Borderless Networks Update Finance Event 2010

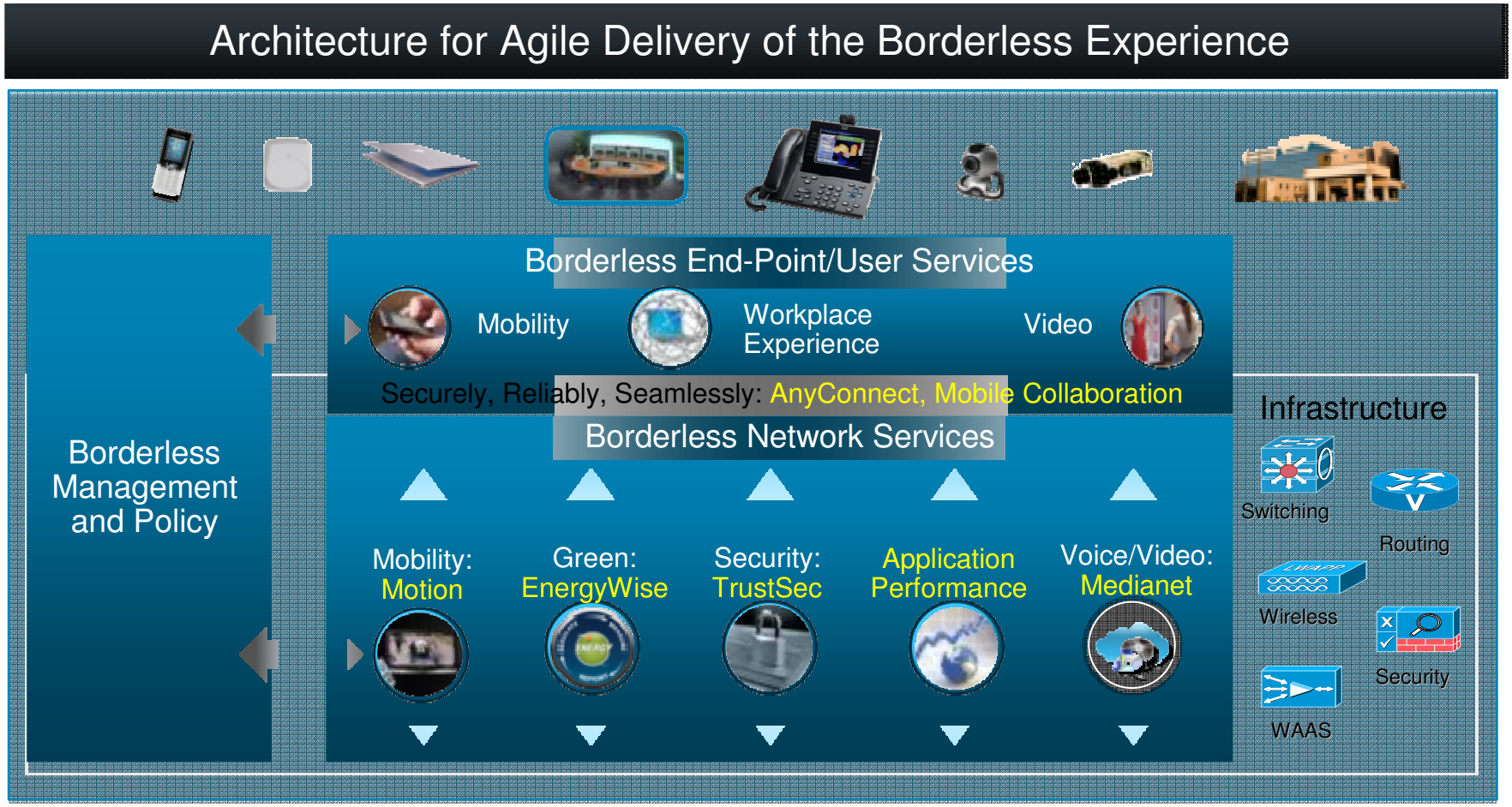
Tatjana Boskovic, Partner SE

tboskovi@cisco.com

Agenda

- Borderless networks – uvod
- EnergyWise
- Trustsec
- Secure Mobility
- Q&A

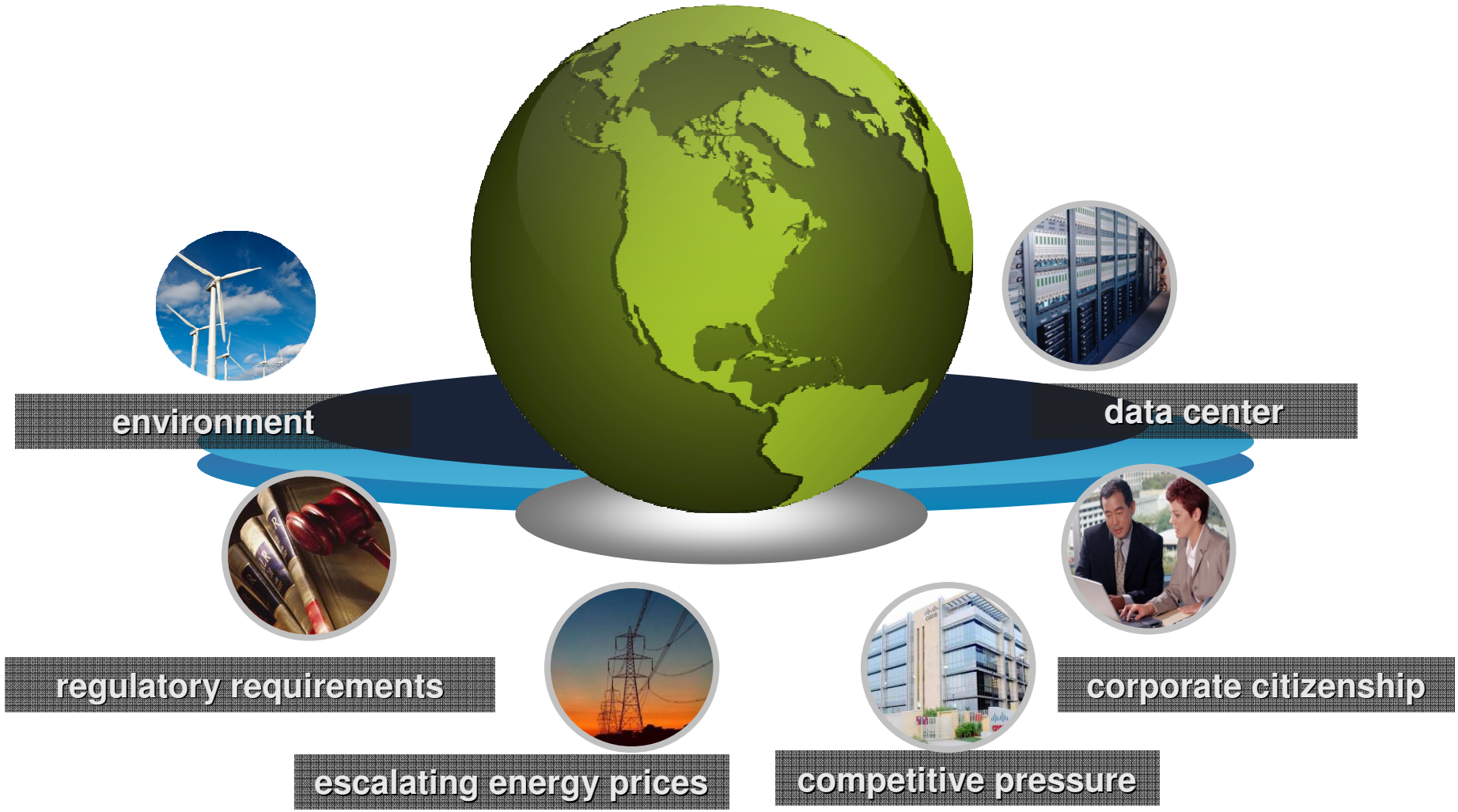
Cisco Borderless Network Architecture



Agenda

- Borderless networks – uvod
- EnergyWise
- Trustsec
- Secure Mobility
- Q&A

What is most important for your organization?



