



Cisco Security update

Dragan Novaković, Security CCIE #26951

dnovakov@cisco.com

Cisco ASA 5500 Series Portfolio

Comprehensive Solutions from SOHO to the D

Performance and Scalability

**Multi-Service
(Firewall/VPN and IPS)**

ASA 5505
(150 Mbps, 4K cps)

ASA 5510
(300 Mbps, 9K cps)

ASA 5520
(450 Mbps, 12K cps)

ASA 5540
(650 Mbps, 25K cps)

ASA 5585 SSP-10
(4 Gbps, 50K cps)

ASA 5585 SSP-20
(10 Gbps, 125K cps)

ASA 5585 SSP-40
(20 Gbps, 200K cps)

ASA 5585 SSP-60
(35 Gbps, 350K cps)

NEW

NEW

NEW

NEW

ASA 5580-40
(20 Gbps, 150K cps)

ASA 5580-20
(10 Gbps, 90K cps)

ASA 5550
(1.2 Gbps, 36K cps)

**Firewall and VPN
Appliance**

SOHO

Branch Office

Internet Edge

Campus

Data Center



Cisco ASA 5585 Series High-End Solutions

NEW



Network Location

Performance

Max Firewall
Max IPS
Max IPSec VPN
Max IPSec/SSL VPN Peers

Internet Edge/
Campus
ASA 5585 SSP-10

4 Gbps
2 Gbps
1 Gbps
5000

Internet Edge/
Campus
ASA 5585 SSP-20

10 Gbps
3 Gbps
2 Gbps
10,000

Campus/
Data Center
ASA 5585 SSP-40

20 Gbps
5 Gbps
3 Gbps
10,000

Data Center
ASA 5585 SSP-60

35 Gbps
10 Gbps
5 Gbps
10,000

Platform Capabilities

Max Firewall Conns
Max Conns/Second
Packets/Second (64 byte)
Base I/O
Max I/O
VLANs Supported
HA Supported

750,000
50,000
1,500,000
8 GE + 2 10 GE
16 GE + 4 10 GE
250
A/A and A/S

1,000,000
125,000
3,000,000
8 GE + 2 10 GE
16 GE + 4 10 GE
250
A/A and A/S

2,000,000
200,000
5,000,000
6 GE + 4 10GE
12 GE + 8 10GE
250
A/A and A/S

2,000,000
350,000
9,00,000
6 GE + 4 10GE
12 GE + 8 10GE
250
A/A and A/S

High Performance Multi-Service Cisco ASA 5585-X Series

Under the Covers

2 RU Chassis

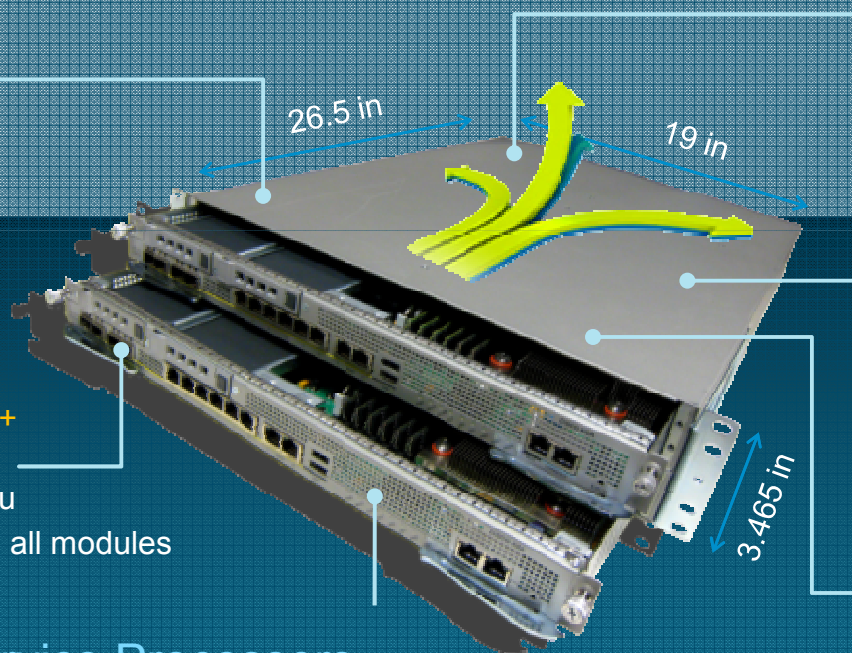
- 2 x full-slot modules
- 1 x full-slot + 2 x half-slot modules
- OIR capable

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

- Multi-services capable
- Dedicated 64bit multi-core processors
- Future-proof hardware



Redundant Hot Swappable Power Supply Units

- Front to back air flow

Multi Gigabit Fabric

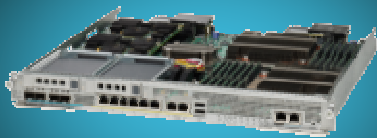
- Passive backplane
- Module to module communications
- Packet prioritization and shaping

eUSB

- 2 GB internal
- Convenience storage
- Security credentials

ASA 5585-X Firewall/VPN Module

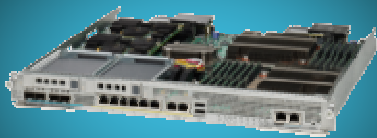
Feature Comparison



ASA 5585-X

	ASA SSP-10	ASA SSP-20	ASA SSP-40	ASA SSP-60
Maximum Throughput	Yes	Yes	Yes (Dual CPU)	Yes (Dual CPU)
Maximum Memory	6 GB	12 GB	12 GB	24 GB
Maximum Storage	2 GB eUSB	2 GB eUSB	2 GB eUSB	2 GB eUSB
Ports	2 x SFP+ 8 x 1GbE Cu 2 x 1GbE Cu Mgmt	2 x SFP+ 8 x 1GbE Cu 2 x 1GbE Cu Mgmt	4 x SFP+ 6 x 1GbE Cu 2 x 1GbE Cu Mgmt	4 x SFP+ 6 x 1GbE Cu 2 x 1GbE Cu Mgmt
Crypto Chipset	Yes	Yes	Yes	Yes

