Dobro Jutro/ Dobar Dan! ☺

Security Update

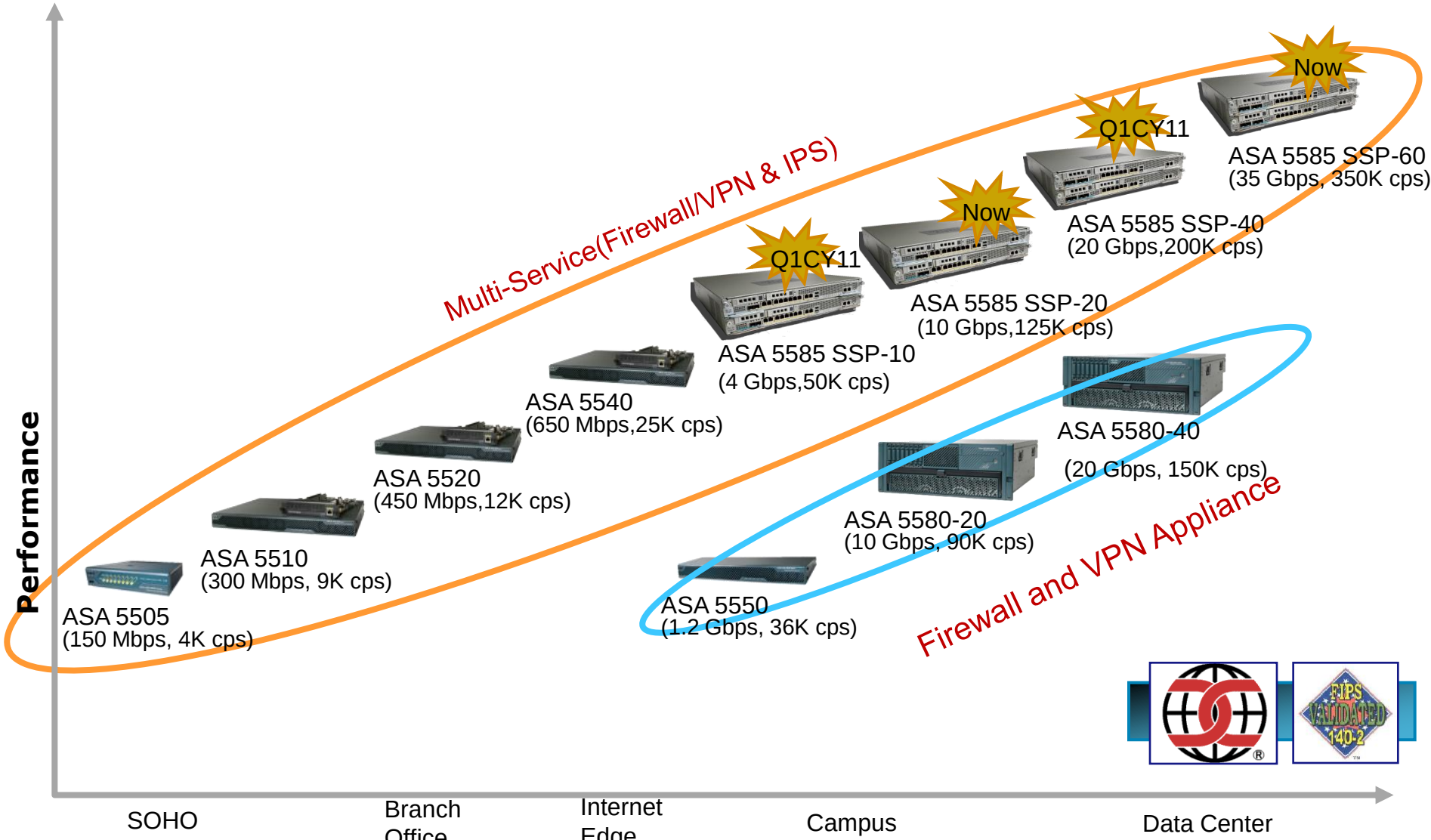
Tobias Mayer, Consulting Systems Engineer

Agenda

- ASA 5500 HW & Software v8.3
- AnyConnect & Secure Mobility
- Cisco Security Manager
- Cisco Email Security

Cisco ASA 5500 Series Portfolio

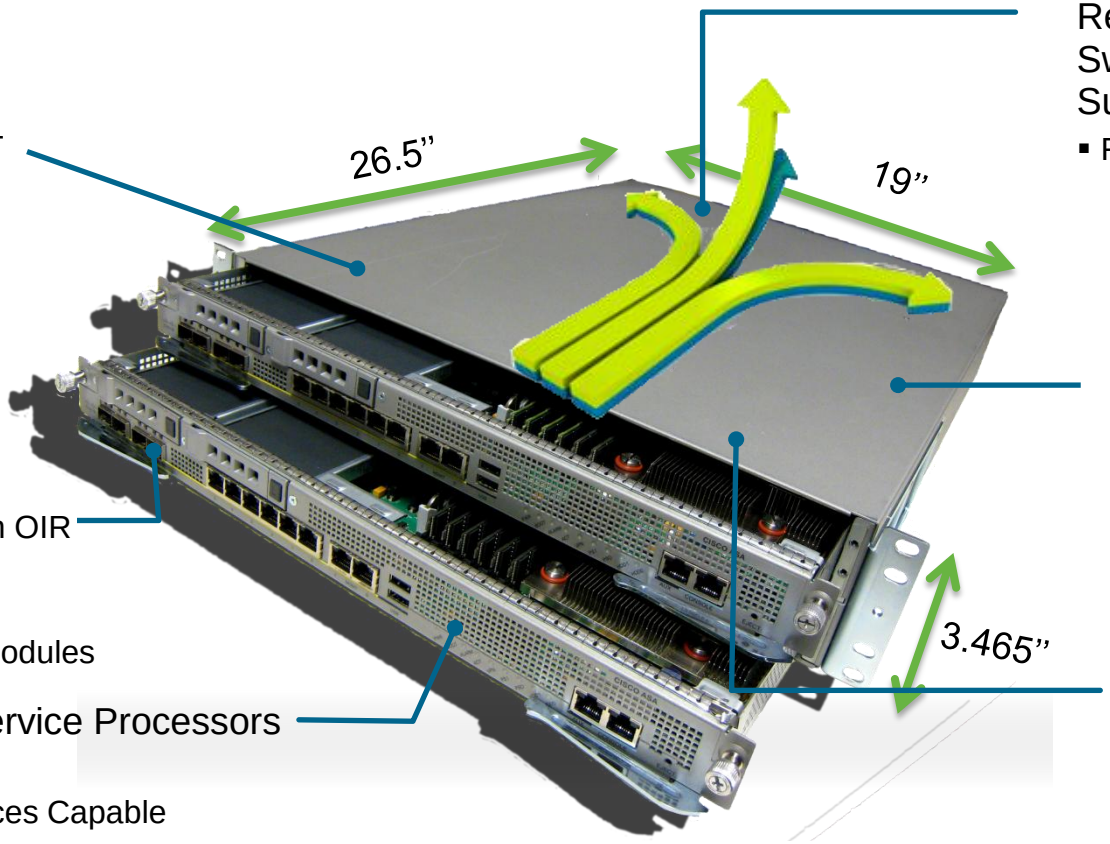
Comprehensive Solutions from SOHO to the Data Center



High Performance Multi-Service Cisco ASA 5585-X Series

Under the Covers

2 RU Chassis
- 2 x Full-Slot Modules
- 1 x Full-Slot + 2 x Half-Slot Modules
- OIR capable



Redundant Hot Swappable Power Supply Units
- Front to Back Air Flow

Multi Gigabit Fabric
- Passive Backplane
- Module to module communications
- Packet prioritization and shaping

GE Ports
- Up to 8 x 10G SFP+ with OIR support
- Up to 16 x 1GbE Cu
- SFP/SFP+ slots on all modules

Security Service Processors (SSP)
- Multi-Services Capable
- Dedicated 64bit Multi-Core Processors
- Future-Proof Hardware

eUSB
- 2 Gb Internal
- Convenience storage
- Security credentials

Cisco ASA 5585-X Series High-End Lineup Solutions

	ASA 5585-X SSP-10 IPS SSP-10	ASA 5585-X SSP-20 IPS SSP-20	ASA 5585-X SSP-40 IPS SSP-40	ASA 5585-X SSP-60 IPS SSP-60
Performance				
Max Firewall (Large Packet)	4 Gbps	10 Gbps	20 Gbps	35 Gbps
Max Firewall (Multi-Protocol)	2 Gbps	5 Gbps	10 Gbps	20 Gbps
Max IPS (Media Rich)	2 Gbps	3 Gbps	5 Gbps	10 Gbps
Max IPSec VPN	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Max IPSec/SSL VPN Peers	5000	10,000	10,000	10,000
Platform Capabilities				
Max Firewall Conns	750,000	1,000,000	2,000,000	2,000,000
Max Conns/Second	50,000	125,000	200,000	350,000 (2x)*
Packets/Second (64 byte)	1,000,000	3,000,000	5,000,000	9,00,000 (2x)*
Base I/O	8 GE + 2 10 GE	8 GE + 2 10 GE	6 GE + 4 10GE	6 GE + 4 10GE
Max I/O	16 GE + 4 10 GE	16 GE + 4 10 GE	12 GE + 8 10GE	12 GE + 8 10GE
VLANs Supported	250	250	250	250
HA Supported	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

Above benchmarks are subject to change.

Access Control

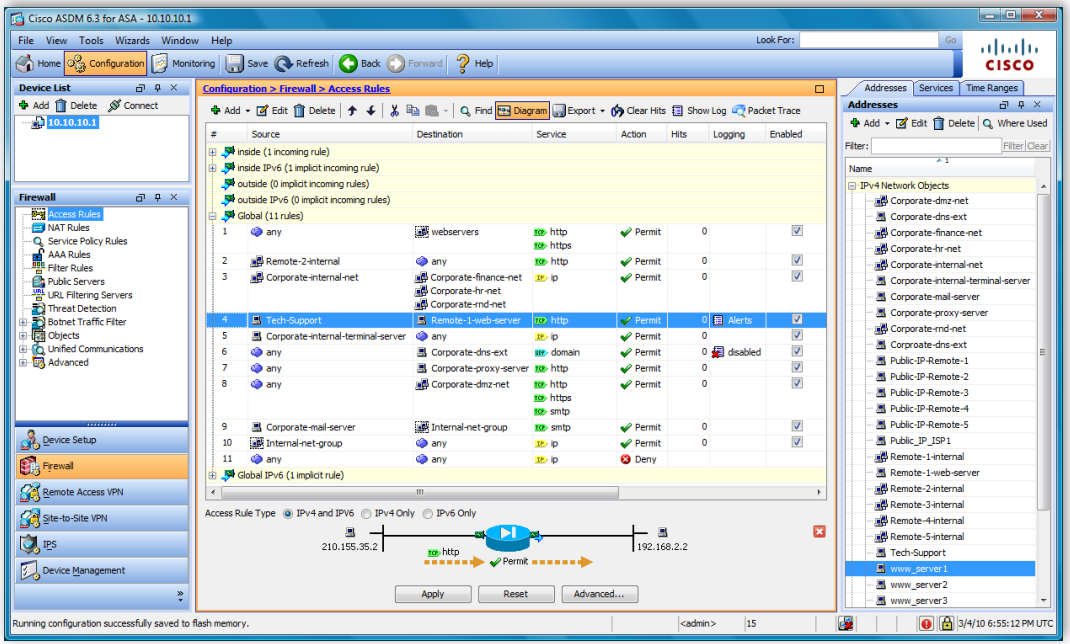
Granular Policy for Modern Networks

ASA scales to support hundreds of thousands of policies

Policies can be created Globally or on a per interface basis

Powerful Network Address Translation engine enables segmentation

ACL Real IP based (NAT)



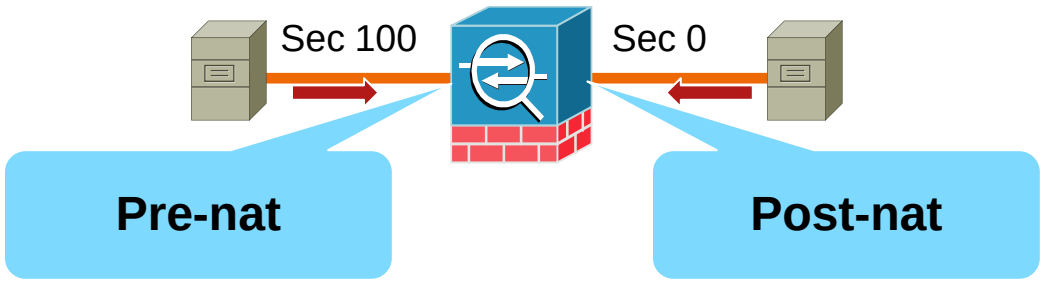
Real IP

- Prior to 8.3, access control policies are constructed such that it references the mapped (NAT'd) IP addresses when NAT is used for a particular host or network.

