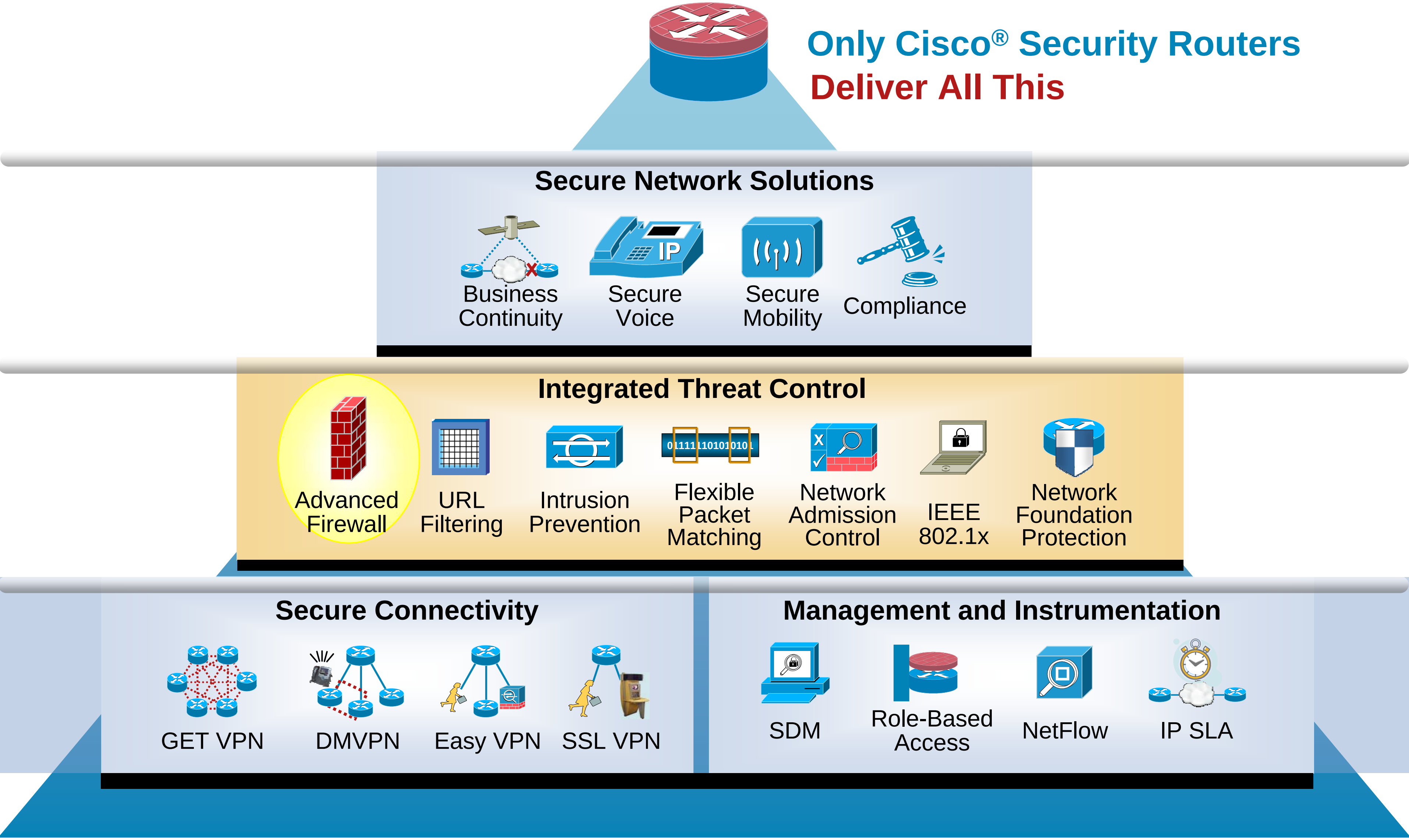
Cisco IOS® Advanced Firewall

Integrated Threat Control for Router Security Solutions

http://www.cisco.com/go/iosfirewall

All-in-One Security for the WAN



Only Cisco® Security Routers
Deliver All This

Secure Network Solutions

Business Continuity

Secure Voice

Secure Mobility

Compliance

Integrated Threat Control

Advanced Firewall

URL Filtering

Intrusion Prevention

Flexible Packet Matching

Network Admission Control

IEEE 802.1x

Network Foundation Protection

Secure Connectivity

GET VPN

DMVPN