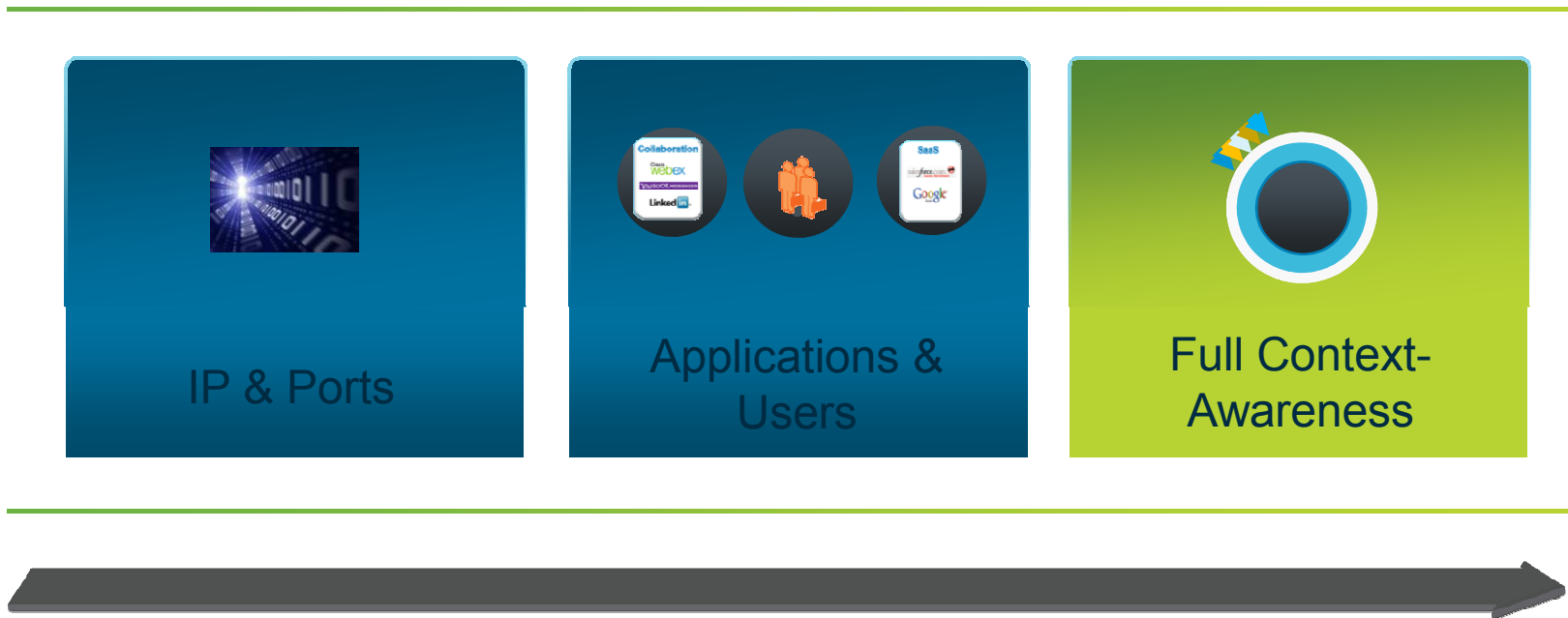
ASA 5585-X IPS Module Feature Comparison



ASA 5585-X

	IPS SSP-10	IPS SSP-20	IPS SSP-40	IPS SSP-60
IPS	Yes	Yes	Yes (Dual CPU)	Yes (Dual CPU)
Maximum Memory	6 GB	12 GB	24 GB	48 GB
Maximum Storage	2 GB eUSB	2 GB eUSB	2 GB eUSB	2 GB eUSB
Ports	2 x SFP+ 8 x 1GbE Cu 2 x 1GbE Cu Mgmt	2 x SFP+ 8 x 1GbE Cu 2 x 1GbE Cu Mgmt	4 x SFP+ 6 x 1GbE Cu 2 x 1GbE Cu Mgmt	4 x SFP+ 6 x 1GbE Cu 2 x 1GbE Cu Mgmt