  Example:

  Pre-nat IP used if your are doing ingress filtering on higher security interface

  Post-nat IP used if you are doing ingress filtering on lower security interface



Presentation_ID

Cisco Confidential
7

Real IP

- In 8.3 you reference the real IP address, which is the address of the host or network before being translated.
- An object with the real IP address of a host, network or range and access control policies are constructed to reference the object pointing to the real IP address(es).
- Advantages:

  Not impacted by any change in NAT configuration

  Only single access list, If address is translated differently based on the interface or destination.

Example:

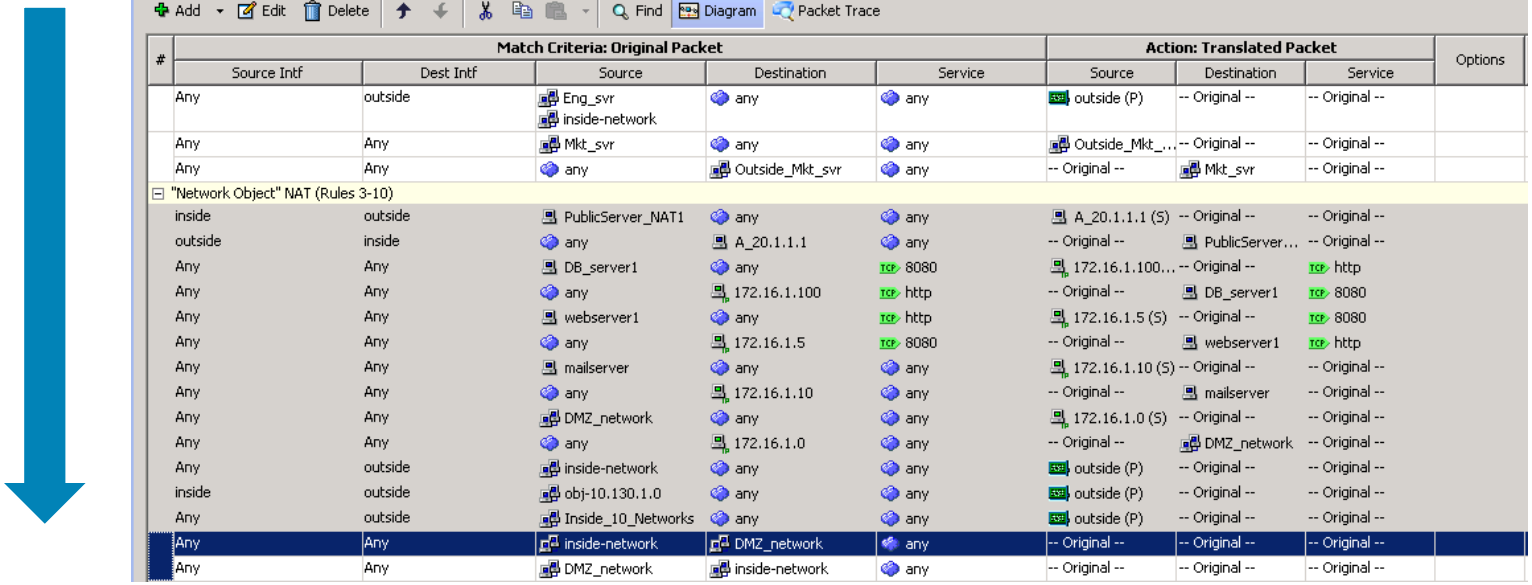
NAT: 192.168.1.100 (inside) -> 1.1.1.100 (outside)

Then the access-list would need to operate on the internal-real address (192.168.1.100) instead of before the outside-post-nat address (1.1.1.100)

Presentation_ID
© 2007 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

NAT Redesign
Unified NAT table

- NAT rules evaluation are applied on a top-down, first match basis.
- Once a particular NAT rule is matched, no further evaluation is done.
- Insert the most specific NAT rules above the broader NAT rules if there are NAT rules that overlap

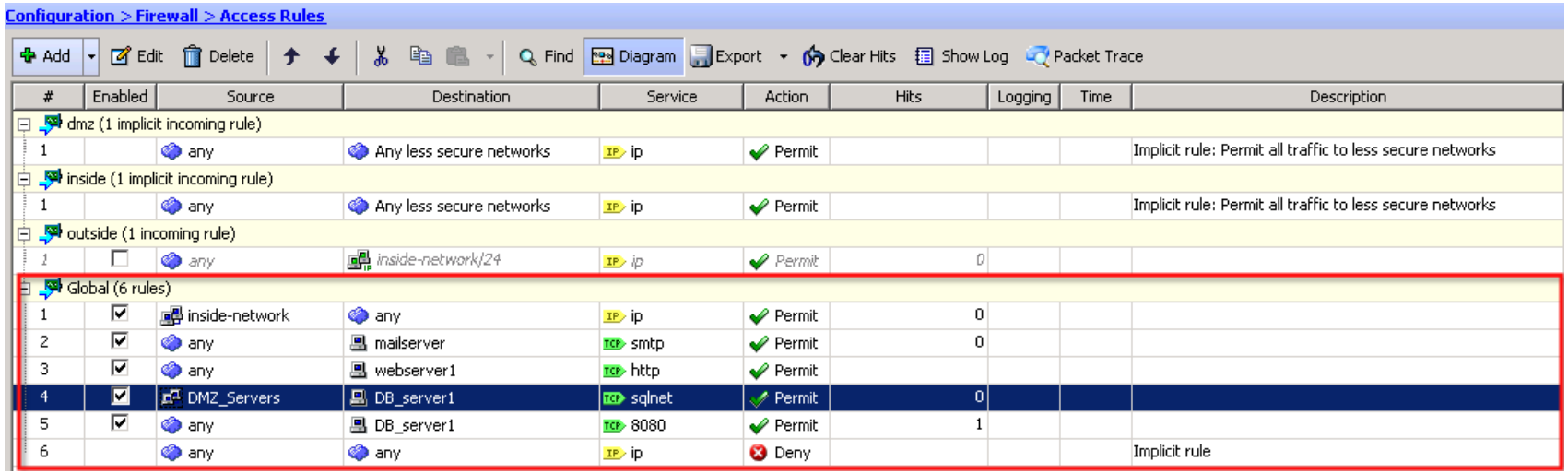


#	Match Criteria: Original Packet					Action: Translated Packet			Options
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	
	Any	outside	Eng_svr inside-network	any	any	outside (P)	-- Original --	-- Original --	
	Any	Any	Mkt_svr	any	any	Outside_Mkt_...	-- Original --	-- Original --	
	Any	Any	any	Outside_Mkt_svr	any	-- Original --	Mkt_svr	-- Original --	
	"Network Object" NAT (Rules 3-10)								
	inside	outside	PublicServer_NAT1	any	any	A_20.1.1.1 (S)	-- Original --	-- Original --	
	outside	inside	any	A_20.1.1.1	any	-- Original --	PublicServer...	-- Original --	
	Any	Any	DB_server1	any	8080	172.16.1.100...	-- Original --	http	
	Any	Any	any	172.16.1.100	http	-- Original --	DB_server1	8080	
	Any	Any	webserver1	any	http	172.16.1.5 (S)	-- Original --	8080	
	Any	Any	any	172.16.1.5	8080	-- Original --	webserver1	http	
	Any	Any	mailserver	any	any	172.16.1.10 (S)	-- Original --	-- Original --	
	Any	Any	any	172.16.1.10	any	-- Original --	mailserver	-- Original --	
	Any	Any	DMZ_network	any	any	172.16.1.0 (S)	-- Original --	-- Original --	
	Any	Any	any	172.16.1.0	any	-- Original --	DMZ_network	-- Original --	
	Any	outside	inside-network	any	any	outside (P)	-- Original --	-- Original --	
	inside	outside	obj-10.130.1.0	any	any	outside (P)	-- Original --	-- Original --	
	Any	outside	Inside_10_Networks	any	any	outside (P)	-- Original --	-- Original --	
	Any	Any	inside-network	DMZ_network	any	-- Original --	-- Original --	-- Original --	
	Any	Any	DMZ_network	inside-network	any	-- Original --	-- Original --	-- Original --	

Presentation_ID
© 2007 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Global Access Policies

- Global access control policies (ACLs)
- Independent of interfaces
- Global access control applied in inbound direction of all interfaces
- Allow user to specify access control based on source and destination addresses regardless of interface.
- Increased readability of security policy



#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
dmz (1 implicit incoming rule)									
1		any	Any less secure networks	ip	Permit				Implicit rule: Permit all traffic to less secure networks
inside (1 implicit incoming rule)									
1		any	Any less secure networks	ip	Permit				Implicit rule: Permit all traffic to less secure networks
outside (1 incoming rule)									
1	☐	any	inside-network/24	ip	Permit	0			
Global (6 rules)									
1	☑	inside-network	any	ip	Permit	0			
2	☑	any	mailserver	smtp	Permit	0			
3	☑	any	webserver1	http	Permit				
4	☑	DMZ_Servers	DB_server1	sqlnet	Permit	0			
5	☑	any	DB_server1	8080	Permit	1			
6		any	any	ip	Deny				Implicit rule

Presentation_ID
© 2007 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Access Policies Order of Operation

- Interface specific rule (ACL) takes precedence when used together with Global ACLs.
- Access control policies are processed
  - Top-down
  - First match
- Presence of Global rule table removes implicit “deny traffic” from interface ACLs
- Traffic falls through to Global rule table for evaluation if no interface match was found

