



FOUNDRY[®]
NETWORKS

Emerging Networking Technologies and Design Techniques within a Regulatory Backdrop

Bill Ryan
Product Marketing Manager
Foundry Networks



Agenda

- **Laws and Regulations Impacting the Network Infrastructure**
- **Data Safe-guarding Network Design Considerations**
- **Lawful Intercept**
- **Q&A**



Laws and Regulations Impacting the Network Infrastructure

❁ **Two Primary Areas of Concern**

- Protecting Data from Unlawful Access
- Allowing Lawful Access to your network

❁ **Data Safe-guarding Laws and Regulations**

- Sarbanes-Oxley for corporate financial information
- HIPPA protection of patients information
- Gramm-Leach-Bliley for customer financial information

❁ **Lawful Intercept Laws and Regulations**

- CALEA in the United States



Safe-guarding Network Data

⚙️ **Network Access Control**

- Protect against malicious Network Entry
- Control against unsecure user access
- Quarantine Guest Users

⚙️ **Network Intrusion Closed Loop Protection**

- Identify anomalous traffic patterns and threats
- Centralized correlation of information with threat analysis
- Closed-Loop appropriate response to threat

⚙️ **Auditing, Monitoring and Reporting**

- Report Data intrusion to required agencies and constituents as required by law
- Continual monitoring of network for finer grain normalized traffic patterns
- Utilize Security Information Management for Compliance Audits



CALEA and Lawful Intercept

- ❁ **If you offer internet access and also act as primary supplier of VoIP services you may need to comply with CALEA**
- ❁ **EDUCAUSE challenged FCC and lost the challenge earlier this year**
- ❁ **Ruling is broad enough to potentially go beyond Higher Education environments**



CALEA and Lawful Intercept

- ❁ **If you offer internet access and also act as primary supplier of VoIP services you may need to comply with CALEA**

- ❁ ***Summary of the four elements to compliance***
 1. *Comply with warrant for all communications to and from a specific user mentioned in the warrant (not necessarily VoIP only).*
 2. *Comply with warrant for calling information for VoIP traffic if you manage the VoIP service including caller id, call services such as conference calling etc.*
 3. *Send this information to the Law Enforcement Agency in a specific format.*
 4. *The target of the warrant as well as anyone else must not know about the tap, including multiple agencies targeting the same user, and send the information to all the agencies with valid warrants independently of each.*



IT Security

- ⚙️ **Network Security is an Integral Piece of Your Larger Corporate Security Solution.**
- ⚙️ **Develop a Holistic Security Strategy**
- ⚙️ **Implement the Security Plan**
- ⚙️ **Evolve Security Anticipating New Threats**



Safe-Guarding the Network



Key Security Solution Components

- ❁ **Integrated L2-3 Security in Foundry wired & wireless switches and routers**
 - DoS Attack Prevention
 - Protocol Protection
 - Spoof Protection
- ❁ **Purpose built, stand-alone security products**
 - SecureIron perimeter defense
- ❁ **Security products that work with Foundry switches to enhance security**
 - Network Anomaly Detection (using sFlow)
 - Network Access Control (using 802.1x)
 - Security Information Management (using logs and sFlow)



Layered Threats and Corresponding Defense Methods

		Defense Methods	
Threats		Access Control	Detection & Filtering
L7	WORMS VIRUSES TROJANS	FIREWALLS URL FILTERING SPAM MITIGATION	INTRUSION PREVENTION ANTI-SPYWARE ANTI-VIRUS
L4	UDP/TCP PROTOCOL ATTACKS ROGUE SERVICES UDP/TCP DOS ATTACKS	IDENTITY ACCESS MGMT	NETWORK ANOMALY DETECTION L4 DOS PREVENTION
L3	ROUTING PROTOCOL ATTACKS L3 DOS ATTACKS NETWORK SERVICE ATTACKS	IPSEC VPN ROUTING AUTHENTICATION SSL VPN	L3 DOS PREVENTION L3 PROTOCOL ATTACK PREVENTION
L2	L2 DOS ATTACKS L2 ROGUE SERVICES L2 SERVICE ATTACKS	802.1X RADIUS NAC SSH PASSWORDS	L2 DOS PREVENTION L2 PROTOCOL ATTACK PREVENTION



Blurry Line



Solution –360 Degree Network Security

sFlow-based Anomaly + Signature Defense

Zero-Day Anomaly IDS

Signature IDS



Open Source Applications



- Integrated Switch and AP Security Features**
- DoS attack protection
 - CPU protection
 - Rate limiting
 - Hardware-based ACLs
 - DHCP, ARP, IP spoof protection
 - Rogue AP detection & suppression
 - Access policy enforcement
 - Threat control enforcement
 - Embedded sFlow traffic monitoring

