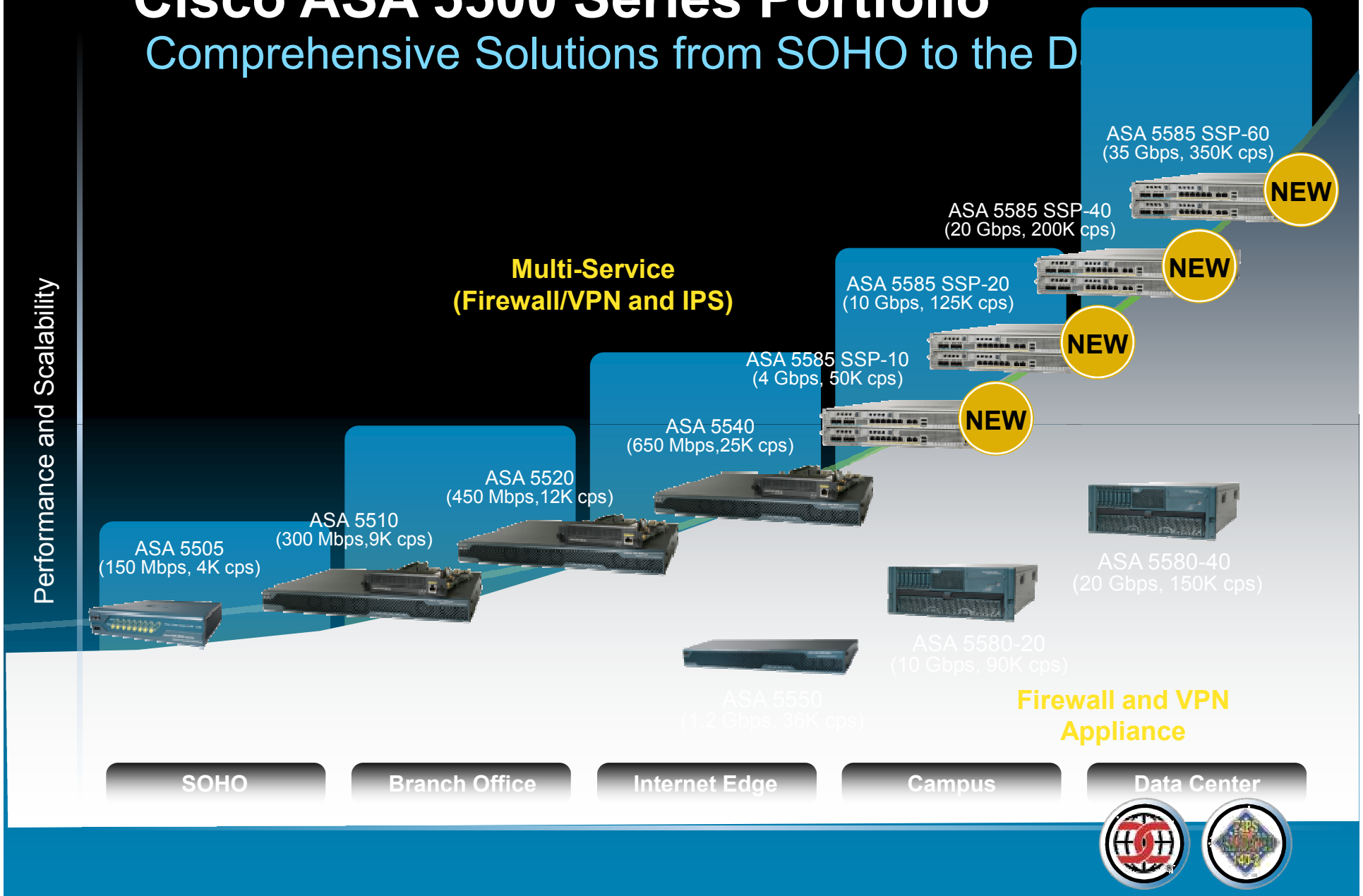
# Cisco Security update

Dragan Novaković, Security CCIE #26951

dnovakov@cisco.com

# Cisco ASA 5500 Series Portfolio

## Comprehensive Solutions from SOHO to the D



# Cisco ASA 5585 Series High-End Solutions


| Network Location | Internet Edge/ Campus ASA 5585 SSP-10 | Internet Edge/ Campus ASA 5585 SSP-20 | Campus/ Data Center ASA 5585 SSP-40 | Data Center ASA 5585 SSP-60 |
|---|---|---|---|---|
| **Performance** | | | | |
| Max Firewall | 4 Gbps | 10 Gbps | 20 Gbps | 35 Gbps |
| Max IPS | 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 |
| Packets/Second (64 byte) | 1,500,000 | 3,000,000 | 5,000,000 | 9,00,000 |
| 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 |

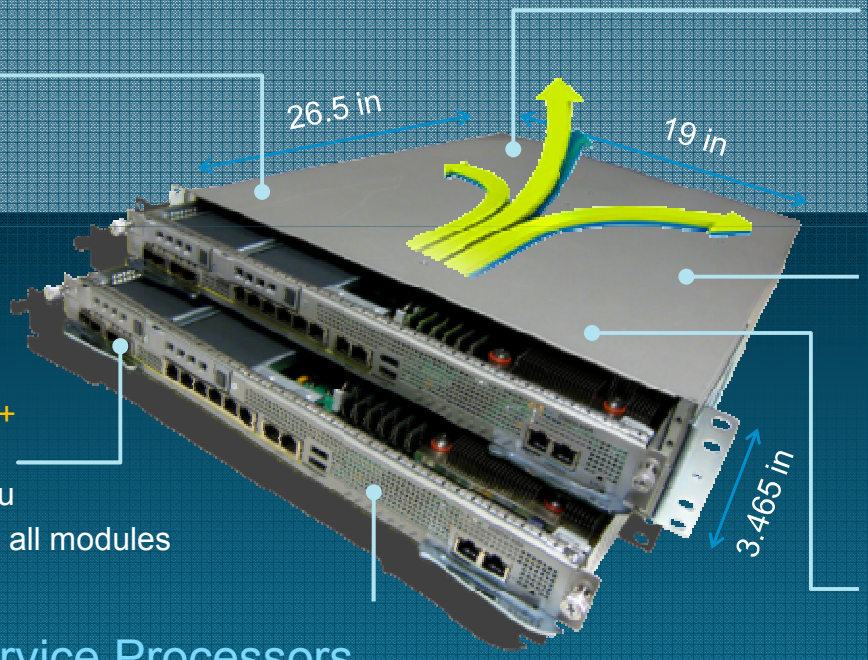
# High Performance Multi-Service Cisco ASA 5585-X Series