Cisco EnergyWise

- Customers want energy solutions from Cisco - Want to measure and control energy of IT and building systems
- Cisco responded by developing **EnergyWise**

  EnergyWise is a technology on foundation products (switches and routers)

  EnergyWise extends to non foundation products (PCs, building controls, anything that draws power)

  With 3rd Party Partners, Cisco can offer centralized monitoring, auditing and control of network attached devices

- **EnergyWise** enables the network as a platform for energy command and control
- **EnergyWise** is part of Cisco's Green solution

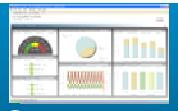
An EnergyWise Network

EnergyWise **Management Application**

EnergyWise **Management Communications** (TCP for Network-wide)

Domain—logical grouping of entities (child/ neighbor)

Endpoints are managed by policies and monitored for energy usage



Cisco® EnergyWise Orchestrator

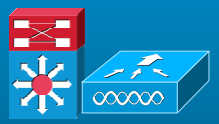
LMS

Third-Party Power Management Applications

SNMP

TCP

Management API



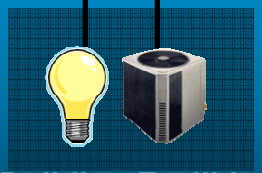
Wireless Controller

AP

EnergyWise Domain

PoE Devices

PCs and Laptops

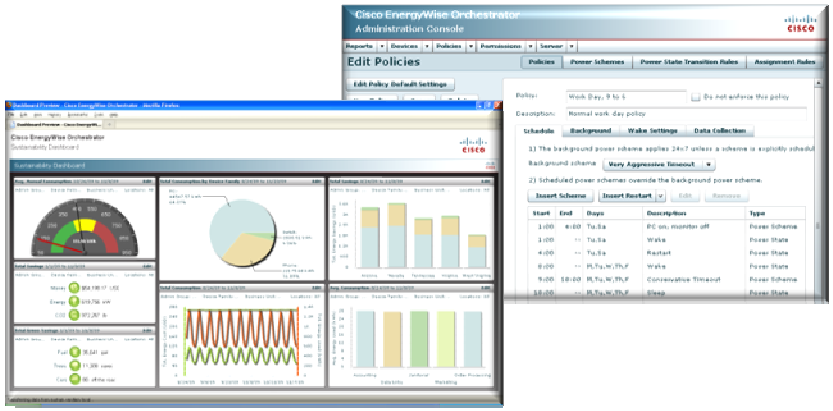


Building Facilities

EnergyWise Endpoints

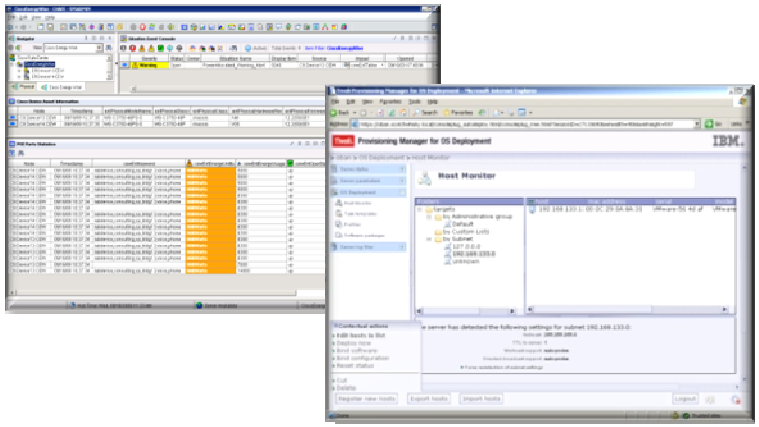
Current Cisco EnergyWise Management Options

Cisco® EnergyWise Orchestrator

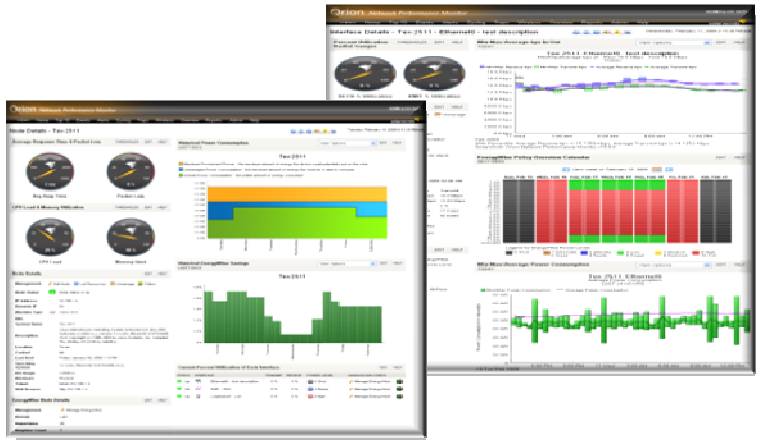


CiscoWorks LMS

IBM Tivoli Monitoring



SolarWinds Orion



Simple exercise

El análisis arroja que si se comparan los precios que paga por la electricidad el sector industrial en la región, Chile está entre los cuatro paises más caros. Para una tarifa de media tensión, que considera una demanda máxima de 300 KW, las empresas nacionales pagan US$0.1104 por KWh

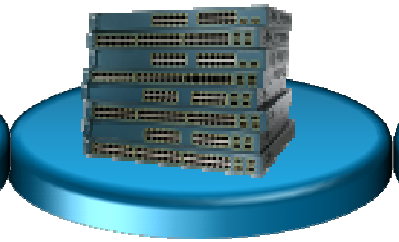
http://latercera.com/contenido/745_108593_9.shtml

- Company with 100 PoE 2960-24 switches, 1200 IP Phones 7911, 600 PC desktop, 600 laptops
- Target is to turn off 570 desktops (95%), 100 laptops (16%), and 1140 IP Phones (95%) after office hours (8pm to 7am .. or 12 hrs)…
- 2960 with 5% throughput, 50% PoE load ~ 160W
- 100 switches * 160W per hour= 16 kWh → 16 kWh → USD 15417/year
- 1200 7911 IP Phones @ 6.3W each → 7.5 kWh → USD 7227/year
- 600 desktops @ 180W each → 108 kWh → USD 104068/year
- 600 laptops @ 45W each → 27 kwH → USD 26017/year
- TOTAL BEFORE ENERGYWISE = USD 152729/year
- TOTAL AFTER ENERGYWISE = USD 55061/year → SAVINGS 64% (~ 100K USD/year)

Cisco EnergyWise Platform and Cisco IOS Software Support

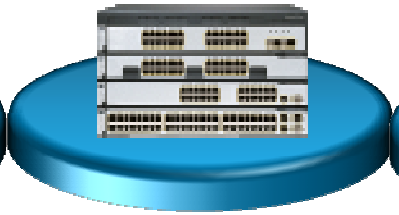
Cisco Catalyst® 2900 including compact switches

Cisco IOS® Software 12.2(50)SE and LAN Lite feature set or higher



Cisco Catalyst 3560-E and 3560 including compact switches

Cisco IOS Software 12.2(50)SE and LAN Base feature set or higher



Cisco Catalyst 3750-E and 3750

Cisco IOS Software 12.2(50)SE and LAN Base feature set or higher

Cisco Catalyst 4500 and 4900

Cisco IOS Software 12.2(52)SG and LAN Base feature set or higher

Cisco Catalyst 6500

Cisco IOS Software 12.2(33)SXI4 or higher

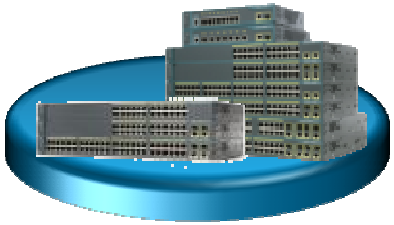
EtherSwitch modules

Cisco IOS Software 12.2(50)SE or higher

Cisco® 1900, 2900, and 3900 Series Integrated Services Routers

ISR G2

Cisco IOS Software 15.0(1)M3 and Universal IP Base feature set or higher



Cisco Catalyst 2960-S

Cisco IOS Software 12.2(53)SE2 and LAN Lite feature set or higher

Cisco Catalyst 3750-X and 3560-X

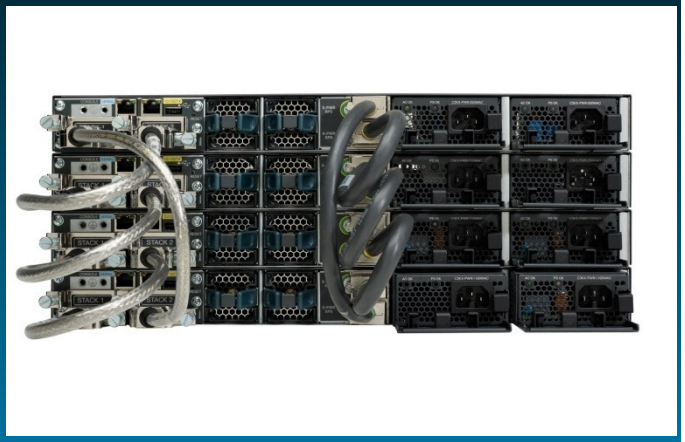
Cisco IOS Software 12.2(53)SE2 and LAN Base feature set or higher

Introducing Catalyst 3750-X & 3560-X

Innovation Leadership: What's New

- 24/48 10/100/1000 ports
- Seamless upgrades from 4x1G to 2x10G
  - No special hardware required, just replace the optics
- StackPower Technology – Industry First
  - Distributes power in the stack where it is needed
- Dual Field Replaceable Power Supplies/Fans
  - Switch can be upgraded and serviced in the field
- TrustSec Enabled
  - Provides advanced authentication and adds encryption on user-facing ports
- Full 802.3at PoE+ Support
  - Standards based power delivery up to 30 watts per port supporting next-generation high-power devices
- Enhanced Limited Lifetime Hardware Warranty
  - NBD delivery where available
  - 90-day 8x5 TAC support

New



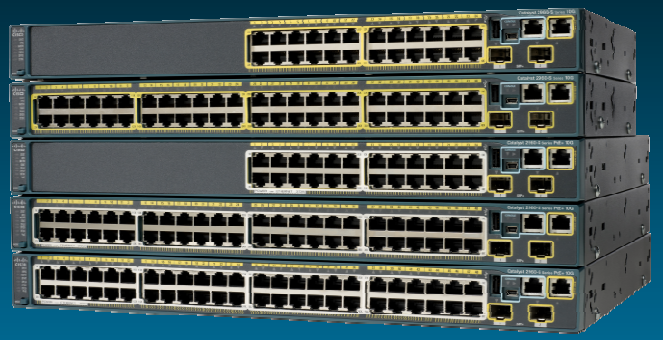
- **3 Software Options: LAN Base, IP Base, IP Services**
  - **Flexible software features and lower entry level pricing**