Easy VPN

SSL VPN

Management and Instrumentation

SDM

Role-Based Access

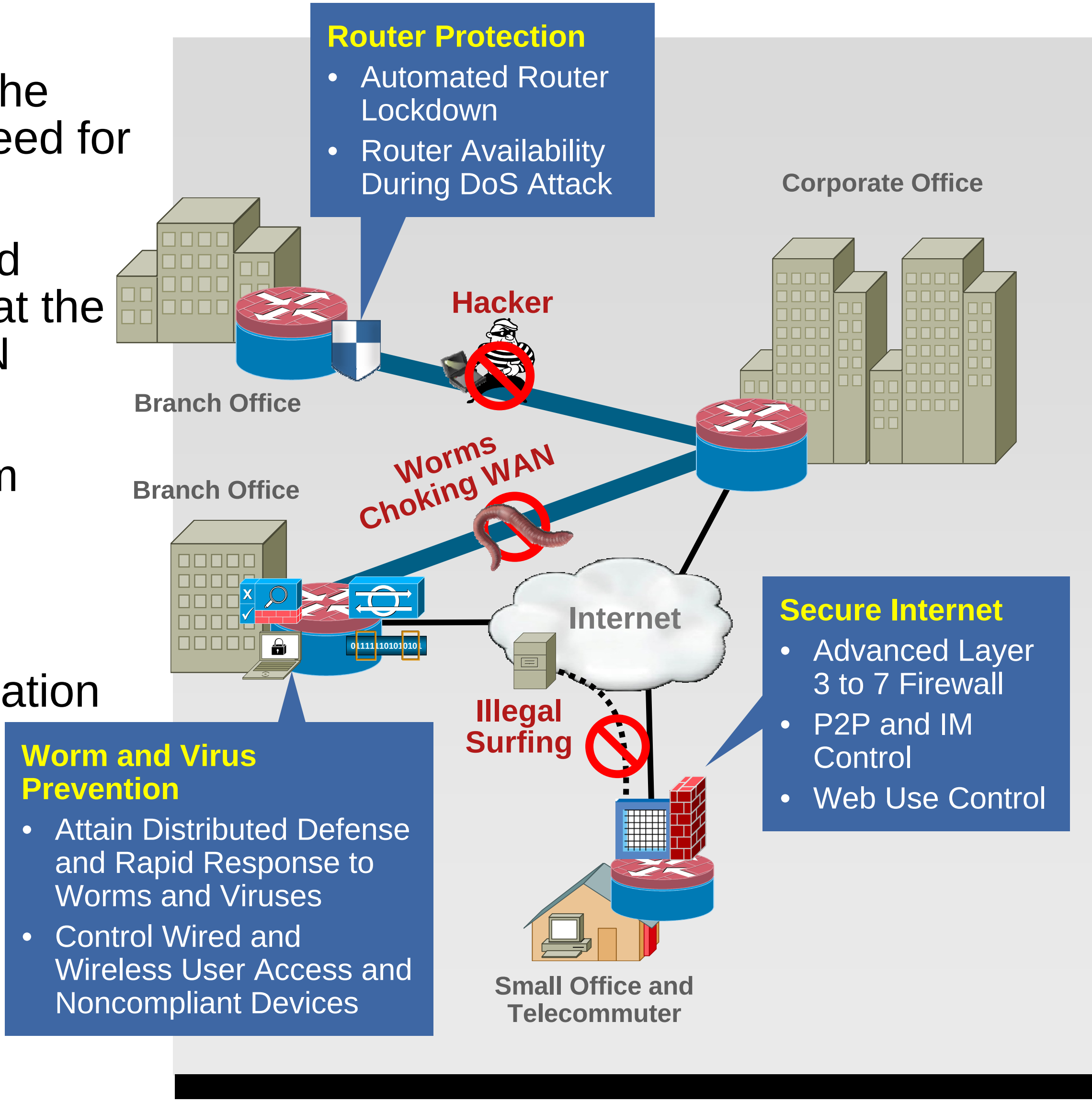
NetFlow

IP SLA

Integrated Threat Control Overview

Industry-Certified Security Embedded Within the Network

- Secure Internet access to the branch office without the need for additional devices
- Control worms, viruses, and adware and spyware right at the remote site; conserve WAN bandwidth
- Protect the router itself from hacking and DoS attacks
- Protect data, voice and video, wired and wireless, and WAN acceleration services