## 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



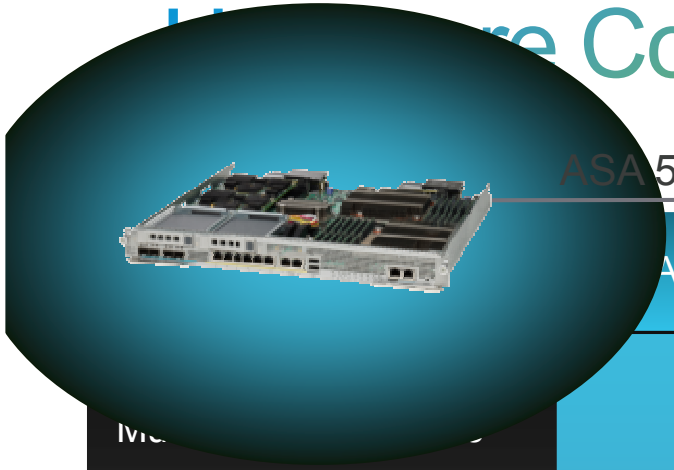

### Redundant Hot Swappable Power Supply Units
- Front to back air flow

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

### eUSB
- 2 GB internal
- Convenience storage
- Security credentials

Reference Slide

# ASA 5585-X Firewall/VPN Module
# Hardware Comparison

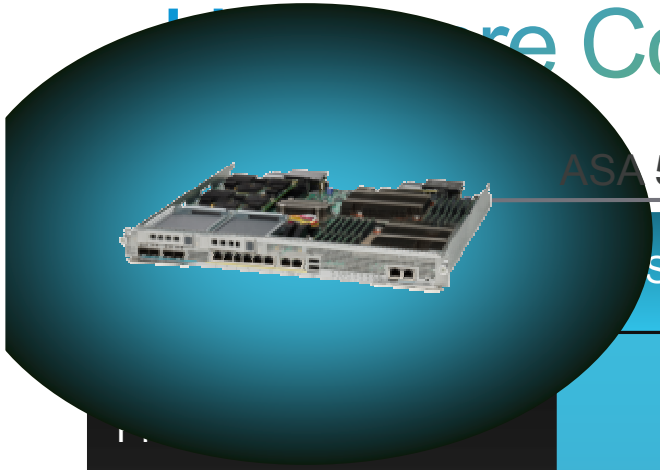


ASA 5585-X

| | A SSP-10 | ASA SSP-20 | ASA SSP-40 | ASA SSP-60 |
|---|---|---|---|---|
| Multi-core | 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+<br>8 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 2 x SFP+<br>8 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 4 x SFP+<br>6 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 4 x SFP+<br>6 x 1GbE Cu<br>2 x 1GbE Cu Mgmt |
| Crypto Chipset | Yes | Yes | Yes | Yes |

Reference Slide

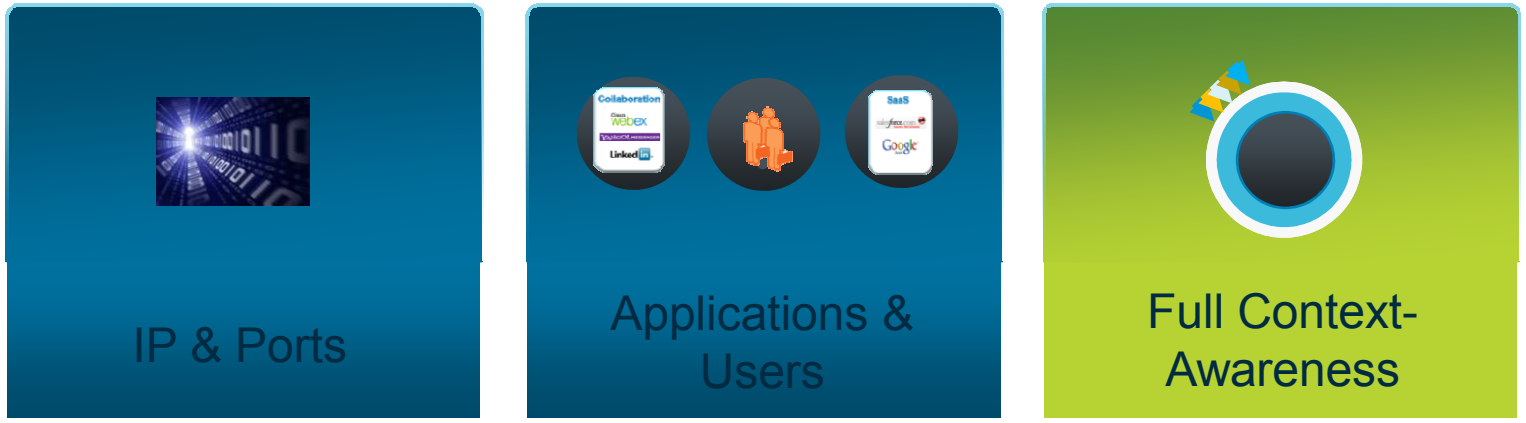
# ASA 5585-X IPS Module re Comparison



ASA 5585-X

| | S SSP-10 | IPS SSP-20 | IPS SSP-40 | IPS SSP-60 |
|---|---|---|---|---|
| | 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+<br>8 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 2 x SFP+<br>8 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 4 x SFP+<br>6 x 1GbE Cu<br>2 x 1GbE Cu Mgmt | 4 x SFP+<br>6 x 1GbE Cu<br>2 x 1GbE Cu Mgmt |

