


I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

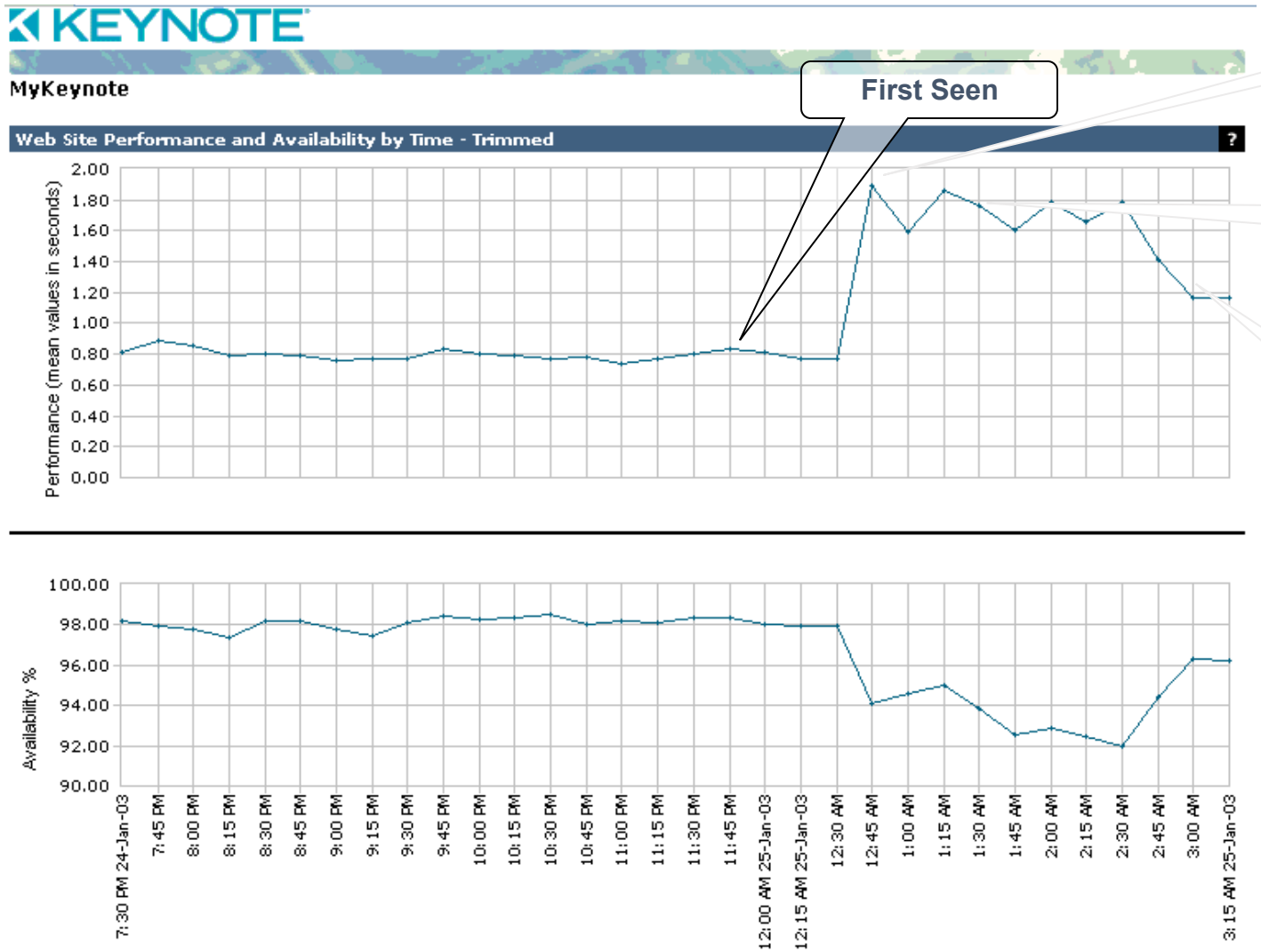
NSP-SEC: Daily DDOS Mitigations



NSP-SEC's Role during Slammer (2003)

- The ISPs were the first to notice something was happening.
  - Circuits saturated, routers spiking, BGP sessions flapped, and customers complained.
- NSP-SEC was the first reporter of the worm. CERT/FIRST Teams got their alert from NSP-SEC.
- NSP-SEC members were the ones who dump the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm.

Impact of NSP-SEC's Containment



First Seen

Real Impact

Containment Starts

Containment Takes Effect

4:00 a.m. PST Containment

In the Skitter Core

NSP-SEC Capabilities & Capacity

- Industry wide Remote Triggered Black Hole
- Industry Wide BGP Response
- Industry Wide Sink Holes
- Mix capability of Backtracing

- Service Level Agreement (SLA) is the driving factor for the NSP-SEC Community

NSP-SEC is not ….

- NSP-SEC is not perfect
- NSP-SEC is not to solve all the challenges of inter-provider security coordination
- NSP-SEC is not the *ultimate solution.*
- *But, NSP-SEC does impact the security of the Internet:*
  - Example: Slammer

Today, NSP-SEC is narrowly focused. Multiple Trust Communities have been created using the principles, where today we have a diverse and functional matrix of “Operational Security Trust Groups.”

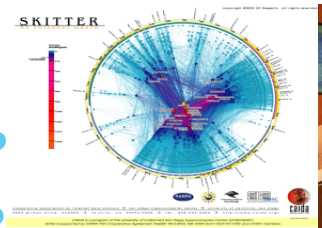
Cyber Strategy of Action (2012)

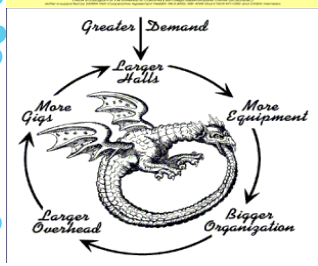
- **Private-to-Private Collaboration with Public participation.** Public policy around the world needs to facility the flexibility of private industry to collaboration with each other and with global public partners – moving beyond National constraints.

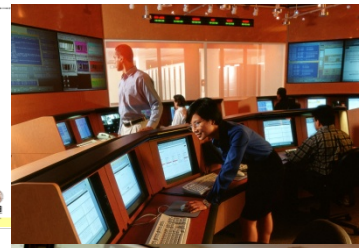
- **Public – Private Partnership activities need to optimize around private industry flexibility, clarity, and action**. Models like NCFTA are successful because of the interface with aggressive Private-to-Private Collaboration Communities. **We know this works through our results.**

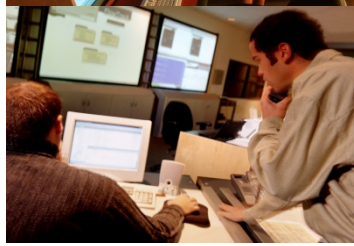
Ask Questions & Interrupt

Putting the Tools to Work – DDOS Attack





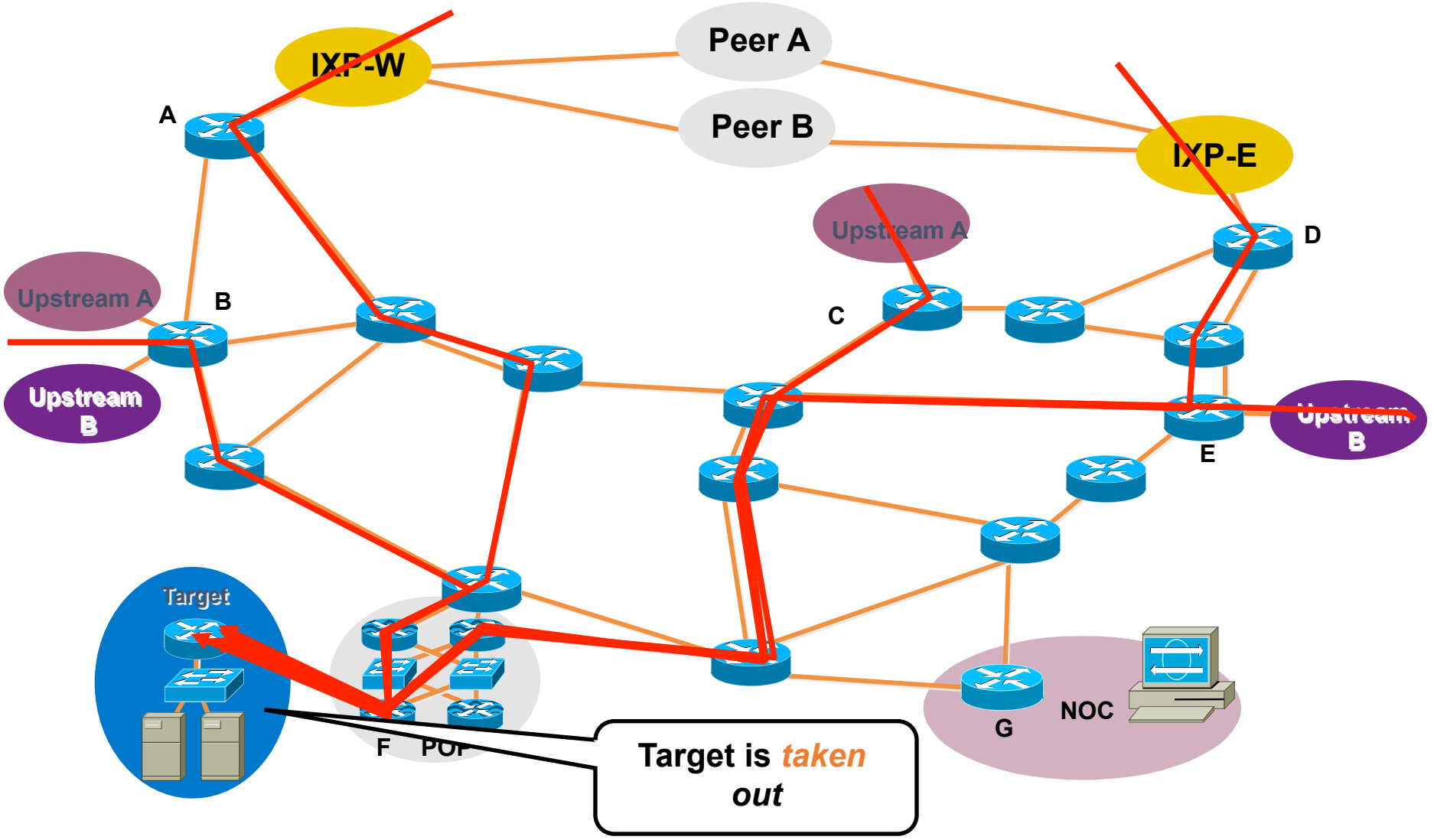




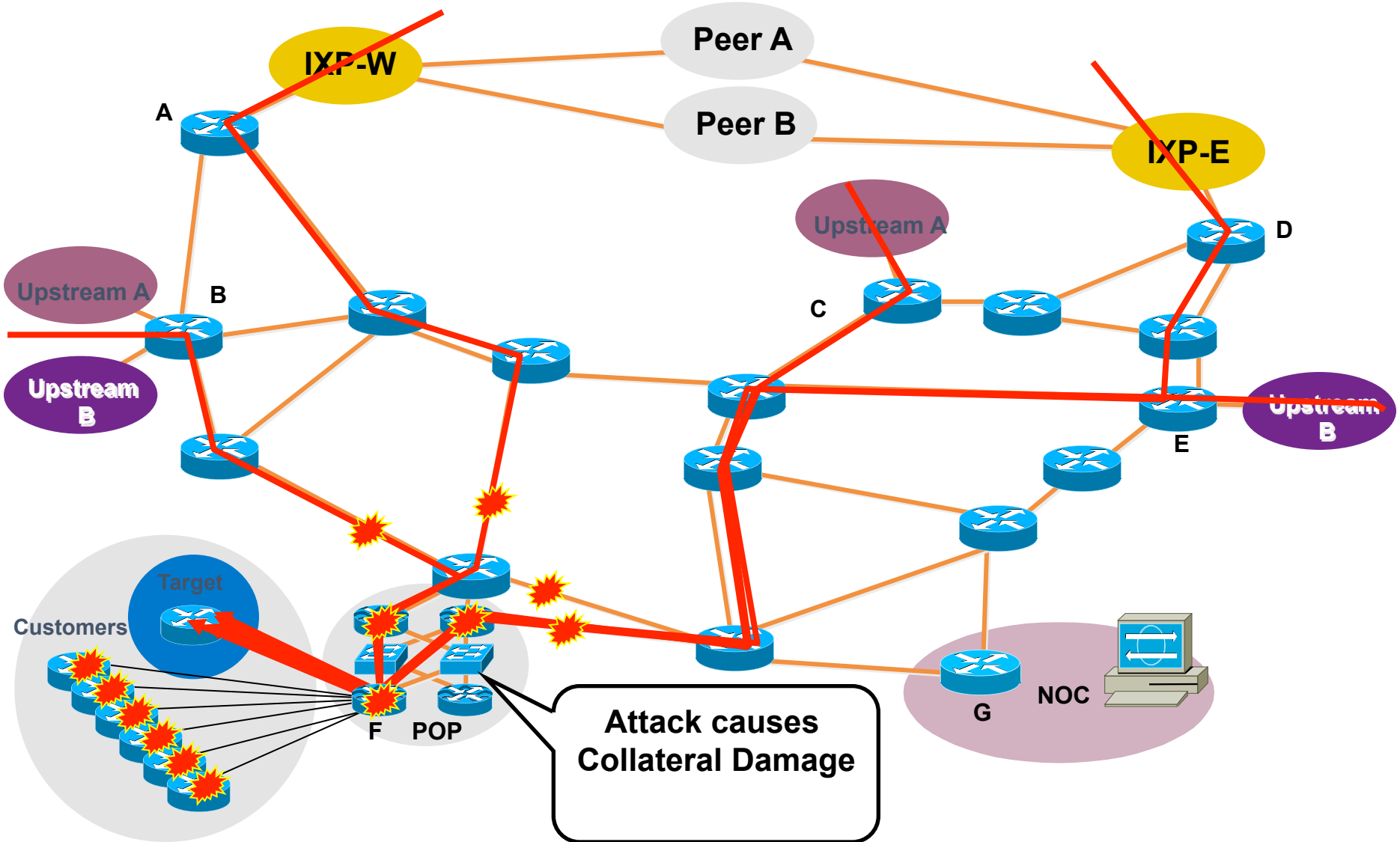
SITREP

- Everything is normal in the Network.
- Then alarms go off – something is happening in the network.

Customer Is DOSed—Before



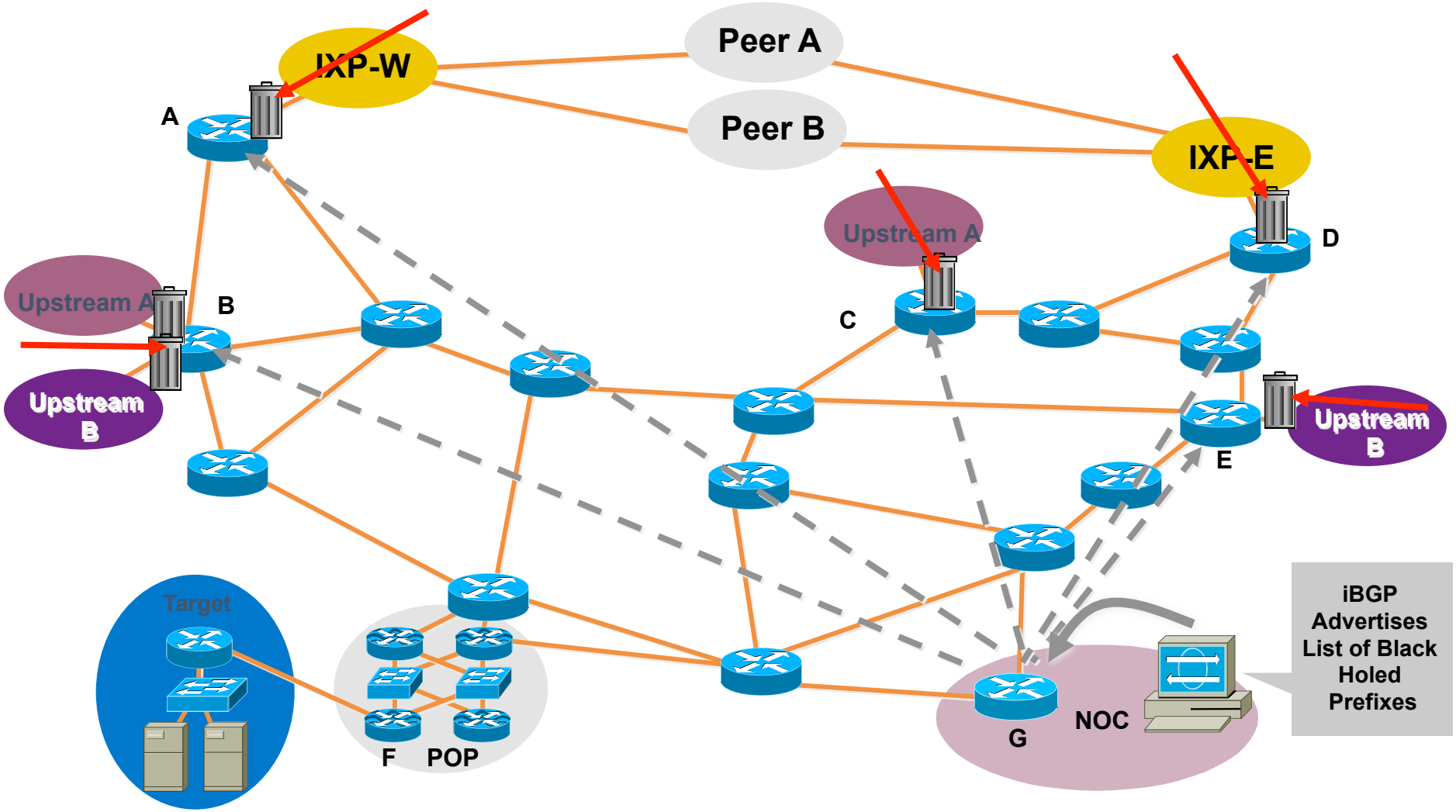
Customer Is DOSed - Before - Collateral Damage



SITREP – Attack in Progress

- Attack on a customer is impacting a number of customers.
- COLATERAL DAMAGE INCIDENT!
- Immediate Action: Solve the Collateral Damage issues.

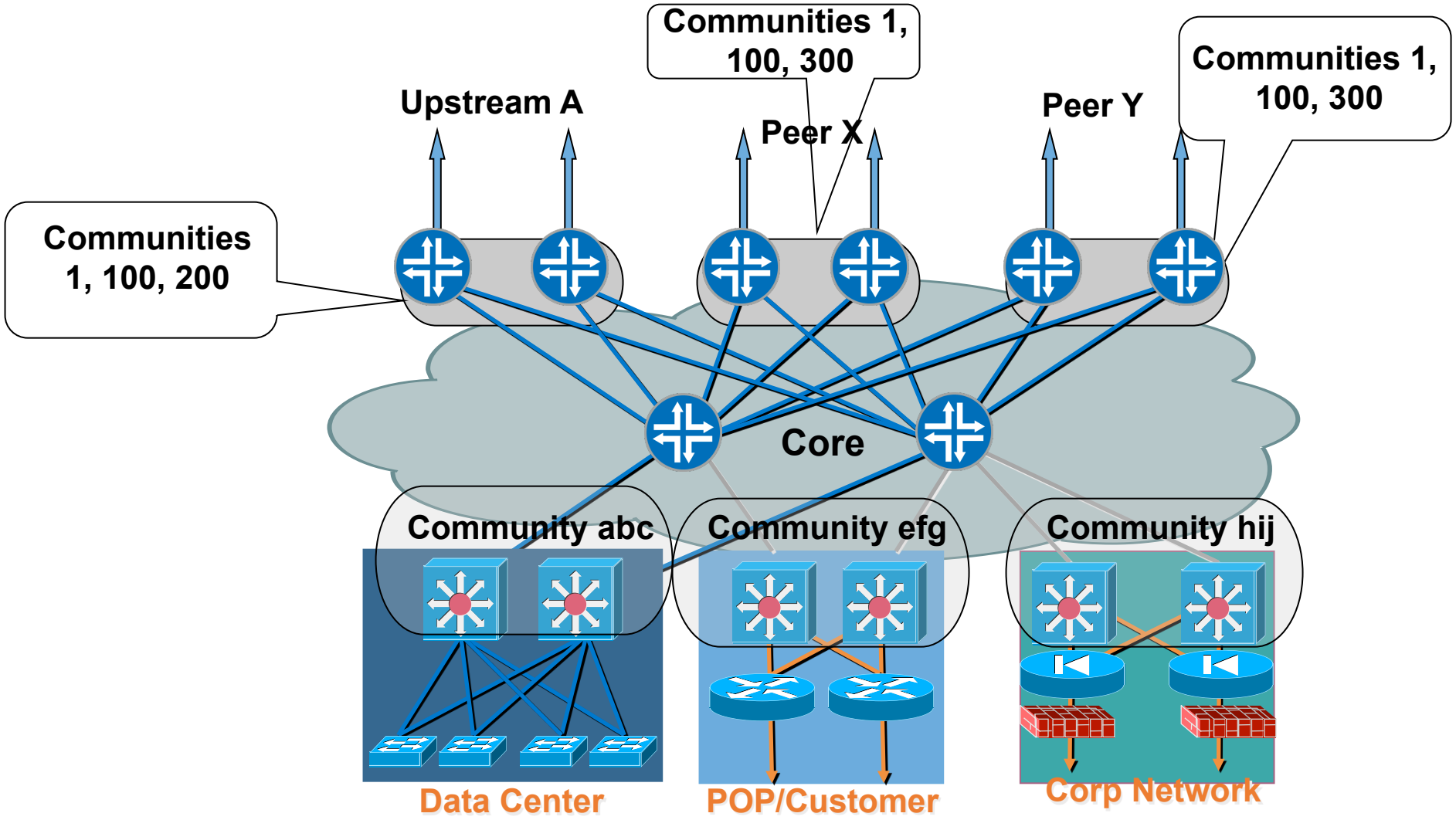
Customer Is DOSed—After—
Packet Drops Pushed to the Edge



SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Options:
  - Sink Hole a part of the traffic to analyze.
  - Watch the DOS attack and wait for Attack Rotation or cessation.
  - Activate “Clean Pipes” for a Full Service Recovery.

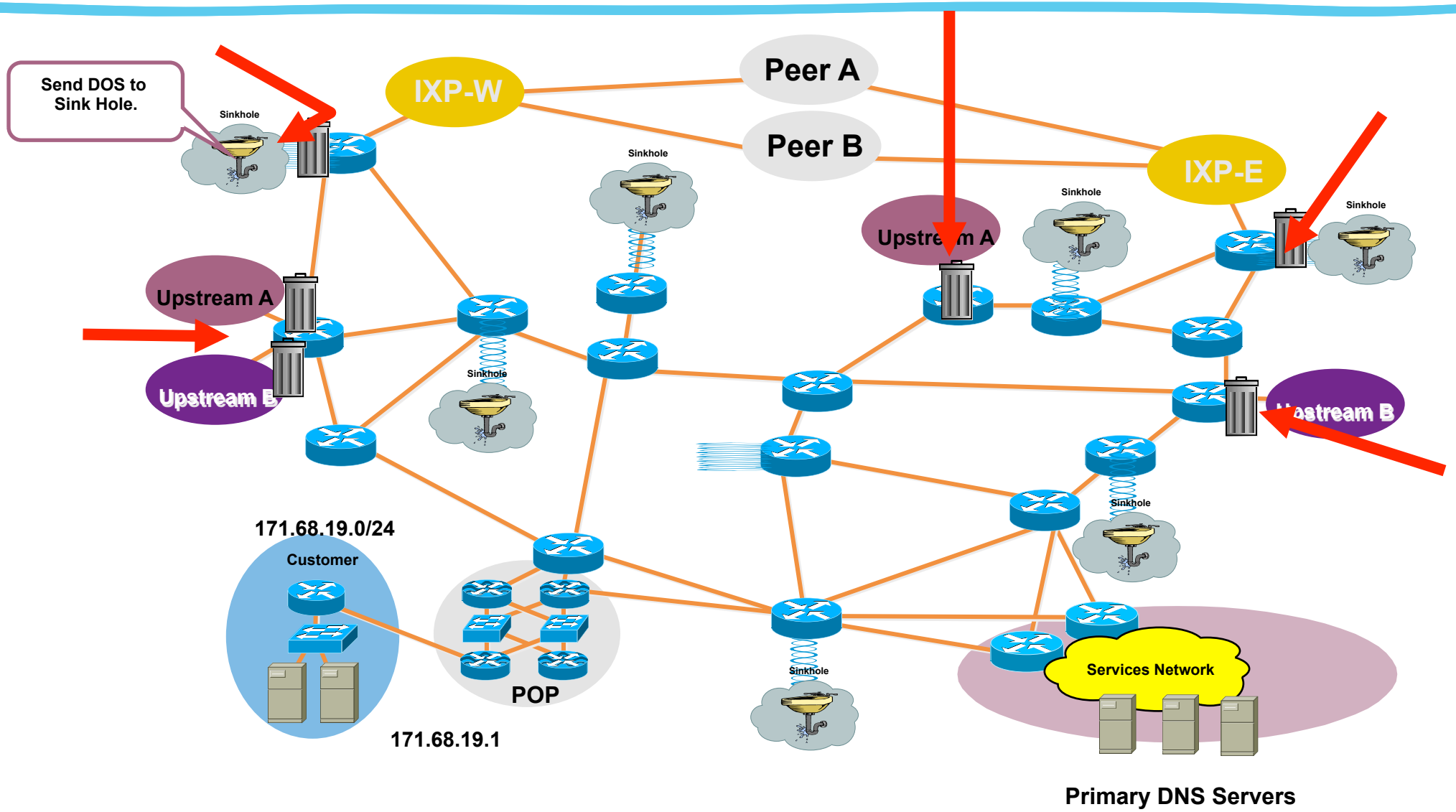
Remote Triggered Drops & BGP Communities



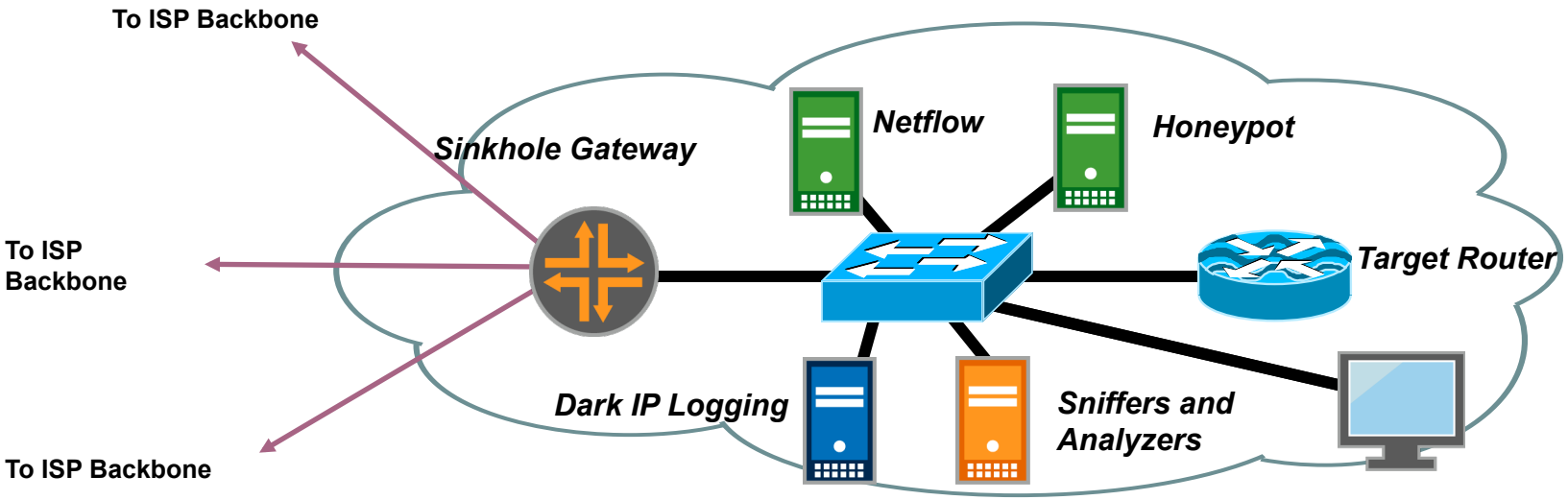
SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Monitor the Attack & Get more details on the Attack – Use BGP Community based triggering to send one regions flow into a Sink Hole

BGP Community Trigger to Sinkhole



Analyze the Attack



- Use the tools available on the Internet and from Vendors to analyze the details of the attack.
- This will provide information about what you can or cannot do next.

SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Provide the Customer who is the victim with a Clean Pipes FULL SERVICE RECOVERY (off to vendor specific details).

What is Full Service Recovery

- “Clean Pipes” is a term used to describe *full service recovery*. The expectations for a full service recovery is:
  - DDOS Attack is in full force and ALL customer services are operating normally – meeting the contracted SLA.
  - The Device used for the full service recovery is not vulnerable to the DDOS & the infrastructure is not vulnerable to collateral damage.
- Full Service Recovery/Clean Pipes products are very specialized. Talk to the appropriate vendor.

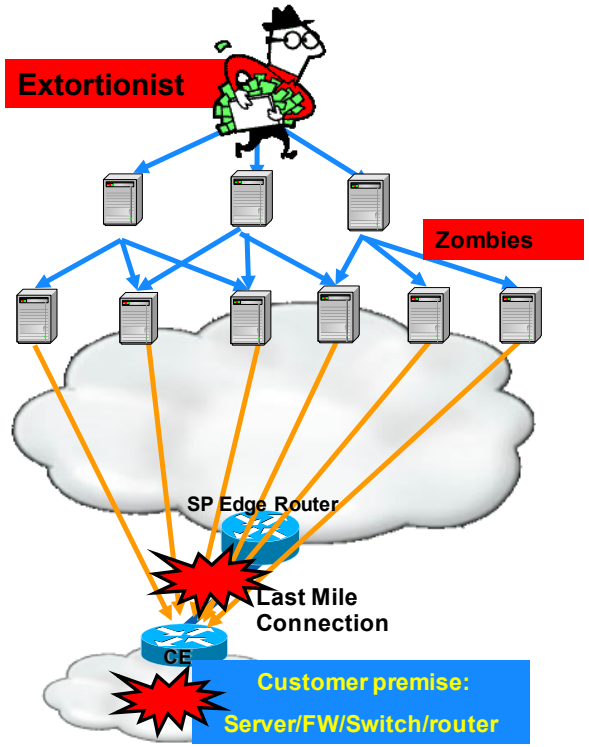
Full vs Partial Service Recovery

- Partial Service Recovery is easy … push back the attack to the ASN Edge.

- Full Service Recover requires focused planning around the key services.

How do you really stop a DDOS Attack?