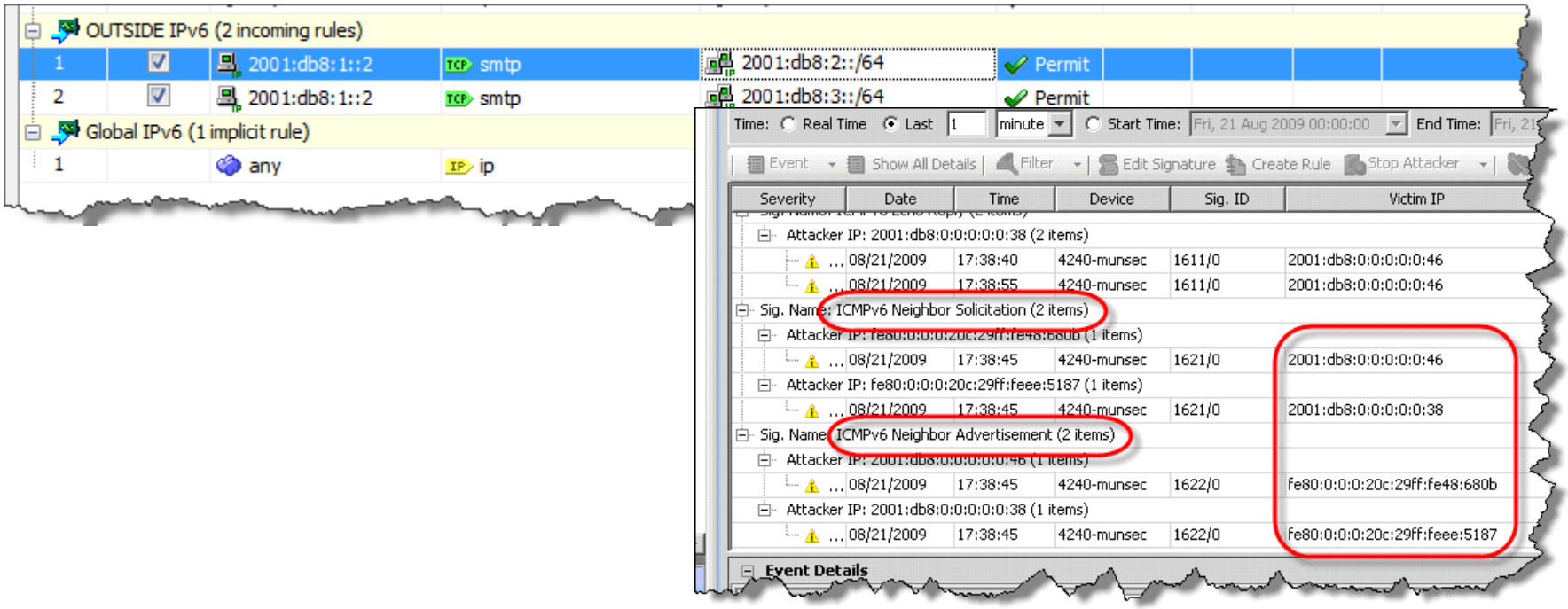
Presentation_ID
© 2007 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Demo

ASA 8.3 Global Rules & NAT

IPv6 Support

- ASA can use IPv6 in Access Rules
- ASA supports IPv6 in failover mode
- IPS Module in ASA can Inspect IPv6 Traffic, natively and tunneled traffic



Cisco Security Intelligence Operations

Global Threat Telemetry

Cisco® Threat Operations Center

Global Threat Telemetry

Cisco Security Services

Corporate Headquarters

Data Center

Branch Office

Coffee Shop

Security in Every Location

Security in Every Form Factor

Appliance

Security Module

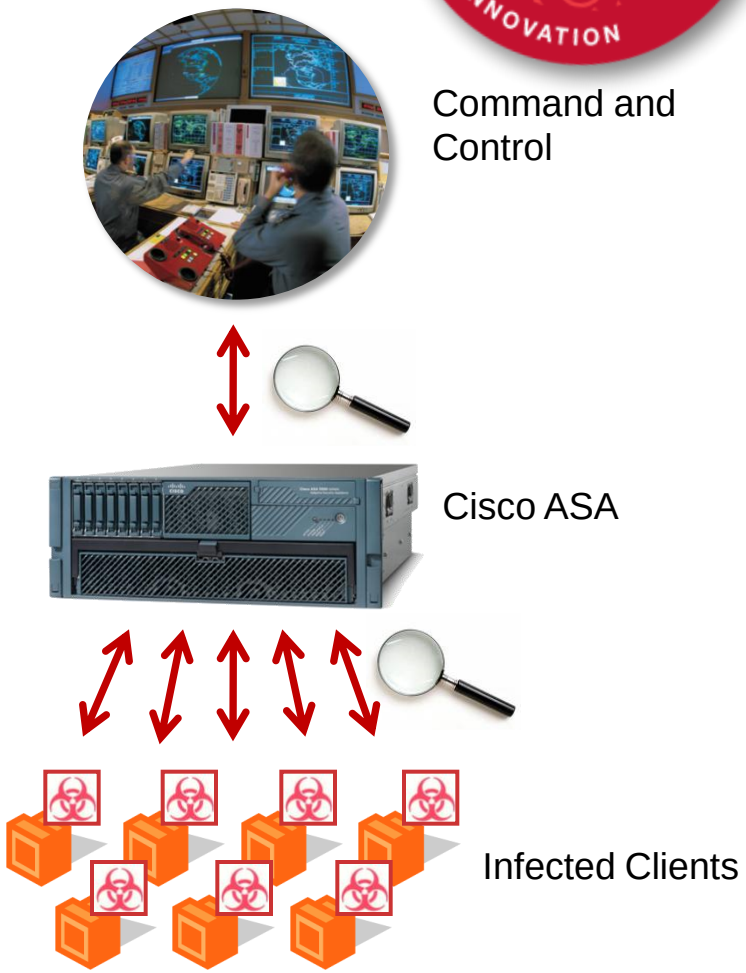
Hybrid Hosted

Security Software

Detecting Client Infections

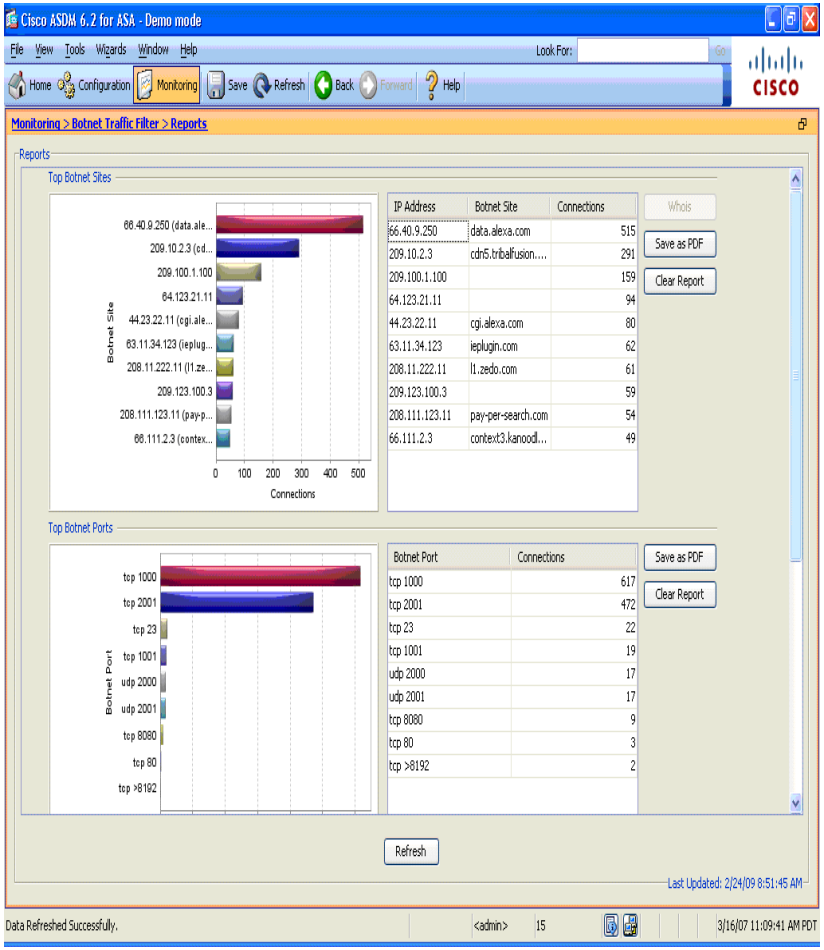
Botnet Traffic Filter on ASA 5500 Series

- **Monitors and blocks malware traffic**
  - Scans all traffic, ports & protocols
  - Detects infected clients by tracking rogue “phone home” traffic
- **Highly accurate**
  - Identifies100,000s of malware connections per week
  - Automatic DNS lookups of addresses
  - Dynamic database integrated into Cisco Security Intelligence Operations

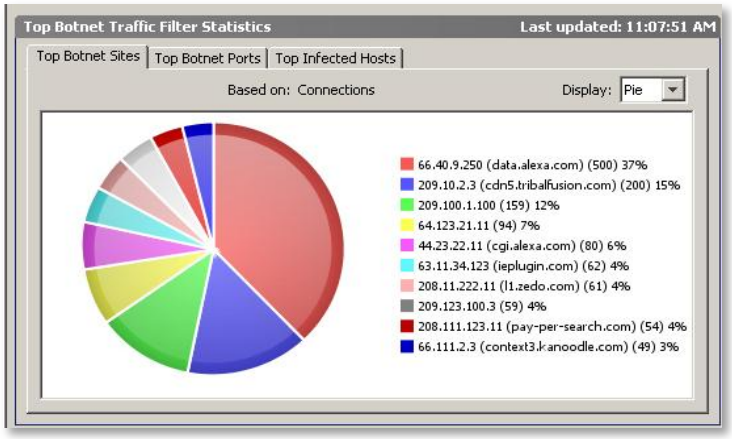


Cisco Botnet Traffic Filter Reports

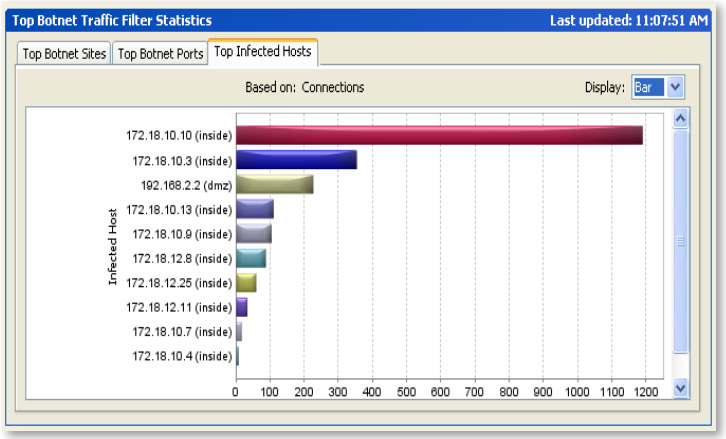
Top Botnet Sites, Ports and Infected Endpoints



Monitoring

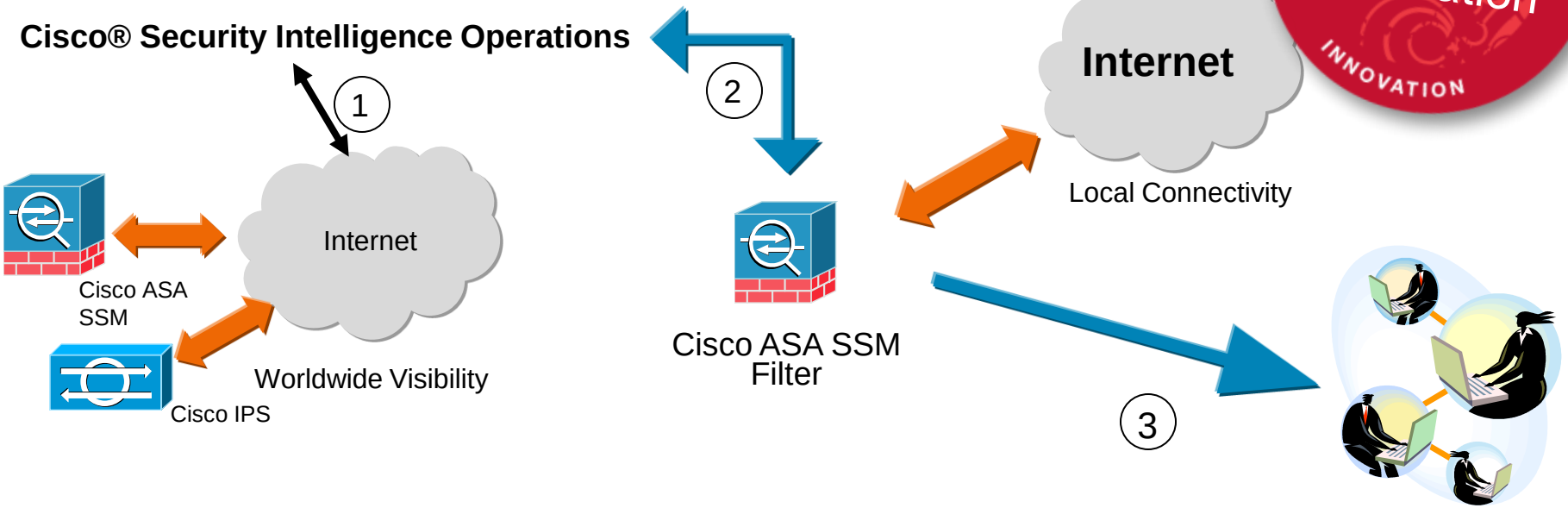


Live Dashboard



Integrated Reporting

IPS – Global Correlation in Action



Step 1:

The sensor base network within the Cisco SIO gathers telemetry data from other sensors across the world

Step 2:

Cisco IPS gets updated reputation filter list; influences policy decisions (deny or drop attacker, etc.)

