



SECURITY UPDATE

Dragan Novaković, Cisco Srbija
CCIE #26951



Agenda

- Cisco ASA 5500-X
- Cisco IPS 4300 Series
- Cisco ASA CX
- Cloud/DC security
- Q & A



ASA 5500-X Series



Next-Generation Security Services Platforms



5 new models to meet varied throughput demands

ASA 5512-X

1 Gbps Firewall
Throughput



ASA 5515-X

1.2 Gbps Firewall
Throughput



ASA 5525-X

2 Gbps Firewall
Throughput



ASA 5545-X

3 Gbps Firewall
Throughput



ASA 5555-X

4 Gbps Firewall
Throughput



1. Multi-Gig Performance

To meet growing throughput requirements

2. Accelerated Integrated Services

(no extra hardware required)

To support changing business needs

3. Next-gen services enabled platform

To provide investment protection

ASA Mid-Range Portfolio

4X Firewall Throughput
(compared to earlier models)

4 Gbps Firewall
1.3 Gbps IPS
700 Mbps VPN



ASA 5555-X

3 Gbps Firewall
900 Mbps IPS
500 Mbps VPN



ASA 5545-X

2 Gbps Firewall
600 Mbps IPS
300 Mbps VPN



ASA 5525-X

1.2 Gbps Firewall
400 Mbps IPS
250 Mbps VPN



ASA 5515-X

1 Gbps Firewall
250 Mbps IPS
200 Mbps VPN



ASA 5512-X

300 Mbps Firewall
300 Mbps IPS
170 Mbps VPN

450 Mbps Firewall
450 Mbps IPS
225 Mbps VPN



ASA 5520

1.2 Gbps Firewall
425 Mbps VPN



ASA 5550

650 Mbps Firewall
650 Mbps IPS
325 Mbps VPN



ASA 5540

300 Mbps Firewall
300 Mbps IPS
170 Mbps VPN

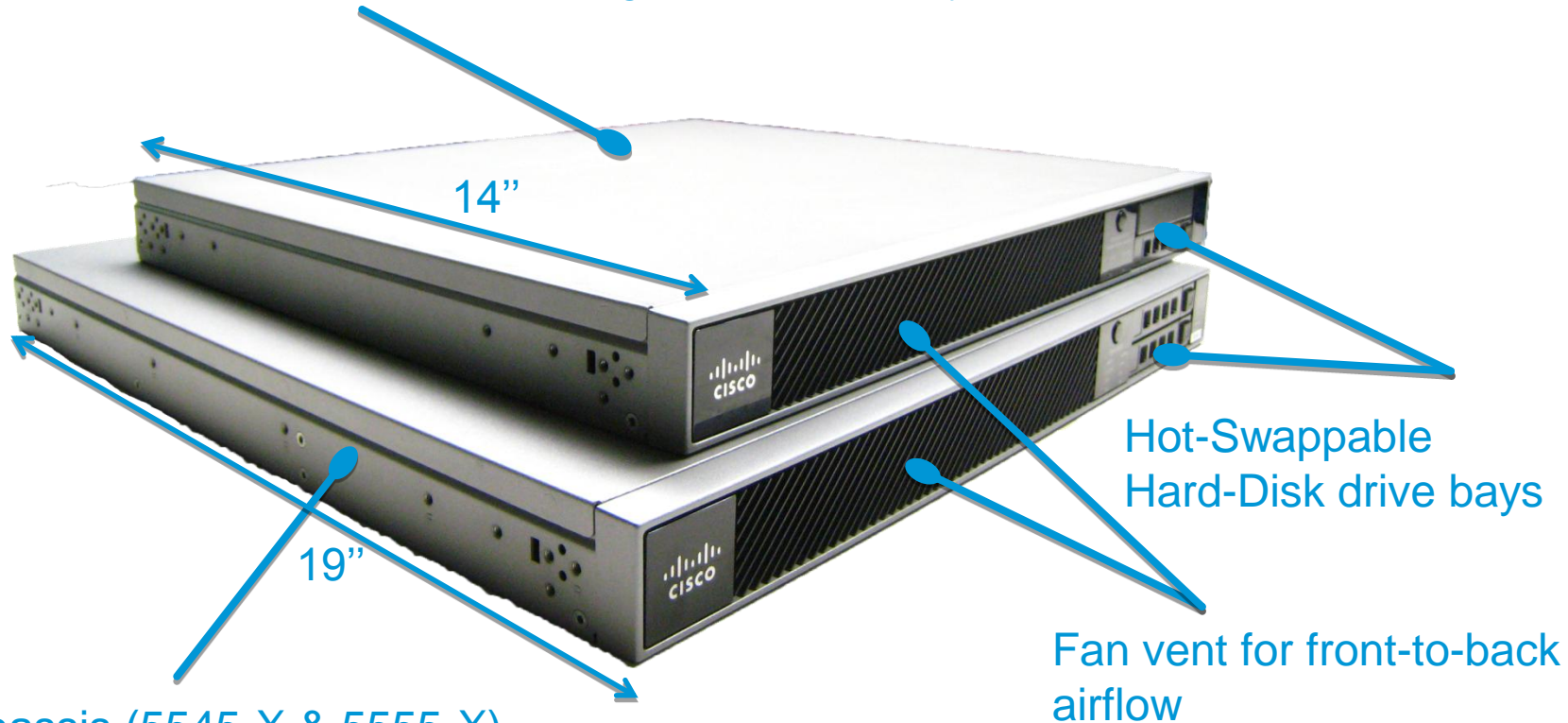


ASA 5510 Base



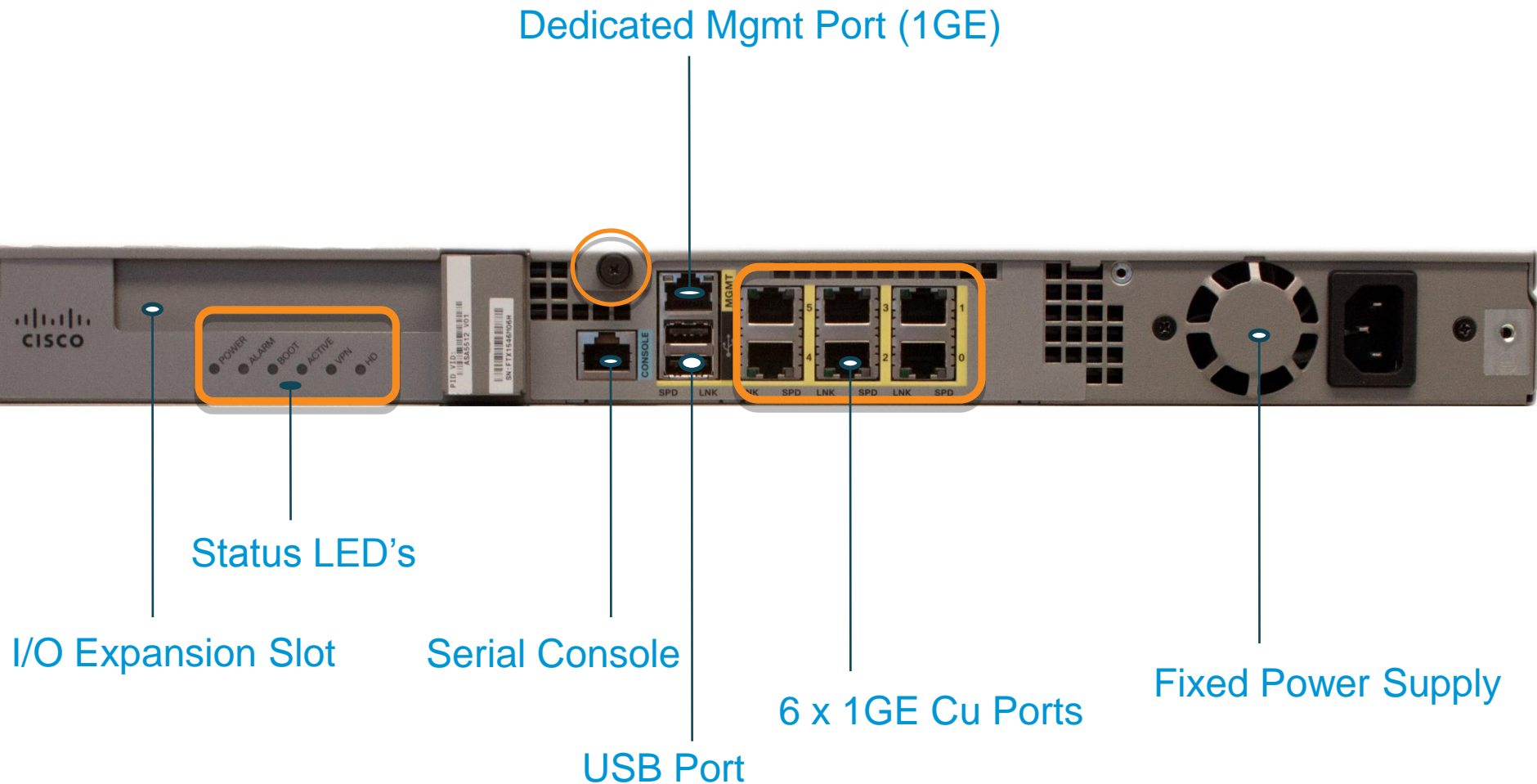
ASA 5510 Plus

Short Chassis (5512-X, 5515-X & 5525-X)
-- Fixed Single Power Supply

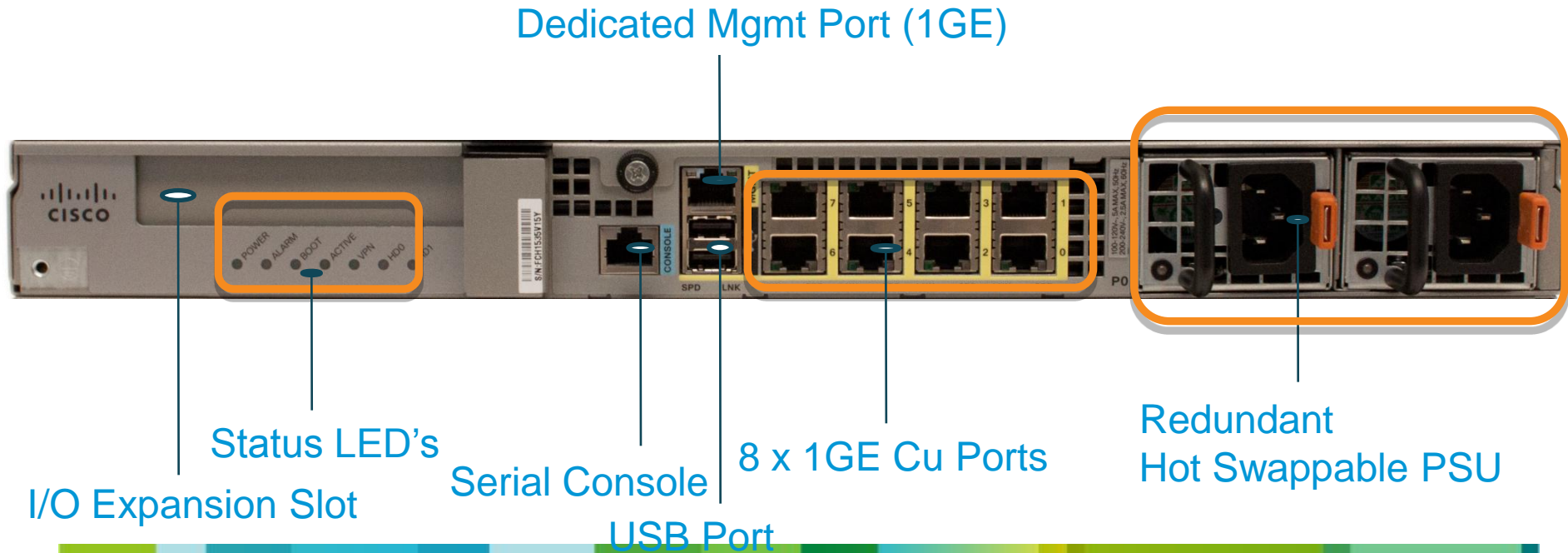
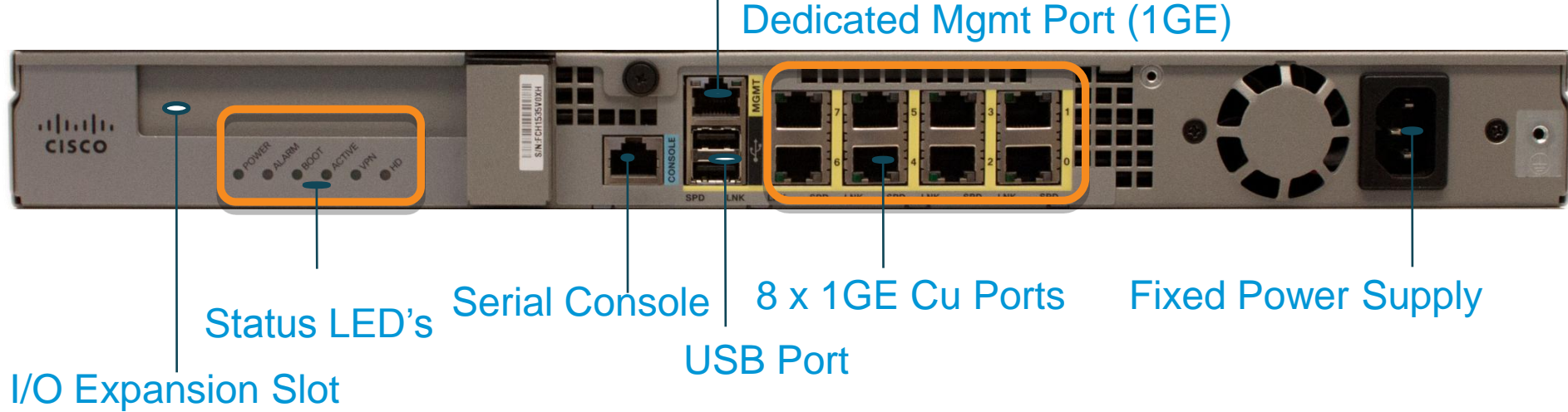