Firewall Evolution



Identity-Aware Firewall

Key Benefits

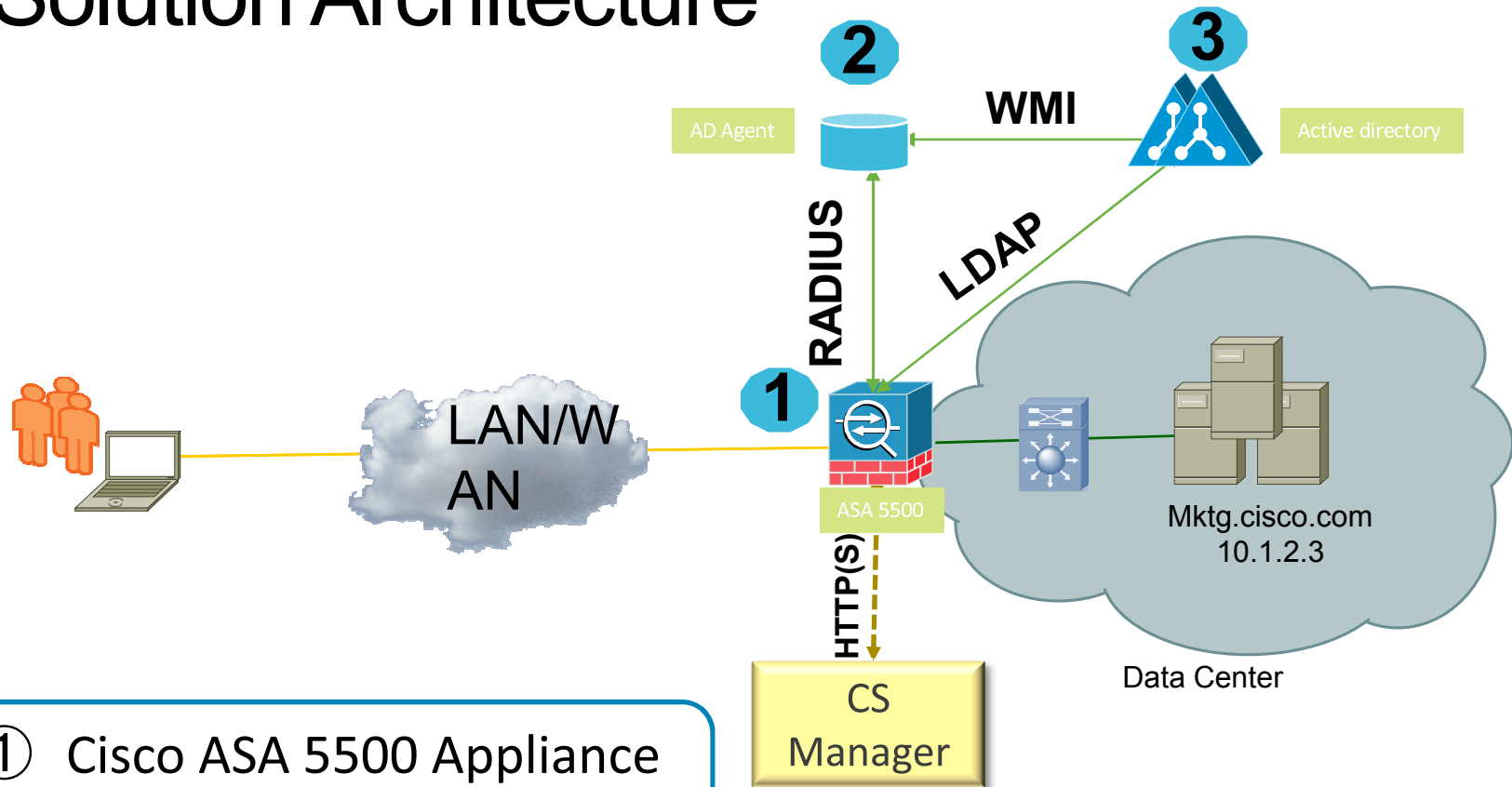
Reduces
operational
complexity

- Decouple topology from policies
- Greater flexibility
- Simplify policies
- Saves cost from administration

Provides
Greater
Visibility

- Identify who's doing what
- Simplify monitoring
- Provide better control based on business needs

Identity-Aware Firewall Solution Architecture



- ① Cisco ASA 5500 Appliance
- ② Off-box AD Agent
- ③ AD Domain Controllers

Key Components

Configuration Example

IDFW Access Control Rules

Users=NONE
would trigger CTP (Cut-Through P.) rule

Global (8 rules)							
1	<input checked="" type="checkbox"/>	any		inside-hosts	IP ip	TOP 10 224	Inf...
2	<input checked="" type="checkbox"/>	any		any	IP ip	✓ Per...	2173 Inf...
3	<input checked="" type="checkbox"/>	any		any		✗ Deny	0
4	<input checked="" type="checkbox"/>	any	IDFW\Administrator	amazon	IP ip	✓ Per...	0
5	<input checked="" type="checkbox"/>	any	IDFW\SJC.WEB_MARKETING.M IDFW\stsales	www.facebook.com	IP ip	✓ Per...	0
6	<input checked="" type="checkbox"/>	any		www.facebook.com	IP ip	✗ Deny	0
7	<input checked="" type="checkbox"/>	any	none	any	IP ip	✓ Per...	
8		any		any	IP in	✗ Deny	Implicit rule

CLI Commands

```

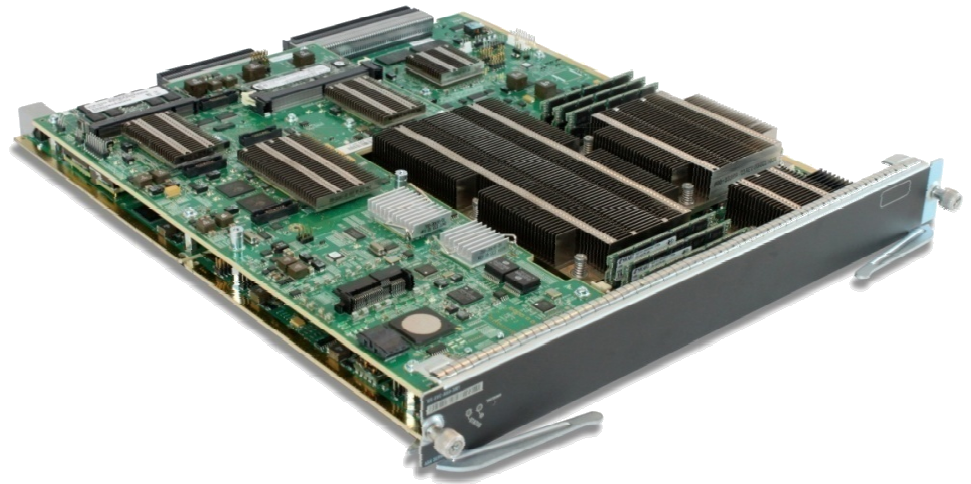
access-list mypolicy permit ip user IDFW\administrator object amazon
access-list mypolicy permit ip user-group IDFW\SJC.WEB_MARKETING.M, IDFW\stsales object
www.facebook.com eq 80
access-list mypolicy deny ip any object www.facebook.com
access-list mypolicy permit ip user NONE any any
access-list mypolicy deny ip any any
access-group mypolicy global
    
```



ASA Services Module (ASASM) update

ASA Service Module

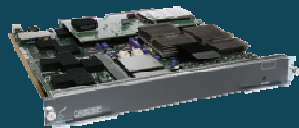
- ASA security blade for the Catalyst 6500
- Places security directly into the datacenter backbone
- Simplified installation and greater flexibility
- High performance and capacity