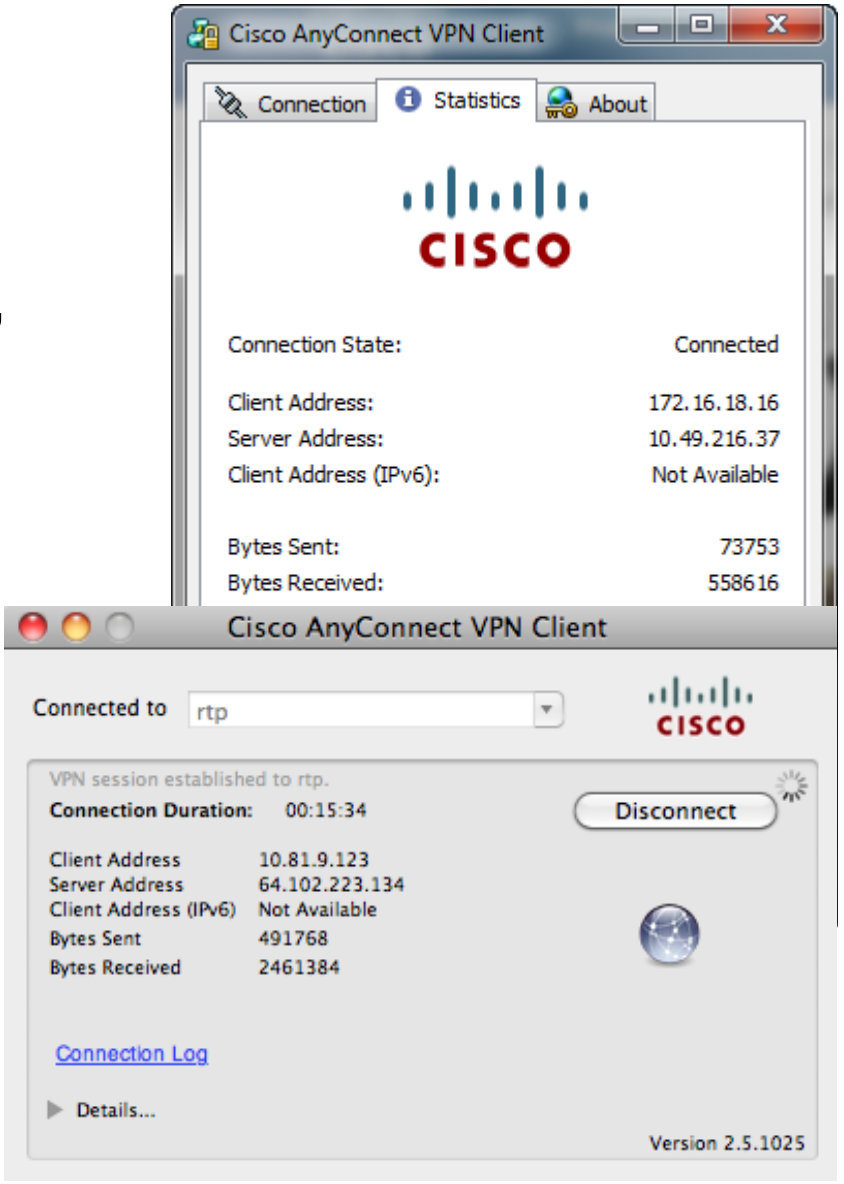
Step 3:

Alerts go out to the security teams for prevention, mitigation, and remediation

AnyConnect Client

AnyConnect 2.5

- Supported on
  - Windows 32-bit & 64 bit, XP, Vista , W7
  - Linux w 2.6 Kernel
  - Mac OSX 10.5 % 10.6
  - Windows Mobile 5,6 & 6.1
  - iPhone OS 4.1 (version 2.4)
- Encryption
  - SSL with DTLS (udp/443
  - For Media & Realtime Traffic



Secure Mobility

Cisco AnyConnect Secure Mobility

1 AnyConnect
Secure Mobility Client

Simplified remote access

Connection and app persistence

Always-on VPN enforcement

OGS & Location Awareness

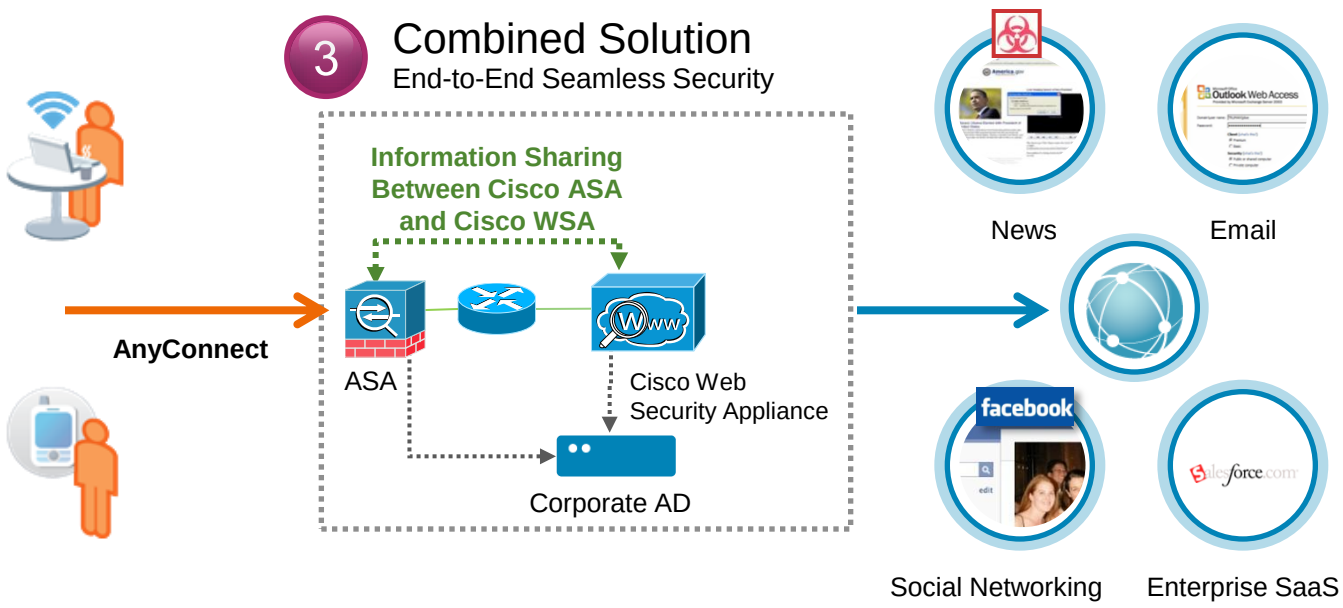
2 Web Security Appliance
Richer Web Controls

