Cisco Systems

poweredbycisco. networkers 2005

Session ID: SEC-2000

SECURE ENTERPRISE DESIGN

Jason Halpern

Preface

“This presentation introduces key concepts to consider when designing and evaluating network security systems. It starts with the fundamentals: axioms, the design process, and design principles. Then these concepts are applied to a variety of best practice designs in an interactive design discussion.”

The Authors at Cisco Systems

Agenda

- Axioms
- Policy Design Process
- Design Principles
- Best Practice Designs
- Conclusion

1: “Network Security Is a System”

- **“Network Security = Firewall + AV” is no longer a common thought**
- **Network security is not for sale, it is more than about buying the latest security gizmos and deploying them on a network**

  Technology will improve, certainly, but policy, operations, and design will have the largest impact

- **“Network Security System” defined:**

  A collection of network-connected devices, technologies, and best practices that work in complementary ways to provide security to information assets

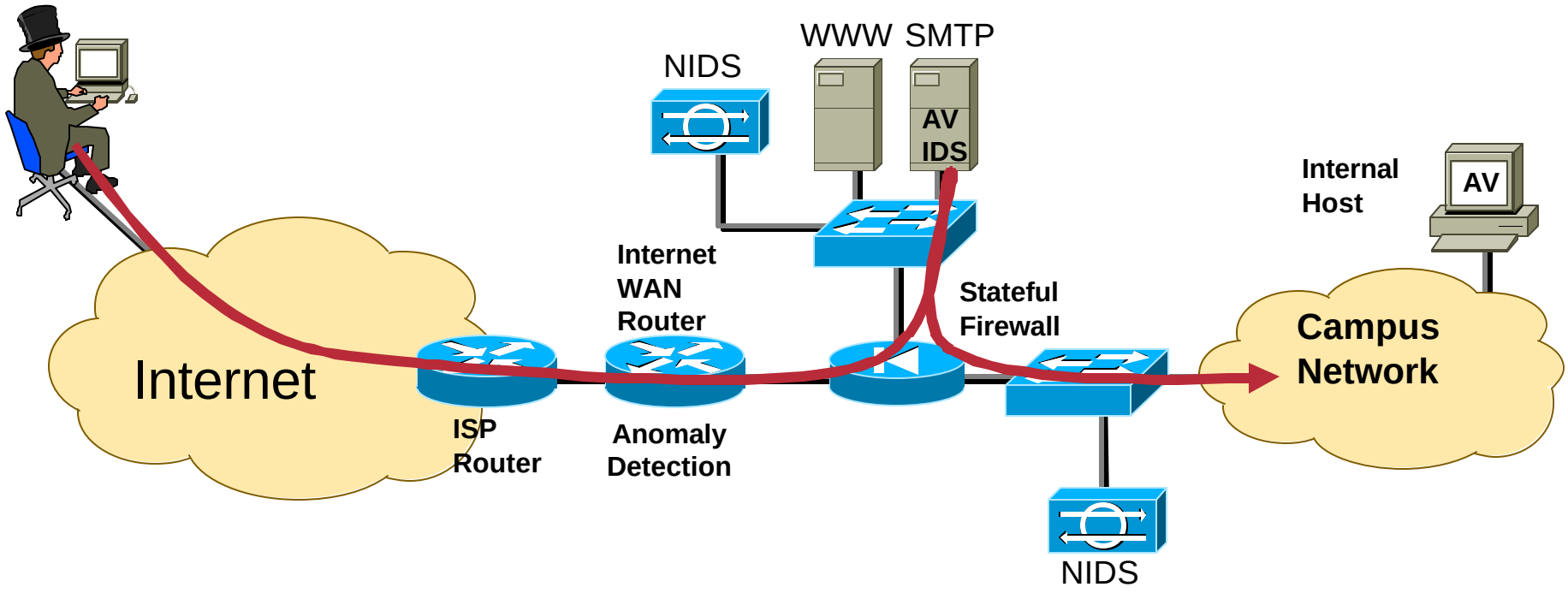
  - Source: “Network Security Architectures”

Countless Examples: Hybrid Virus/Worm

- **What types of devices play a role in stopping the attack?**

  IDS (Anomaly and Signature, Host and Network), Anti-Virus (Network and Host)

  Notably absent: a stateful firewall which does little to stop the attack



2: “Everything Is a Target and Weapon”

- **Hosts are the target du jour for worms and viruses**
  - **In the past year, large number of attacks targeted user hosts**
  - **Compromised hosts are often used as attack launch points**
- **But there are other juicy alternatives, such as:**
  - **Routers**
  - **Switches**
  - **DHCP servers**
  - **DNS servers**
  - **Management stations**
  - **Network capacity**

Router Example

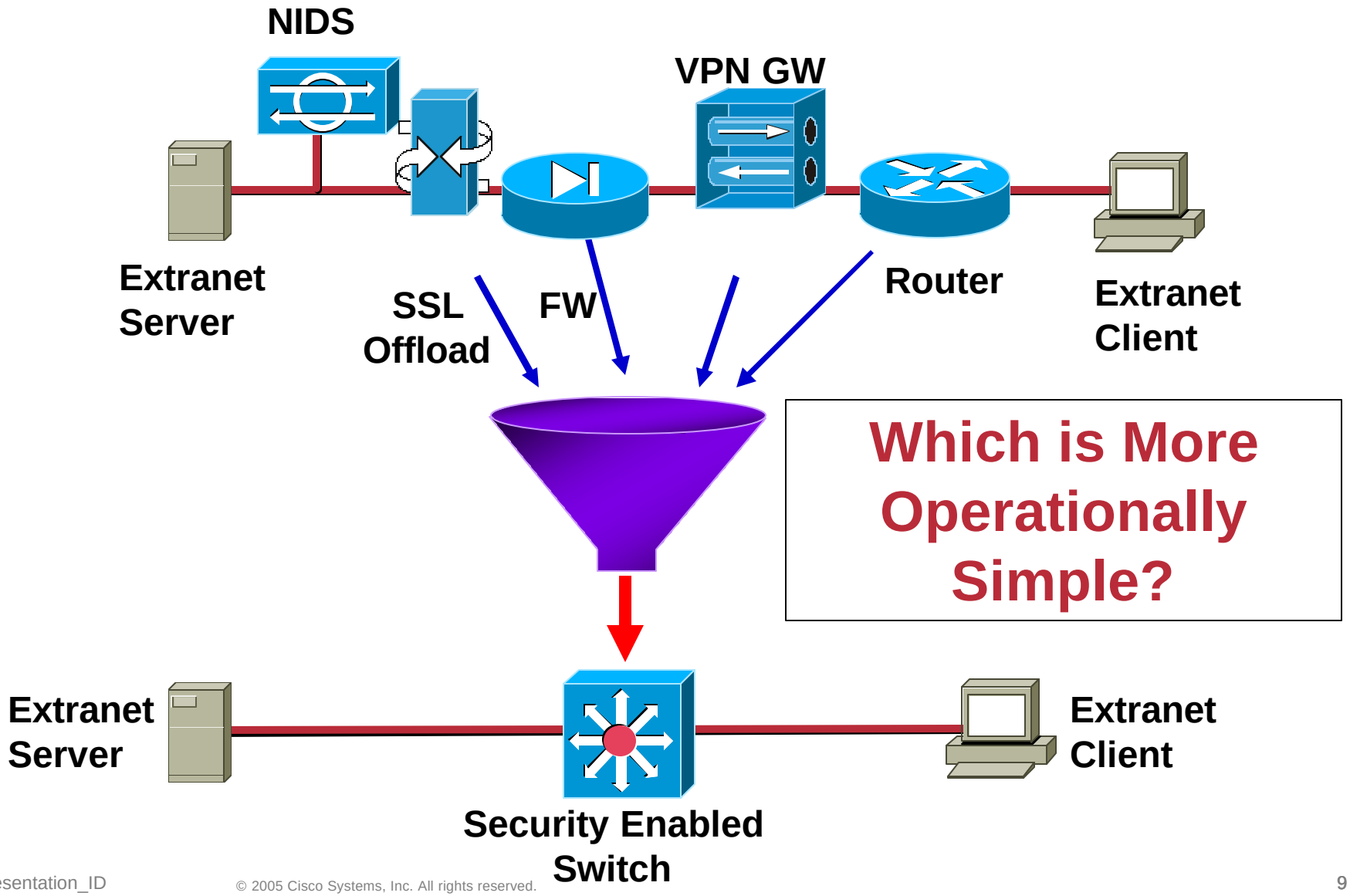
Cisco.com

- **For example, what can you do to a router?**
  - **Change configurations**
  - **Change IOS loads**
  - **Alter administrative access and audit trail tracking**
  - **Shut it down**
  - **Snoop packets = recon**
  - **Snoop network peers = recon**
- **How can you use a router as a weapon?**
  - **Disable interfaces = DoS**
  - **Change ACLs = change access policy and DoS**
  - **Alter routing tables = change access policy and DoS**
  - **Packet generator = DoS**
  - **Serve false addresses = DoS and Man-in-the-Middle (MitM)**
- **Routers are potentially a hacker's best friend**

3: “Strive for Operational Simplicity”

- **Have you ever heard a network design called “elegant”?**
  - **Was it elegant in operation, or elegant in Visio?**
- **When designing a security system it is critical to think about the operation of the network**
  - **How will your system hold up when under attack?**
  - **Will you have the tools you need to respond effectively?**
- **Operational simplicity is about not just good management tools, but an understanding of how your system will behave when things go really bad**
  - **Be sure when under attack that you can manage your devices**
  - **Ensure late night changes aren’t likely to cripple your security**
- **Sometimes achieving operational simplicity means introducing topological complexity**

Simplicity Example



4: “Avoid Security Through Obscurity”

- **Keeping too many secrets is bad for security**
  - **Good crypto is not secure because it is secret, but because it is public (and has been reviewed)**
  - **The only “secret” is the key material itself**
- **Security design should follow the same principles**
  - **Avoid security dependencies on keeping several secrets (i.e., running an insecure web server on an obscure TCP port, hiding the manufacturer of your FW, etc.)**
- **That said, there is no need to advertise the details of your security (if the obscurity is low cost, feel free to use it)**
  - **While your security shouldn’t be significantly affected by the publication of your security architecture, there’s no reason to post Visio drawings on your website**

5: “Confidentiality Is Not the Same as Security”

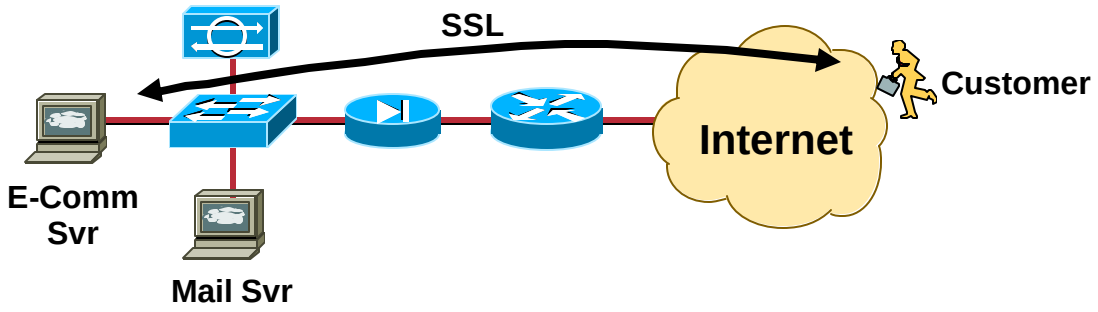
- **What is confidentiality?**

  Confidentiality is the protection of information in order to ensure it is not disclosed to unauthorized audiences

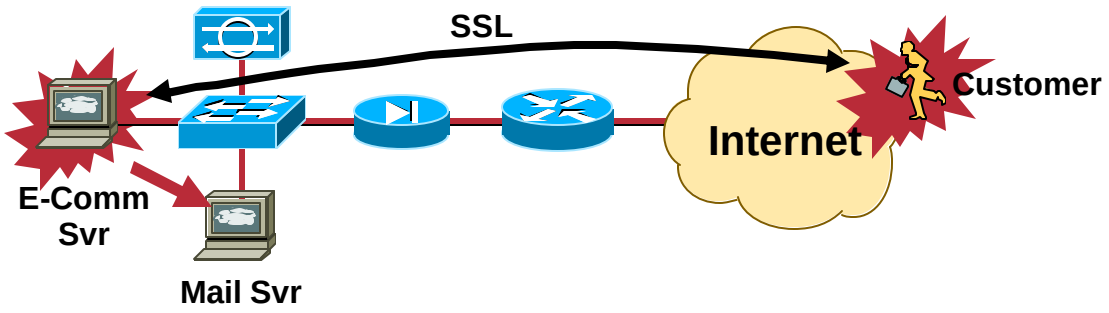
- **What is security?**

  Security is the protection of systems, resources, and information from unintended and unauthorized access or misuse

- **Some overly rely on confidentiality in security designs**
- **Example: SSL from a customer to an e-commerce server**



Confidentiality Example



- **What if the customer's host is infected?**
  - **Infection propagates through SSL, infects the e-commerce server**
  - **NIDS and other network security devices are blind to it**
  - **Secondary exploitation may occur unless safeguards exist**
    - **Such as HIPS, PVLANs, and host security**
- **The e-commerce host is the only point of detection and protection**
  - **Host hardening, anti-virus, and IPS are key in this design**

Agenda

- Axioms
- Policy Design Process
  - Business Goals/Risk Analysis
  - People vs. Technology
  - Overall Life Cycle
  - Security Is Not an Add-On
  - Domains of Trust
- Design Principles
- Best Practice Designs
- Conclusion

Business Goals/Risk Analysis

- **An org's security drivers come from business goals, and risk analysis**
- **Regardless of the security implications, business needs must come first**
  - **If your business can't function due to security concerns, you have a problem**
    - **Though "air gap" networks are very secure, business often can not deal with their limitations**
  - **Your security system must be designed to accommodate the goals of the business, not hinder them**
- **Risk analysis is understanding two key elements:**
  - **What is the cost / benefit analysis of your security system**
  - **How will the latest attack techniques play out in your network environment**

People vs. Technology

- **Effective security is a blend**
  - Skilled staff
  - Operational life cycle
  - Technology
- **Staff requires diverse skills—challenging!**
  - Risk and policy governance
  - Host, app, LAN, and WAN technology (L1-L7)
  - Operational understanding—process (L8)
  - Security and network design
  - Security technology theory and use
  - Threats and mitigation techniques
- **Know the threat and your weaknesses**
  - Track threat tools and security technologies
  - Proactive approach to mitigation
  - Audit posture regularly

OR

Overall Life Cycle

A Security System Is One Part of a System Life Cycle

- **Business needs**

  What does your organization want to do with the network?