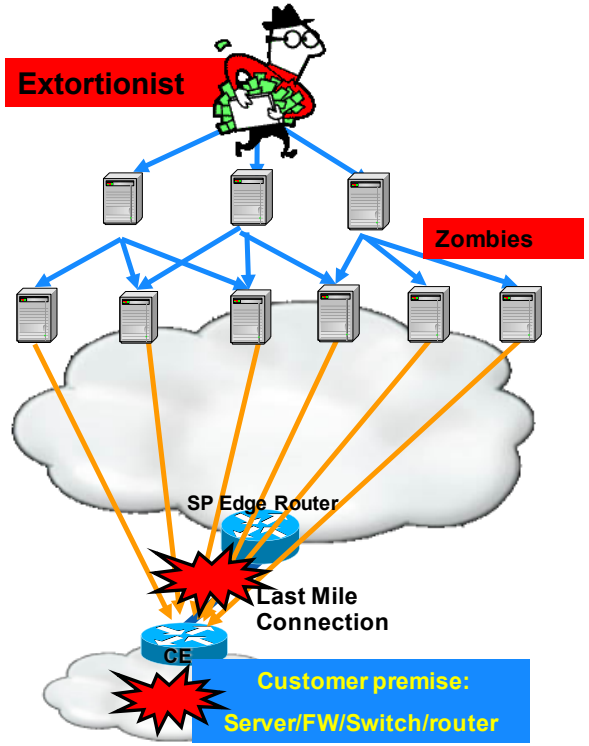
- Clean Pipes, Scrubbing Centers, and other “Anti-DDOS” tools *do not stop DDOS Attacks*.
- These tools are critical, but their should only be used to provide:
  - ✓ Full Service Restoration for selected mission critical services
  - ✓ Time to Remediate the DDOS Attack



How do you really stop a DDOS Attack?

- Stopping a DDOS Attack requires an ability to do:

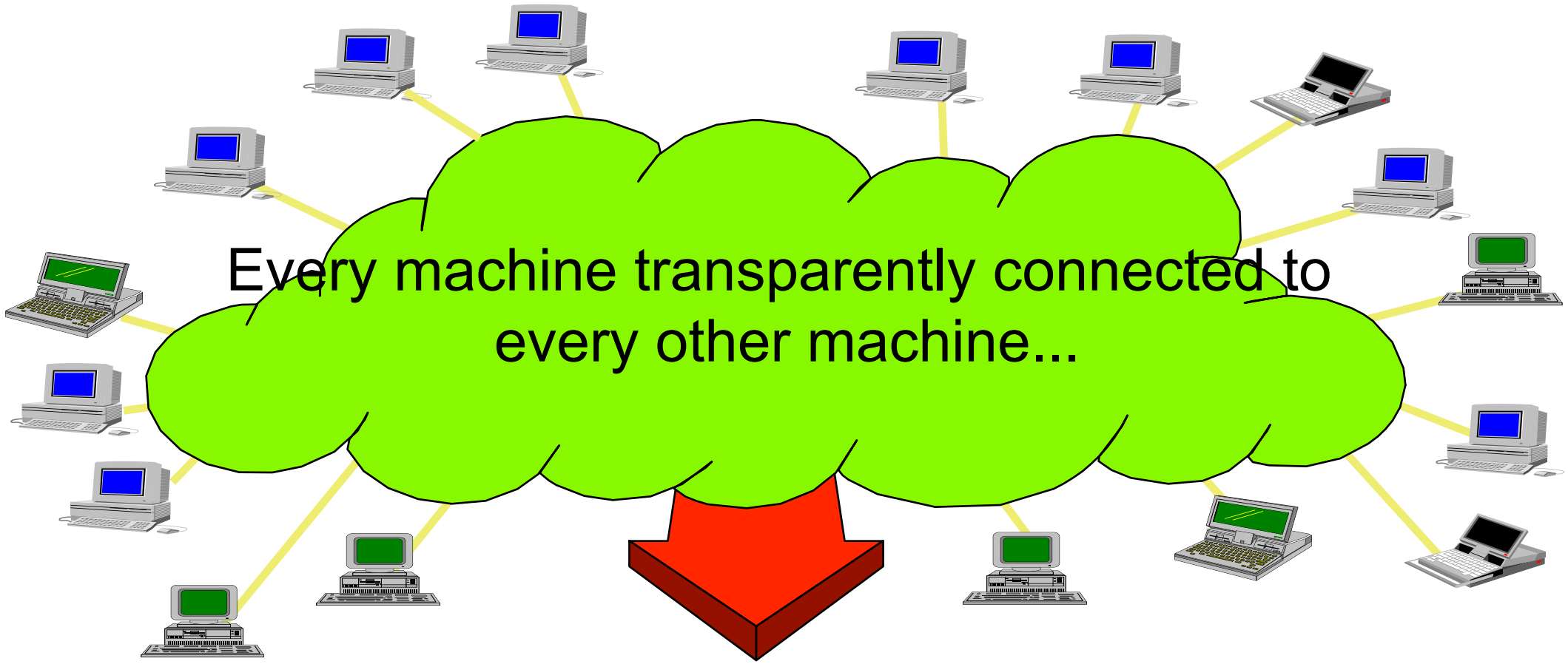
1. Withstand the attack and not given in to the extortion/threat
2. Visibility/Traceback to the Sources of the Attack
3. Remediating the Tools used in the Attack (BOTNETs and Reflectors)
4. Backtracing to the C&C used to drive the attack.
5. Triangulating on the person(s) launching the attack.



Pause for Questions

The End-to-End Principle’s Impact to Resiliency-Security Design

What people think of the Internet …

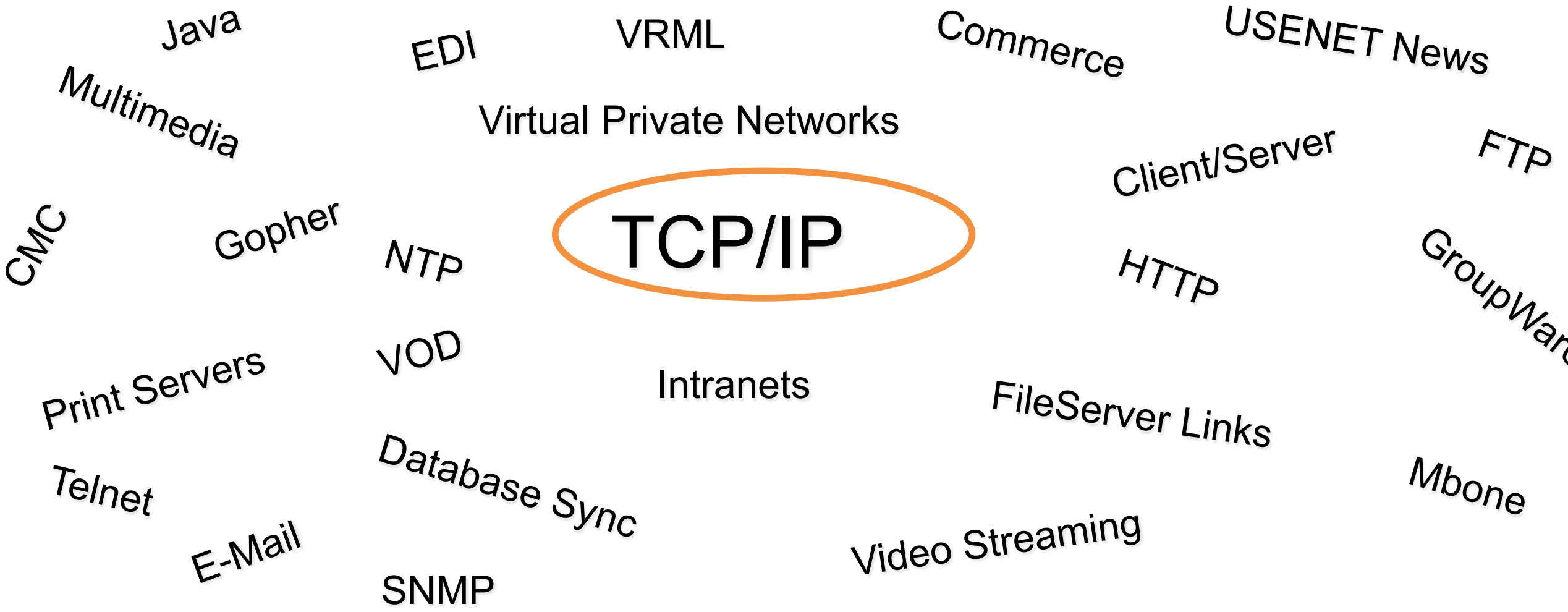


Slide originally created in 1994

What the Internet really is …

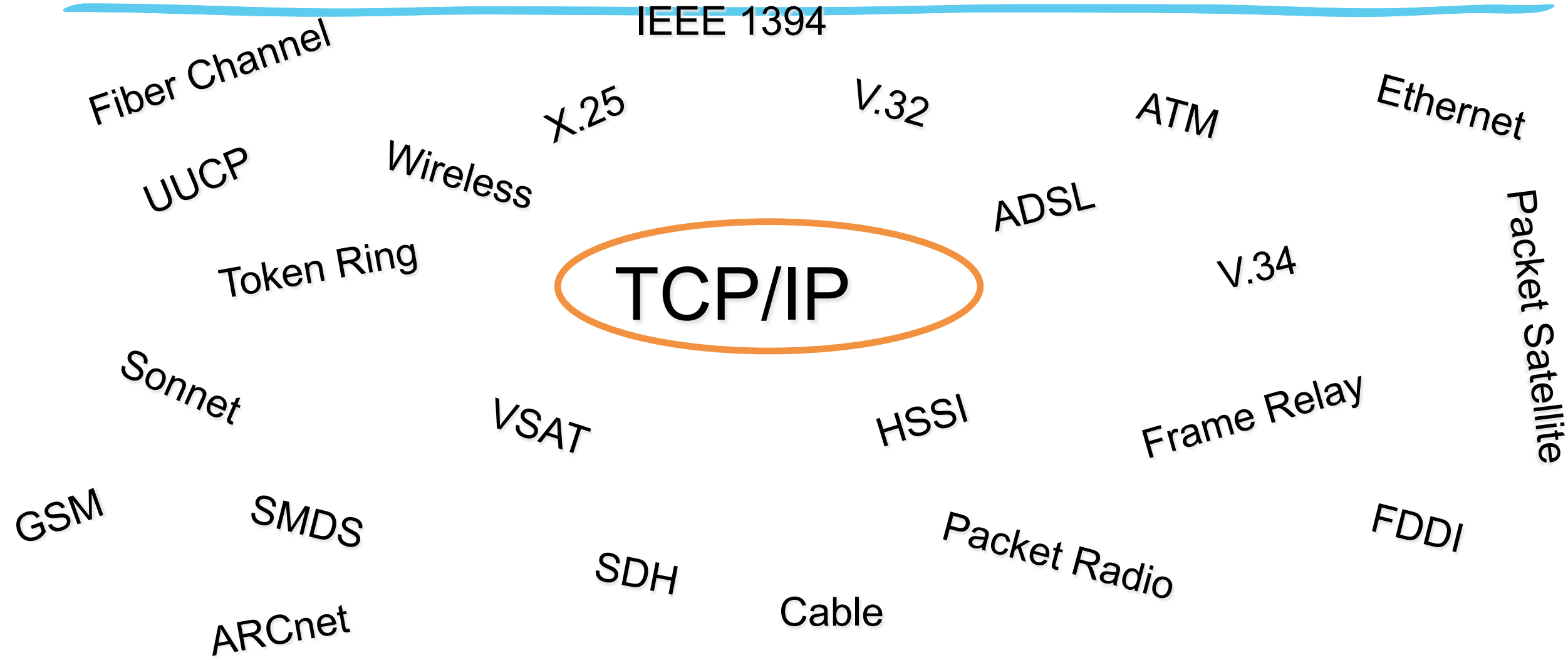
Slide originally created in 1994

Why is the Internet a Success?



Slide originally created in 1994

Why is the Internet a Success?

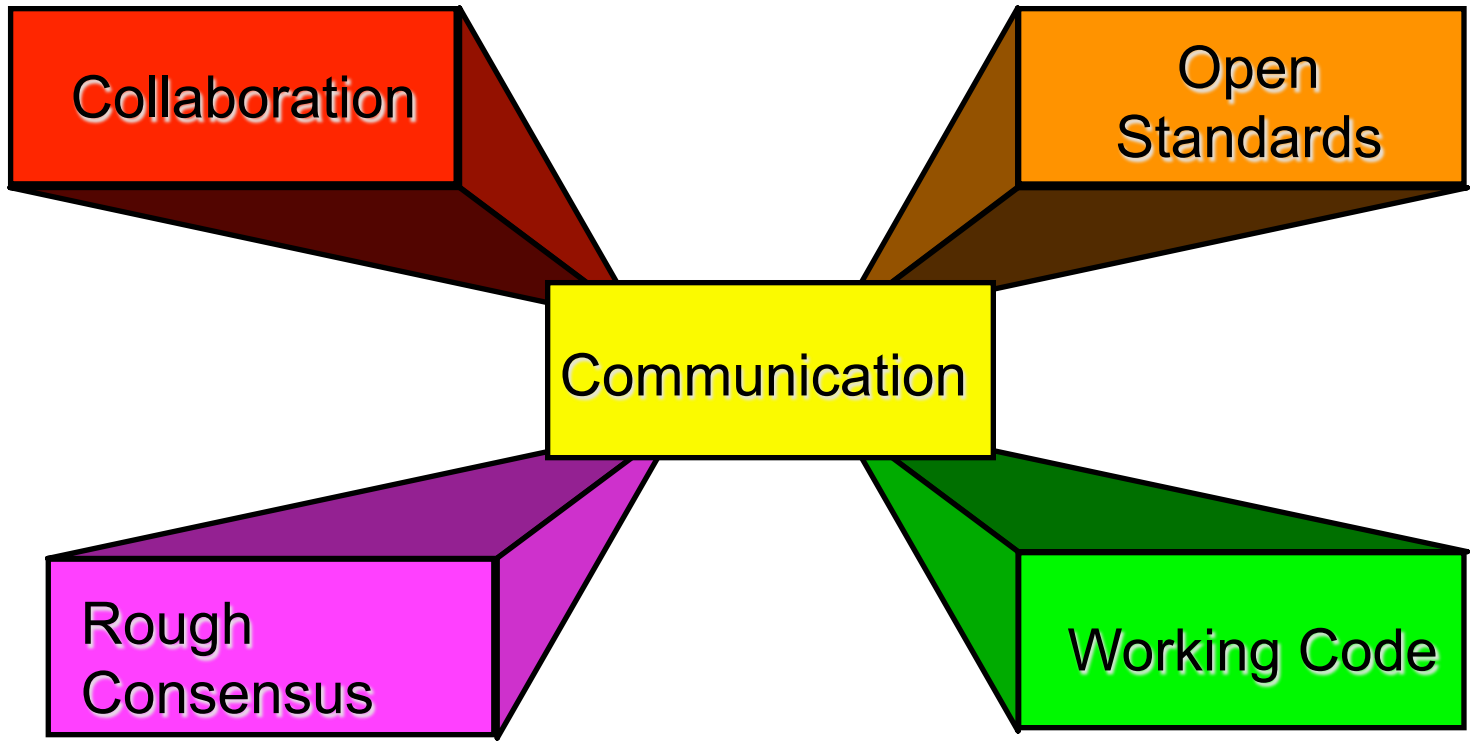


Slide originally created in 1994

The Internet Model

The Core Values of the Internet

From the perspective of the IETF



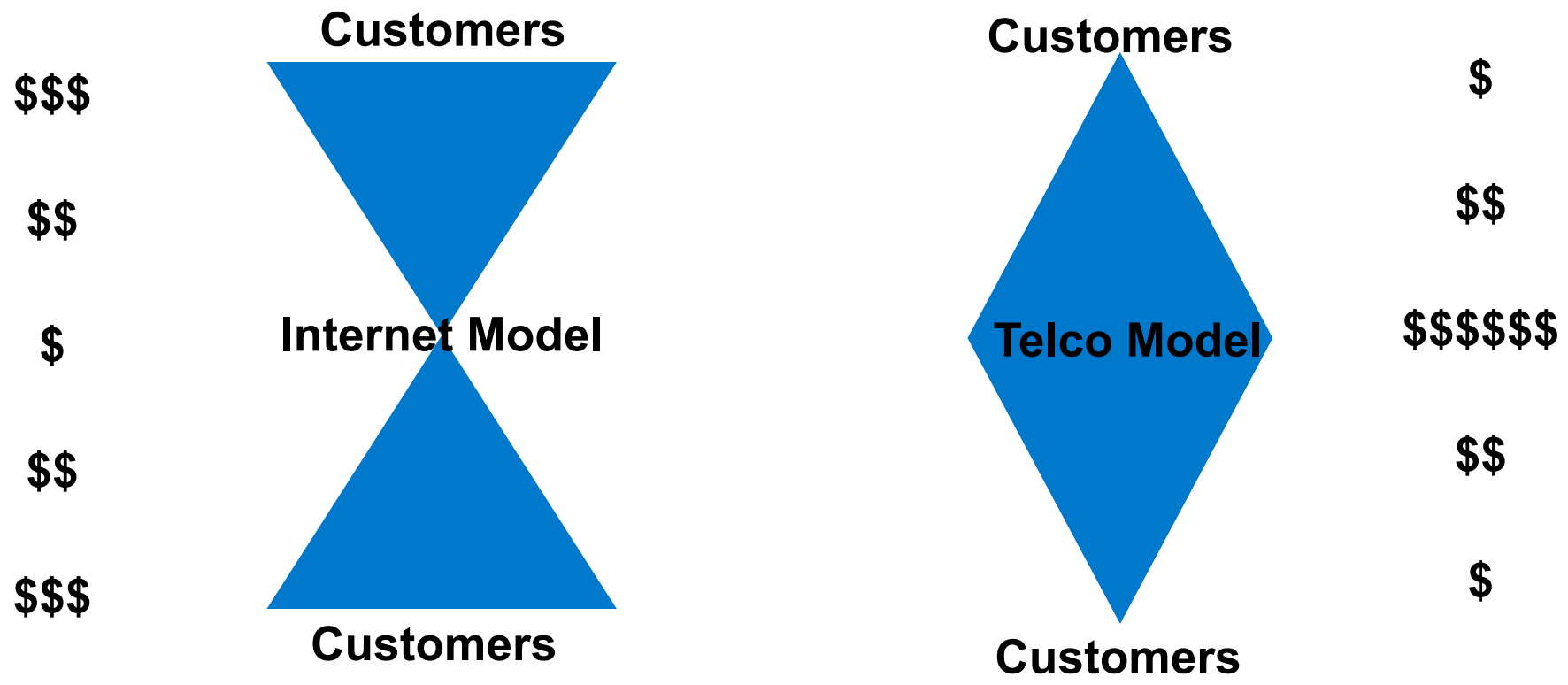
Slide originally created in 1994

What does IP over everything really mean?

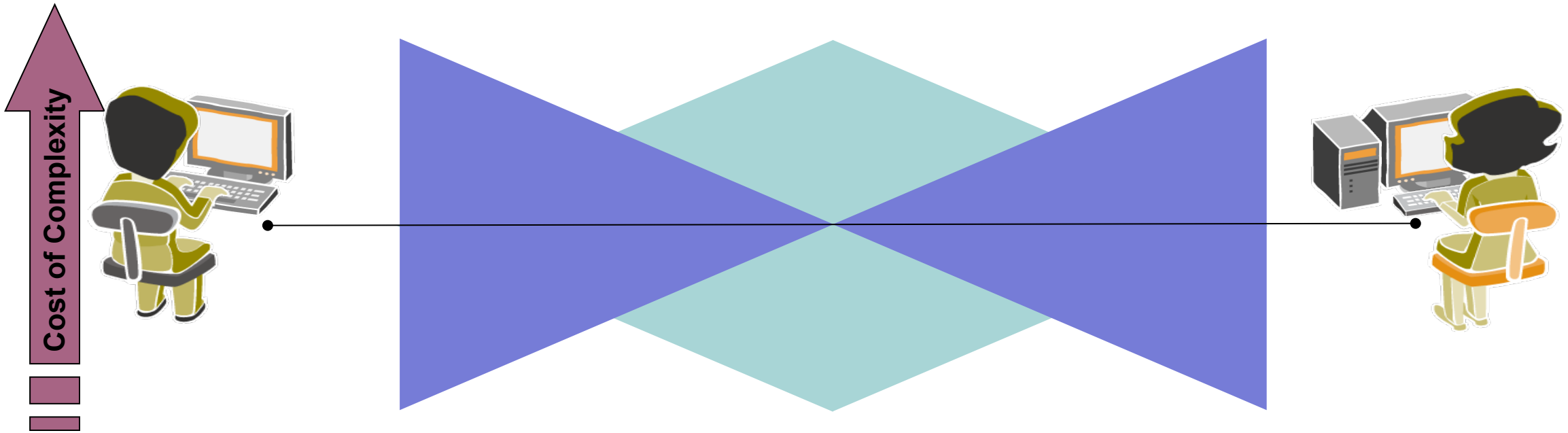
- **The End-to-End Principle puts all the hard work on the endpoints – with the core being as simple as possible.**
- **Simplicity in the middle allows for dynamics in the network to not break the end-to-end conversation.**
- **Think of how TCP is built and how its robustness allows for a lot of flexibility in the middle.**
- **This model allows customers (endpoints) to drive value upgrades to the network without adding complexity to the core.**

The End-to-End Principle and SPs

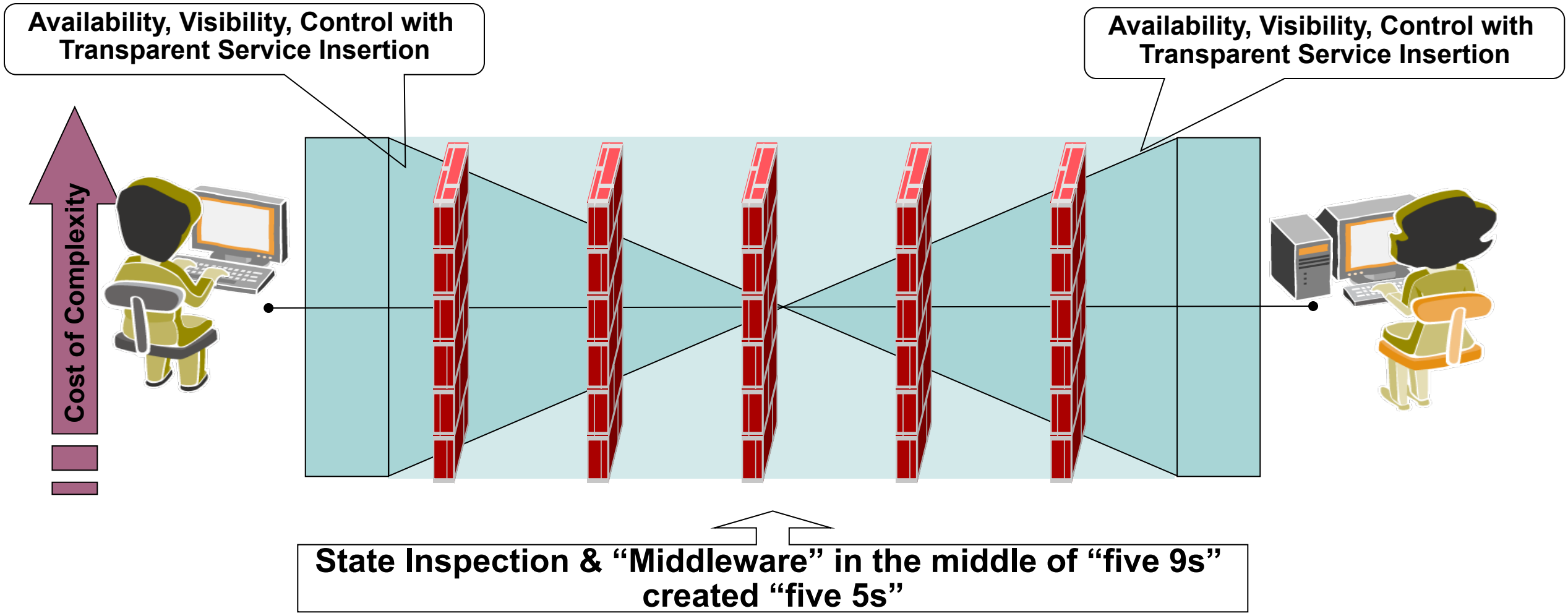
- The End-to-End model is 180^0 out from what conventional service providers and marketecture states.



End-to-End – Cost and State

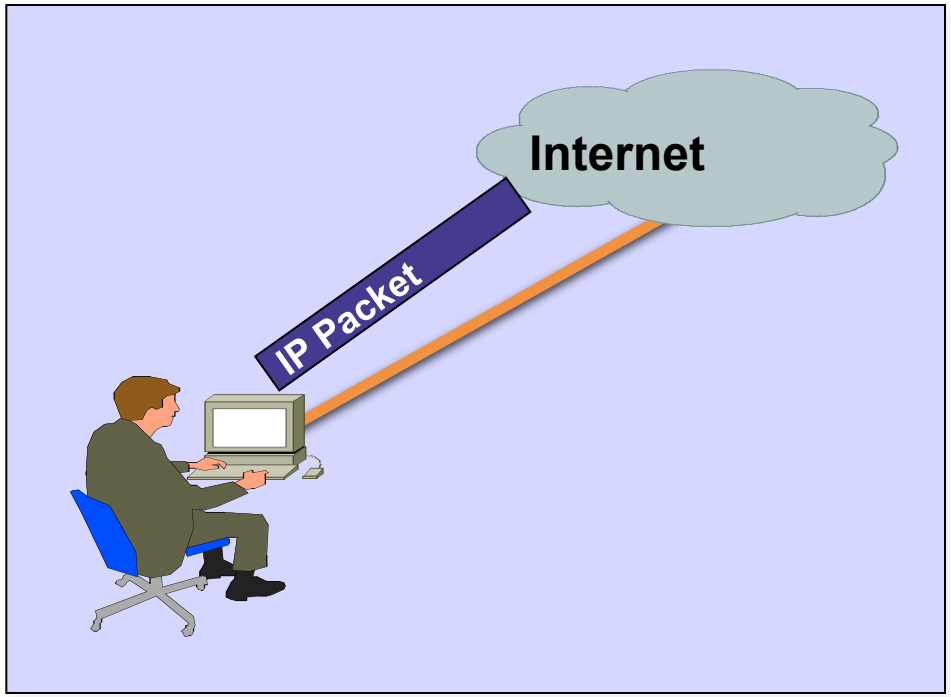


End-to-End – Cost and State

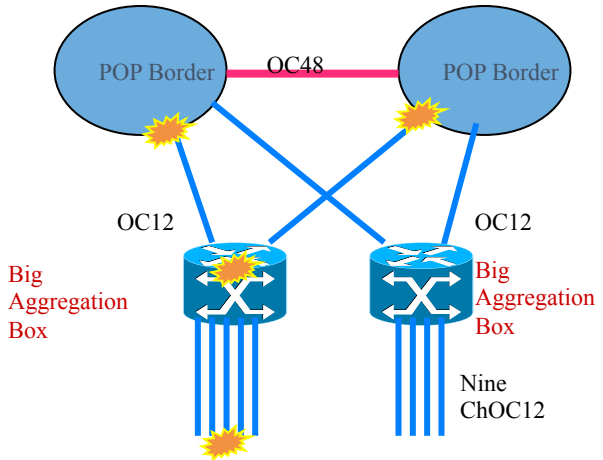


The Law of the Packet

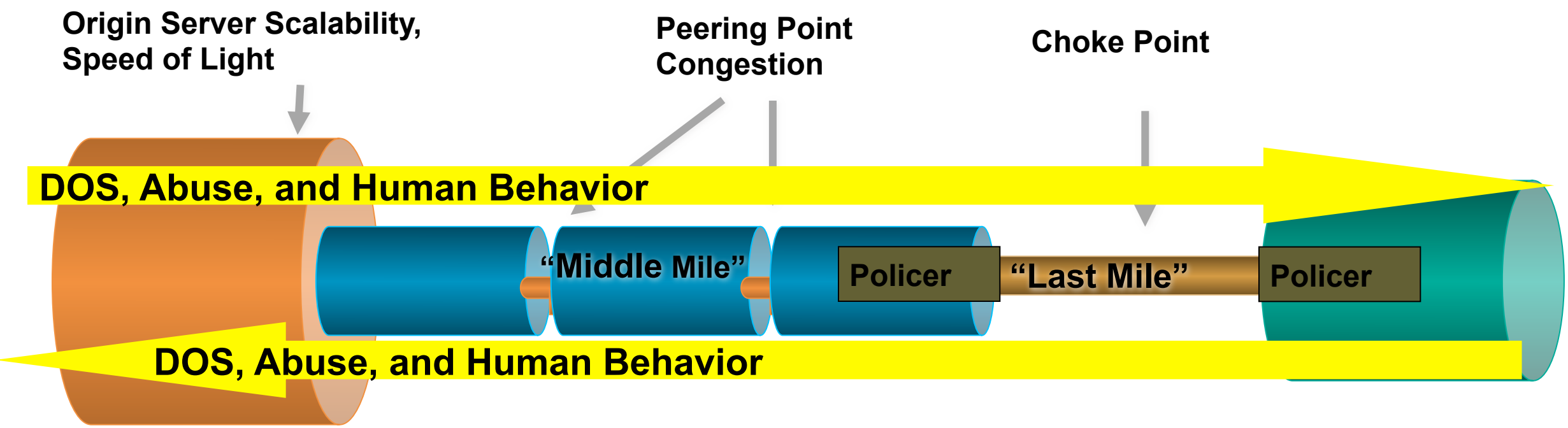
It is all about the packet ……..