# Firewall Evolution



# Identity-Aware Firewall
## Key Benefits

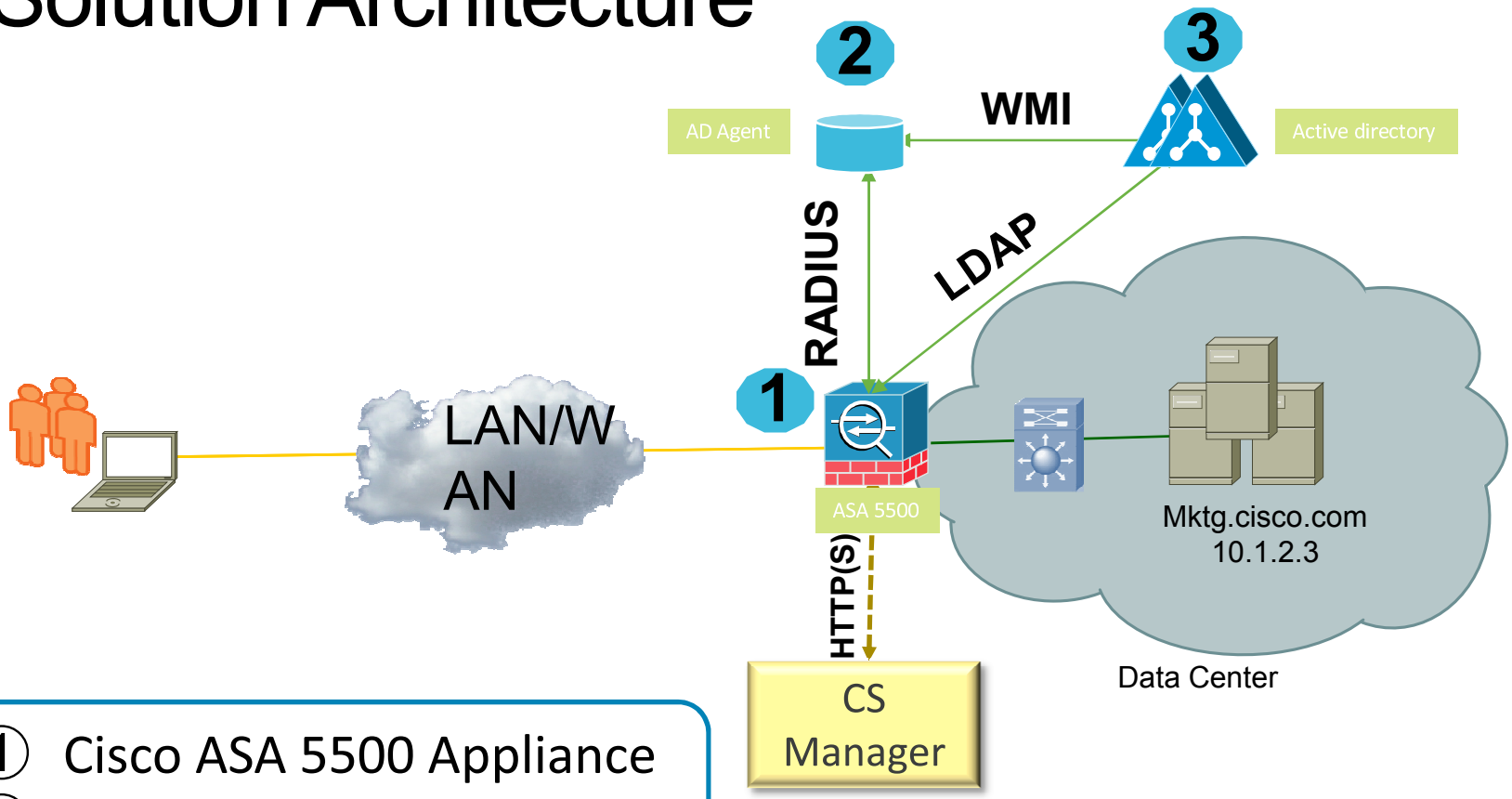
**Reduces operational complexity**

- 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

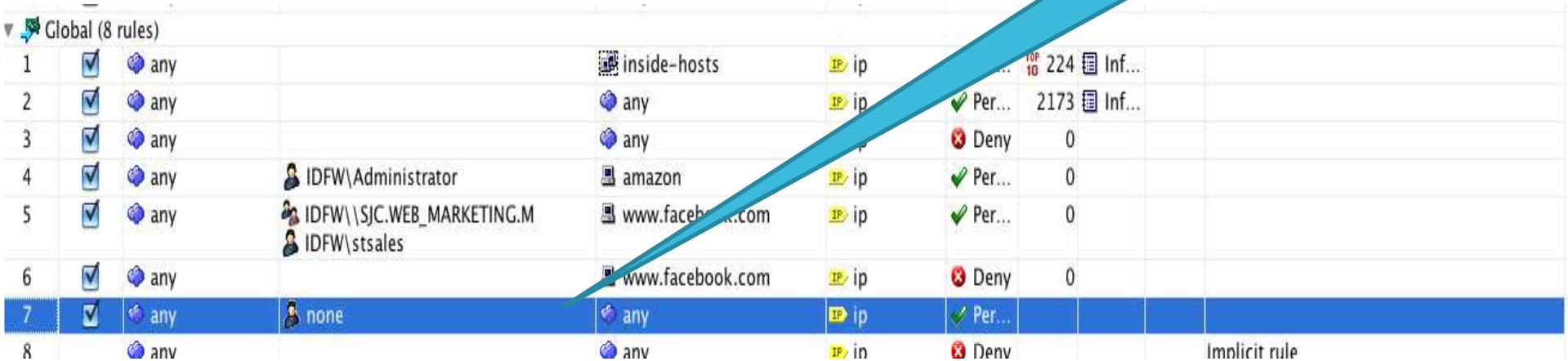



① Cisco ASA 5500 Appliance
② Off-box AD Agent
③ AD Domain Controllers

**Key Components**

# Configuration Example
# IDFW Access Control Rules

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



