Overall Security in IT environment

ITAPA 2007

Tomáš Ondovčík

tondovci@cisco.com

The Security Situation

Threat environment has reached unprecedented levels of complexity

- Multiple types of security threats
- Fast spreading

No single technology or device stops everything

- It is not a Firewall but a distributed approach

Source can be inside or outside

- Need to be able to isolate source
- Need to enable a suite of features that complement each others

Everything is a Point of Attack
Everything needs to be a Point of Defense

Everything is a target

Some of these can be turned into weapons

New breed of attacks have multiple vectors that cannot be blocked by one device

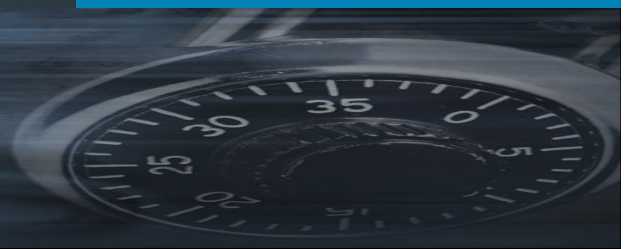
Network security is a system

Layers of security are required

Security Integrated "EVERYWHERE"

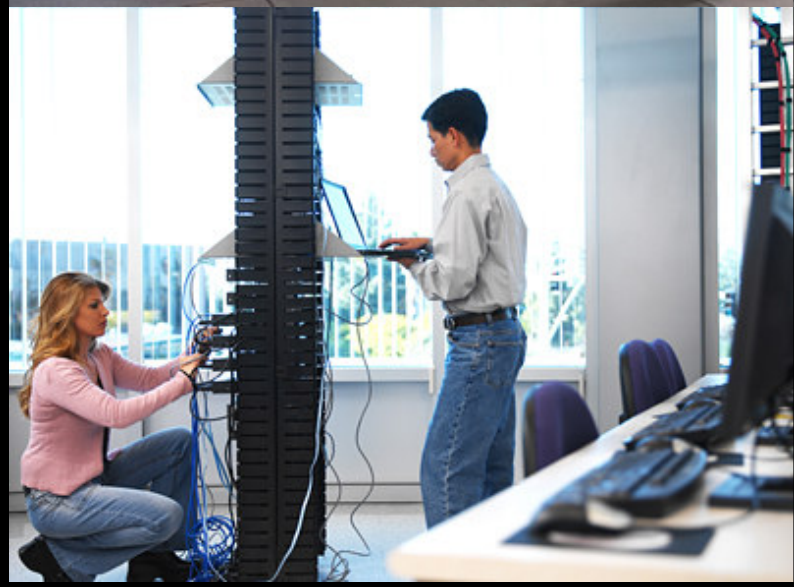
Secure management and reporting

- Routers are targets
- Switches are targets
- Hosts are targets
- Networks are targets
- Applications are targets
- Information is a target
- Management tools are targets