Router Protection

- Automated Router Lockdown
- Router Availability During DoS Attack

Worm and Virus Prevention

- Attain Distributed Defense and Rapid Response to Worms and Viruses
- Control Wired and Wireless User Access and Noncompliant Devices

Secure Internet

- Advanced Layer 3 to 7 Firewall
- P2P and IM Control
- Web Use Control

Cisco IOS® Firewall

Benefits

- Integrated perimeter and branch defense using proven Cisco® IOS Software routing, quality-of-service (QoS), voice, and wireless technologies
- Low total cost of ownership (TCO) through integration of firewall, IPS, and other security features on a popular networking platform
- Protection against network and application layer exploits and threats such as denial-of-service (DoS) attacks
- Compliance with requirements such as PCI, Sarbanes-Oxley, and HIPAA
- Ease of management and deployment
- Numerous WAN interface and density options on Cisco routers
- Green technology—reduced power consumption and footprint because the existing router is used

Cisco IOS® Firewall
Overview

Stateful firewall: Full Layer 3 through 7 deep packet inspection

Flexible embedded application layer gateway (ALG): Dynamic protocol and application engines for seamless granular control

Application inspection and control: Visibility into both control and data channels to help ensure protocol and application conformance

Virtual firewall: Separation between virtual contexts, addressing overlapping IP addresses

Intuitive GUI management: Easy policy setup and refinement with SDM and CSM

Resiliency: High availability for users and applications with stateful firewall failover

WAN interfaces: Most WAN and LAN interfaces

Selected List of Recognized Protocols

- HTTP, HTTPS, and JAVA
- E-mail: POP, SMTP, IMAP, and Lotus
- P2P and IM (AIM, MSN, and Yahoo!)
- FTP, TFTP, and Telnet
- Voice: H.323, SIP, and SCCP
- Database: Oracle, SQL, and MYSQL
- Citrix: ICA and CitrixImaClient
- Multimedia: Apple and RealAudio
- IPSec VPN: GDOI and ISAKMP
- Microsoft: MSSQL and NetBIOS
- Tunneling: L2TP and PPTP

Common Criteria

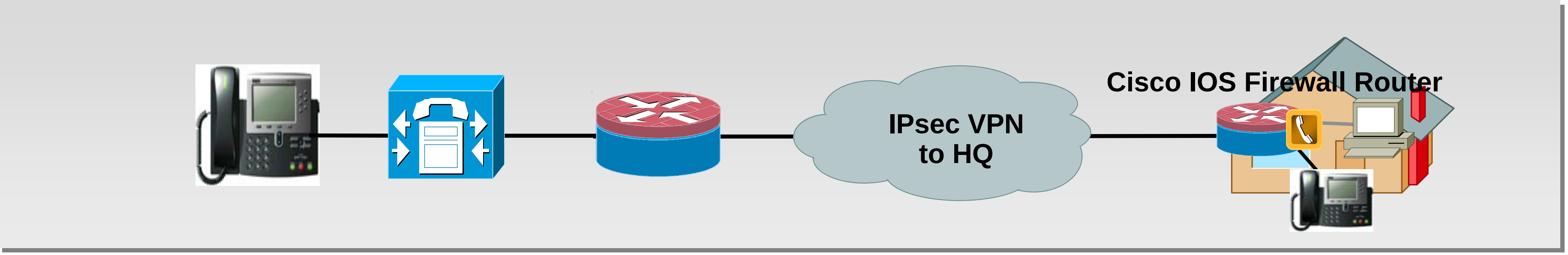
PCI Security Standards Council™

SIP Protection for Secure Unified Communications

Enhance the Integrity and Availability of Cisco® Unified Communications

Session Initiation Protocol (SIP) (RFC 3261) inspection and granular access control for voice-over-IP (VoIP) traffic across branch networks

- Prevent unauthorized calls, call hijacking, any SIP protocol exploits, and related DoS attacks
- Remove malformed packets from reaching Cisco Unified Communications Manager at the head office
- Maintain high availability of mission-critical IP telephony calls while upholding high level of call experience



Cisco IOS® Firewall:
Common Deployments Scenarios

- **Split tunnel:** Remote branch, retail store, and clinic

  Division between VPN traffic to the LAN and direct public network connection for Internet traffic