Network Switches, Routers, & Access Points

App & Web Servers



Access Policy



Radius, DNS, DHCP



Call Manager



Multiple endpoints
IEEE 802.1x + MAC Authentication



Network Access Control

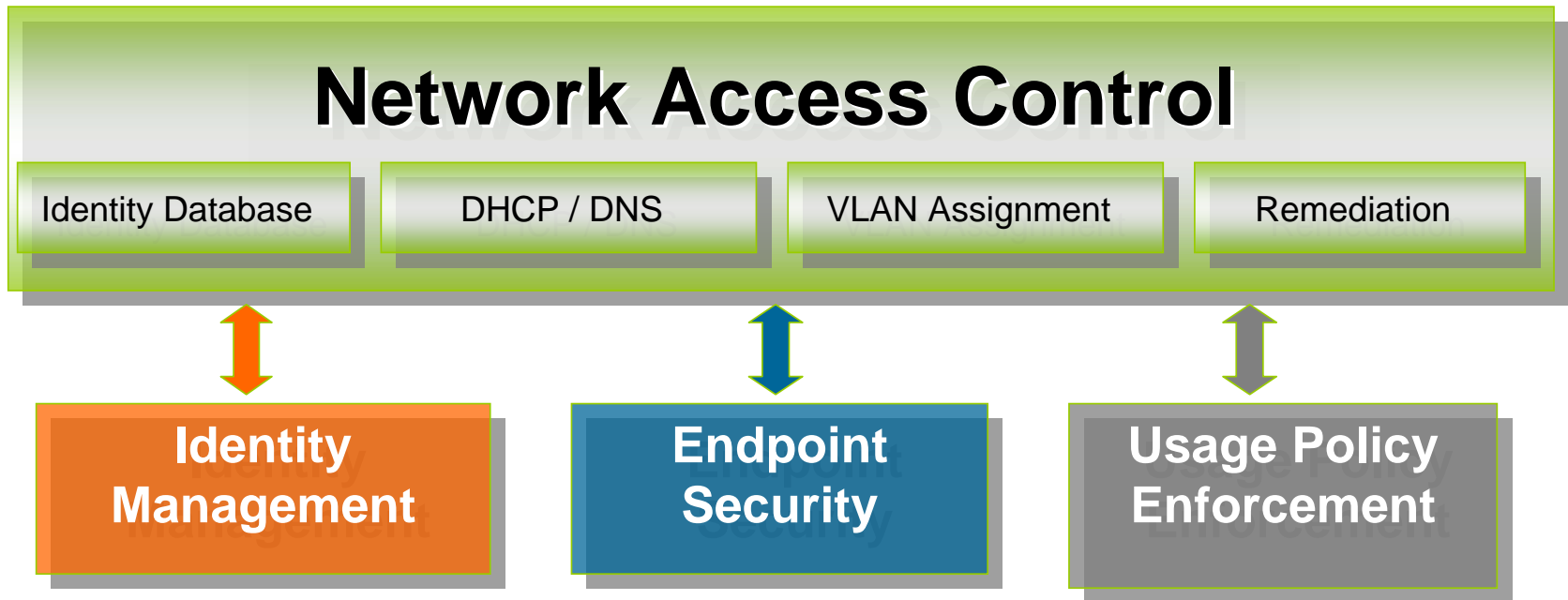


Endpoint (Host) Security

- **Endpoint security composed of up to four defenses**
 - Personal Firewall
 - Host IPS
 - Threat Assessment
 - Network Access Control
- **Personal Firewall and IPS protects against incoming attacks**
- **Threat Assessment determines if host already infected or has security holes**
- **Network Access Control helps protect against incoming and outgoing threats**
 - Policy check made before entry into network granted
 - Policies could include check for A/V software, OS patch level, etc...
 - Helps protect host and the internal network by preventing viruses from spreading
- **Multiple methods: Persistent client NAC, NAC appliance (inline, out-of-band)**
- **Top vendors include: Symantec (Sygate), CheckPoint (Zone Labs), Cisco, and Microsoft (NAP)**
- **Many NAC appliance vendors**



NAC Solution Architecture





Why NAC?

- ❁ **Organizations continue to be plagued by worms, viruses, and spyware**
 - Viruses are #1 cause of financial loss (FBI)
- ❁ **Mobile PCs and wireless allow users to get infected outside of the organization**
- ❁ **Infected PC's get connected to the Enterprise and infect others**
- ❁ **Users run software that is not authorized by the Enterprise**
- ❁ **Simple authentication is not enough**
- ❁ **Network Access Control provides tools that validate health and policy compliance of the clients**

“Endpoint systems are vulnerable and represent the most likely point of infection from which a virus or worm can spread rapidly and cause serious disruption and economic damage.”

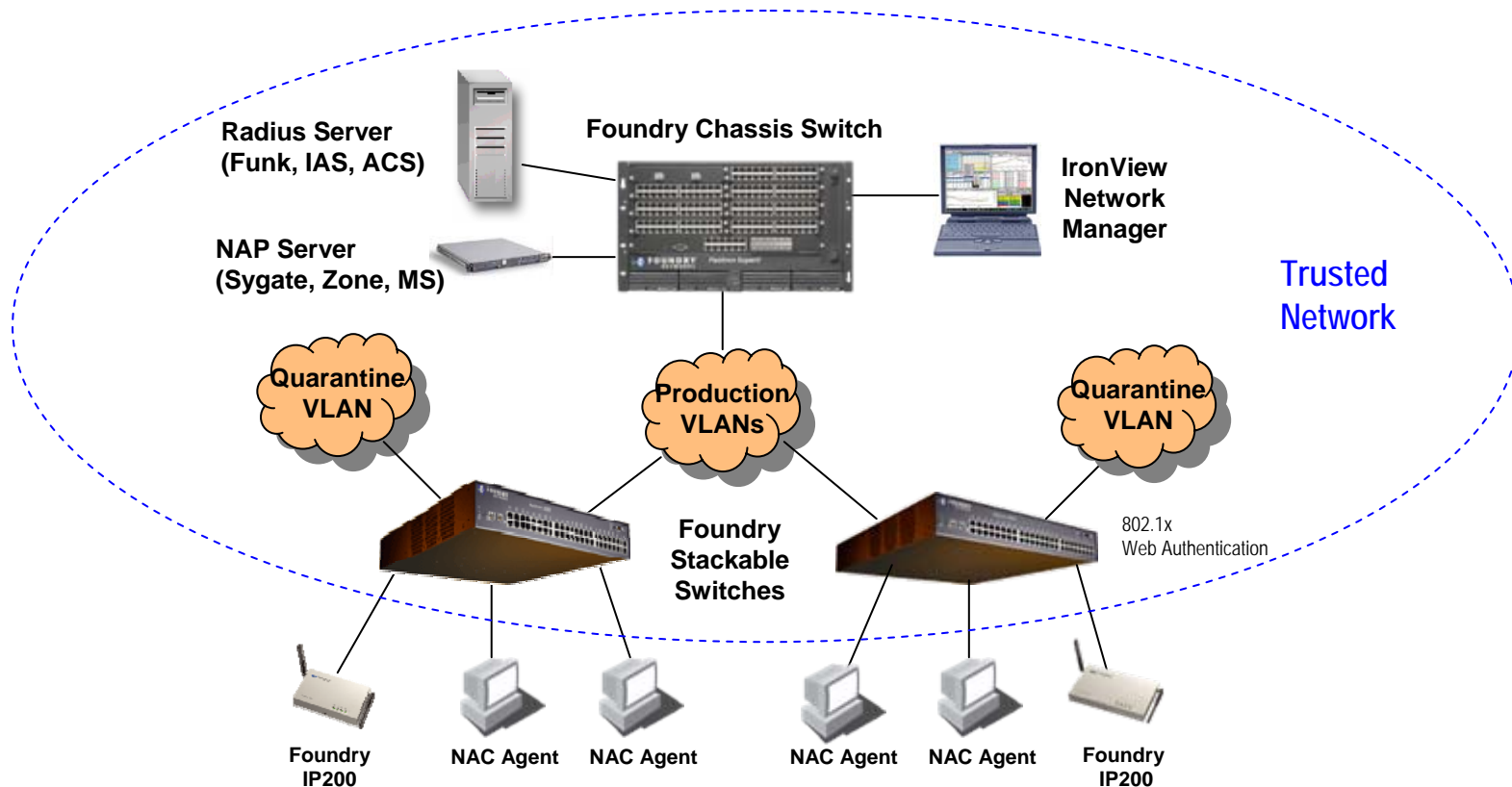
– Burton Group

“Because of worms and other threats, you can no longer leave your networks open to unscreened devices and users. By year-end 2007, 80 percent of enterprises will have implemented network access control policies and procedures.”