ASASM / ASA-5585-X



ASA 5585-SSP10



FWSM



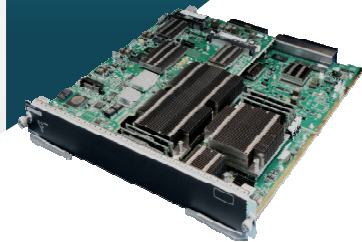
ASA 5585-SSP20



ASA 5585-SSP40



ASA 5585-SSP60



ASA Service Module

Multi Gigabit Fabric

- Chassis Backplane
- Virtualized Interfaces
- Module to module communications

24 Gigabytes Memory

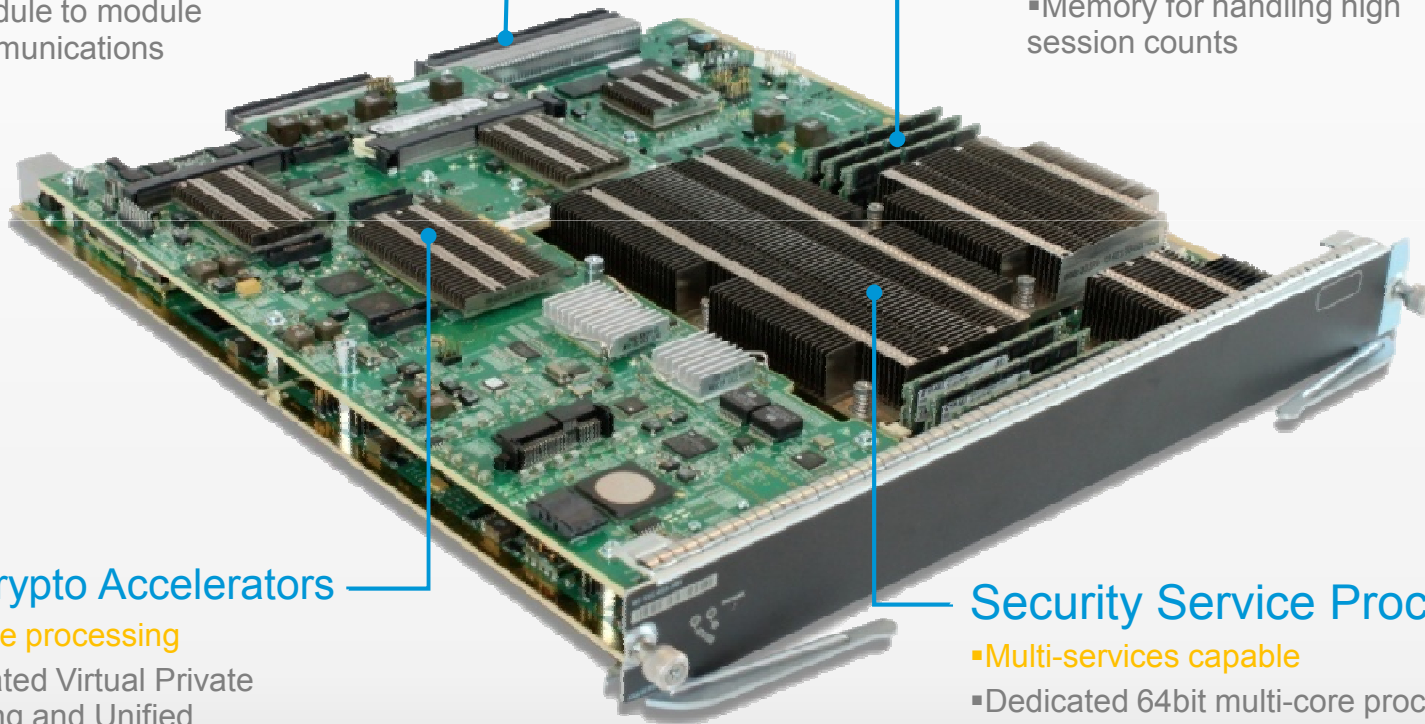
- High Capacity
- Memory for handling high session counts

Dual Crypto Accelerators

- Hardware processing
- Accelerated Virtual Private Networking and Unified Communications encryption

Security Service Processors

- Multi-services capable
- Dedicated 64bit multi-core processors
- Future-proof hardware



Specifications

Component	Rating
Processor	2 CPU - 24 Cores
Memory	24 GB
Storage	8 GB Flash
Security Contexts	250
VLANs	1000
Blades per Chassis	4

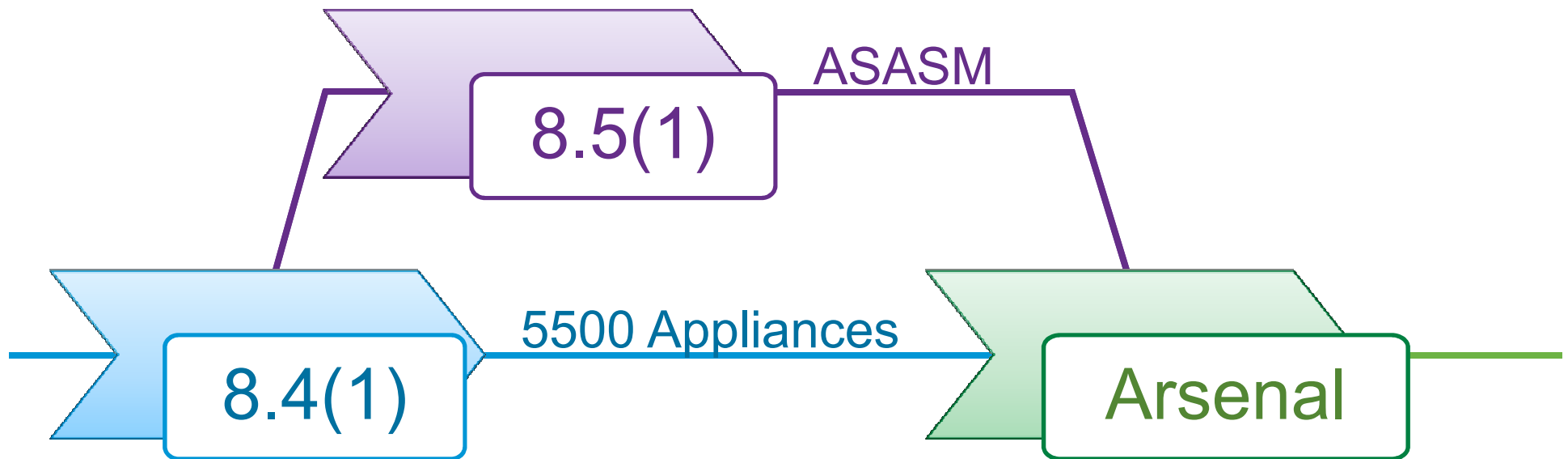
Performance

Metric	ASASM
Concurrent Sessions	10 Million
New Connections/Second	300,000
Throughput (EMIX)	16 Gbps
Chassis Throughput (EMIX)	64 Gbps

Performance

Metric	5585-SSP60	ASASM
Concurrent Sessions	10 Million	10 Million
New Connections/Second	350,000	300,000
Throughput (EMIX)	20 Gbps	16 Gbps
Chassis Throughput (EMIX)	40 Gbps	64 Gbps

ASA Release Branches





ScanSafe

Dragan Novakovic
dnovakov@cisco.com

Vision

- Pioneer in SaaS Web Security
- Our vision - a service that offered:
 - Scale
 - Reach
 - First
 - Visibility
- Recognized by analysts as the leading provider of SaaS Web security

"The first successful in-the-cloud secure Web gateway service"