- **Virtual firewall:**

  Retail chains

  Firewall between virtual contexts (VRFs) and to the WAN

  Segregation of networks for photo and pharmacy with overlapping IP addresses

  Internet for partners: Co-location

  WAN connection sharing between business partners

  Bank ATMs at retail store locations

- **Direct Internet connection:** Small office and managed firewall

- **Internal firewall:** International financial branches

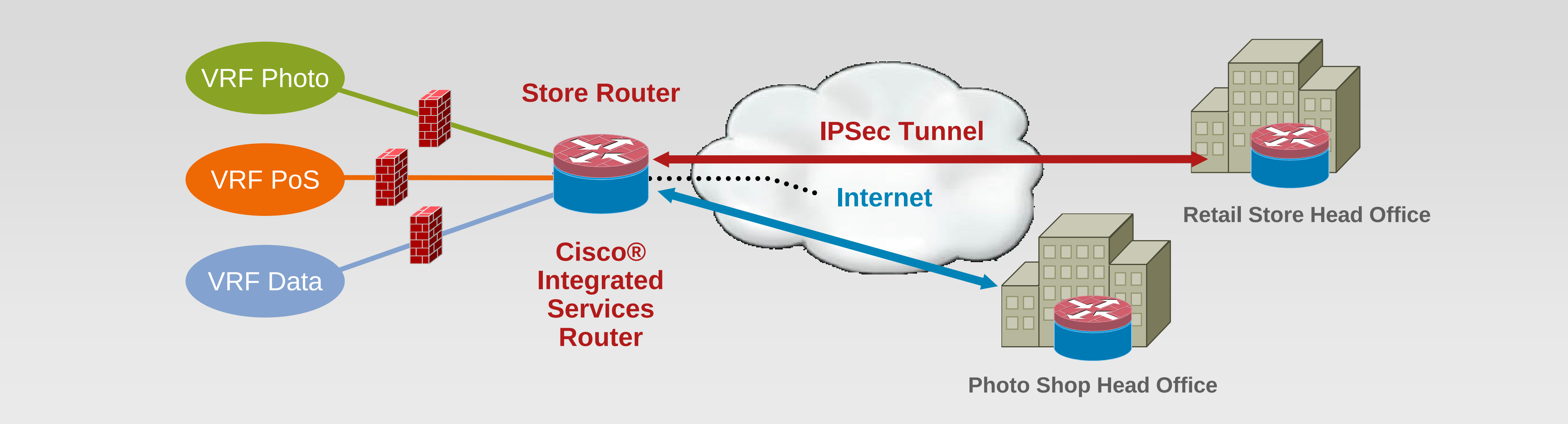
  Between international or untrusted locations or segments, often for compliance requirements

  Transparent or routed environments

  Wireless to wired segments

Cisco IOS® Firewall Deployment

Case Study: National Retailer



- Photo kiosk a potential security threat at the store—media card slots
- Support needed for overlapping address space
  - Multiple partners co-located at the store
- Direct Internet access needed for partners
- PCI compliance requires retail stores to firewall wired and wireless and Packet-over-SONET (PoS) segments
  - Inter-VRF routing + firewall may be enabled for wired VPN Routing and Forwarding (VRF) and wireless VRF
  - Cisco has its retail design guide certified through a third party (CyberTrust)

PCI Security Standards Council™

Cisco® Security Router Certifications

Routers	FIPS	Common Criteria	
	140-2, Level 2	IPSec (EAL4)	Firewall (EAL4)
Cisco 870 Series	✓	In progress	✓
Cisco 1800 Series	✓	In progress	✓
Cisco 2800 Series	✓	In progress	✓
Cisco 3800 Series	✓	In progress	✓
Cisco 7200 Series VAM2+	✓	In progress	✓
Cisco 7200 Series VSA	✓	In progress	---
Cisco 7301 VAM2+	✓	In progress	✓
Cisco 7600 Series IPSec VPN SPA	✓	In progress	---
Cisco Catalyst® 6500 Series IPSec VPN SPA	✓	In progress	---
Cisco 7600 Series	✓	In progress	✓