Introducing Catalyst 2960-S

Mainstream Features in a Cost Optimized Platform

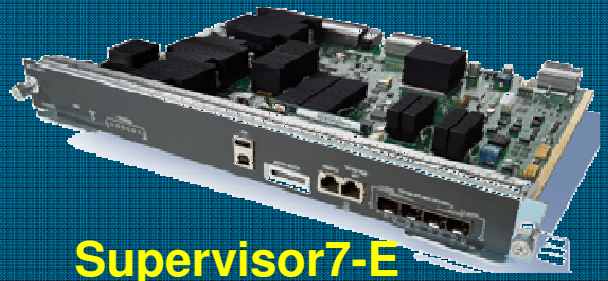
- 24/48 10/100/1000 ports with fixed uplinks
- Fixed Uplink Options: 4x1G or 2x10G SFP+
  - 10 Gigabit Ethernet in a cost optimized platform
- FlexStack Technology
  - Brings stackable ease-of-use features to the 2960 family, features 20G stacking links
- Power over Ethernet
  - Full standards-based PoE on every port
  - PoE+ support for next-generation high-power devices
- Cisco Online Diagnostics & Onboard Fault Logging
  - Hardware innovations that deliver preventative early fault detection
- Enhanced Limited Lifetime Hardware Warranty
  - NBD delivery where available
  - 90-day 8x5 TAC support

New



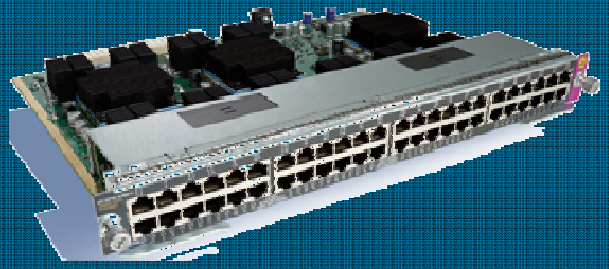
- **LAN Lite and LAN Base Software Options**
- **LAN Lite option provides entry-level Gig-E platform**

Next Generation Catalyst 4500E System



Supervisor7-E

848Gbps Switching Capacity
48G/slot
Rich hardware features
(FnF, TrustSec, Wireless, ERSPAN,
Tunneling, VRF-NG, VSS and more…

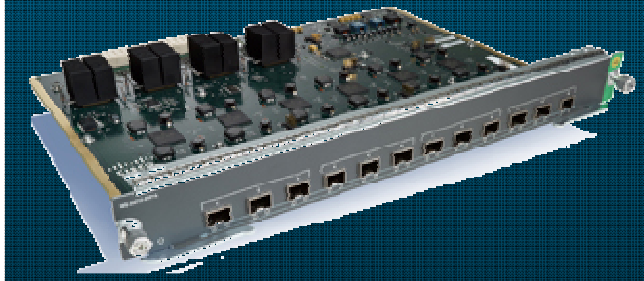


WS-X4748-RJ45V+E

48p 10/100/1000 non-blocking
30W/port (PoE+) on all 48 ports
Cisco TrustSec in Hardware

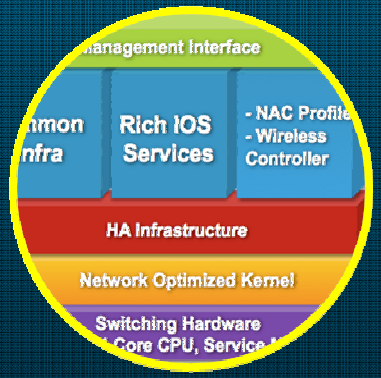
Catalyst 4500E and 4500E+ Chassis

Forward and backward compatible
48G/slot
Lifecycle till year 2020



WS-X4712-SFP+E

12 PORT 10GE 2.5:1 Line Card
Cisco Trustsec in
HardwareSFP+ SR modules
(Lower power mode)



Cisco IOS XE

Modern OS to support multi-core CPU
IOS investment protection
Enabling Open Service Platform

CiscoWorks LMS 4.0

A New Management Paradigm

Seamless end-to-end management

Complete Life Cycle Management

- Monitoring, troubleshooting, configuration

Simplified Deployment

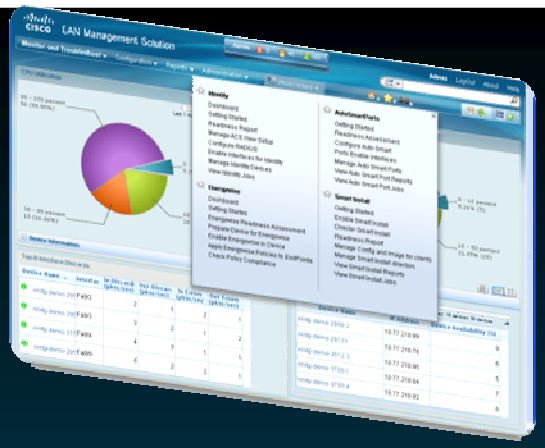
- Work Centers for EnergyWise, TrustSec/Identity, Auto Smartports

Comprehensive Device Coverage

- Day-one device support for over 560 Cisco devices

Open Extensible Framework

- Integration with CMDB, trouble ticketing and other SNMP-based management platforms



Simplified monitoring, deployment, and troubleshooting

- ISR G2
- Catalyst 2960-S
- Catalyst 3560-X, 3750-X
- Catalyst 4500-E

Cisco ASR 1001

Superior density and performance for mission–critical data centers

Smallest footprint (1RU) with largest number of on-demand services

- Up to **5G** integrated Borderless Network Services: Security, Application Performance, Voice/Video
- Integrated ESP, RP, and SIP

On-demand Performance Upgrade

- ESP throughput can be upgraded from 2.5G to 5G with no additional HW via a license

Simplified provisioning and deployment

- New Branch and WAN services enabled via software licenses

Software redundancy on non-redundant hardware

- Active and standby IOS versions on same hardware

Industry's most-compact high performance router

- Purpose built for high-end branch, managed services
- Feature parity with ASR 1k family
- Same I/O SPA support

Agenda

- Borderless networks – uvod
- EnergyWise
- Trustsec
- Secure Mobility
- Q&A

Security Challenges

Who? Identify users and provide differentiated access in a dynamic, borderless environment

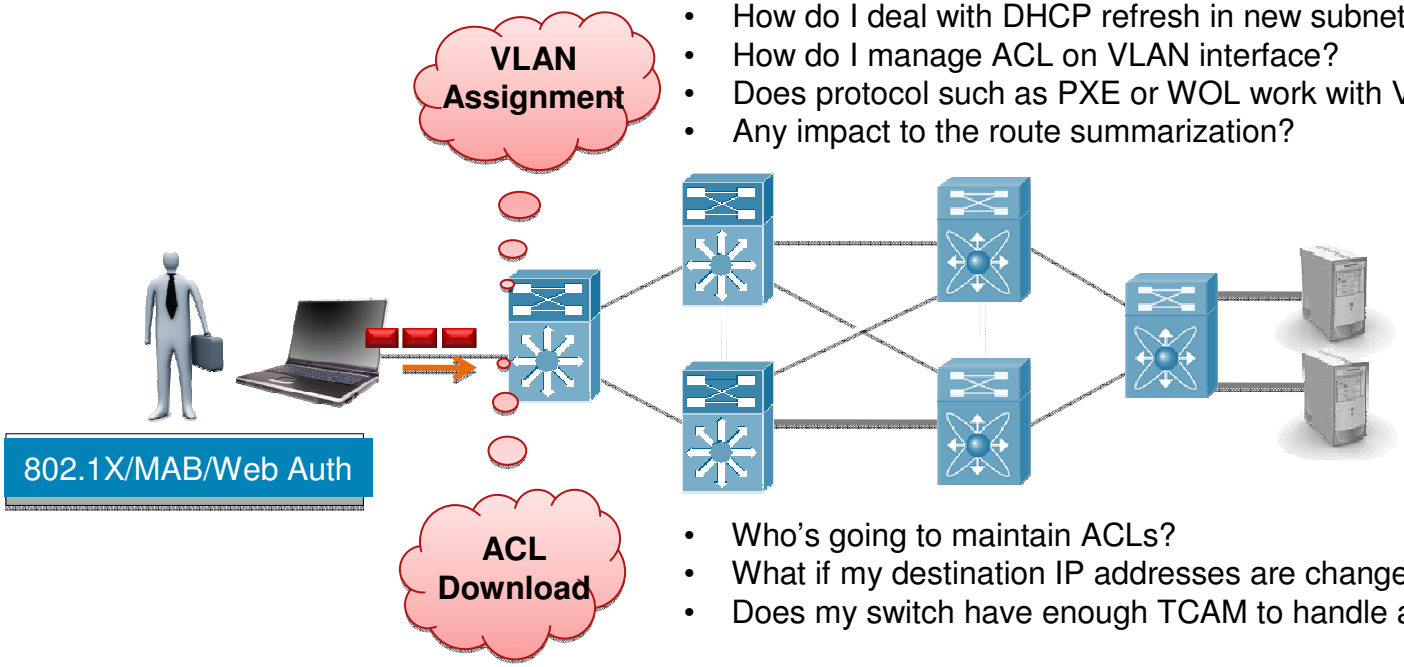
What ? Devices are proliferating, including network capable purpose-built devices.

Where ? Traditional borders are blurred. Access is possible from anywhere.