Gartner, *Protect Your Resources With a Network Access Control Process*



Foundry Endpoint Security Solutions

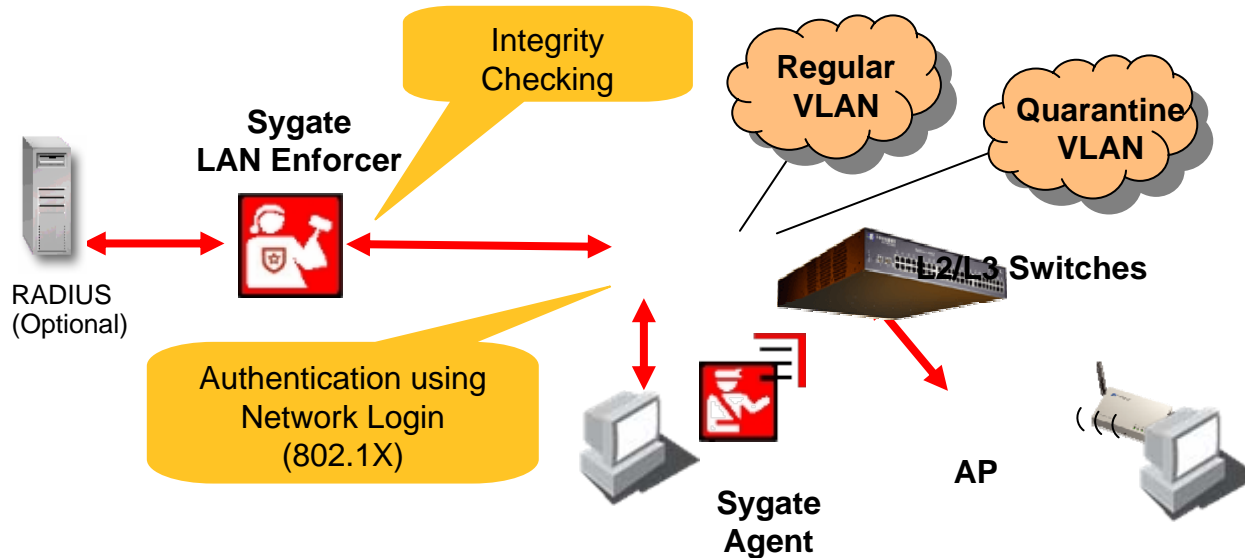


Foundry Edge products have been validated with best-of-breed NAC, personal firewall, and host based IPS solutions from the two top solution vendors: Sygate and Check Point (Zone Labs).



Symantec (formerly Sygate)

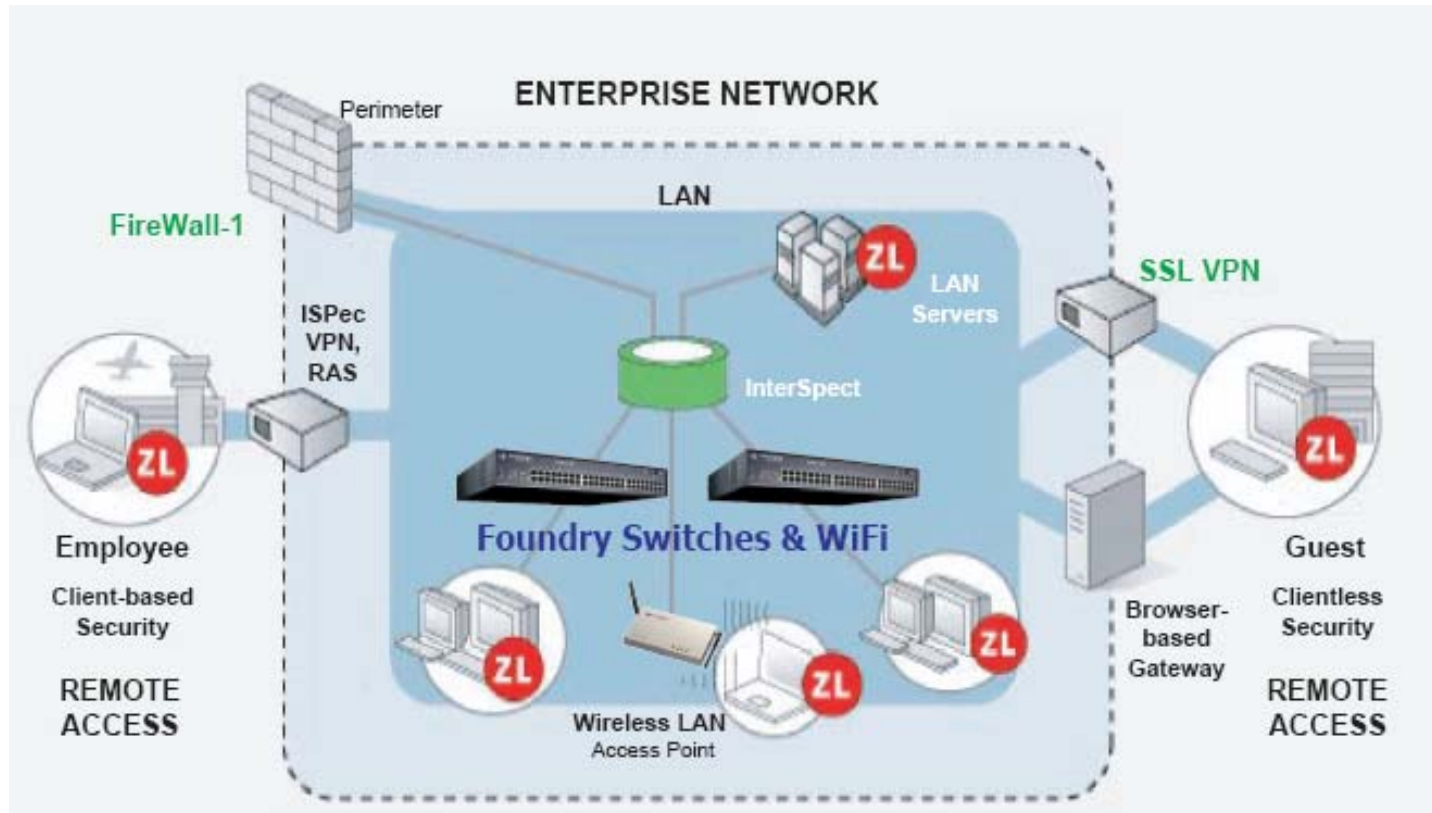
Secure Enterprise Client based NAC



- Sygate offers standards based 802.1x L2/L3 switching & network admission control solutions today
- Support for both Sygate Basic and Transparent Mode (no Radius server required)
- Best-of-breed Foundry L2/L3 switches & routers, and Sygate Secure Enterprise software
- Works with a variety of Radius servers (Funk, IAS, ACS, FreeRadius)
- Supports admission control on both wireless and wired infrastructure
- Host IPS + Firewall + NAC
- Foundry + Symantec have received Army TIC certification