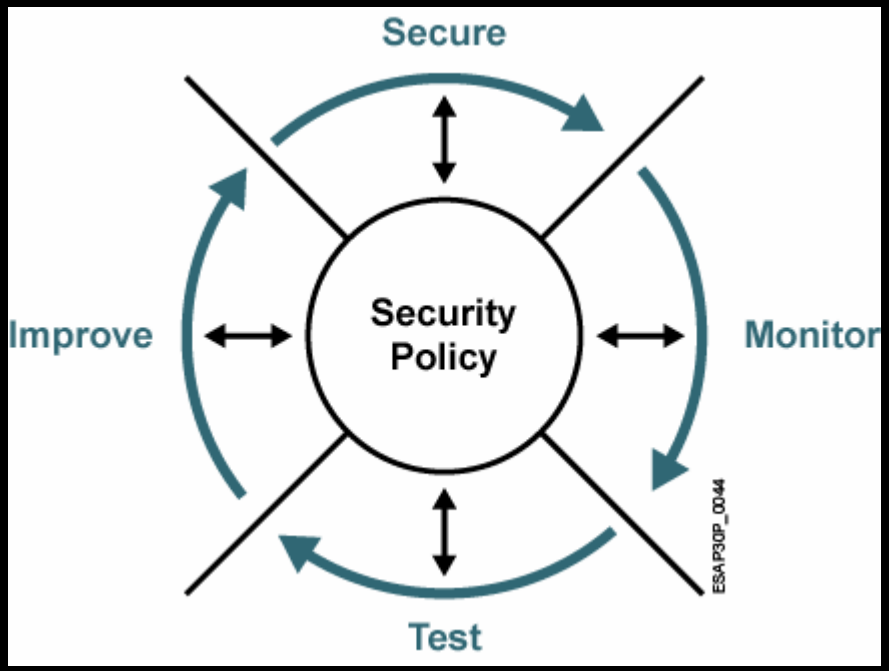


Strive for Operational Simplicity

- Security design and network operation are tight together
- Security operations have two sides: normal operations and under attack behavior.
- When designing security overall organization processes must be considered
- Operational simplicity can help reduce time to resolution



The Process of Security



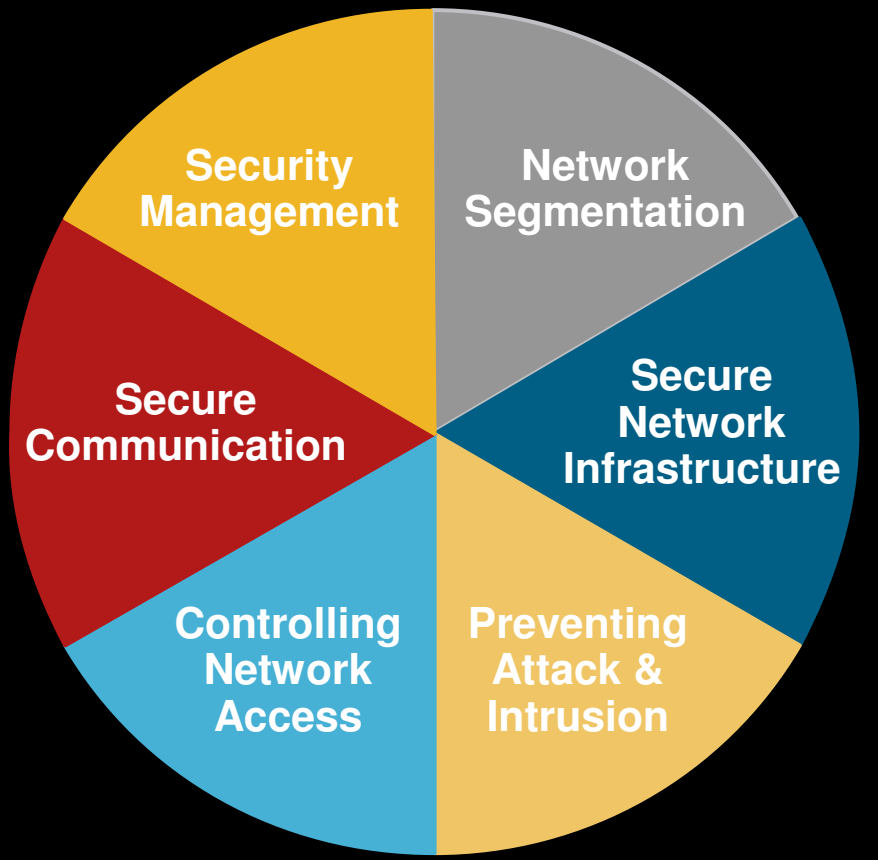
- The security wheel is a metaphor for security, done as a dynamic process:
  - The security policy influences all other process components

1. Threat Identification
2. Risk Assessment
3. Loss Expectancy
4. Risk Management
5. Policy Implementation
6. Incident Handling

Security
“Areas of Focus”