- **Risk analysis**

  What is the risk and cost balance?

- **Security policy**

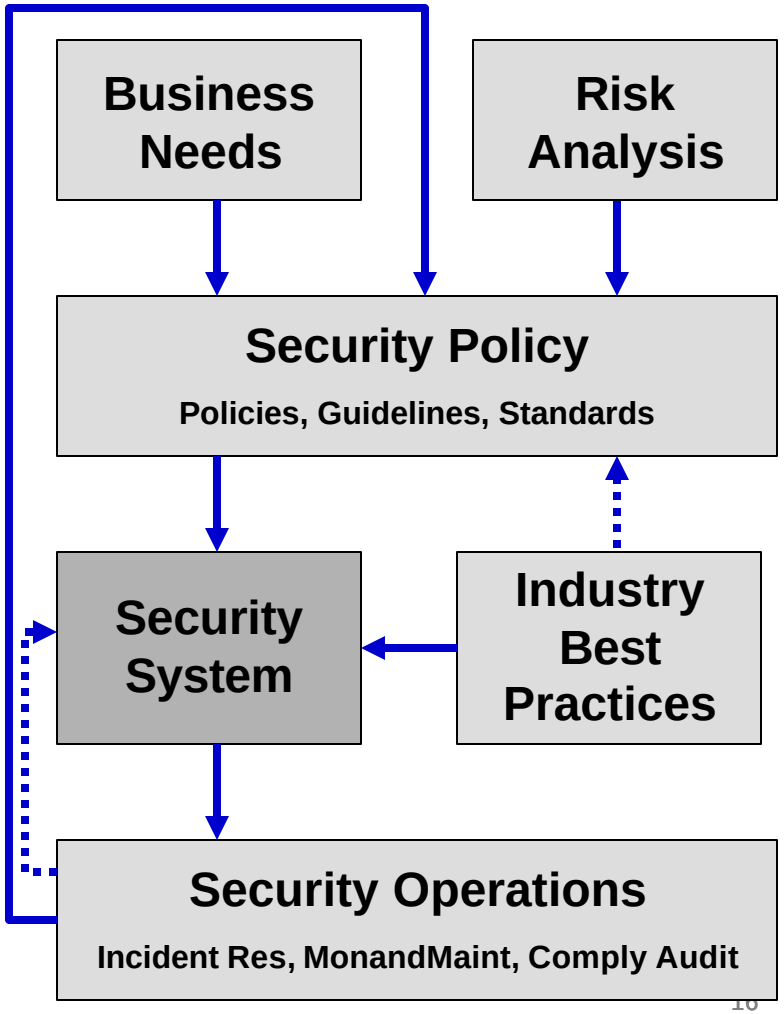
  What are the policies, standards, and guidelines to address business needs and risk?

- **Industry best practices**

  What are the reliable, well-understood, and recommended security best practices?

- **Security operations**

  Incident response, monitoring, maintaining, and compliance auditing of the system



Security Is Not an Add-On

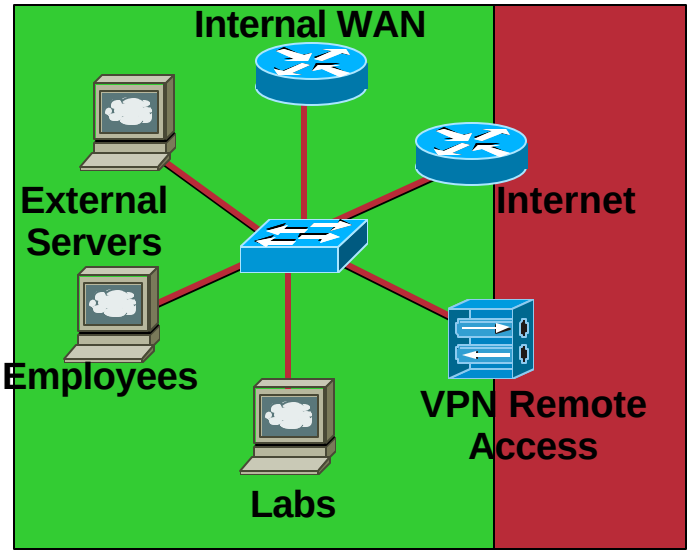
- **As security becomes more and more an embedded part of the network:**

  The days of designing the network, and then the security are *over*

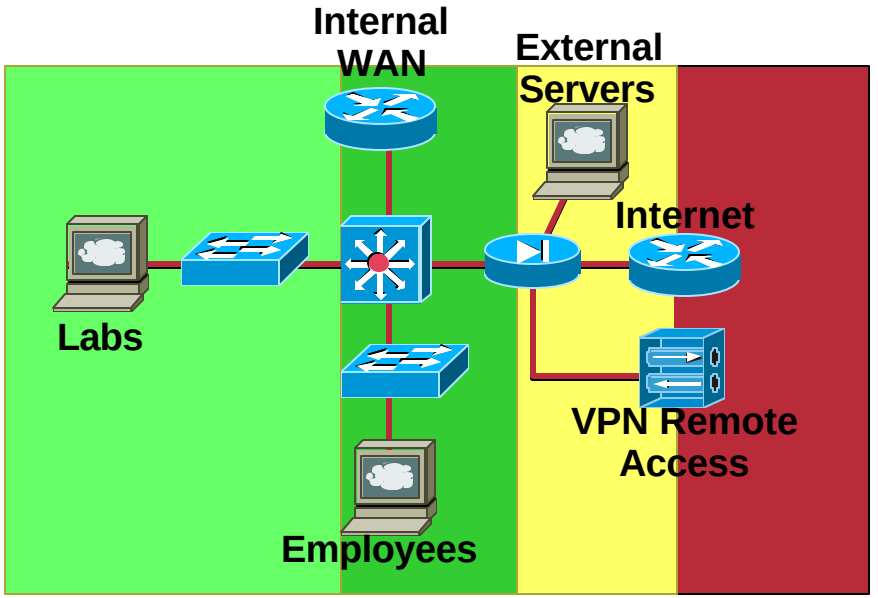
- **Firewalls, IDS, SSL, IPsec, etc. can now reside inside network infrastructure**
- **Security design with network design is far more manageable and better integrated**
- **Doing this right requires coordination not just between your network and security teams, but all of IT including the original policy design team and desktop ops**

Domains of Trust

Newbie.com



Seasoned.com



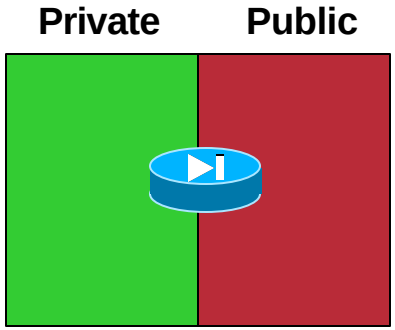
From a Security Design Perspective, What Is the Key Difference Between Newbie.com and Seasoned.com?

Segmenting the Environment into Domains of Trust

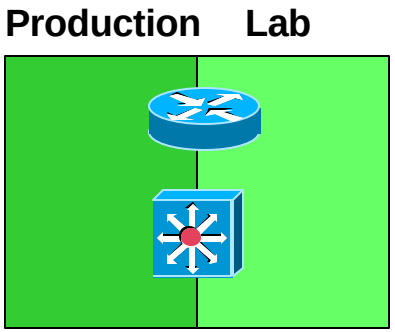
Purpose of Domains of Trust

- The security of systems within a network vary in terms of
  - Importance to the business
  - Likelihood of being attacked
- Domains of Trust facilitate segmentation based on like “policy”
  - Segments have different trust models
  - Apply consistent security controls within a segment
  - Define trust relationships between segments
- The Gradient of Trust determines the trust level between domains
  - The trust level difference may be minor or extreme
  - This gradient determines the extent of security safeguards and attention to monitoring
- Use Choke Points to control trust relationship between segments
  - Commonly Choke Points are some form of network firewalls
- Mastering domains of trust is key to good network security design

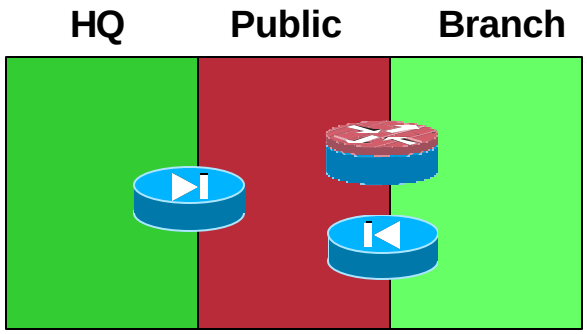
Sample Domains of Trust



- Steep gradient = high risk
- Considerable safeguards
  - Advanced Firewalling
  - Flow-based inspection
  - Misuse detection (IDS)
  - Constant monitoring



- Lesser gradient = low risk
- Basic safeguards
  - Basic access control
  - Casual monitoring



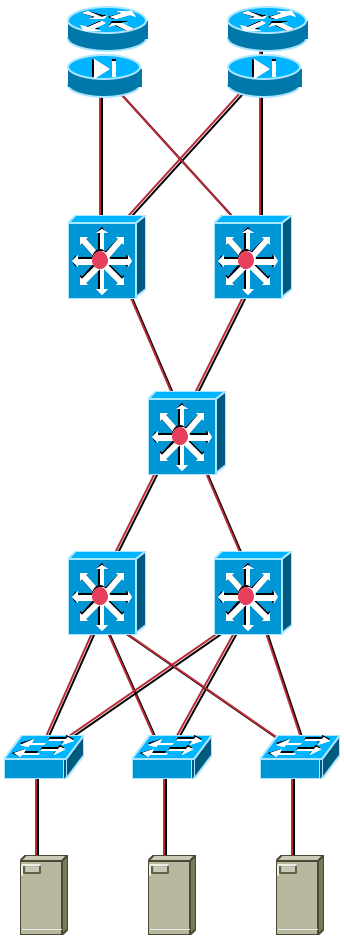
- Considerable safeguards between offices and public
- Transport between HQ and Branch over steep gradient
  - Communication security
  - Auth, confidentiality, integrity

Agenda

Cisco.com

- Axioms
- Policy Design Process
- Design Principles
  - Key Security Technologies
  - Mitigation Technologies
  - Physical Security
  - Device Hardening
  - Layer 2 Security
  - Address Translation
  - ICMP Filtering
  - Network Anti-Spoofing
  - Network Anomaly Detection
  - DDoS Handling
  - Network Driven AAA
  - Assymetric Traffic Flow
  - Management Channel Security
  - Routing Security
- Best Practice Designs
- Conclusion

Key Security Technologies



***Perimeter*: device integrity, stateful firewall, NIDS, uRPF and spoof mitigation, L3 filtering, DDoS mitigation, URL filtering, CAR**

***Distribution*: device integrity, stateful and stateless firewall, NIDS, crypto, uRPF and L3 spoof mitigation, L3 filtering, routing auth, DDoS mitigation, flow anomaly detection**

***Core*: device integrity, crypto, routing auth**

***Distribution*: as above**

***Access*: device integrity, L2 security (AAA, FW, integrity)**

***Endpoints*: device integrity, device and user AAA, host firewall, file system encryption, vuln scanning**

Mitigation Technologies (1/2)

Threat Category	Attack	Detection	Prevent
Recon	Probe	NIDS, Flow AD	Host & Network FW HIPS
	Wardriving/Dialing		802.1x, WEP
Sniff	Sniffer		L2 Integrity Network Crypto
	Direct Access		User Authentication Host & Network Crypto Host & Network FW
Manipulate	Network	NIDS	Network Crypto Network FW
	Buffer	File CRC	HIPS, AV (known)
	Application		HIPS, AV (known)
Spoof	MAC	NIDS	L2 Integrity
	IP	NIDS	L3 Integrity Network Firewalls Network Crypto
	UDP/TCP	File CRC	HIPS
	Device	Network Scanning	Device Authentication
	User		User Authentication

Mitigation Technologies (2/2)

Threat Category	Attack	Detection	Prevent
Flooding	MAC		L2 Integrity
	Transport (TCP, UDP, ICMP)	NIDS, Network AD HIDS	L3 Integrity Network FW CAR
	DDoS	Network AD NIDS (some)	uRPF, CAR DDoS Gateway NIPS (some)
	Application	Network AD (some) NIDS (some)	DDoS Gateway (some) NIPS (some)
Redirection	ARP	NIDS	L2 Integrity
	IP	L3 Integrity	Network FW L3 Integrity
	Transport		HIPS

Many Attacks Are Composites, Using Multiple of the Attacks in the Tables:

- **MitM: Sniffing, Network Manipulate, Spoofing, Redirection**
- **Viruses and Worms: Probe, Buffer and Application Manipulate, DDoS**
- **Rootkits: Sniffing, Manipulate, Spoofing, Redirection**

Physical Security

- **Though not a focus of this talk, it is important to understand where physical security impacts or augments your network security system**

  Are you using physical access to your facility as an authentication factor? (most do)

  If so, work closely with the physical security teams to ensure that the increased trust for users is warranted

  Do you have locations which are less trusted physically?

  Be sure to use location specific identity credentials for these locations to ensure a compromise of these systems does not compromise your broader network

  ```
  Router(config)# no service password-recovery
  ```

  Do you work in a business where the L1 network transmission choice has security implications (copper vs. fiber)?

Hardening

- Hosts and network gear is both a target and weapon
- Harden all the devices in your environment!!
- Develop consistent baselines for “images” and audit use
- The level of hardening to apply depends on the device location and function
  - Importance to the business
  - Likelihood of being attacked (often based on ease-of-reach)
- Hosts
  - Pervasive: patch OS, patch apps, service hardening, file access, user auth, AV, file system integrity checkers
  - Optional: FW, IPS, file system encryption

- Network Devices
  - Pervasive: admin AAA, secure command channel comms, audit trail, service hardening
  - Optional: authenticated routing, secure output comms, resource throttles, L2 hardening (no auto trunk, disable unused ports, PVLANs)
  - Links: www.cisco.com/warp/public/707/21.html

Layer 2 Security

- **Check out SEC-2002 for more details**
- **Layer 2 security is starting to receive increased attention**

  Attackers can try to use control protocols (STP, 802.1q, DTP, VTP) to cause DoS, or to gain access to unauthorized locations on the network.