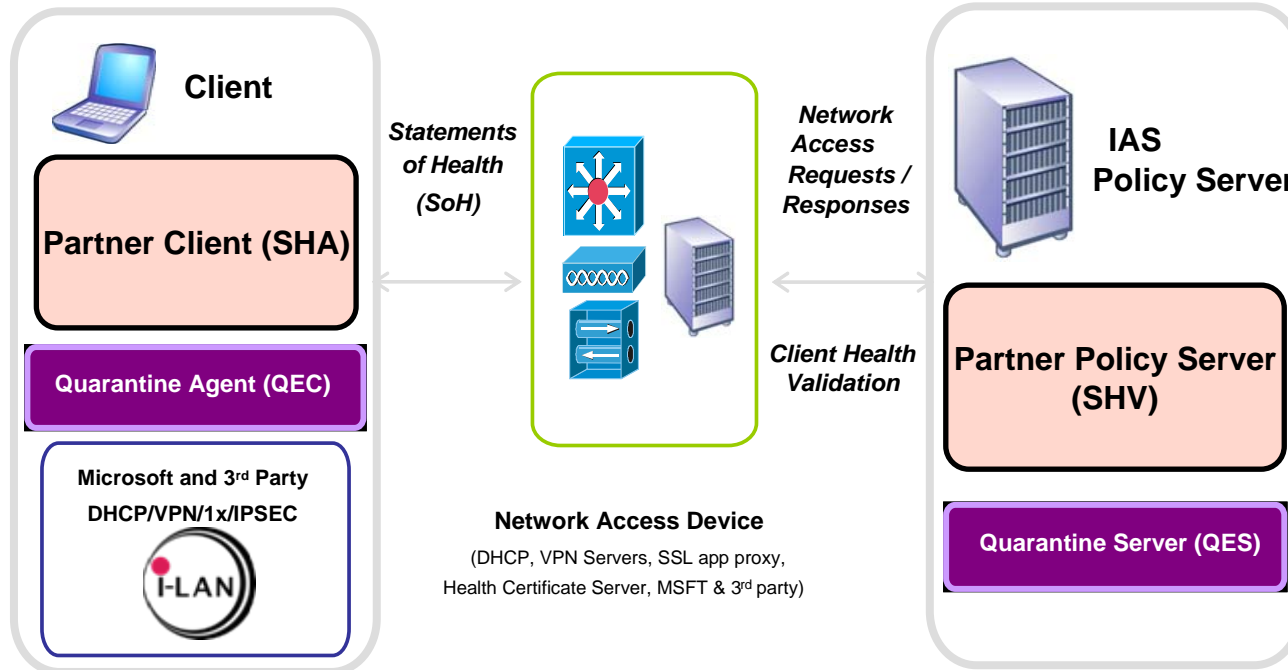
Check Point Software (Zone Labs) *Integrity Family of Client based NAP*



- Integrated solution supports wired and wireless client admission control
- Uses standards based 802.1x approach that is available today
- Works with a variety of Radius servers (Funk, IAS, ACS, FreeRadius)
- Support for Session termination for automatic quarantine VLAN remediation
- Integrated Host IPS + Firewall + NAC
- Supports Windows and Linux



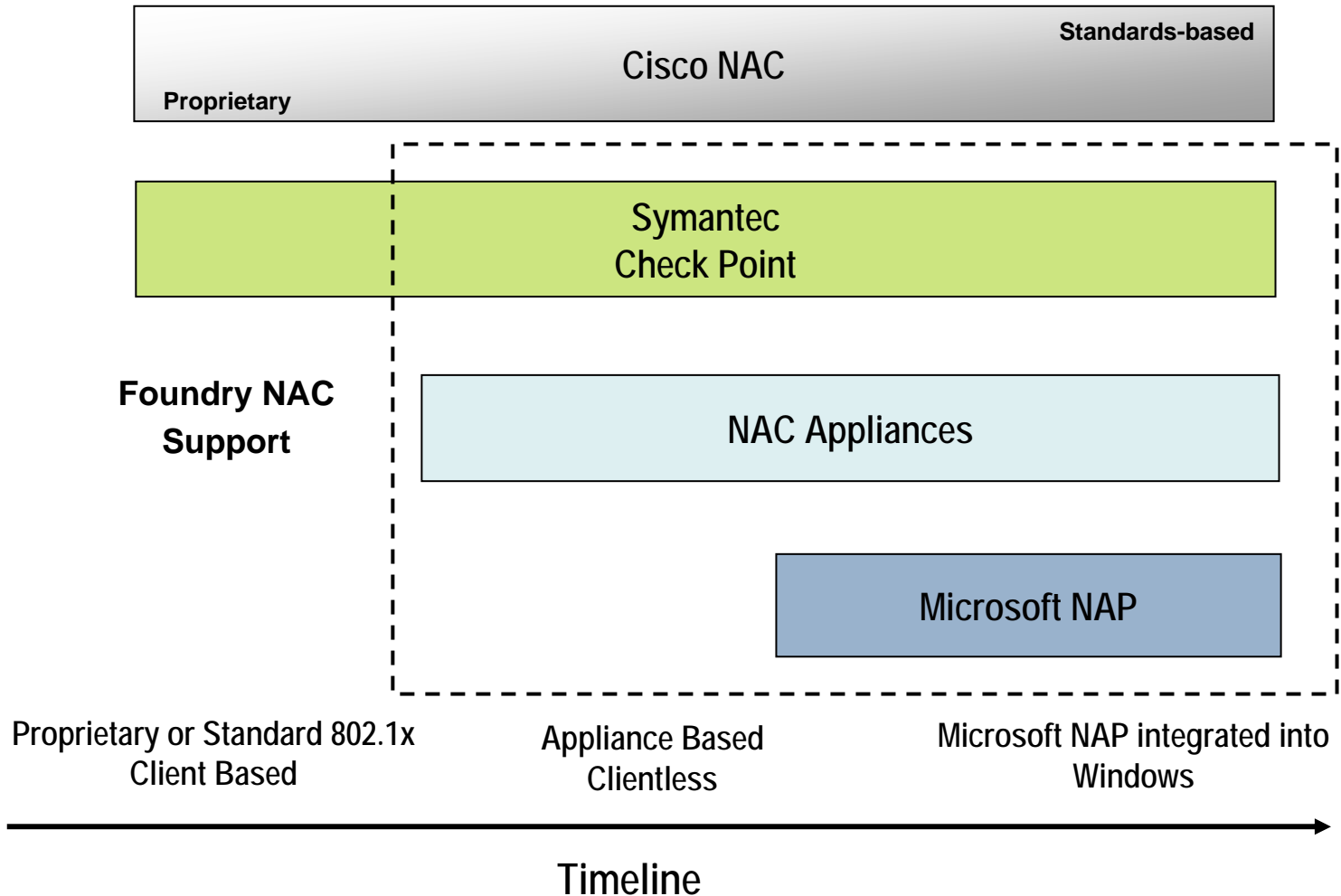
Microsoft NAP Architecture



- ❁ Microsoft Solution can use standard 802.1x (Radius) to interact with Foundry switches, but IAS is required
- ❁ Cisco NAC uses proprietary 802.1x (Cisco routers only) and requires ACS
- ❁ Symantec and Check Point use standard 802.1x and can use any Radius Server