Long Chassis (5545-X & 5555-X)
-- Hot-Swappable redundant dual power-supply

ASA 5512-X/ASA 5515-X Back Panel



ASA 5525-X & 5545-X/ 5555-X



Saleen ASA Platform Matrix

Specification	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X
Platform Base	1RU Short chassis 19" Rack Mountable	1RU Short chassis 19" Rack Mountable	1RU Short chassis 19" Rack Mountable	1RU Long chassis 19" Rack Mountable	1RU Long chassis 19" Rack Mountable
CPU	1x 2.8 Ghz Intel 2C/2T	1 x 3.06 Ghz Intel 2C/4T	1x 2.40 Ghz Intel 4C/4T	1x 2.66 Ghz Intel 4C/8T	1x 2.80 Ghz Intel 4C/8T
DRAM	4GB	8 GB	8GB	12GB	16GB
Regex Accel Mezz Card	N/A	N/A	1	1	1
Compact Flash	4GB eUSB	8GB eUSB	8GB eUSB	8GB eUSB	8GB eUSB
I/O Ports	6 x 1GbE Cu 1 x 1GbE Cu Mgmt	6 x 1GbE Cu 1 x 1GbE Cu Mgmt	8 x 1GbE Cu 1 x 1GbE Cu Mgmt	8 x 1GbE Cu 1 x 1GbE Cu Mgmt	8 x 1GbE Cu 1 x 1GbE Cu Mgmt
Optional I/O Module	6 x 1GbE Cu or 6 x 1GbE SFP	6 x 1GbE Cu or 6 x 1GbE SFP	6 x 1GbE Cu or 6 x 1GbE SFP	6 x 1GbE Cu or 6 x 1GbE SFP	6 x 1GbE Cu or 6 x 1GbE SFP
Power	Single Fixed AC Power Supply	Single Fixed AC Power Supply	Single Fixed AC Power Supply	Dual Hot-Swappable Redundant AC Power Supply	Dual Hot-Swappable Redundant AC Power Supply
Crypto Capacity	1 x Crypto Chip 4C	1 x Crypto Chip 4C	1 x Crypto Chip 4C	1 x Crypto Chip 8C	1 x Crypto Chip 8C

ASA 5500-X I/O Module Options

Available
on all
5500-X
platforms

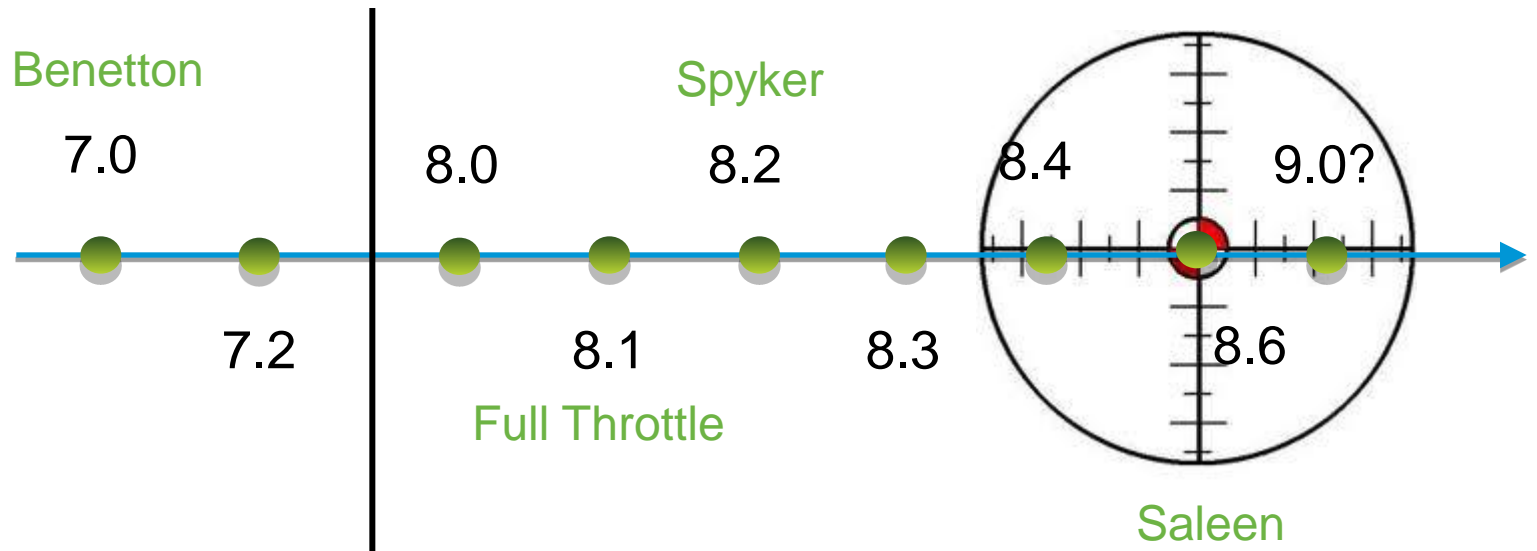
I/O expansion cards are available in two flavors

- 6 Port 10/100/1000 Base T , RJ45 Connector I/O NIC Card
- 6 Port 1GbE SFP Connector I/O NIC Card



Saleen hardware comparison with ASA 5510 – ASA 5550

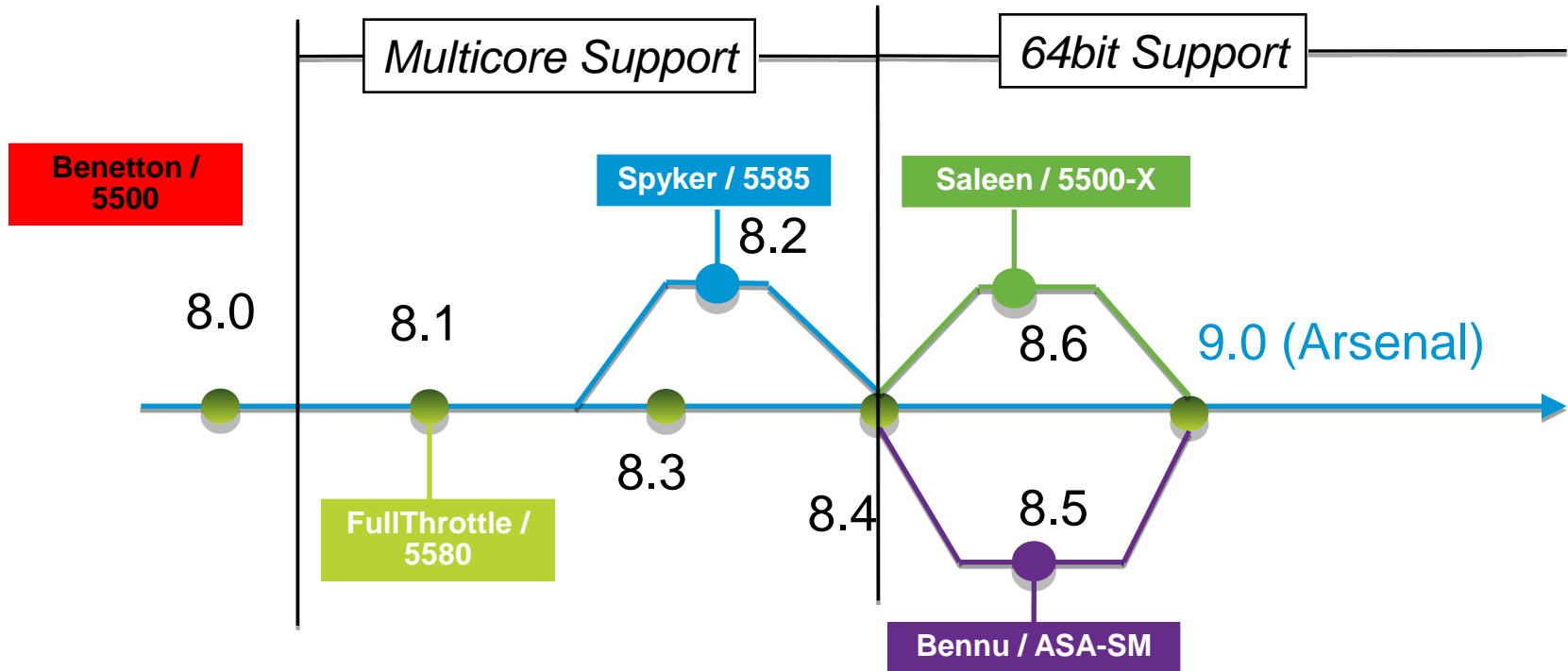
ASA 5510 – ASA 5550	ASA 5512-X – ASA 5555-X
Single Core CPU	Multi-Core CPU
1GB to 4GB DDR1 RAM	4GB to 16GB DDR3 RAM
Base I/O ports limited to 4 x 1GbE Copper interfaces	Base I/O ports up to 8 x 1GbE Copper interfaces
4 x 1GbE I/O port expansion module	6 x 1GbE Copper or fiber SFP I/O expansion module
IPS on SSM card	Integrated IPS service within the same chassis
N/A	Redundant Hot-Swappable power supply units
N/A	Regex accelerator card
N/A	Hard Disk Support



Software



ASA Software (Firewall & VPN Services)



- ASA 5500-X platform software be based on 8.4 code-train
 - All software feature functionality up to ASA 8.4.2
 - Platform support for newer hardware
 - Software version will be 8.6.1

IPS Software

- IPS SSP module are based on 7.1(4) release
 - Platform support for new hardware
 - Based on ASA 5585-X line of code
 - Supports existing E4 Engine Update
 - Supports all latest Signature Updates
 - Sig S615 is bundled with Saleen images.
 - 7.1.4 IDM version included with the IPS image.
 - 7.2.1 IME version provides full support.
 - CSM support with version 4.3
 - IPS 7.1(4) version supports all –X platforms (including 5585-X)
 - Additional CFD bug fixes and a few serviceability enhancements also included in this version.

High-Performance features on Saleen

- SMP-enabled Kernel
- 64-bit architecture
- Environment Monitoring
- Jumbo-Frame support
- Hardware Regex Accelerator support for IPS string-XL engine



ASA Licensing

New Feature – IPS Module

- A new licensing feature was introduced to enable the use of the IPS Software Module.
- Traffic destined to IPS will be dropped by ASA if this license is not enabled **AND** 'fail-close' is configured.
- IPS Signature Update license is required on top of the above license.
- All other license features remain unchanged and are based on ASA 8.4.2 software.

Permanent Activation Key

Serial No.:

Permanent Activation Key

New Activation Key

Configure a new activation key

New Activation Key

Time-based License

Activate | Deactivate

License Activation

0xe40f25e9

0xb207d6c1

0x432953eb

0x772a17c0

Effective Running

License Feature

Device license

Maximum Physical

Maximum VLANs

Inside Hosts

Failover

VPN-DES

VPN-3DES-AES

Security Contexts

License details of the permanent activation key



License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	perpetual
Maximum VLANs	50	perpetual
Inside Hosts	Unlimited	perpetual
Failover	Disabled	perpetual
VPN-DES	Enabled	perpetual
VPN-3DES-AES	Disabled	perpetual
Security Contexts	0	perpetual
GTP/GPRS	Disabled	perpetual
AnyConnect Premium Peers	2	perpetual
AnyConnect Essentials	250	perpetual
Other VPN Peers	250	perpetual
Total VPN Peers	250	perpetual
Shared License	Disabled	perpetual
AnyConnect for Mobile	Disabled	perpetual
AnyConnect for Cisco VPN Phone	Disabled	perpetual
Advanced Endpoint Assessment	Disabled	perpetual
UC Phone Proxy Sessions	2	perpetual
Total UC Proxy Sessions	2	perpetual
Botnet Traffic Filter	Disabled	perpetual
Intercompany Media Engine	Disabled	perpetual
IPS Module	Enabled	perpetual

OK

IPS Module SKU's

ASA5512-IPS-SSP

ASA5515-IPS-SSP

ASA5525-IPS-SSP

ASA5545-IPS-SSP

ASA5555-IPS-SSP

IPS License

Enabling IPS service



Enabling IPS Service

Enable IPS Module License

- Apply ASA55xx-IPS-SSP license
- Signature Updates are covered under separate license.