  Protections include:

  BPDU Guard / Root Guard—Prevent unauthorized STP changes

  http://www.cisco.com/warp/public/473/74.html

  VLAN hopping BCPs – use dedicated VLANs for trunk ports vs. user ports, don't allow host ports to become trunks (set port host)

  SEC-2002 or http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

  VTP MD5 Authentication – prevent spoofed VTP messages

  http://www.cisco.com/warp/public/473/21.html

Layer 2 Security

- **Attackers can also spoof ARP and IP messages, masquerade as DHCP servers, and flood CAM tables**
- **Protections include:**

  ARP Inspection—prevent ARP spoofing

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0ca.html

  DHCP Snooping/IP Source Guard—prevent rogue DHCP servers and IP spoofing

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a00801cddbc.html

  Port Security—Prevent CAM table flooding, and DHCP DoS

  http://cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm

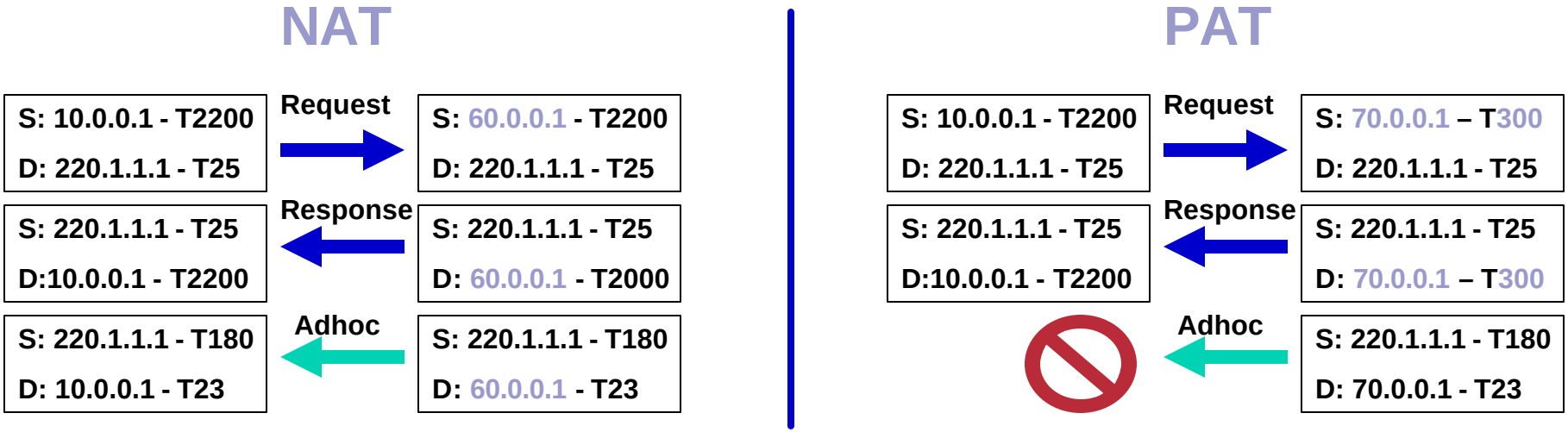
- **Some of these capabilities are only available on a select set of switches and are considered “advanced L2 capabilities.” (ARP inspection, DHCP snooping, IP source guard)**

Types of Address Translation

- **Two common types of address translation**

  NAT (Network Address Translation) = IP address translation based on static mappings or a pool of available addresses

  PAT (Port Address Translation or NAT overload) = many to one NAT by modification of the source port of a conversation



Are NAT or PAT Security Features (NAT FW, PAT FW)?

NAT/PAT Security Observations

- **NAT Security Observations**
  - **Static NAT is a pass through, no real protection**
  - **Dynamic NAT is a pass through, though the source is only "visible" or "routable" while the translation is in place**
  - **NAT does not provide L3 or L4 security features common in firewalls (TCP sequence checking, fragmentation checks, IP options abuse**
  - **NAT is not a security feature**
- **PAT Security Observations**
  - **PAT is a pass through at L4, it blocks non-defined L4 flows**
  - **Administrators cannot control which L4 flows to block**
  - **As with NAT, PAT does not perform other L3 or L4 security features**
  - **PAT does not replace firewalling, but it is better than nothing**

ICMP Filtering

- Lots of guidelines out there, very little agreement
- Basically, you need three types of messages:

  ICMP Echo and Echo Reply—blocking these messages will likely cause more harm than good

  ICMP Destination Unreachable—fragmentation needed but DF bit set—Needed for path MTU discovery

  ICMP Time Exceeded—Used by traceroute
- Additionally, ICMP fragments can be blocked since ICMP messages are very small
- Any additional messages are not necessary though they may be desirable in your network environment
- ICMP can be used as a transit method of attacks (particluarly using echo) so some risk is unavoidable

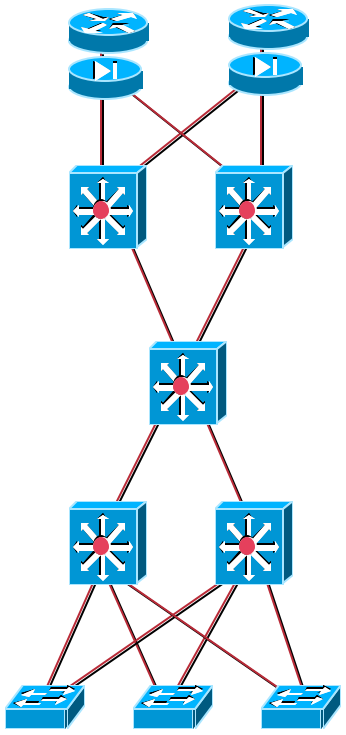
Agenda

Cisco.com

- Axioms
- Policy Design Process
- Design Principles
  - Key Security Technologies
  - Mitigation Technologies
  - Physical Security
  - Device Hardening
  - Layer 2 Security
  - Address Translation
  - ICMP Filtering
  - Network Anti-Spoofing
  - Network Anomaly Detection
  - DDoS Handling
  - Network Driven AAA
  - Assymetric Traffic Flow
  - Management Channel Security
  - Routing Security
- Best Practice Designs
- Conclusion

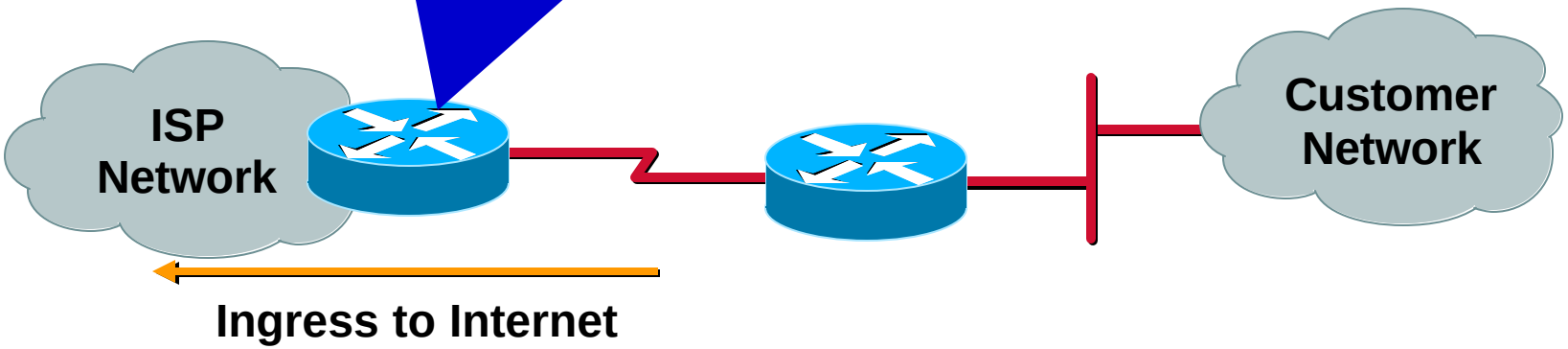
Network Anti-Spoofing (and L3 Filtering)

- Anti-spoofing within the network
- Protects against flood and MitM attacks
- Sporadically practiced today
- Applies to all layers of the network
- Focuses on L2 and L3 spoof mitigation
- Ties to L3 filtering
- Assists in bandwidth optimization
- Refer to http://www.cymru.com/Bogons/



RFC 1918 and Bogon Filtering

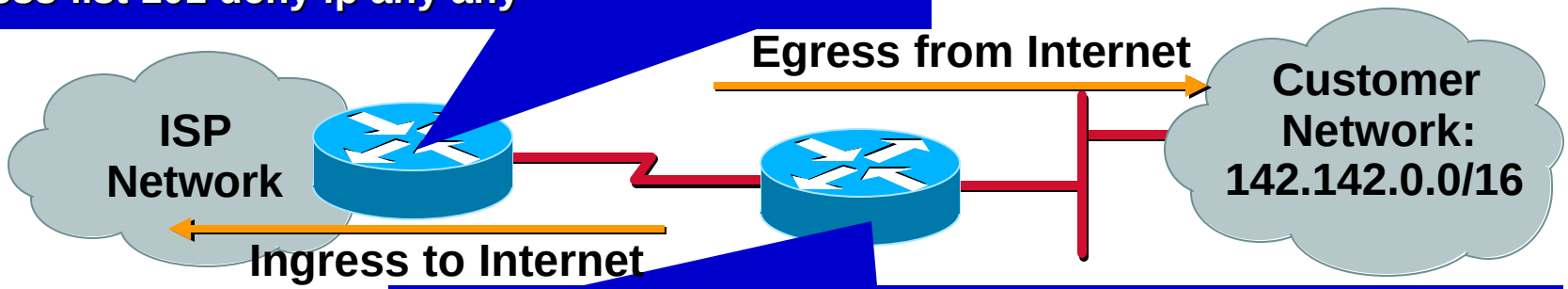

```
interface Serial n
  ip access-group 101 in
!
access-list 101 deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
…
access-list 101 deny ip 2.0.0.0 0.255.255.255 any
access-list 101 deny ip 5.0.0.0 0.255.255.255 any
access-list 101 deny ip 7.0.0.0 0.255.255.255 any
…
access-list 101 permit ip any any
```



RFC 2827 (BCP 38) Filtering


```
interface Serial n
  ip access-group 101 in
!
access-list 101 permit 142.142.0.0  0.0.255.255 any
access-list 101 deny ip any any
```

- Ingress packets must be from customer addresses



- Egress packets cannot be from and to customer
- Ensure ingress packets are valid

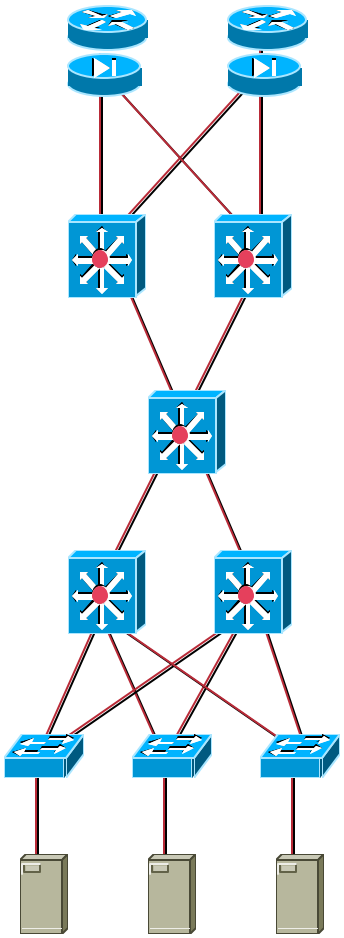
```
interface Serial n
  ip access-group 120 in
  ip access-group 130 out
!
access-list 120 deny ip 142.142.0.0  0.0.255.255 any
access-list 120 permit ip any any
!
access-list 130 permit 142.142.0.0  0.0.255.255 any
access-list 130 deny ip any any
```

Verify Unicast Reverse-Path

- **Mitigates source address spoofing by checking that a packets' return path uses the same interface it arrives on**
- **Consider 'strict' uRPF at edge 'choke-points' (symmetric routing)**
- **SPs consider 'loose' uRPF for asymmetric environments with full routing tables (no default routes)**
- **Requires CEF**

```
ip cef distributed
!
interface Serial n
  ip verify unicast source reachable-via rx
```