Gartner

Customers



Awards



Partners



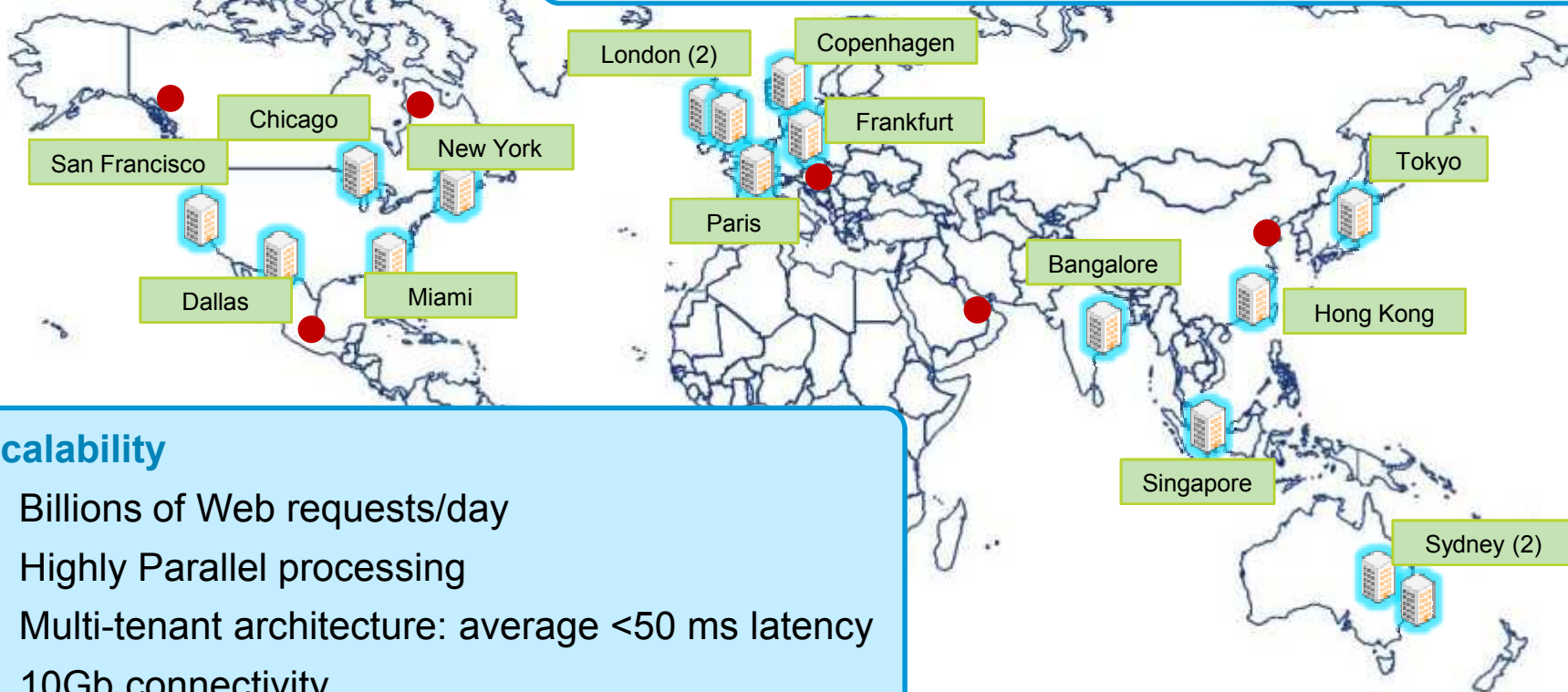
Scalability & Reliability



User Granularity

Reliability

- 16 Data Centers spanning four continents
- Top tier certification
- Thousands of devices deployed
- 100% availability, automated monitoring, full redundancy



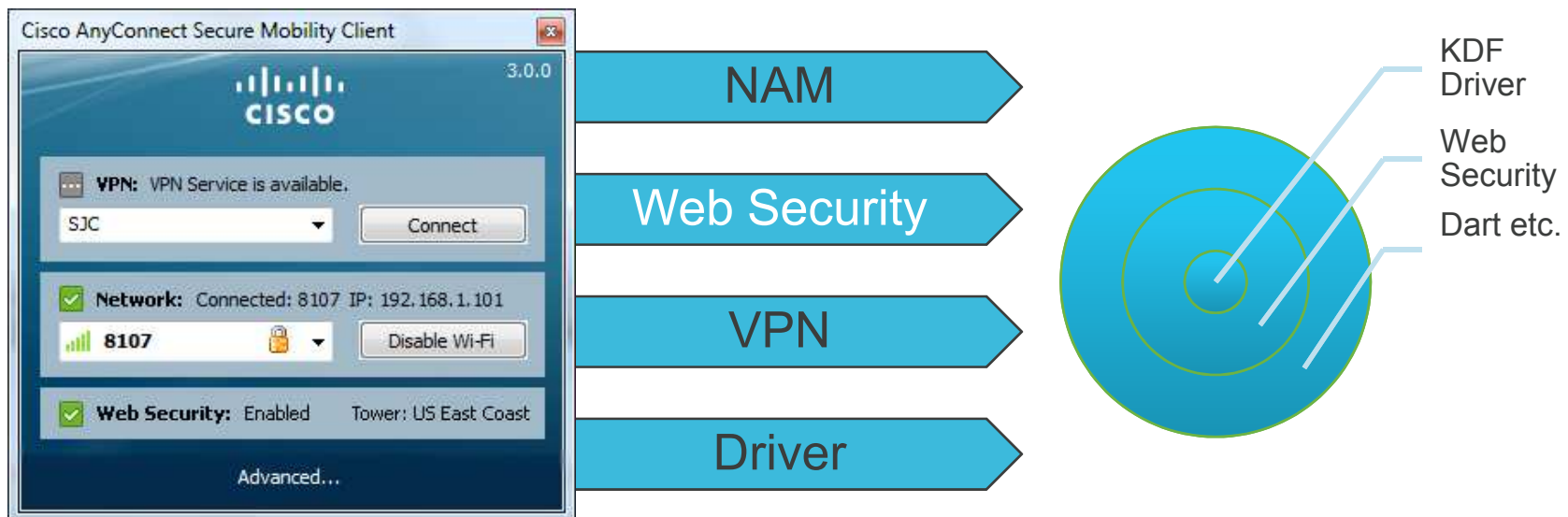
Scalability

- Billions of Web requests/day
- Highly Parallel processing
- Multi-tenant architecture: average <50 ms latency
- 10Gb connectivity
- Redundant network providers