Download IPS software

- IPS software should be present on internal flash.
- Use 'sw-module' CLI to configure IPS boot options

Use ASDM startup Wizard

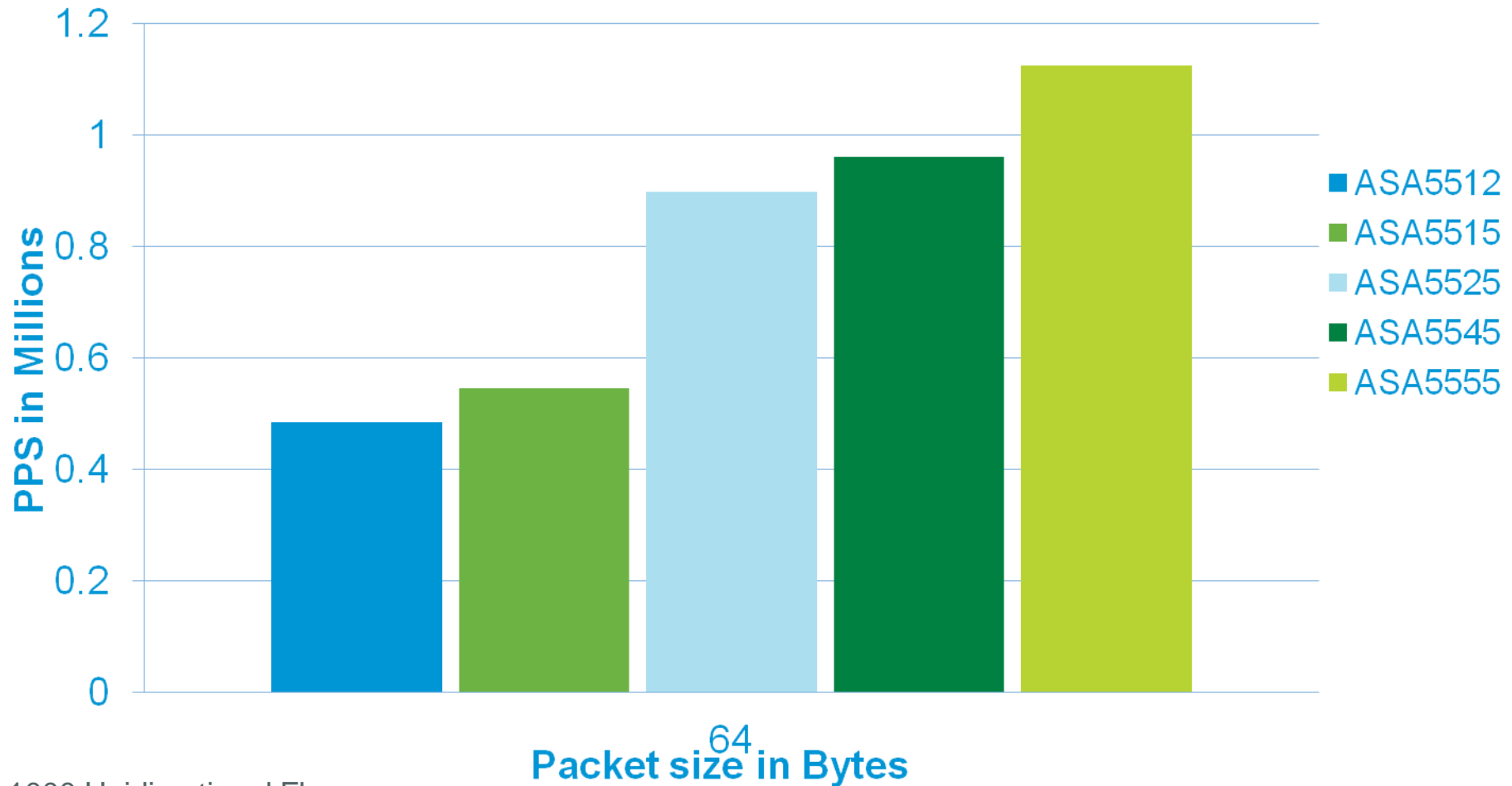
- Intrusion Prevention Tab will be enabled within ASDM
- On boot, IPS module can be configured via ASDM startup wizard

ASA Management Model

- Dedicated Out-Of-Band management port M0/0
- Failover & VLAN sub-interface features are not configurable on M0/0
- ASA and integrated IPS management are independent of each other.
 - Management model is similar to previous ASA/SSM appliances
 - ASA and IPS software module have separate management IP addresses but share the same physical port M0/0 for outbound connectivity
 - ASA can log IPS module's console messages "show module 1 log console"
- ASA configures and manages all external data ports

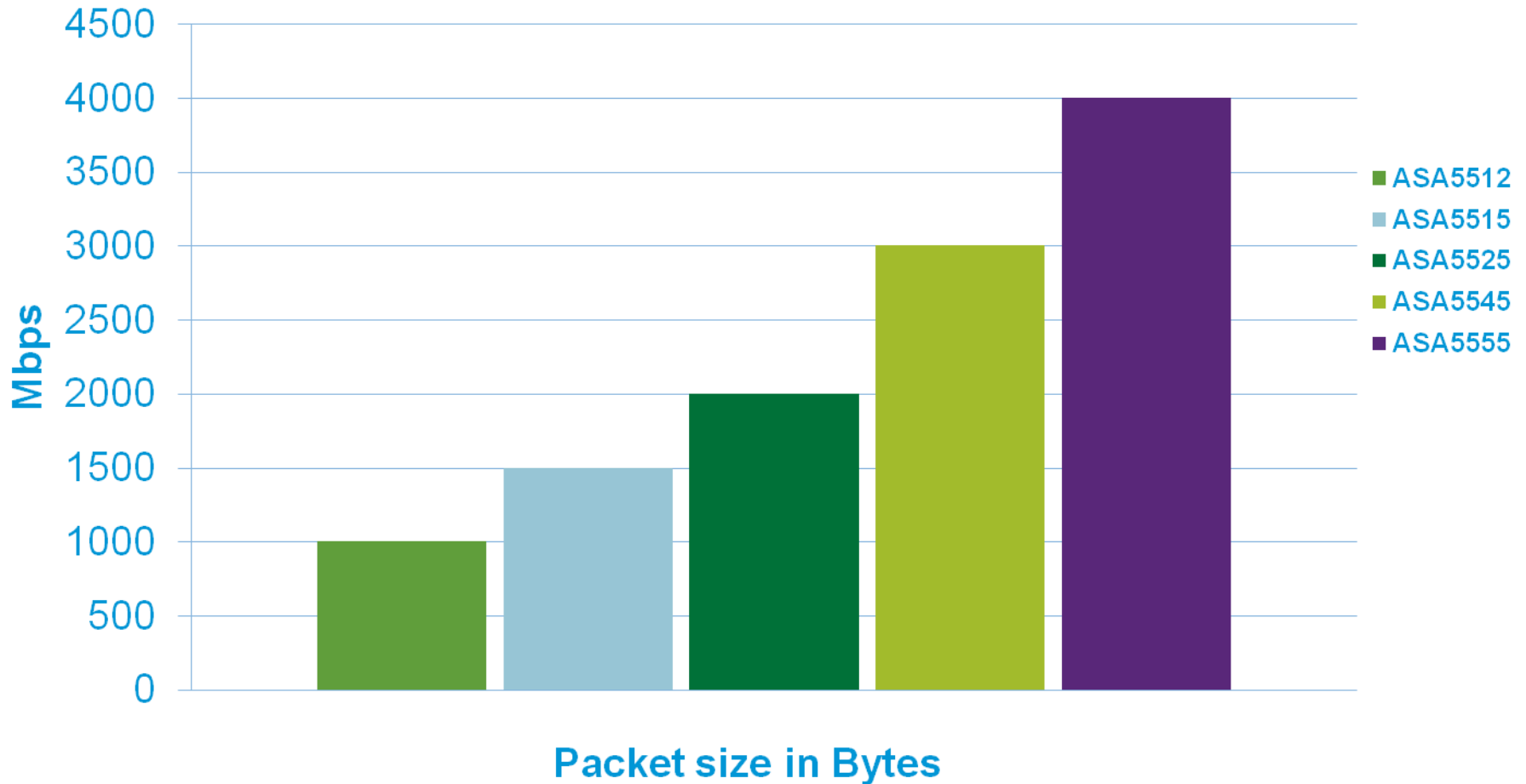
IPv4 UDP Performance (Firewall Only)

PPS



IPv4 UDP Performance (Firewall Only)