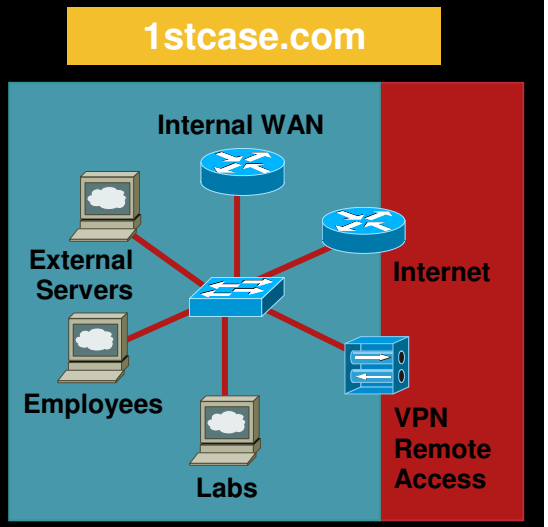
Security "Areas of Focus"

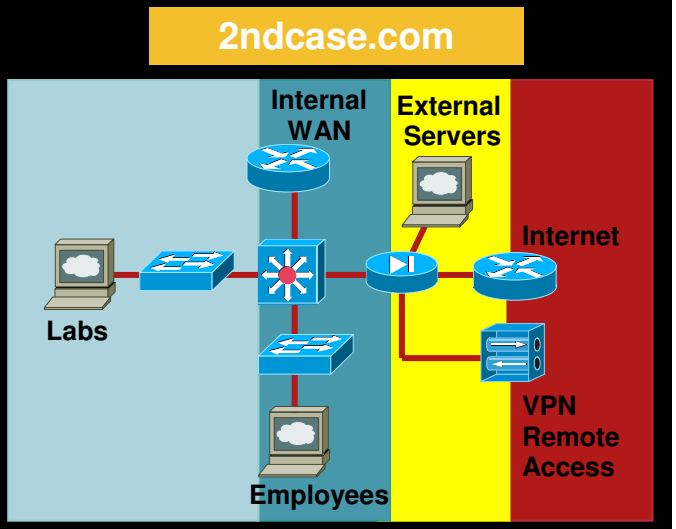
- Can all be applied to the endpoint, application, or network
- Provides focused way of addressing the required security criteria
- Helps to better understand the various technologies and how to best leverage them



Network Segmentation

- **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
- **However the strict separation of the old days is fading away with ubiquitous network access**





Secure network infrastructure

- The measures taken to preserve the integrity and availability of the network infrastructure as a transport and service entity
- Goals:
  - That the network devices are not accessed or altered in an unauthorized manner
  - That the end-to-end network transport and any integrated services remain available
- Policy enforcement technologies can help preserve:
  - Directly: the integrity and availability of the network

Secure network infrastructure Technologies

- Control Plane Policing (CoPP)
- Infrastructure ACLs
- Anti-spoofing
  - RFC2827
  - uRPF
  - Dynamic ARP inspection
  - DHCP snooping
  - Port Security
- Layer 2
  - BPDU guard/root guard
  - VLAN Usage BCPs
  - VTP MD5 authentication
- Layer 3
  - Filtering of malicious traffic
- Routing Protocol Security
  - Autentication of routing protocol
  - Prefix filtering
- Management Channel Security
  - InBand, Out-Of-Band
  - SSH, HTTPS, SSL, SCP, SNMPv3