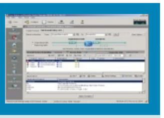
FIPS VALIDATED 140-2

Common Criteria®

cisco.com/go/securitycert

Management and Instrumentation Overview

Cisco® Security Device Manager

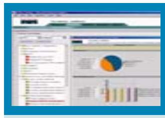


Quickest way to set up a device

Wizards to configure firewall, IPS, VPN, QoS, and wireless

Ships with device

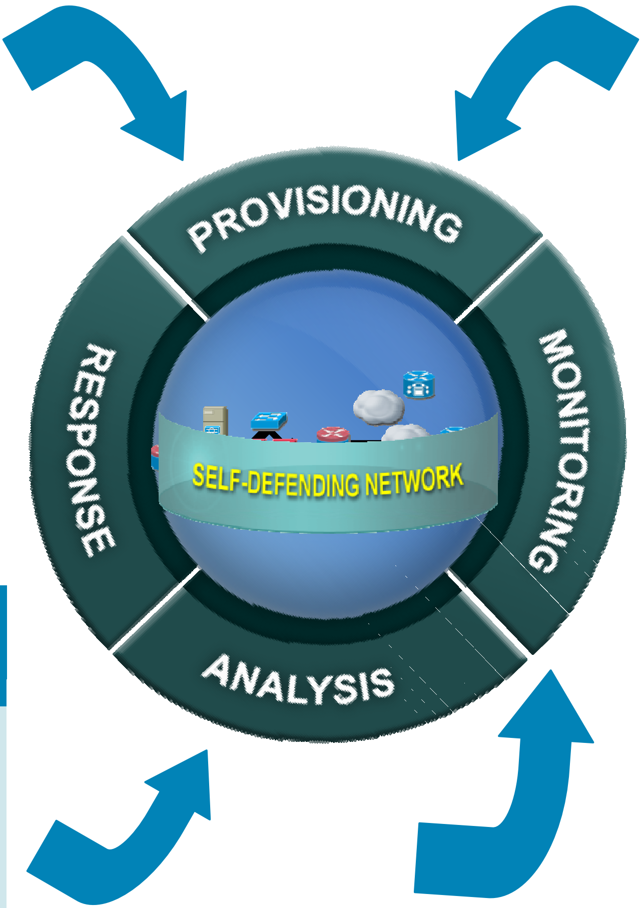
Cisco Security Manager



New solution for configuring routers, appliances, and switches

New user-centered design

New levels of scalability



Cisco Security Monitoring Analysis and Response System (MARS)