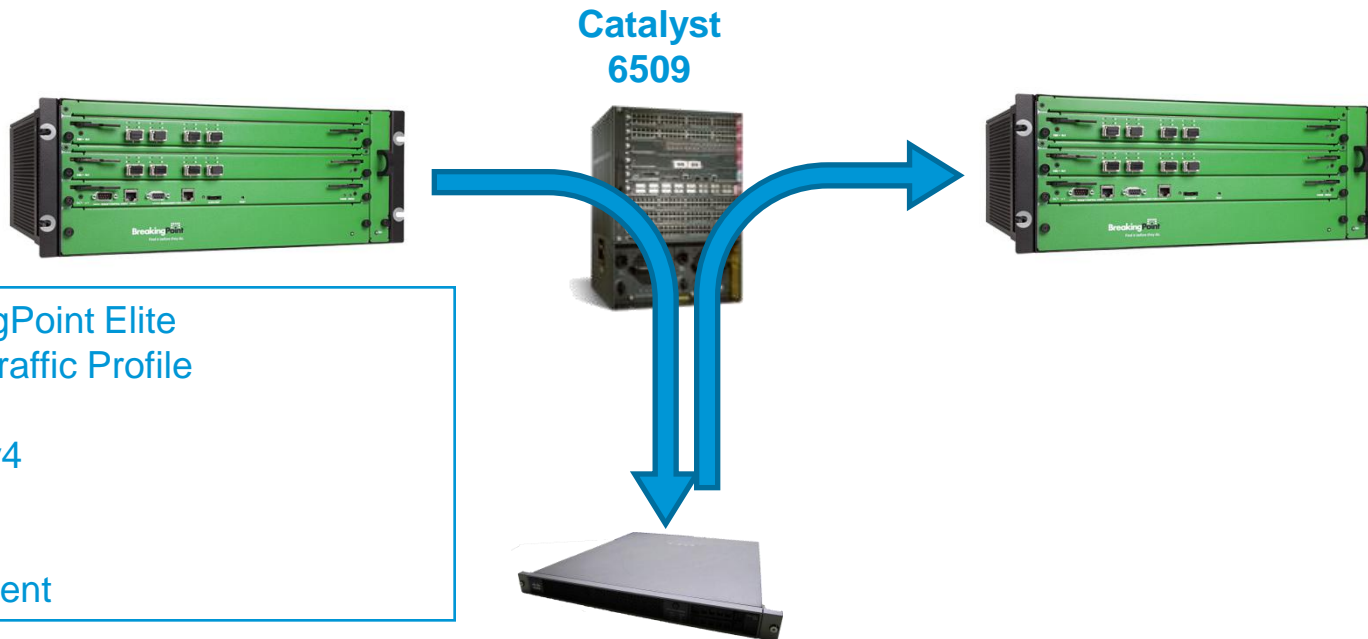
Maximum Throughput



1000 Unidirectional Flows



ASA Firewall Multi-Protocol (eMIX) Performance Test



BreakingPoint Elite

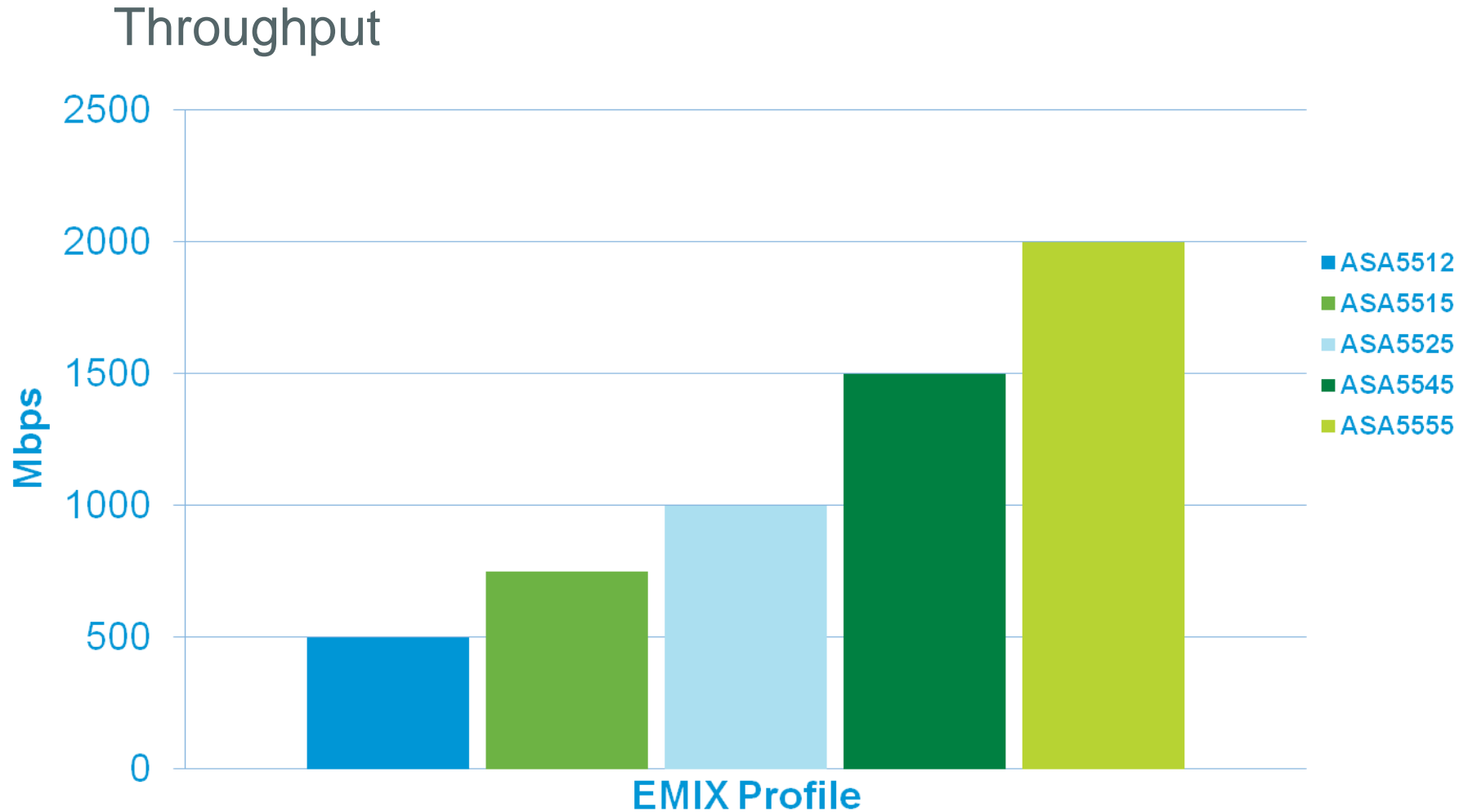
▪eMIX Traffic Profile

- HTTP
- IMAPv4
- SMTP
- FTP
- BitTorrent

ASA

- Single Routed Mode
- Firewall Only (IPS Disabled)
- Default Configuration
- Syslogs are disabled
- 4 x 1GE Ports used for maximum throughput

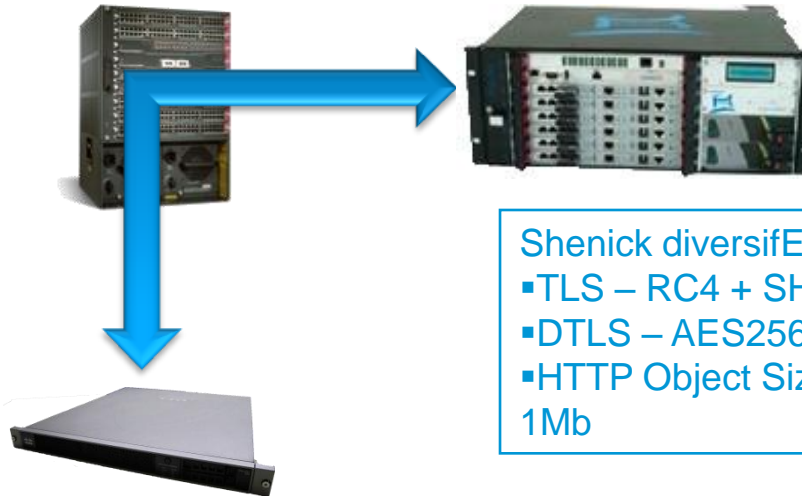
Multi-Protocol (EMIX) Performance (Firewall Only)



ASA VPN Performance Test Approach

Catalyst
6509

Shenick
diversifEye



ASA

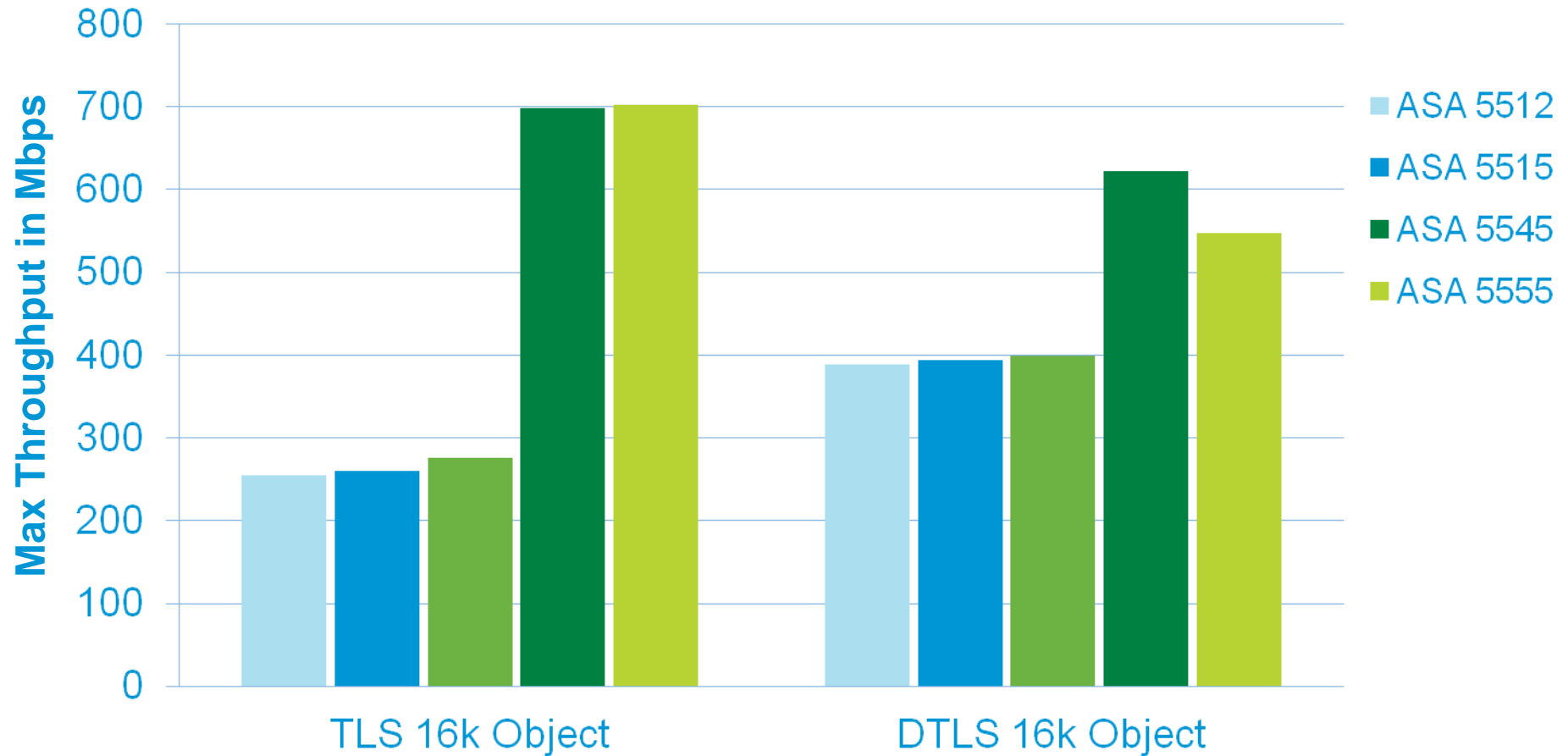
- Single Routed Mode
- IPS Disabled
- Default Configuration
- Syslogs are disabled
- 2 x GE Ports used for maximum PPS & Throughput