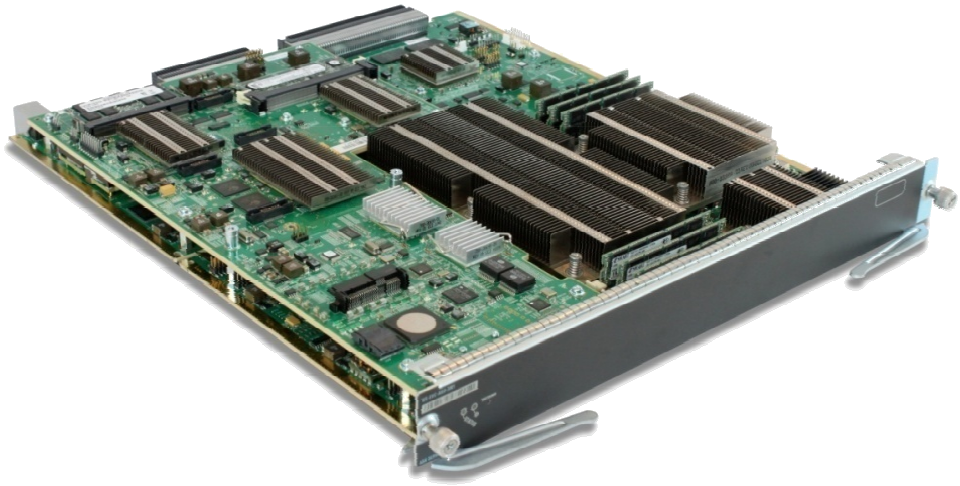

## CLI Commands

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

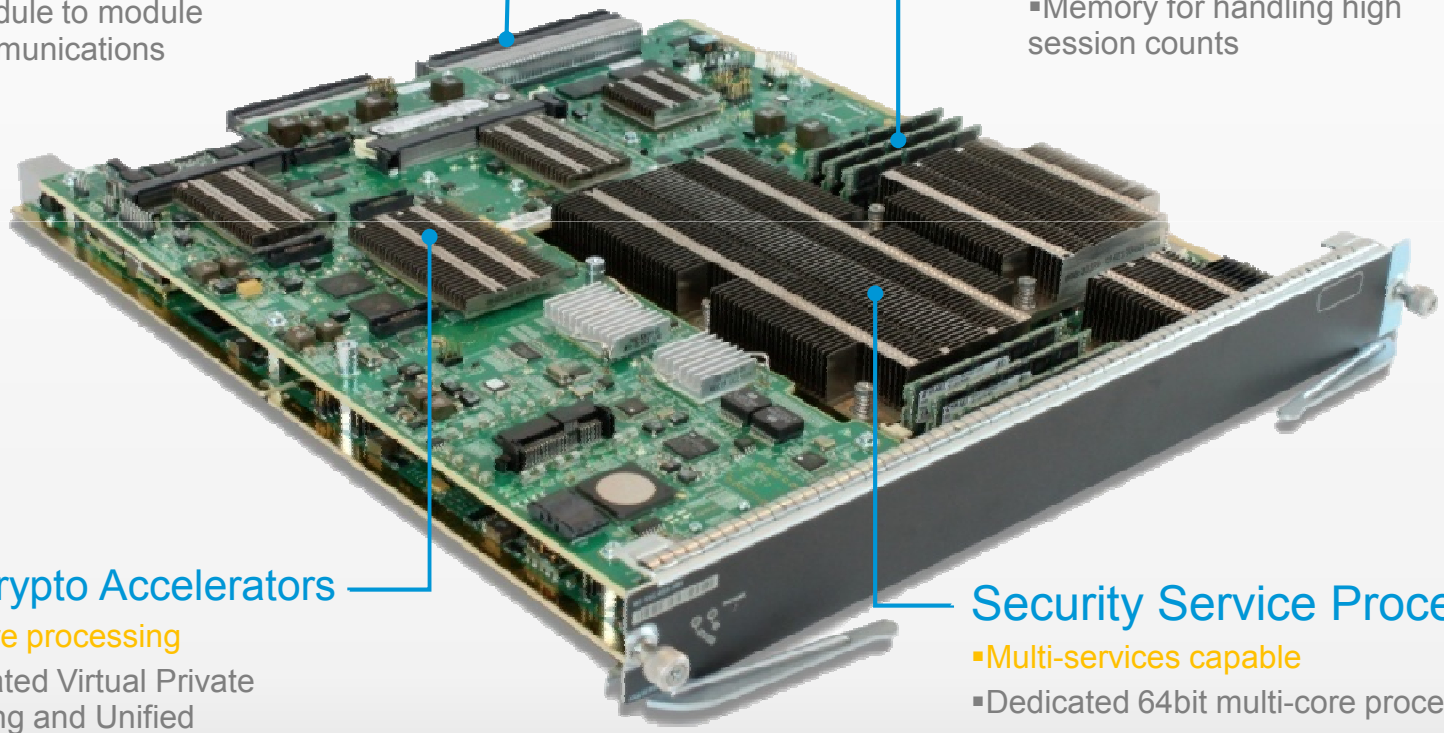


# ASASM / ASA-5585-X

# ASA 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 |

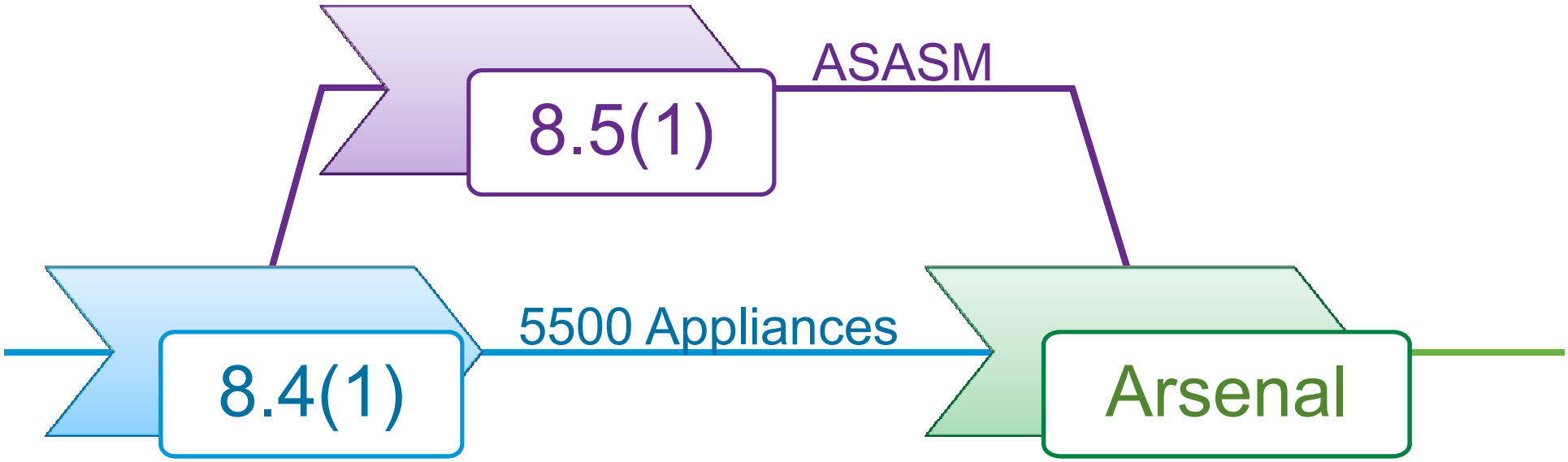
# Performance

| 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"*