Anti-Spoof and Filtering Application



***Perimeter*: uRPF, RFC 1918 and 2827, Bogon filtering**

***Distribution*: uRPF, L3 filtering (network isolation, watchdog and unused network screening)**

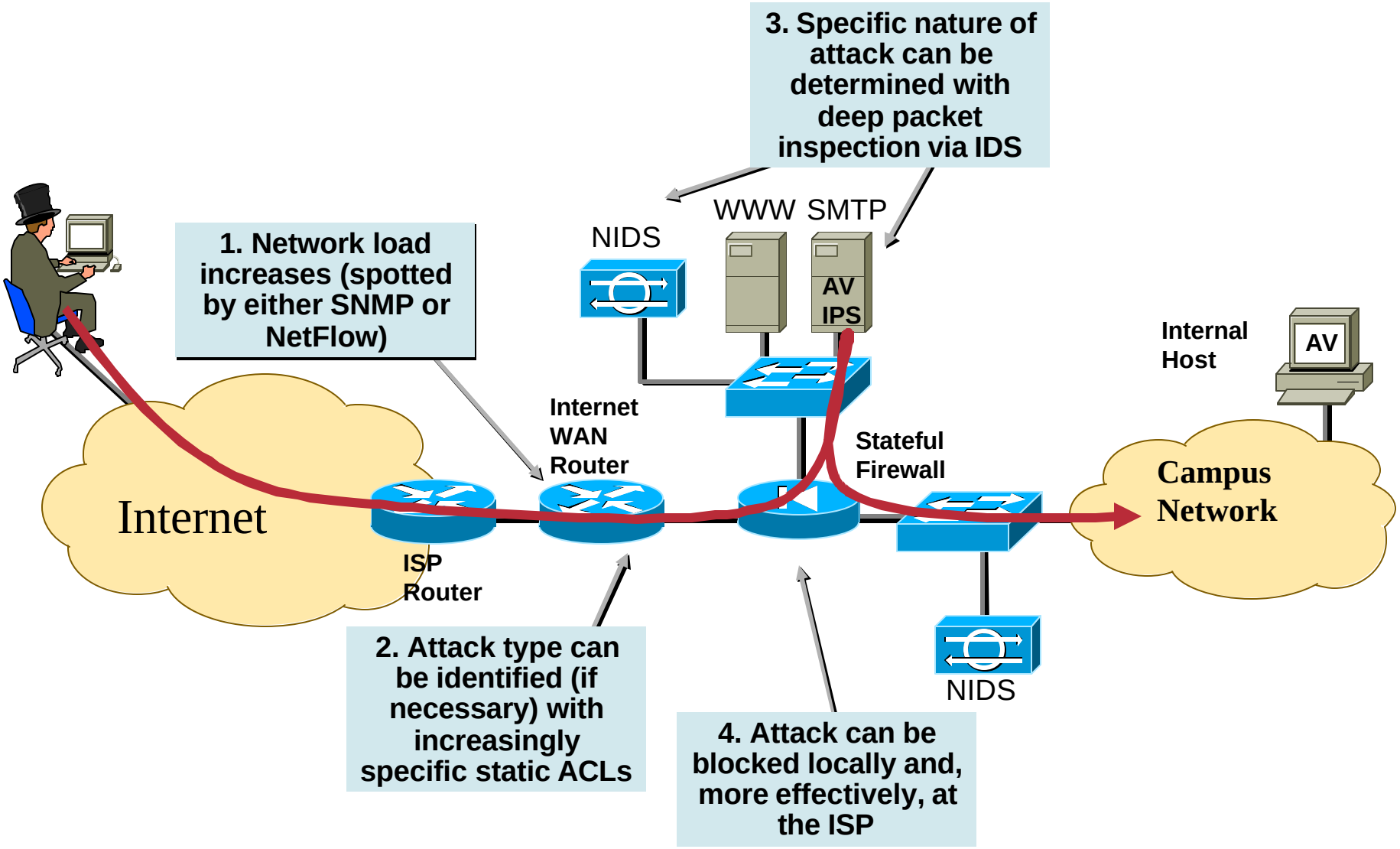
***Core*: none**

***Distribution*: as above**

***Access*: ARP inspection, 802.1x and EAP authentication, PVLANs, Port Security , DHCP Snooping, IP Source Guard**

***Endpoints*: none**

Worm Attack Detection and Isolation



Traffic Inspection: Under Attack

- A key element to a successful network security system is understanding which of these feeds to look at and when
- A good security information manager will help you aggregate this data and present it in a format that is useful

  Basic ACL and Stateful FW—useful for granular traffic isolation and blocking after an event is uncovered via NetFlow

  Signature IDS—useful to extract payloads and provide visibility into the nature of a traffic spike

  NetFlow/Anomaly IDS—provides early warning of larger network events by measuring variance in expected network load

  Host Security—can help stop specific attacks and provide visibility (along with signature IDS) into specific attack details

Traffic Inspection: NetFlow Example

- **NetFlow gives you visibility into packet sizes, traffic types, and more**

  When combined with an effective analysis engine, this can be one of the best early warnings before a virus or worm outbreak

- **Enable at the interface level on a Cisco router:**

```
router(config-if)#ip route-cache flow
```

- **To view flow data locally on a device:**

```
router#show ip cache flow
```

SP Attack Mitigation

- Attend SEC-2008 for more detail
- Though this isn't an ISP session, it is useful to understand what to ask of your ISP
  - Large enterprises often share similarities with small ISPs
- NetFlow and Anomaly IDS will identify most DDoS attacks
- Several options which usually stop both harmful and legitimate traffic from reaching destination (DNS change required to get site back up [unless doing source based drops])
  - Basic ACL—Drop traffic to the target IP address
  - Black Hole Filtering—Inject host route into ISP to route traffic to IP under attack to null:
    - http://www.secsup.org/CustomerBlackHole/
  - Sinkhole Routing—Inject host route to redirect attack traffic to specific location for inspection:
    - http://www.nanog.org/mtg-0110/greene.html
- Two techniques to limit DDoS while keeping a site up and running
  - Committed Access Rate (CAR) Filtering
  - E-Commerce Specific Filtering

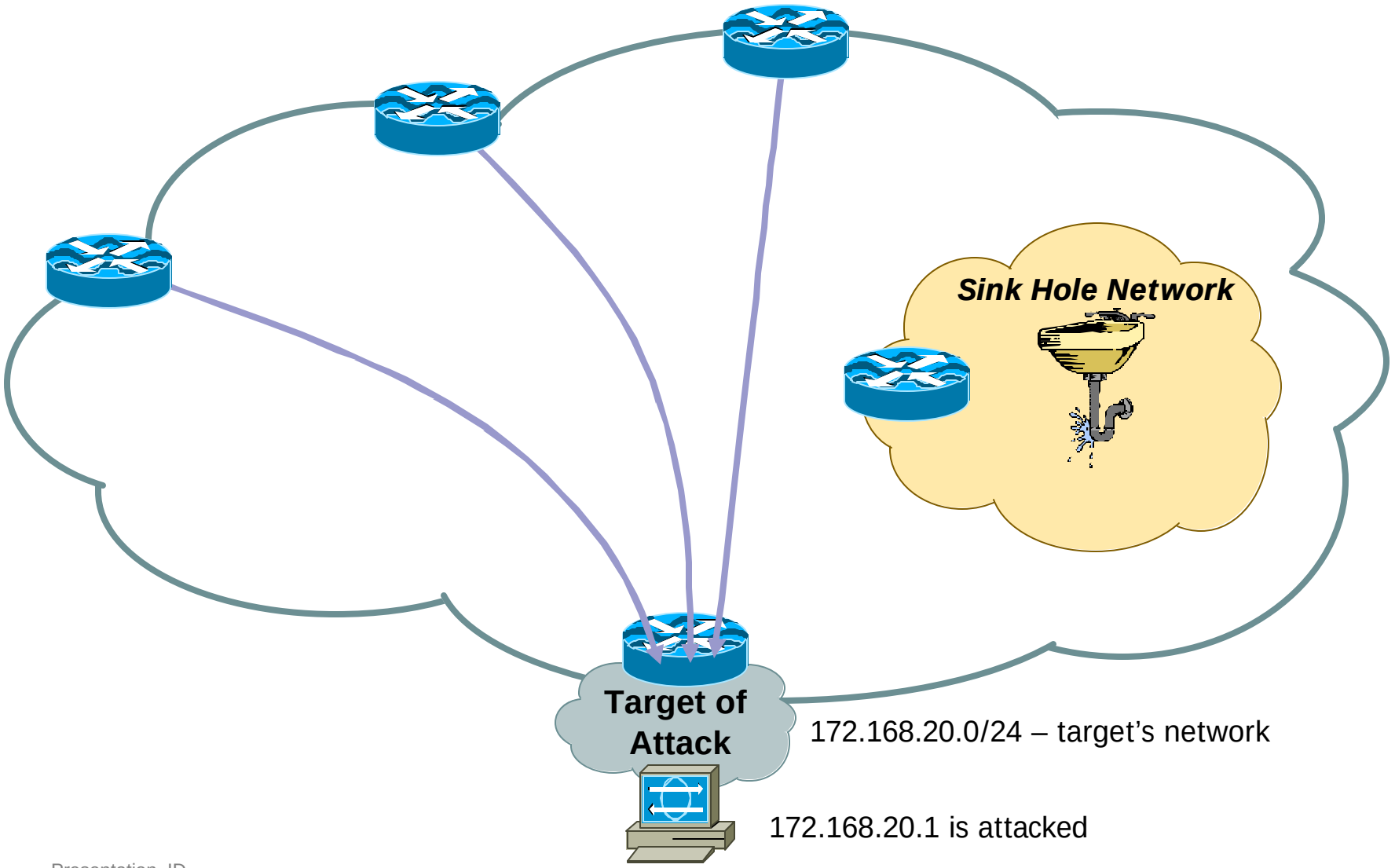
Black Hole Filtering

- BGP triggers a network wide response to a range of attack flows
- A simple static route and BGP will allow an ISP to trigger network wide black holes (null routing) as fast as iBGP can update the network
- This provides ISPs a tool that can be used to respond to security related events or used for DoS/DDoS Traceback
- Attend SEC-2008 for more information

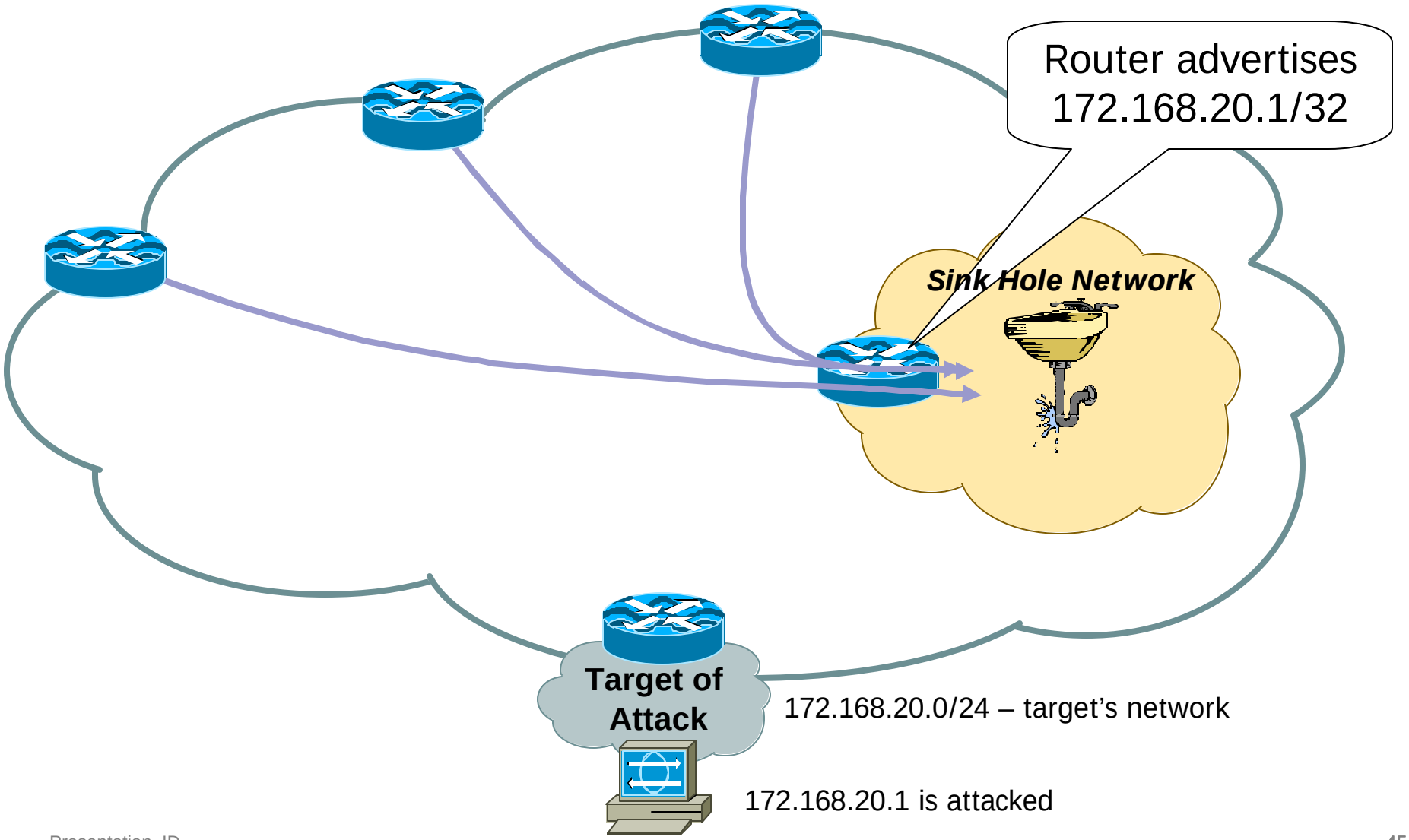
Sink Hole Routers/Networks

- **Sink Holes are a good general purpose security tool in large networks**
  - **BGP speaking router or workstation that is built to redirect attacks to itself for examination**
  - **Used to redirect attacks away from the customer but still allow analysis by the ISP**
  - **Used to monitor attack noise, scans, and other activity (via the advertisement of default)**
    - **Default advertisement will cause all sorts of traffic to redirect to the sinkhole**
      - **Customer traffic when circuits flap**
      - **Network scans**
      - **Failed attacks**
      - **Worm traffic**
      - **Backscatter**