Location-aware policy

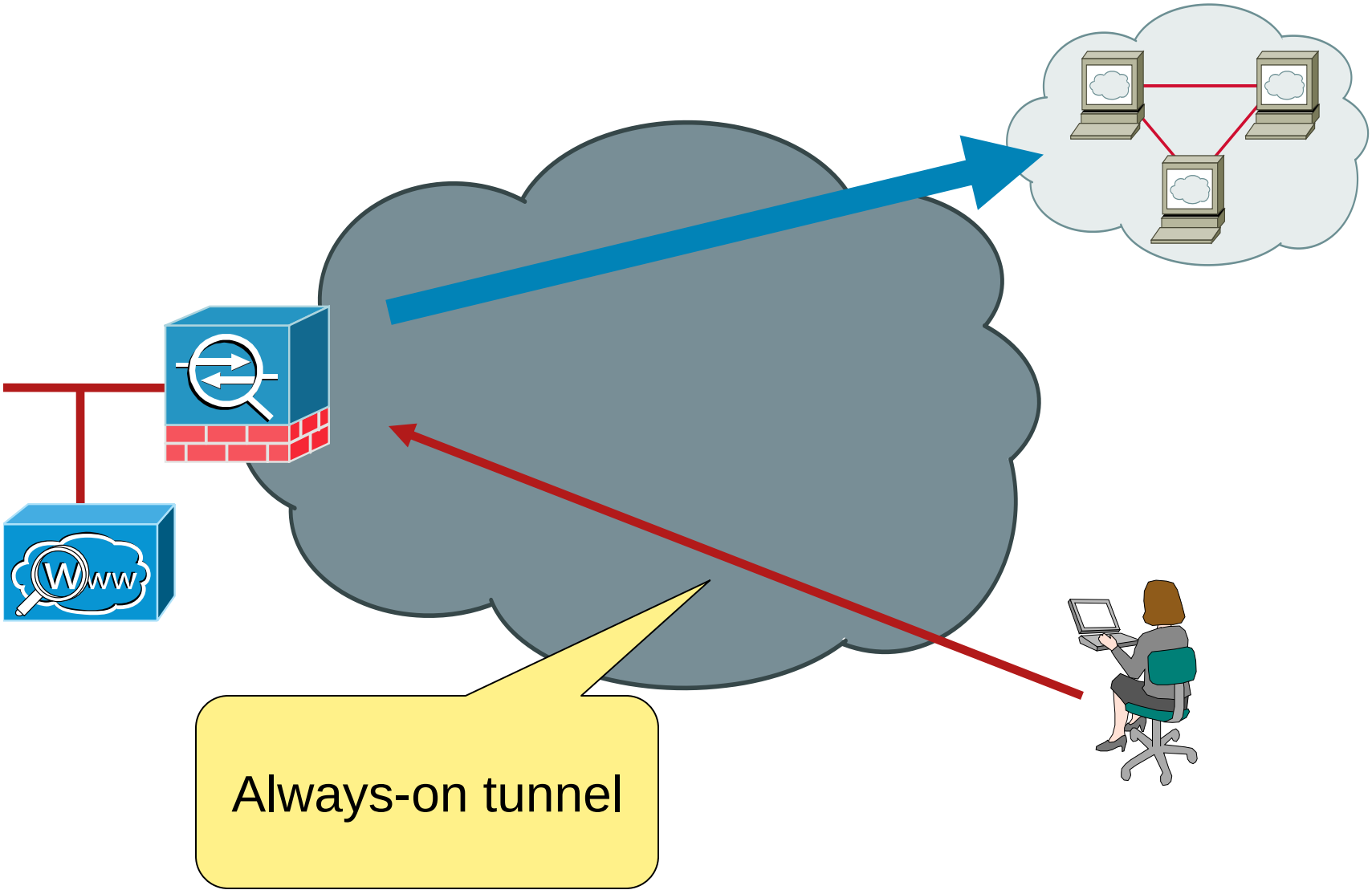
Application controls

SaaS Access Control

3 Combined Solution
End-to-End Seamless Security

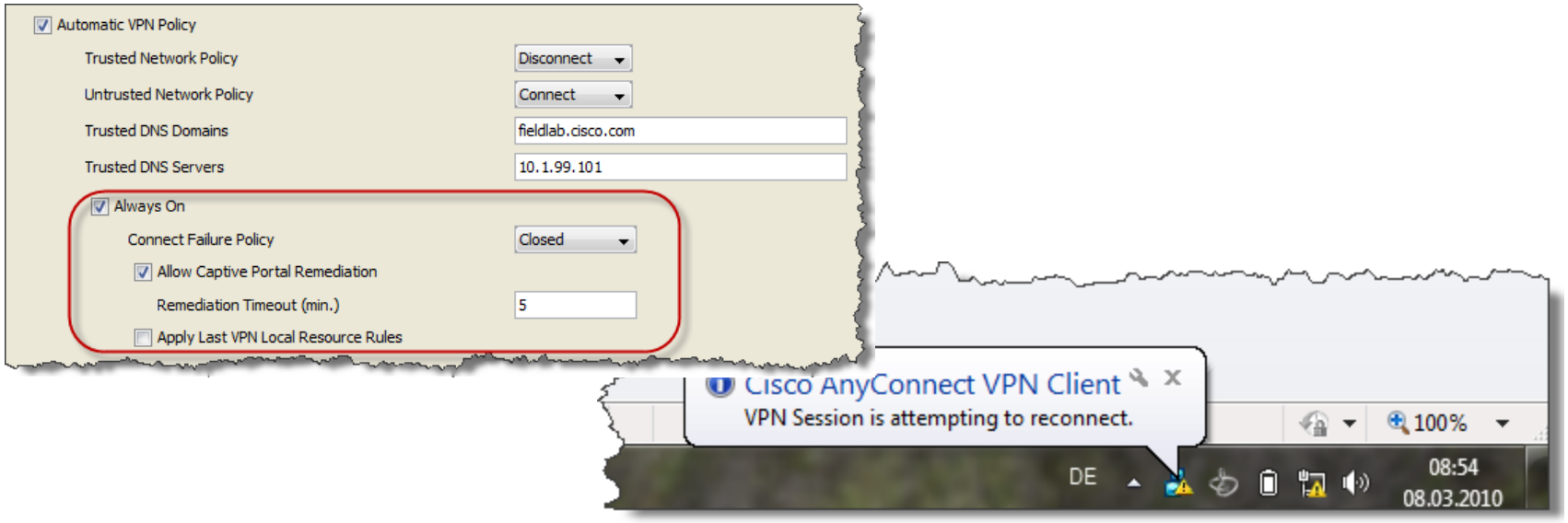


AnyConnect 2.5: Secure Mobility



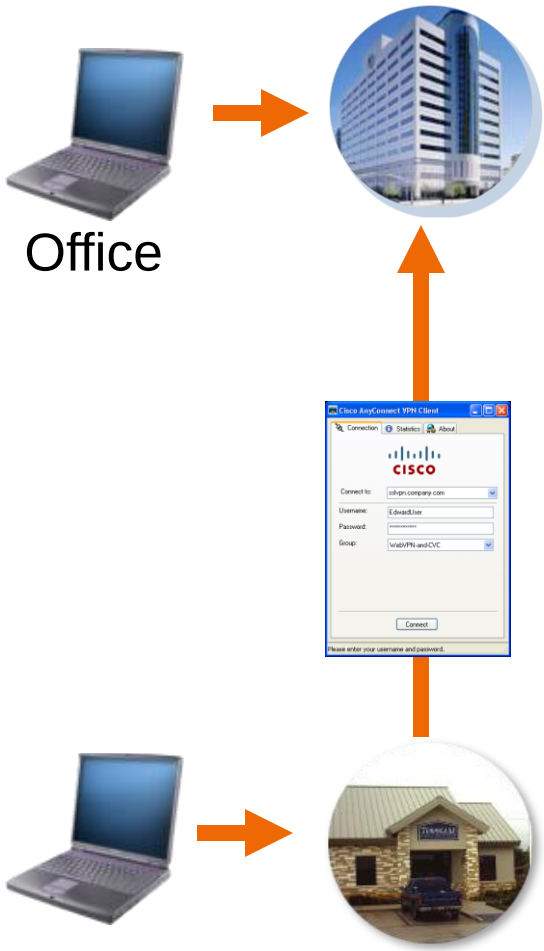
AlwaysOn

- Client Connection is kept both on ASA and on the Client
- If PC is coming back from Standby or is changing network, Client re-authenticates silently using a signed Cookie
- User does not need to manually reconnect

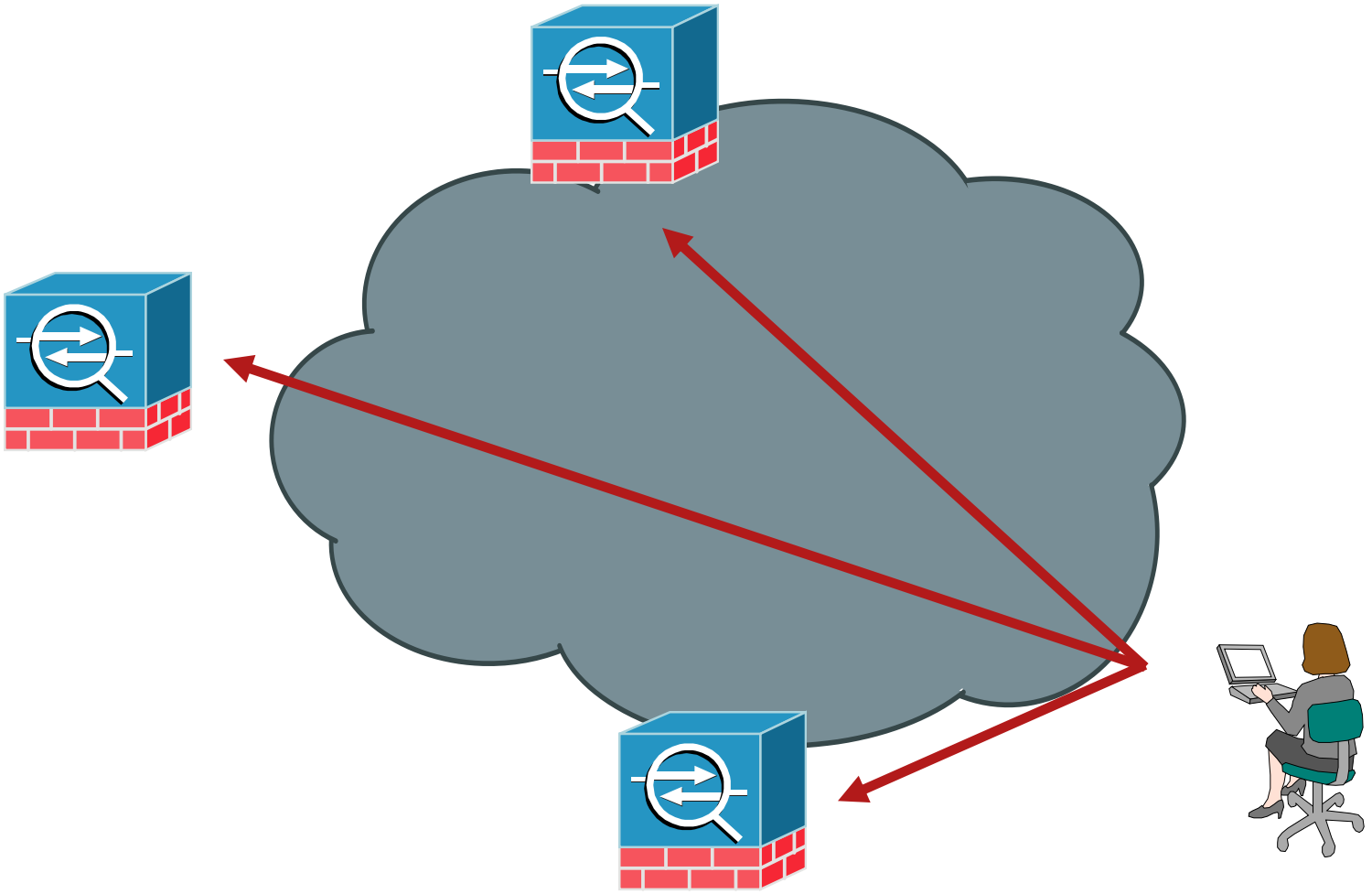


AnyConnect Trusted Network Detection

- Trusted Network Detection is Configurable via the AnyConnect Profile
- Trusted Networks can be Defined as DNS Suffixes or DNS Server IP Addresses
- DNS Suffixes and DNS Server IP addresses must be defined dynamically (DHCP) on the client
- If both, the trusted DNS Suffix and DNS Server IP address are defined, the entries will be ANDed to determine the Trusted Network



AnyConnect 2.5: Optimal gateway selection



Optimal Gateway Selection (OGS)

- Administrator Managed Feature
- Client determines the “nearest” ASA (a.k.a fastest response)
- OGS will initiate upon the following conditions:

  Prior to initial connection

  Upon reconnects (ex. coming out of standby)

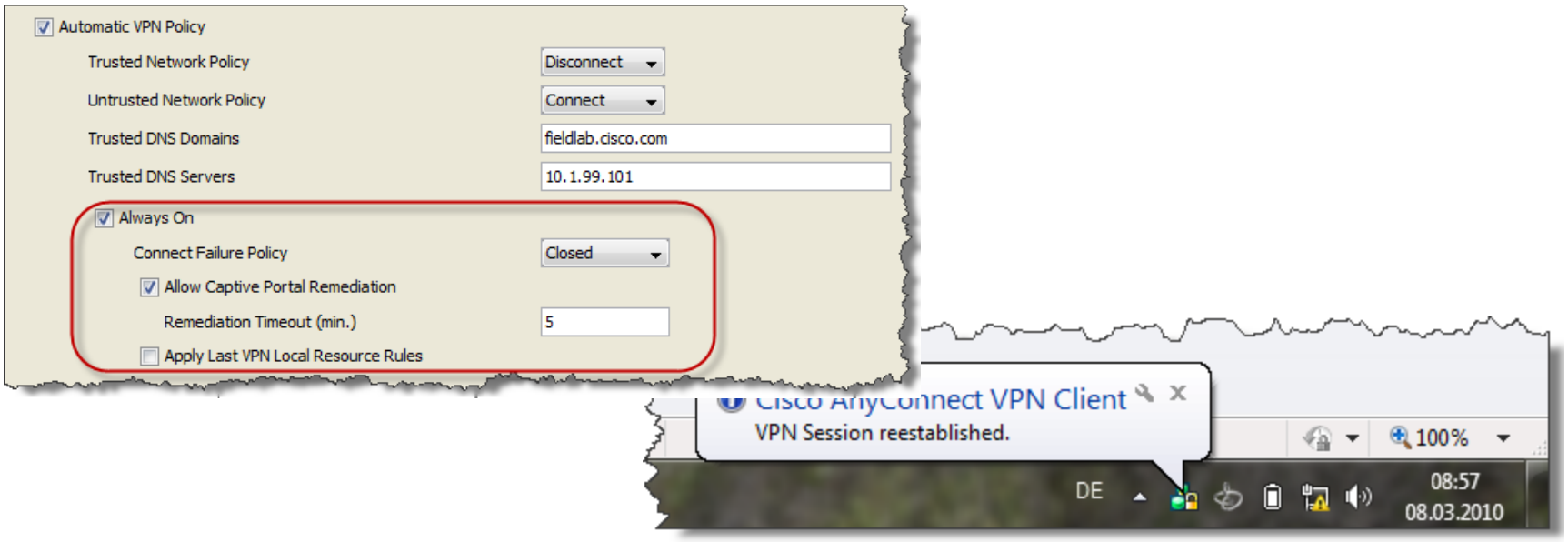
  4 hours have elapsed since last connection