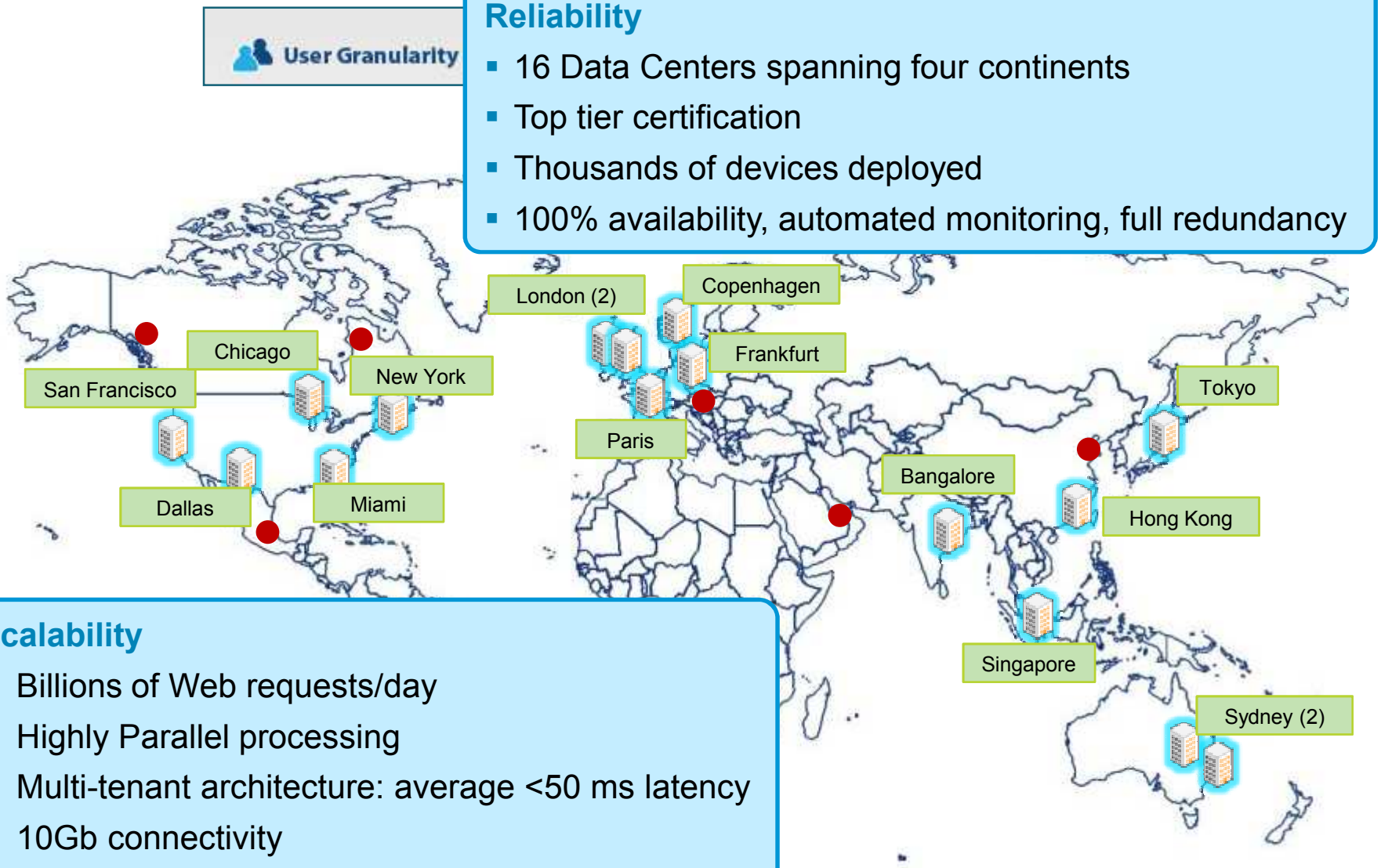
Gartner

## Customers

## Awards

## Partners

# Scalability & Reliability




**Reliability**

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

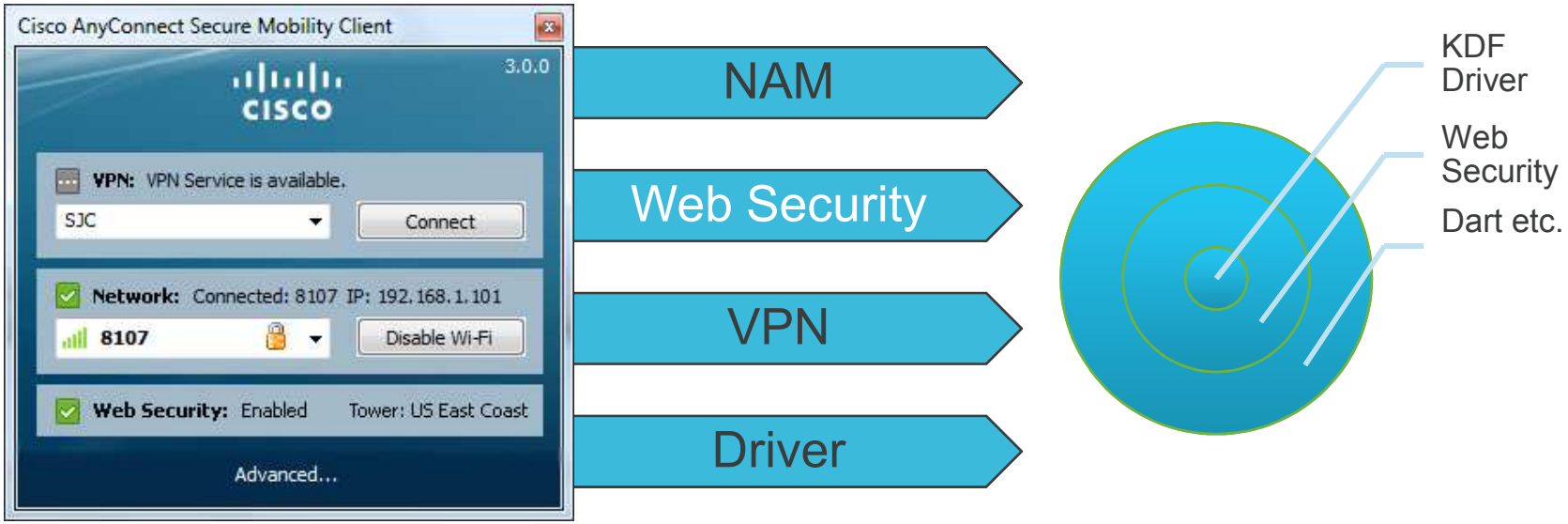
**Scalability**

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

**Centers planned**

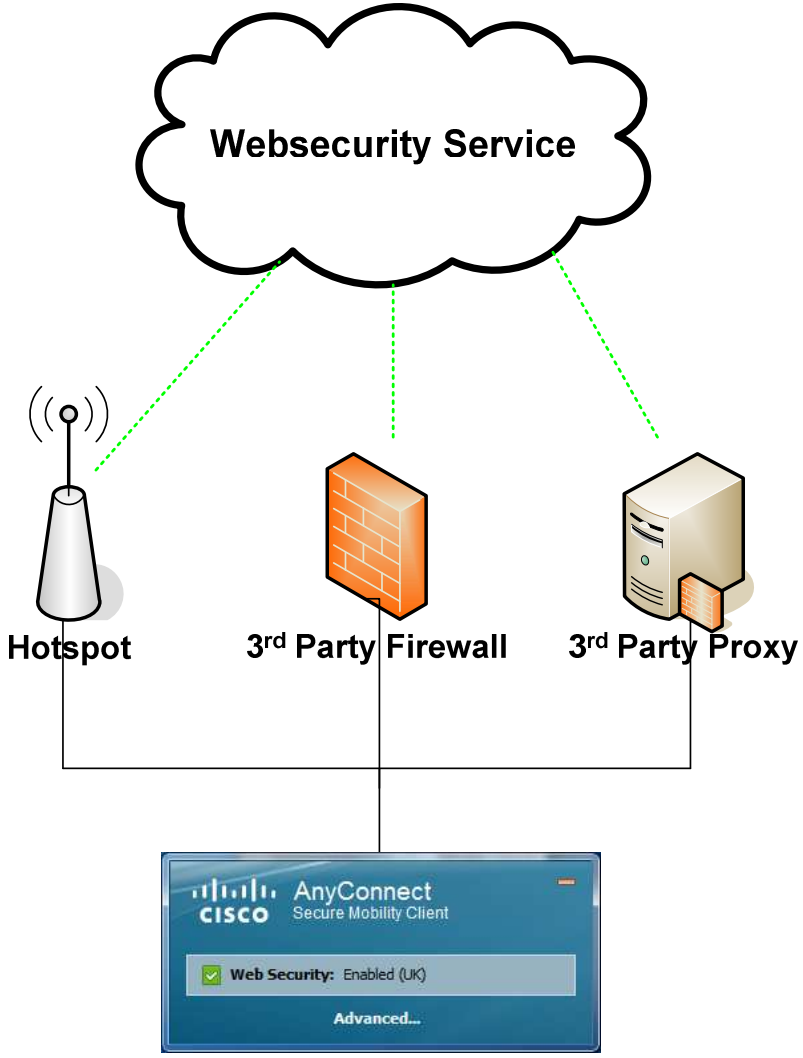
# What is Cisco Web Security?