Network Admission Control Market Technology Direction

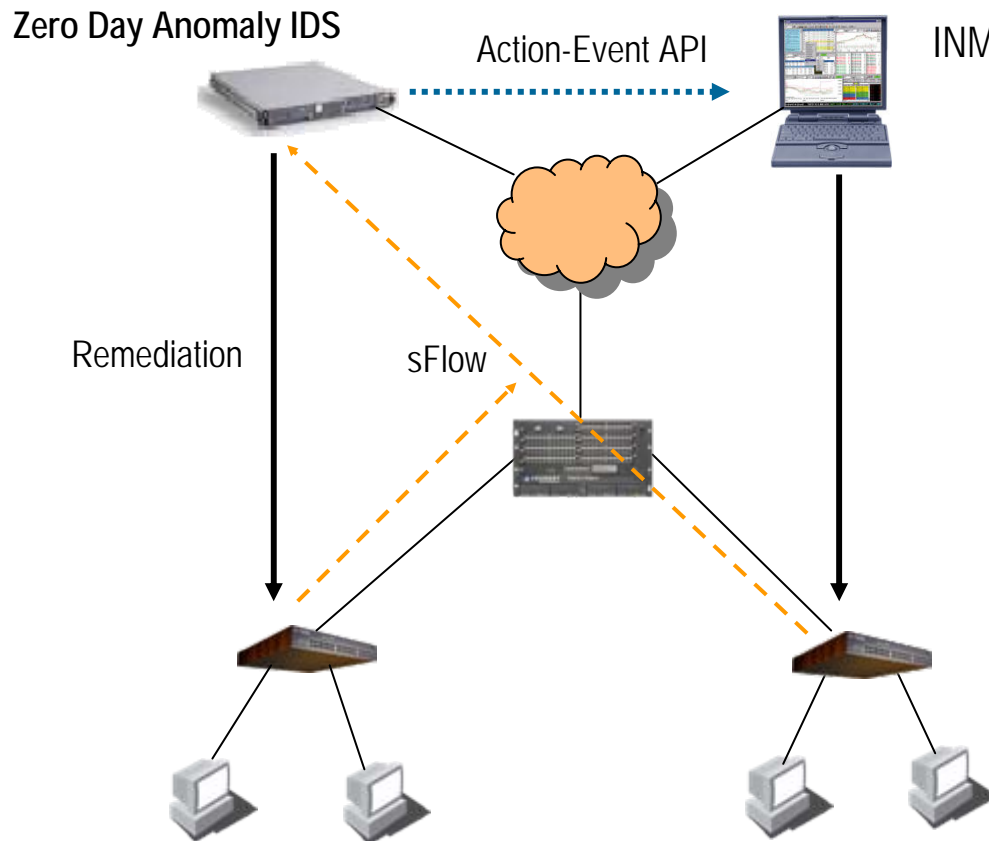




Network Based Anomaly Detection



Anomaly Detection & Zero Day Solution Remediation Through INM-Action Event API



❁ **sFlow based Anomaly Detection can be provided through Security alliance Partners**

- Lancope
- Arbor Networks

❁ **INM Action-Event API**

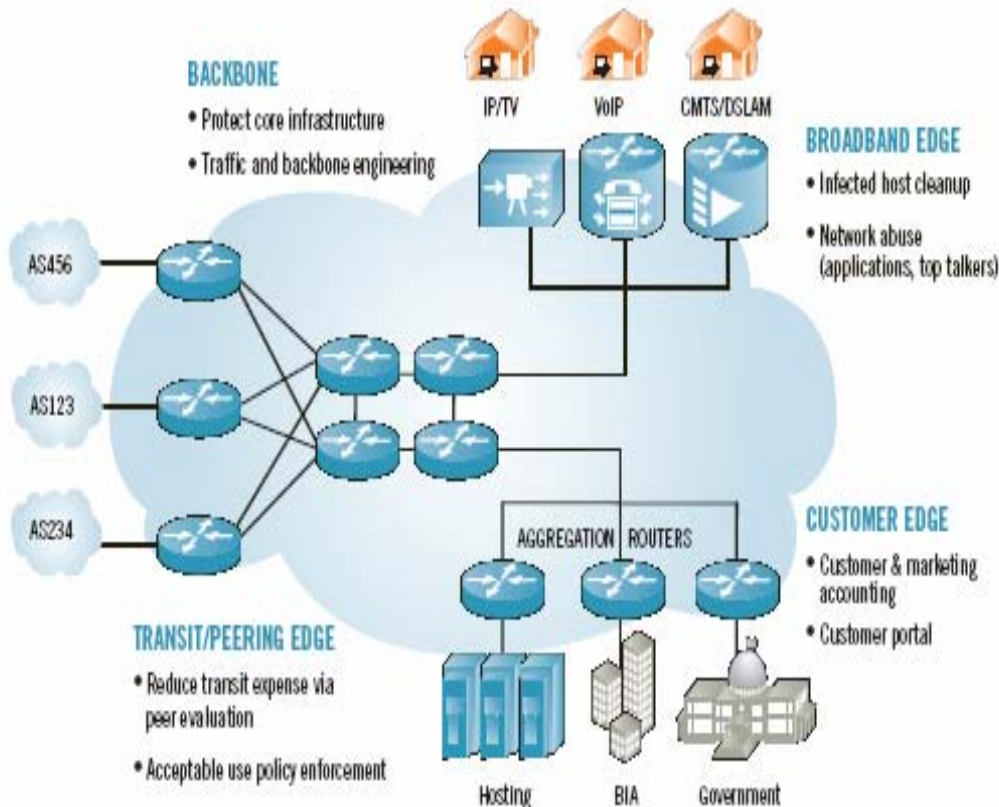
- Log to Event File
- Email alerts
- Block Port
- Rate Limit
- VLAN reassignment

❁ **sFlow reduces or eliminates need for sensors to be placed throughout network**



Arbor Networks PeakFlow & Foundry

High Speed Service Provider & Enterprise based Network Anomaly Detection Solutions