Solution for monitoring and mitigation

Uses control capabilities within infrastructure to eliminate attacks

Visualizes attack paths

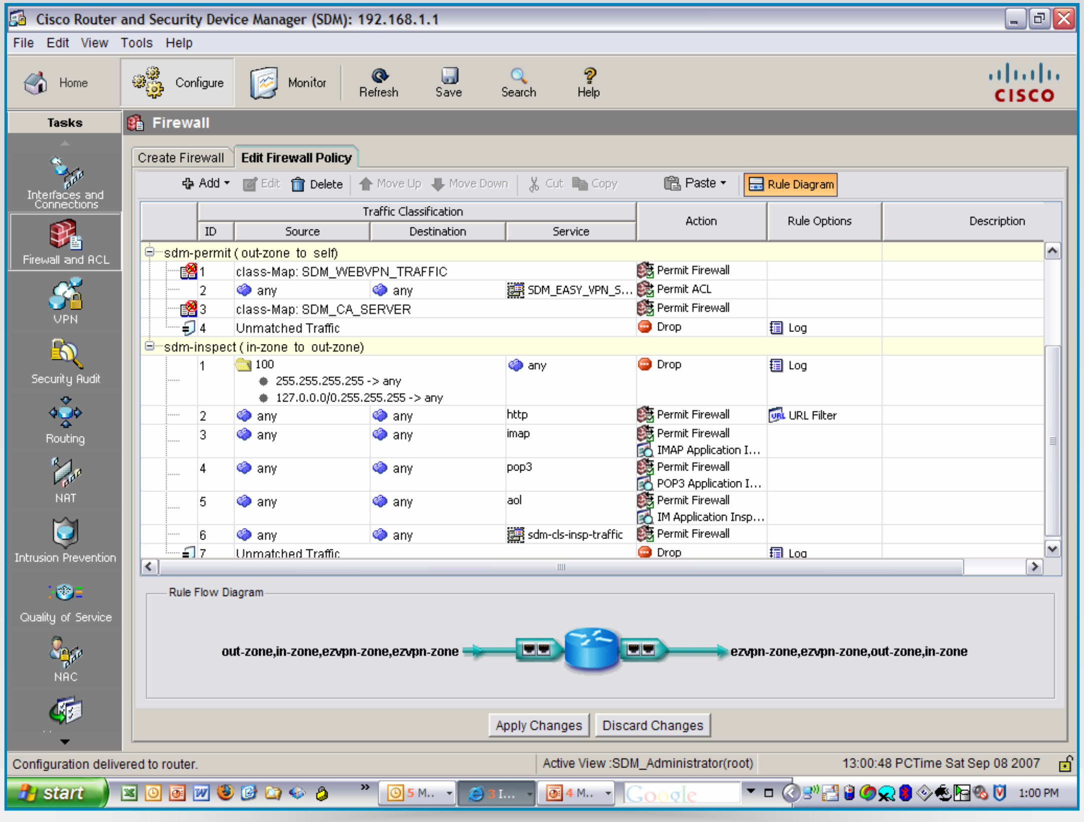
Cisco IOS® Instrumentation

Industry leadership in instrumentation

Feeds into Cisco Security MARS

Partitioned access for network and security operations teams

Cisco® Router and Security Device Manager (SDM)



	Traffic Classification				Action	Rule Options	Description
	ID	Source	Destination	Service			
sdm-permit (out-zone to self)							
	1	class-Map: SDM_WEBVPN_TRAFFIC			Permit Firewall		
	2	any	any	SDM_EASY_VPN_S...	Permit ACL		
	3	class-Map: SDM_CA_SERVER			Permit Firewall		
	4	Unmatched Traffic			Drop	Log	
sdm-inspect (in-zone to out-zone)							
	1	100 ● 255.255.255.255 -> any ● 127.0.0.0/0.255.255.255 -> any		any	Drop	Log	
	2	any	any	http	Permit Firewall	URL Filter	
	3	any	any	imap	Permit Firewall IMAP Application I...		
	4	any	any	pop3	Permit Firewall POP3 Application I...		
	5	any	any	aol	Permit Firewall IM Application Insp...		
	6	any	any	sdm-cls-insp-traffic	Permit Firewall		
	7	Unmatched Traffic			Drop	Log	

Rule Flow Diagram

out-zone,in-zone,ezvpn-zone,ezvpn-zone → ezvpn-zone,ezvpn-zone,out-zone,in-zone

Configuration delivered to router. Active View :SDM_Administrator(root) 13:00:48 PCTime Sat Sep 08 2007

- **Web-based device management tool** for Cisco routers that simplifies router deployments and helps troubleshoot complex network and VPN connectivity problems
- **Zone-based firewall** for granular policy control between virtual zones
- **Application control and URL filtering** unique on a per-rule basis