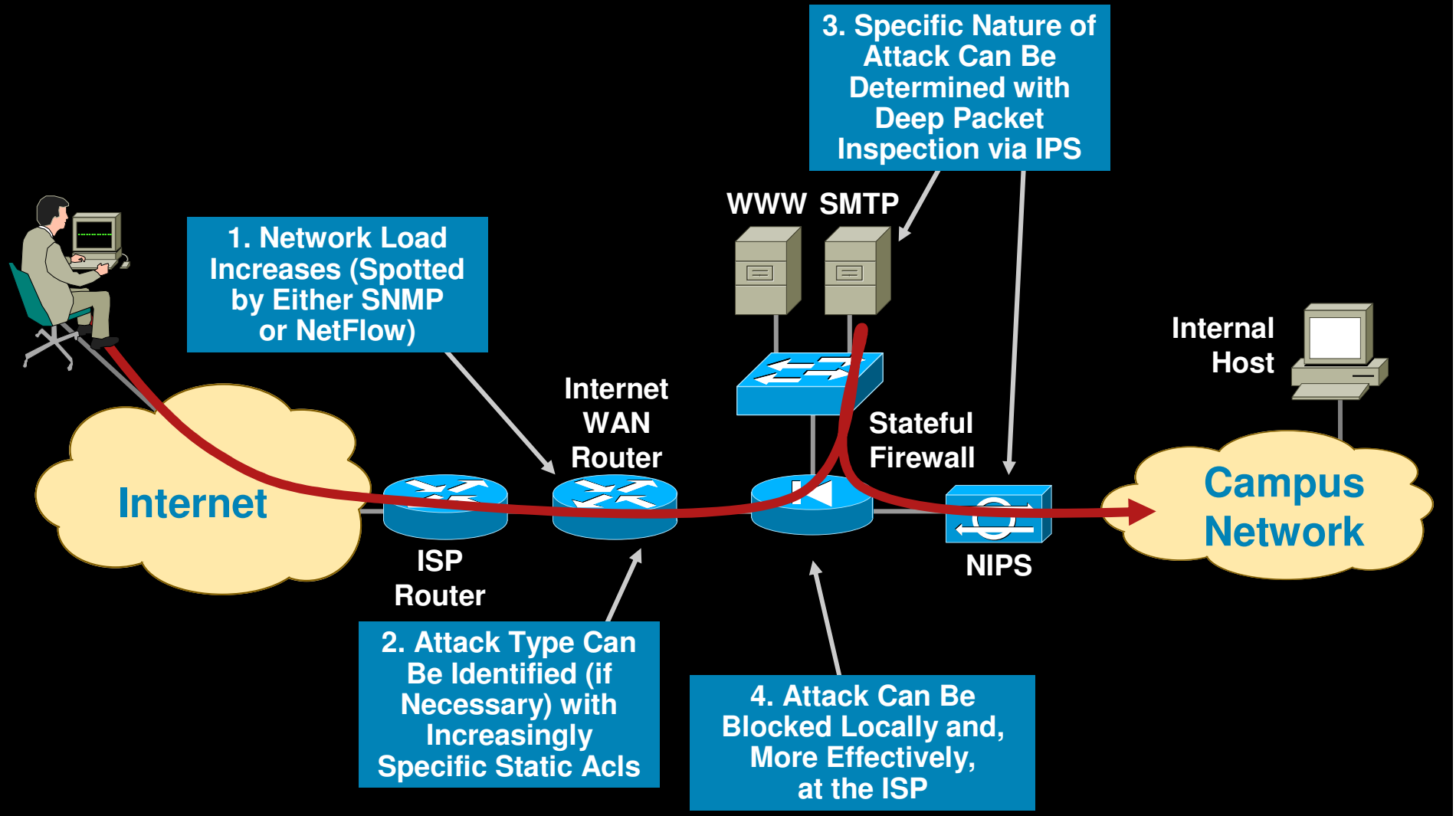
Preventing Attack & Intrusion

- The technologies that can be used to provide early warning detection and notification of unpredicted malicious traffic or behavior
- Goals:
  - To detect, notify, and help stop events or traffic that are unauthorized and unpredictable
  - To help reduce the time to execute the Security Wheel
- Threat control and containment technologies can help preserve:
  - Directly: the availability of the network—particularly against unknown or unforeseen attacks

Preventing Attack & Intrusion

- Network-based Intrusion Prevention Systems (NIPS)
  - Adaptive Security Appliance (ASA)
  - IPS
  - Cisco IOS IPS
- Host-based Intrusion Prevention Systems (HIPS)
  - Cisco Security Agent (CSA)
- NetFlow
- Remote-trigger blackholes
- Sinkhole routing
- Syslog
- Event correlation systems
  - Monitoring, Analysis, and Response System (MARS)
- Anomaly detector module
- Anomaly guard module
- SNMP traps
- RMON
- Packet capture