How ? Establish, monitor, and enforce consistent global access policies

Challenge of Ingress Access Control

- Can I create / manage the new VLANs or IP Address scope?
- How do I deal with DHCP refresh in new subnet?
- How do I manage ACL on VLAN interface?
- Does protocol such as PXE or WOL work with VLAN assignment?
- Any impact to the route summarization?



- Who's going to maintain ACLs?
- What if my destination IP addresses are changed?
- Does my switch have enough TCAM to handle all request?

- Traditional access authorization methods leave some deployment concerns
  - Detailed design before deployment is required, otherwise…
  - Not so flexible for changes required by today's business
  - Access control project ends up with redesigning whole network

Cisco TrustSec

- **TrustSec is a broad umbrella** for security improvements based on the **capability to strongly identify users, hosts and network devices within a network**
- TrustSec provides **topology independent and scalable access controls** by uniquely classifying data traffic for a particular role
- TrustSec **ensures data confidentiality and integrity** by establishing trust among authenticated peer and encrypting links with those peers

What TrustSec Does

NAC Appliances

802.1x/Infrastructure

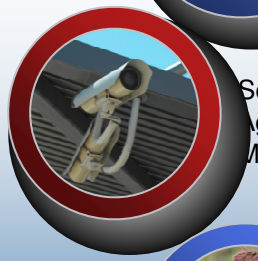
Identity Information

Other Conditions

Authorization (Controlling Access)

Vicky Sanchez
Employee, Marketing
Wireline
3 p.m.

Frank Lee
Guest
Wireless
9 a.m.



Security Camera G/W
Agentless Asset
MAC: F5 AB 8B 65 00 D4

Francois Didier
Consultant
HQ—Strategy
Remote Access
6 p.m.

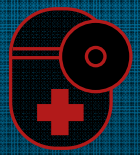
Group:
Full-Time Employee

Group:
Contractor

Group:
Guest

+

Time and Date



Posture

Location

Device Type

Access Type

Broad Access

Limited Access

Guest/Internet

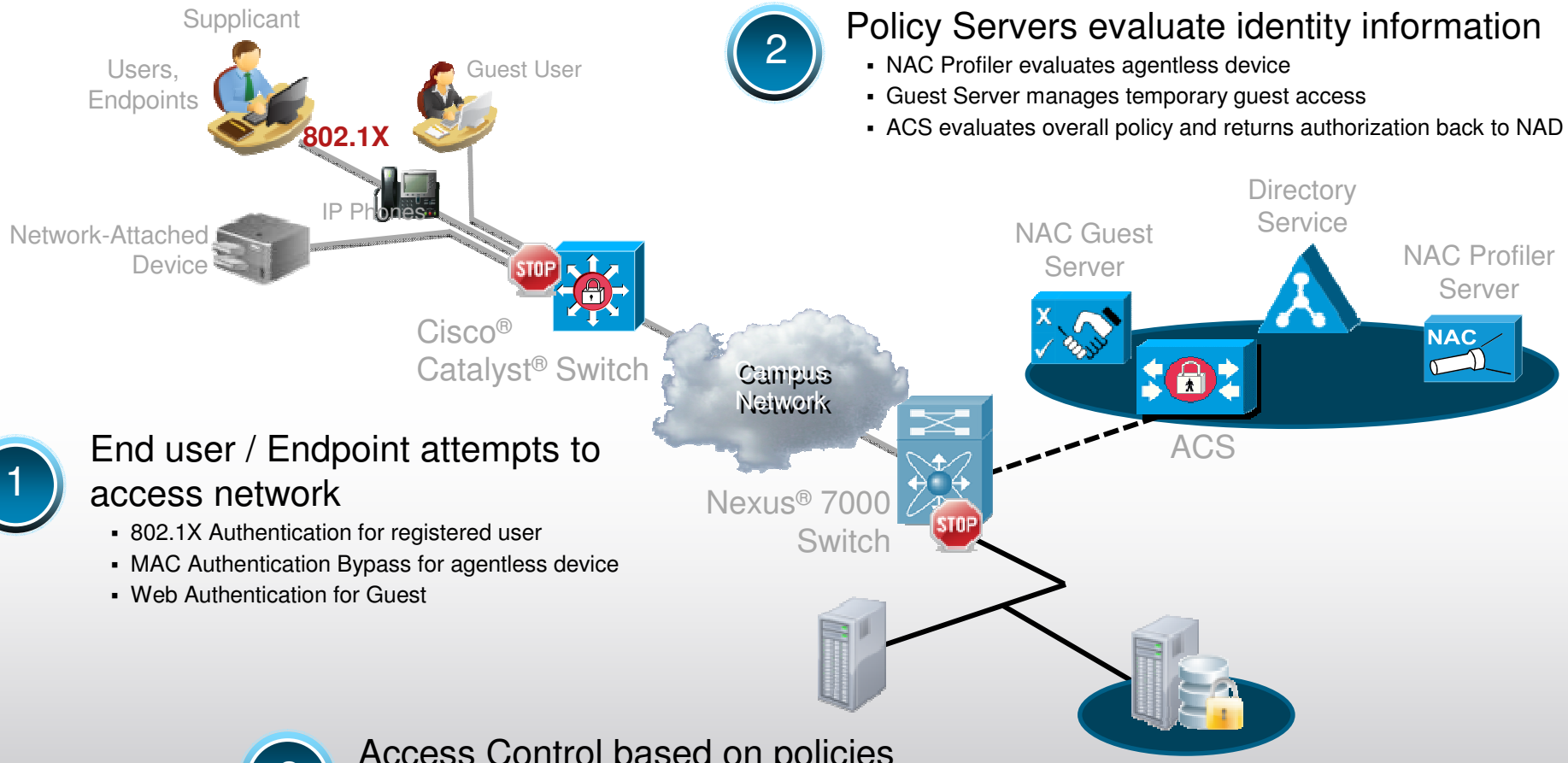
Quarantine

Deny Access

Access Compliance Reporting

802.1X/Infrastructure in Action
A Conceptual View

802.1X/Infrastructure



2

Policy Servers evaluate identity information

- NAC Profiler evaluates agentless device
- Guest Server manages temporary guest access
- ACS evaluates overall policy and returns authorization back to NAD

1

End user / Endpoint attempts to access network

- 802.1X Authentication for registered user
- MAC Authentication Bypass for agentless device
- Web Authentication for Guest

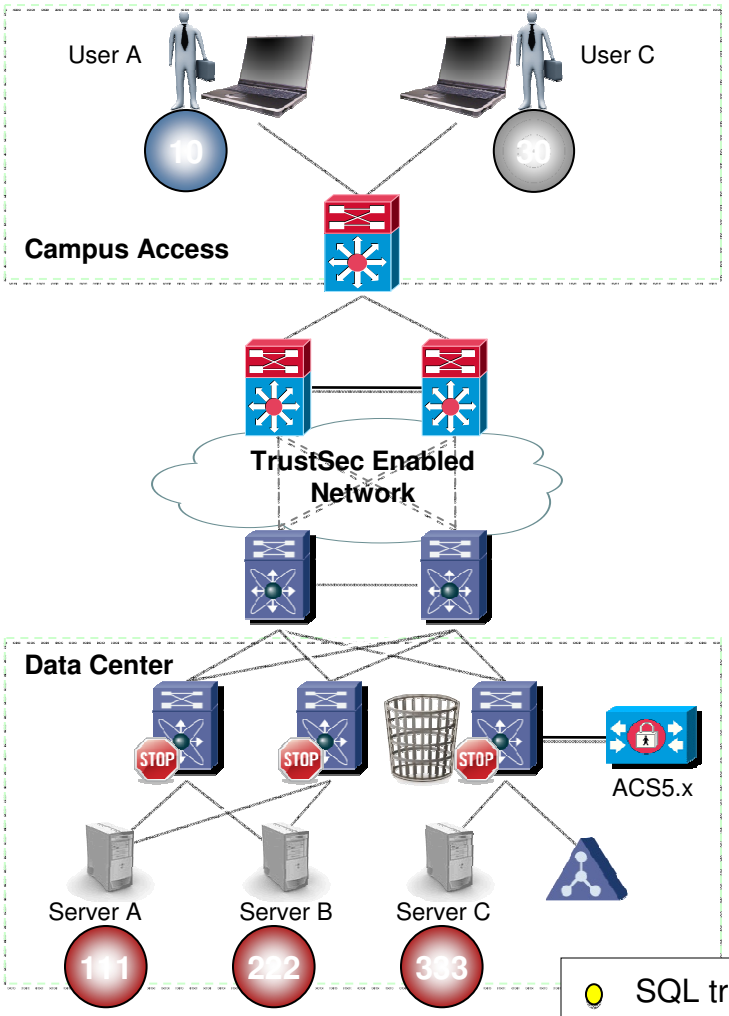
3

Access Control based on policies

- Catalyst switch to enforce access control based on policy (VLAN Assignment, dACL, SGT)
- Nexus 7000 to apply SGACL based on SGT mapped to role

Control Plane: **RADIUS**

Using SGACL for Access Control



SGACL allows topology independent access control

- Even another user accesses on same VLAN as previous example, his traffic is tagged differently
- If traffic is destined to restricted resources, packet will be dropped at egress port of TrustSec domain