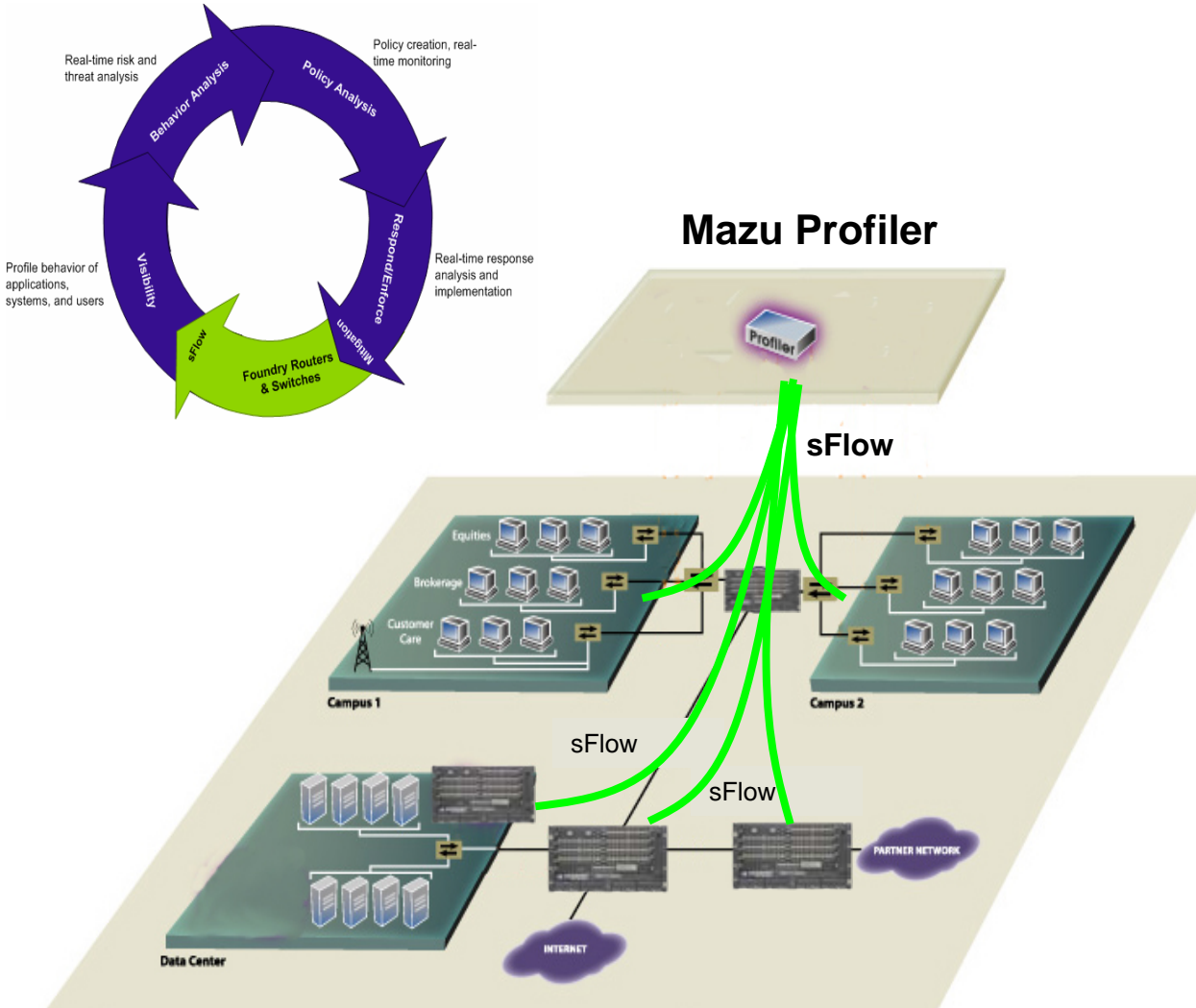


- sFlow based anomaly detection and DDoS prevention at speeds up to 10Gig for Service Providers
- Support for Foundry edge and core SP and enterprise switches and routers
- Network wide tracking and analysis of converged network security
- Platform for network and security service offerings
- Evaluate network peering relationships and reduce transit costs
- Network wide traffic engineering and real-time topology/event correlation



Mazu Profiler & Foundry

sFlow based Visibility, Zero-Day Protection, and Compliance Monitoring

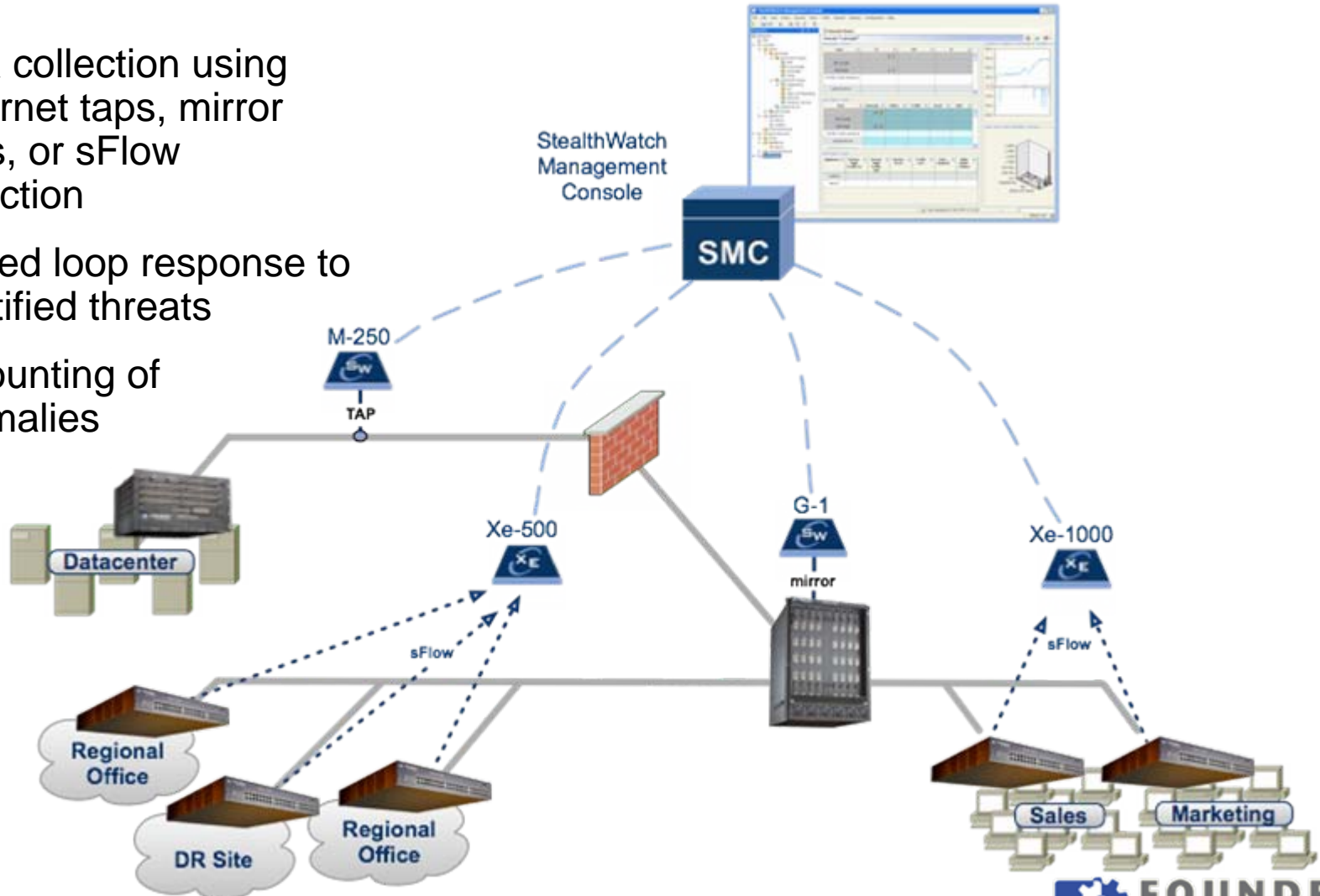


- Behavioral modeling of all endpoints and applications
- Zero-Day Anomaly Detection & Prevention
- Leverages Foundry sFlow implementation to analyze edge and core network traffic
- Ideal for network visibility in a Gig and 10Gig network environment
- Provides compliance monitoring for HIPAA and other regulatory regimes



Lancope Enterprise STEALTHWATCH Deployment

- Data collection using Ethernet taps, mirror ports, or sFlow collection
- Closed loop response to identified threats
- Accounting of anomalies