- 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



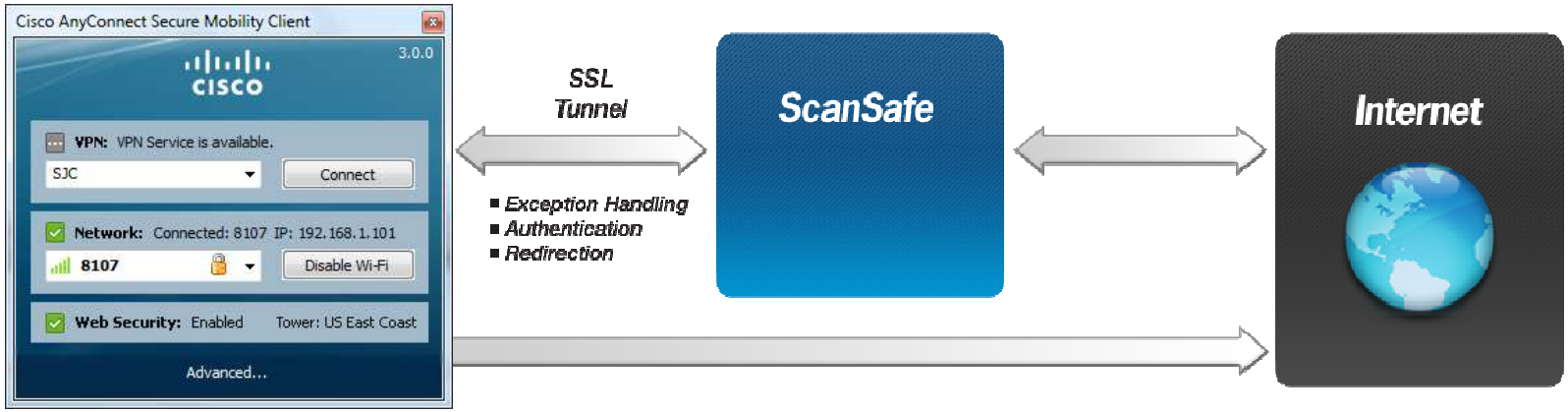
# Protecting Roaming Users - Web Security

- 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**

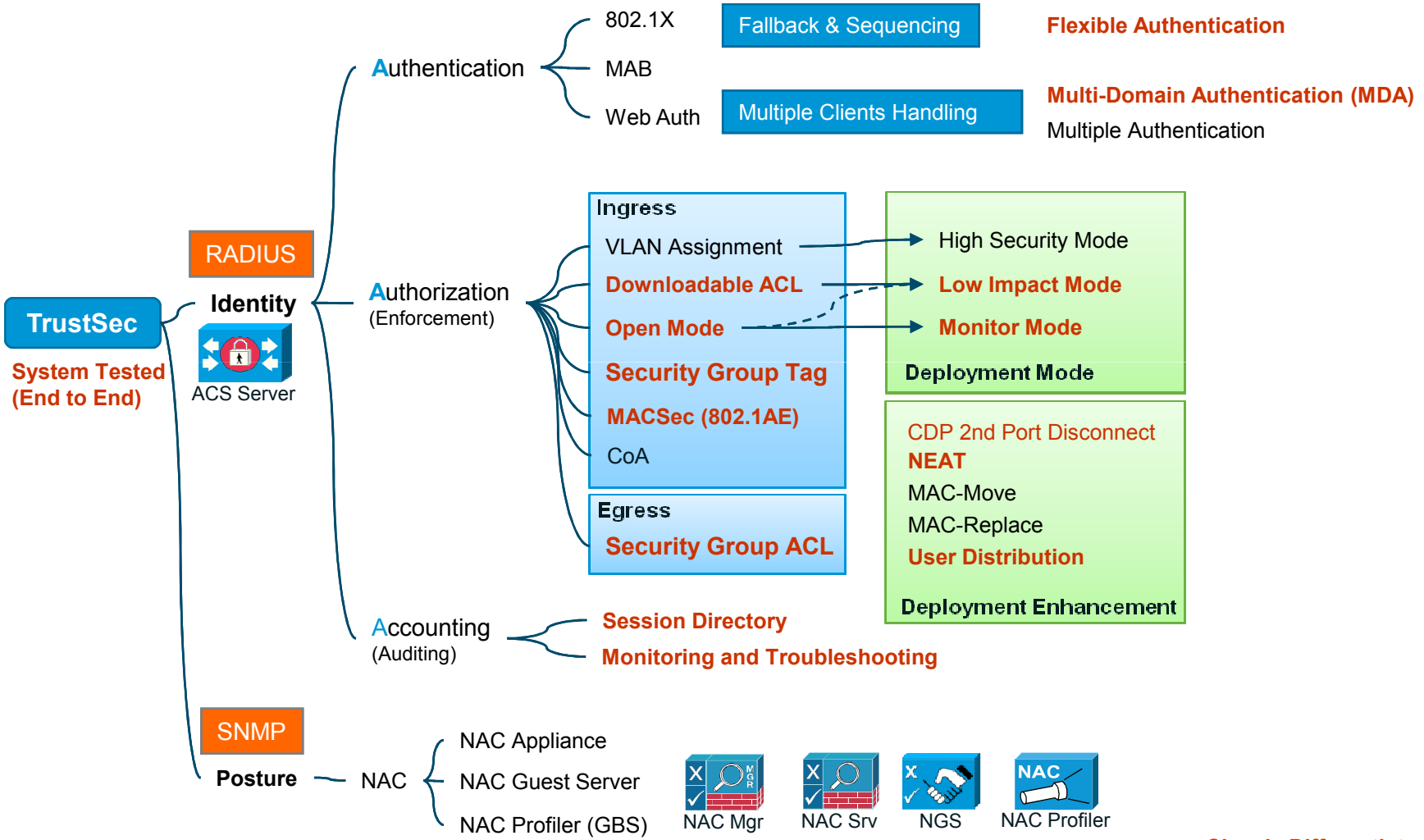
1. A system that provides strong network access control and classification mechanisms using user and/or device identity and associated contexts