Worm Attack Detection and Isolation



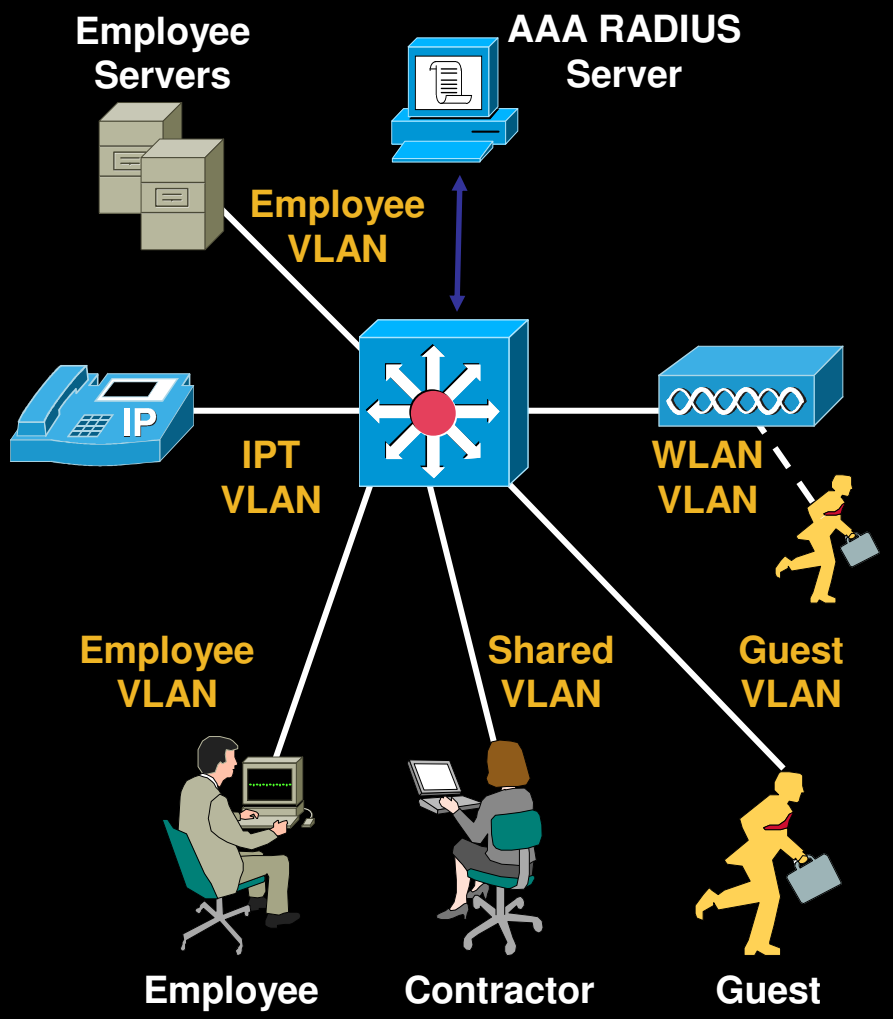
Controlling Network Access

- The measures taken to preserve the trusted nature of a given domain
- Used to assure:
  - Someone/something is allowed to be there in the first place
  - That same someone/something is limited to doing what they should be doing
- Good access control usage enables two main things:
  - Effective risk mitigation
  - The ability to apply policy and access control in a more granular and accurate manner
- Identity and access control technologies help preserve:
  - Directly: the integrity of the asset
  - Indirectly: the confidentiality and availability of an asset

Controlling Network Access (cont.)

AAA (Authentication, Authorization, Accounting)

- AAA at L2 ports
  - Authenticate asset (cert) and/or user
  - Authorization via dynamic VLANs or PACLs
  - Accounting for audit trail and forensics
- Segmentation techniques
  - Guest VLANs
  - Dynamic VLANs
- Firewalls (stateful and application)
- Access lists



Controlling Network Access (cont.)

NAC (Network Admision Control)

Using the network to enforce policies ensures that incoming devices are compliant.