Centers planned

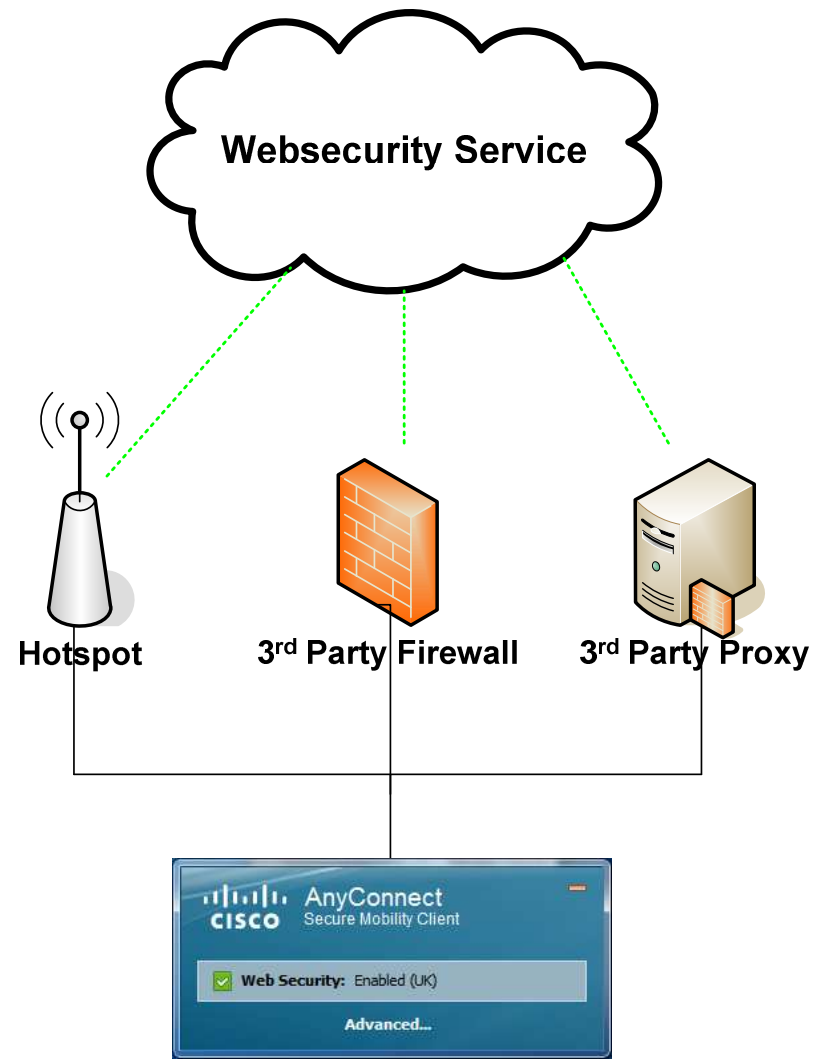
What is Cisco Web Security?

- Cisco Web Security is a new component of Cisco's AnyConnect 3.0 VPN client
- This component is comprised of ScanSafe's Anywhere+ functionality
- Web Security is an additional layer within Any Connect, that works with the driver, alongside the other existing features



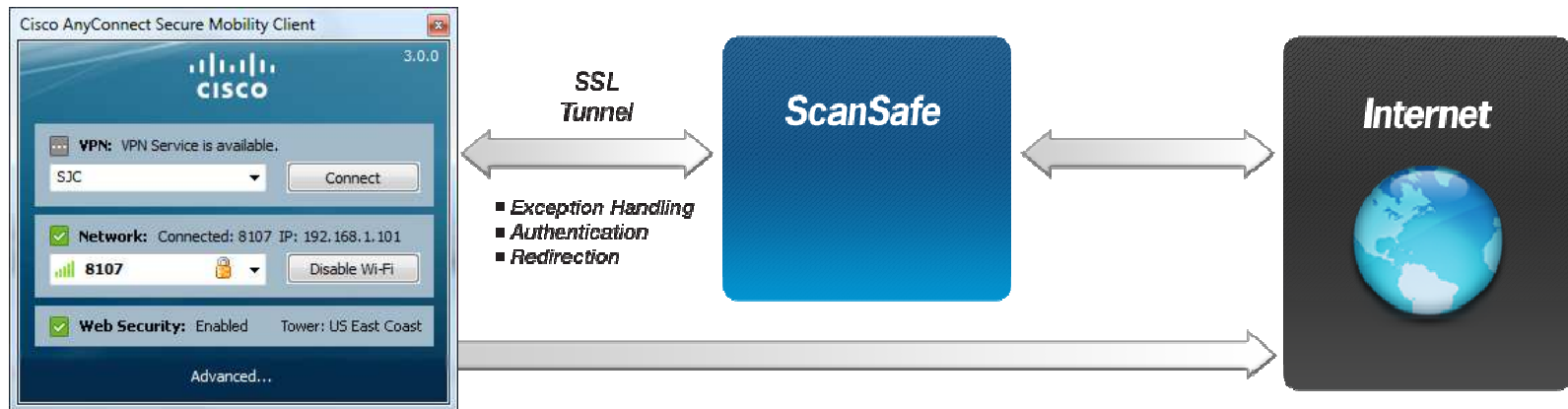
Protecting Roaming Users - Web Security

- Web Security installs a Network Driver which binds to all connections (LAN, Wireless, 3G)
- Automatic Peering Identifies nearest ScanSafe Datacenter and whether a connection is possible
- AD information can be remembered from when the user was last on the corporate network using the Gpresult API (group policy)



How does Web Security Work?

- Authenticates and directs the user's external web traffic to ScanSafe's scanning infrastructure
- Numerous datacenters are located all over the world ensuring that users are never too far from ScanSafe's scanning services
- All web traffic is SSL encrypted for improved security over public networks
- Works with Full or Split Tunnel VPN clients (AnyConnect, or others)



AnyConnect 3.0 Features

Network Access Manager (NAM)

- Manage network connections on machine

DART

- Integrated troubleshooting info collection tool

Posture

- Cisco Secure Desktop with improved Cisco Secure Hosts Scan

Telemetry

- Reports PC virus infection from desktop AV to WSA



Wi-Fi Integration

- Wi-Fi integration is a common deployment method for retail & commercial enterprises who want to provide internet access to their customers
- Wi-Fi integration can be deployed in two ways:
 1. Fully managed by the hotspot provider (Cellular network and Internet Service Providers)
 2. Customer-managed Cisco solution



ISR G2 with ScanSafe - Concept

- The Connector will be available in IOS (universal) images with security feature set (SEC) licenses
- Supported on the 880, 890, 19xx, 29xx & 39xx/E ISR G2 platforms
- IOS ver 15.2(1)T
- Supports re-direction of HTTP/HTTPS traffic
- No need to install Connector on dedicated hardware, or make any browser changes/install AnyConnect on end users' machines





TrustSec Identity Services Engine

TrustSec [trəstsek]