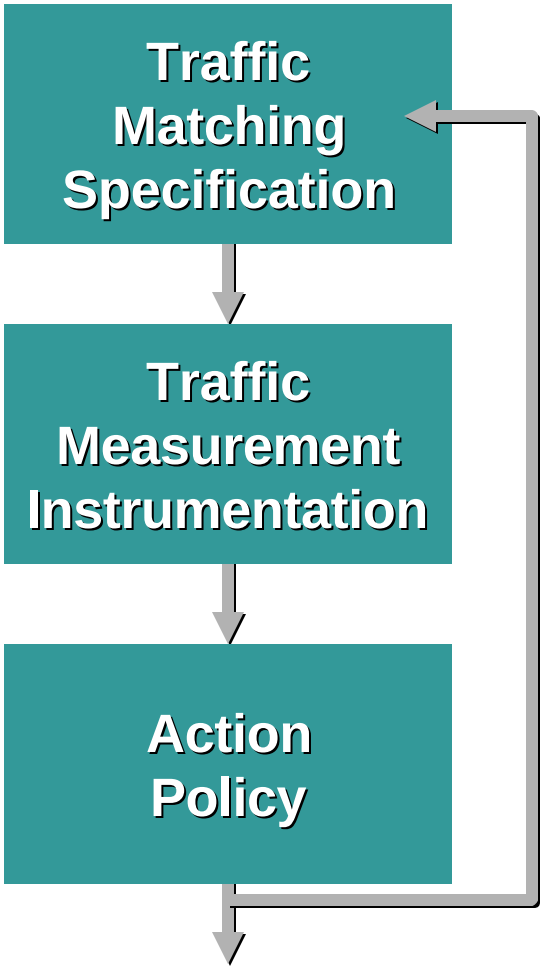
Sink Hole Routers/Networks



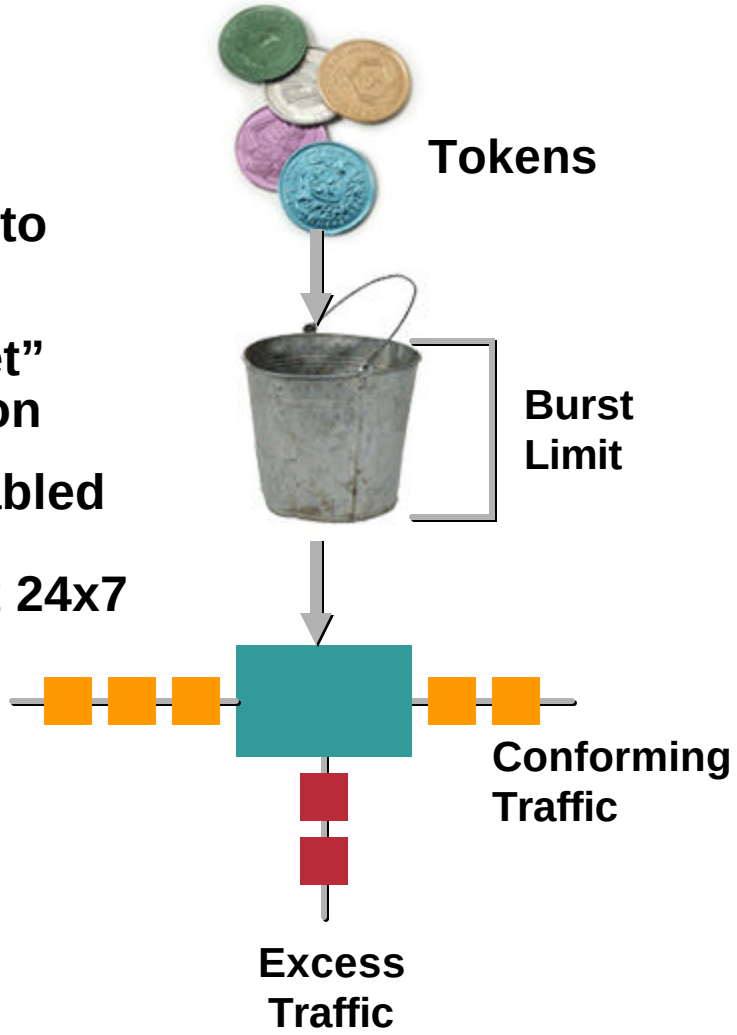
Sink Hole Routers/Networks



Committed Access Rate



- Rate limiting
- Several ways to filter
- “Token bucket” implementation
- Generally enabled after attack detection, not 24x7



CAR Rate Limiting

- **Limit outbound ping to 256 Kbps**

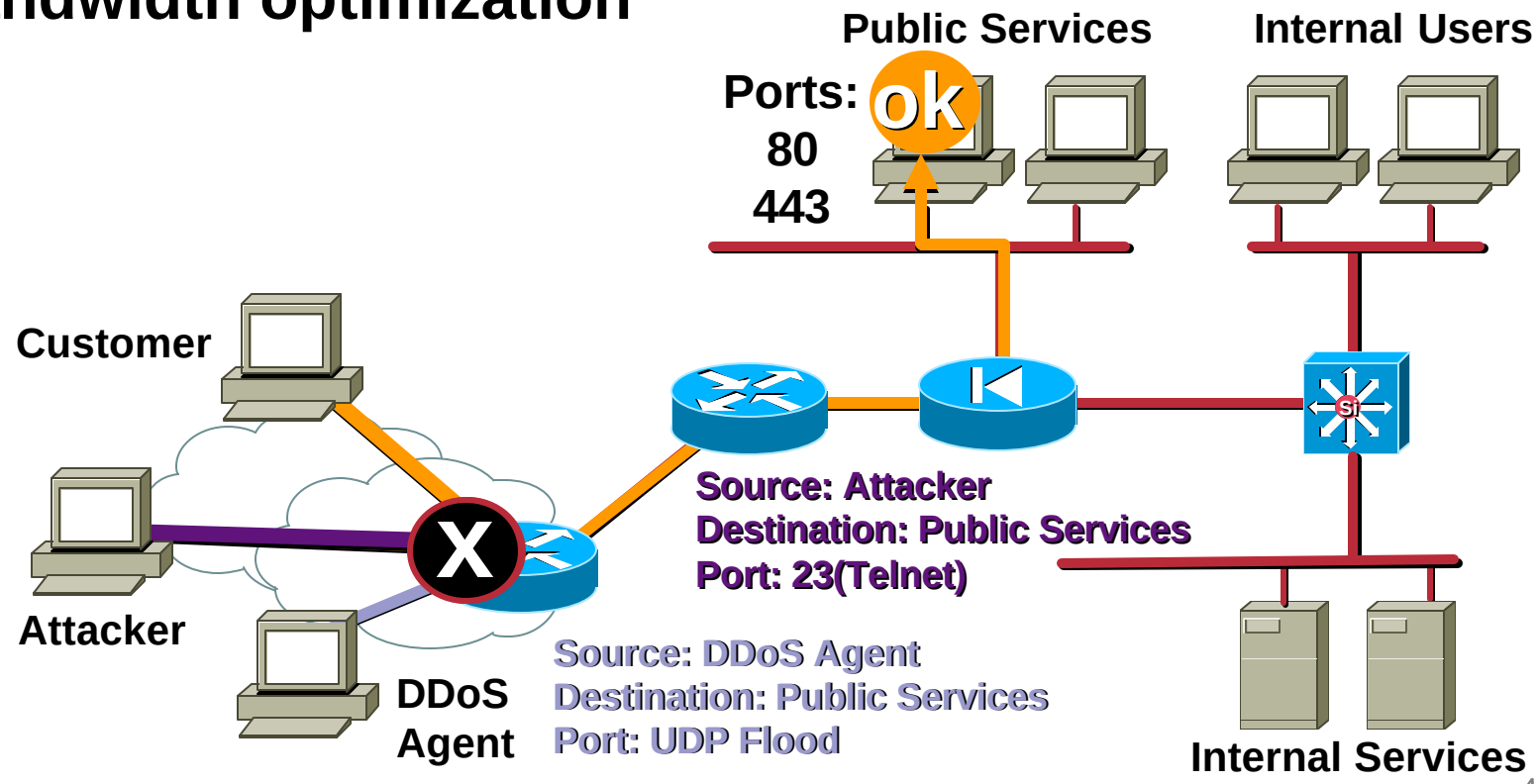
```
interface xy
     rate-limit output access-group 102 256000 8000 8000
          conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

- **Limit inbound TCP SYN packets to 8 Kbps**