Authenticate & Authorize

- Enforces authorization policies and privileges
- Supports multiple user roles

Scan & Evaluate

- Agent scan for required versions of hotfixes, AV, etc
- Network scan for virus and worm infections and port vulnerabilities

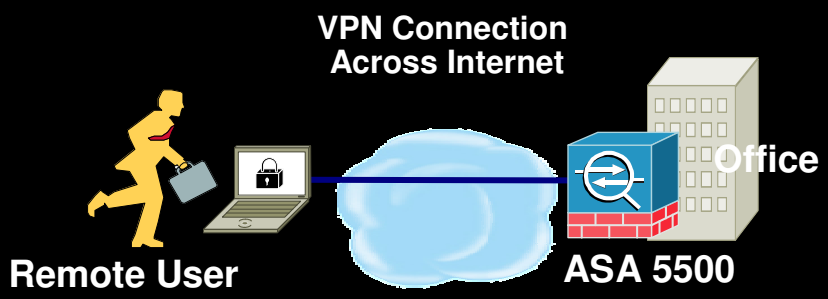
Quarantine & Enforce

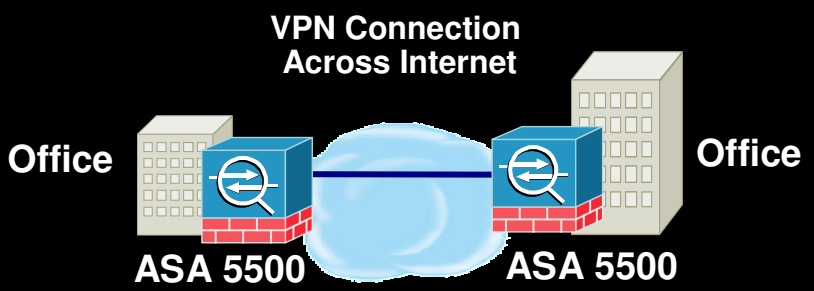
- Isolate non-compliant devices from rest of network
- MAC and IP-based quarantine effective at a per-user level

Update & Remediate

- Network-based tools for vulnerability and threat remediation
- Help-desk integration

Secure Communication





Remote Access VPN

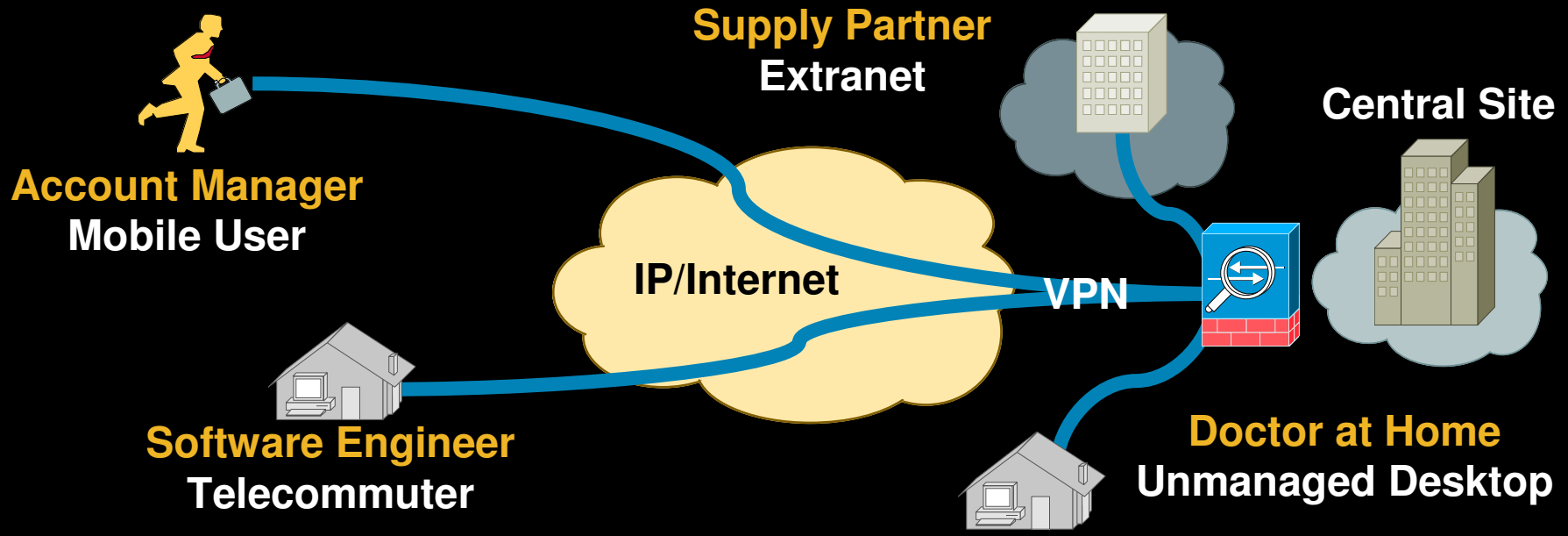
- Improve productivity by extending network resources to employees at home or on the road
- Business resiliency – enabling network access in the event of a disaster
- Decrease costs relative to older access technologies