Shenick diversifEye

- TLS – RC4 + SHA1
- DTLS – AES256 + SHA1
- HTTP Object Sizes used – 16k & 1Mb

ASA SSLVPN Performance

Max Throughput Test



ASA WebVPN Performance

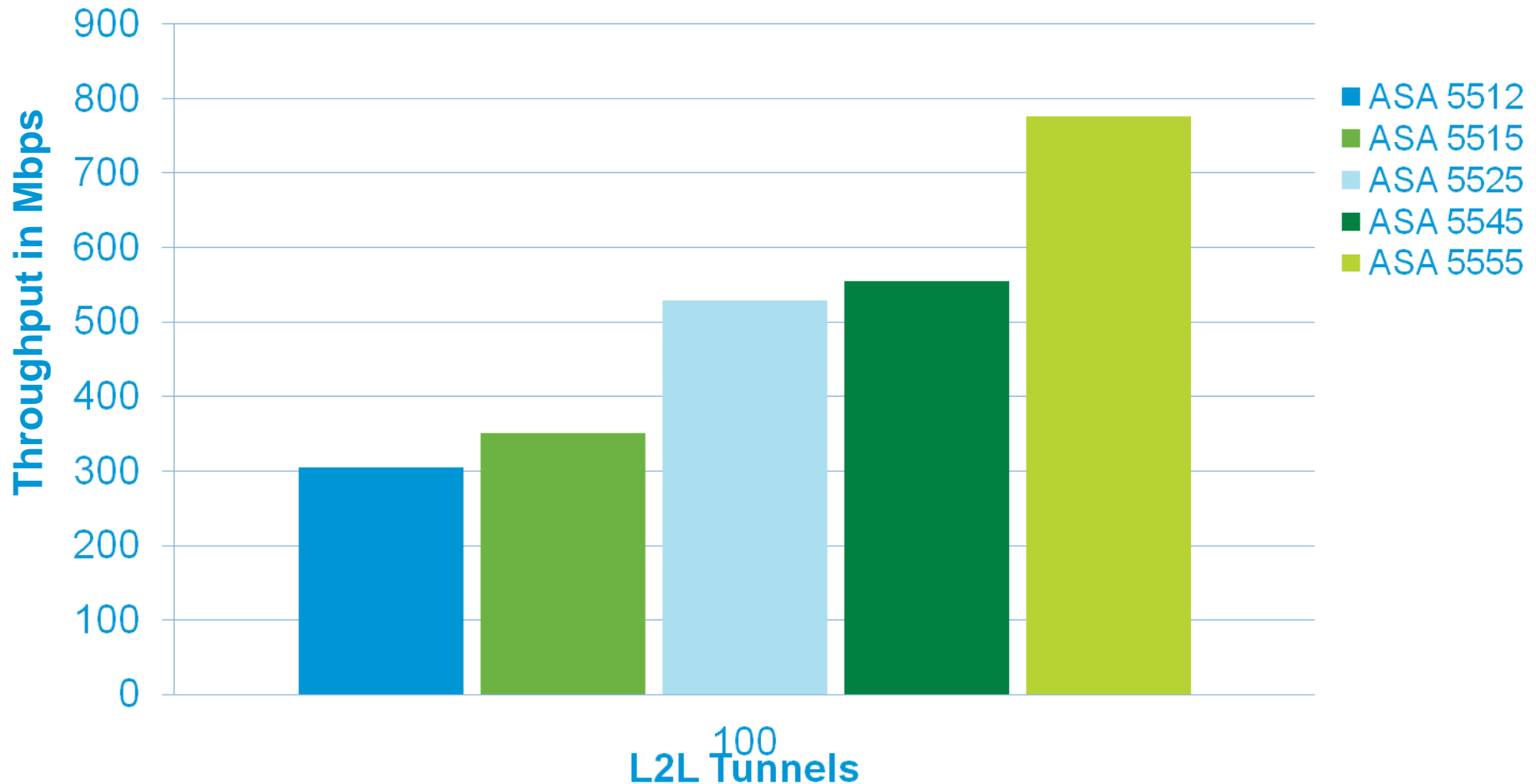
Max Throughput Test



Encryption: 3DES Hashing: SHA-1

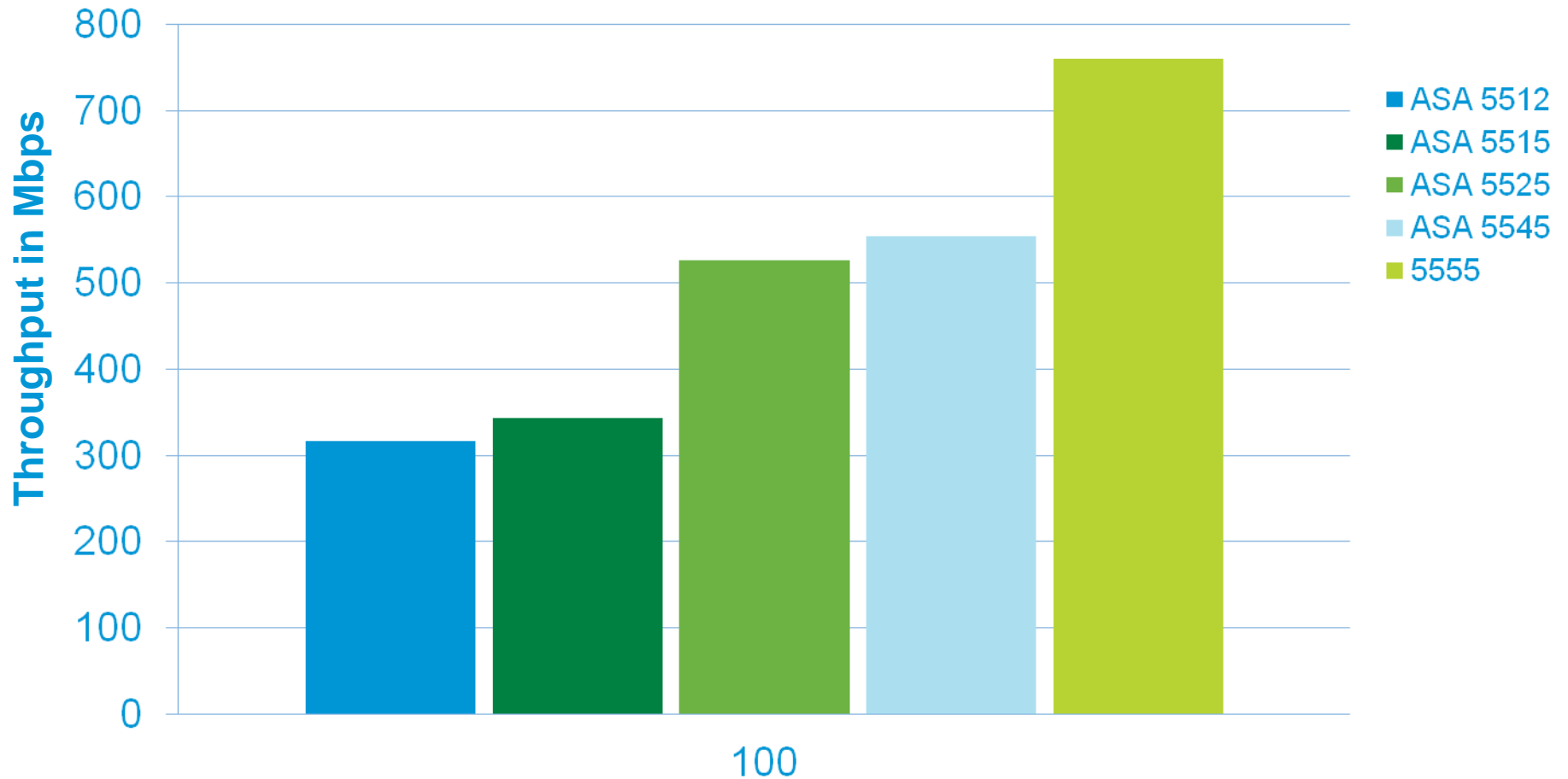
ASA 5585-X IPSEC L2L

Throughput results for HTTP avg pkt size of 450B



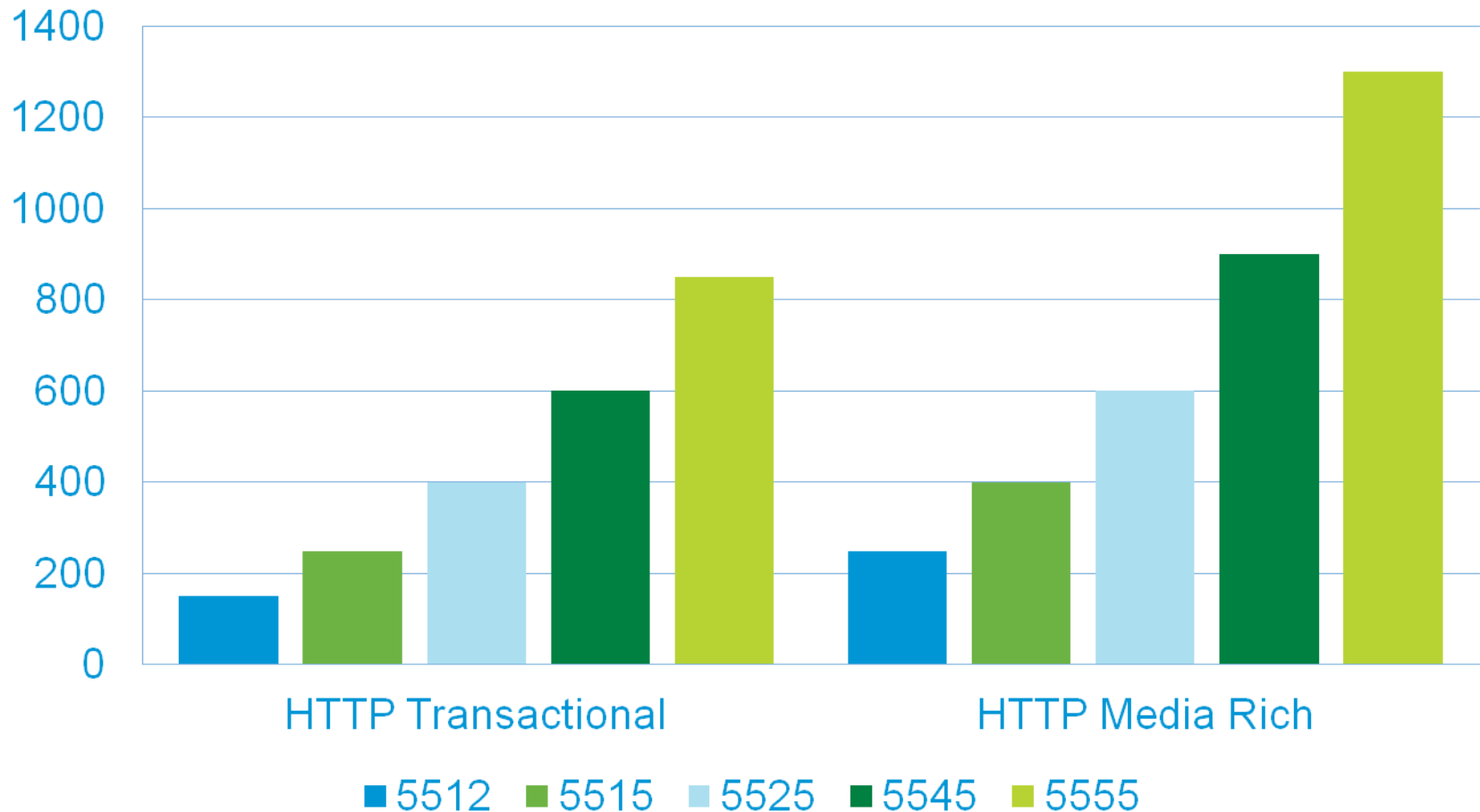
ASA 5585-X IPSEC RAS

Throughput results for HTTP avg pkt size of 450B



5500-X IPS Inline Performance

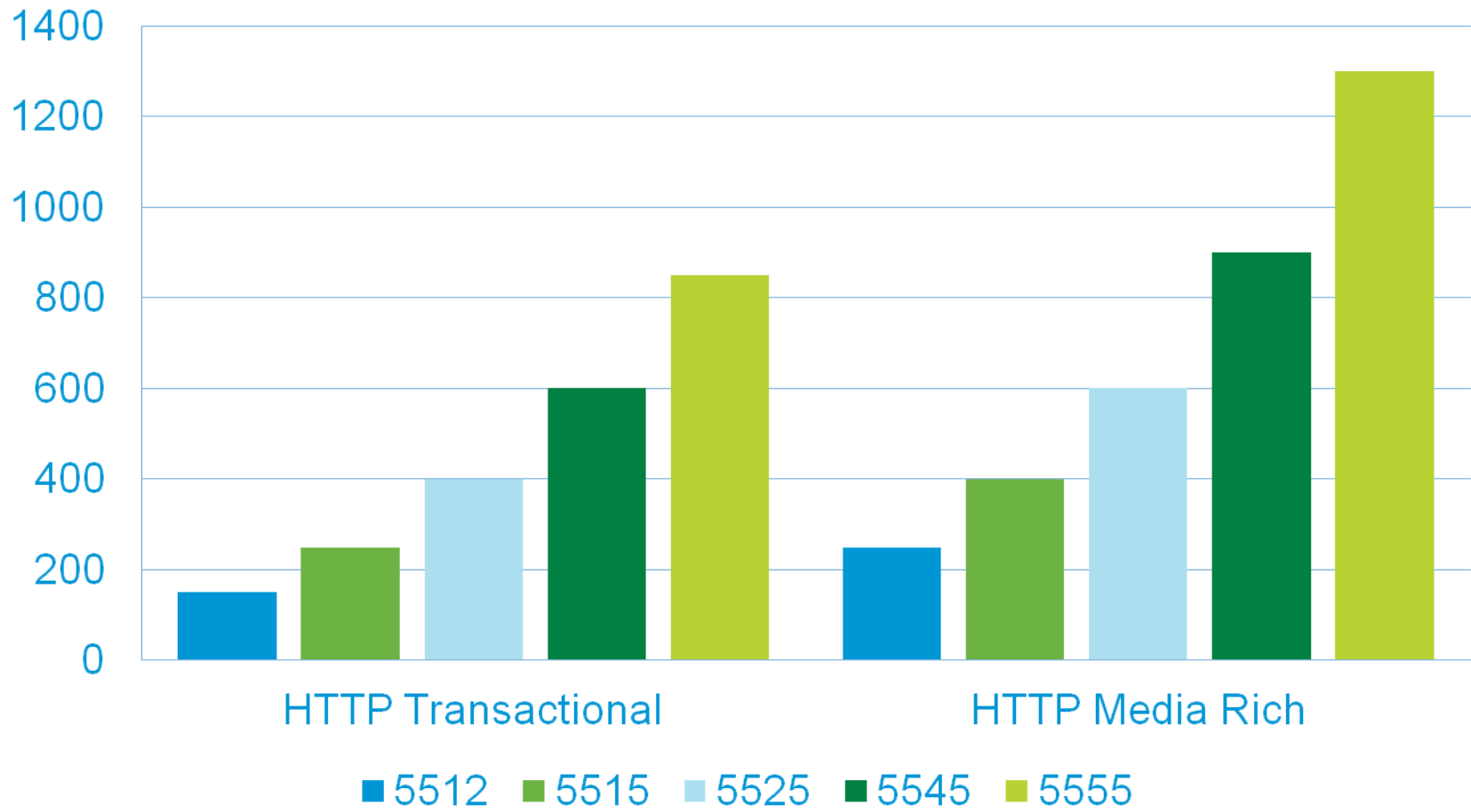
Maximum Throughput (Mbps)



This compares “easy” transactional test with the “difficult” Enterprise Apps test.

5500-X IPS Inline Performance

Maximum Throughput (Mbps)



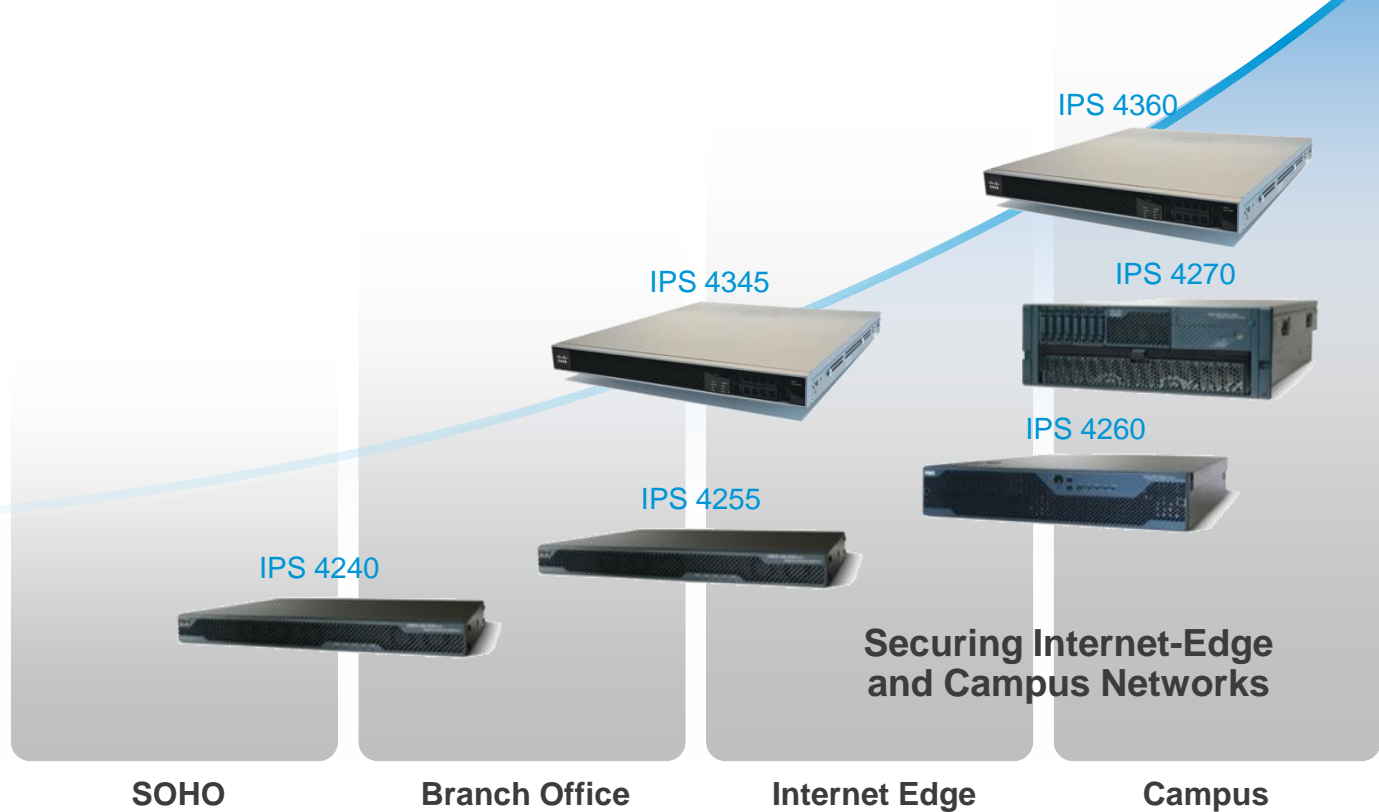
This compares “easy” transactional test with the “difficult” Enterprise Apps test.