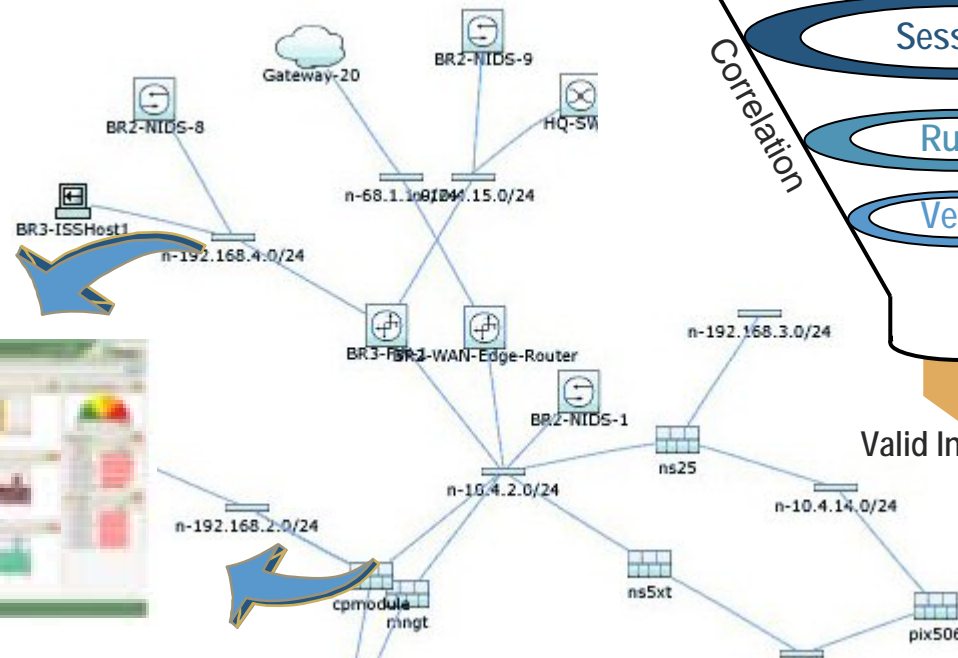
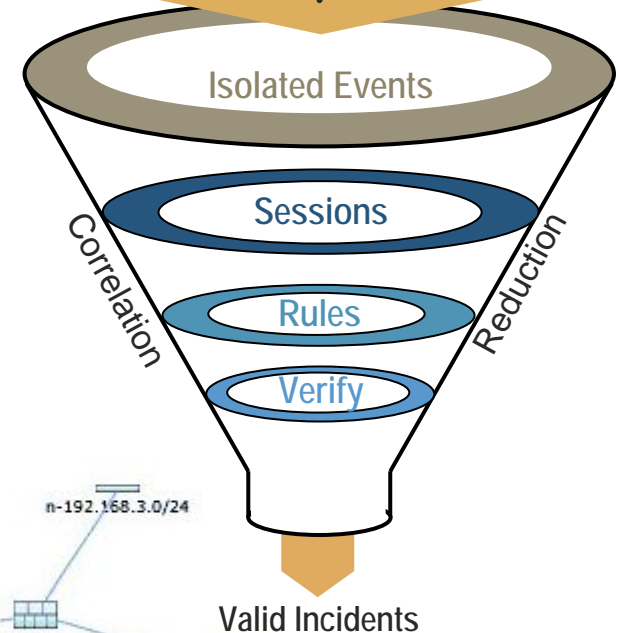




Security Information Manager Products

- Network Intelligence**
 - Topology, traffic flow
 - device configuration,
 - and enforcement devices
- Event Correlation**
 - Correlates, reduces and categorizes events
 - Validates incidents
- Remediation**
 - Change FW rules
 - Change port config

Firewall Log	IDS Event	Server Log
Switch Log	Firewall Cfg.	AV Alert
Switch Cfg.	NAT Cfg.	App Log
Router Cfg.	sFlow	VA Scanner
⋮		



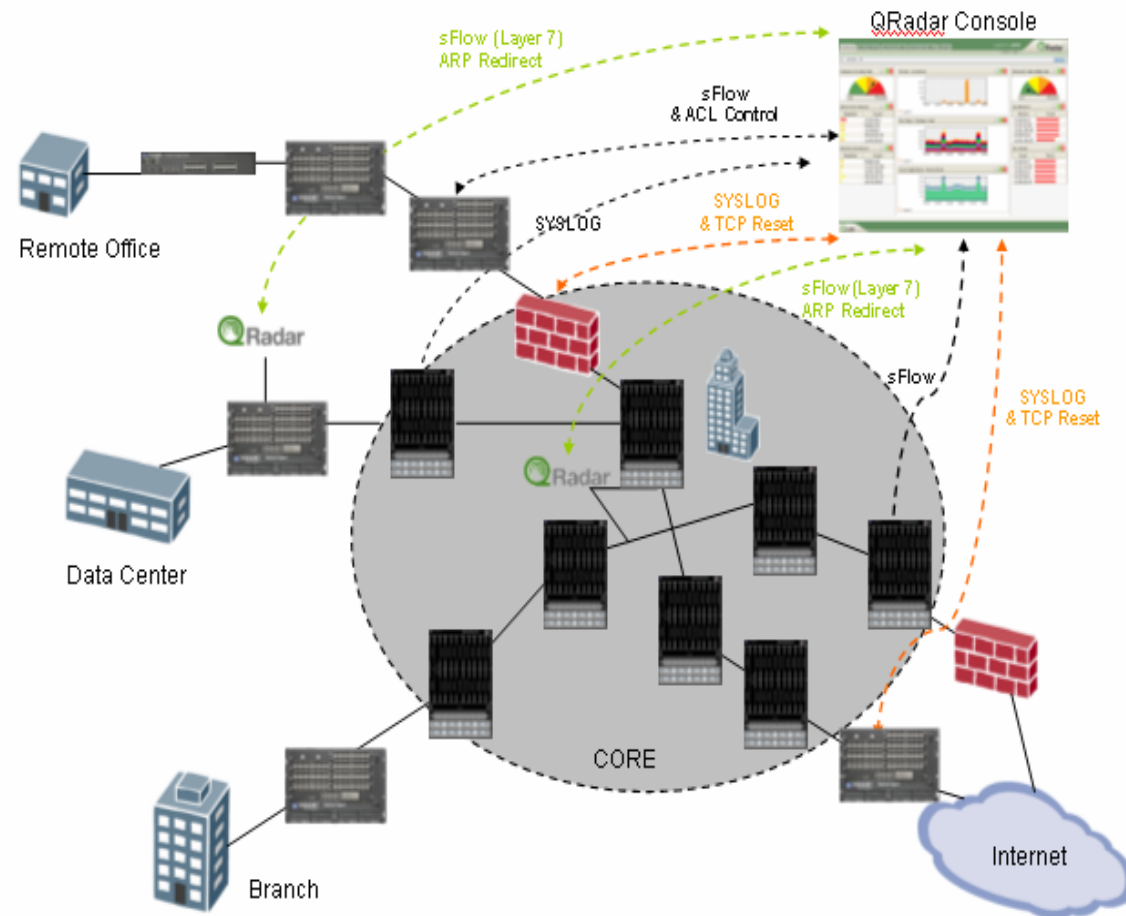
SIM Console





Q1 Labs QRadar

Flow Based Security *Event Correlation*



- Flow based security event correlation and asset-based vulnerability assessment
- Industry's most complete, integrated and responsive solution for thwarting threats to networks
- Event correlation using sFlow, netflow, syslog, and vulnerability assessment analysis
- Pulls syslog from firewalls as well
- Can remediate firewalls, switches, routers
- Support for regulatory compliance initiatives
- Interoperable with all Foundry sFlow based switches and routers