Site-to-Site VPN

- Decrease WAN costs while increasing bandwidth relative to older WAN technologies
- Enabling more flexibility and control over WAN provisioning by using Internet connectivity

Secure Communication

Remote Access - Deployment example



Clientless (L7) SSL Clientless/Thin Client SSL VPN	IPsec Full Network Access (L3) VPN Client
▪ Partner—Few apps/servers, tight access control, no control over desktop software environment, firewall traversal ▪ Doctor—Occasional access, few apps, no desktop software control	▪ Engineer—Many servers/apps, needs native app formats, VoIP, frequent access, long connect times ▪ Account Manager—Diverse apps, home-grown apps, always works from enterprise-managed desktop

Security Management

- Provides eyes, ears, and fingers into the network
- Biggest risk to security in a properly planned architecture is policy error
- Security implementation is only as good as policies provisioned
- Security management does the following:
  - Collects, analyzes, and presents data
  - Allows structured provisioning of policies on security devices
  - Maintains consistency and change control of policies
  - Provides roles-based access control and accounts for all user activity

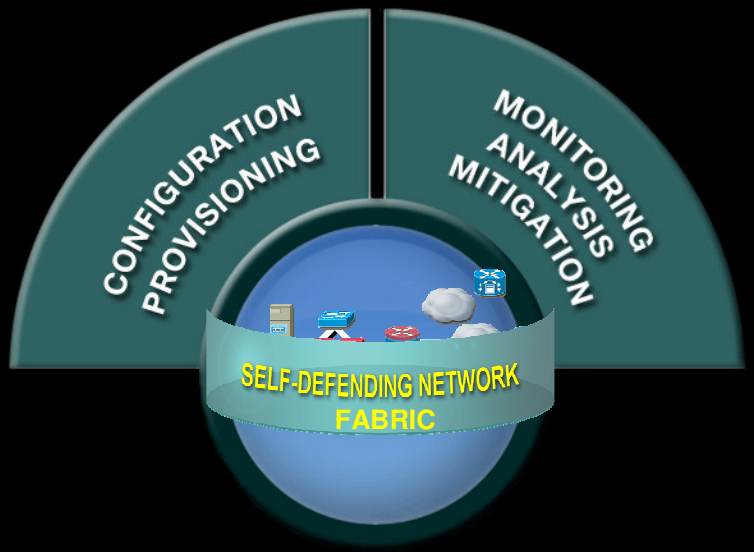
Security Management

Cisco® Security Manager

Simplified Policy Administration

End-to-End Configuration

Network wide or Device Specific



Cisco® Security Mars

Network-intelligent correlation

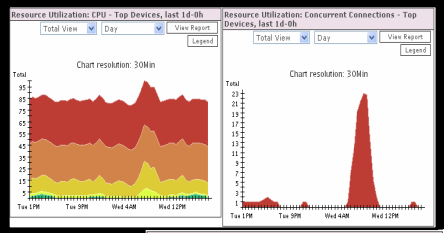
Incident validation

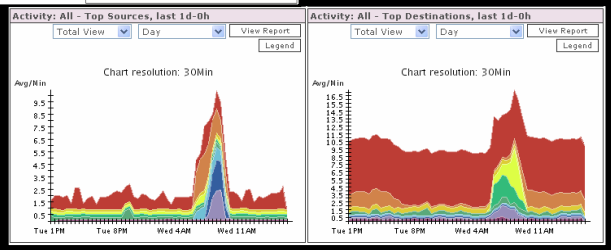
Attack visualization

Automated investigation

Leveraged mitigation

Compliance management





Q and A