Cisco IPS 4300 Series

Cisco Standalone IPS Family

Performance, Scalability, Adaptivity

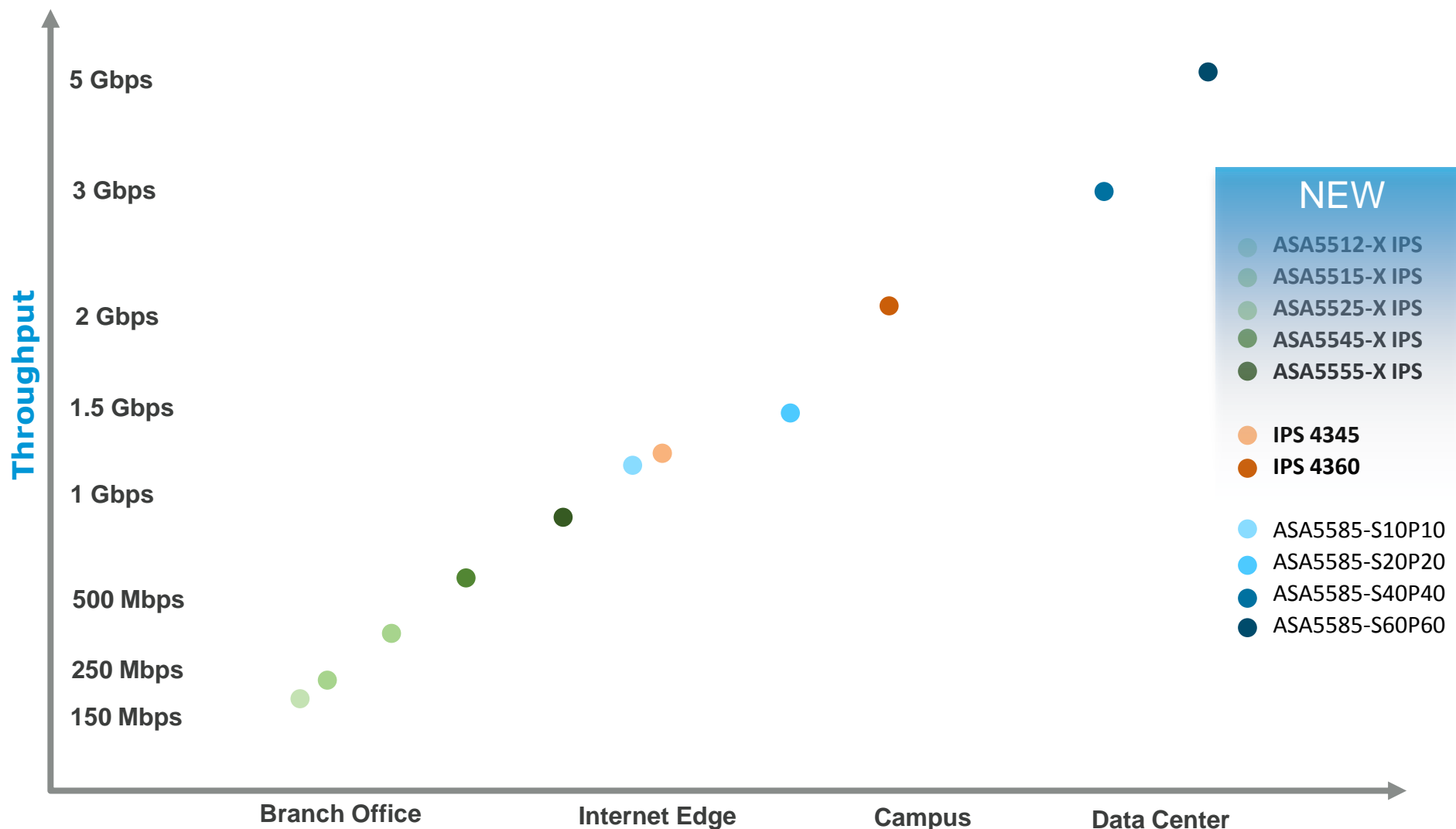


Current Cisco IPS Portfolio





Cisco IPS Performance Positioning

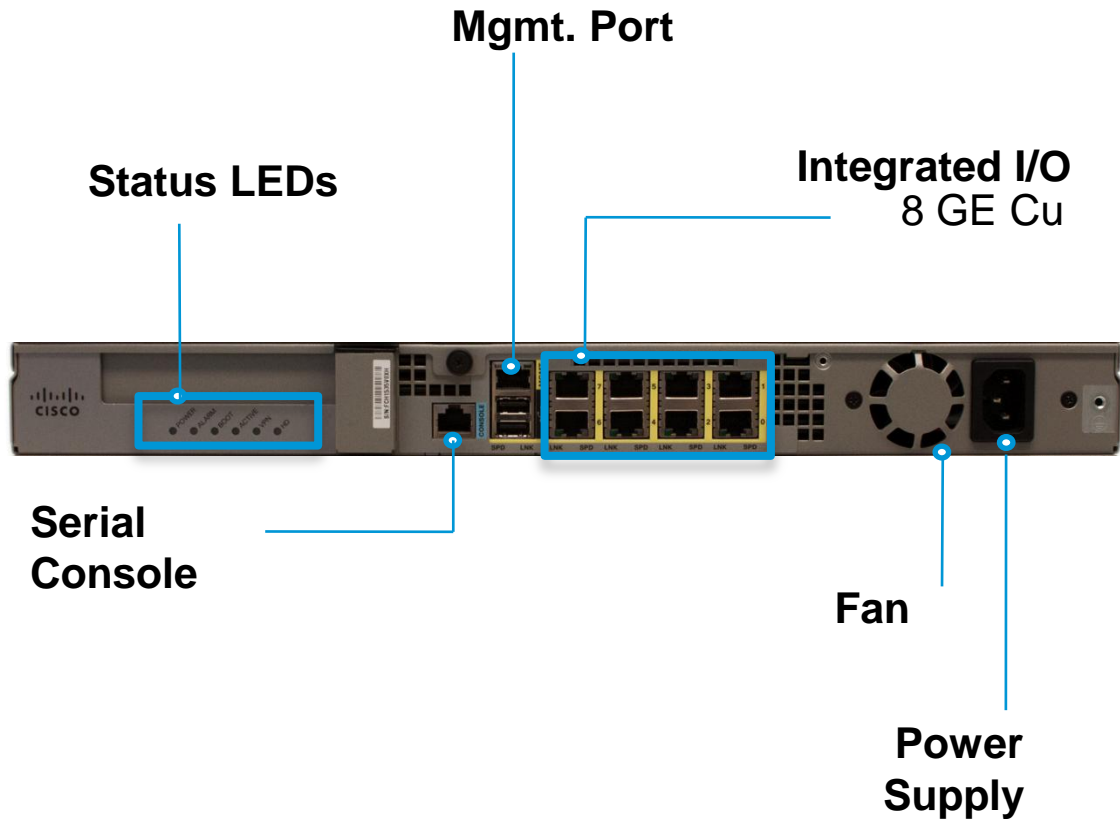
HTTP Transactional IPS Performance



IPS 43xx Series Mid-Range Appliances

	 New IPS 4345	 New IPS 4360
Performance IPS Throughput (Real World)	750 Mbps	1.25 Gbps
Platform Capabilities Max Connections Max Conns/Second Packets/Second (64 byte) Base I/O Average Latency	250,000 20,000 500,000 8 x 1GbE < 100 Micro sec	750,000 50,000 500,000 8 x 1GbE < 100 Micro sec

Cisco IPS 4345



Performance:

- Real World: 750 Mbps
- HTTP Transactional: 1.2 Gbps

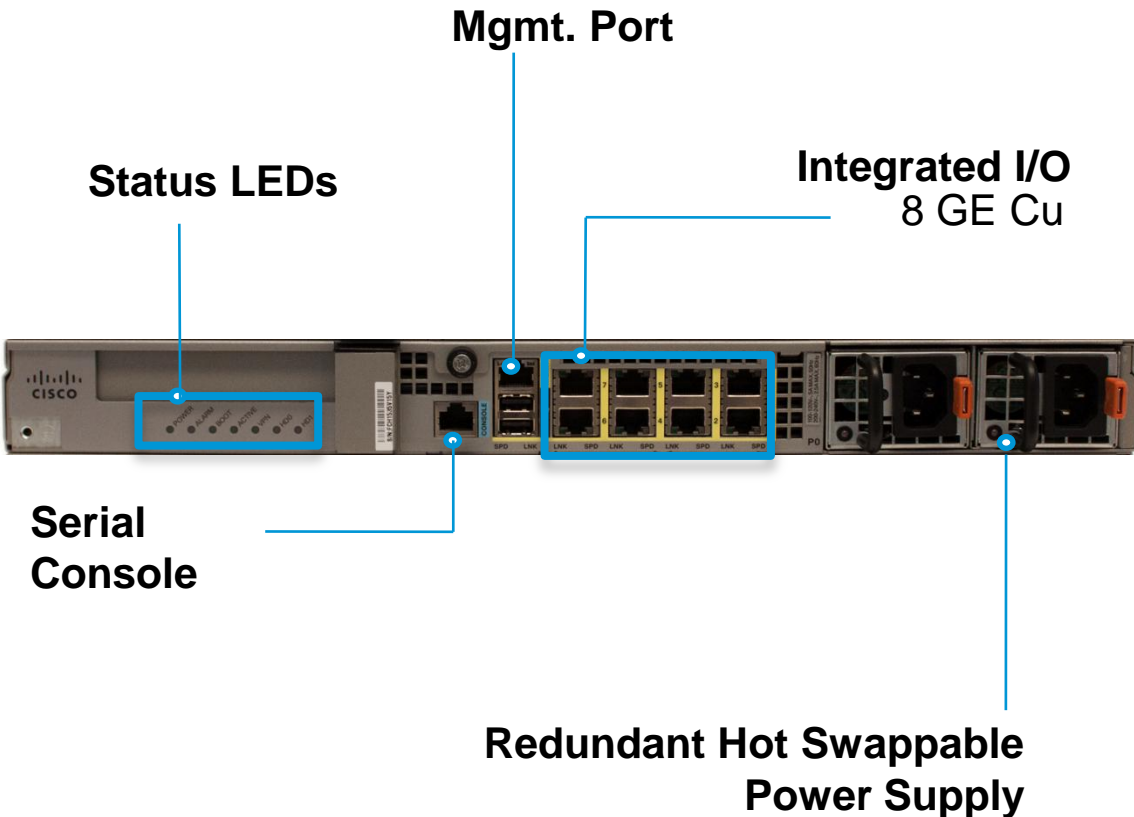
Platform Characteristics:

- 1 RU
- Multi-core enterprise-class CPU (4 Cores/4 Threads)
- 8 GB RAM

Where to Deploy:

- Medium-large enterprises
- Branch – Internet Edge
- 750 Mbps “real-world” IPS throughput requirement
- Dedicated IPS requirement

Cisco IPS 4360



Performance:

- Real World: 1.25 Gbps
- HTTP Transactional: 2 Gbps

Platform Characteristics:

- 1 RU
- Multi-core enterprise-class CPU (4 Cores / 8 Threads)
- 16 GB RAM
- Redundant Power Supply option

Where to deploy:

- Medium-large enterprises
- Internet Edge – Campus
- 1.25 Gbps Real World IPS throughput required
- Requirement for Redundant Power Supply.
- Dedicated IPS requirement

IPS 4345/60 versus IPS 4240/55/60

Key Changes

Performance

- Superior IPS Throughput
- Faster regex processing

Hardware

- Hardware Regex accelerator
- Higher port density
- Multi-core CPUs
- Significantly more memory
- 1 RU form factor
- Redundant Power Supply Option (4360)

Architecture

- 64-bit
- SMP-enabled kernel to make use of the multi-core hardware



4345

-- Fixed Single Power Supply

14"

4360

19"

-- Hot-Swappable
redundant dual power-
supply

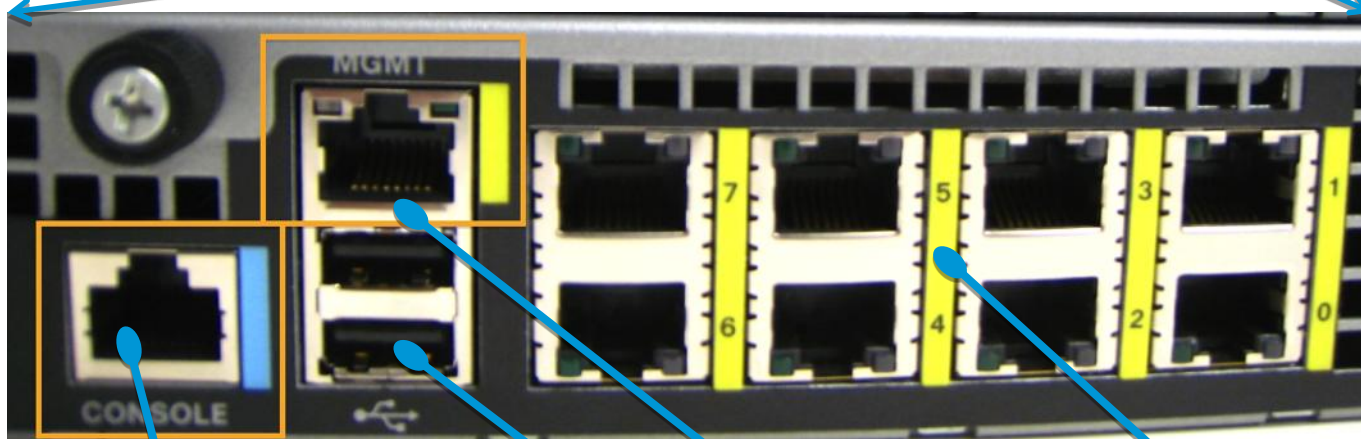
Fan vent for front-to-back
airflow

IPS 43xx Hardware Chassis

Single I/O Expansion slot



4360: Dual Power-Supply



Serial Console Port

Single Mgmt Port
USB Ports

8x 1GbE ports
(numbered left-to-right)

IPS 43xx Back Panel

Hardware comparison with IPS 4240, IPS 4255 and IPS 4260

	IPS 4240	IPS 4255	IPS 4260	IPS 4345	IPS 4360
Form Factor	1 RU	1 RU	2 RU	1 RU	1 RU
CPU	Single Core CPU	Single Core CPU	2 x Single Core CPU	Multi-Core CPU	Multi-Core CPU
Memory	2GB DDR1 RAM	4GB DDR1 RAM	4GB DDR2 RAM	8 GB DDR3 RAM	16GB DDR3 RAM
Interfaces	Base I/O ports limited to 4 x 1GbE Copper interfaces	Base I/O ports limited to 4 x 1GbE Copper interfaces	Base I/O ports limited 1 x 1GbE Copper interface	Base I/O ports up to 8 x 1GbE Copper interfaces	Base I/O ports up to 8 x 1GbE Copper interfaces
PSU	Single Fixed power supply	Single Fixed power supply	Optional Redundant power supply units	Single Fixed power supply.	Redundant Hot-Swappable power supply units
Hardware Regex Capability	N/A	N/A	N/A	Regex accelerator card	Regex accelerator card

Performance

- New Testing Methodology
- BreakingPoint tests
- Test Results

New Testing Methodology

- Determine maximum throughput with a mixture of various protocols and packet sizes.
- Traffic mixes vary depending on network type and location.
- Standard Breaking Point tests representing different traffic mixes:
 - Enterprise Applications
 - Enterprise Datacenter
 - Small/Medium Business
 - Service Provider
 - Higher Education

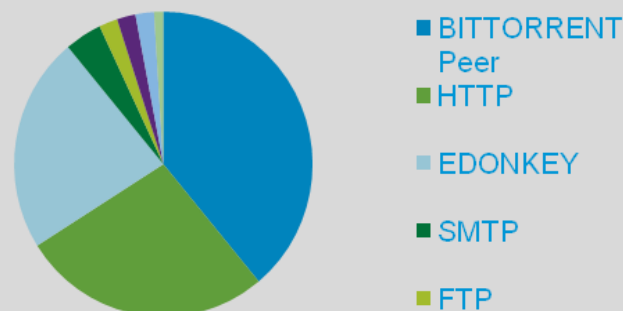
Advantages of Breaking Point tests

- Provide better guidance to customers
- Easily reproducible by customers
- Tests independent of Cisco



BreakingPoint Higher Education

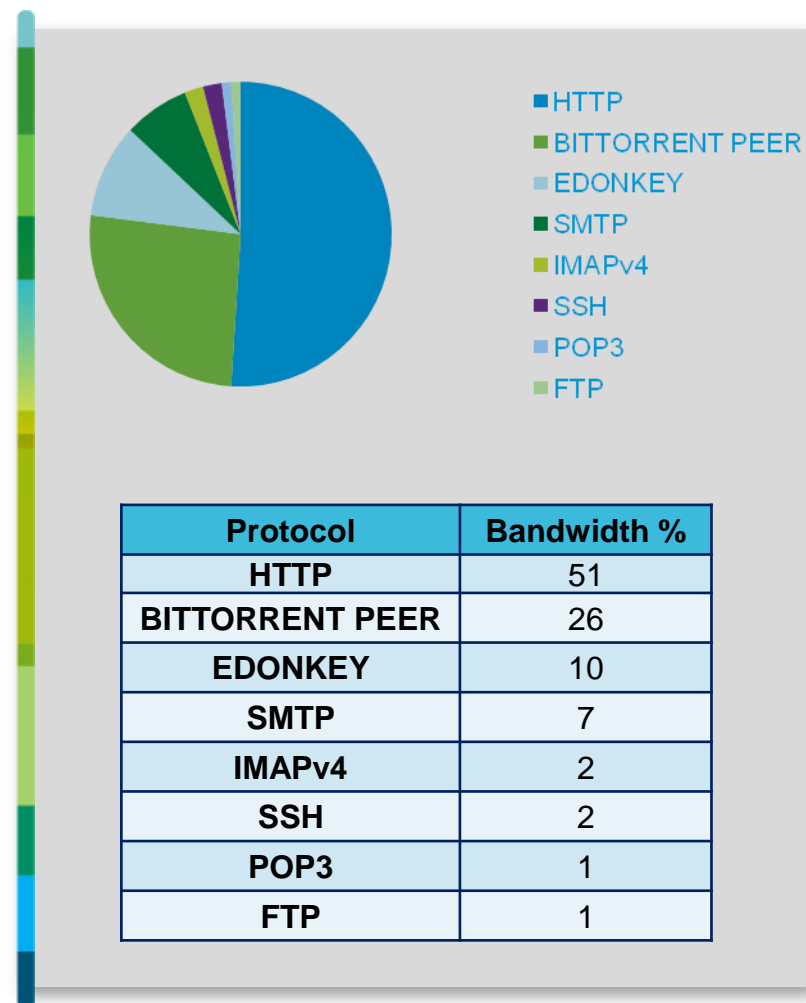
- Represents edge of a “Higher Education” network
- Large percentage of traffic consists of P2P traffic including Bittorrent and Edonkey
- HTTP makes up for about 30% of the bandwidth.



Protocol	Bandwidth %
BITTORRENT Peer	39
HTTP	27
EDONKEY	22
SMTP	4
FTP	2
IMAPv4	2
SSH	2
AOL IM	1

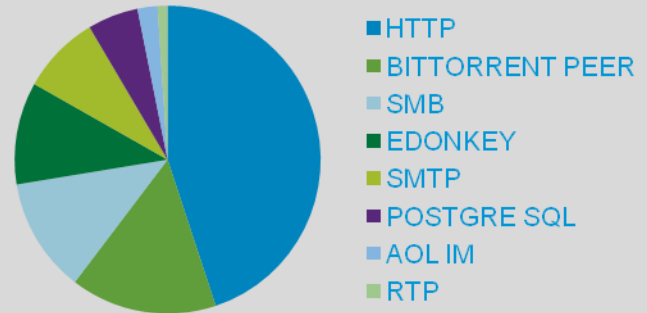
BreakingPoint Service Provider

- Representative for a Service Provider Network
- Statistics collected from a well-known service provider
- Mostly http, followed by peer-to-peer traffic. HTTP text/data, with a fair amount of music and video transfers.
- HTTP and Peer-to-peer make up close to 90% of the traffic



BreakingPoint Small Business

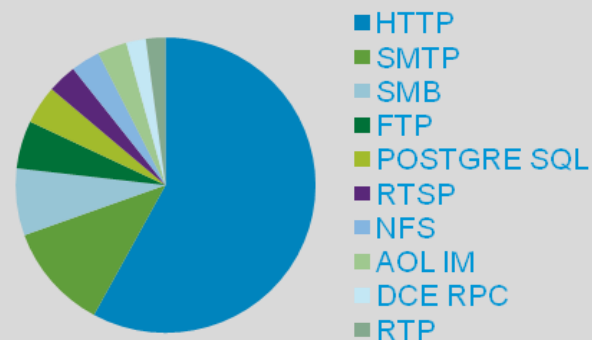
- Internet Edge of a Small Business Network
- Mostly HTTP with voice, database connections and file transfers



Protocol	Bandwidth %
HTTP	43
BITTORRENT PEER	14
SMB	11
EDONKEY	10
SMTP	8
POSTGRE SQL	5
AOL IM	2
RTP	1

BreakingPoint Enterprise Applications

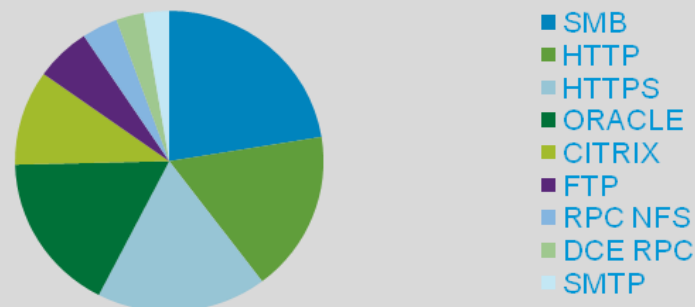
- Representative for traffic used by various applications on an enterprise network
- Wide distribution of protocols, including SMTP, SMB, RTP and others.



Protocol	Bandwidth %
HTTP	55
SMTP	11
SMB	7
FTP	5
POSTGRE SQL	4
RTSP	3
NFS	3
AOL IM	3
DCE RPC	2
RTP	2