- ❑ **It is all about the packet …..**
- ❑ **Once a packet gets into the Internet, someone, somewhere has to do one of two things:**
  - ***Deliver the Packet***
  - ***Drop the Packet***
- ❑ **In the context of DoS attacks, the questions are *who* and *where* will the "drop the packet" action occur?**



Choke Points = Collateral Damage



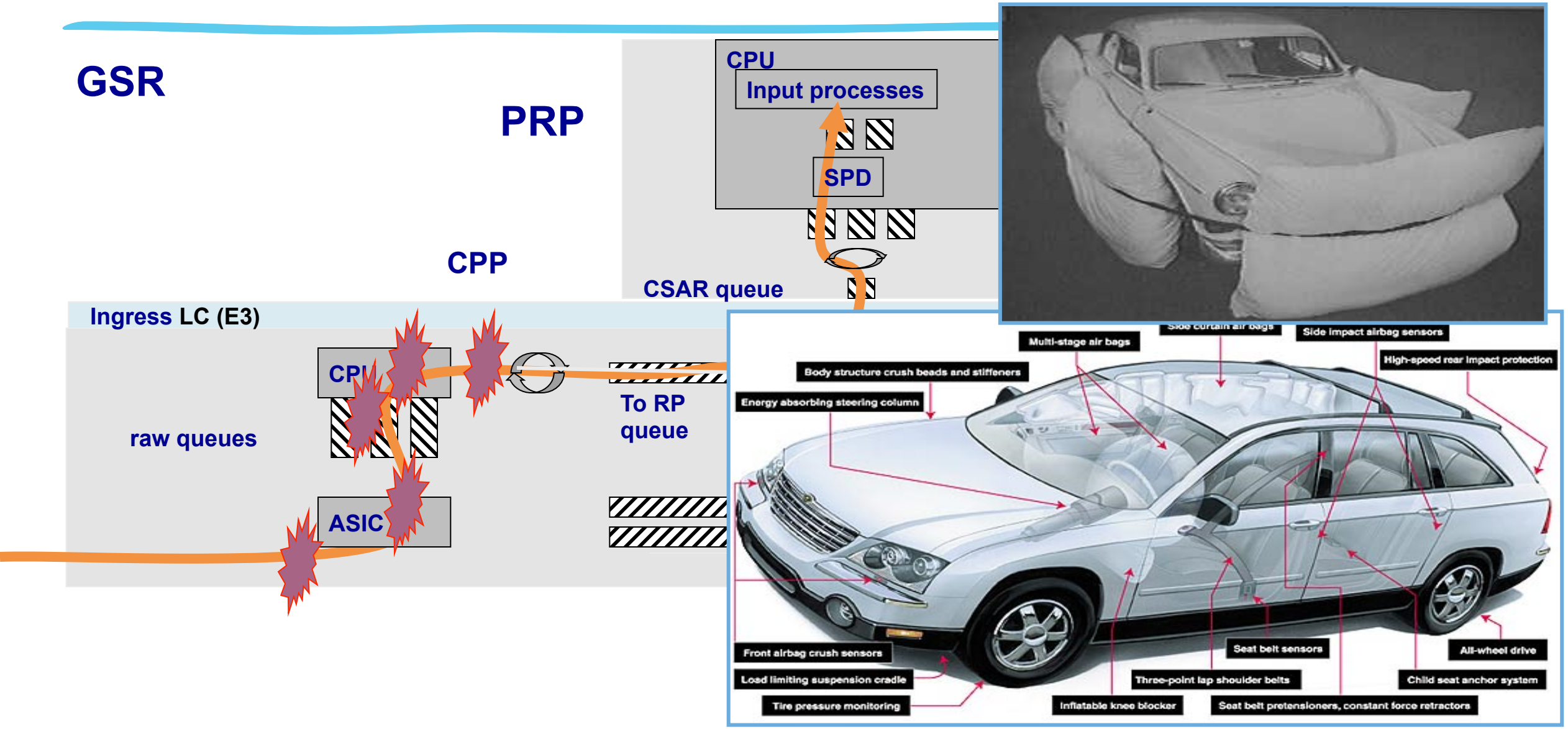
Internet Backbone

Cross-Internet connections

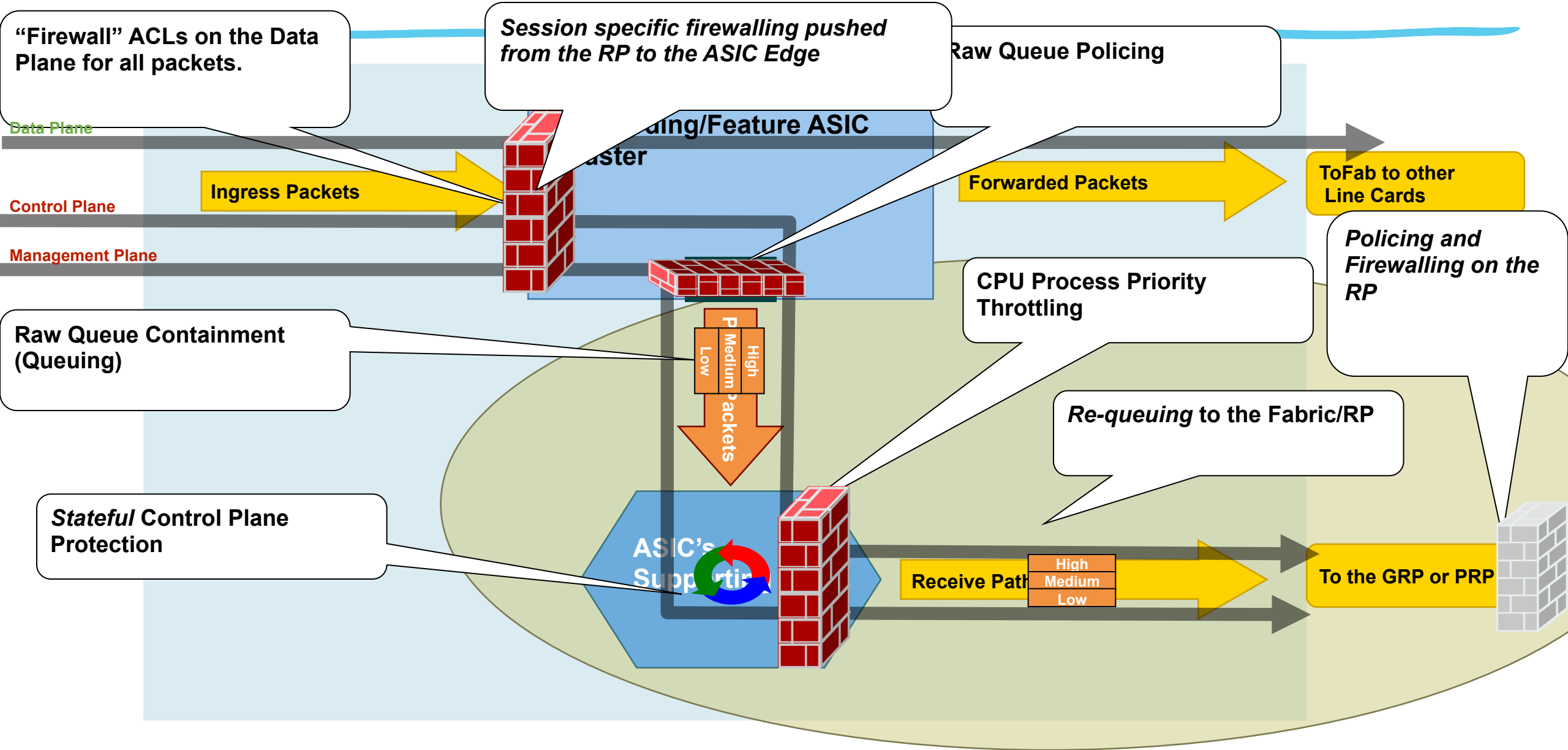
Local Loop

Premises Network

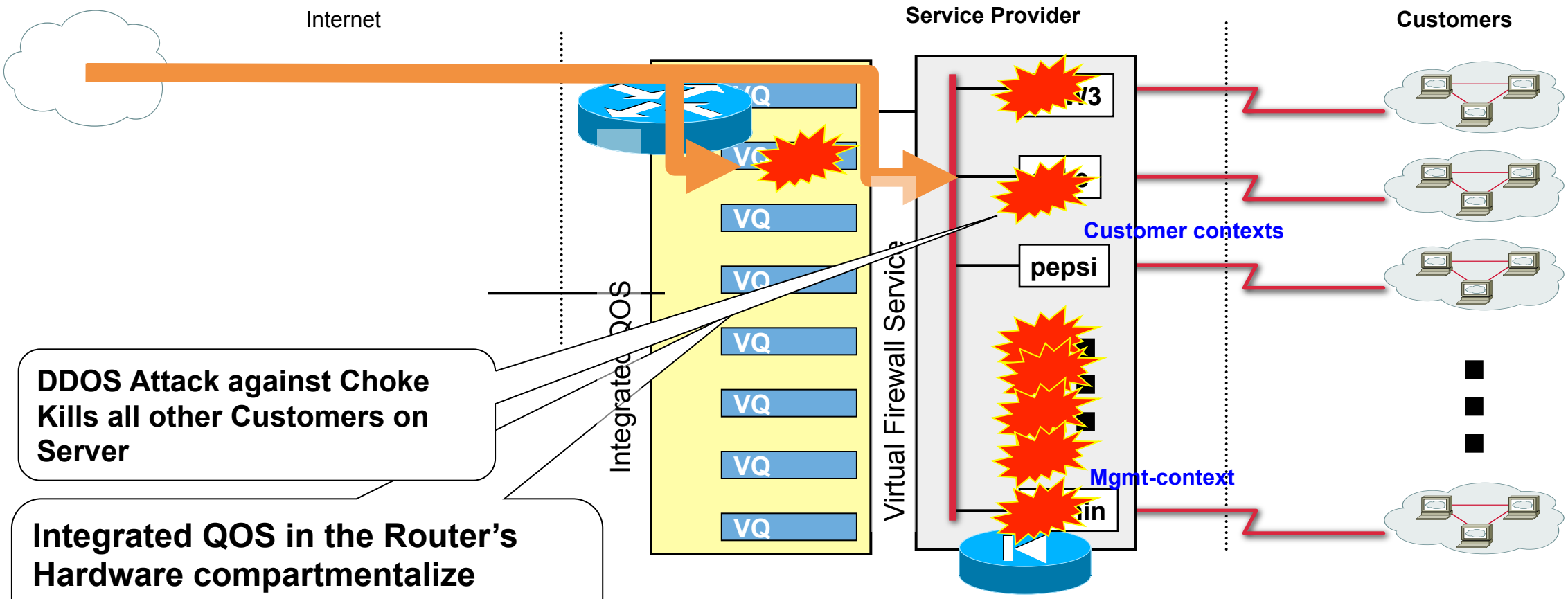
Security is an After Thought – Think *Safety Features*



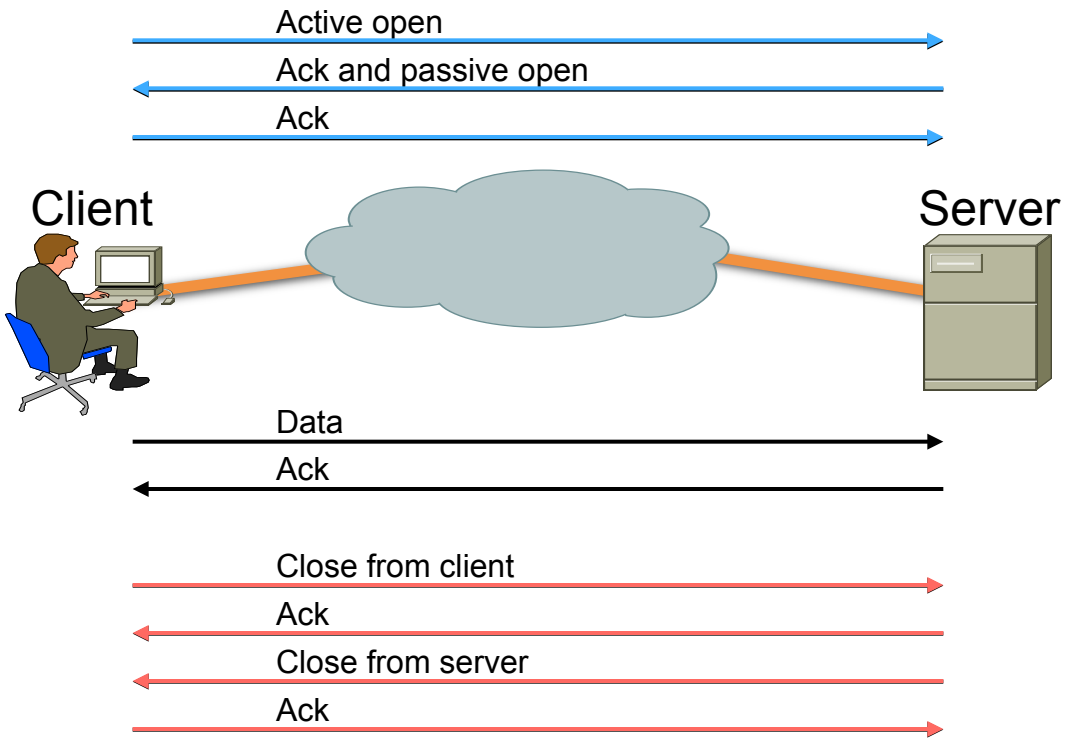
Example of Security Built into a Router

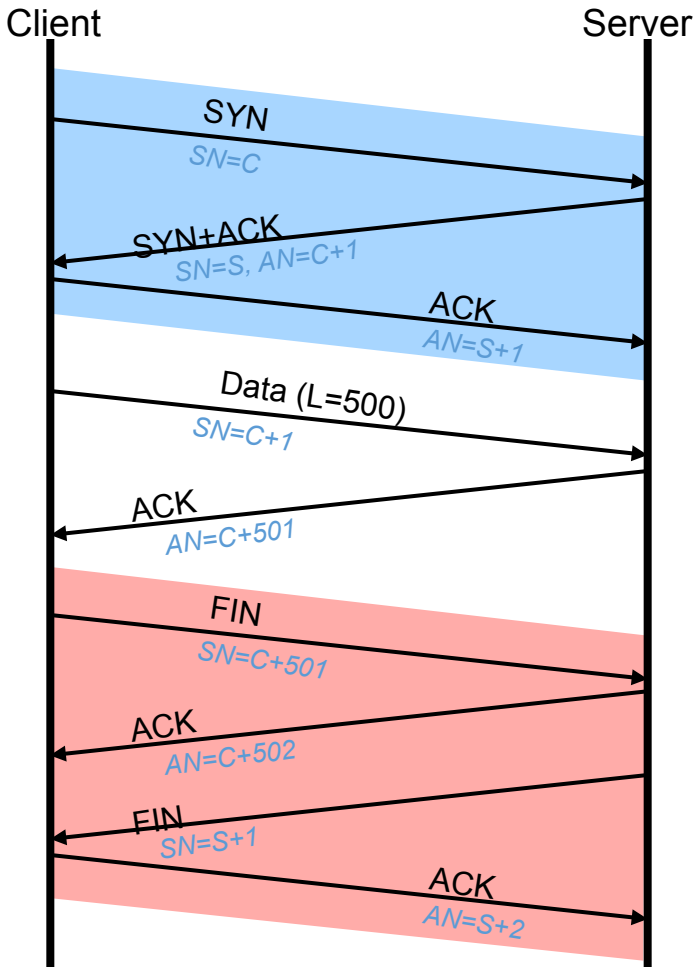


Throwing Hardware at the Problem?



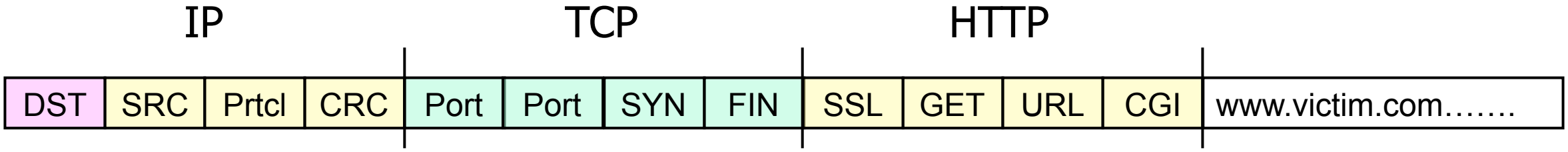
TCP Establishment and Termination



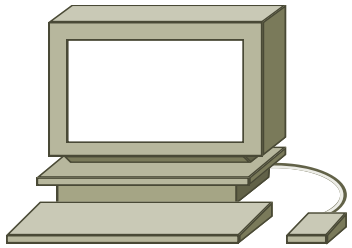


Packet Spoofing Review

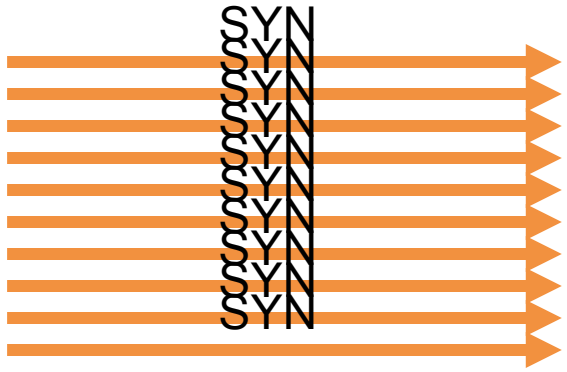
- What can be spoofed?
  - Any field in an packet header! – With 1 exception
  - Source-address spoofing is often combined with spoofing of values in other TCP packet fields
- Spoofing is used to:
  - Hide the source so the attacker or resource is not revealed.
  - Bypass Security – masquerading as valid packets.
  - Masquerade as the *real* target – fooling others into taking out the target, doing the attacker's work for him.



TCP SYN-Flood – Pushing out the Old Entries

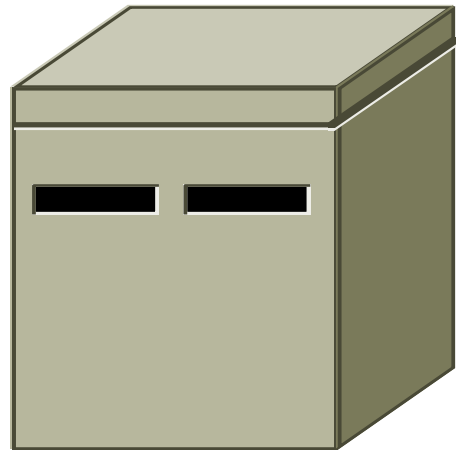


Attacker



Server's TCP Table
Filling faster than it can FIFO out.

SYN_RCVDSYN_
RCVDSYN_RCVD
SYN_RCVDSYN_
RCVDSYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
drop



TCP Server

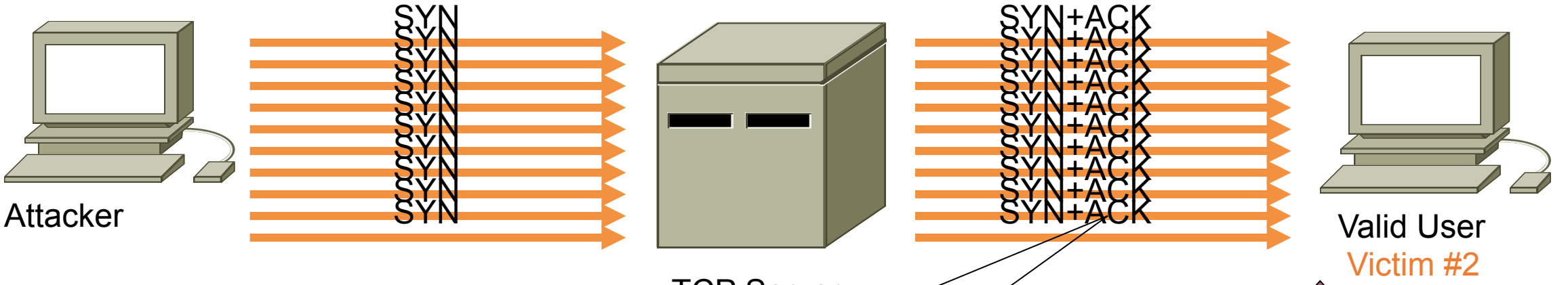
New SYNs push out oldest SYN_RCVD entries

SYN Attack Expanding Consequences

A
Masquerading as C
SYN-Floods B

B
Site Under Attack

C
Secondary Attack



Reflection Attack can be an unintentional side-effect, or by design.

Which is the real target? #1 or #2?

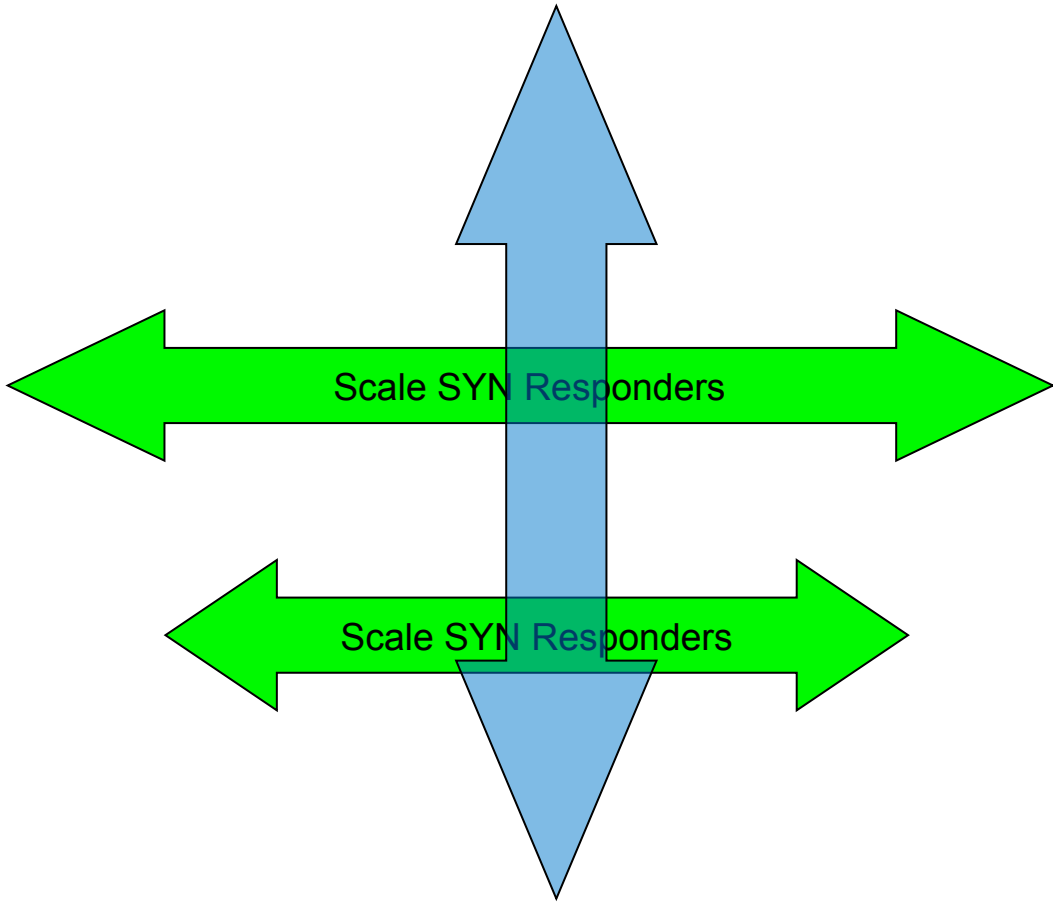
Three SYN-Flood Protection Options

1. Ride out the SYN-Flood by expanding the SYN-responder pool, essentially ‘eating’ the attack. This is considered *passive protection.*
2. Filter the SYN-Flood based on some variable which will minimize impact to the customer. Packet filtering is considered *active protection.*
3. *Divert & scrub out the attack traffic, allowing the good traffic through.*

Generic rate-limiting is not a viable option – we end up rate-limiting both good and bad SYN traffic.

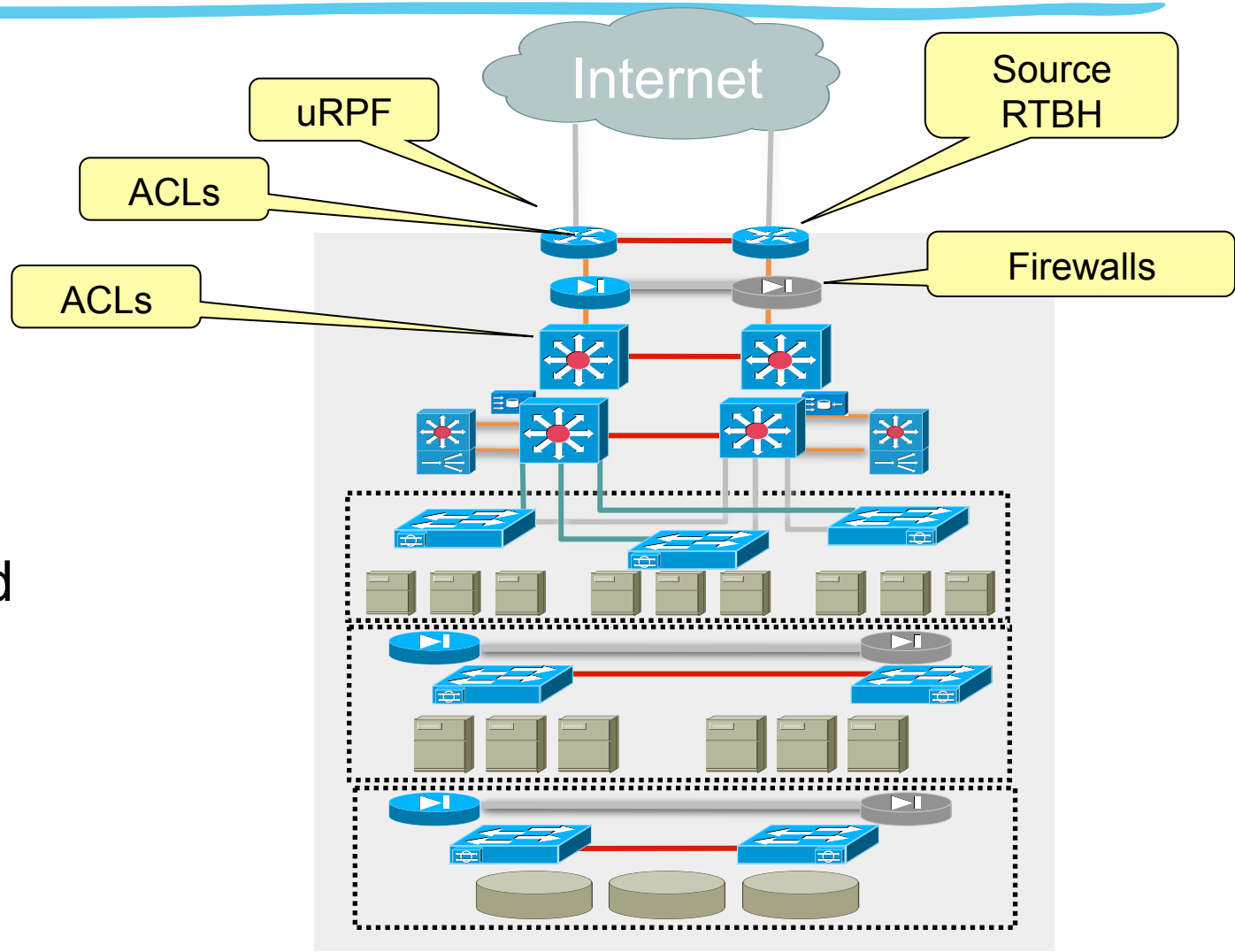
Option 1 – Scale the Number of SYN Responders

- The more devices responding to TCP SYNs, the more SYN-Flood traffic can be absorbed.
- Multiple directions of scaling:
  - More hosts
  - Layered hosts
  - Layered devices
  - Topologically-distributed devices



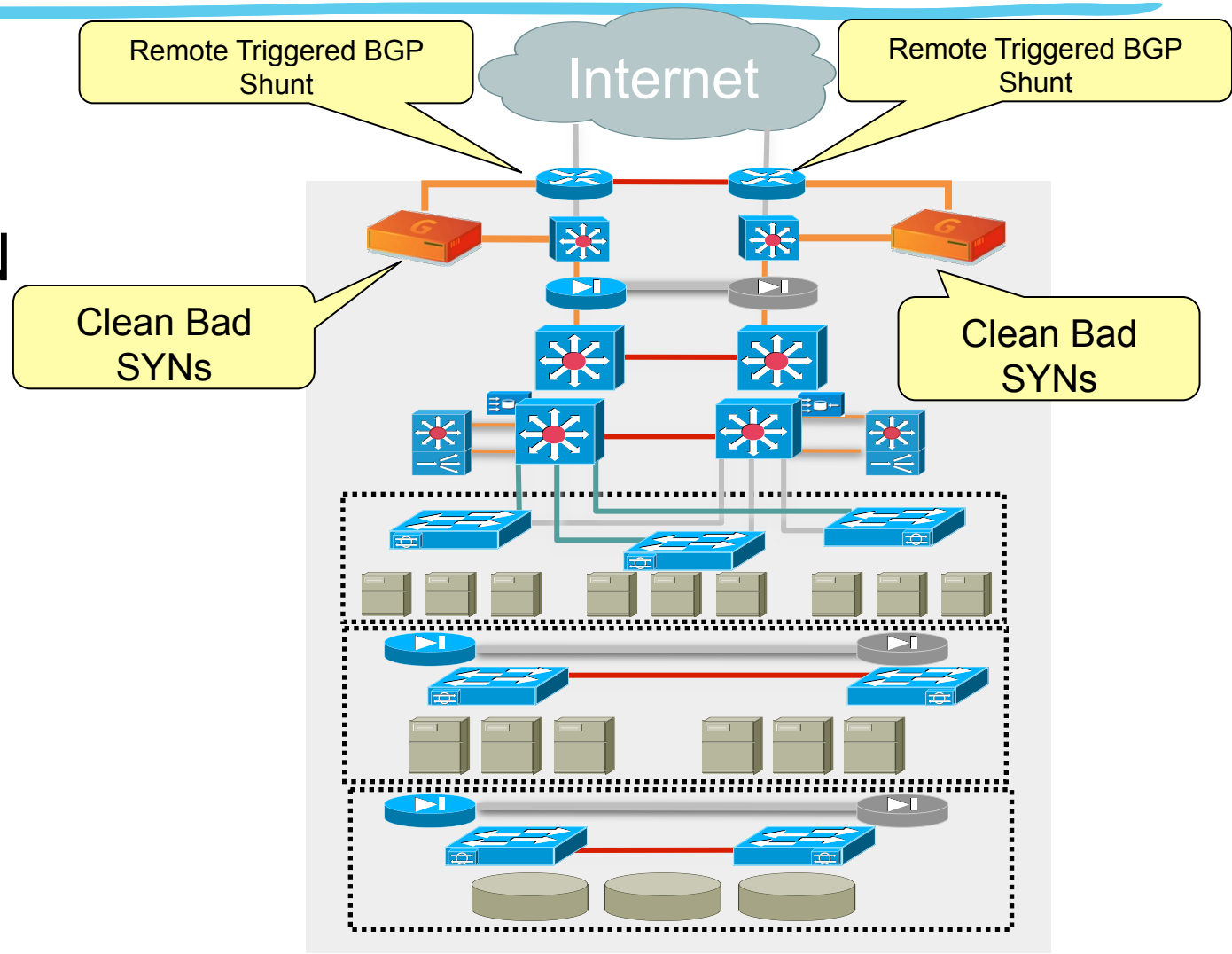
Option 2 – Filter the Packets

- Based on specific, identifiable characteristics, drop the packets:
  - Source address
  - TTL
  - TCP Options
  - Source Port numbers
  - And so on . . .
- Multiple drop technologies can (and should) be layered - for example, combining source-based uRPF Remotely-Triggered Blackholing (RTBH) with ACLs and firewall rules.



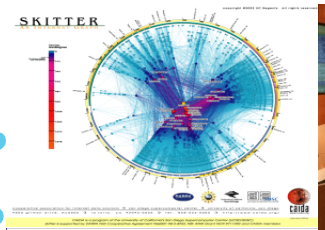
Option 3 – Divert, Scrub, & Re-inject

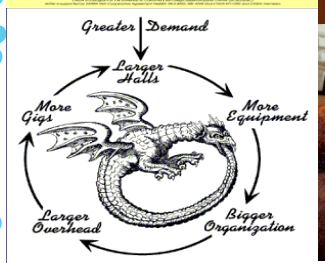
- Use diversion, scrubbing, and re-injection to drop bad SYN traffic while allowing good SYN traffic through.
- Remotely-triggered BGP shunts allow the cleanup tools to be dynamically inserted into the path during an attack, and withdrawn after the attack has been handled.