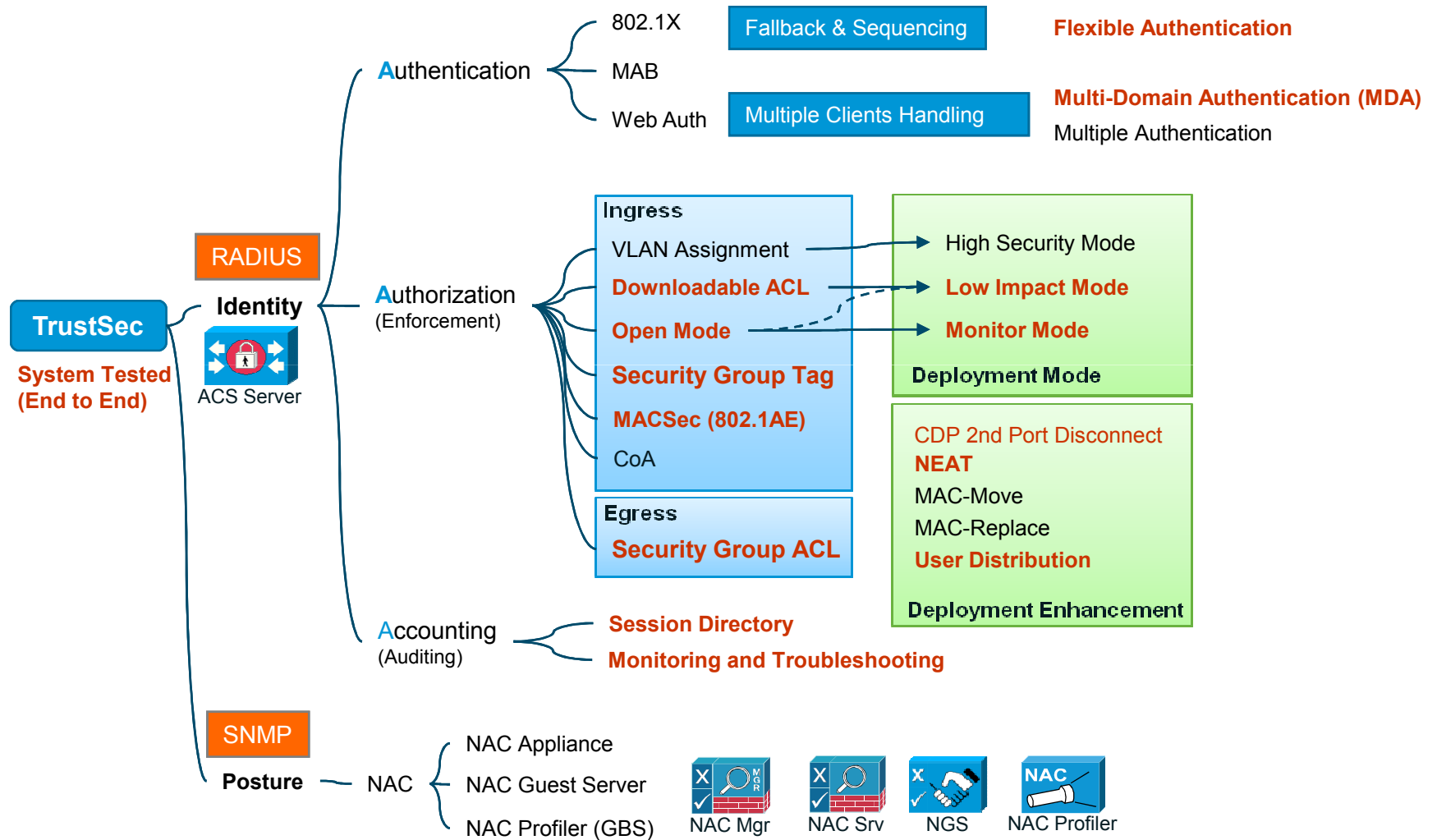
noun

1. A system that provides strong network access control and classification mechanisms using user and/or device identity and associated contexts
2. A system that provides variety of services that enhance overall network security
3. A system that provides segmentation mechanisms to control traffic from end user to destination resources

ORIGIN: CPS, CTS, IBNS, NAC, NPF, NAC Framework, NAC Appliance, OneNAC, NAC RADIUS