Cisco® Security Manager

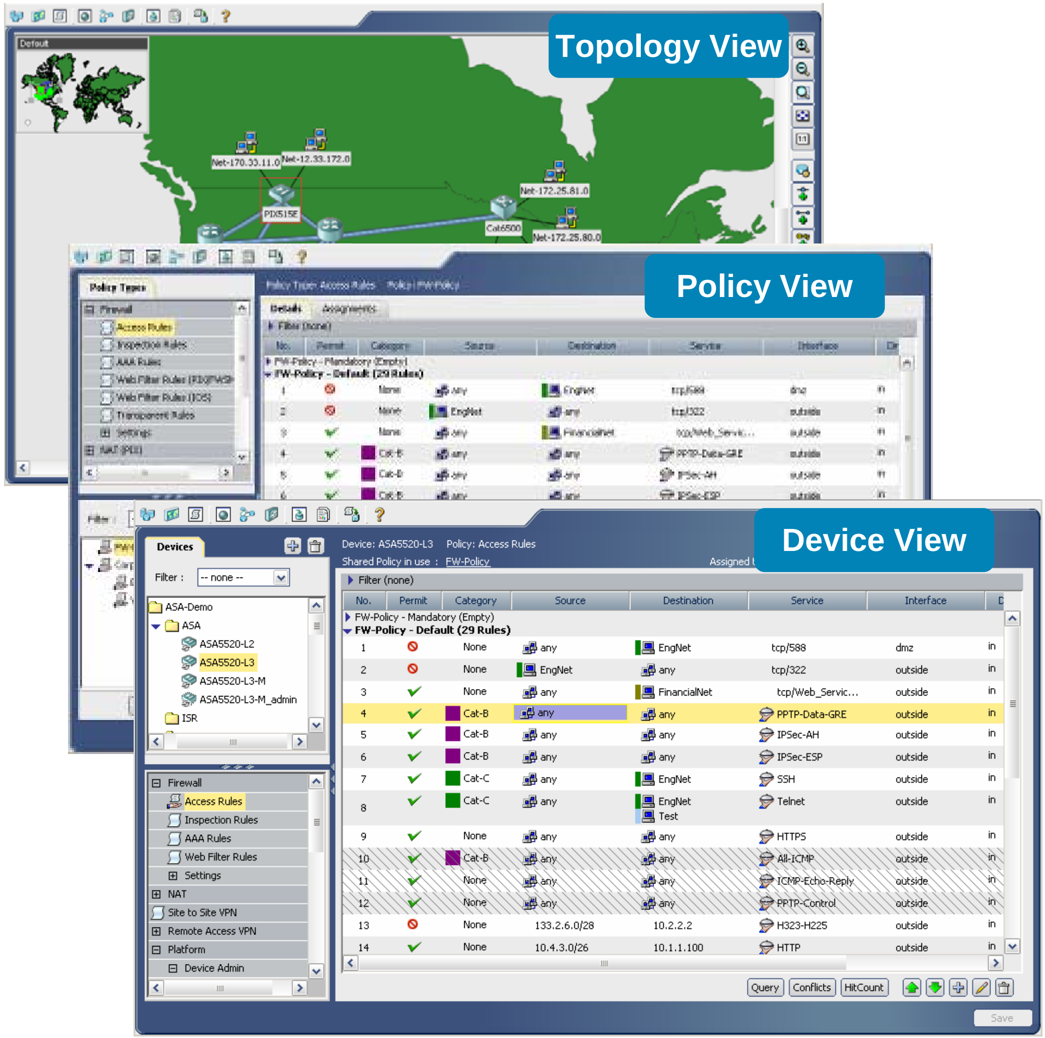
- State-of-the-art user interface
- Multiple views to suit administrator preferences

  Device, policy, and topology views

- Unified management of multiple security services

  Firewall, VPN, and intrusion prevention system (IPS)

- Supports Cisco Integrated Services Routers, ASA, PIX®, IPS Sensors, and Catalyst® Service Modules



Device: ASA5520-L3 Policy: Access Rules

Shared Policy in use : FW-Policy

Filter (none)

No.	Permit	Category	Source	Destination	Service	Interface	D
FW-Policy - Mandatory (Empty)							
FW-Policy - Default (29 Rules)							
1	⊘	None	any	EngNet	tcp/588	dmz	in
2	⊘	None	EngNet	any	tcp/322	outside	in
3	✓	None	any	FinancialNet	tcp/Web_Servic...	outside	in
4	✓	Cat-B	any	any	PPTP-Data-GRE	outside	in
5	✓	Cat-B	any	any	IPSec-AH	outside	in
6	✓	Cat-B	any	any	IPSec-ESP	outside	in
7	✓	Cat-C	any	EngNet	SSH	outside	in
8	✓	Cat-C	any	EngNet Test	Telnet	outside	in
9	✓	None	any	any	HTTPS	outside	in
10	✓	Cat-B	any	any	All-ICMP	outside	in
11	✓	None	any	any	ICMP-Echo-Reply	outside	in
12	✓	None	any	any	PPTP-Control	outside	in
13	⊘	None	133.2.6.0/28	10.2.2.2	H323-H225	outside	in
14	✓	None	10.4.3.0/26	10.1.1.100	HTTP	outside	in

Cisco® Security Monitoring, Analysis and Response System (MARS)