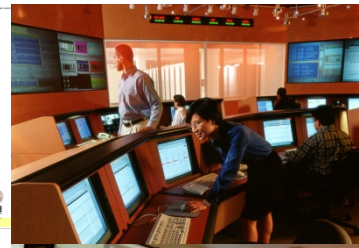


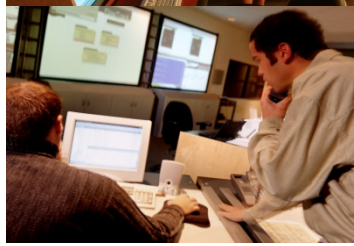
Pause for Questions

Understanding Today's Cyber-Criminal Behavior Drivers



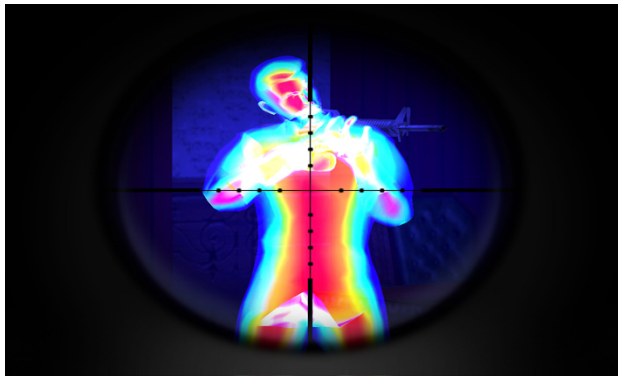






The Good Guys are a Big Part of the Security Problem

Who we need to Target

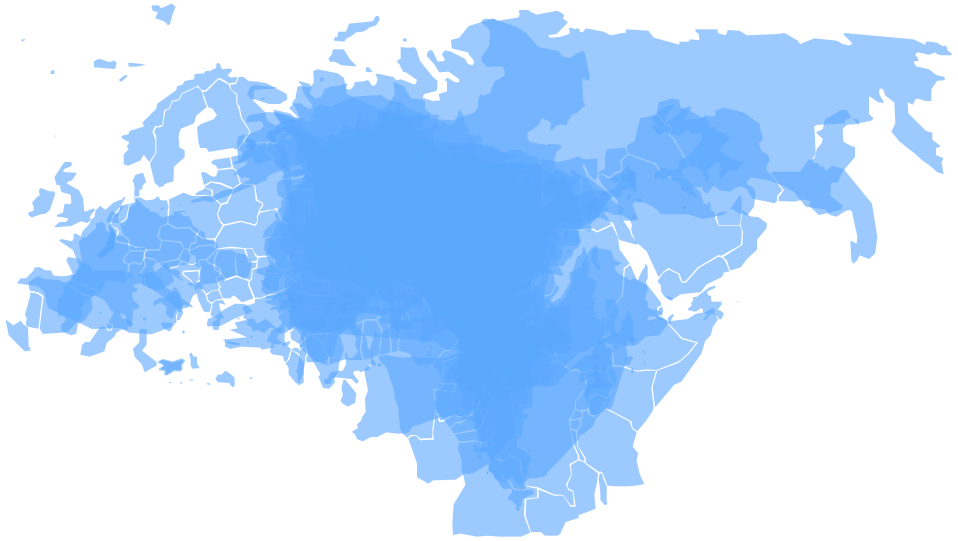


This is nice to know

Not understanding that our problem is a human problem leads to “security solutions” which get bought, deployed, and never used.

Our Traditional View of the World

The Reality of the Internet - No Borders



How do you project civic society and the rule of law where there is no way to enforce the law?

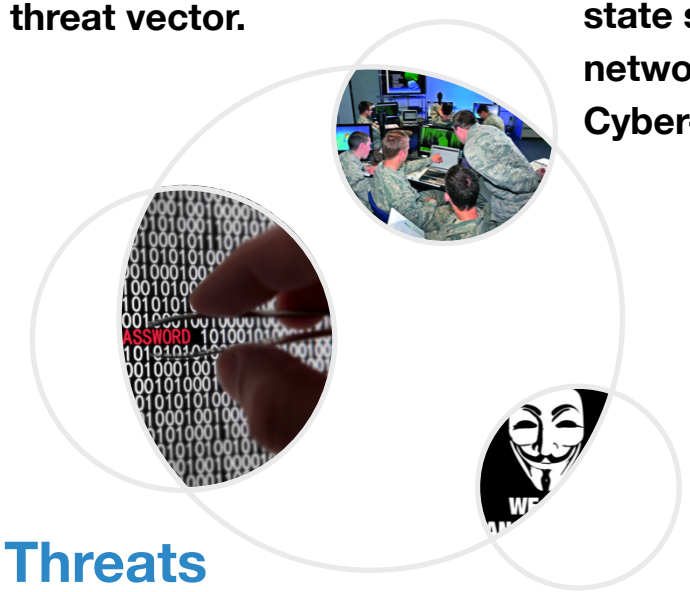
Threat Vectors have Evolved

Corporate Threats (New!)

The dialog between US & China will accelerate the corporate on corporate threat vector.

Nation State Threats

Post-Snowden, the secret world of nation state security is now all in the open. Your network is a valid “Battle Space” for any Cyber-War.



Cyber-Criminal Threats

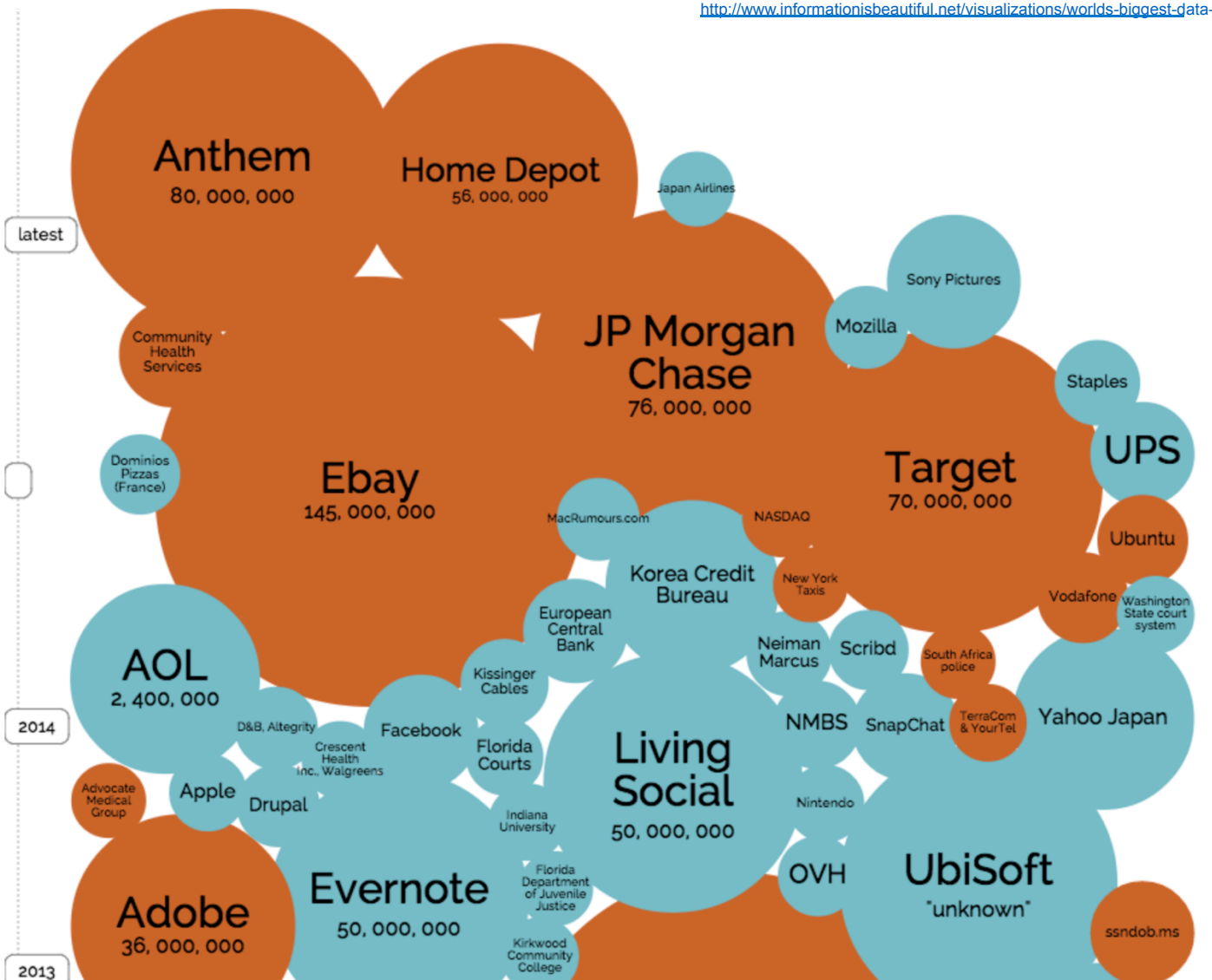
Cyber-Crime is an International Legal problem that has no short term resolution. There will always be someplace in the world that is a harbor for cyber-criminal activity.

Political, Patriotic, Protestors (P3)

There are always going to be someone, somewhere, who is upset with society - with the ability to make their anxiety know through any network - any where.

What really happens if I’m attacked?

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

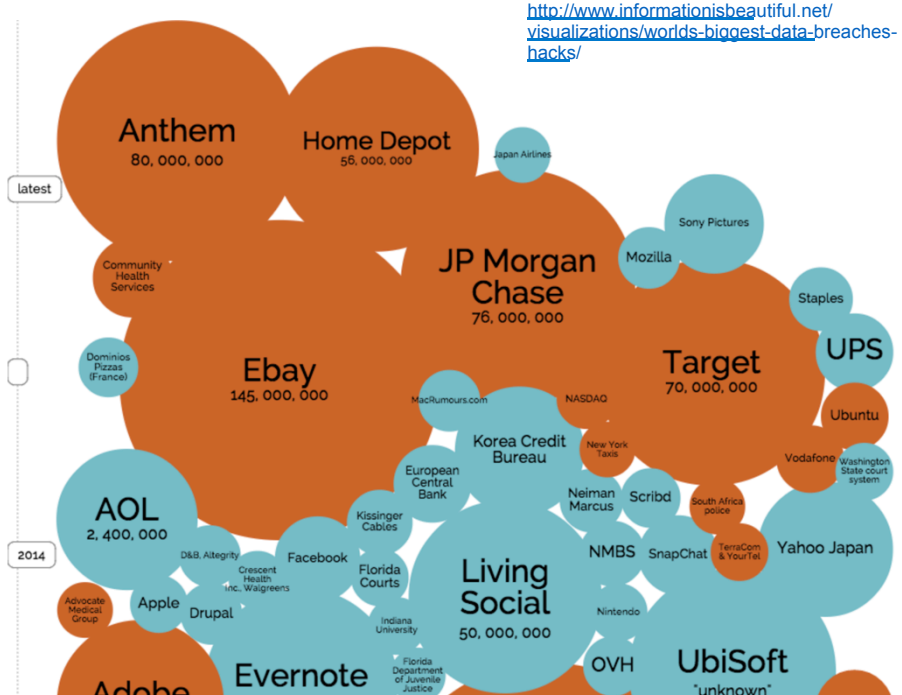


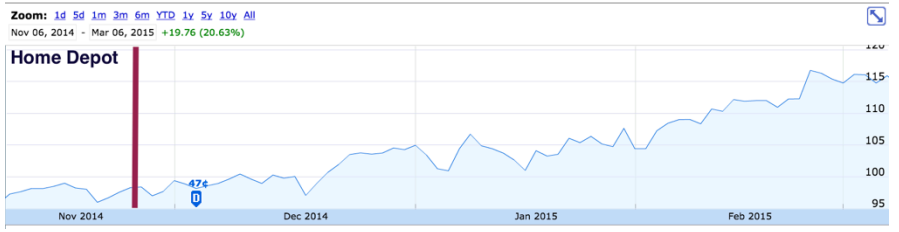
The market does not penalize!

The “market” is forgiving IF you have a security reaction plan.

A security reaction plan will not prevent revenue losses, customer churn, and legal actions, but … organizations do recover from “big data breaches”

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/





Liability “Should be” Flowing Down Hill

Emergency Services

Outage Causing Death

FCC Investigation

Provider Liability

Vendor Liability

Security Threats are a Force of Nature

- Think of the current and future security threats as a force of of the environment we live in. This is not new to human society. We have to live with the issues of nature all the time.

- Like a hurricane, it is not a matter of if, but when. Even worse, you can be in a zone where the hurricane, tornado, flood, earth quake, and blizzard are all a major risk.

Forces of Nature cannot be stopped - the only thing you can do is mitigate risk through your design, preparation, and investment.

Key Takeaways …..

- If the threat vectors are not going away, then the risk will be persistent for the next few DECADES!
- If the market does not penalize companies for the major security violations, then there are no “market forces” to drive major security improvements.
- The massive growth in the “security eco-system” is driving decision makers into no action. They are not sure what really needs to be done.
- Vendors are not being help up as liable to security risk. This means there normal capitalistic forces that drive for change.
- Thinking of security as a “force of nature” is a more appropriate way of considering the real risk security threats have on the business and society.

Essential Criminal Principles

- There are key essential principles to a successful miscreant (i.e. cyber criminal)
- These principles need to be understood by all Security Professionals
- Understanding allows one to cut to the core concerns during security incidents
- Attacking the **dynamics** behind these principles are the core ways we have to attempt a **disruption** of the Miscreant Economy*

* The cyber-criminal “economic cycles” were first observed in 2001 by Rob Thomas (Team CYMRU) and Barry Greene during a postmortem investigation. This “Miscreant Economy” has been growing exponentially since that time.

Principles of Successful Cybercriminals

1. Don’t Get Caught
2. Don’t work too hard
3. Follow the money
4. If you cannot take out the target, move the attack to a coupled dependency of the target
5. Always build cross jurisdictional attack vectors
6. Attack people who will not prosecute
7. Stay below the pain threshold

Principle 1: Do Not Get Caught!

- The first principle is the most important – it is no fun getting caught, prosecuted, and thrown in jail
  - (or in organized crime – getting killed)
- All threat vectors used by a miscreant will have an element of un-traceability to the source
- If a criminate activity can be traced, it is one of three things:
  1. A violated computer/network resources used by the miscreant
  2. A distraction to the real action
  3. A really dumb newbie

Principle 2: Do Not Work Too Hard!

- Use the easiest attack/penetration vector available in the toolkit to achieve the job's objective
- Example: If your job is to take out a company's Internet access the day of the quarterly number's announcement, would you:
  1. Penetrate the Site and Delete files?
  2. Build a custom worm to create havoc in the company?
  3. DOS the Internet connection?
  4. DOS the SP supporting the connection?

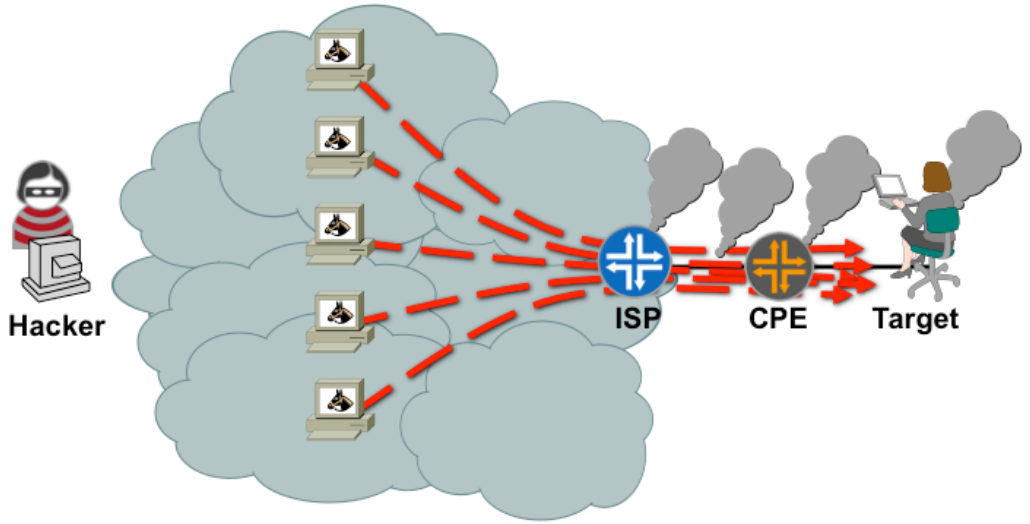
Why Use DNS "Noisy" Poisoning when it is easier to violate a ccTLD?

Principle 3: Follow the Money

- *If there is no money in the crime then it is not worth the effort.*
- *Follow the money* is the flow of money or exchanged value as one miscreant transfers value to another miscreant (or the victim transfers value to the criminal)
- A ***Cyber-Criminal Threat Vector*** opens when the miscreant finds a way to **move 'stored value' from the victim through the economy**
- It is worse if the cyber 'stored value' can cross over to normal economic exchange

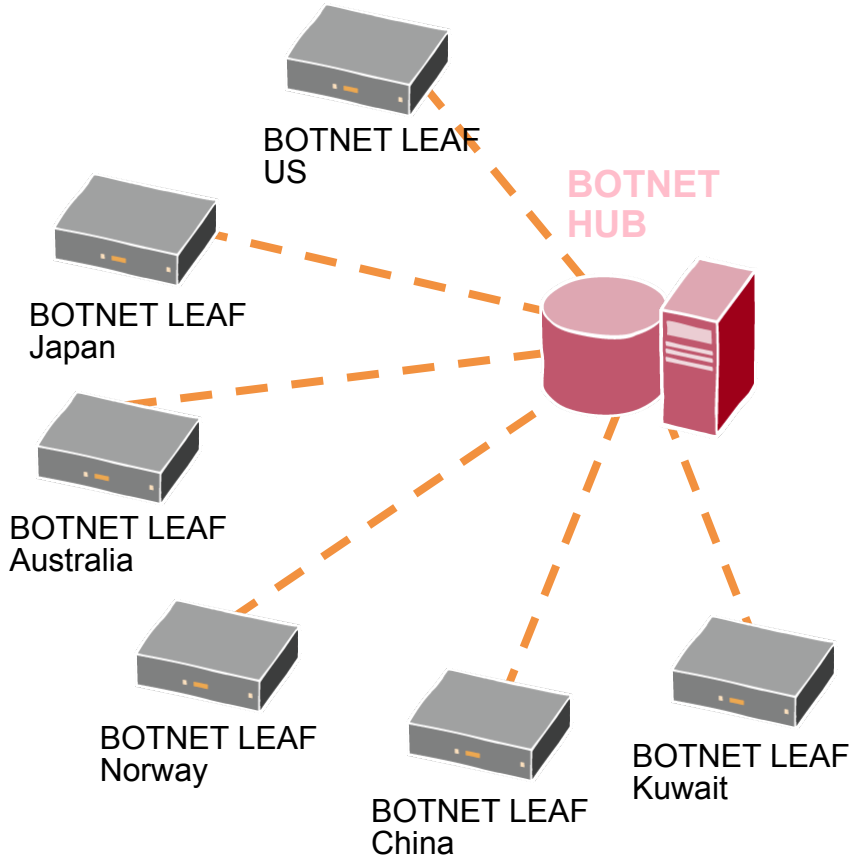
Principle 4: If You Cannot Take Out The Target…

- If you cannot take out the target, move the attack to a coupled dependency of the target
- There are lots of coupled dependencies in a system:
  - The target's supporting PE router
  - Control Plane
  - DNS Servers
  - State Devices (Firewalls, IPS, Load Balancers)
- Collateral Damage!



Principle 5: Always Build Cross Jurisdictional Attack Vectors

- Remember – Don’t get caught! Do make sure ever thing you do is cross jurisdictional.
- Even better – cross the law systems (Constitutional, Tort, Statutory, Islamic, etc.)
- Even Better – Make sure your “gang” is multi-national – making it harder for Law Enforcement



Principle 6: Attack People Who Will NOT Prosecute

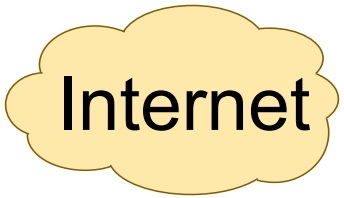
- If your activity is something that would not want everyone around you to know about, then you are a miscreant target
- Why? Cause when you become a victim, you are not motivated to call the authorities
- Examples:
  - Someone addicted to gambling is targeted via a Phishing site
  - Someone addicted to porn is targeted to get botted
  - Someone addicted to chat is targeted to get botted
  - Someone new to the Net is targeted and abused on the physical world
  - Government, Finance, and Defense, Employees – who lose face when they have to call INFOSEC

Principle 7: Stay below the Pain Threshold

- The *Pain Threshold* is the point where an SP or Law Enforcement would pay attention
- If you are below the pain threshold – where you do not impact an SP's business, then the SP's Executive Management do not care to act
- If you are below the pain threshold – where you do not have a lot of people calling the police, then the Law Enforcement and Elected Official do not care to act
- The Pain Threshold is a matter of QOS, Resource Management, and picking targets which will not trigger action

Criminal Trust

- Miscreants will guardedly trust each other
- They can be competitors
- They can be collaborators
- But when there is money on the table, criminal human behavior and greed take over.
- Cybercriminal cannibalize each other's infrastructure.
- Cybercriminals attack each other's infrastructure.



Dire Consequences

- The Miscreant Economy is not a joke. It is not a game. It is not something to play with.
  - **PEOPLE DIE**
- Once organized crime enter the world of the Miscreant Economy, the days of *fun* were over.
- Now that Cyber-Criminals will use any resource on the net to commit their crime, they don’t worry about the collateral damage done.
  - Think of computer resources at a hospital, power plant, or oil refinery – infected and used to commit phishing and card jacking.
  - What happens if someone gets mad at the phishing site, attacks it in retaliation, unintentionally knocking out a key systems.

Enduring Financial Opportunities

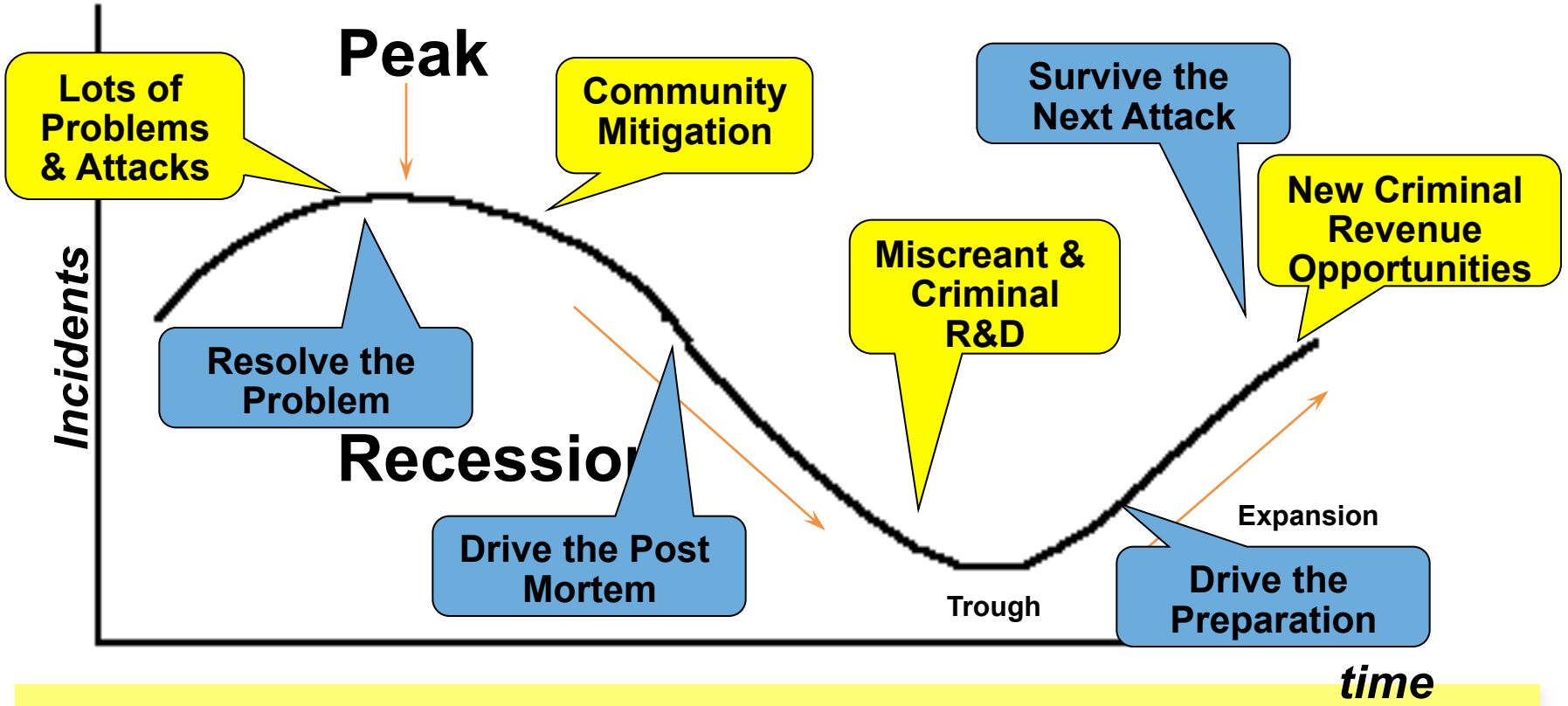
2007 Prediction: Strong, Enduring Criminal Financial Opportunities Will Motivate Participants in the Threat Economy to Innovate to Overcome New Technology Barriers Placed in Their Way

Enduring *criminal* financial opportunities:

- Extortion
- Advertising
- Fraudulent sales
- Identity theft and financial fraud
- Theft of goods/services
- Espionage/theft of information

Today's Reality!

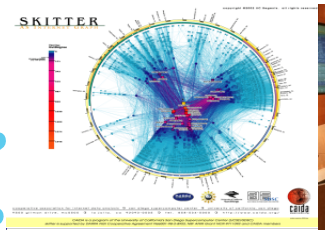
Miscreant - Incident Economic Cycles

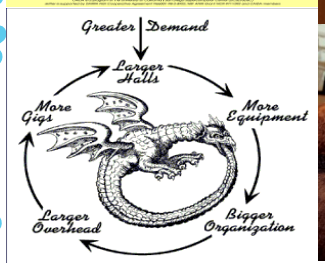


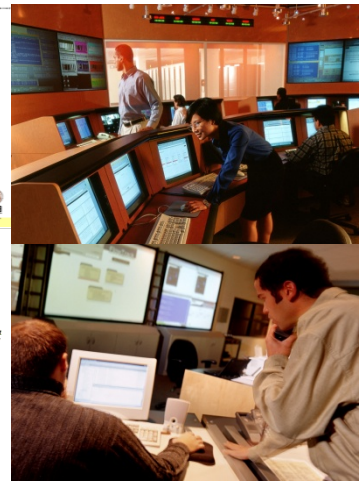
These Cycles Repeat

Pause for Questions

Operator's Security Toolkit Overview







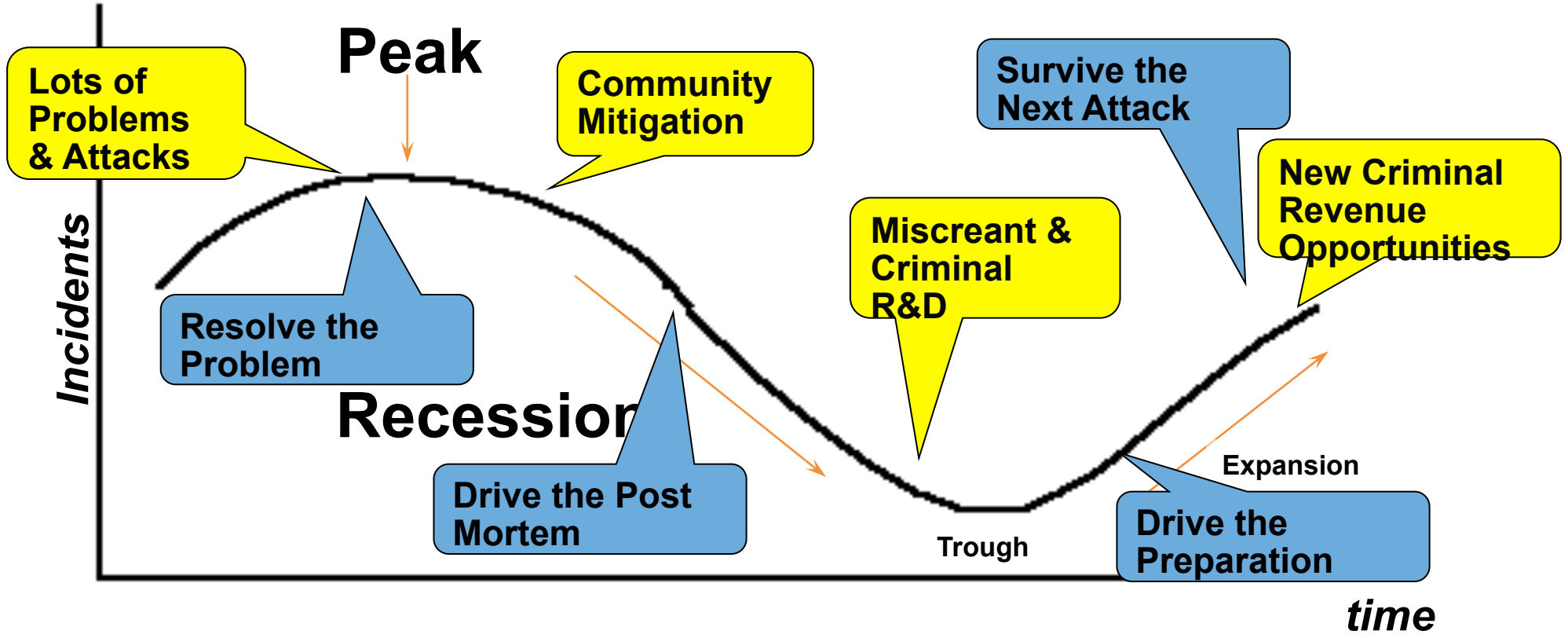
ISOI #1 (2006) – Reviewed our ”Top 10”

- Security “Side Door” Session:
  - BGP Prefix filtering
  - Source Address Validation
  - Close open ports
  - Danger of Reflection attacks
  - Danger of DoS attacks
  - “Advance Persistent Threat” (used a different phrase)
  - Patch your systems
  - Monitoring the scanning of the network
- Does this all resonate?