Lawful Intercept



Lawful Intercept

- ❁ **There are Three Levels of Lawful Intercept**
 - Capturing Calling Information; who is calling the person of interest, who the person of interest is calling and any three-way calling.
 - Capturing the two-way conversation of a VoIP call.
 - Capturing all data two and from the person of interest.
- ❁ **There are Three Distinct Elements for implementation**
 - Access Function which captures the information
 - Delivery Function which correlates and relays the information
 - Collection Function which receives the information
- ❁ **The Collection Function resides at the requesting Law Enforcement agency**
- ❁ **The Access Function and Delivery Function resides at the location implementing the Intercept as defined in a Warrant**



Lawful Intercept – A few Caveats

- ❁ **Multiple Warrants may be served**
 - They must be handled independently
 - Each agency must be unaware of the others warrants
 - Duplicate copies are sent independently by the DF to each requesting CF as needed
- ❁ **The Warrant must remain confidential**
 - The person of interest must not know of the intercept
 - No one on your staff that is not authorized to know may no about the warrant
- ❁ **Warrants have specific timeframes and the DF must ensure that no information is collected and sent to the CF outside the scope of the warrant**

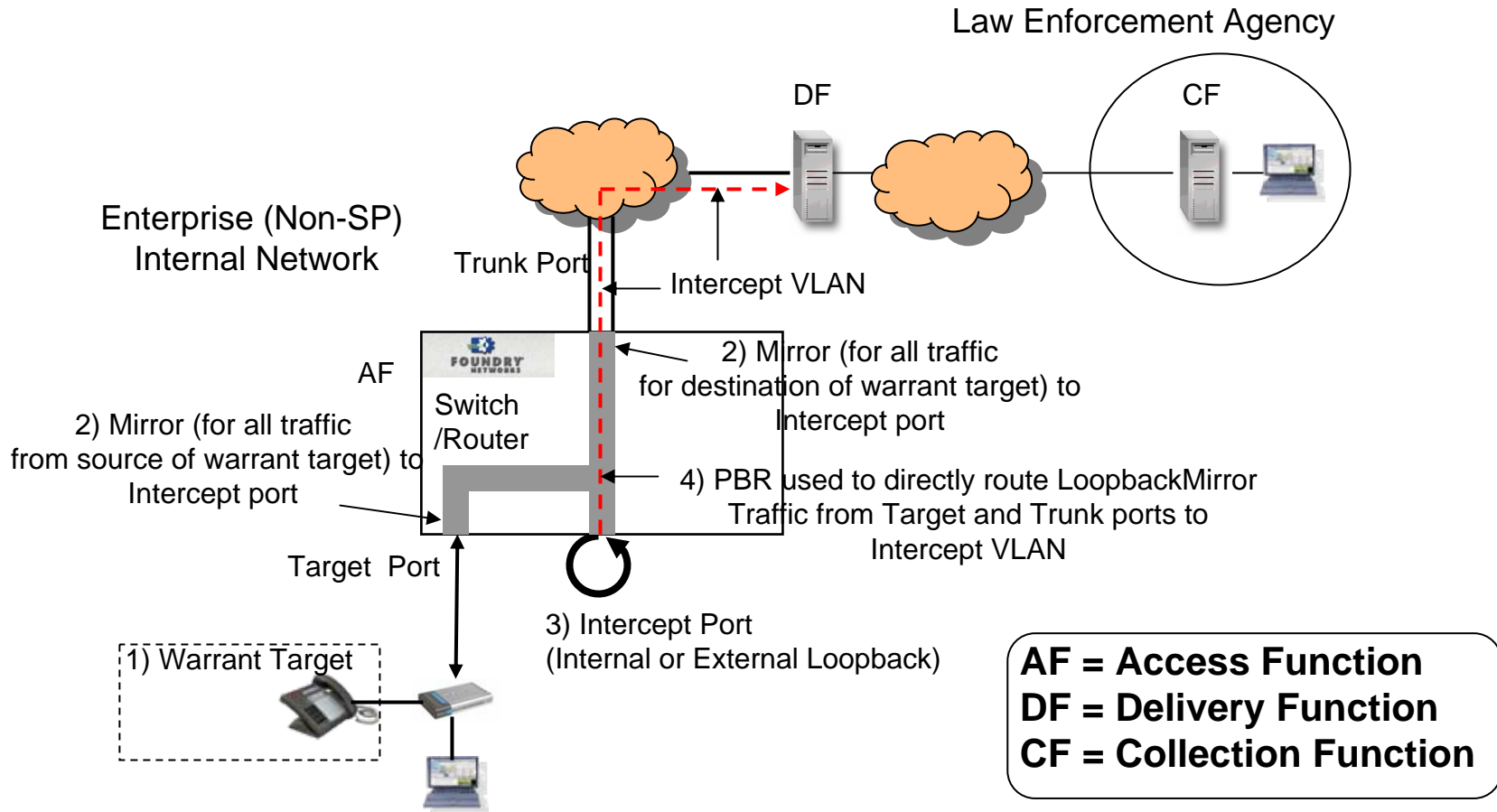


Lawful Intercept Function Demarcation

- ❁ **The Collection Function (CF) is owned by the Law Enforcement Agency.**
 - Starts the Lawful Intercept process by submitting the Warrant to the Delivery Function (DF).
 - It receives the information in a specific standards based format from the DF
- ❁ **The Delivery Function (DF) is located and owned by the entity receiving the warrant (you).**
 - It receives and authenticates warrants
 - It configures the Access Functions to trap the requested information and send to the DF
 - It packages the data in a standards-based format and sends it encrypted to the CF
 - It disables the configuration on the AF(s) at the end of the warrant period
- ❁ **The Access Function (AF) is also owned by the entity receiving the warrant**
 - If it is a call feature warrant then this is done on the Session Border Gateway or the Call Manager using Vendor Specific mechanisms to collect and transmit the data
 - If it is a content (VoIP only or all data) collection is done by the switch or router closest to the person of interests entry point to the network using Vendor specific mechanisms
 - The DF device needs to understand the vendor mechanism (raw mirrored traffic is the easiest) that is why this is sometimes also called the mediation device



Lawful Intercept Example





Summary

- **A growing number of Laws and Regulations require securing the access to data.**
- **Attacks from within and without the network need to be secured against**
 - Crackers trying to hack into the system
 - Malcontent Employees, Visitors or Contractors trying to access data
 - Worms and Viruses unleashed by unsuspecting users
- **Perimeter Security needs to be Enhanced with Cost-Effective Internal Security**
- **Lawful Access to the Network is coming starting with Higher Education Networks**

Q&A

Thank You