```
interface xy
     rate-limit input access-group 103 8000  8000 8000
          conform-action transmit exceed-action drop
!
access-list 103 permit tcp any any syn
```

Service Provider Filtering

- Best in e-commerce environments
- DDoS mitigation
- Bandwidth optimization



ISP DDoS Traceback Options

- **ACLs with "log-input"—very manual process**

  Need to work from router to router (starting at the customer edge router under attack) to determine which ISP routers are carrying the DoS traffic

- **Backscatter—Works very quickly assuming attackers are spoofing with unallocated "bogon" ranges:**

  http://www.secsup.org/Tracking

  Blackhole routes traffic to null

  This results in ICMP unreachables sent to originating hosts

  Sinkhole advertises bogon ranges, sucking in ICMP unreachables from all the spoofed source IPs

  Source IPs in ICMP unreachables are from all routers seeing the attacks!

Agenda

Cisco.com

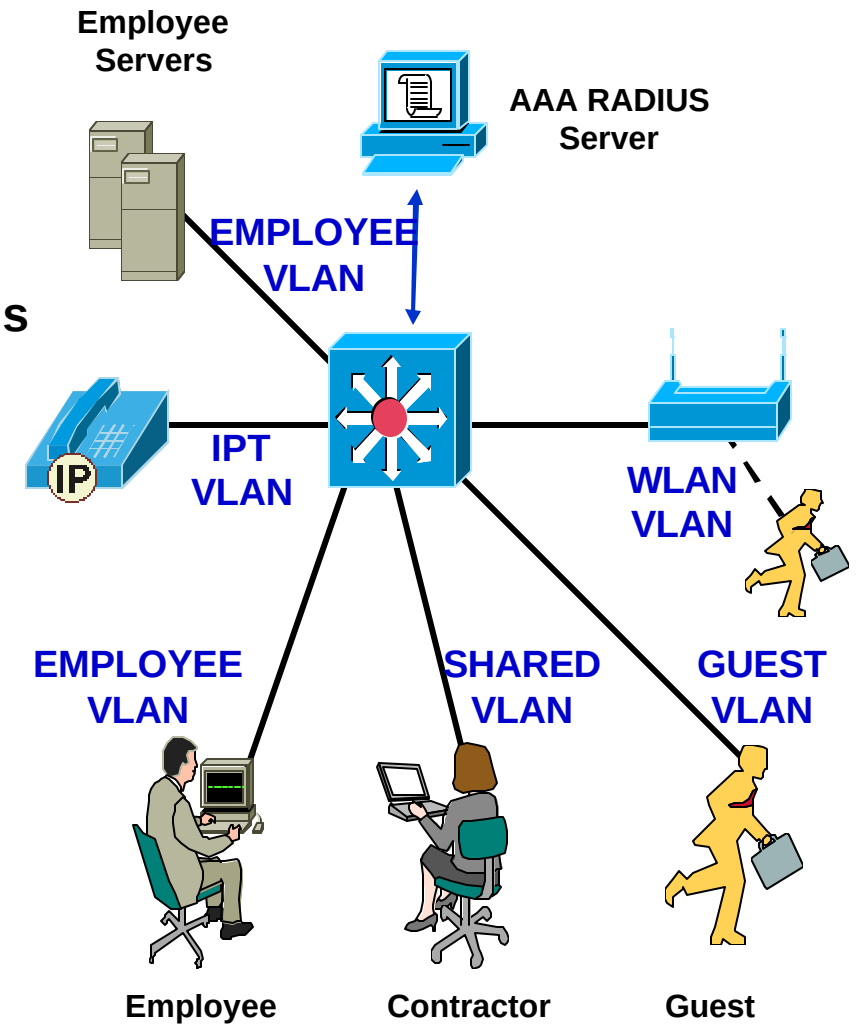
- Axioms
- Policy Design Process
- Design Principles
  - Key Security Technologies
  - Mitigation Technologies
  - Physical Security
  - Device Hardening
  - Layer 2 Security
  - Address Translation
  - ICMP Filtering
  - Network Anti-Spoofing
  - Network Anomaly Detection
  - DDoS Handling
  - Network Driven AAA
  - Assymetric Traffic Flow
  - Management Channel Security
  - Routing Security
- Best Practice Designs
- Conclusion

Network-Driven AAA

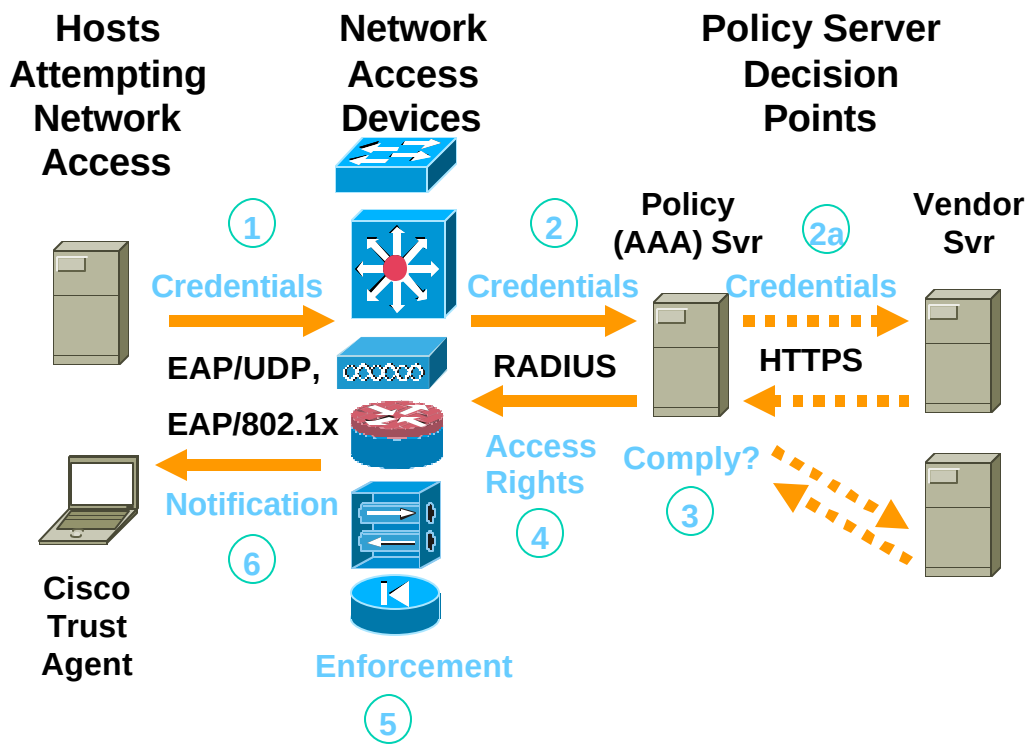
Technology	Where	User Auth	Device Auth	Device State (OS, Apps)	Authorization
IPsec & Xauth	Remote Access VPN	Yes – Reusable, OTP	Yes – CERT	Varies	L4 ACLs
PPP	Remote Access Dial	Yes – Reusable, OTP	No	No	L4 ACLs
802.1x	LAN & WLAN	Yes – Reusable, OTP	Yes – CERT	No	L2 VLANs
Network Admission Control	L3 Perimeter More Later	No	No	Yes	L4 ACLs
Cut Through Proxy	L3 Perimeter	Yes – Reusable	No	No	L4 ACLs

802.1x AAA

- **AAA at L2 Ports**
  - **Authenticate asset (cert) and/or user**
  - **Authorization via dynamic VLANs**
  - **Accounting for audit trail and forensics**
- **Segmentation techniques**
  - **Guest VLANs**
  - **Dynamic VLANs**
- **Depends on 802.1x supplicants**
- **Centralized AAA server**

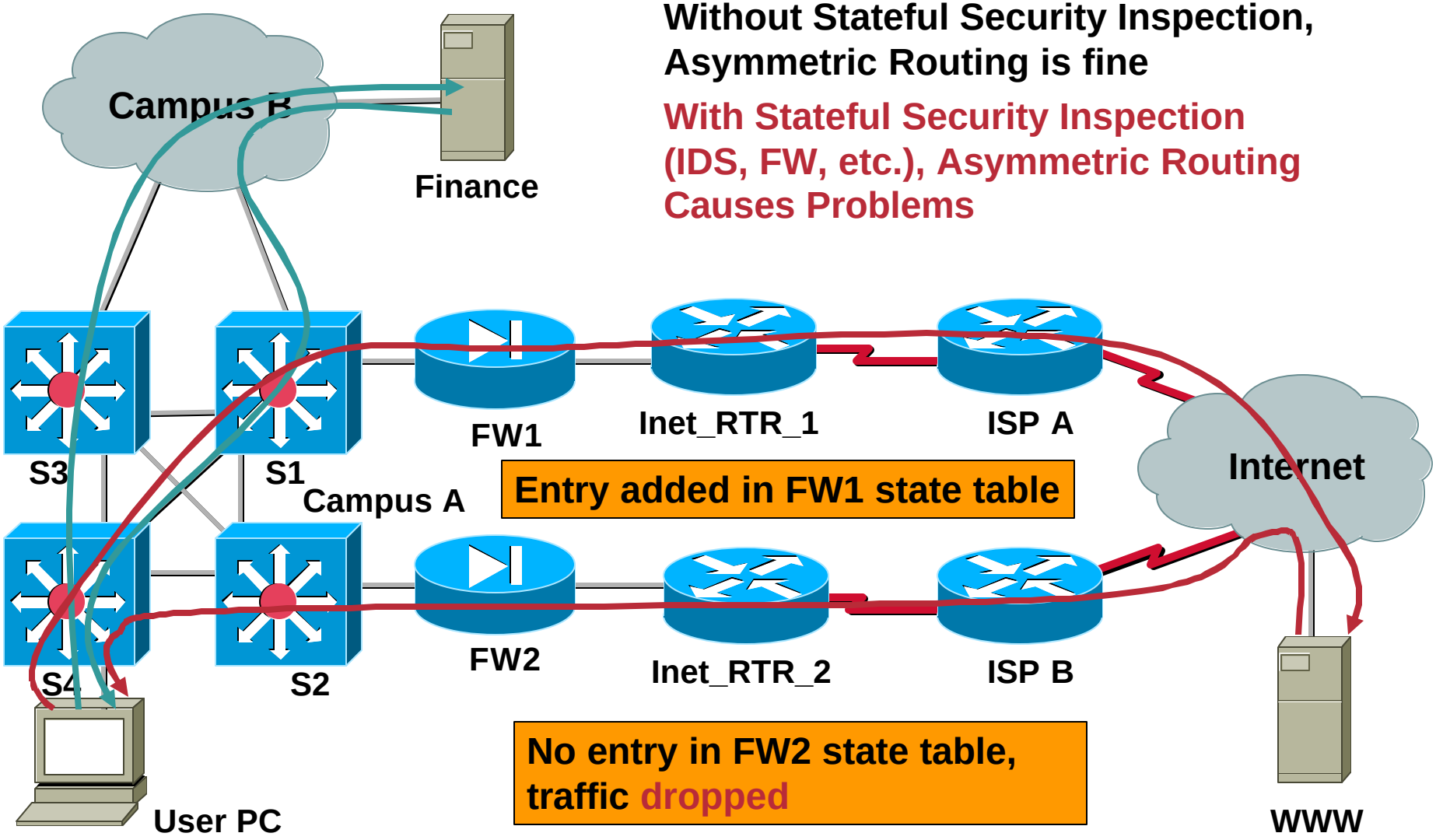


Network Admission Control (NAC)



- NAC provides device state (OS and apps) to govern authorization rights
- Now in Cisco IOS routers in T-train, coming on switches and other devices
- Useful for perimeter deployments (intranet, extranet, lab, …, like FWs)
- In phase 1, most useful when the Cisco Trust Agent can be deployed on all/most of the endpoints

Asymmetric Routing and Security



Without Stateful Security Inspection, Asymmetric Routing is fine

With Stateful Security Inspection (IDS, FW, etc.), Asymmetric Routing Causes Problems

Asymmetric Traffic Design Considerations

Cisco.com

- **Make your routing symmetric—not ideal, but a sure fire way to solve the problem**
- **Load balance per flow rather than per packet—allows IDS systems to at least consistently see half of the traffic (return route can still go through another path)**
- **Use state-sharing security devices—allows asymmetric routing while maintaining state information for sessions**