Private-to-Private Collaboration w/ Public Participation

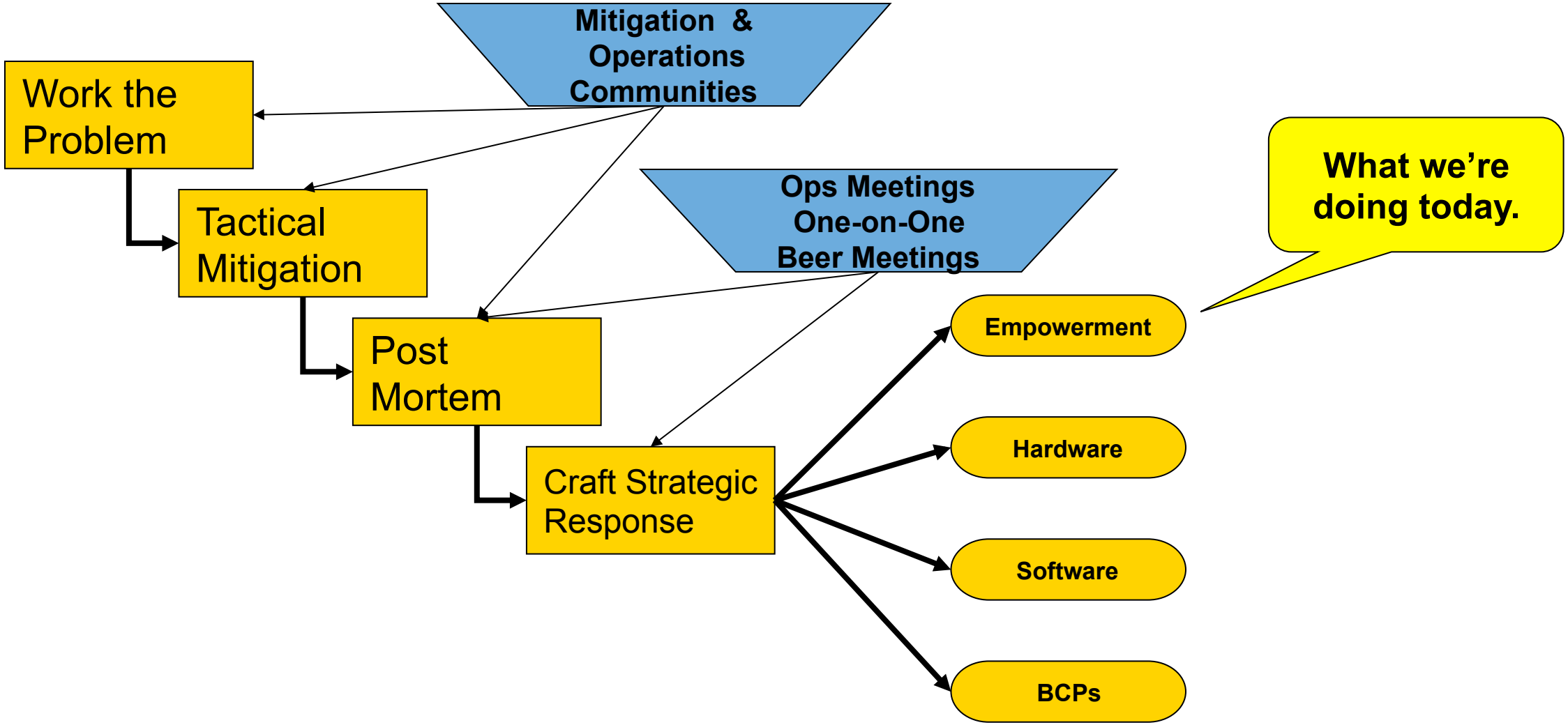
- Our industry effectiveness is based on private industry's ability to collaborate with their peers (i.e. many time competitors).
- We share information, exchange data, do join investigative work.
- Once there is enough understanding of the threat actors, private industry reached out to public (law enforcement) to move to next stage of the investigation.

Miscreant - Incident Economic Cycles



These Cycles Repeat

The Original Model



The Original Top 10

- **Prepare your NOC** - Ensure everyone in the NOC/SOC knows how to use the entire toolkit.
- **Mitigation Communities** - Invest in Communities of peer who you work with to investigate and resolve the security issues facing your customers.
- **iNOC-DBA Hotline (Inter ASN Communication)** - have clear inter-ASN communications that allows NOCs to talk to NOC. This enables the direct communications required to investigate, mitigate, and remediation security incidents.
- **Point Protection on Every Device** - Assume the whole network is a potential threat vector. Each element on the network requires point protection to minimize the threat.
- **Edge Protection** - Protection tools on the edge of the ASN

The Original Top 10

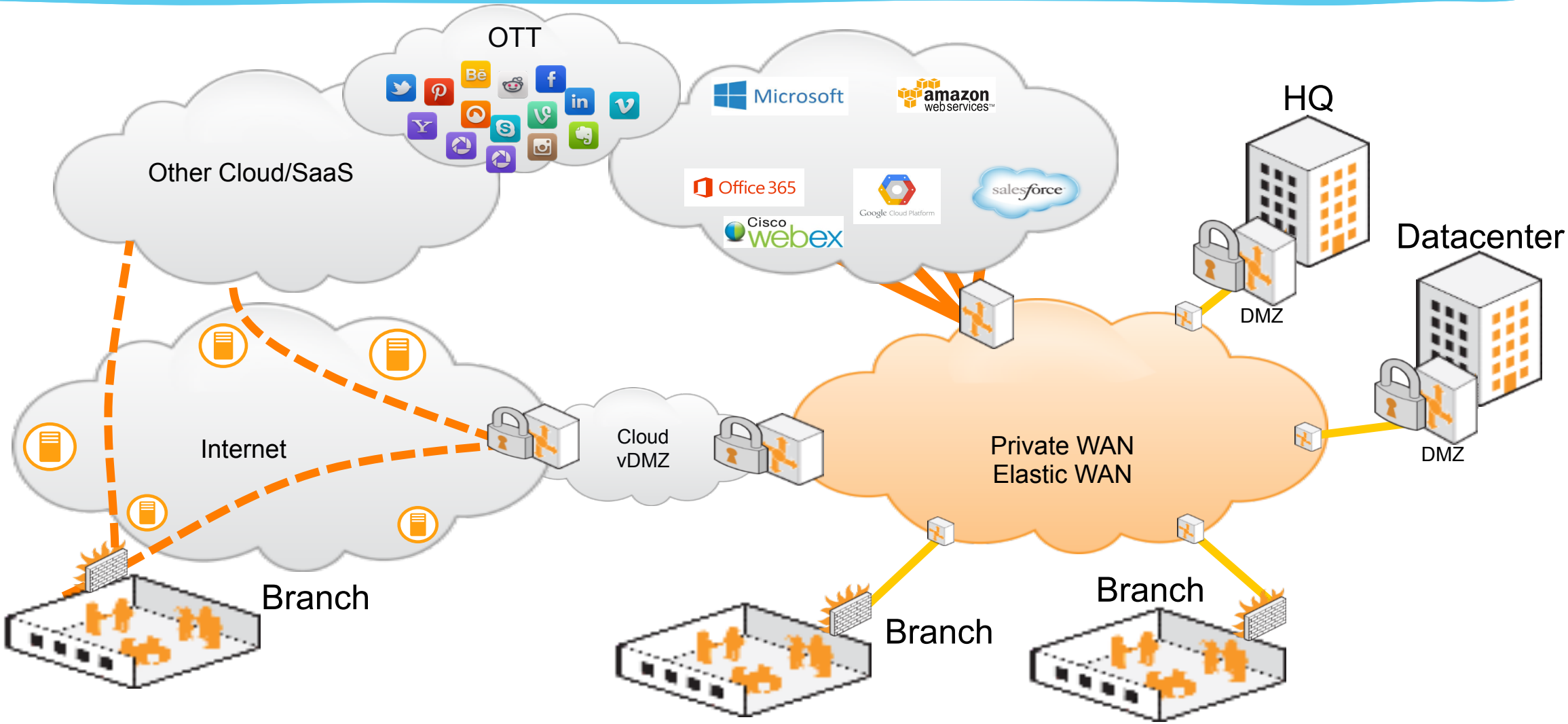
- **Remote Triggered Black Hole Filtering** - Set up BGP & MPLS to use the full strength of “moving/removing” traffic flows updated at routing protocol speeds.
- **Sink Holes** - Set up sections of the network to move bad traffic to sections that allow for detailed forensics.
- **Source Address Validation on all customer traffic**. All device traffic should be checked to ensure the source address and DSCP and other spoofable fields are validated.
- **Control Plane Protection -** Today’s Control Plan protection expands beyond routing protocols. “Controllers,” cloud systems, and configurations systems all expand the surface area of attack.
- **Total Visibility (**Data Harvesting – Data Mining). Traceback, backtrace, PCAPs, and extensive visibility logs are essential.

A Typical Example of a “Workshop”

- http://www.senki.org/sp-security/maawg-2012-security-workshop/

- Segment 1 – Top SP Security Essential Technique (Video) (Slides)
- Segment 2 – Types of Malware Problems ISPs Encounter (Video) (Slides)
- Segment 3 – Understanding the Threat: A Cyber-Criminal’s Work Day & Cyber-Criminal Behavior Drivers (Video) (Slides)
- Segment 4 – Turning Point – Strategy for Change (Video) (Slides)
- Segment 5 – Remediating Violated Customers (Video) (Slides)
- Segment 6 – US FCC’s Anti-Botnet Code of Conduct (ABC’s for ISPs) – Overview & Code on a Shoestring Budget (Video) (Slides)

The World has Changed



It is time for a Refresh

- We will build a new set of “Operator’s Security Toolkit.”
- The materials will be used @ tutorials in the Internet Operations Meeting (see http://www.senki.org/sp-security/network-operations-groups-meeting/) with “passionate presenters.”
- We will learn from the past, this time having White Paper/ Guides, Presentation Materials, and Labs.
- “Customer RFP Checklist,” Targeted Interaction @ NOGs, and Smoke Jumping

What is Smoke Jumping?

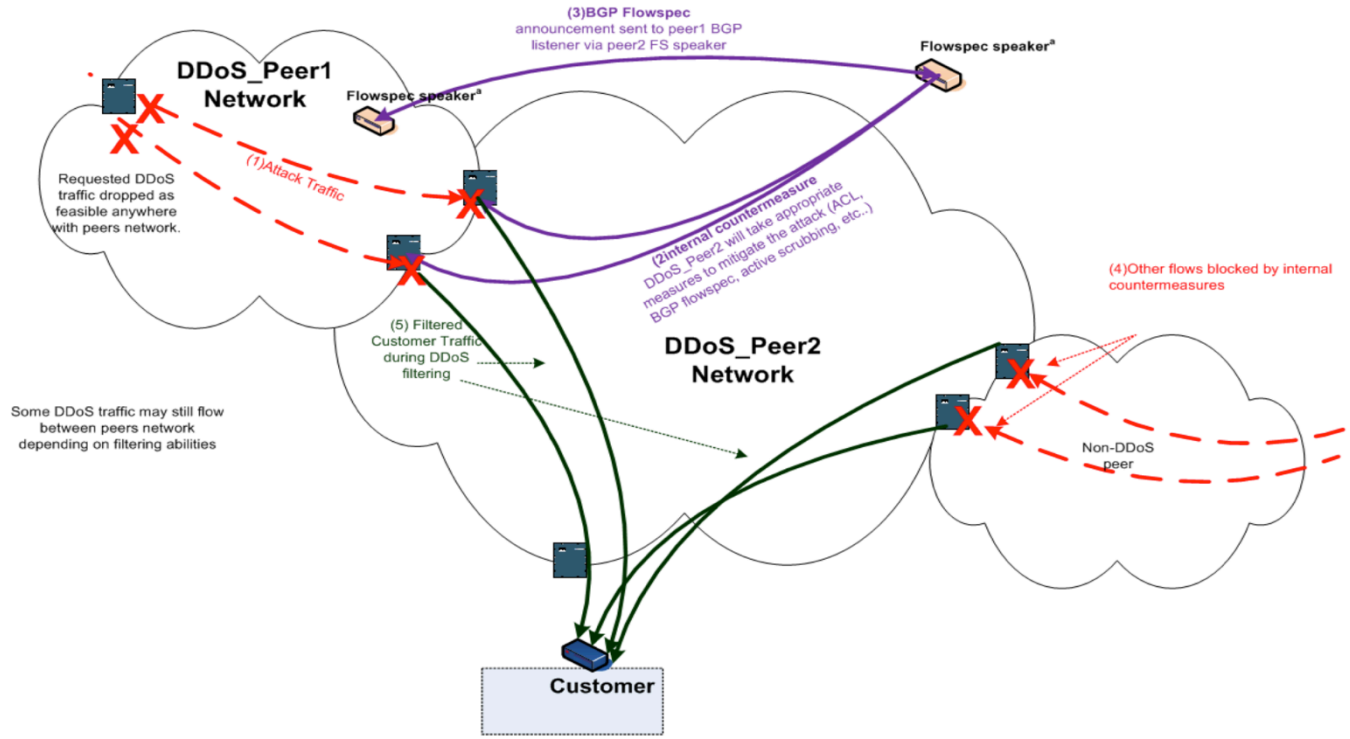
- Smoke Jumping is a “security intervention” technique where we have a team of “volunteers” or ”vendors” target an Operator (ASN) who has known “Hot Spots” of nefarious activities.
- The Team works with the Operator to deploy the “Security Toolkit” to mitigate the risk AND to set up telemetry to “clear the path” for investigation/operation actions.

Working the 40/40/20 Rule

- Sean Donelan's (back in his SBC days) [sean@donelan.com] rule for end point patching:
  - 40% of the customers care and will proactively patch
  - 40% of the customers may someday care and fix/patch/ delouse their machines
  - 20% of the customers just do not care and have never responded to any effort to fix them.

We Evolve – DDOS Peering

Multi-ASN Collaborative Flow-Spec … Community Collaboration



Operationalizing ISP cooperation during DDoS attacks (NANOG 71)
https://pc.nanog.org/static/published/meetings//NANOG71/daily/day_4.html#1447

The Human Network is the #1 Security Tool

"Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool."

Barry Raveendran Greene

Example of Specializations

- Situational Consultation (Map the Crime Vector): **OPSEC Trust's Main Team**
- Situational Awareness: BTFC, Anti-S, SCADASEC (and others)
- Dissecting Malware: **YASMIL, II** (perhaps MWP)
- Big Back Bone Security and IP Based Remediation: **NSP-SEC**
- Domain Name Takedown: **NX-Domain**
- DNS System Security: **DNS-OARC**
- Anti SPAM, Phishing, and Crime: **MAAWG & APWG**
- Vulnerability Management: **FIRST**
- Many other Confidential Groups specializing into specific areas, issues, incidents, and vulnerabilities.
- Investigative Portals providing focused, confidential investigation: **OPSEC Trust Investigative Teams**

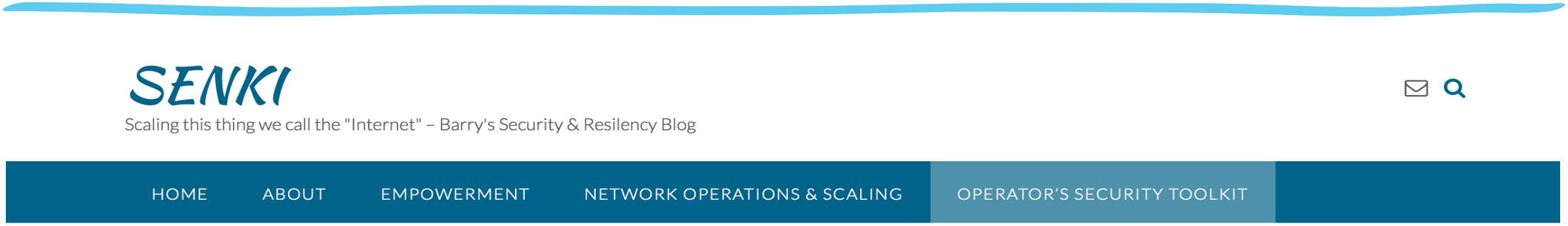
Results – DNS Changer Take Down

- The "DNS Changer" (aka ‘Ghost Click’) crew that has been hijacking your constituent's DNS configs were arrested, infrastructure seized, and a major data center shutdown.
- www.dcwg.org

How to Participate Workshops??

- E-mail Barry Greene - bgreene@senki.org
- Does your Community Need a Workshop: Ask. There are people who will help you make it happen.
- Presenter Interest: Are you interested to be one of the presenters? This effort will take a couple of years before Operators are “motivated” to ”invest” in the Security Toolkit.
- Will be using OPS-T Main, CW, NSP-SEC, ISOI, and FIRST and the forums to send progress updates.

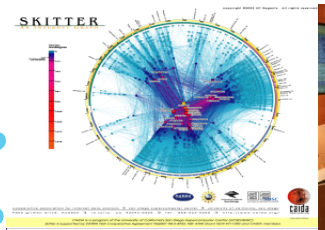
Operators Security Toolkit Slides & Papers

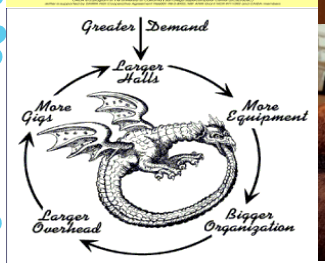


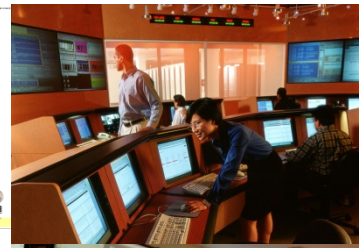
http://www.senki.org/sp-security/operators-security-toolkit/

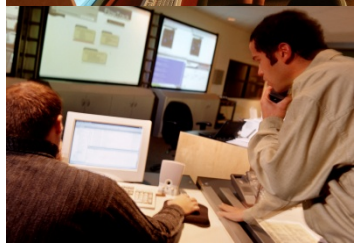
Barry Raveendran Greene bgreene@senki.org

Top Operator Security Tools
The Executive Summary







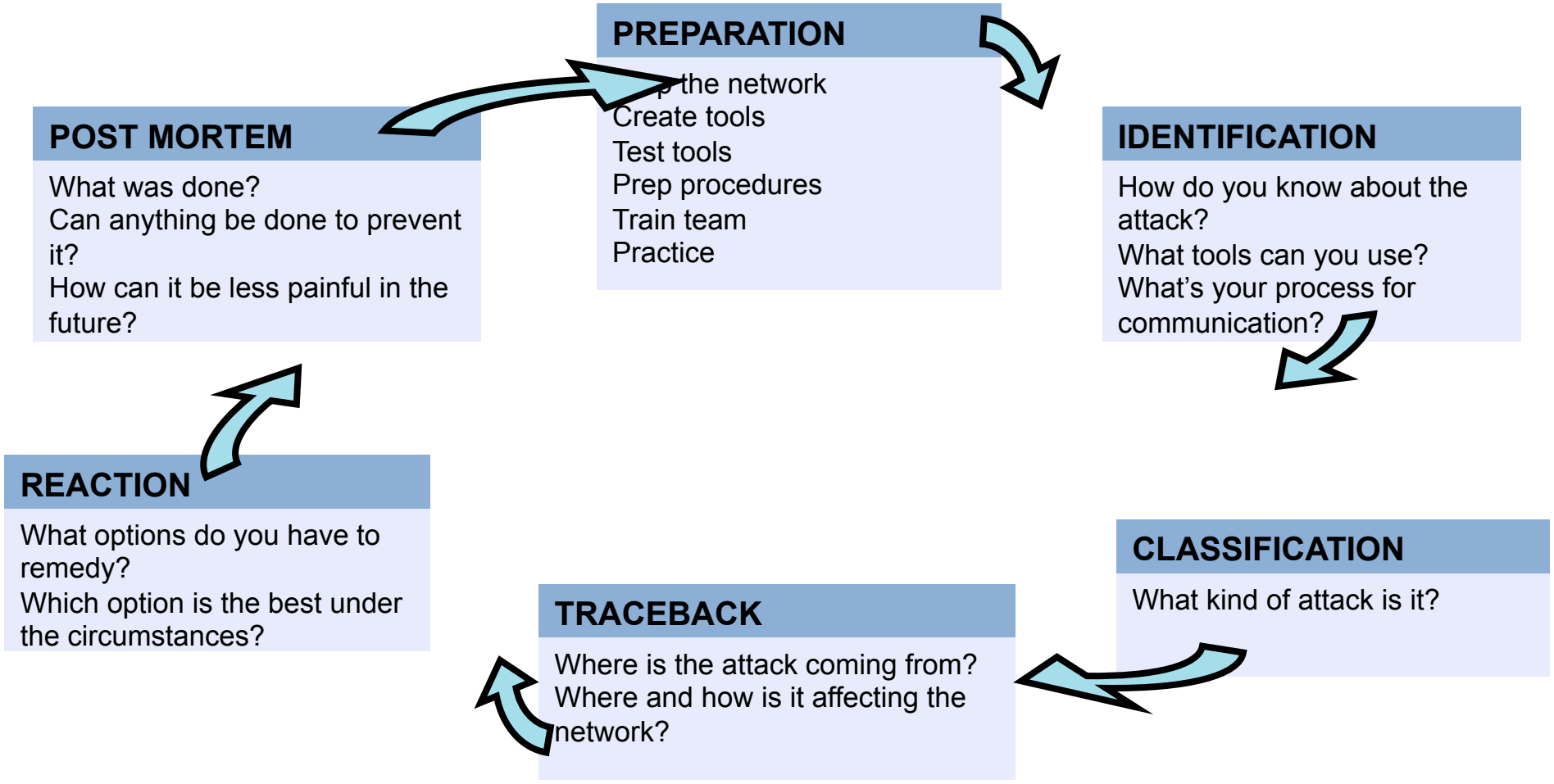


Top List of Operator Security Fundamentals

- Prepare your NOC
- Mitigation Communities
- Peer Communication in a Crisis
- Point Protection on Every Device
- Edge Protection
- Remote triggered black hole filtering
- Sink holes
- Source address validation on all customer traffic
- Control Plane Protection
- Total Visibility (Data Harvesting – Data Mining)
- Remediating Victimized Customers
- DNS Resolver as a Security Tool

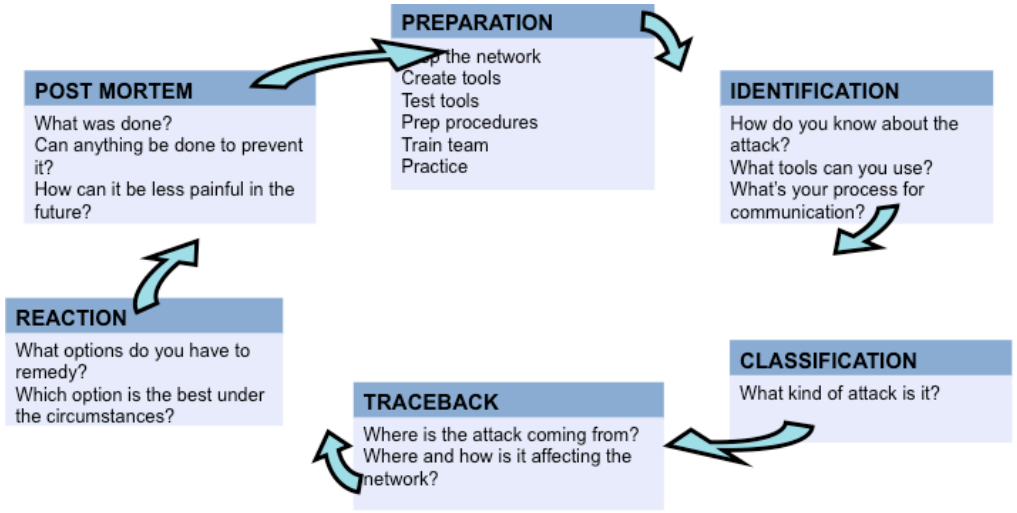
This list applies to Enterprises, Banks, Governments, On-line providers, Cloud deployments, etc …

Operator’s Security in the NOC - Prepare

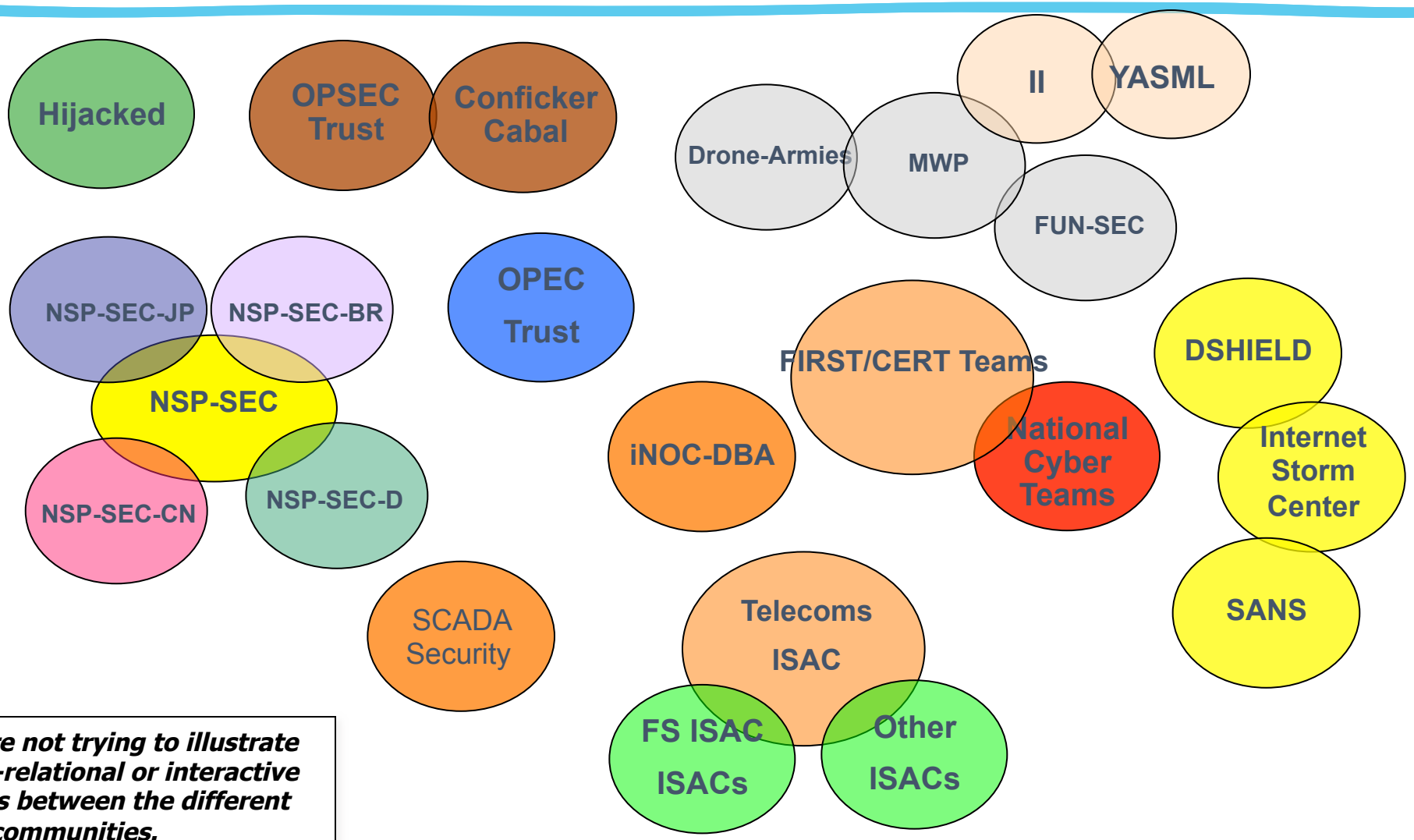


Operator’s Security in the NOC - Prepare

- Critical Conversation:
  - What are your processes to respond to an attack?
  - How do you work with Law Enforcement when attacked?
  - How fast can you patch when there is critical vulnerability?
  - How are your security operations team organized?
  - How can we work better together?



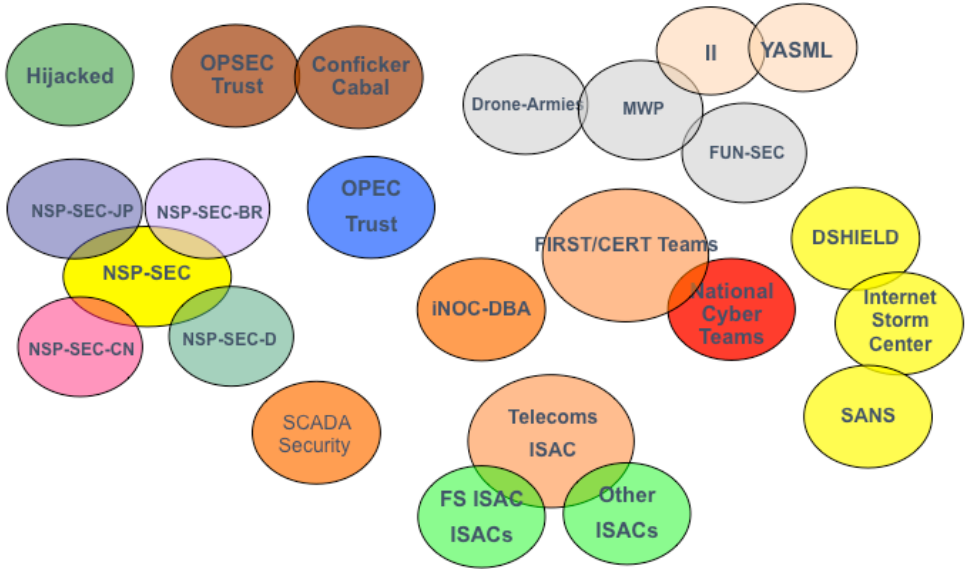
Aggressive Collaboration is the Key



Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.

Aggressive Collaboration is the Key

- Critical Conversation:
  - What Security Organizations are you actively participating?
  - How are these organization helping your customers?
  - Do you share security telemetry to these groups?
  - Do you pull in security telemetry from any of these groups?
  - How can there be a better security organization?