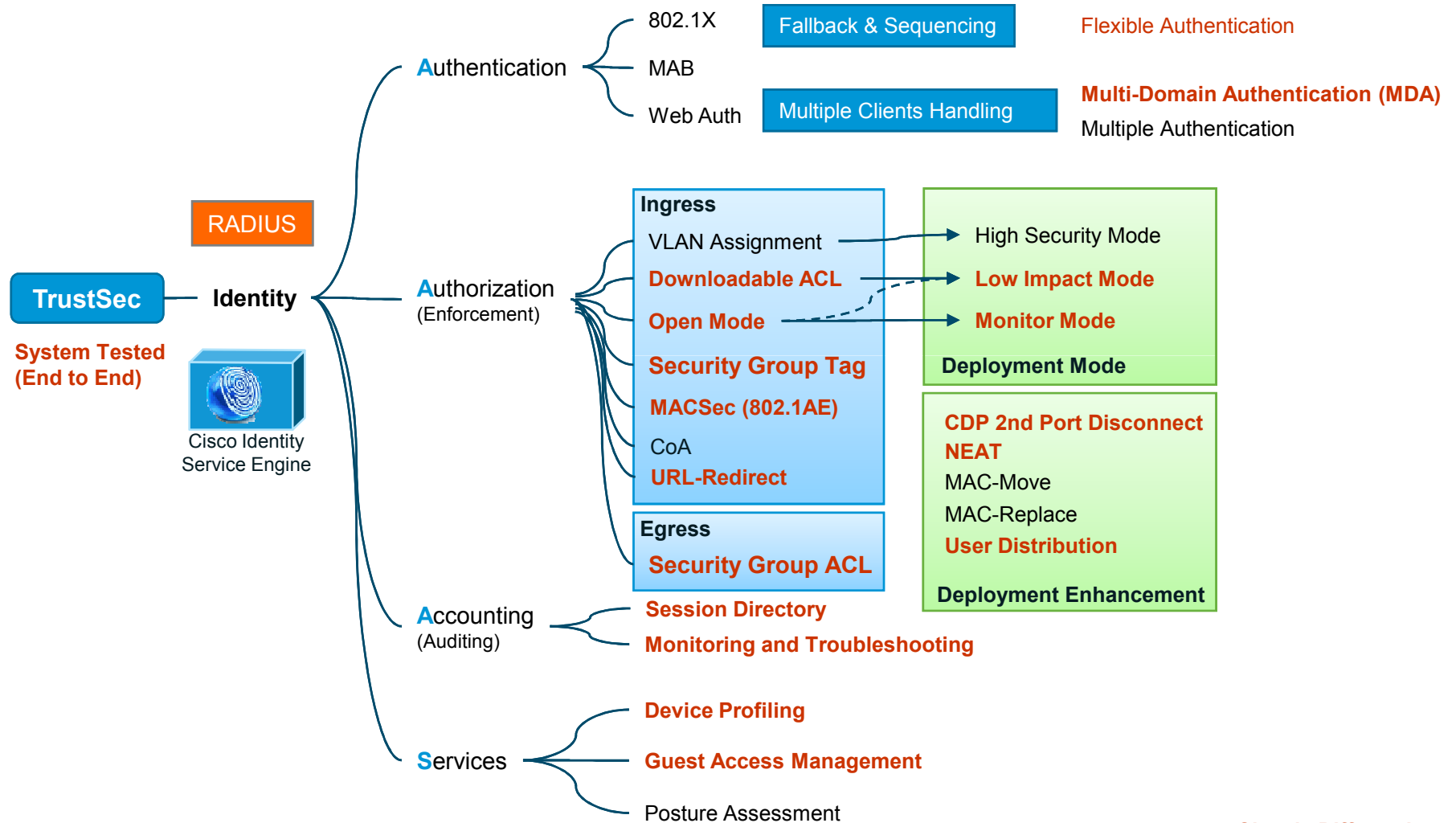


TrustSec 1.0



Cisco's Differentiator

TrustSec with ISE

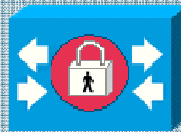


Cisco's Differentiator

Introducing Identity Services Engine

Next Generation PMBU Solution Portfolio

Identity & Access Control



Access Control Solution



NAC Manager NAC Server



NAC Profiler NAC Collector

Standalone appliance or
licensed as a module on
NAC Server



NAC Guest Server



ISE



NAC Agent

Guest Lifecycle Management

Robust UI

The screenshot displays the Cisco Policy Manager interface, showing a policy configuration screen. The main area is divided into sections for Rule Name, Identity Groups, Conditions, and Authorization Profiles. The 'Rule Name' section shows 'Compliant Employees' and 'Guest Authorization'. The 'Identity Groups' section shows 'SF Employees' and 'Select Group'. The 'Conditions' section shows 'No Conditions' and 'AccessMethod'. The 'Authorization Profiles' section shows 'Allow All', 'Internet Only', 'Printer Access', and 'Voice Access'. The interface includes a search bar, a 'Save' button, and a 'Cancel' button. The bottom status bar shows 'Alarms' with 5, 45, and 107 indicators.

Drag-and-Drop functionality for re-ordering rules

Reusable simple and compound 'Condition' objects

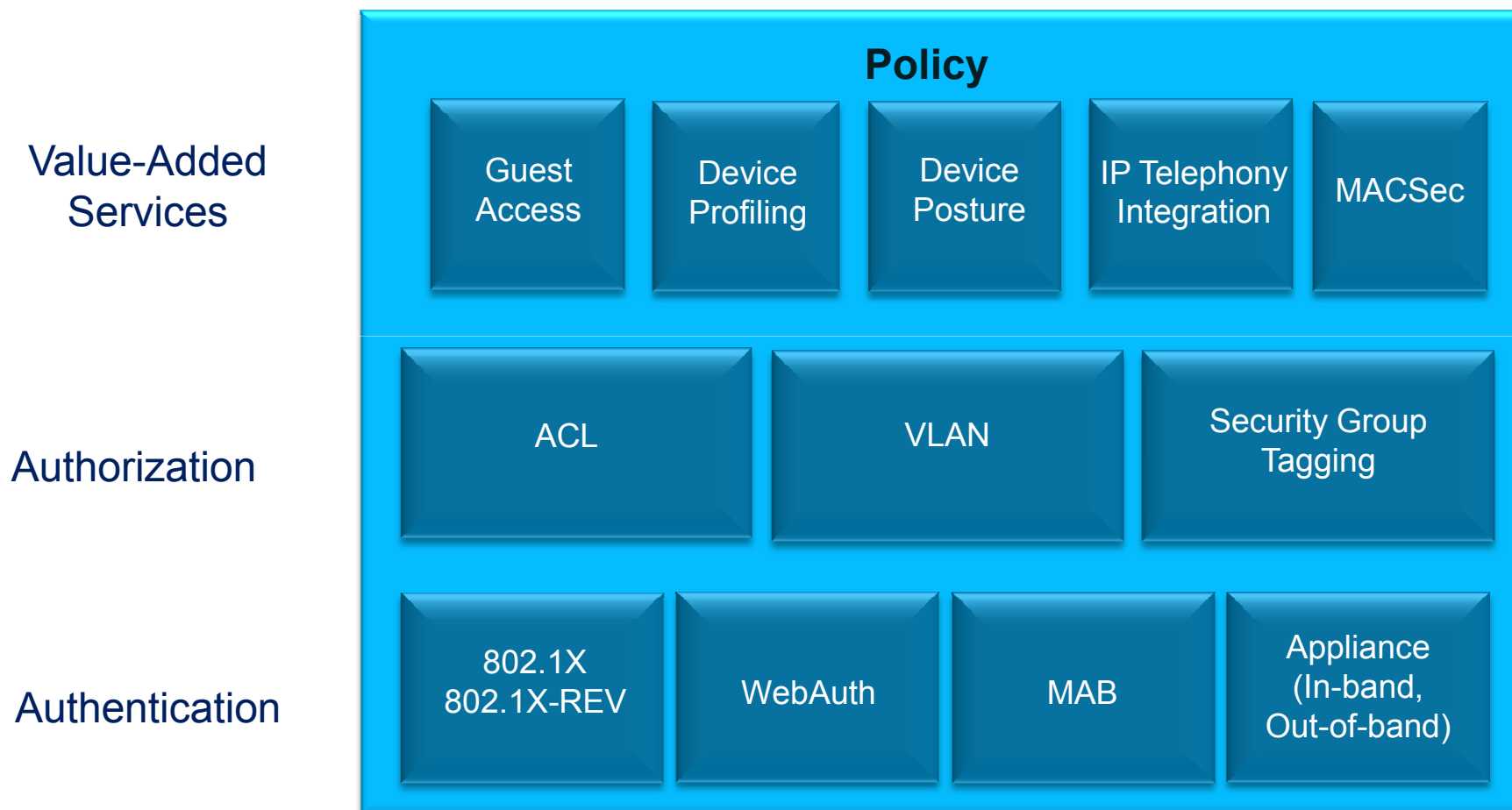
Tabular View is also available

In-context configuration of Identity Groups

New Identity Groups can be created without leaving Policy screen

Object Selector pop-up with search and filtering capabilities

Cisco TrustSec Architecture



Thank you.