  Will not switch ASA’s when results are not faster by > 20%

- If ASA switch occurs, this results in a disconnect/connect

Captive Portal Remidiation

- Captive Portal Remidiation allows User to authenticate to a HOTSPOT Portal
- AnyConnect discovers CaptivePortal
- User has option to authenticate via Browser
- Connection of AnyConnect is resumed after successfull authentication



Captive Portal Remediation

Client Firewall

- Uses the native OS firewall to configure firewall rules on the endpoint device - basic ipv6 and ipv4, no app FW rules
- ASA will pass the firewall rules to the client on connect
- Rules will be applied when:

  The VPN tunnel is active

  Or:

  The user is in a Fail Close state (allows user to do local print if no VPN is active)
- The original FW rules are cached upon connect and the original rules are restored after disconnect

Client Firewall: ASDM Configuration

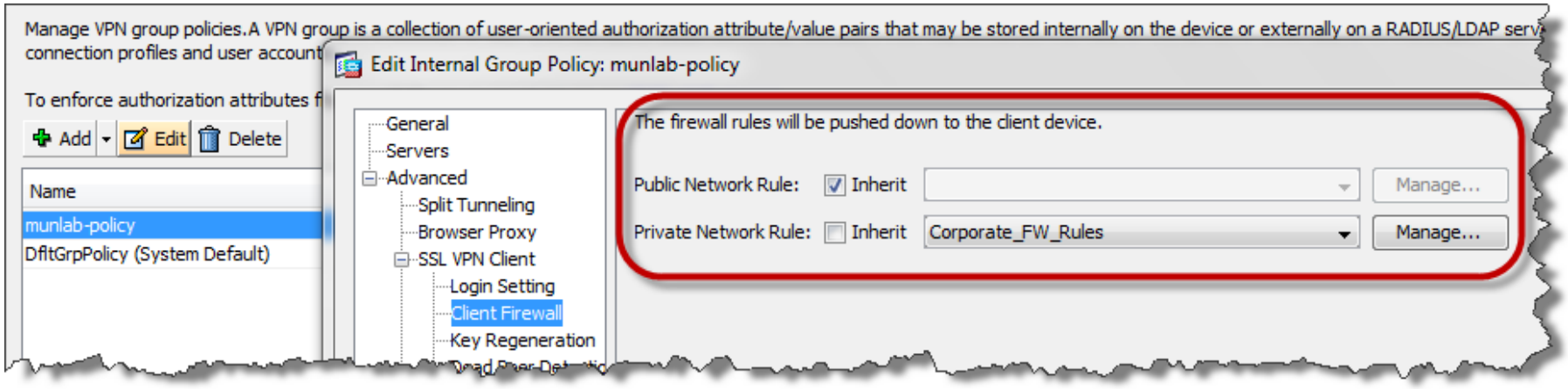
- **Public**

Any physical interface that has direct connectivity to a network other than the VPN
Only applied with a split tunneling configuration
If public rules can not be applied -> full tunneling will be applied.

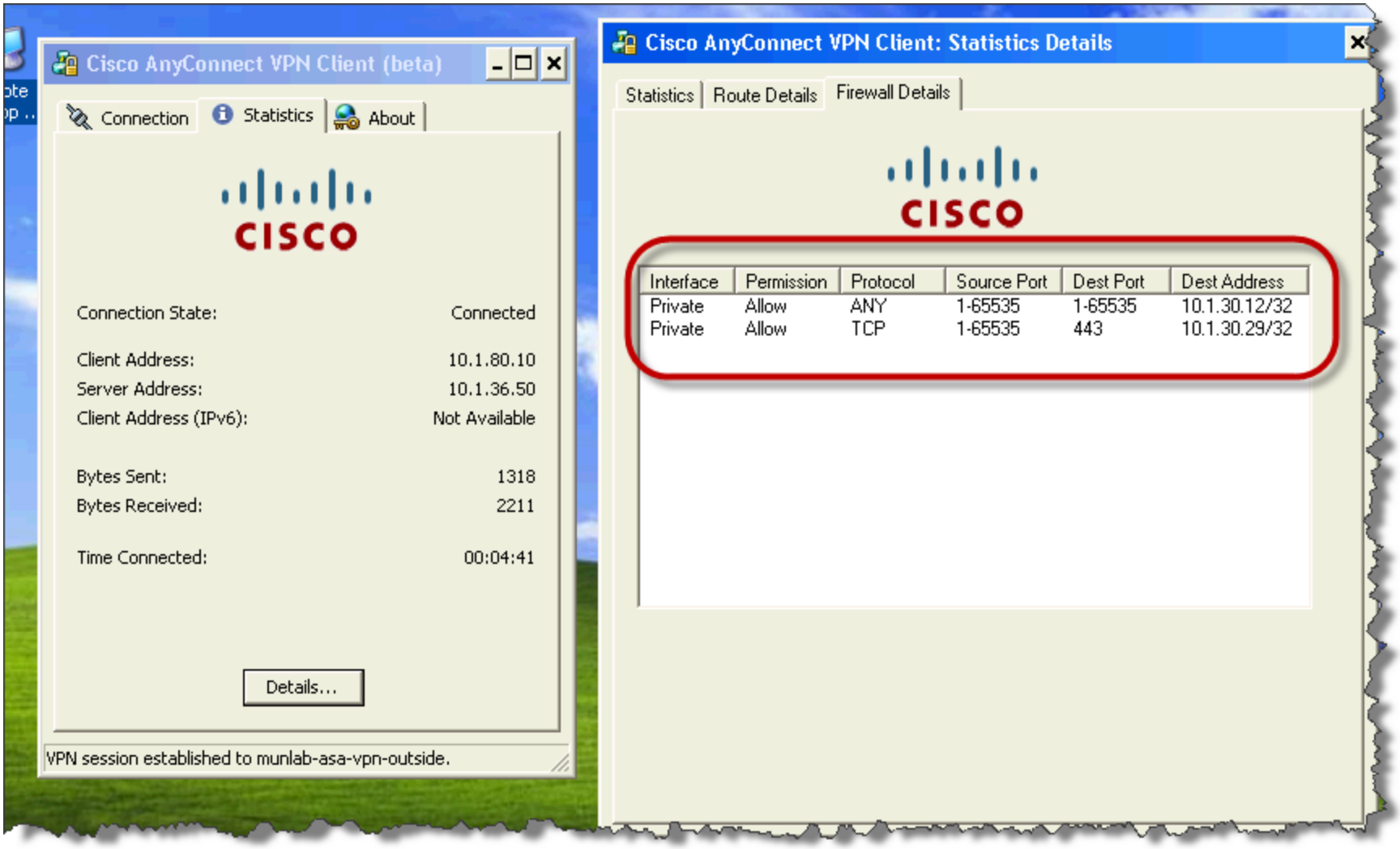
- **Private**

The Virtual Adapter interface

Rules are independent of the public interface



Client FW Rules



Benefits of Secure Mobility

- Different policies for local and remote Users

  Example: Block high bandwidth sites for remote users
- Single Sign-On for users on wsa for authentication
- Dramatically enhancend user experience through

  new client features

  AutoHeadendSelection

  AlwaysOn

  Trusted Network Detection

  SSO for SaaS

AnyConnect 3.0

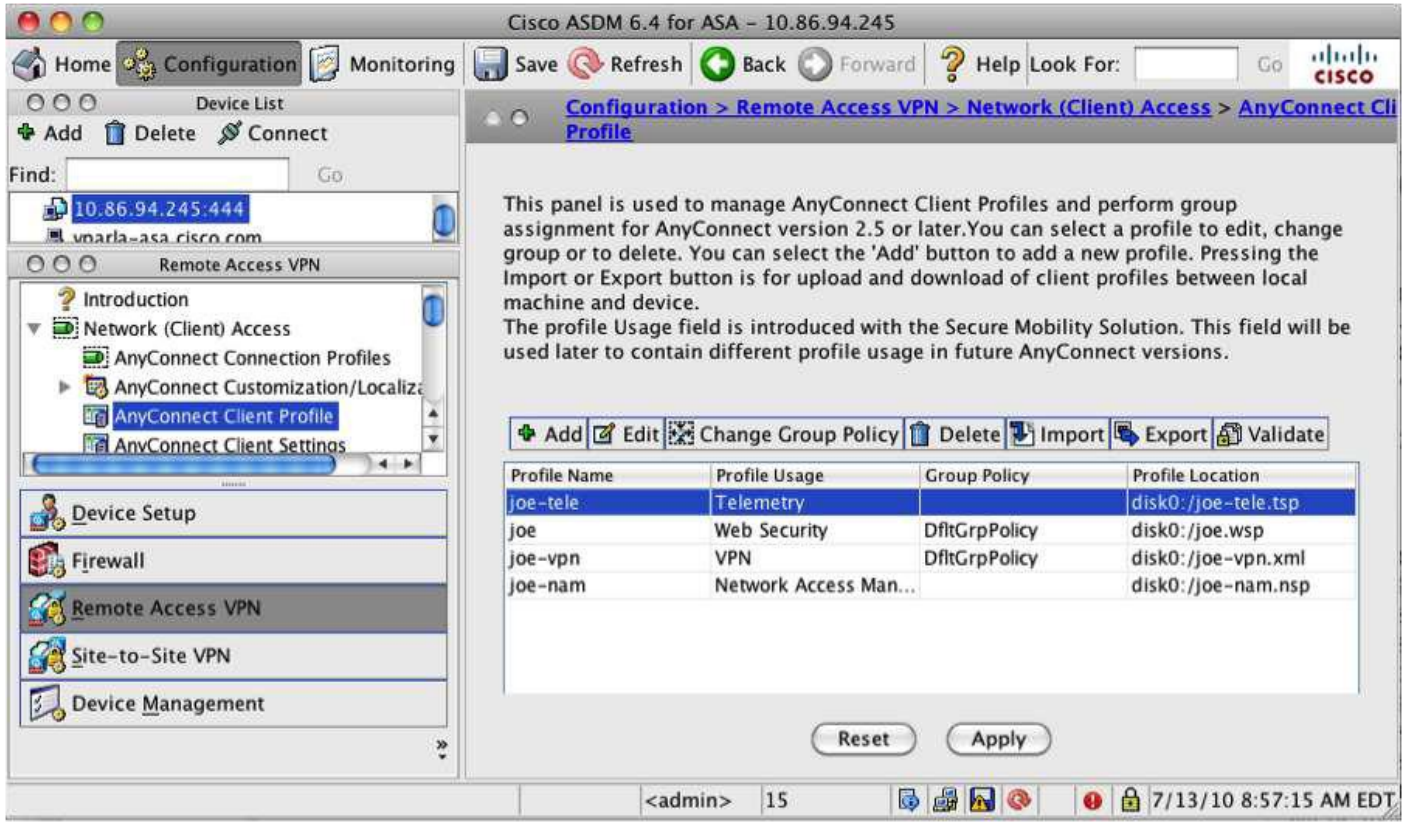
AnyConnect 3.0 – Unified Client

- New Modules include
  - Anywhere+ (Ex-ScanSafe)
  - Network Access Manager
  - Telemetry
- Components can be centrally distributed from ASA, at initial install or at later point of time
- Additional new features
  - IKEv2/IPSEC
  - SCEP proxy