Peer Communication in a Crisis

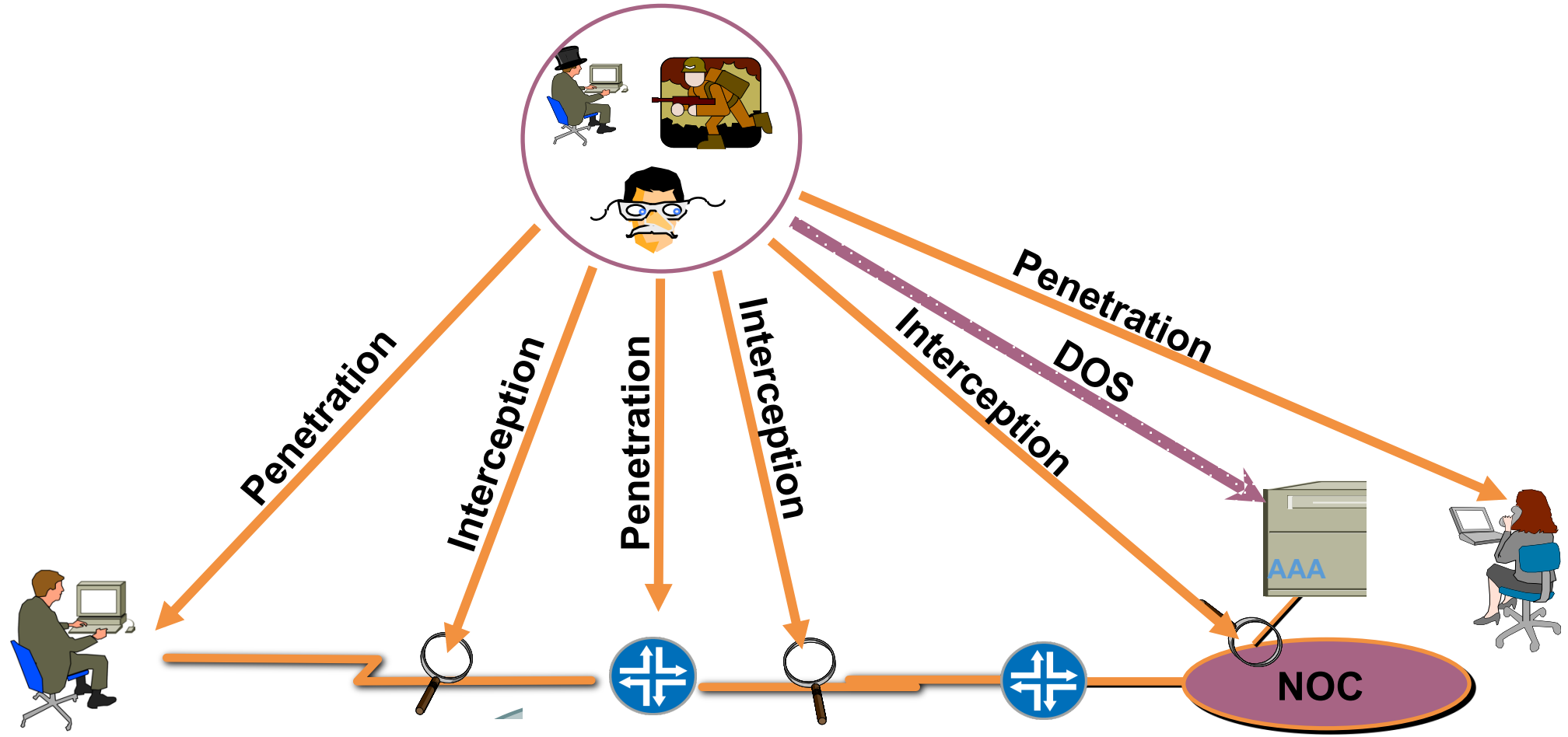
- Build the direct peer to peer communications channels and out of band access before there is a security crisis.
- Examples:
  - INOC-DBA: *Inter-NOC Dial-By-ASN*
  - Whatsapp
  - Slack

- The key is a system that works during a Inter-ASN Crisis

Peer Communication in a Crisis

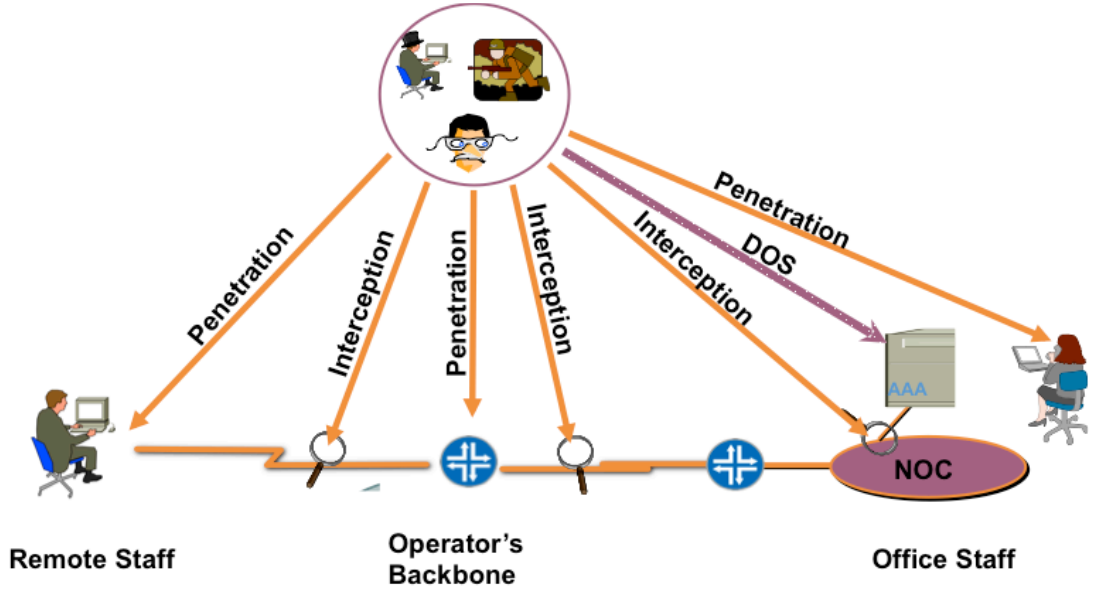
- Critical Conversations:
  - How do you work with your peers (competitors) during a crisis?
  - What happens when the mobile phone system fails?
  - What happen when the Internet is impacted?
  - Do you test these systems?
  - How can we help build better crisis communications?

Point Protection

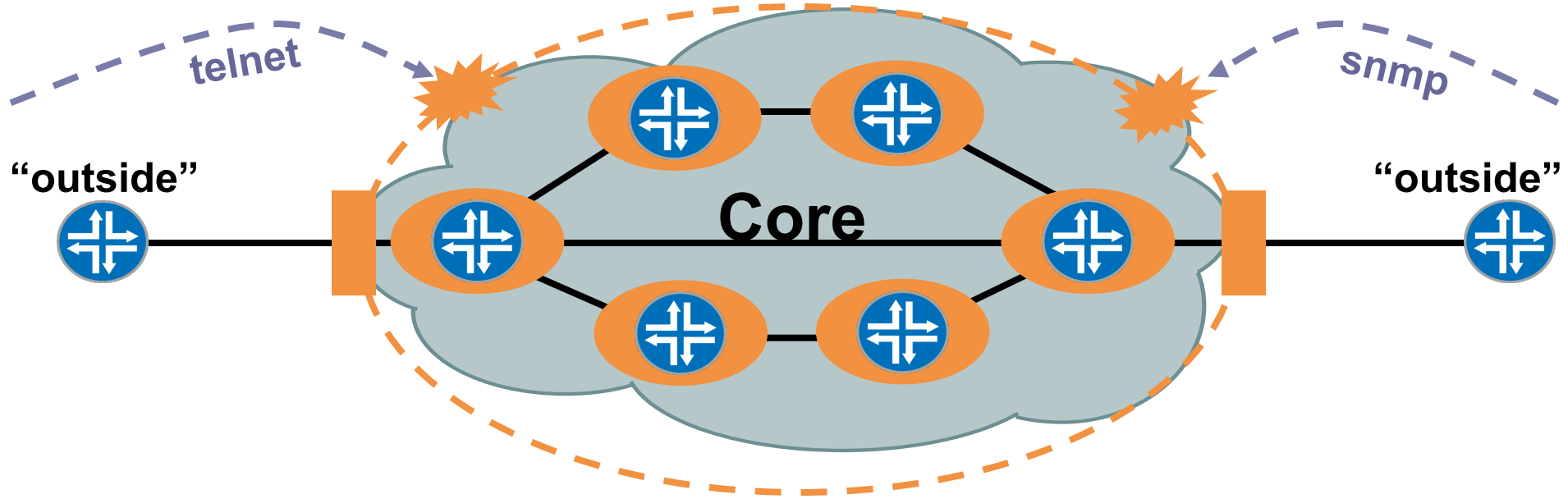


Point Protection

- Critical Conversations:
  - Do you have Exploitable Port Filtering on your ingress & egress?
  - Are you logging the scans on your infrastructure?
  - Are you tracking the interest on your infrastructure?
  - What can we do to help?



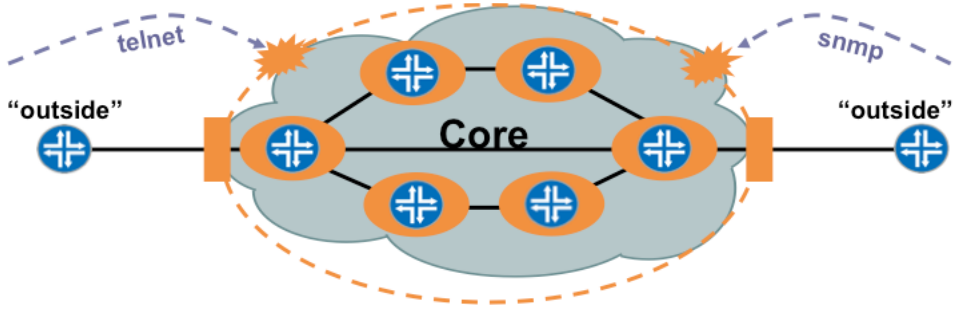
Edge Protection



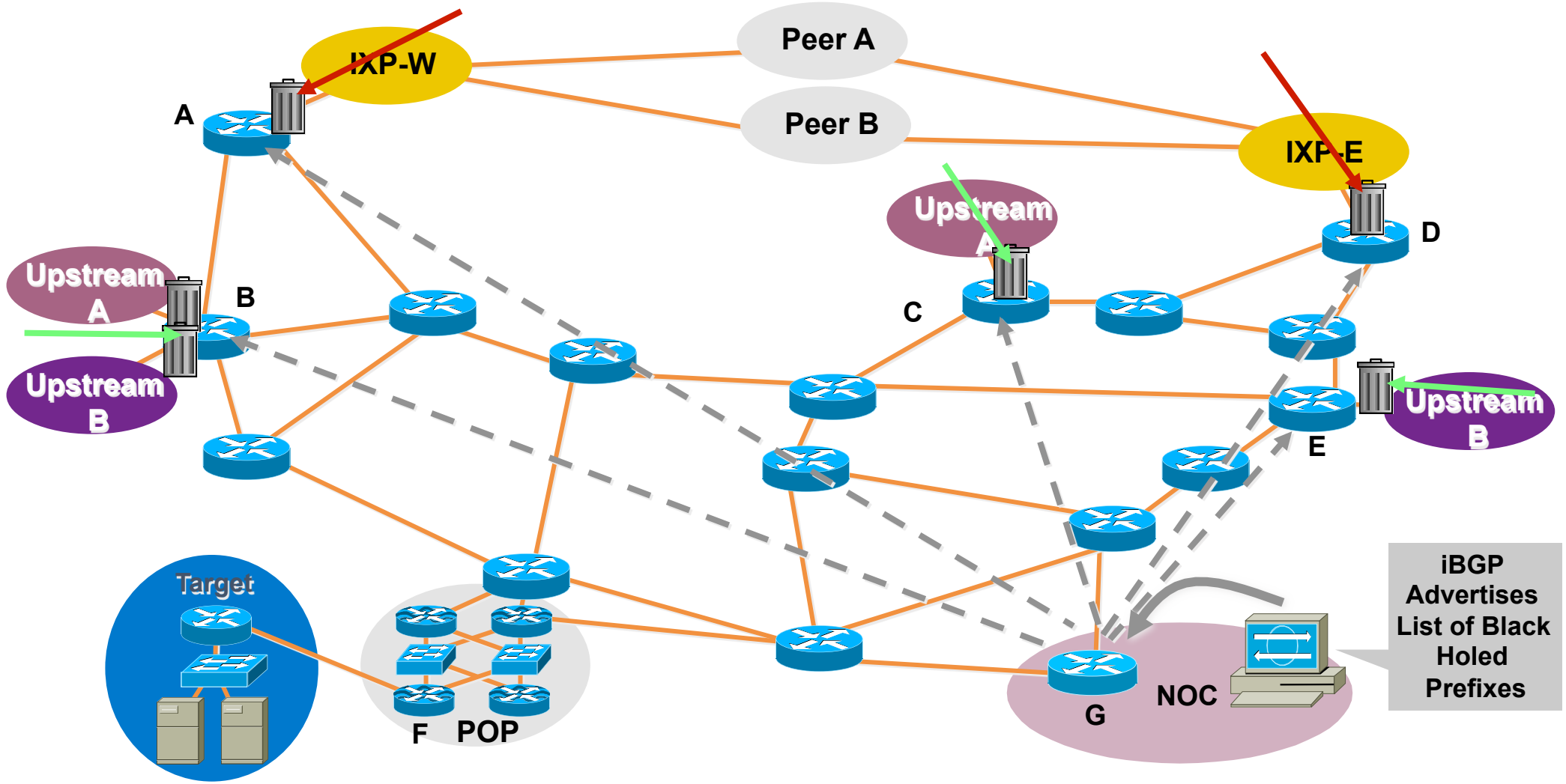
- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Edge Protection

- Critical Conversation:
  - How do you segment your network to protect from outside & inside attack?
  - How do you respond to probes against critical infrastructure (i.e. SIP/ Voice gateways)?
  - How can we help?

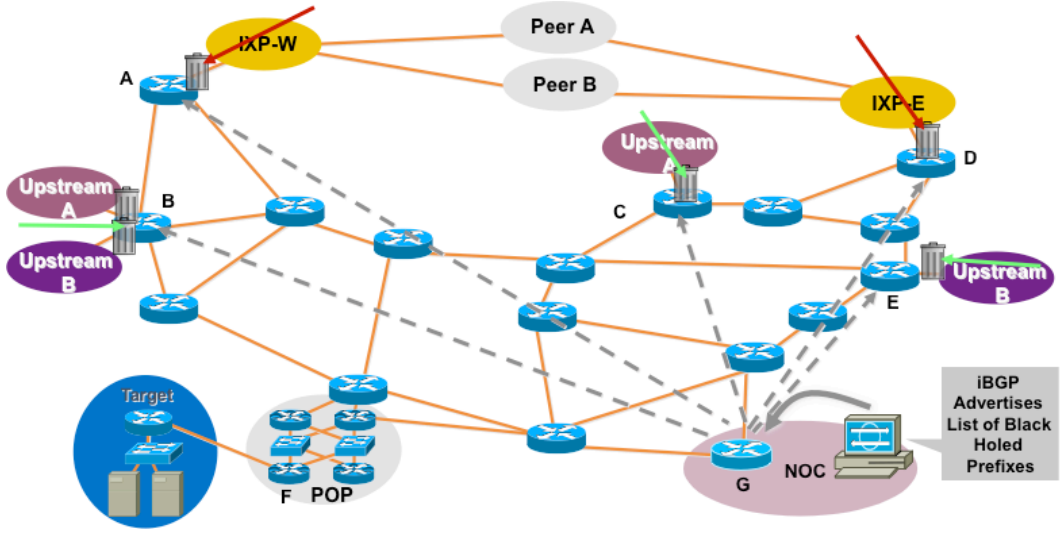


Destination Based RTBH

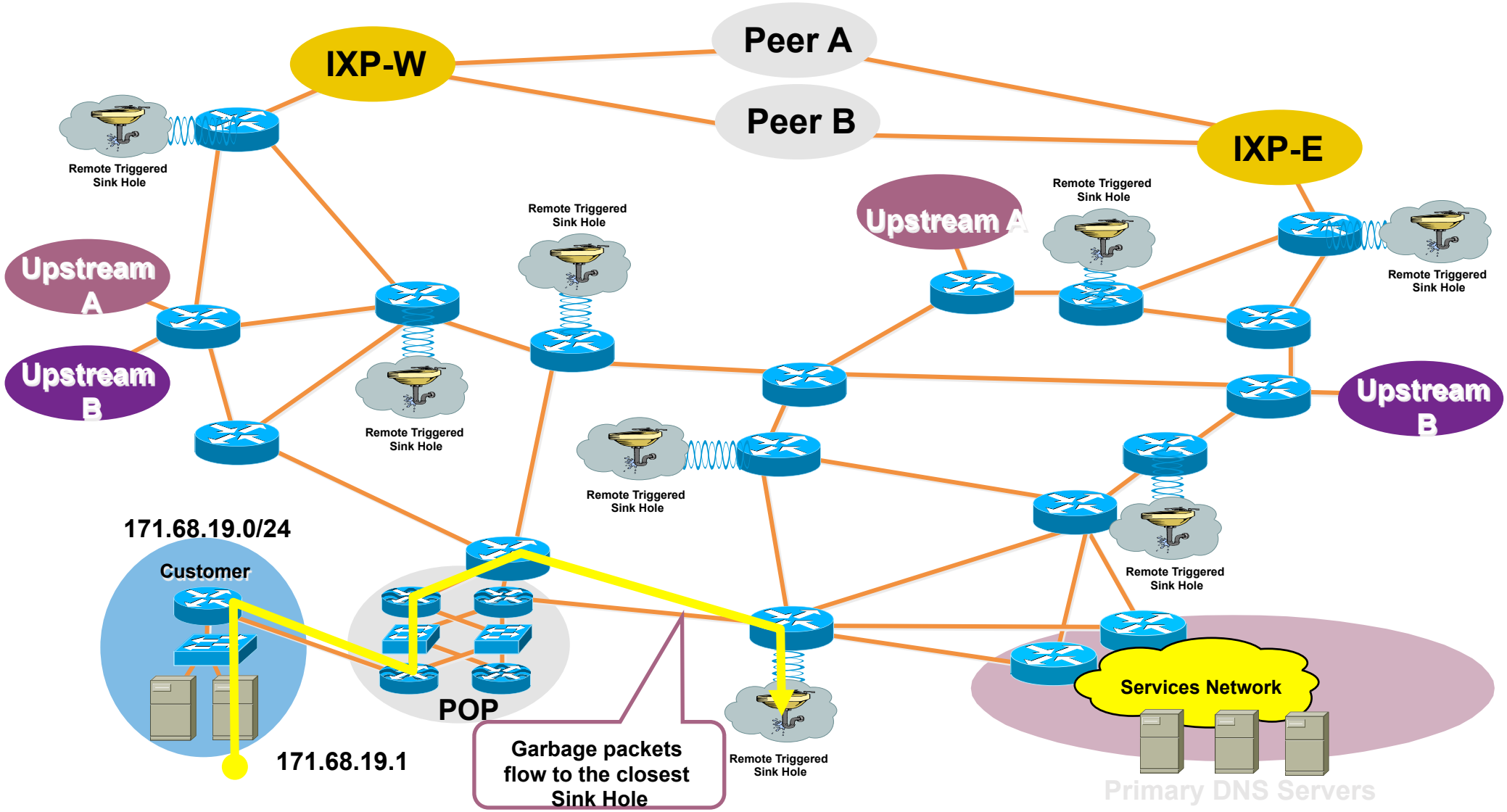


Destination Based RTBH

- Critical Conversations:
  - Have you deployed BGP Community Based RTBH?
  - Have you deployed FlowSpec?
  - How often do you use RTBH?
  - How can a customer or another agency work with you to deploy RTBH?
  - Do you have the protections in place to ensure you do not leak?

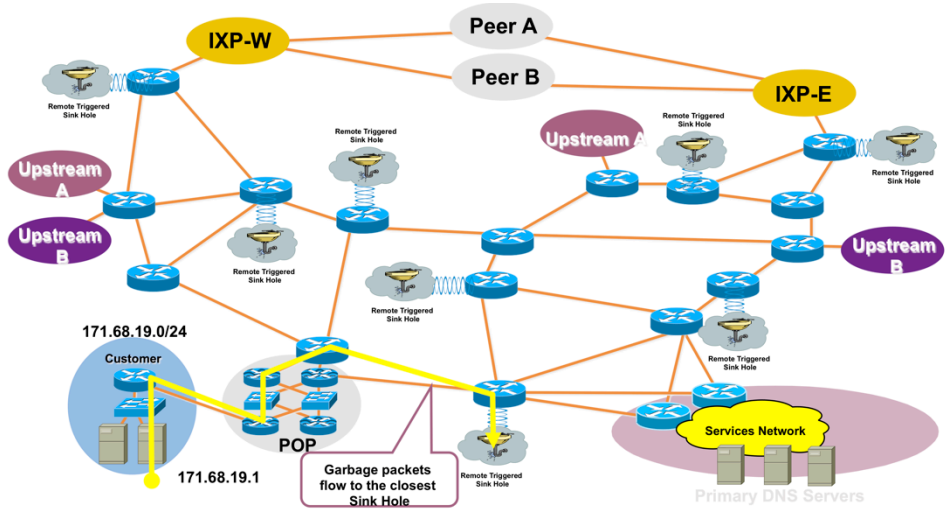


Sink Holes


IXP-W
Peer A
Peer B
IXP-E
Remote Triggered Sink Hole
Upstream A
Upstream B
Upstream A
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
171.68.19.0/24
Customer
POP
171.68.19.1
Garbage packets flow to the closest Sink Hole
Services Network
Primary DNS Servers

Sink Holes

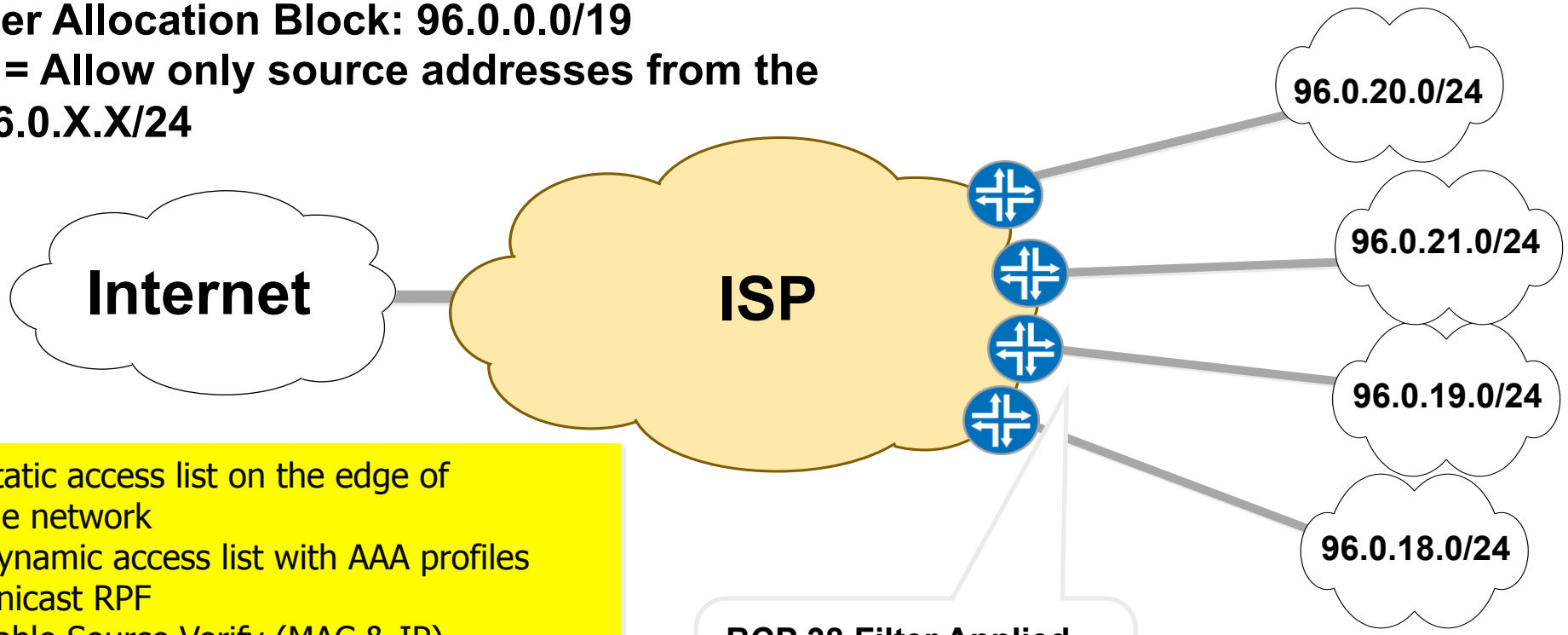
- Critical Conversations:
  - Do you have Sink Holes built into your network?
  - What sensors/monitoring is set up in your sink holes?
  - Can you shunt an attack into a Sink Hole?
  - Have you set up DNS Sink Holes?
  - Do you coordinate your Sink Hole activity with your peers?



SAV - BCP 38 Ingress Packet Filtering

Source Address Validation (SAV) & IETF's Best Common Practice 38 are Critical to Internet Operations

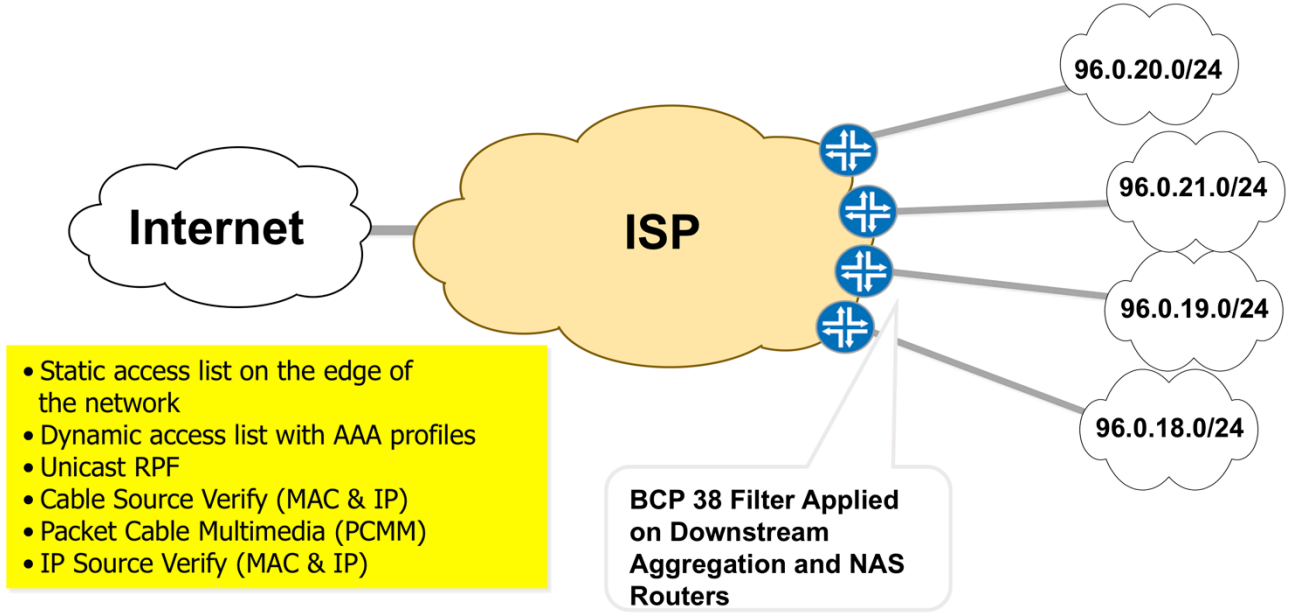
ISP's Customer Allocation Block: 96.0.0.0/19
BCP 38 Filter = Allow only source addresses from the customer's 96.0.X.X/24



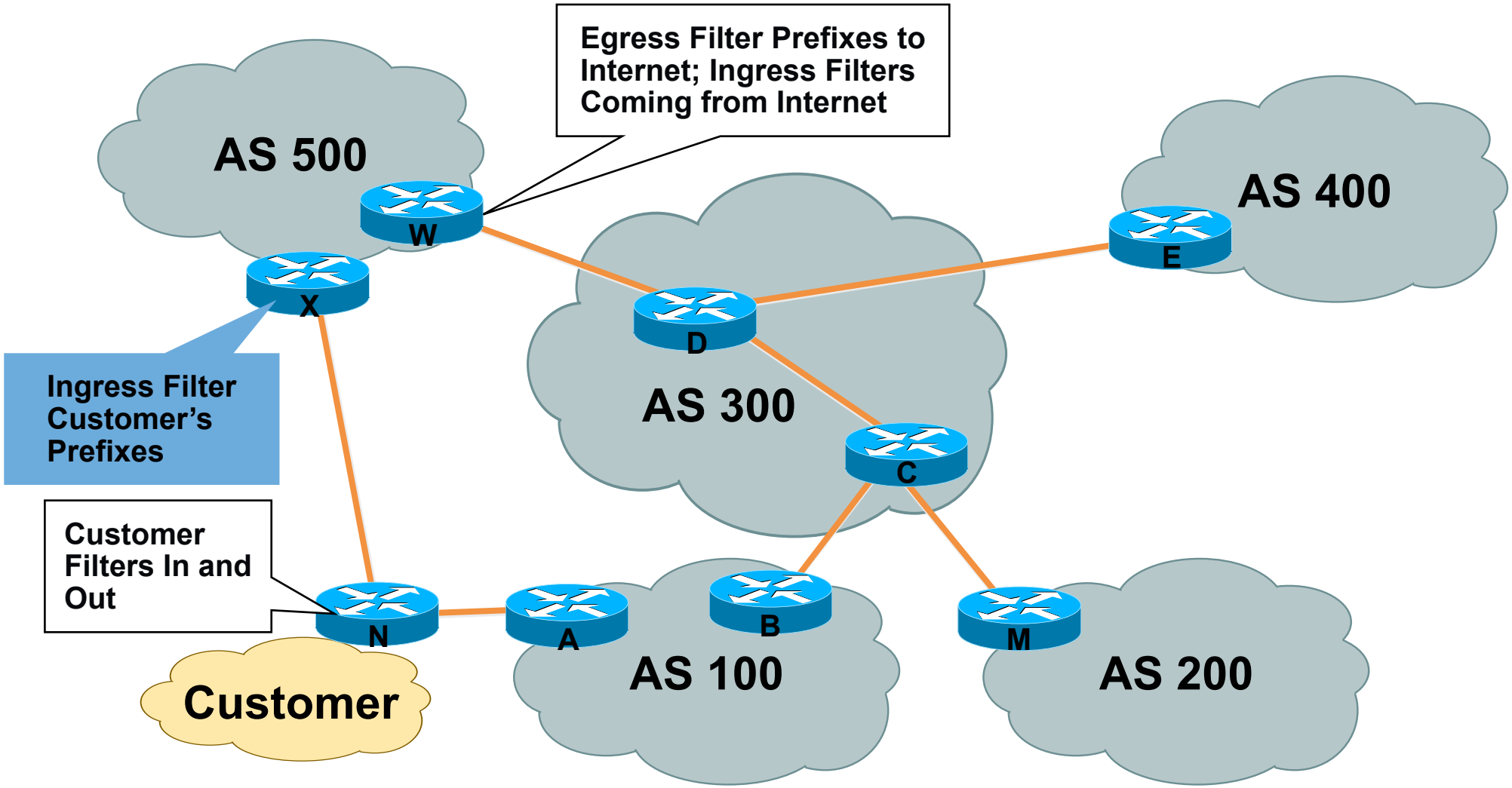
- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)

SAV - BCP 38 Ingress Packet Filtering

- Critical Conversations:
  - Do you have SAV deployed for IPv4 & IPv6 in your network?
  - Which techniques do you use?
  - How do you monitor?
  - Do you participate with the Spoofer Project?