- **Consider L2 redundancy as a workaround—collapse your design to a single subnet with L2 redundancy and VRRP/HSRP; all traffic will flow through a single security device regardless of how asymmetric the traffic is on either end**
- **Manipulate flows by using routing or NAT—routing options exist to influence path selection to be more symmetric even when alternate paths exist; NAT at each security device the packet passes through can force the return traffic**
- **Use stateless security features—another option which isn't ideal but may be OK if you have a robust security system**

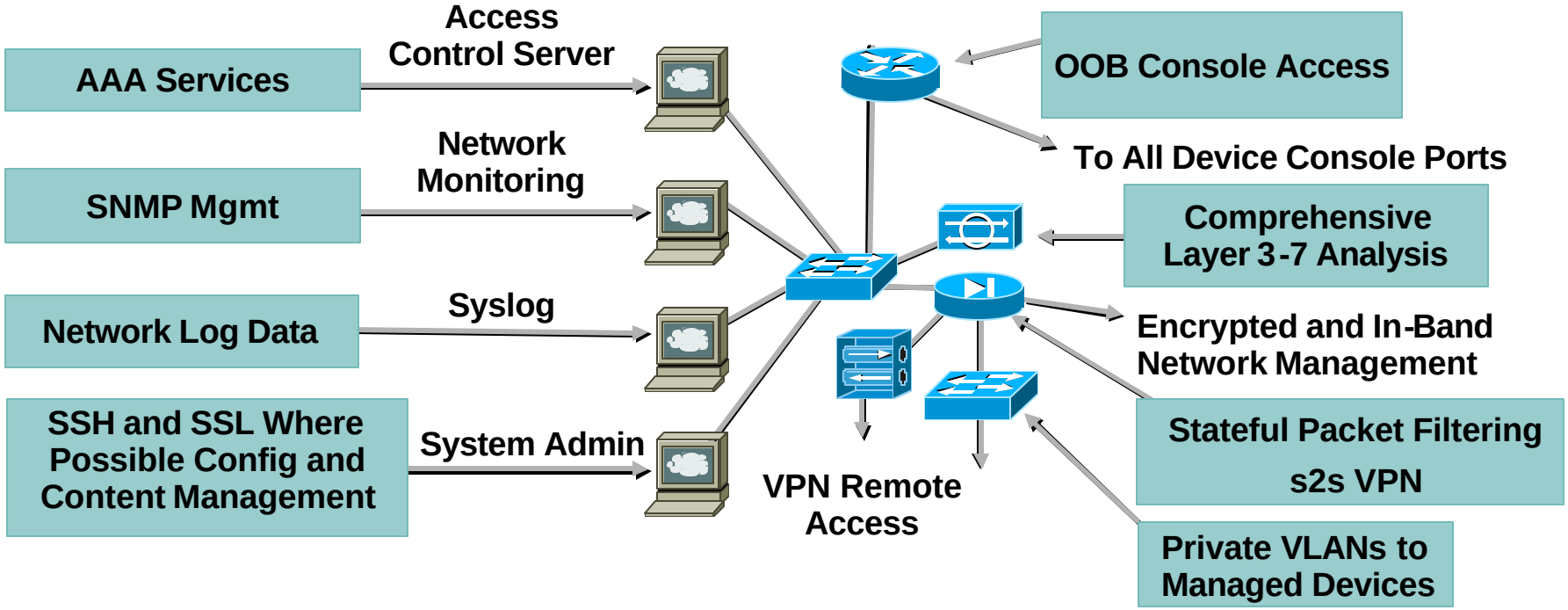
Management Channel Security

- **In-band in the clear**
  - Optionally with strong authentication
- **In-band secured**
  - Application layer encryption (SSH, SSL)
  - Network layer encryption (IPsec)
    - Good for non-configuration protocols
      - Syslog, TFTP, SNMP
- **Out-of-band management**
  - Strongest security
  - Beware topology sensitive management systems
- **Hybrid**
  - Combination of methods listed above
  - Based on proximity, scale and type of managed device

Protect C&C from Resource Starvation Attacks

Out-of-Band Secure NOC Sample

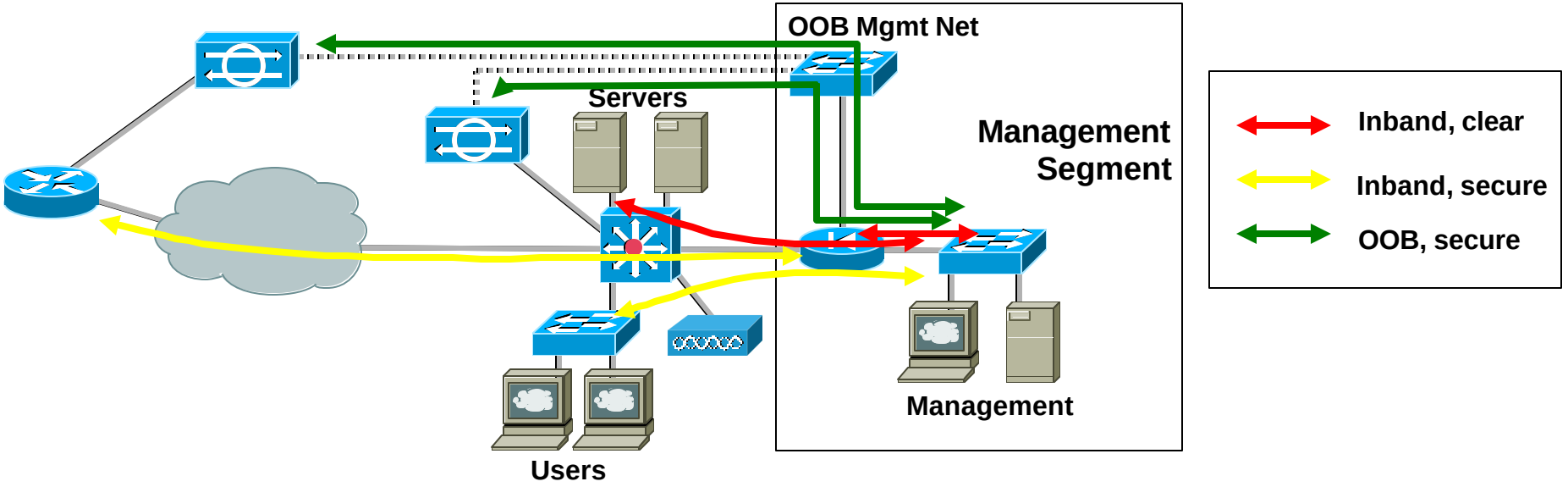
Cisco.com



- Out-of-band management
  - Separate physical networks, separate address space (i.e. 192.168.25x.xxx)
  - Use IPsec if physical separation is not possible
- Firewall between management subnet and managed-device subnet

- Isolate managed ports to minimize impact of compromised device
- NIDS and HIPS on the management subnet
- One-time passwords for authentication of administrators
- SNMP read-only

Hybrid Sample



- Focus on secure session and application layer protocols
- When clear-text is only viable option
  - In low-risk areas, use filtering and L2 best practices
  - In high-risk areas, use IPsec OOB management
- Combining separate addressing for OOB
  - In-band management will likely be filtered
  - Must use NAT for OOB or in-band (choice based on ease)

Routing Protocol Security

- Threats vary based on type of attack (traffic redirection, traffic black hole, router/routing protocol DoS, unauthorized prefix origination)
- The most damaging attacks can be caused by an attacker compromising a router
  - Hardening is critical
- Prefix filtering (defining what routing prefixes you should allow from specific locations) is key to preventing bogus advertisements
- At a minimum, message authentication via MD5 should be done (available for RIPv2, OSPF, BGP, EIGRP, IS-IS)
  - This helps not just with malicious attacks but with accidental ones (someone introducing a router into your network with incorrect information)

Agenda

- Axioms
- Policy Design Process
- Design Principles
- Best Practice Designs
  - Introduction to Designs
  - Internet Perimeter Design
  - Remote Access Design
  - Campus Design
- Conclusion

Introduction to Designs

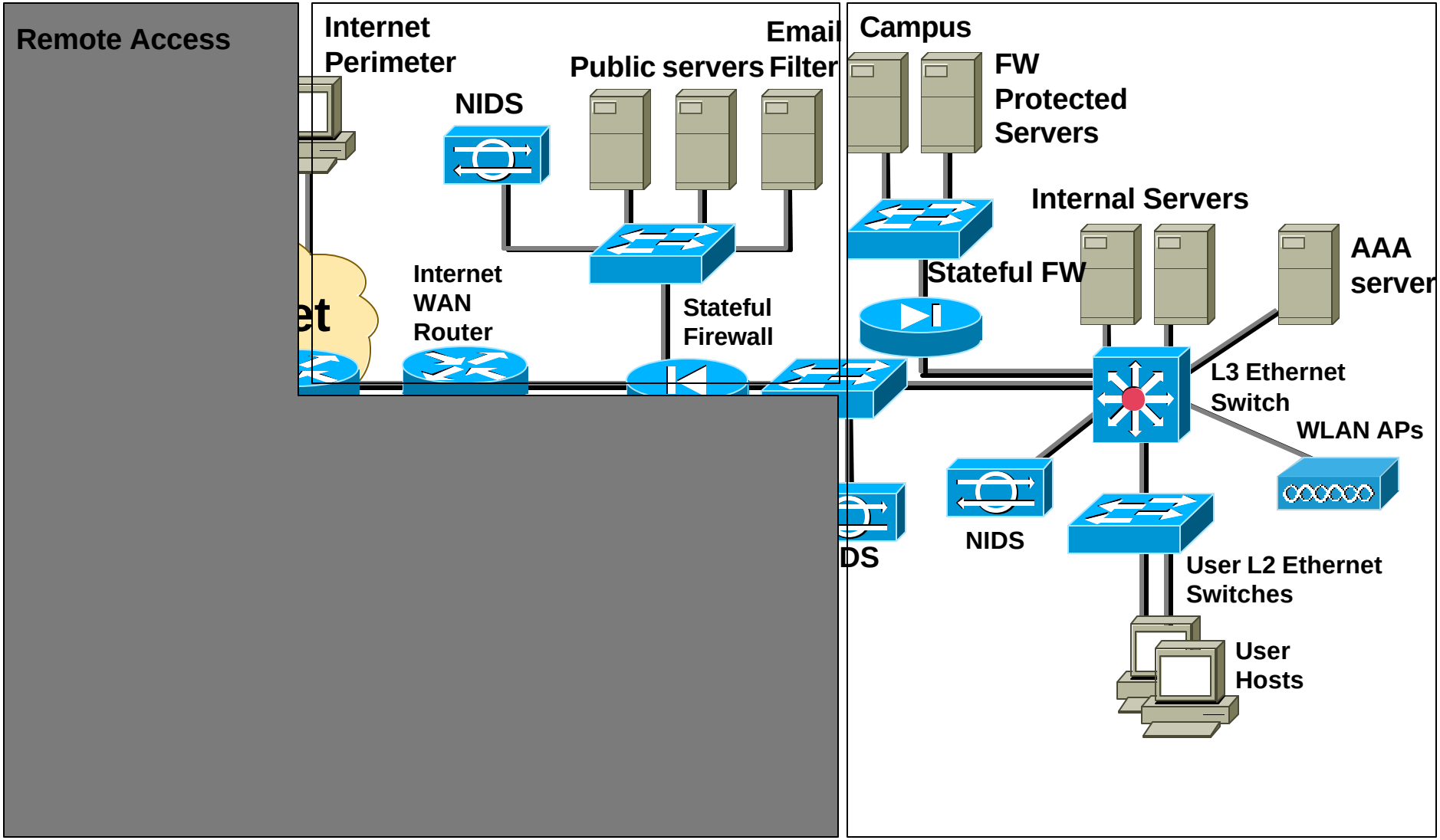
"Knowledge is to be acquired only by a corresponding experience. How can we know what we are told merely? Each man can interpret another's experience only by his own. "