Profile Editor

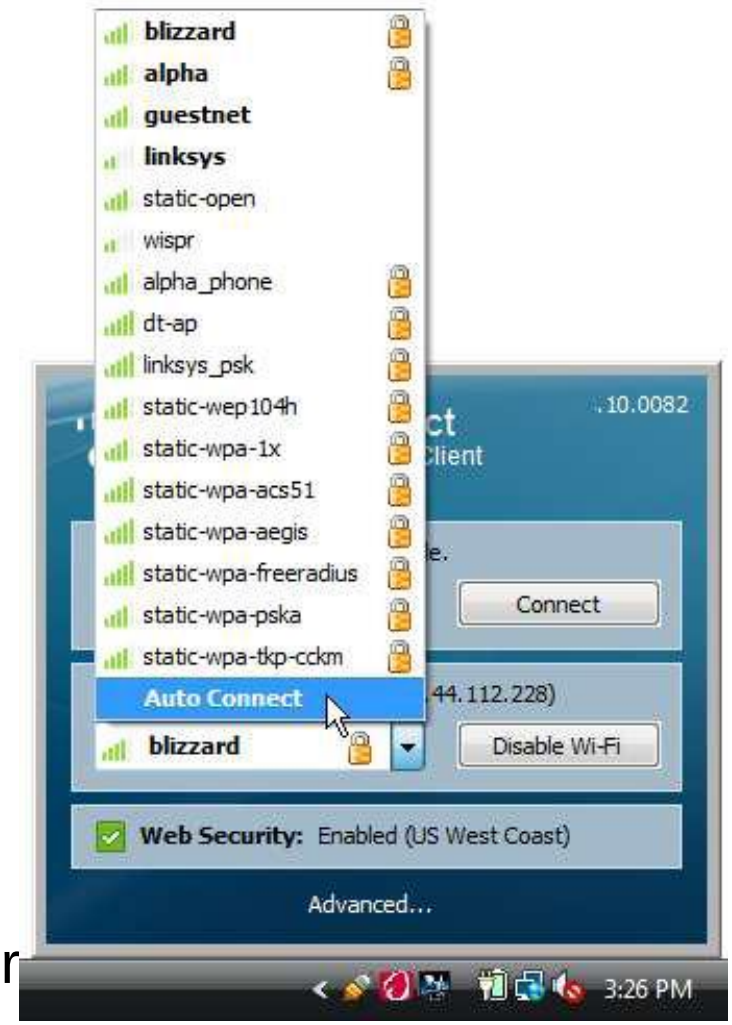
Integrated in ASDM on ASA

- Profile for VPN is ported from previous Versions
- Profiles for ScanSafe, NAM and Telemetry are new



AC 3.0 with Network Access Manager

- Connection Management for Layer 2
  - Windows XP (32 bits)
  - Windows Vista and 7 (32/64 bits)
- Wired (802.3) and wireless (802.11) connectivity
- Layer-2 user and device authentication:
  - 802.1X, 802.1X-REV (wired key establishment)
  - 802.1AE (MACSec: wired encryption)
  - Supports numerous EAP types
  - 802.11i (Robust Security Network)
- Supports both Admin (office) and User (home) network configurations.

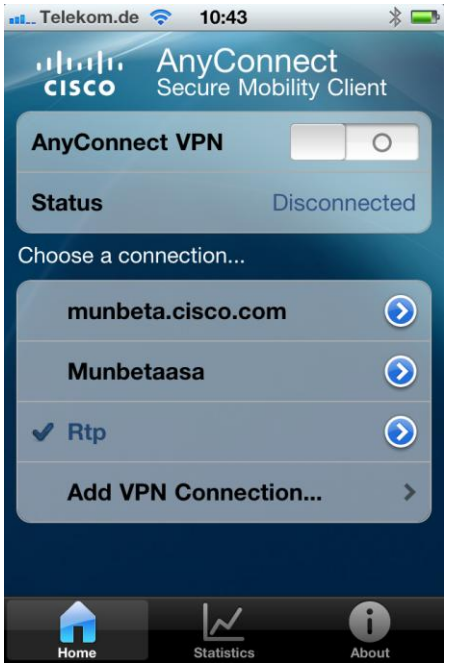


Demo

AnyConnect 3.0 with Cert Authentication

Summary

- Cisco ASA gives a broad Range of Platforms for Firewalling, VPN & IPS
- Cisco ASA & IPS dramatically improve accuracy due to integration with Cisco SIO
  - Global Correlation for IPS
  - Telemetry for AnyConnect
  - Botnet Traffic Filter for ASA
- Cisco AnyConnect Client gives many functions in one single, modular Client
- Cisco ASA is centrally managed & monitored by Cisco Security Manager
- Cisco Secure Mobility is a Solution to deliver Websecurity and ease of use to many different devices, including mobile devices like iPhone



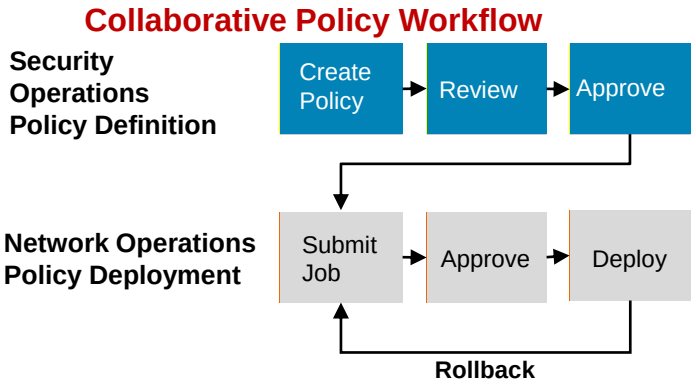
Cisco Security Manager

Management and Operations - CSM

Configuration and Policy Management

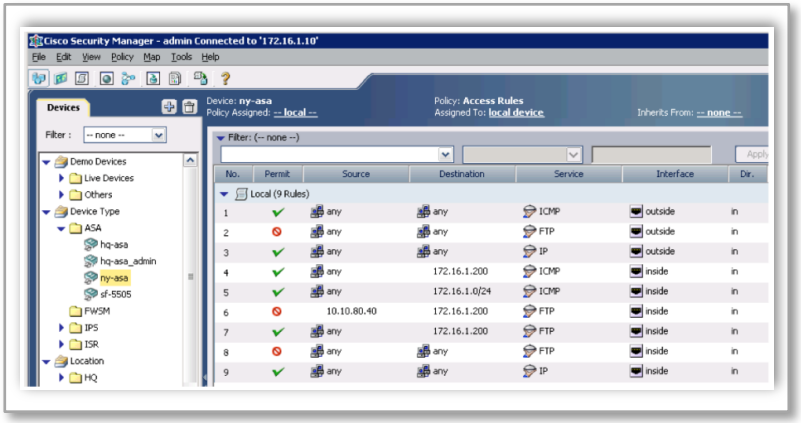
Policy Lifecycle Management

- Complex, hierarchical policy support
- Rule analysis tool identifies policy conflicts and overlap
- Rule combiner simplifies rule sets
- Rule expiration timers with alerts
- ACL Hit Counter identifies and removes unused rules



Change Mgmt and Control

- Manage privileges for rule creation, approval and deployment
- Automatically push updated rule sets per pre-defined schedule



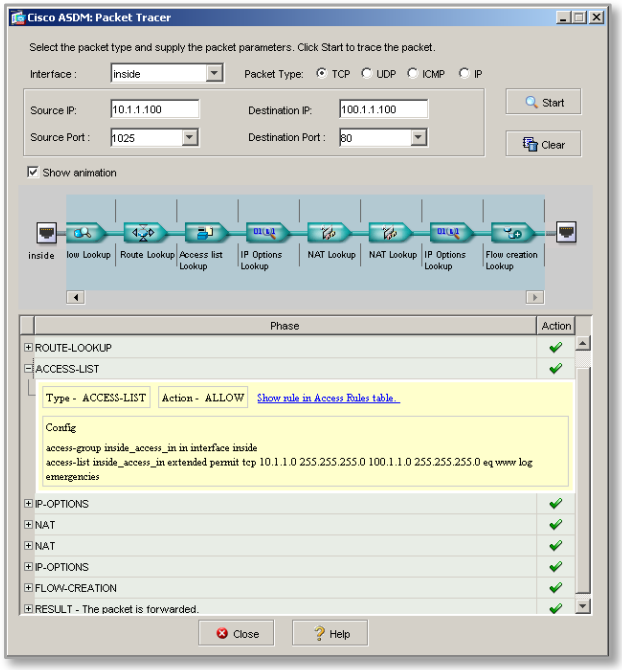
Management and Operations - CSM

Configuration and Policy Management

Troubleshooting

Create Packets flowing through your policy with Packet Tracer

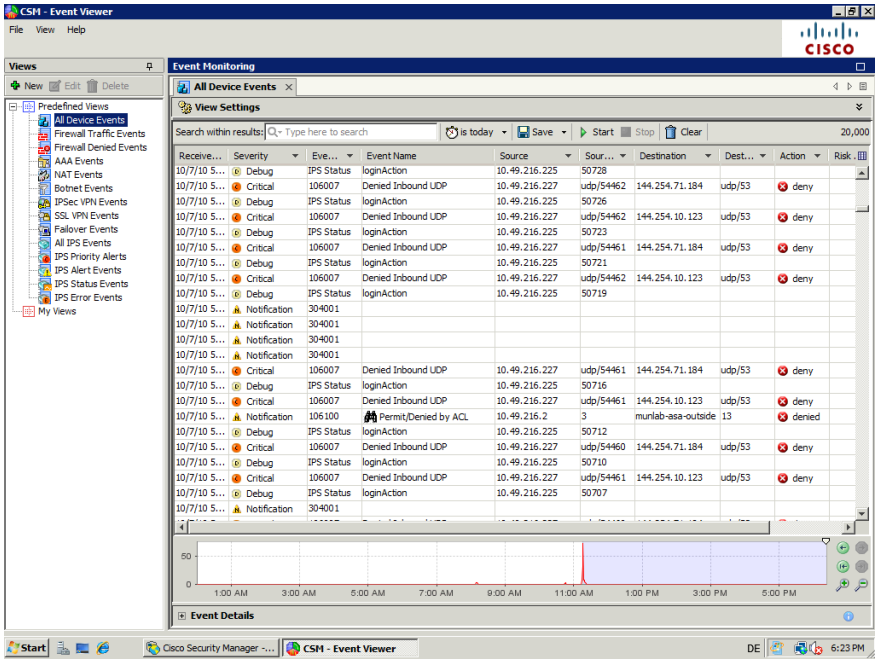
Get immediate Results



Monitoring

Monitoring of Firewall & IPS Alerts

Powerfull Filtering to analyze Firewall & IPS logs



Demo

Cisco Security Manager 4.0

Cisco Email Security

DLP Concerns – EU 95/46/EC

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The PCI Data Security Standard

- Purpose of standard – Protect credit card data by reducing fraud & theft
- Applies to all companies that handle credit card information
- Developed by MasterCard and Visa, endorsed by the other payment brands
- Merchants required to be PCI compliant or face penalties / termination by the credit card issuers.