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	**SGACL-D**	Permit all

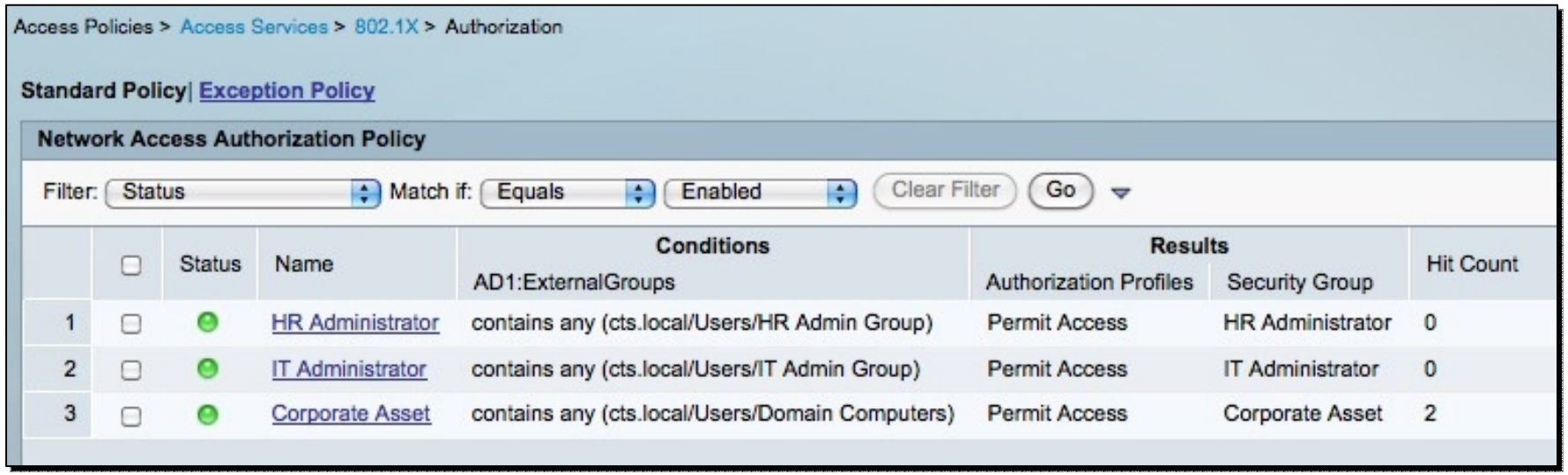
SGACL-D

```
permit tcp src dst eq 1433
permit tcp src eq 1433
permit tcp src dst eq 80
permit tcp src dst eq 443
deny all
```

SQL traffic
Windows File Sharing traffic
SGACL

Sample SGT Assignment Policy

- Sample 802.1X authorization policy to assign Security Group to individual role



Access Policies > Access Services > 802.1X > Authorization

Standard Policy | Exception Policy

Network Access Authorization Policy

Filter: Status | Match if: Equals | Enabled | Clear Filter | Go

		Status	Name	Conditions	Results		Hit Count
				AD1:ExternalGroups	Authorization Profiles	Security Group	
1			HR Administrator	contains any (cts.local/Users/HR Admin Group)	Permit Access	HR Administrator	0
2			IT Administrator	contains any (cts.local/Users/IT Admin Group)	Permit Access	IT Administrator	0
3			Corporate Asset	contains any (cts.local/Users/Domain Computers)	Permit Access	Corporate Asset	2

Confidentiality and Integrity 802.1AE-based Encryption

- Provides strong 128-bit AES-GCM* encryption (NIST** Approved)
- Line-rate encryption / decryption
- Standards-based key management: IEEE802.1X-REV

Benefits

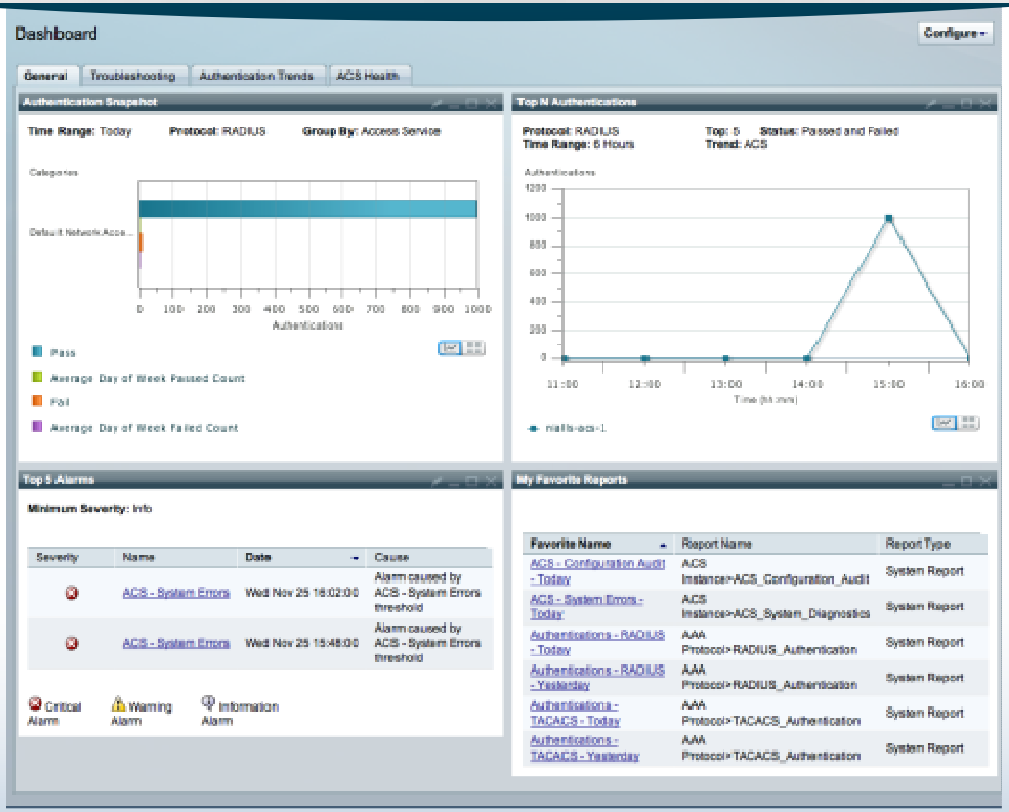
- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Network service amenable to hop-by-hop approach compared to end-to-end approach (e.g., IPsec enforcement)

* NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

* Galois/Counter Mode

Cisco Secure ACS
Monitoring, Troubleshooting, and Reporting

802.1X/Infrastructure



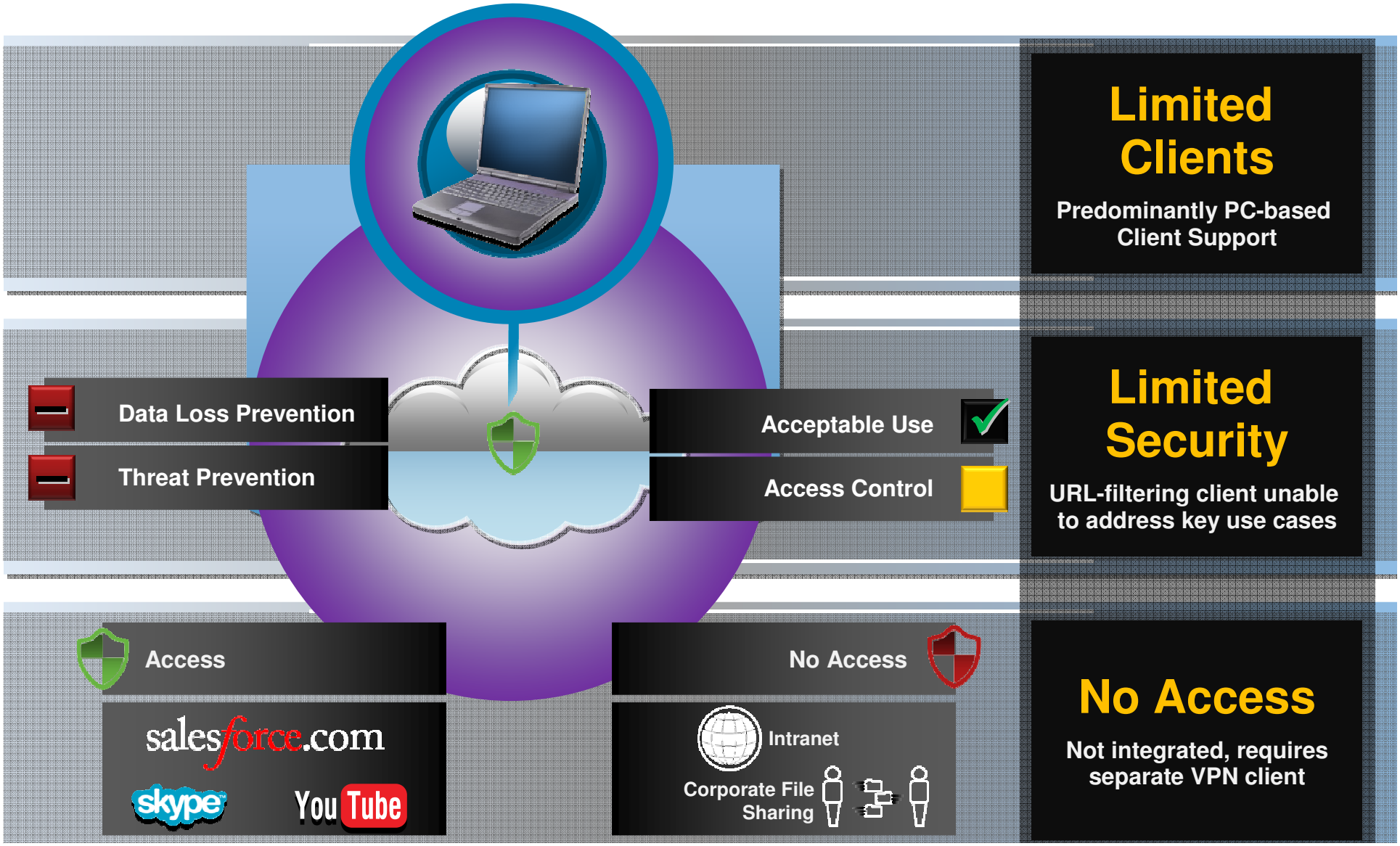
Simplify operations with a centralized system dashboard