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

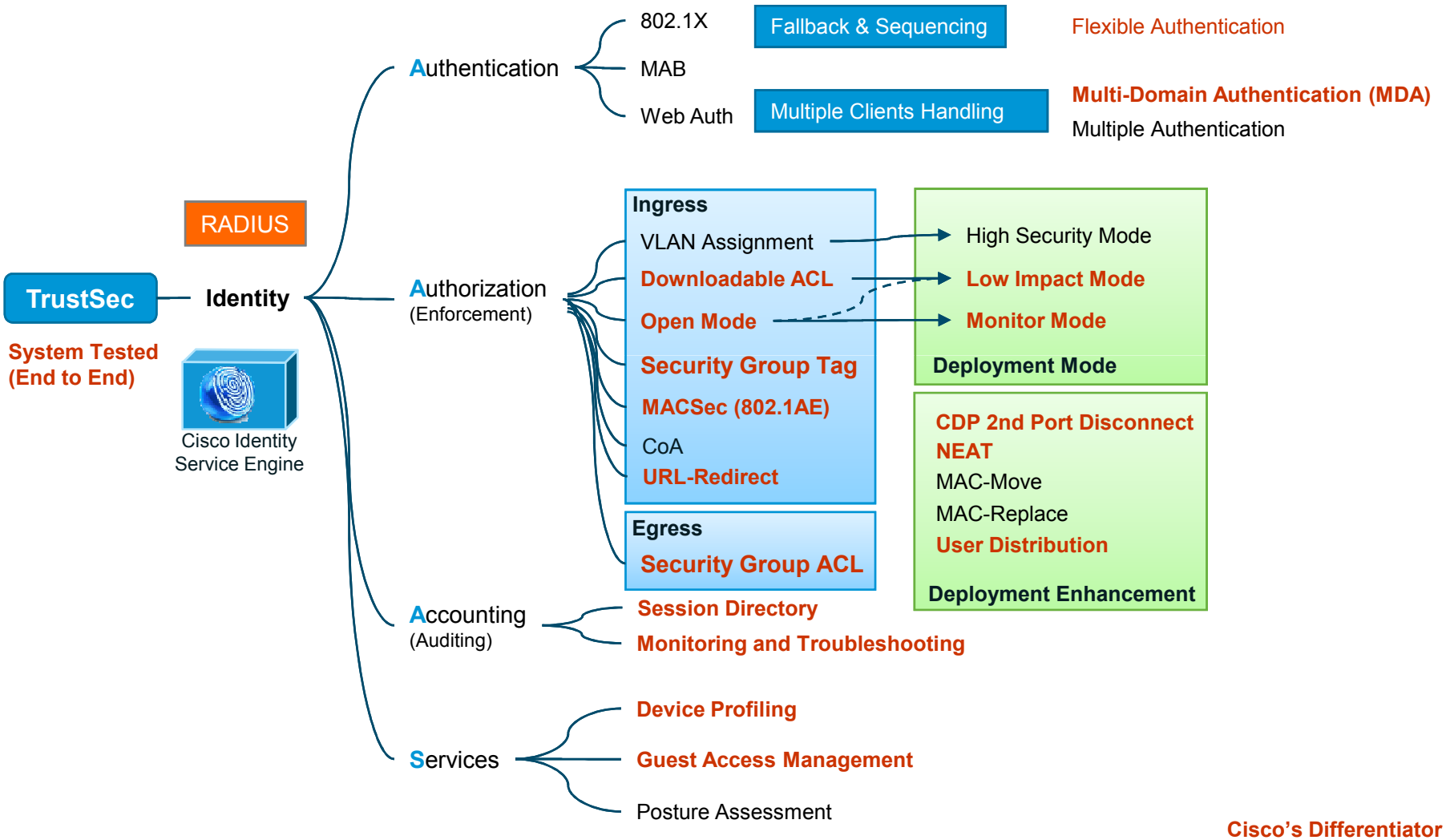
**ORIGIN: CPS, CTS, IBNS, NAC, NPF, NAC Framework, NAC Appliance, OneNAC, NAC RADIUS**