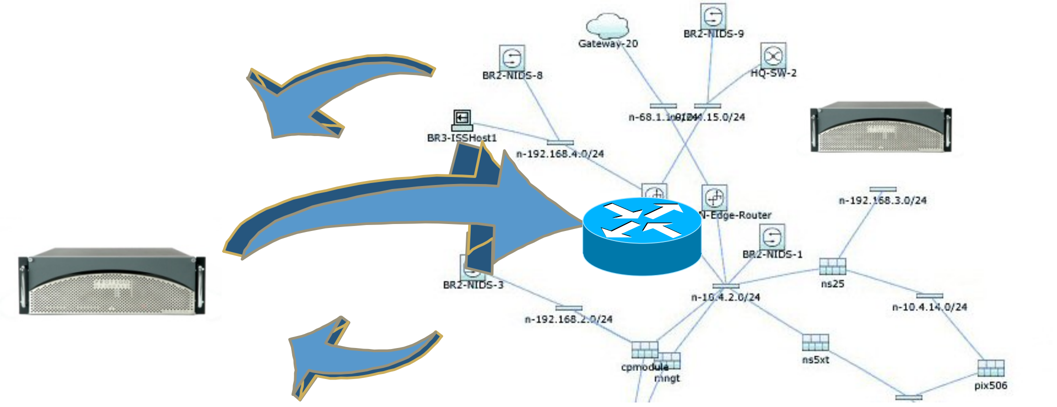
- Cisco Security MARS “Know the battlefield”: Mitigation and response turnkey system
- Gain network intelligence

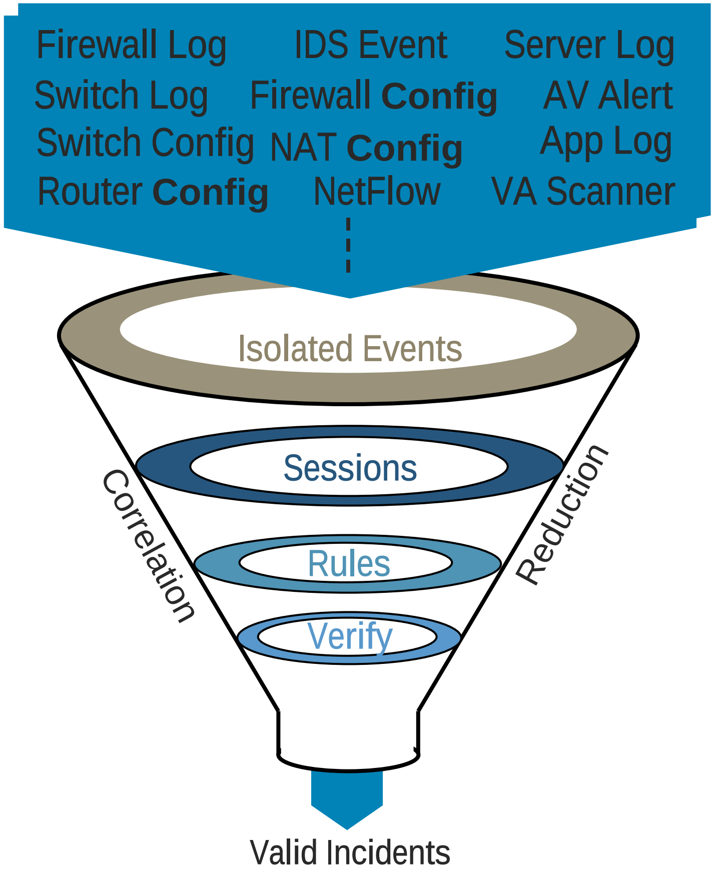
  Use the network you have; correlate router’s NetFlow (WAN data) with firewall, intrusion detection system (IDS), and switch data

  Build topology and traffic-flow model

  Know device configuration and enforcement abilities
- ContextCorrelation™

  Correlates, reduces, and categorizes events and validates incidents
- Allows for response





Firewall Log IDS Event Server Log

Switch Log Firewall **Config** AV Alert

Switch Config NAT **Config** App Log

Router **Config** NetFlow VA Scanner

Isolated Events

Sessions

Rules

Verify

Correlation

Reduction

Valid Incidents

Cisco Services and Support

Cisco and its partners provide a broad portfolio of security services that help you to:

- **Protect privacy and integrity of information**
- **Achieve and maintain regulatory compliance,**
- **Protect your network investment,**
- **Optimize network operations, and**
- **Extend the power of your business by preparing your network for new applications**

For more information, visit http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html .

Cisco IOS® Firewall

Summary

- Fundamental building block for defense-in-depth approach (Layers 3 to 7)
- Widely deployed fully stateful firewall
- Common criteria (EAL4) certified
- Low TCO
  - Use network investment to deploy firewall at the branches
  - Available as part of security bundles on Cisco Integrated Services Routers
- Critical for compliance conformity to PCI, Sarbanes-Oxley, and HIPAA