- Real-time network access visibility and monitoring
- Compliance reporting
- Diagnostics and failure analysis
- Custom query response and troubleshooting
- Alarms and alerts
- Tracks events from switches & ACS

Agenda

- Borderless networks – uvod
- EnergyWise
- Trustsec
- Secure Mobility
- Q&A

Traditional Mobile Web Security



Limited Clients

Predominantly PC-based Client Support

Limited Security

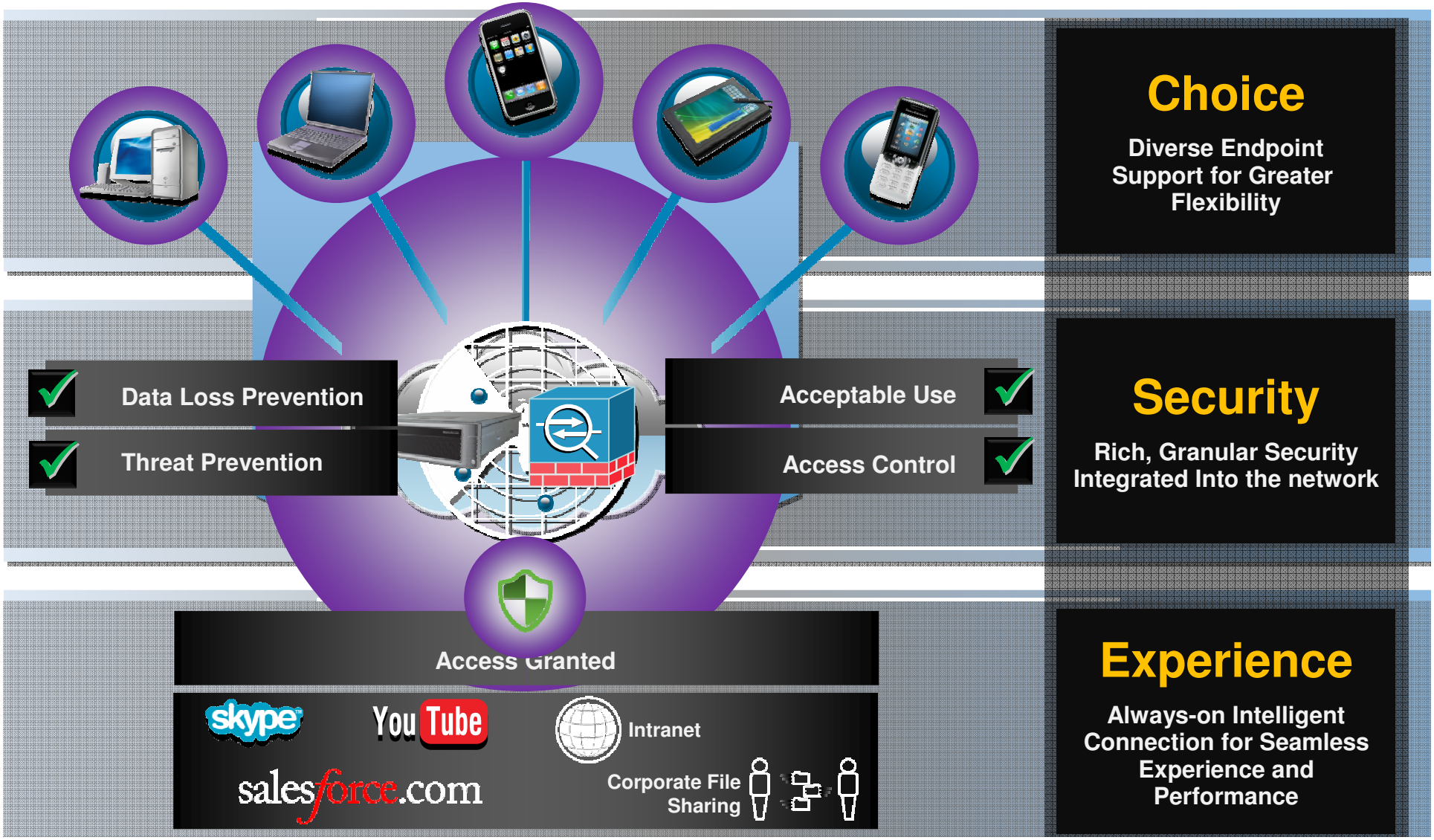
URL-filtering client unable to address key use cases

No Access

Not integrated, requires separate VPN client

Cisco AnyConnect Secure Mobility

Web Security with Next Generation Remote Access



Choice

Diverse Endpoint Support for Greater Flexibility

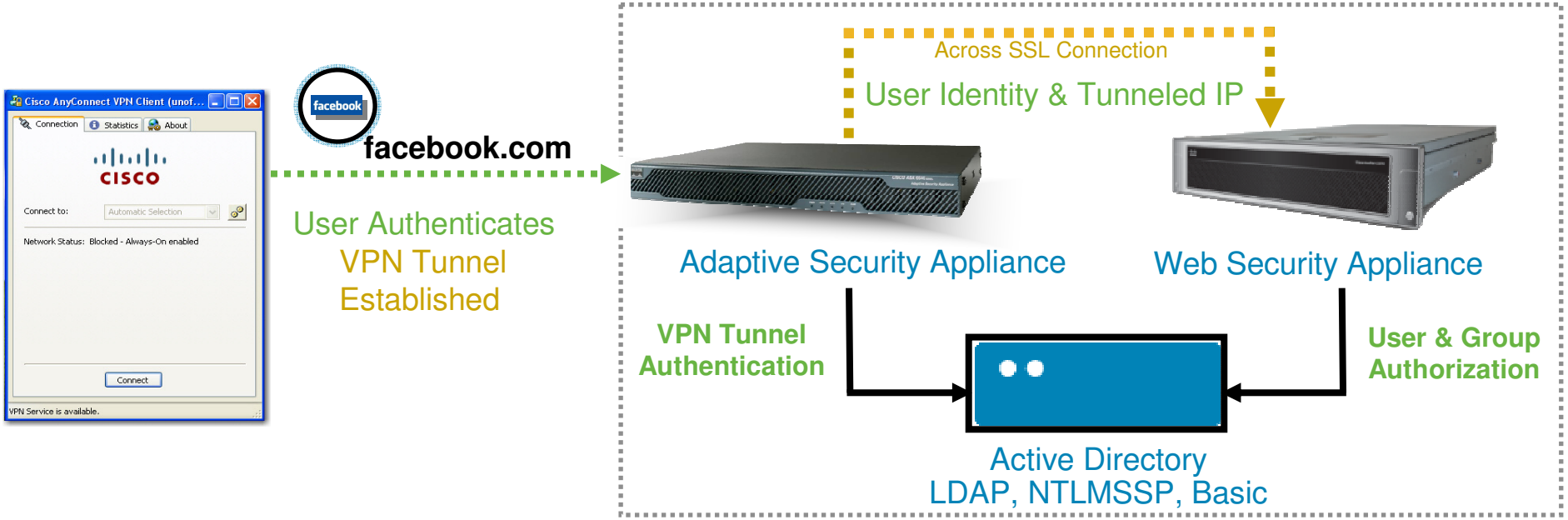
Security

Rich, Granular Security Integrated Into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

Cisco AnyConnect Secure Mobility ASA–WSA Communication



ASA ⟶ WSA

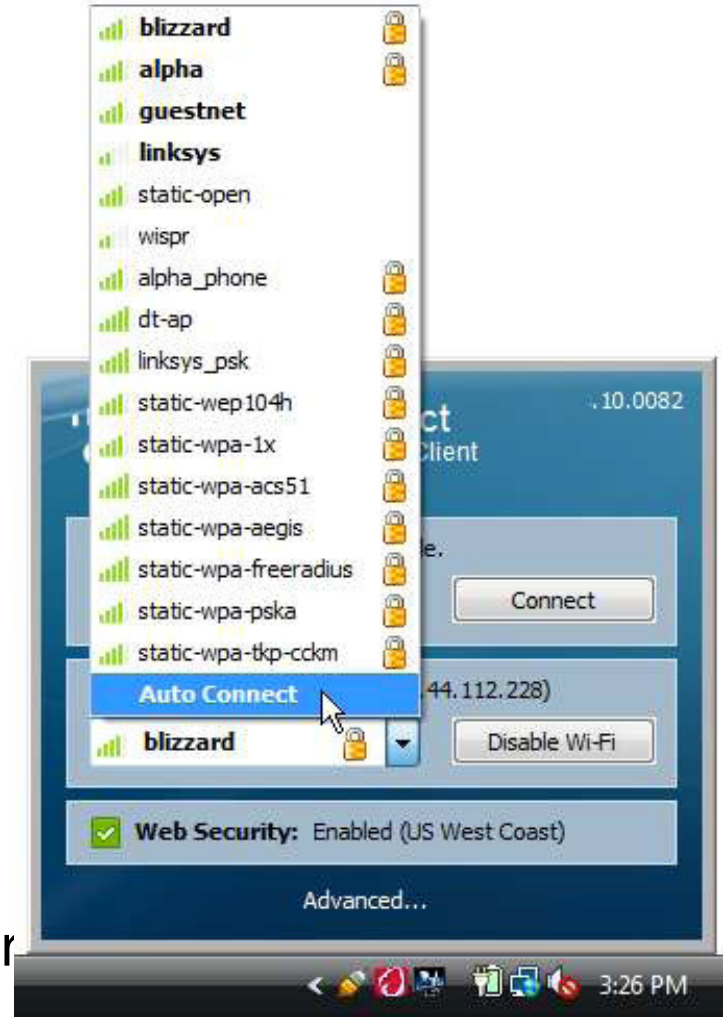
1. AnyConnect Authenticates and Establishes a VPN Tunnel to the ASA
2. ASA Extracts Username from Certificate or AAA Server
3. ASA Forwards Username and Tunneled IP Address to the WSA
4. WSA Verifies Username and Group Membership against Active Directory
5. WSA Applies Policies based on Username or Group Membership

AnyConnect 3.0
Highlights

- Components displayed are modular and can be centrally distributed from ASA, at initial install or at later point of time
- Broad protocol support
- Unification of 4 Cisco clients
- Some Components are OS dependant
  - Anywhere+
  - Telemetry
  - Network Access Manager

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.