Henry David Thoreau

- **These are examples, not designs in production today**
- **Management designs are not included, nor are high-end ecommerce or data center designs**

The Goal of These Examples Is to Explore What Is a Good Default Design and Then Examine How Designs Change with Unique Considerations.

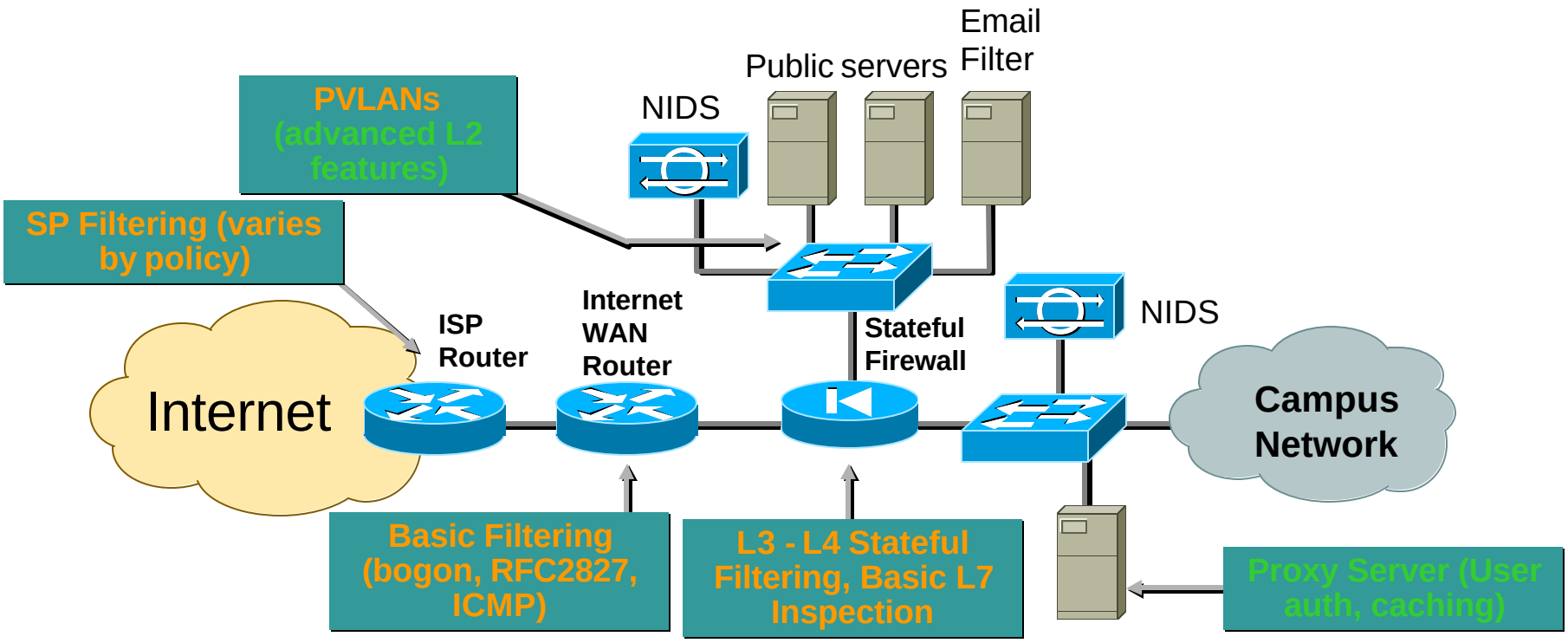
Overall Enterprise Design



Internet Perimeter Design

- **Design considerations**
  - Usually the largest threat point
  - 3 domains of trust (untrusted, public service, private)
  - Large trust gradients between each zone
  - Many variations depending on policy
- **Design approach**
  - Access control
  - Misuse detection
  - DoS mitigation

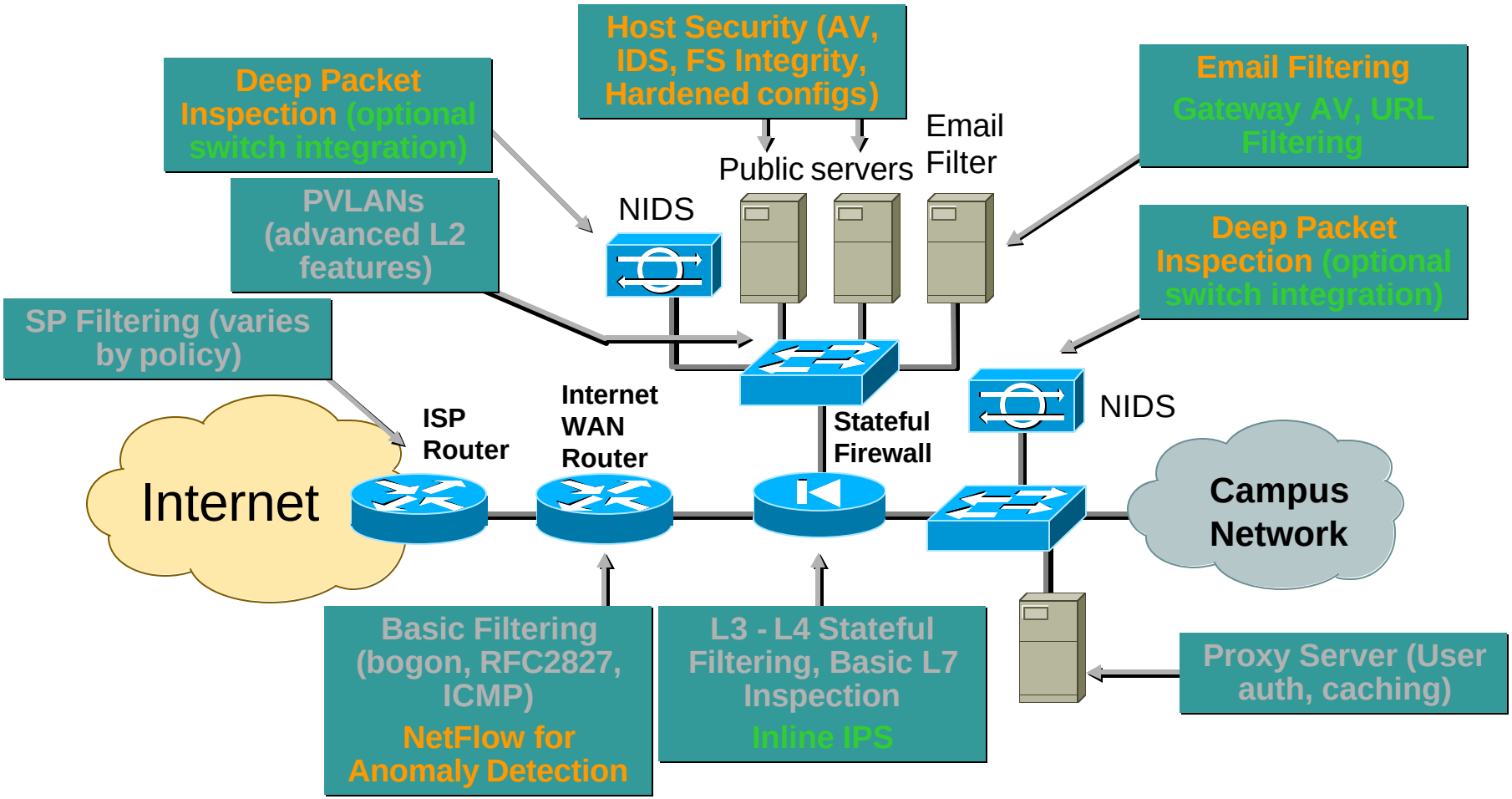
Internet Perimeter: Access Control



Recommended, Optional, Previously Discussed

Internet Perimeter: Misuse Detection

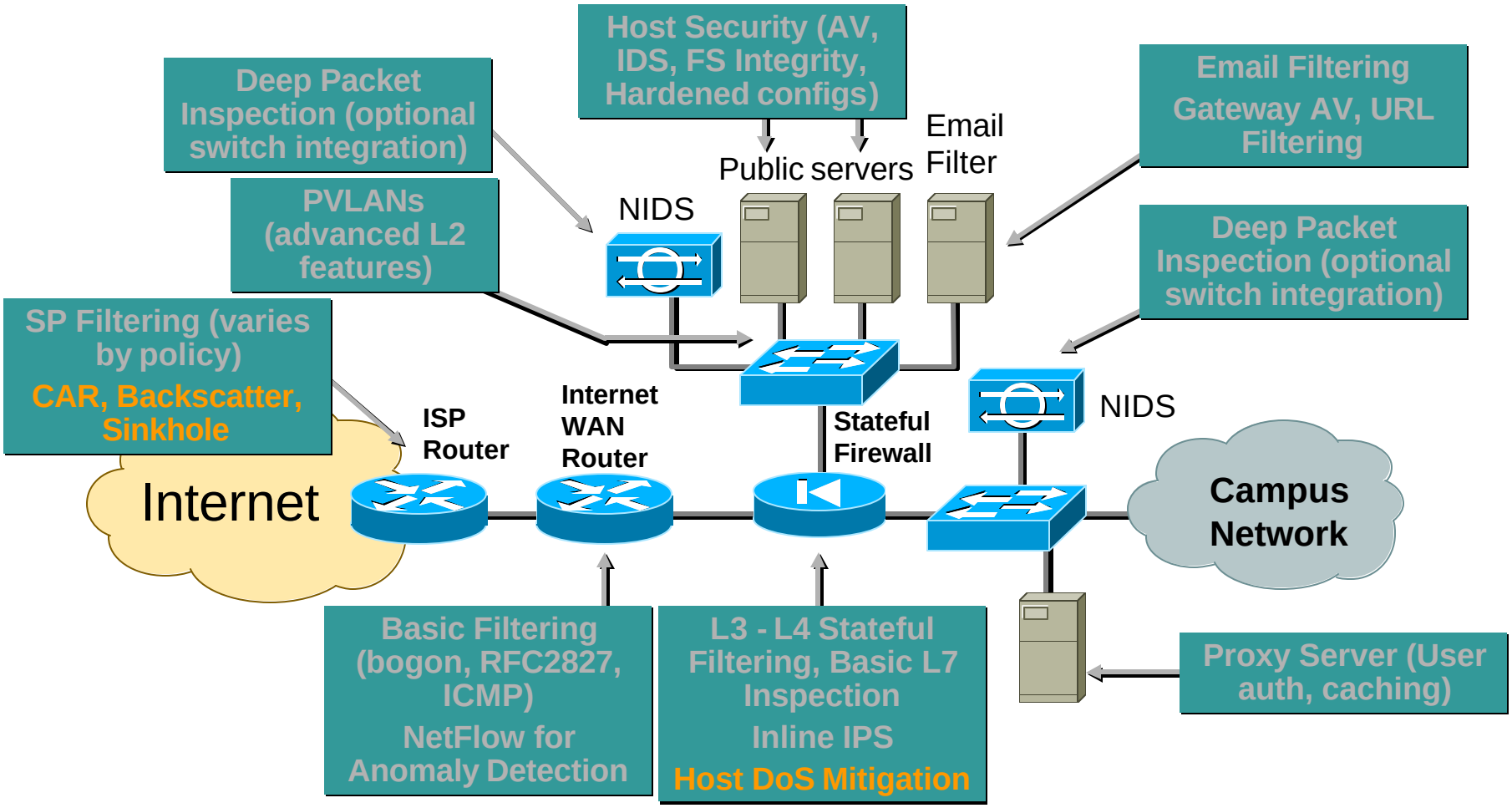
Cisco.com



Recommended, Optional, Previously Discussed

Internet Perimeter: DoS Mitigation

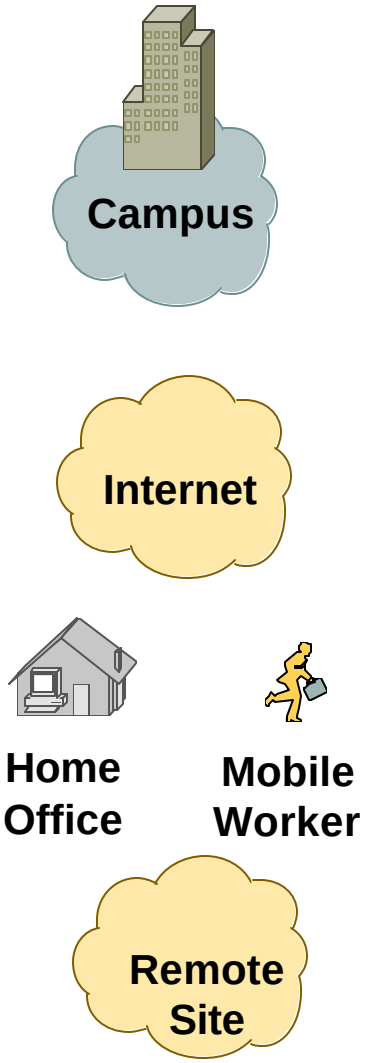
Cisco.com



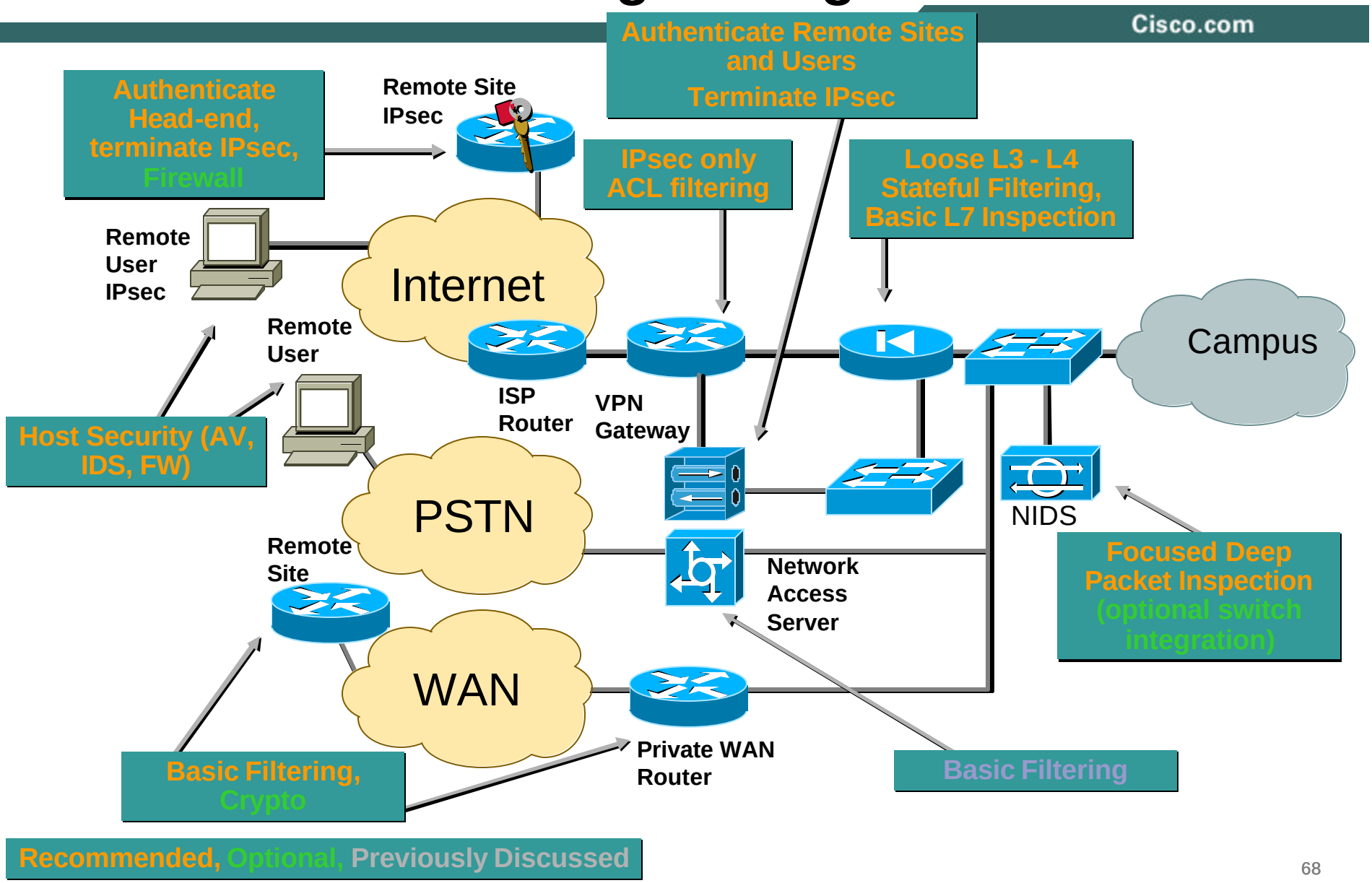
Recommended, Optional, Previously Discussed

Remote Access Edge Design

- **Design considerations**
  - Remote stations tougher to manage
  - Provide full service access, akin to campus
  - Domains of trust: remote WAN, remote user (PSTN), and remote IPsec (user and site)
  - Confidentiality over public links (optional on private)
- **Design approach**
  - Secure communications
    - Authentication and confidentiality
    - Aggregate remote communications
  - Primary goal to protect campus
    - Access control, misuse detection, spoof mitigation
    - Network admission control
  - Secondary goal to protect remote asset
    - Device hardening



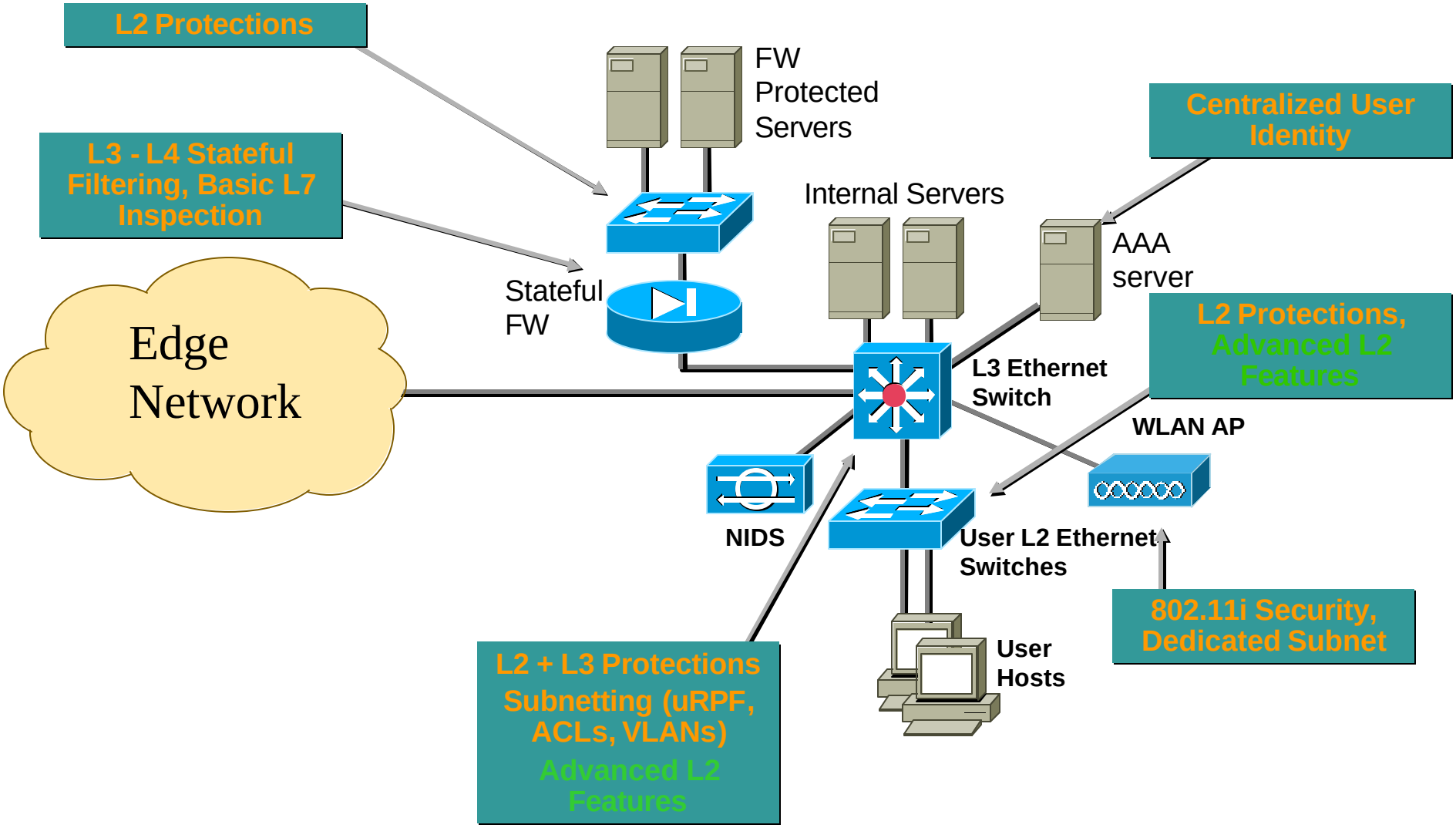
Remote Access Edge Design



Campus Design

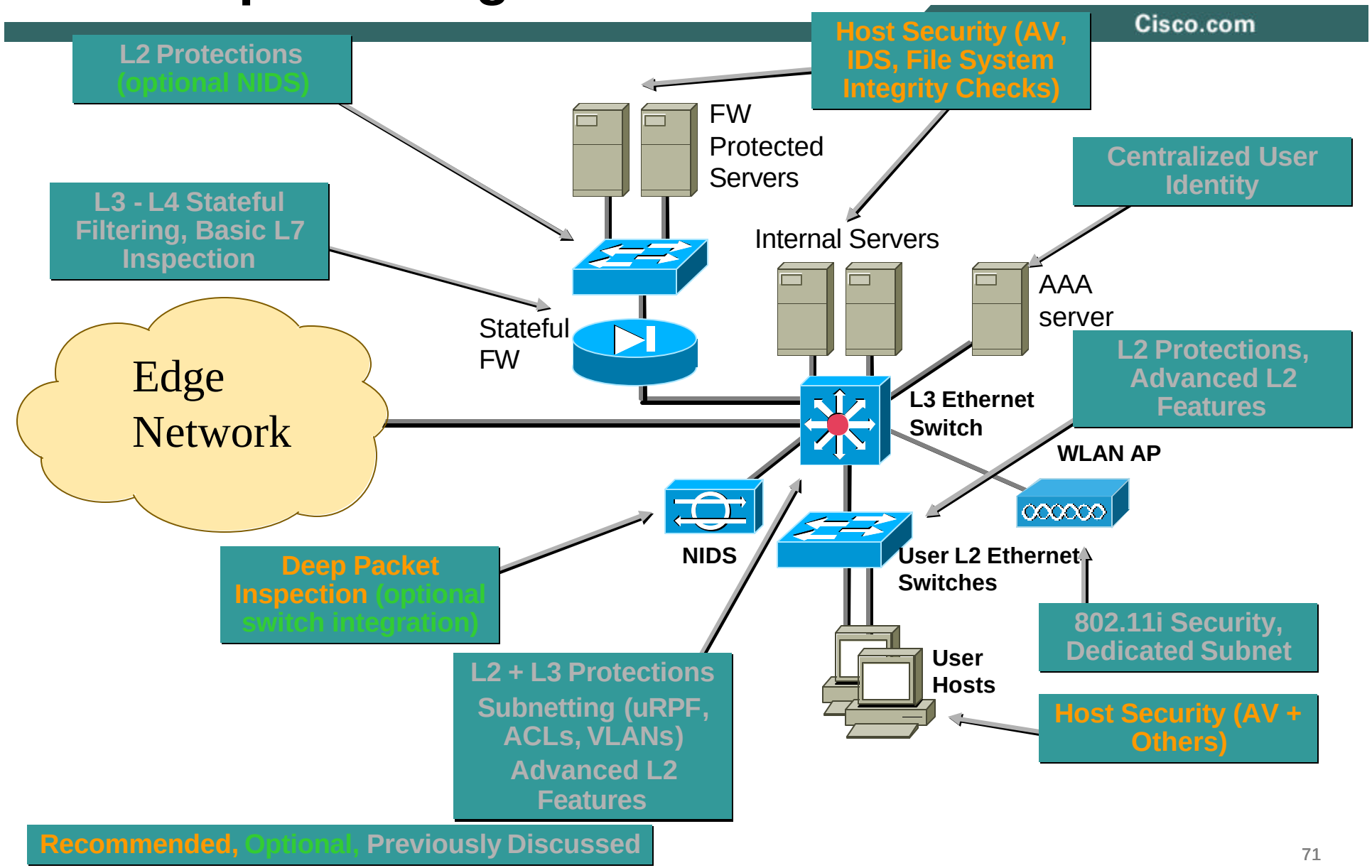
- **Often campus security design is dictated by the physical makeup of the network connectivity and location of resources**
  - **3 domains of trust (users, servers, sensitive servers)**
  - **Inter-zone trust gradients are smaller, allowing less stringent choke points**
  - **Separating users and servers into different trust domains is possible depending on make-up and location of groups and technologies like 802.1x**
- **Design approach**
  - **Access control**
  - **Misuse detection**

Campus Design: Access Control



Recommended, Optional, Previously Discussed

Campus Design: Misuse Detection



Conclusion

- **Summary**

  Network security is a system

  That system needs to incorporate your business needs, security policy, industry best practices, and risk analysis

- **Food for thought**

  While sample designs are helpful in getting a starting point, each network has unique considerations

  New technologies can be helpful in augmenting your system but be somewhat wary as best practices take time to develop

Complete Your Session Evaluation Form

Cisco.com

Thank you for attending this session.

Complete your session evaluation, por favor.

Give to the room attendants as you leave the room.

Muchas Gracias