Where PCI Assessments Are Failing

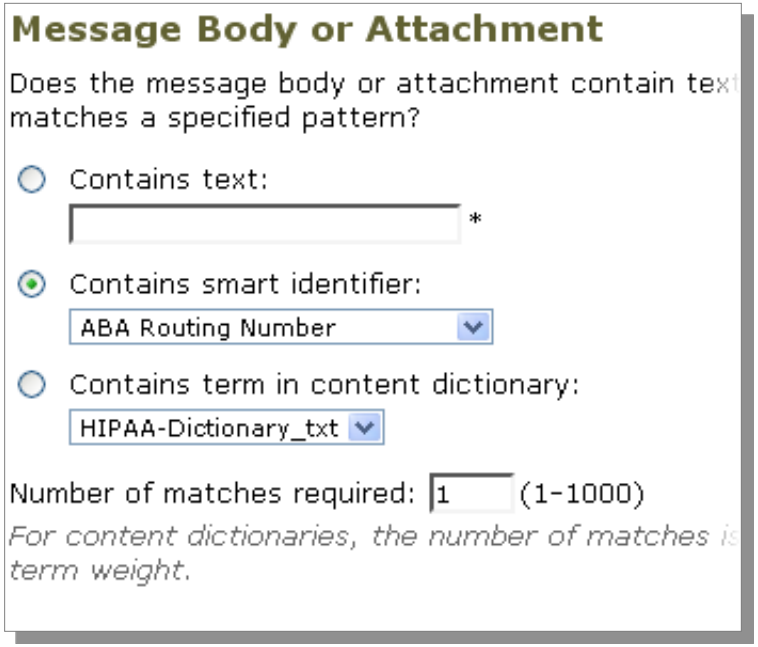
PCI Requirement	Percentage of Assessments Failing
Requirement 3: Protect Stored Data	79%
Requirement 11: Regularly Test Security Systems and Processes	74%
Requirement 8: Assign a Unique ID to Each Person with Computer Access	71%
Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data	71%
Requirement 1: Install and Maintain a Firewall Configuration to Protect Data	66%
Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters	62%
Requirement 12: Maintain a Policy That Addresses Information Security	60%
Requirement 9: Restrict Physical Access to Cardholder Data	59%
Requirement 6: Develop and Maintain Secure Systems and Applications	56%
Requirement 4: Encrypt Transmission of Cardholder Data and Sensitive Information Across Public Networks	45%

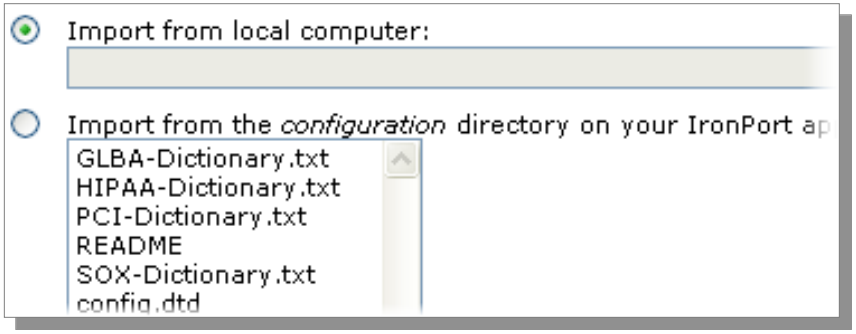
Cisco Ironport protection coverage

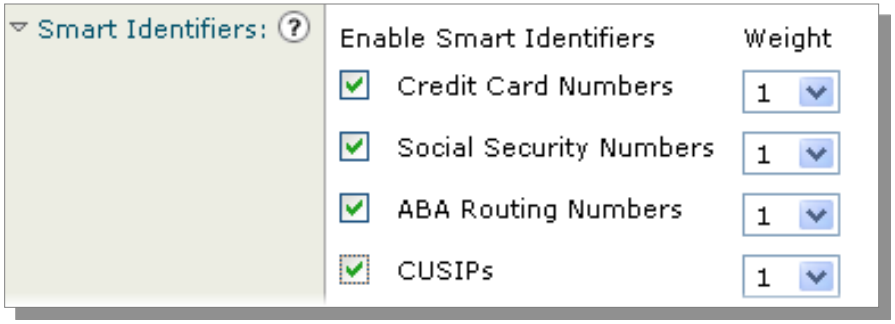
Source: VeriSign. “Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them.”

Data Loss Prevention
Simple Set Up

- On-Box Integration of RSA Dictionary
- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

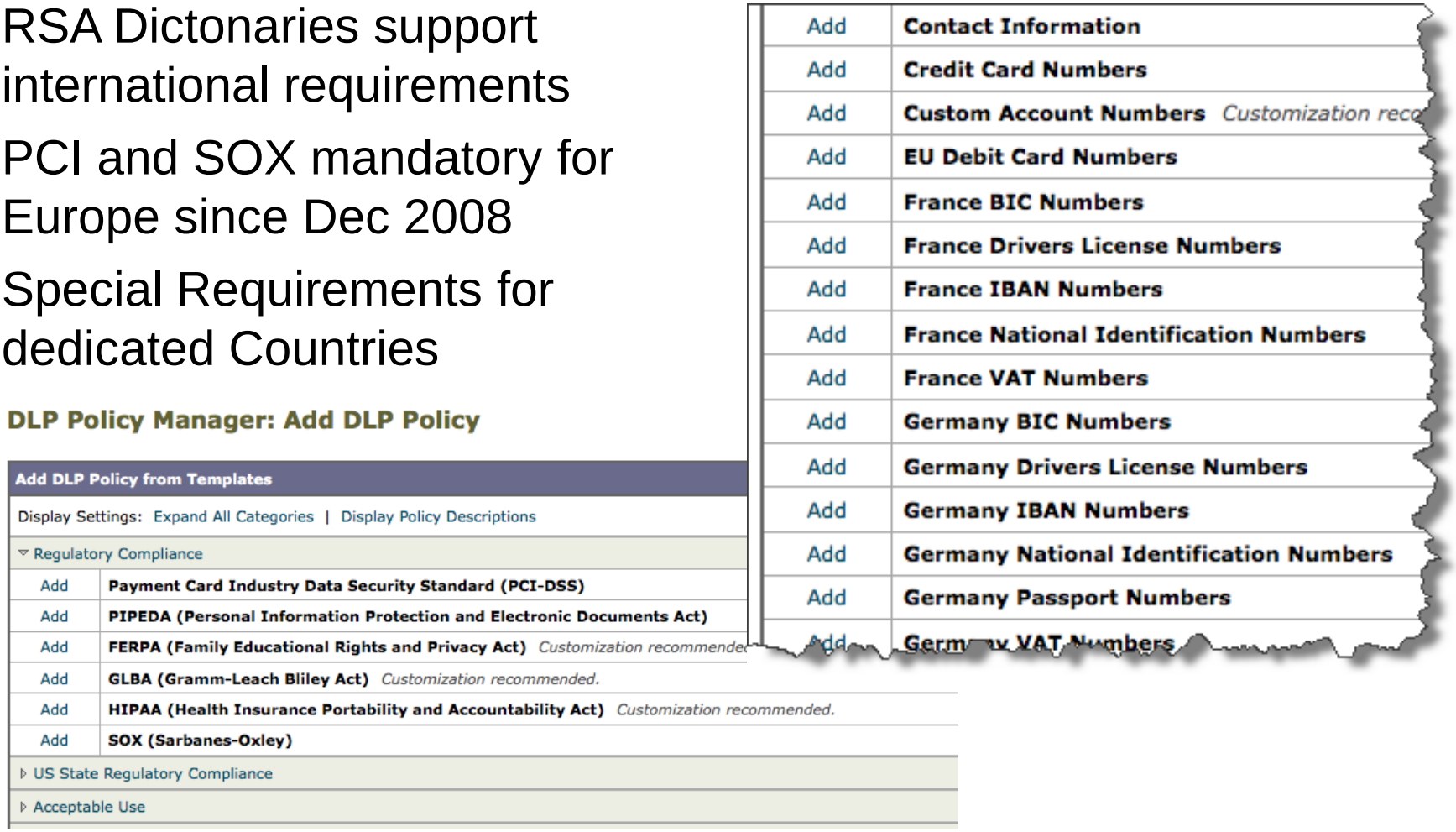






Data Loss Prevention
International Categories

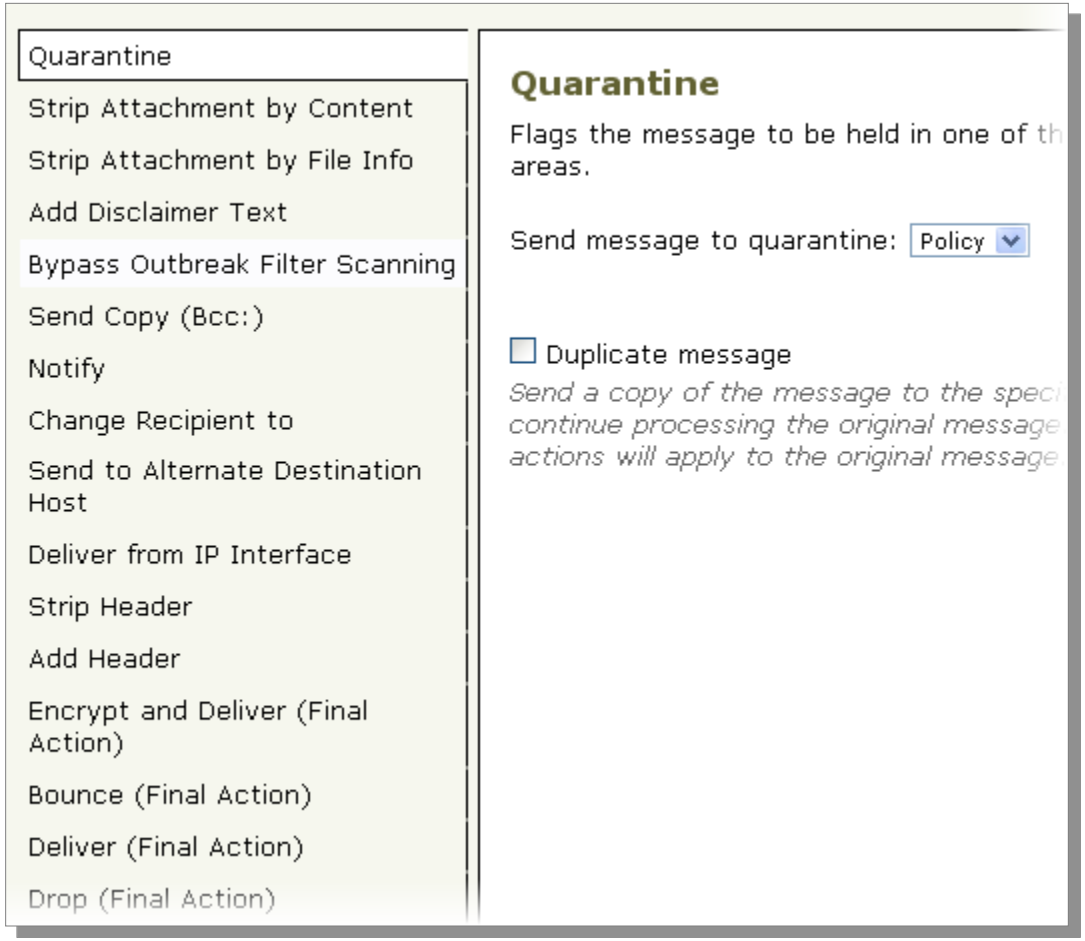
- RSA Dictonaries support international requirements
- PCI and SOX mandatory for Europe since Dec 2008
- Special Requirements for dedicated Countries



Data Loss Prevention

Comprehensive Remediation & Reporting

- Multiple remediation actions – encrypt, quarantine, drop, bounce, BCC, strip content
- Offending content highlighted in quarantine for easy analysis
- Reporting on a per policy and per user basis



Cisco live!

Registrujte se za Cisco Live Networkers u Londonu ili Bahreinu!
Više informacija na:
http://www.ciscolive.com/

Thank you.

HVALA PUNO! ☺