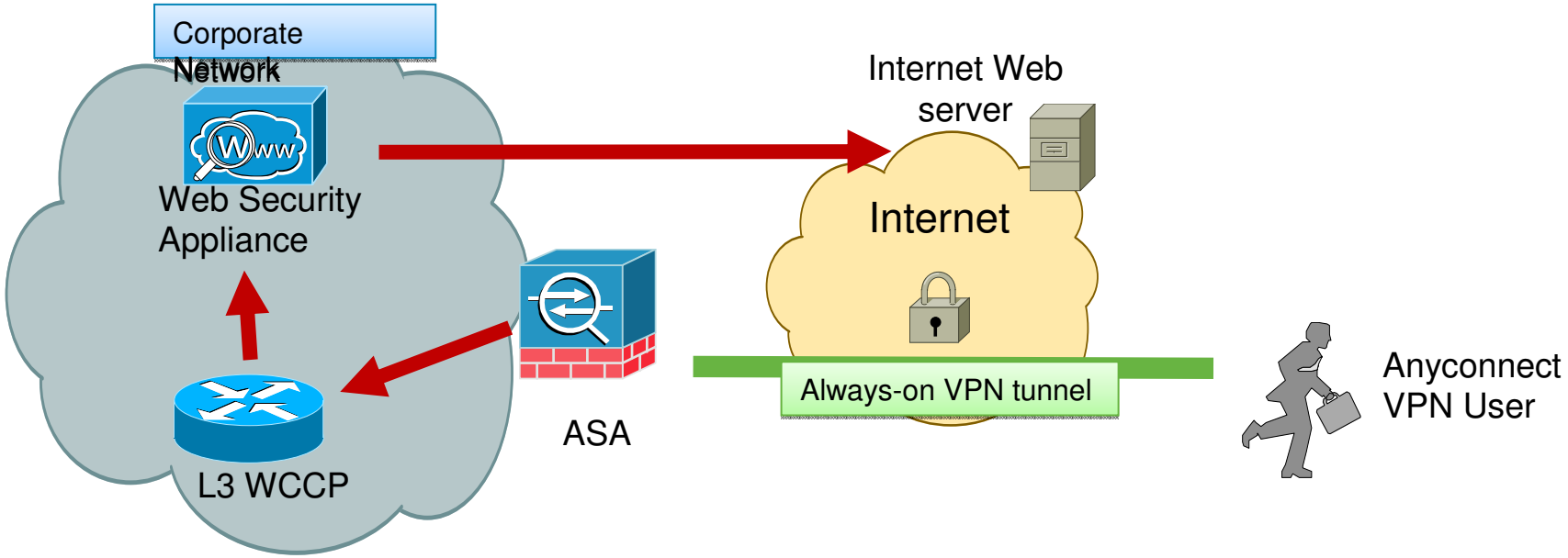


Websecurity

- AnyWhere+ Client as AC 3.0 Module
- Centrally configured via ASA Headend
- Config File from ASA is placed in Websecurity Directory
- Windows Only Support

Telemetry

- AnyConnect Telemetry Component tracks all Fileoperations on the Client
- If 3rd Party AV detects Malware, Telemetry is performing lookup of the URL
- Incident Report is generated and delivered to WSA via Secure Mobility
- Telemetry requires ASA and WSA running in Secure Mobility Setup
- Monitoring 3rd Party Apps via OPSWAT Library
- Windows 32-Bit and 64-bit supported only



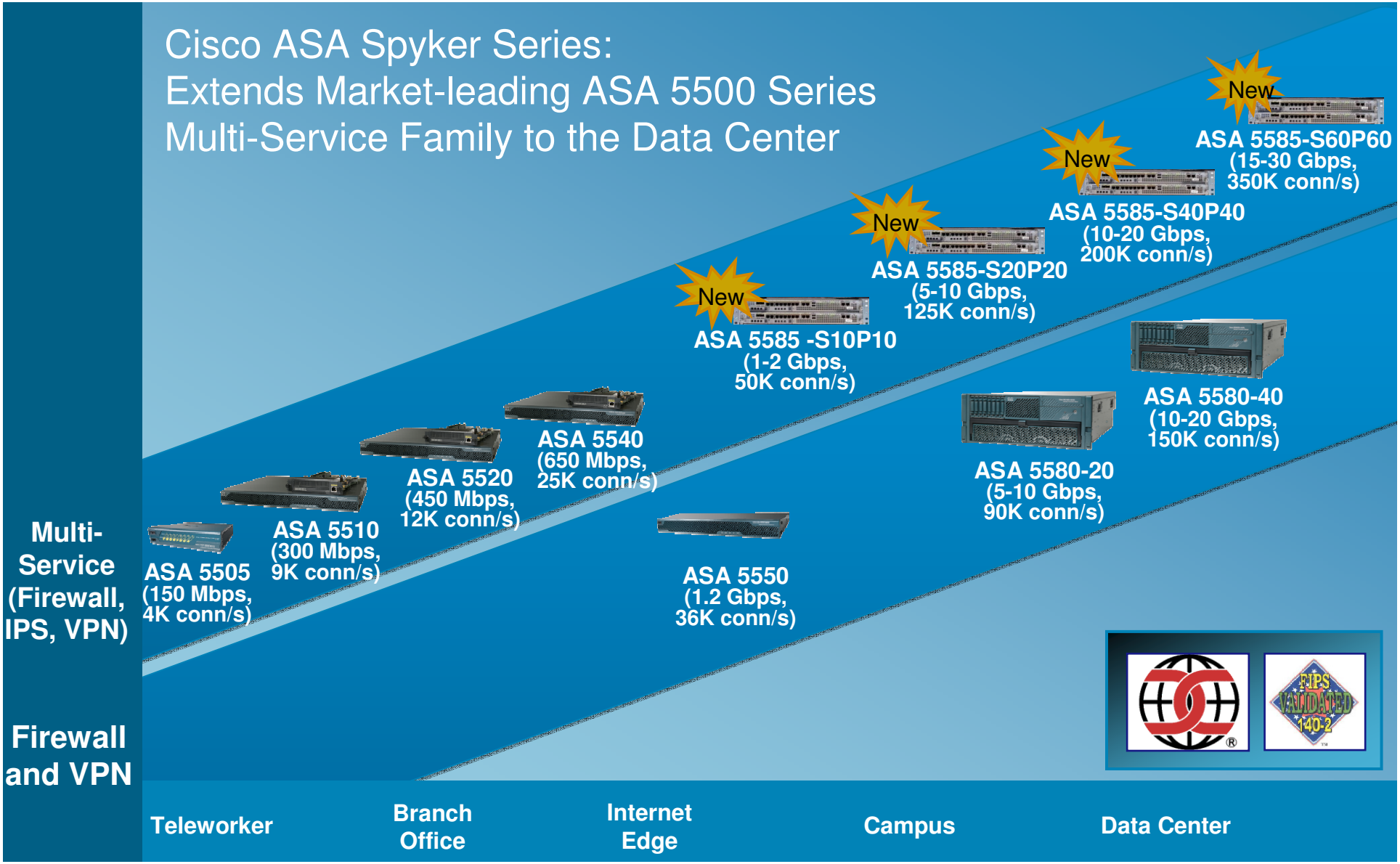
AnyConnect 3.0 with MACsec

- AnyConnect 3.0 provides
  - Unified access interface for SSL-VPN, IPSec and 802.1X for LAN / WLAN
  - Supports MACsec / MKA data encryption in software (Performance CPU-dependent)
  - MACsec capable hardware (network interface) enhances performance

MACsec-ready hardware:

Intel 82576 Gigabit Ethernet Controller
Intel 82599 10 Gigabit Ethernet Controller
Intel ICH10 - Q45 Express Chipset (1Gbe LOM)
(Dell, Lenova, Fujitsu, and HP have desktops shipping with this LOM)