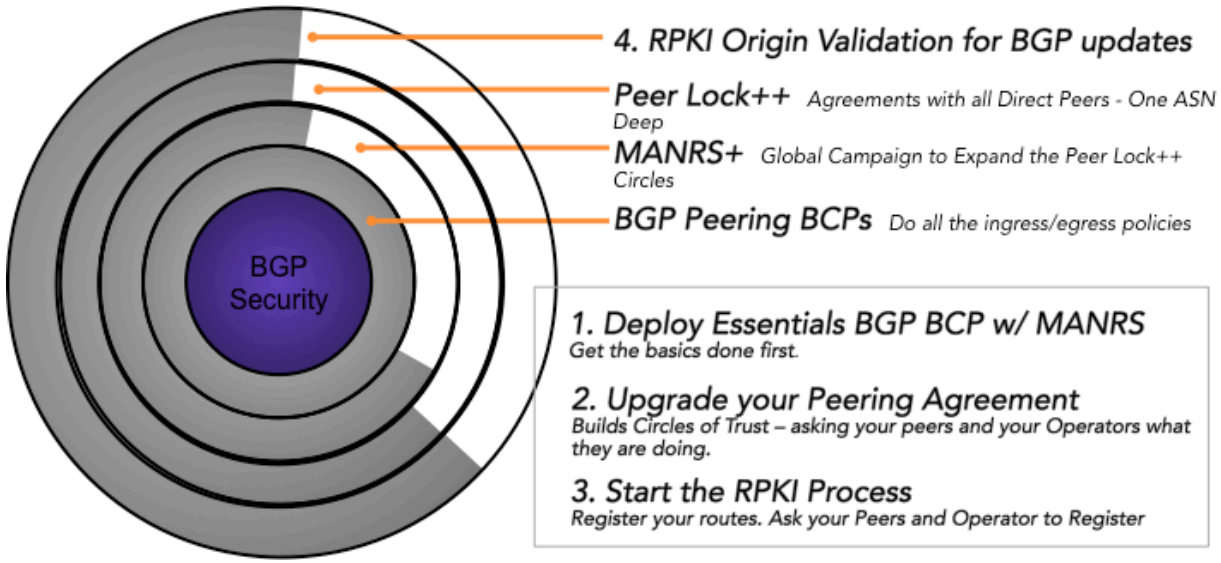


BGP Prefix Filtering



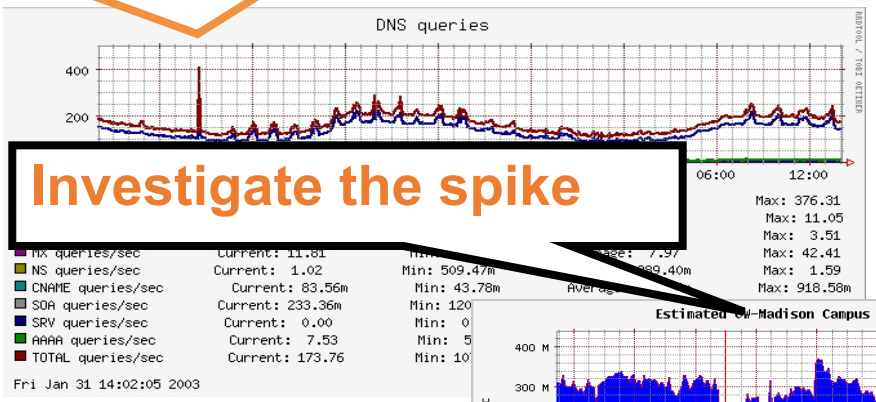
BGP Prefix Filtering?

- Critical Conversation:
  - Which BGP filtering techniques have you deployed?
  - How do you protect your network, services, and customers for BGP Hijack Attacks?
  - What can we do to help?

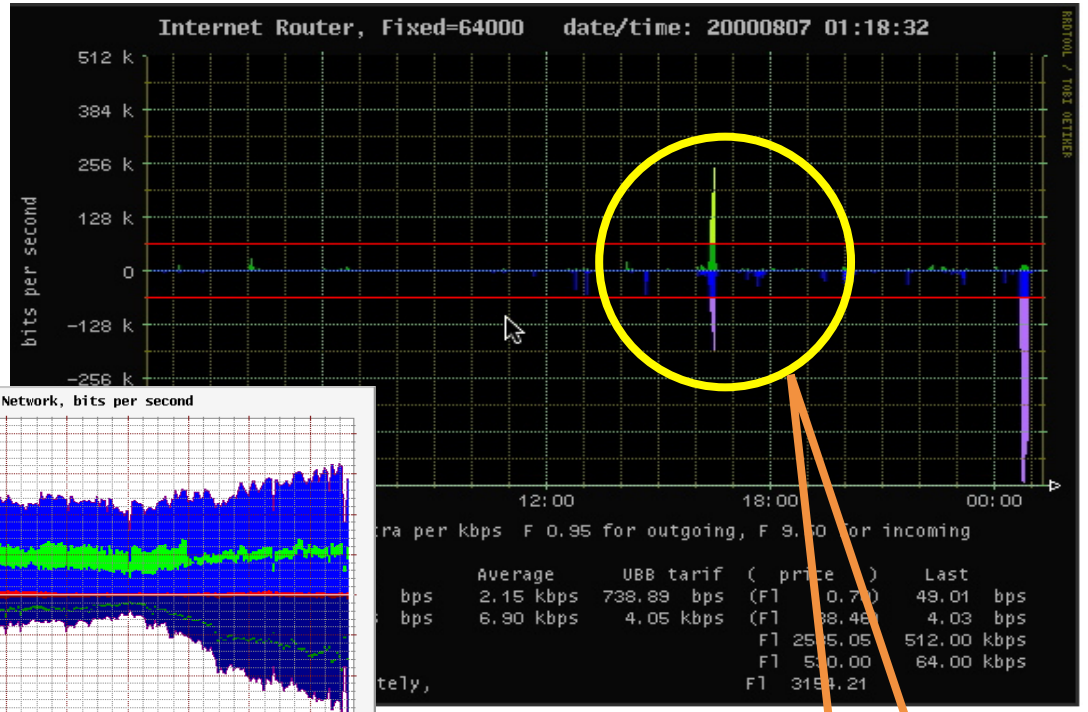


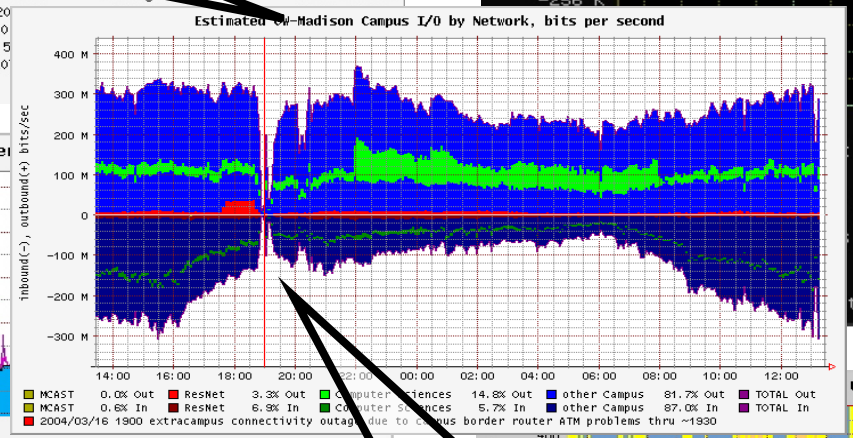
Total Visibility

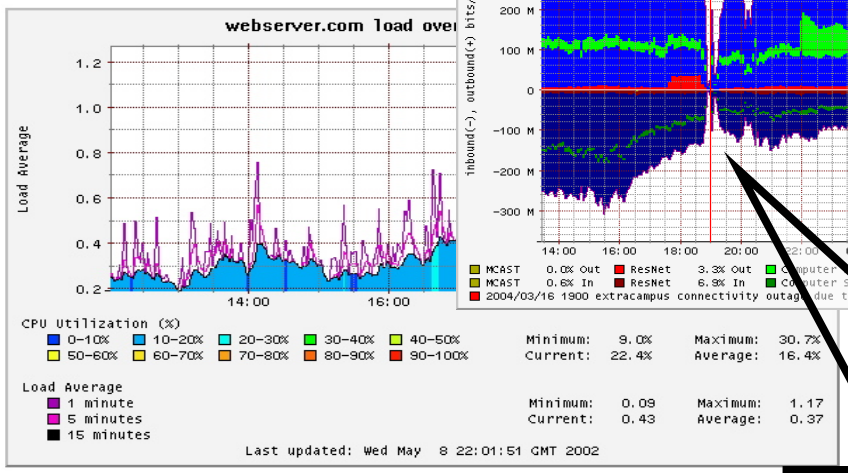
Anomaly for DNS Queries

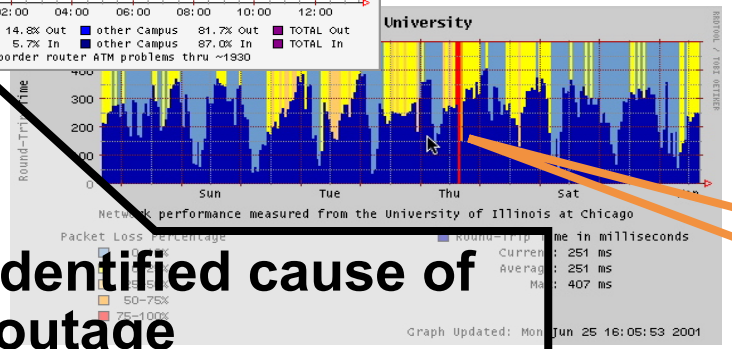


Investigate the spike









Thru'put Spike

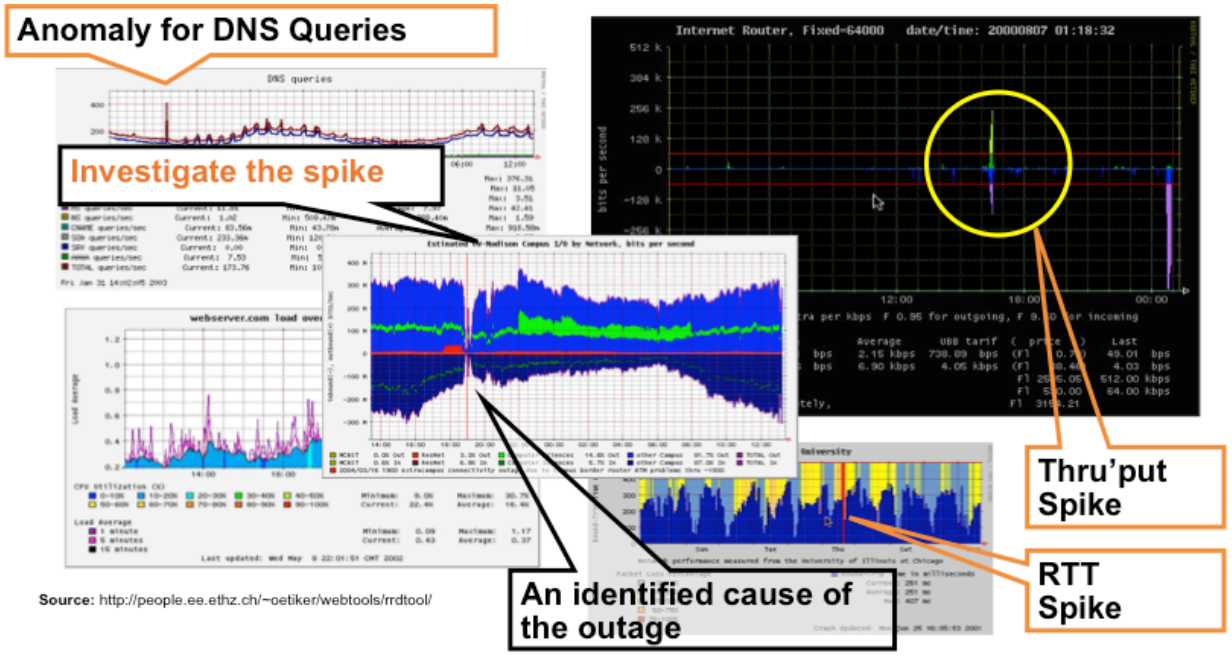
RTT Spike

An identified cause of the outage

Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

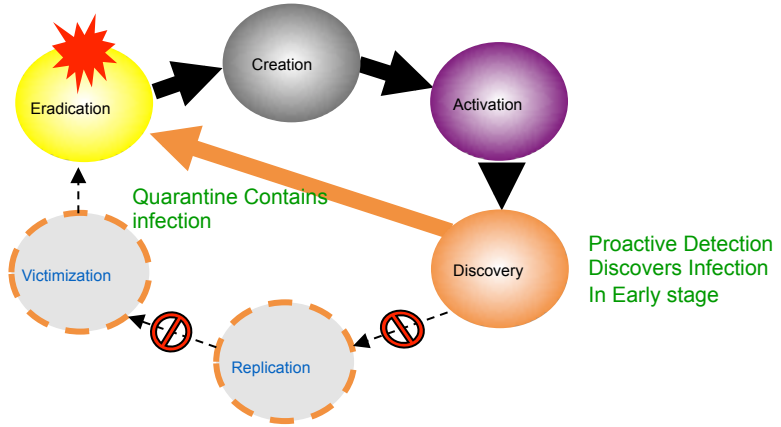
Total Visibility

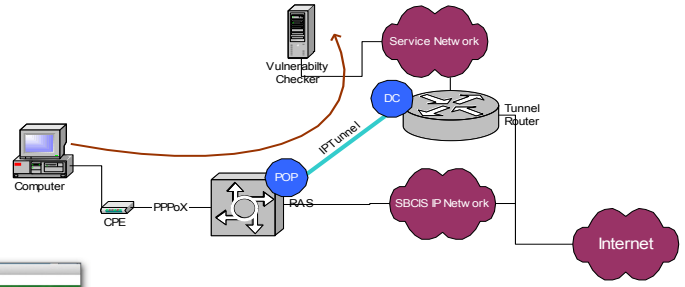
- Critical Conversations:
  - How do you maintain total visibility inside your network?
  - What tools do you use?
  - How do you use the tools for investigation?
  - How can we work together?

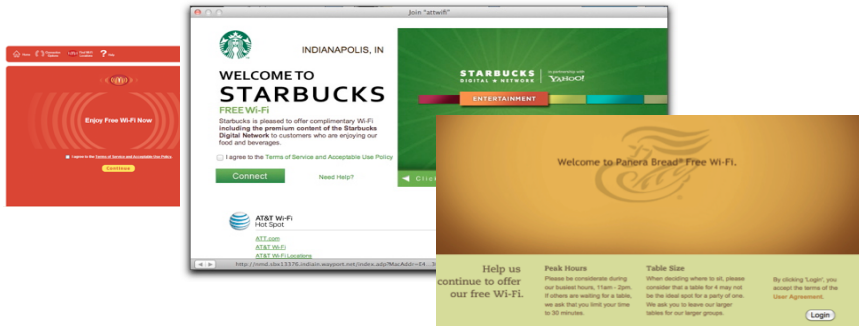


Remediating Violated Customers

- We have enough experience in the industry to move remediation of violated customers to a normal part of the business.
- Leaving violated customers on your network puts your whole operation at risk.

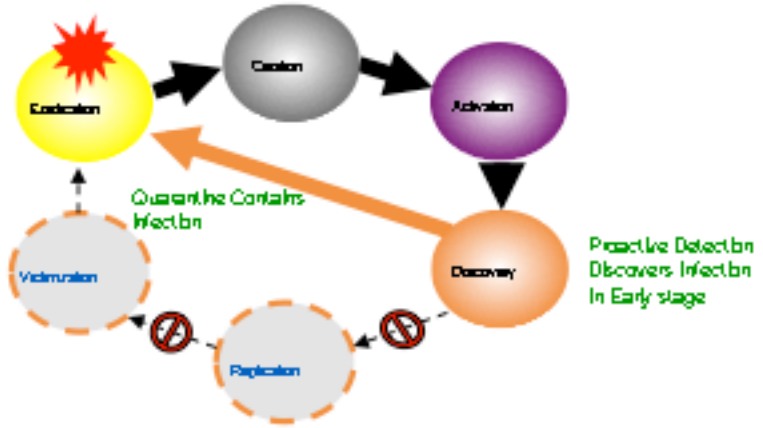






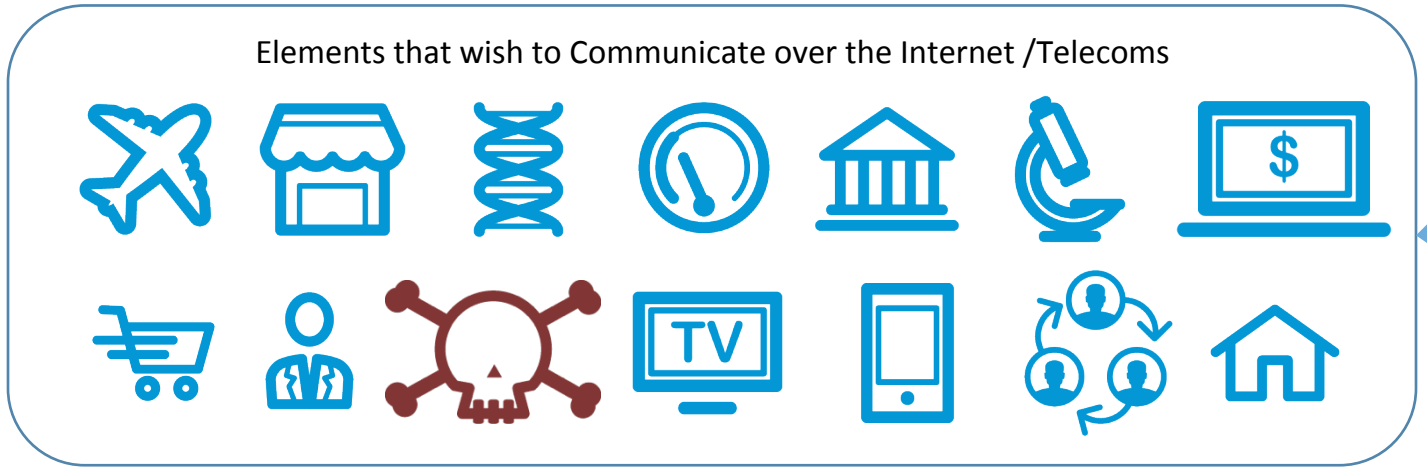
Remediating Violated Customers

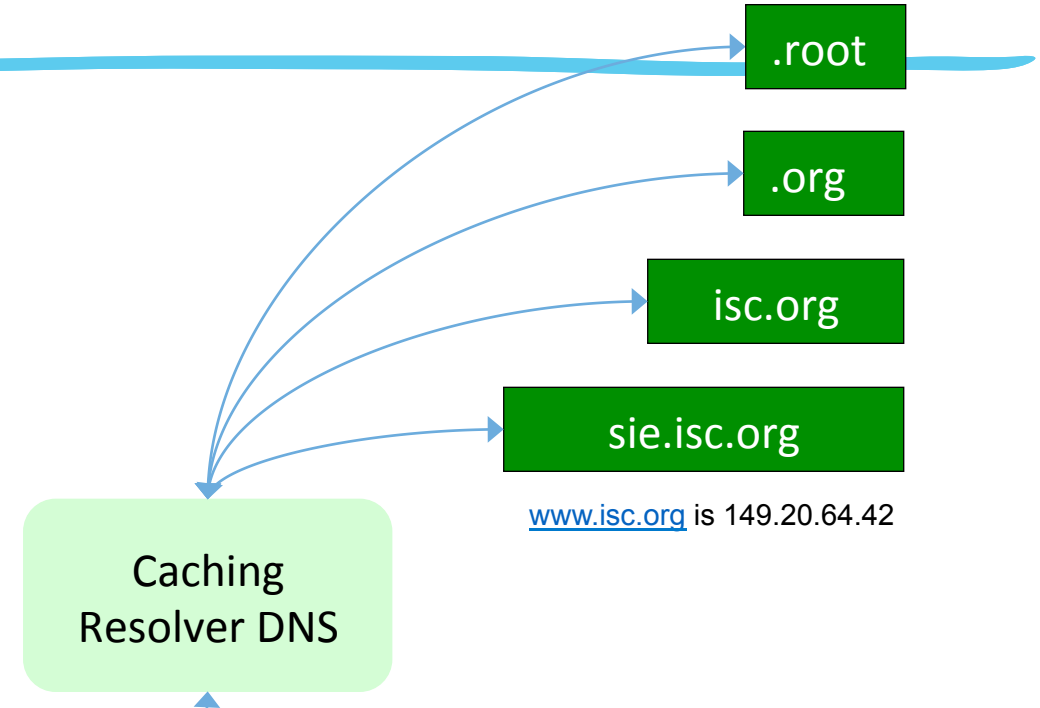
- Critical Conversations:
  - Do you notify your customers when you suspect they are violated with malware?
  - How do you notify?
  - What happens if they do not respond?
  - Where do you get your “you are infected” data?
  - How can we help?



Everything Must Use DNS!

- Everything on the Internet will be interacting with DNS in some way.
- IPv6 addressing will complicate applications, programs, services, and malware that tries to “hardcode” IPv6 into their software.
- Hardcoding IP addresses into malware makes it easy to reverse engineer the malware and blackhole/sinkhole the malware’s command and control.

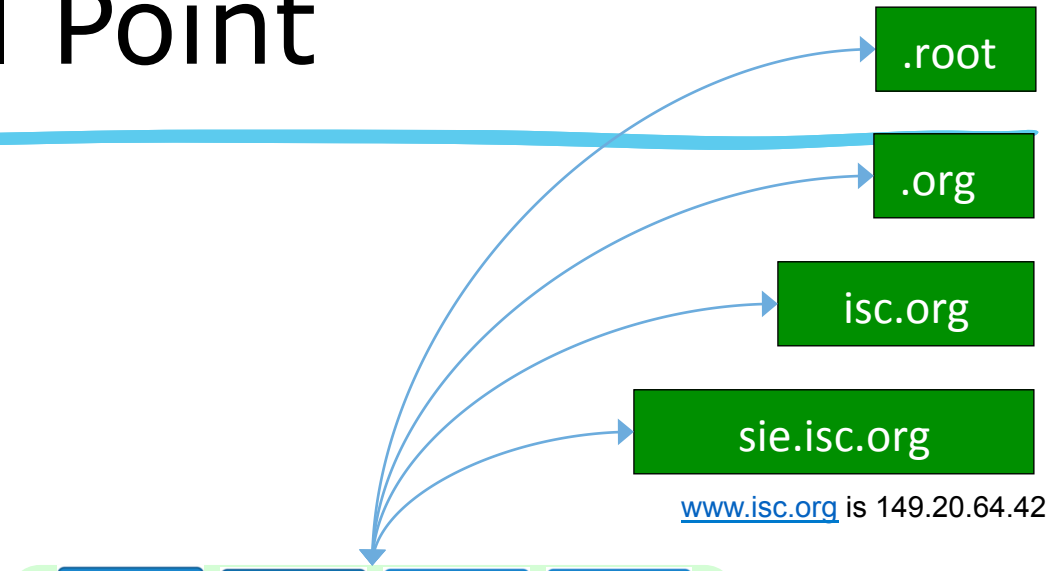


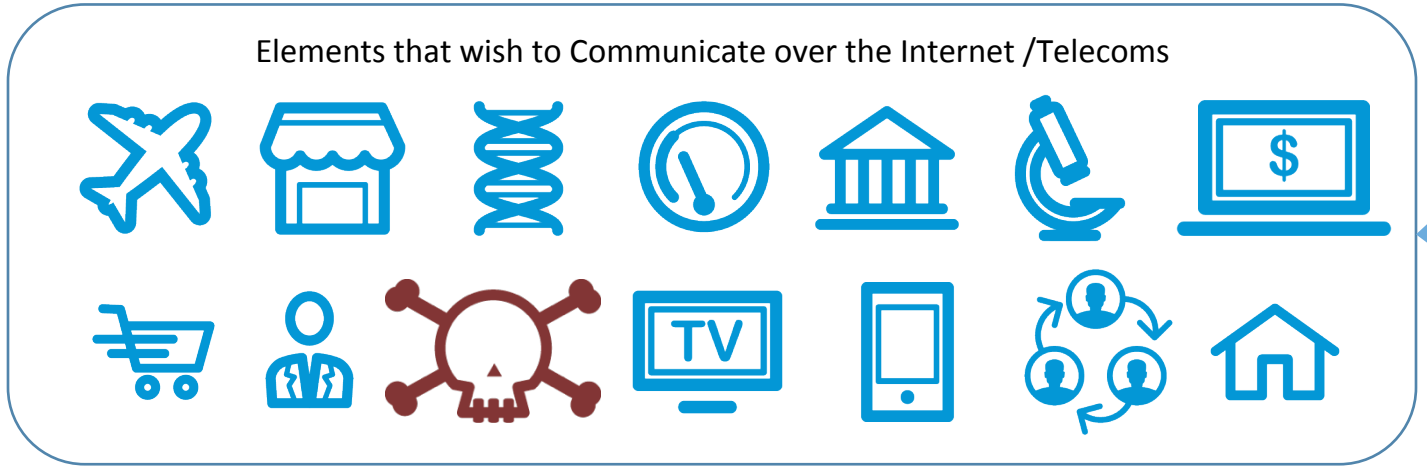


rDNS is a Logical Control Point

rDNS Control Point

- Business Intelligence
- Block Phishing
- Block Malware
- Block BOTNETs
- Parental Control
- Security Intelligence (What the bad guys are using DNS in their activities.
- Notifying Customers that they are infected with malware (Malware Remediation).

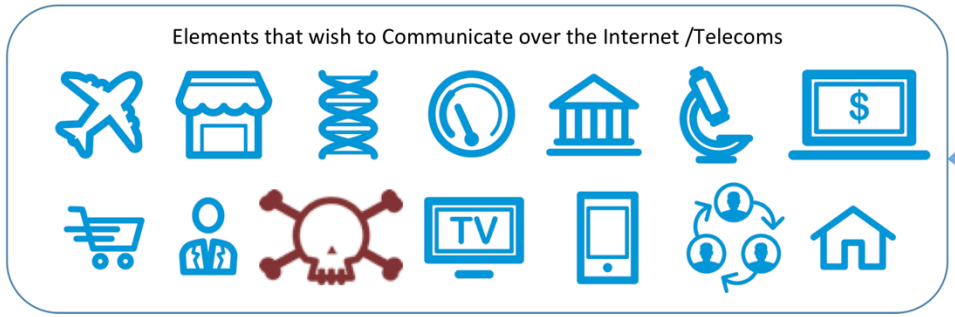


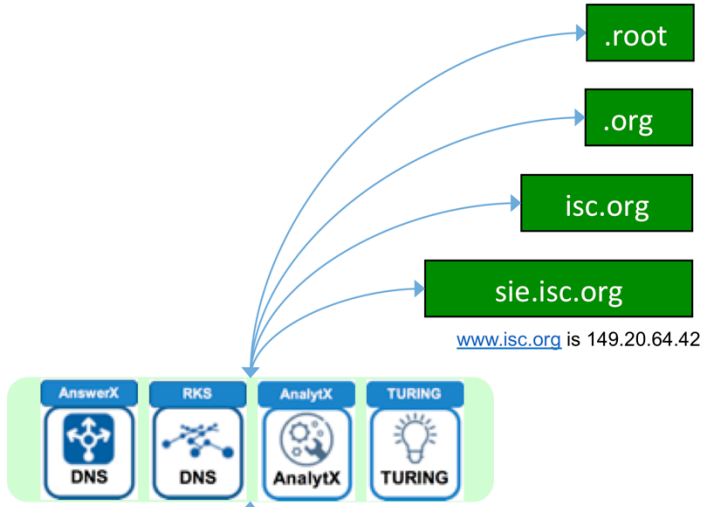


What is the IPv4 for www.isc.org?
What is the IPv6 for www.isc.org?
What is the DNSSEC Certificate for www.isc.org?
Where are my closest video gateways to www.isc.org (future of DNS)?

rDNS is a Logical Control Point

- Critical Conversations:
  - Have your turned your DNS Resolver into a security tool?
  - Are you using DNS RPZ?
  - Are you using your rDNS for customer notification?
  - Are you using commercial tools?
  - How can we help?