# TrustSec 1.0



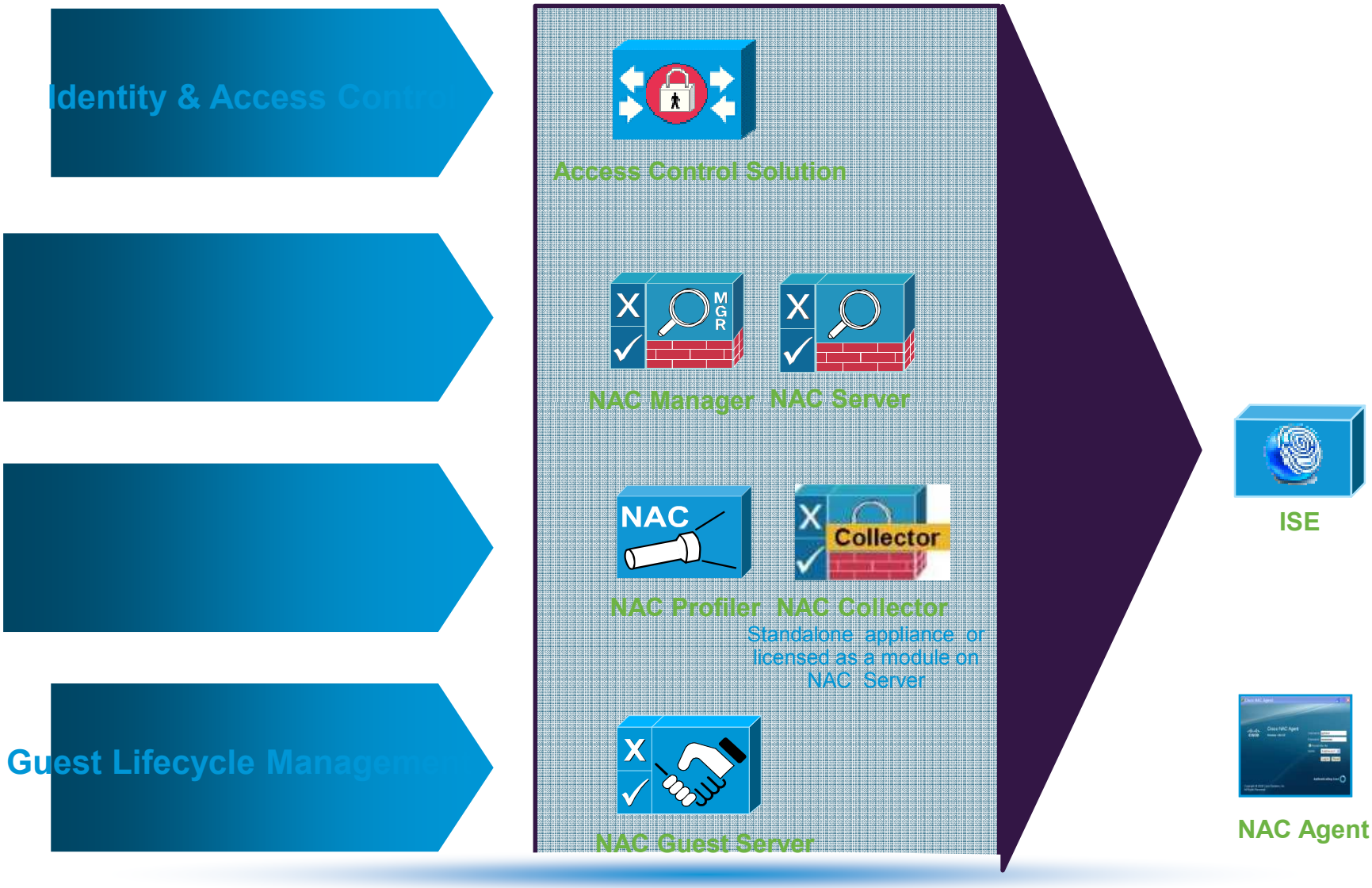

**Cisco's Differentiator**

# TrustSec with ISE

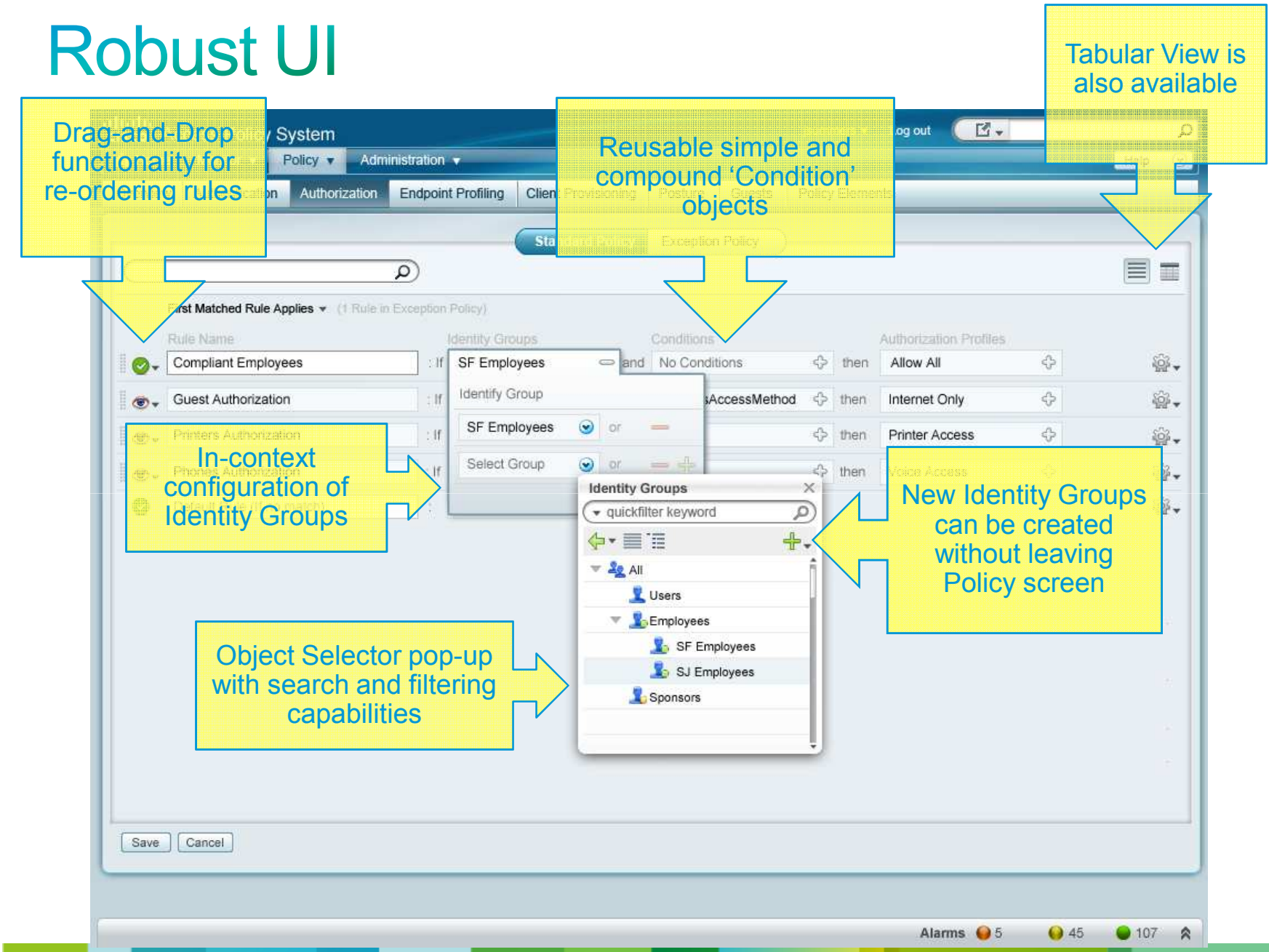


# Introducing Identity Services Engine

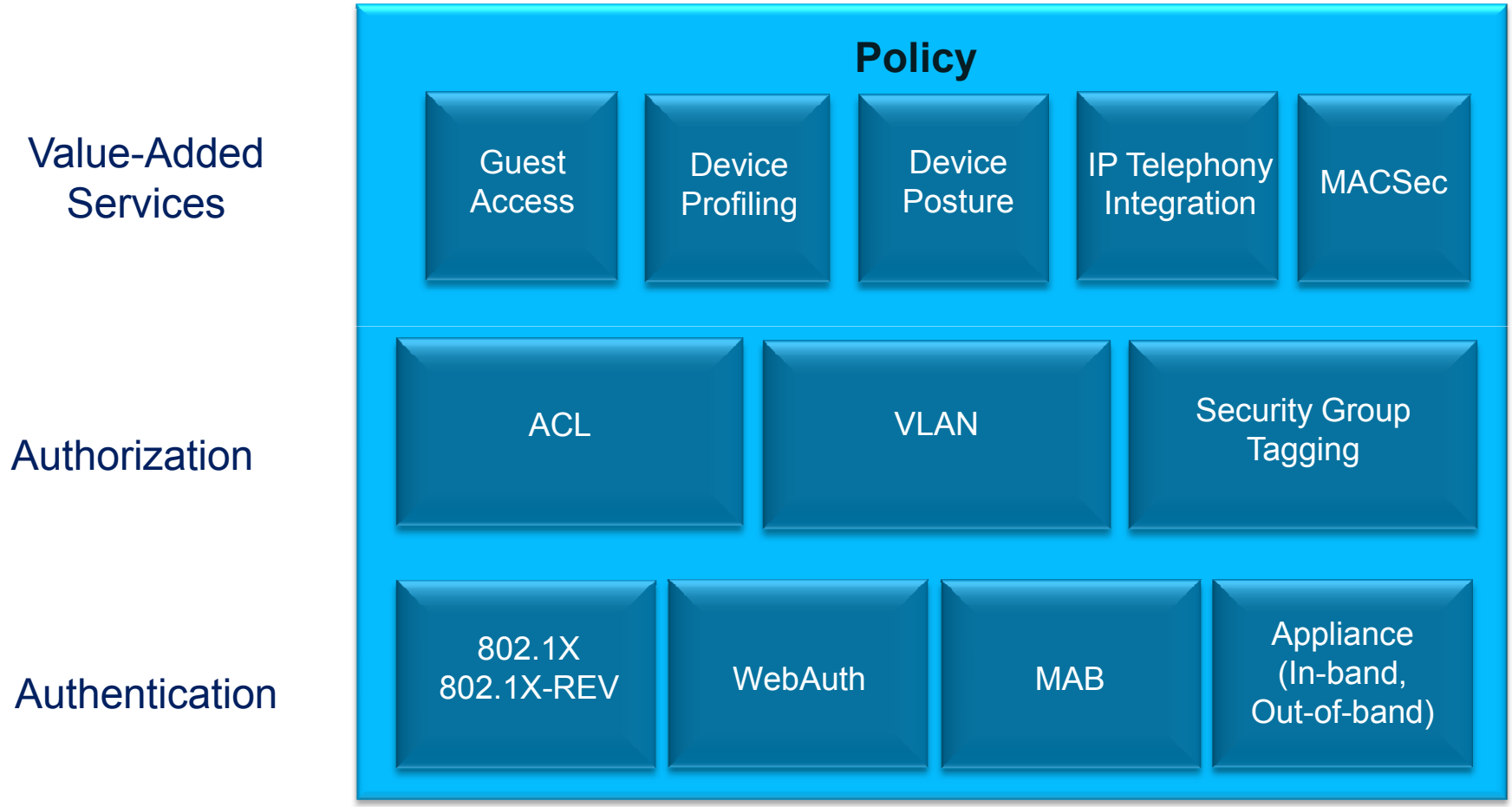
## Next Generation PMBU Solution Portfolio



# Robust UI



# Cisco TrustSec Architecture



Thank you.