Cisco ASA 5500 Series Adaptive Security Appliances



Cisco ASA 5500 Series High-End Solutions

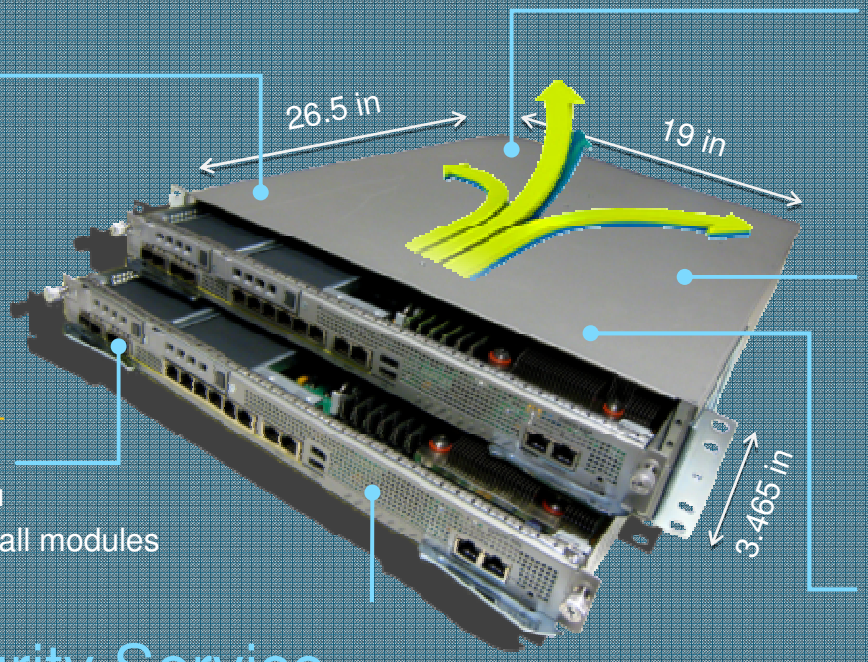
Network Location	Internet Edge/ Campus ASA 5585 SSP-10	Internet Edge/ Campus ASA 5585 SSP-20	Campus/ Data Center ASA 5585 SSP-40	Data Center ASA 5585 SSP-60
Performance				
Max Firewall	4 Gbps	10 Gbps	20 Gbps	35 Gbps
Max IPS	2 Gbps	3 Gbps	5 Gbps	10 Gbps
Max IPSec VPN	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Max IPSec/SSL 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



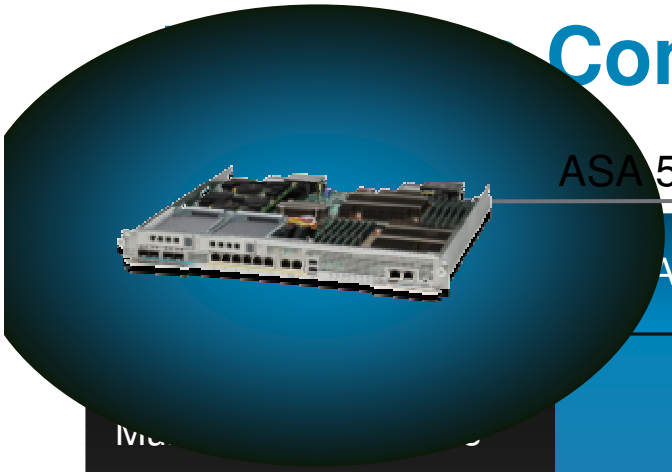
Redundant Hot Swappable Power Supply Units
- Front to back air flow

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

eUSB
- 2 GB internal
- Convenience storage
- Security credentials

Security Service Processors
- Multi-services capable
- Dedicated 64bit multi-core processors

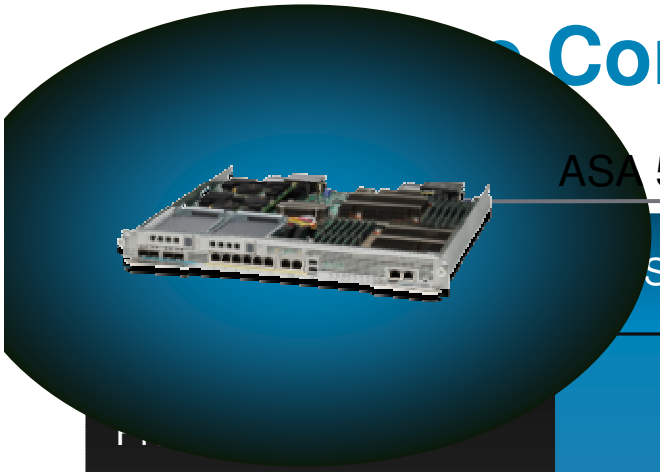
ASA 5585-X Firewall/VPN Module Comparison



ASA 5585-X

	A SSP-10	ASA SSP-20	ASA SSP-40	ASA SSP-60
M...	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 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+ 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

SSP Interfaces

SSP-10 SSP-20 IPS SSP-10 IPS SSP-20	SSP-40 SSP-60 IPS SSP-40 IPS SSP-60
	
8 10/100/1000 interfaces	6 10/100/1000 interfaces
2 GE SFP/10 GE SFP+* interfaces	4 GE SFP/10 GE SFP+ interfaces
Supported SFP/SFP+ modules 1 GE SX SFP modules** 10 GE SR and LR SFP+ modules**	Supported SFP/SFP+ modules 1 GE SX SFP modules** 10 GE SR and SFP+ modules**
2 x Dedicated 10/100/1000 management interfaces	2 x Dedicated 10/100/1000 management interfaces

* 10 GE SFP+ interfaces require license upgrade
** SFP and SFP+ modules sold separately

Software Support

ASA 8.2.3 Release

- Follow-on to Release 8.2.2 Mainline
- Features and platform support inheritance from Release 8.2
- New features

  10G I/O support requires software license on SSP-10 and SSP-20

  QoS support for 10G NIC ports

IPS 7.1.(1)E4 Release

- Based on 7.0(3) Software Release
- IDM 7.0.(1)E4 and IME 7.1.(1)E4
- New Features

  Support for String-XL engine

Cisco Security Manager 4.0.1

CSM Support : available

Single Integrated Application

- Unified graphical interface for managing policy and troubleshooting of Firewall, VPN and IPS devices

Enterprise Class Security Device Management

- Manages hundreds of Cisco security devices

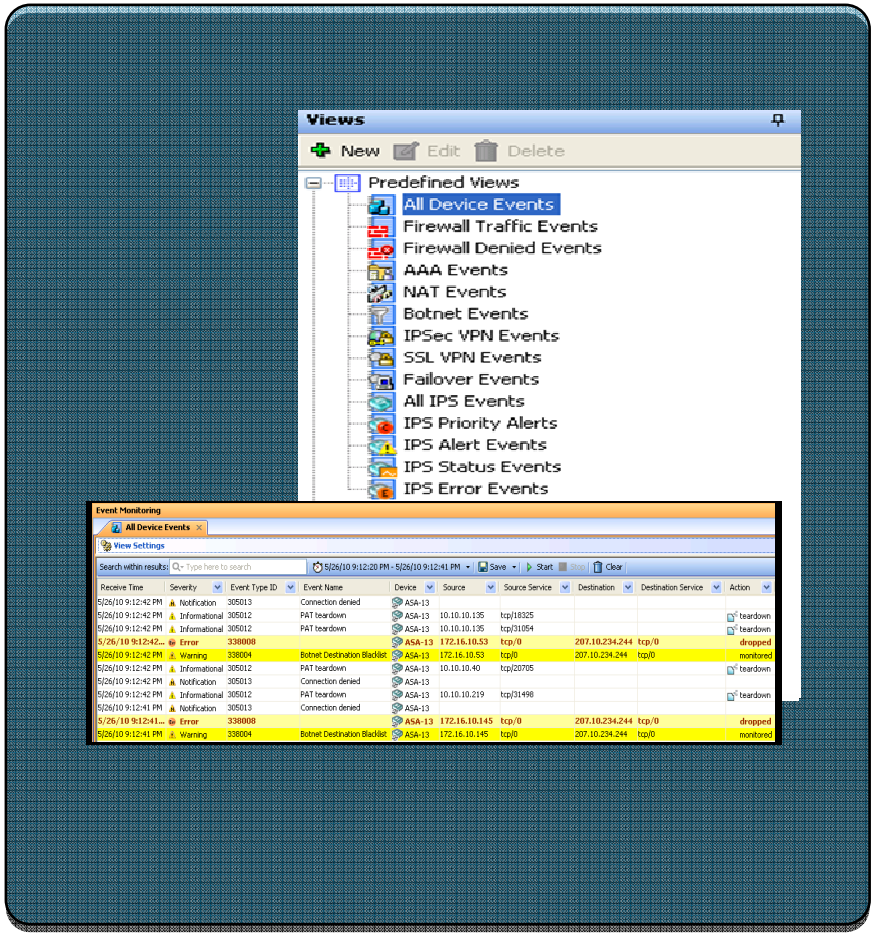
Cisco ASA 5585 Platform Series

- Part of CSM managed device family with CSM 4.0.1 release

Integrated Event Management

Simplified Troubleshooting Experience

- Real-time monitoring
- Historical tracking
- Event-to-policy navigation
- Consolidated logs
- Quick filters and sorting
- Predefined and customizable views
- Intuitive time scale
- High performance



Agenda

- Borderless networks – uvod
- EnergyWise
- Trustsec
- Secure Mobility
- Q&A


Cisco Expo
2010
Kolaboracija i virtuelizacija bez granica.
Jubilarna 10. Cisco Expo konferencija
7. i 8. decembar 2010.
Hotel Hyatt Regency Beograd
Registrujte se po specijalnim uslovima na www.cisco.com/yu
CISCO