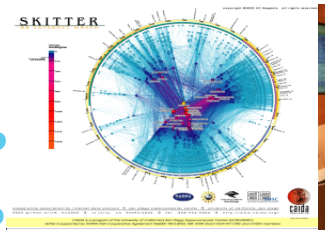
Operator Security Fundamentals

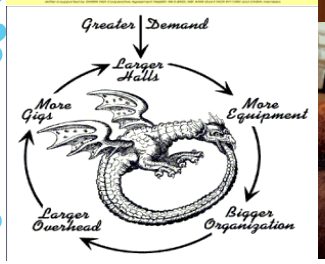
1. Prepare your NOC
2. Mitigation Communities
3. Peer Communication in a Crisis
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data Mining)
11. Remediating Victimized Customers
12. DNS Resolver as a Security Tool

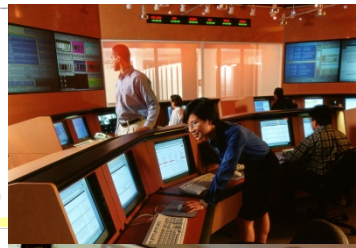
This list applies to Enterprises, Banks, Governments, On-line providers, Cloud deployments, etc …

Pause for Questions

DNS Resolver as Security

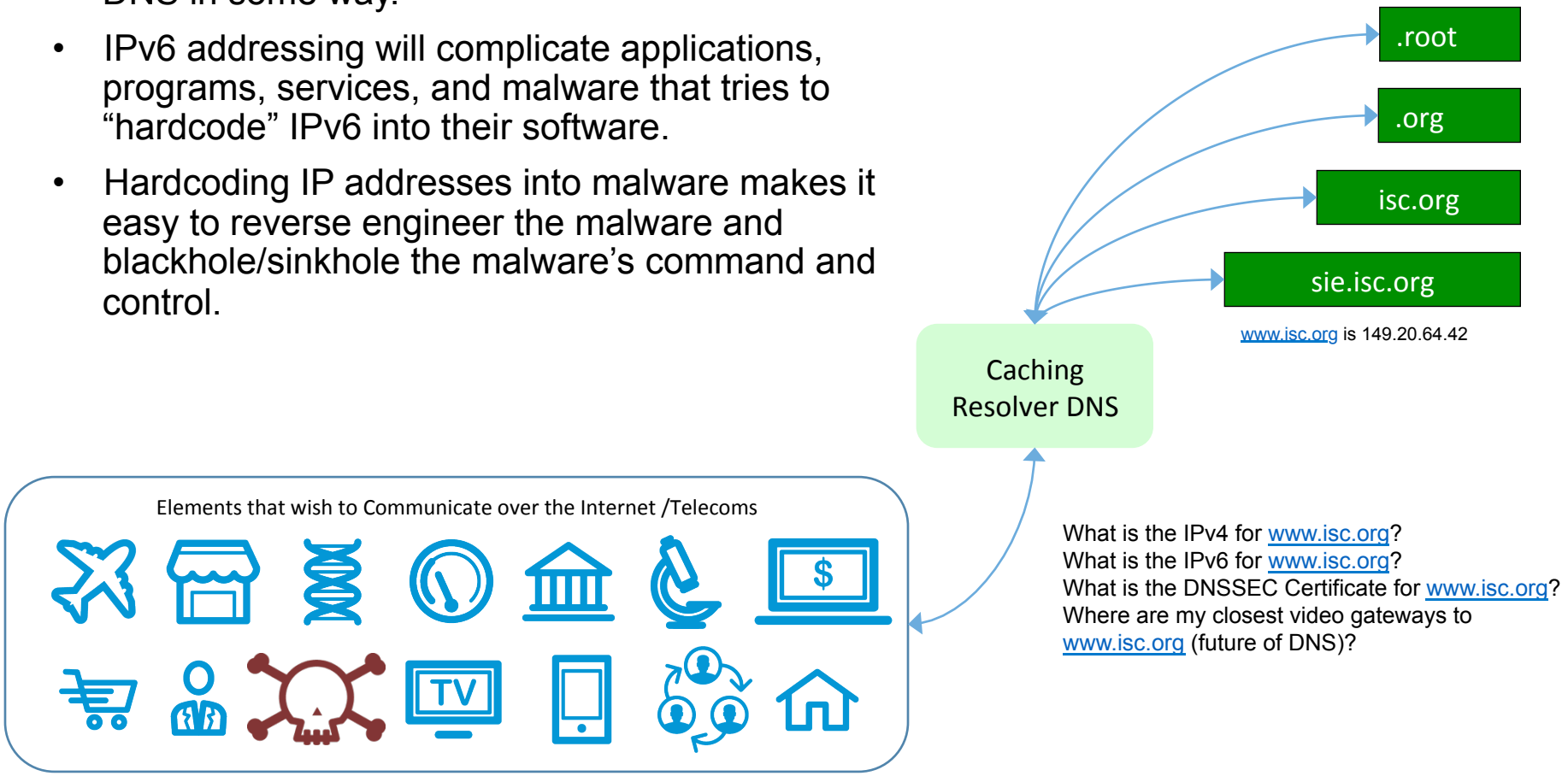




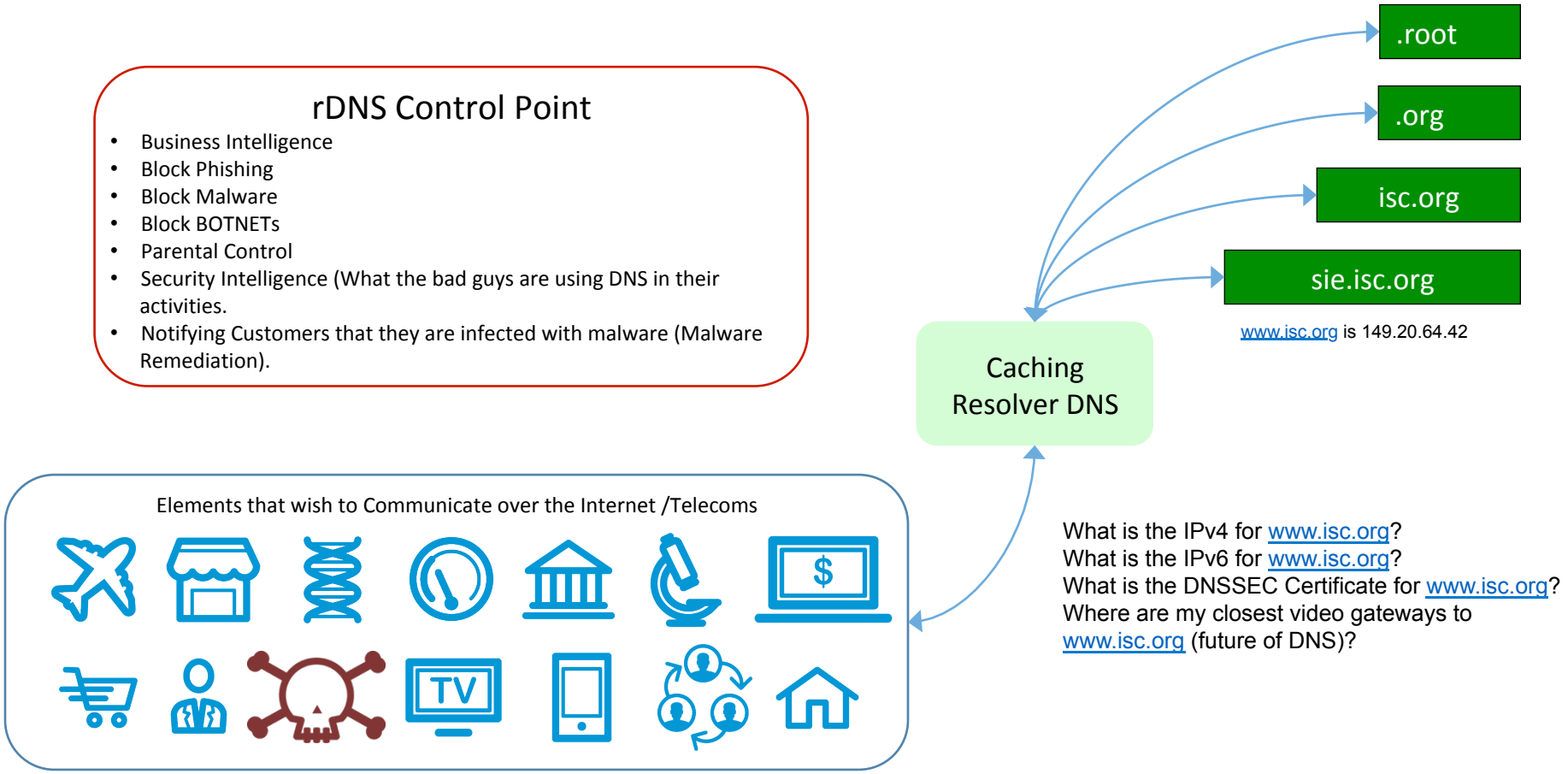


Everything Must Use DNS!

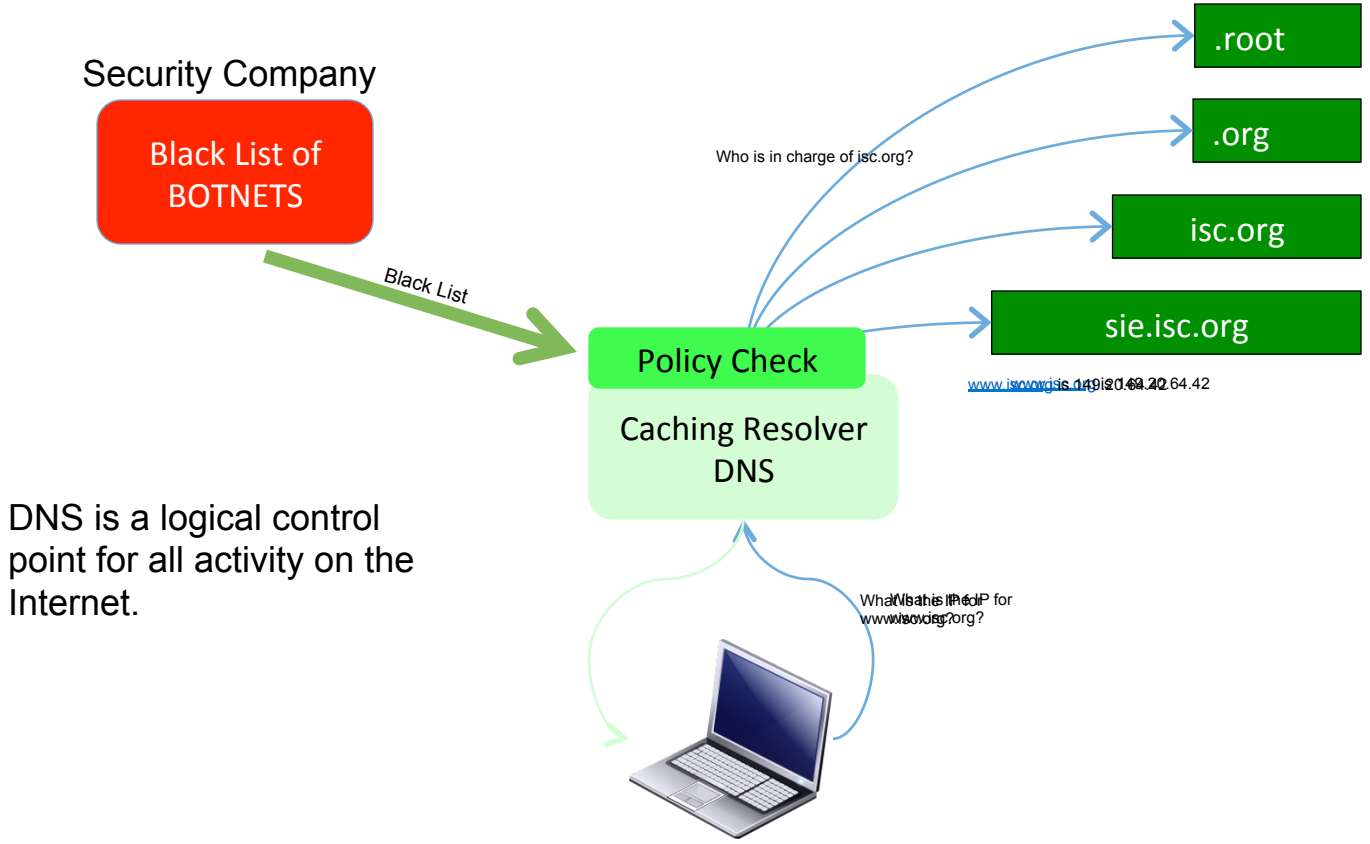
- Everything on the Internet will be interacting with DNS in some way.
- IPv6 addressing will complicate applications, programs, services, and malware that tries to “hardcode” IPv6 into their software.
- Hardcoding IP addresses into malware makes it easy to reverse engineer the malware and blackhole/sinkhole the malware’s command and control.



rDNS is a Logical Control Point

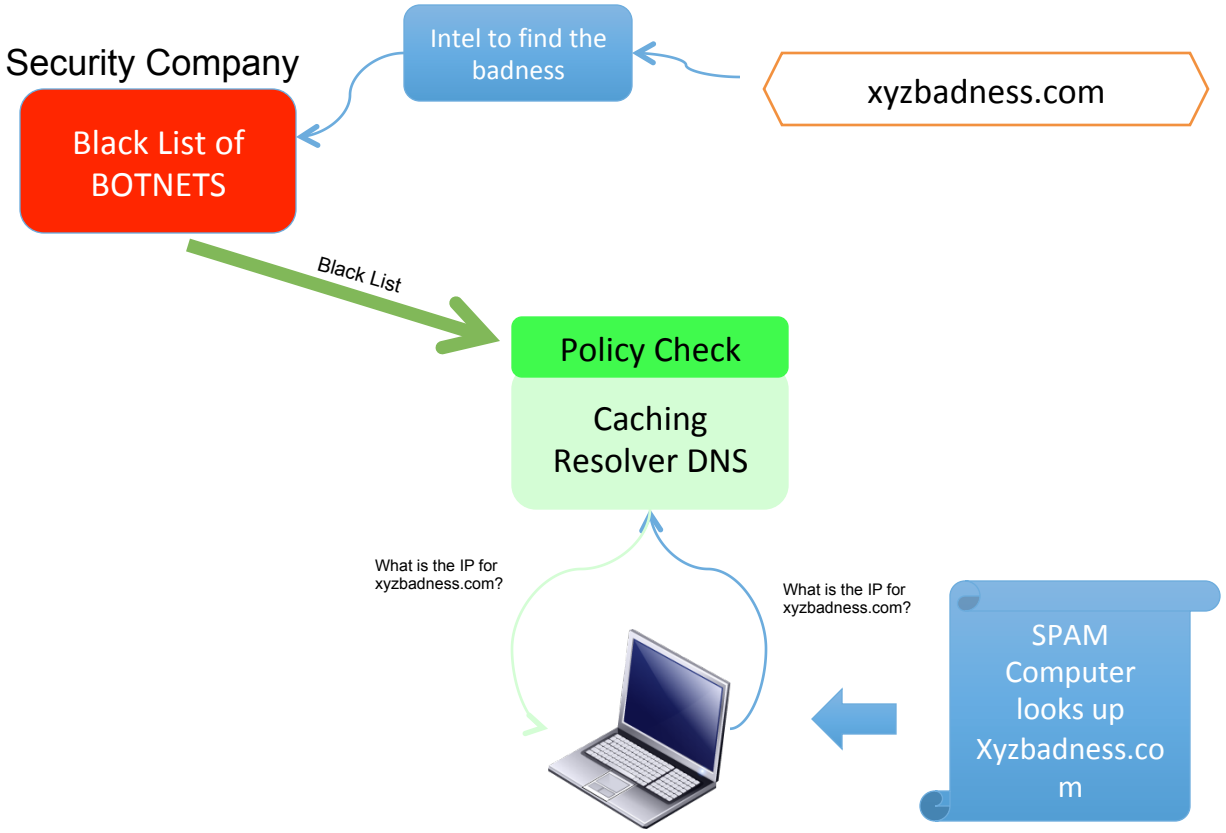


Using DNS as a Control Point



DNS is a logical control point for all activity on the Internet.

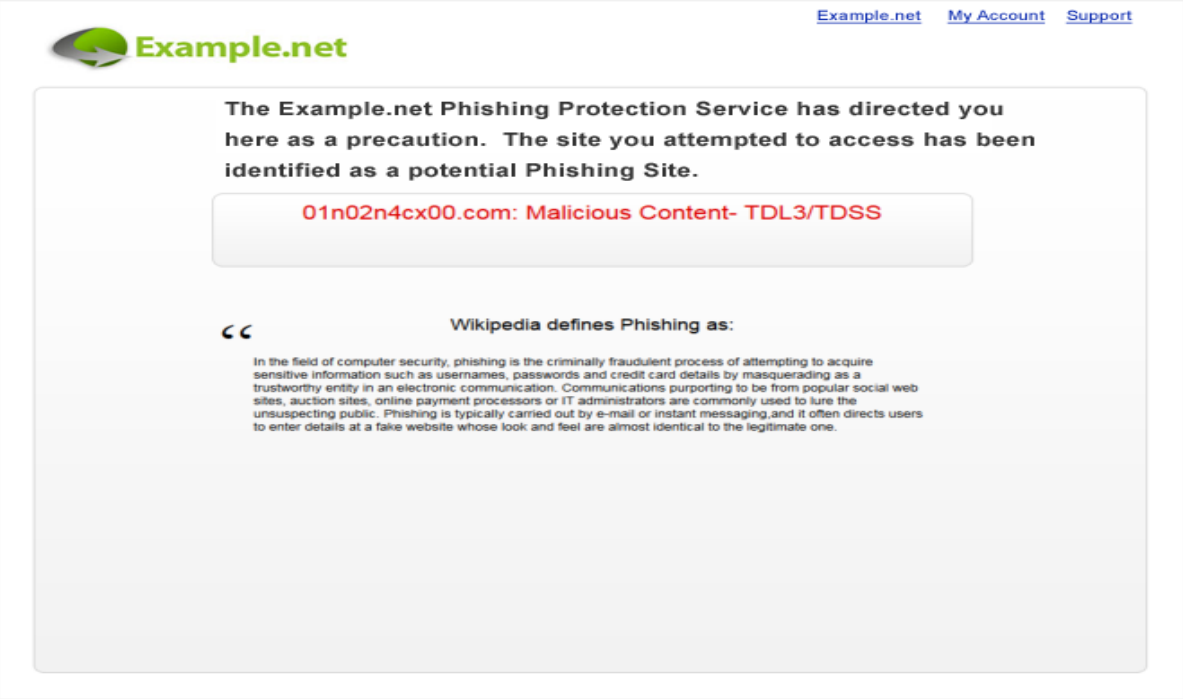
DNS Policy Checking in Action



Demo – Before – Subscribers get Infected

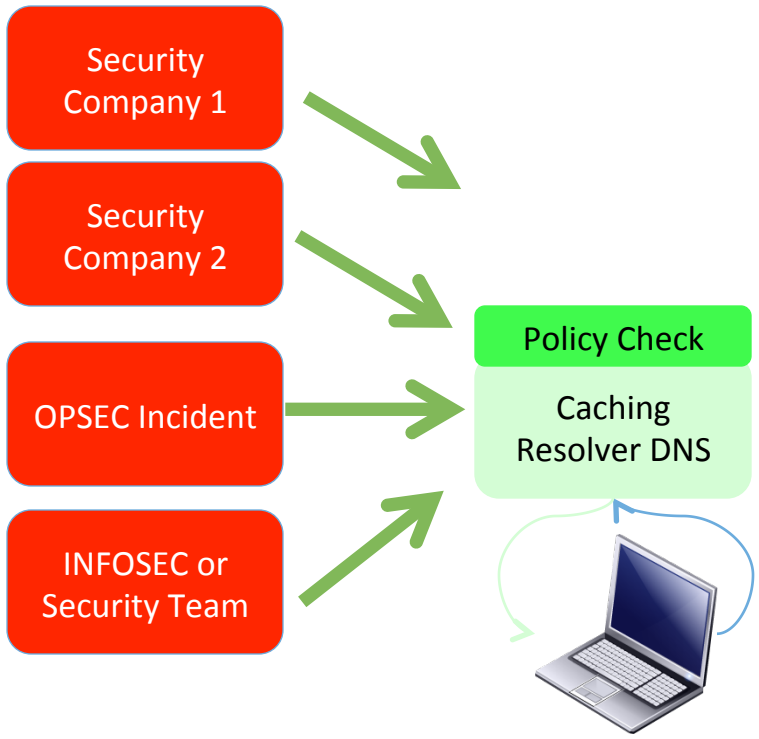
- Zero Day infection load onto the device with zero interaction by the user.
- They would look at the page and then "leave."
- In the mean time, the zero day exploit has infected the system.

Demo – After – Subscribers are Protected



- Black Listed Sites will be redirected.
- Subscribers are redirected to a to a site letting them know that they have been stopped.
- Additional redirection can happen to have subscribers to a check on their system just to be safe.

Multiple Threat Feeds



- Multiple "threat intelligence" providers – building a richer list of "bad actors"
- Allows for industry incident feeds.
- Allows for local incident management feeds.

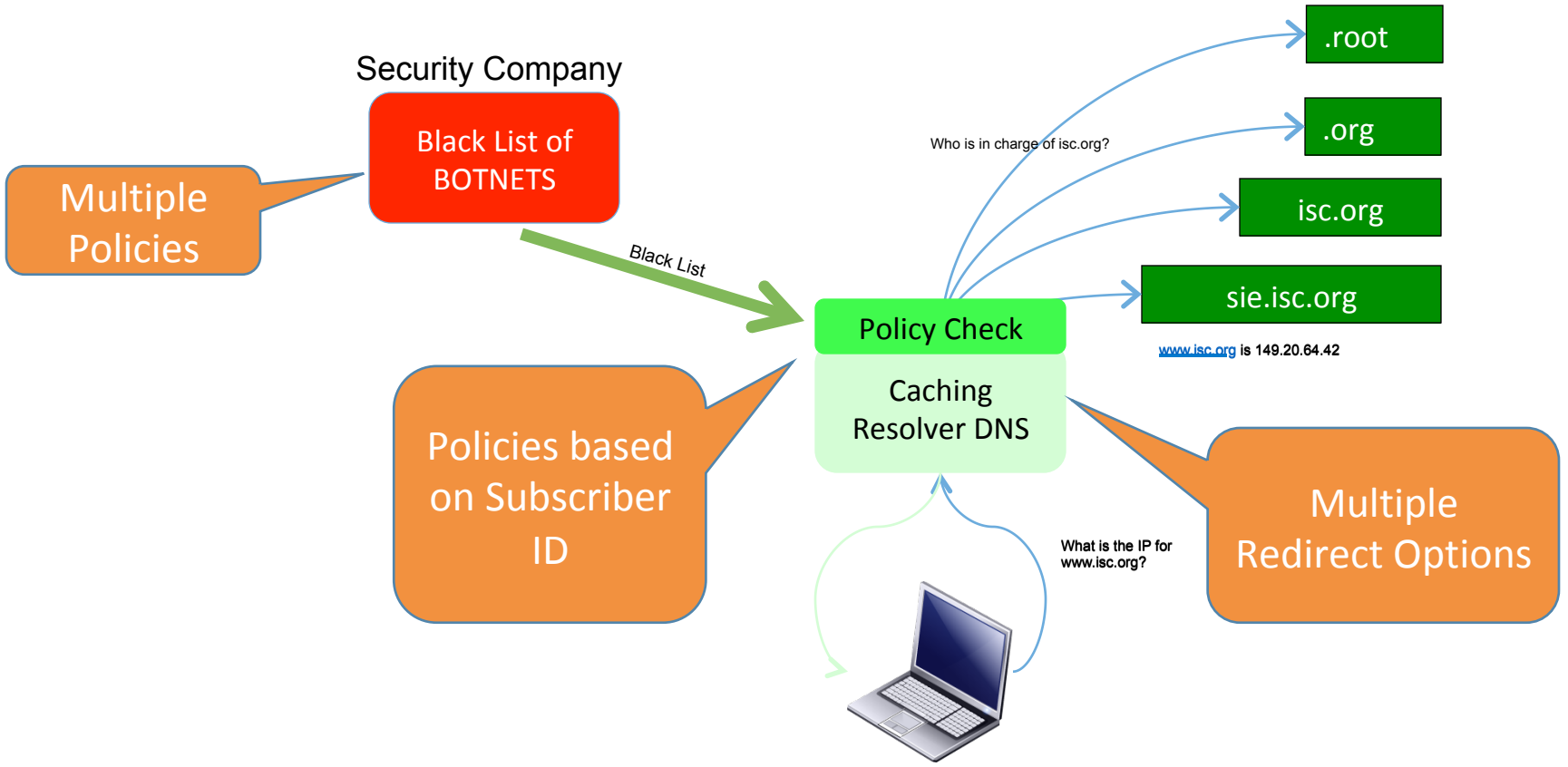
IID

Akamai Cloud Security Intelligence (CSI)

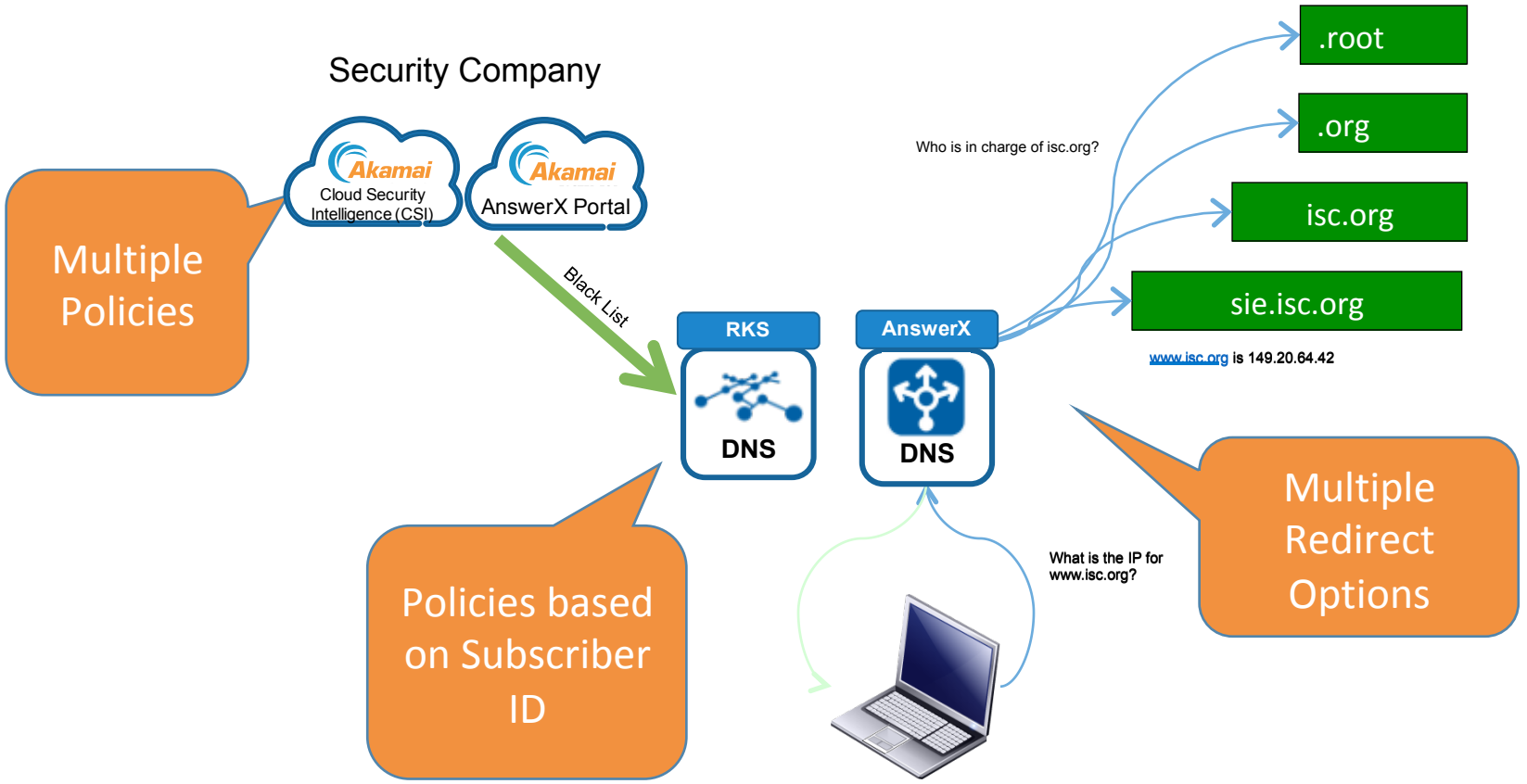
SURBL

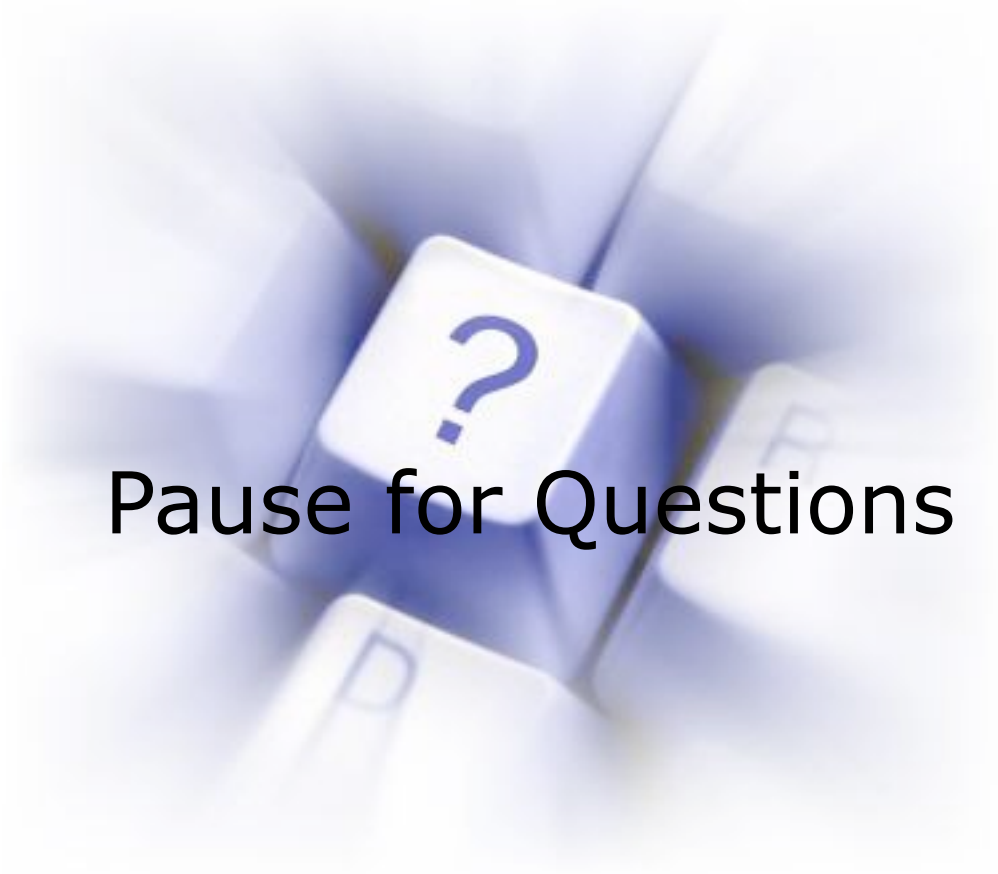
THE SPAMHAUS PROJECT

What do we really need for “DNS Policy Control?”



What do we really need for “DNS Policy Control?”





Pause for Questions

Example of “New Tools”

- **Principle of Remediation**. All Operators must have the ability to remediate devices which are known to be violated by malware. Remediation actions can range from notification to removal (for example an IoT device).
- **Malware Remediation.** Show each operator use a set of tools to measure the “invention rate” of the devices connected to their network? The infection rate would be an indicator for the risk level to the network.
- **Next Get - Sink Hole Operations.** Private Industry working together and with Law Enforcement have proven that Internet wide “take downs” of the infrastructure used by the Threat Actors is viable. These Take Downs will range from IP black holes to domain name black list. These take downs often have a remediation component - where the Operator’s customers/ constituents are notified if their devices are seen going to the Threat Actor’s infrastructure.

Example of “New Tools”

- **Rapid and Scalable DNS Black List (DNS Firewall).** There is enough experience with using DNS black list on the DNS Resolvers (rDNS) to recommend this as a critical tool in the “Tool Kit.” What would be the drawbacks for this recommendation?
- **What are the tools we need to to a traceback of an incident?** Traceback is where the infected device is isolated and the malware C&C telemetry analyzed to build a C&C map
- **Backtrace is the next step.** At times the C&C infrastructure will be tracked to an Operator. That Operator would then use tools from their Tool Kit to track traffic. The objective is to "backtrace" to the Threat Actor.

Example of “New Tools”

- **Internet Embargo.** Why receive traffic you know is bad into your network. Why accept traffic from an ASN whose empirically measured reputation score is crap?
- **Closed Network Layers to protect and isolate.** Divide the connected from the customer to the rest of the Internet into three buckets - critical, clean, and dirty. You can also view this as breaking the data plane into three. vCPEs make this easier. A vCPE puts the NAT functionality in the cloud, giving operators view on the other side (in the default customer connections).

Example of “New Tools”

- **Transparent “Feed” Capacity & Operations**. Netflow/IPFIX, Passive DNS, and other feeds from Operators would have the infrastructure, capacity, and policy to encourage a vibrant “good guy” community. The “good guy” community would also provide clear “service exchange” provided to the Operator to facilitate a “win - win” exchange of value.
- **Monitoring, Probe, and Measurement Community Deployments.** Organizations like RIPE Atlas/RIS, CAIDA, and others have systems that deploy probes throughout the world. Operators would work on a clear plan to promote the deployment and use of these systems to better effect the measurement and study of the quality of the Internet.
- **Sinkhole Sensors, Collectors, and Telemetry Boxes.** Many Security Organizations place “collectors” with Operator Partners. These systems collect telemetry that is then exported and used to track the badness. This practice is chaotic and not “Operator Friendly.” That impacts the deployability, limiting the number of Operators, limits the surface area of detection, and is threatened by “champion attrition” (where the person who set up the sensor in the Operators leaves).