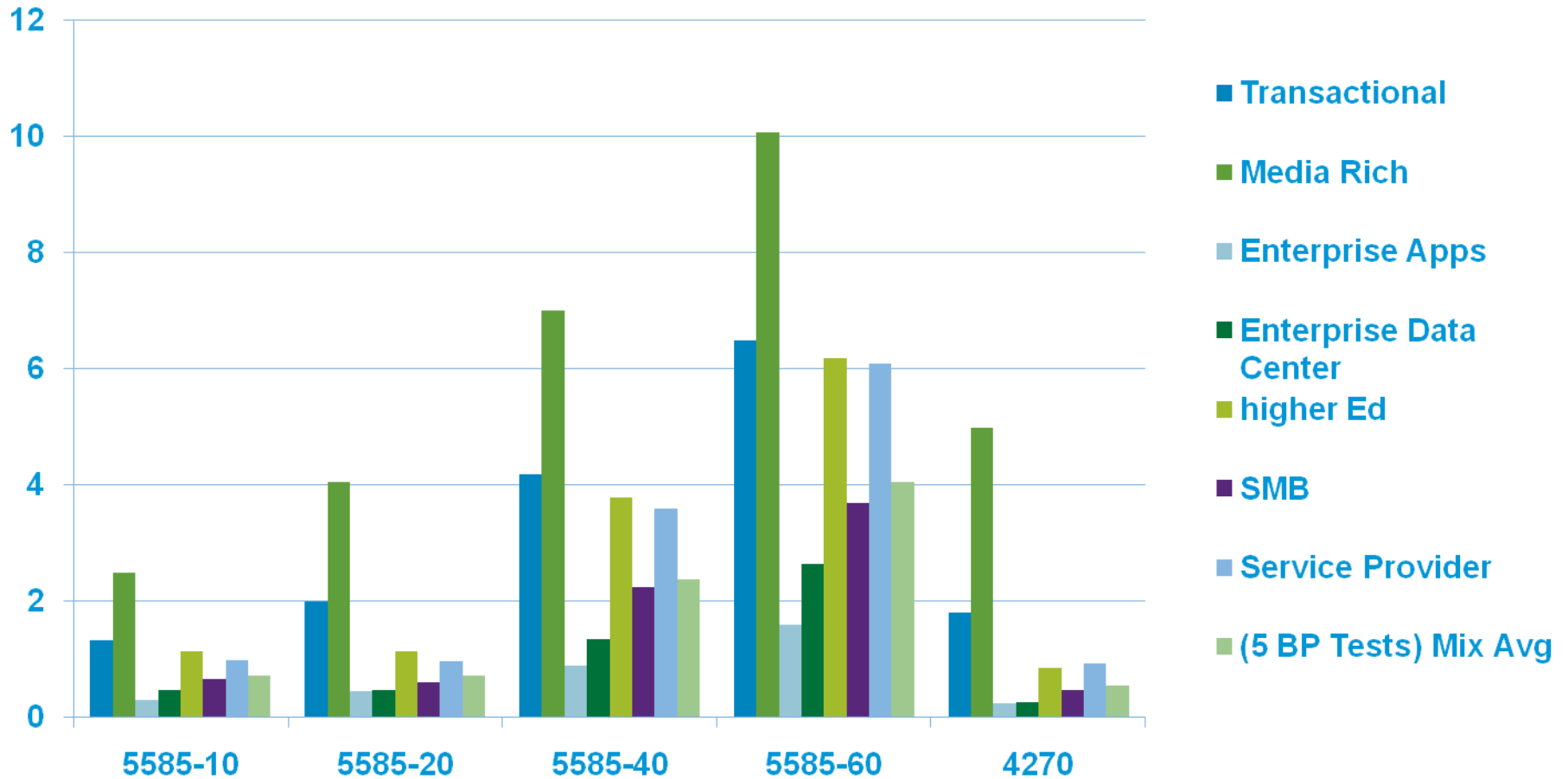
BreakingPoint Enterprise Datacenter

- Datacenter specific
- Most traffic is either file transfer (SMB,FTP), database connection, or HTTP(s)

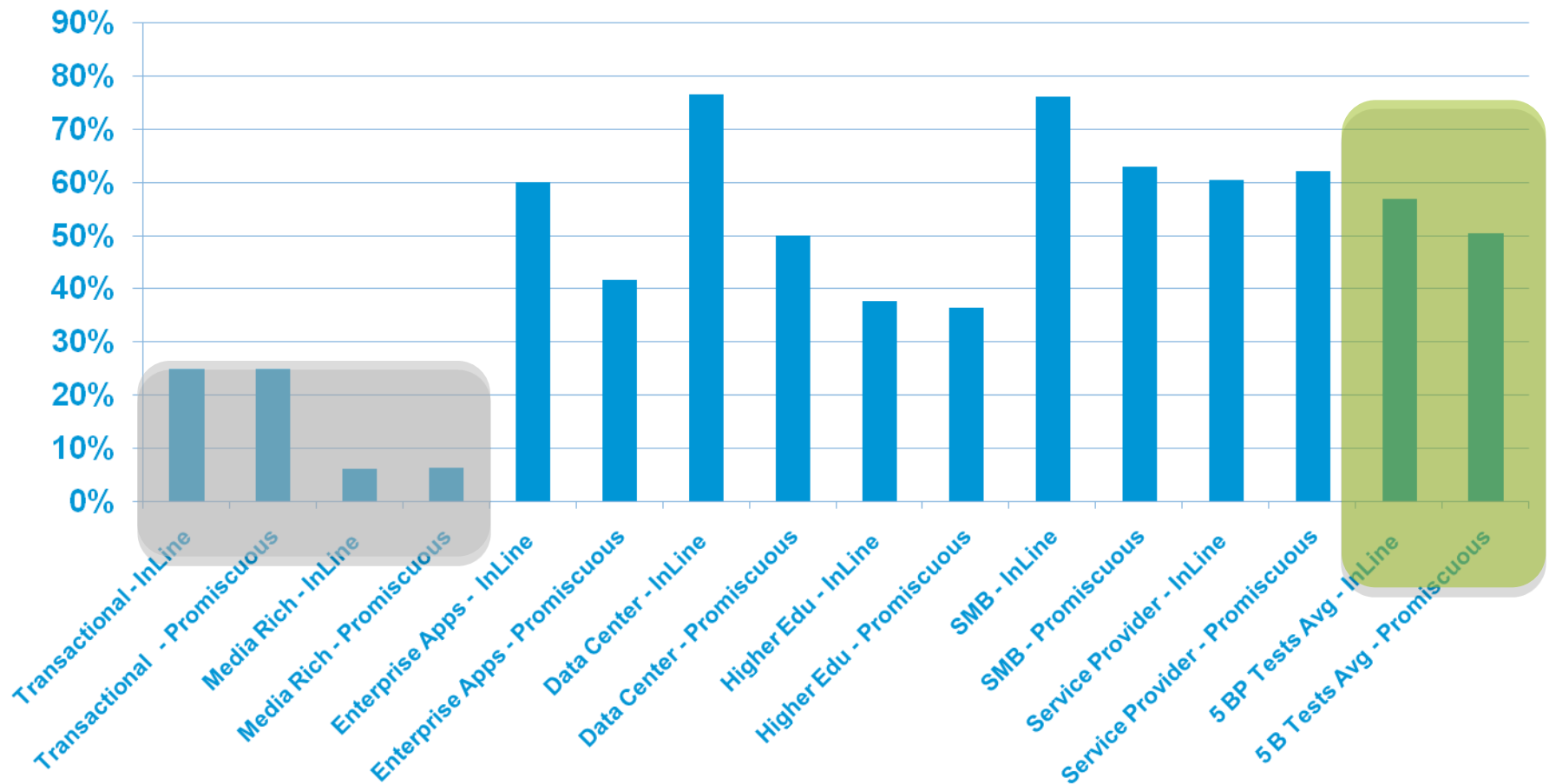


Protocol	Bandwidth %
SMB	21
HTTP	16
HTTPS	16
ORACLE	16
CITRIX	10
FTP	5
RPC NFS	4
DCE RPC	3
SMTP	3

Performance Results with 7.1(3)



Performance Gains With 7.1(3)



What's New ?

Identity Firewall with IPS

Who:

#	Enabled	Source	User	Destination	Service	Action	Logging	Time	Description
global_mpc_1									
1	<input checked="" type="checkbox"/>	any	Sales Marketing	any	IP ip	Permit			Rule to send traffic from Sales/Marketing users to Vs0 in inline mode
global_mpc									
1	<input checked="" type="checkbox"/>	any	NetOps SecOps	any	IP ip	Permit			Rule to send traffic from SecOps/NetOps users to Vs1 in promiscuous mode

What To Do:

Traffic Classification									
Name	#	Enabled	Match	Source	Destination	Service	Time	Rule Actions	Description
Global; Policy: global-policy									
CMPA_IPS_MGMT	1	<input checked="" type="checkbox"/>	Match	any	any	IP ip		ips promiscuous, permit traffic, sensor vs1	Rule to send traffic from SecOps/NetOps users to Vs1 in promiscuous mode
CMPA_IPS_USERS	1	<input checked="" type="checkbox"/>	Match	any	any	IP ip		ips inline, permit traffic, sensor vs0	Rule to send traffic from Sales/Marketing users to Vs0 in inline mode

Industrial Control Systems Security

- Regulations and severity of impact driving interest in protecting industrial systems
- Cisco has contracted with a world renowned leader in industrial security to create highly specialized signatures
- Sold as license (honor system enforcement)
- Delivered with current signatures
- 20+ new signatures a quarter



Industrial Control Signature Coverage

All types of equip.

- SCADA
- DCS
- PLC
- SIS
- EMS
- All major vendors
 - Schneider
 - Siemens
 - Rockwell
 - GE, ABB
 - Yokogawa
 - Motorola
 - Emerson
 - Invensys
 - Honeywell
 - SEL
- and growing..

Policies

- sig1
- sigNhi
- sig0
- sigJeremy
- sigFrank
- demo
 - Active Signatures
 - Adware/Spyware
 - Attack
 - Configurations
 - DDoS
 - DoS
 - Email
 - IOS IPS
 - Instant Messaging
 - L2/L3/L4 Protocol
 - Network Services
 - OS
 - Other Services
 - P2P
 - Reconnaissance
 - Releases
 - TelePresence
 - UC Protection
 - Viruses/Worms/Trojan
 - All Signatures

Configuration > Policies > Signature Definitions > demo > All Signatures

Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine
						Alert and Log	Deny	Other		
50011/0	WORM_MYTOB	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50011/1	WORM_MYTOB	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50012/0	TROJ_SMALL	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50012/1	TROJ_SMALL	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50012/2	TROJ_SMALL	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50012/3	TROJ_SMALL	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/0	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/1	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/2	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/3	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/4	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Default	Multi String
50013/5	BKDR_VANBOT	✓	Medium	100	75	Alert	✗ Packet	✗ Reset Tcp	Tuned	Multi String
61011/0	Modbus Illegal Read Coils Request Parameters	✓	Medium	75	56	Alert			Custom	String TCP
61012/0	Modbus Illegal Read Coils Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61015/0	Modbus Illegal Read Coils Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61021/0	Modbus Illegal Read Discrete Inputs Request Parameters	✓	Medium	75	56	Alert			Custom	String TCP
61022/0	Modbus Illegal Read Discrete Inputs Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61025/0	Modbus Illegal Read Discrete Inputs Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61031/0	Modbus Illegal Read Holding Registers Request Parameters	✓	Medium	75	56	Alert			Custom	String TCP
61032/0	Modbus Illegal Read Holding Registers Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61035/0	Modbus Illegal Read Holding Registers Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61041/0	Modbus Illegal Read Input Registers Request Parameters	✓	Medium	75	56	Alert			Custom	String TCP
61042/0	Modbus Illegal Read Input Registers Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61045/0	Modbus Illegal Read Input Registers Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61051/0	Modbus Illegal Write Single Coil Request Parameters	✓	Medium	75	56	Alert			Custom	String TCP
61052/0	Modbus Illegal Write Single Coil Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61151/0	Modbus Illegal Write Multiple Coils Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61161/0	Modbus Illegal Write Multiple Registers Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61201/0	Modbus Illegal Read File Record Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61205/0	Modbus Illegal Read File Record Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61211/0	Modbus Illegal Write File Record Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61215/0	Modbus Illegal Write File Record Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61231/0	Modbus Illegal Read/Write Multiple Registers Request Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61235/0	Modbus Illegal Read/Write Multiple Registers Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61245/0	Modbus Illegal Read FIFO Queue Response Parameters	✓	Medium	75	56	Alert			Custom	Service Generic
61905/0	SIS Remote Programming Mode Unlock	✓	Medium	75	56	Alert			Custom	Service Generic
62077/0	Modbus Unauthorized Write Request	✓	Medium	75	56	Alert			Custom	String TCP
62088/0	Modbus Illegal Function Code Response	✓	Info...	75	18				Custom	String TCP
62088/1	Modbus Function Code Scan	✓	Medium	75	56	Alert			Custom	Meta
62097/0	Modbus Point List Scan	✓	Medium	75	56	Alert			Custom	String TCP
63002/0	DNP3 DDL Empty User Data Denial of Service	✓	Medium	75	56	Alert			Custom	String TCP

Sensor Setup

Interfaces

Policies

Default Signature Reset

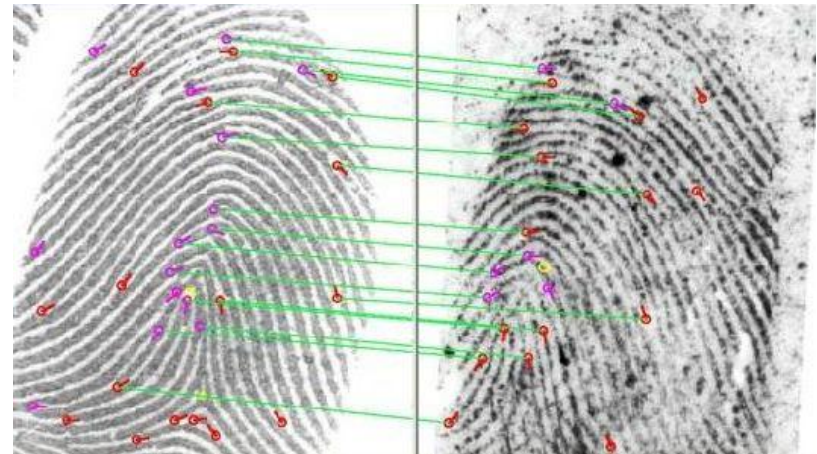
- What is Happening?

Sig team is doing a review of our default signature settings
- Why?

Improve performance impacts and current threat updates
- When is this Happening?

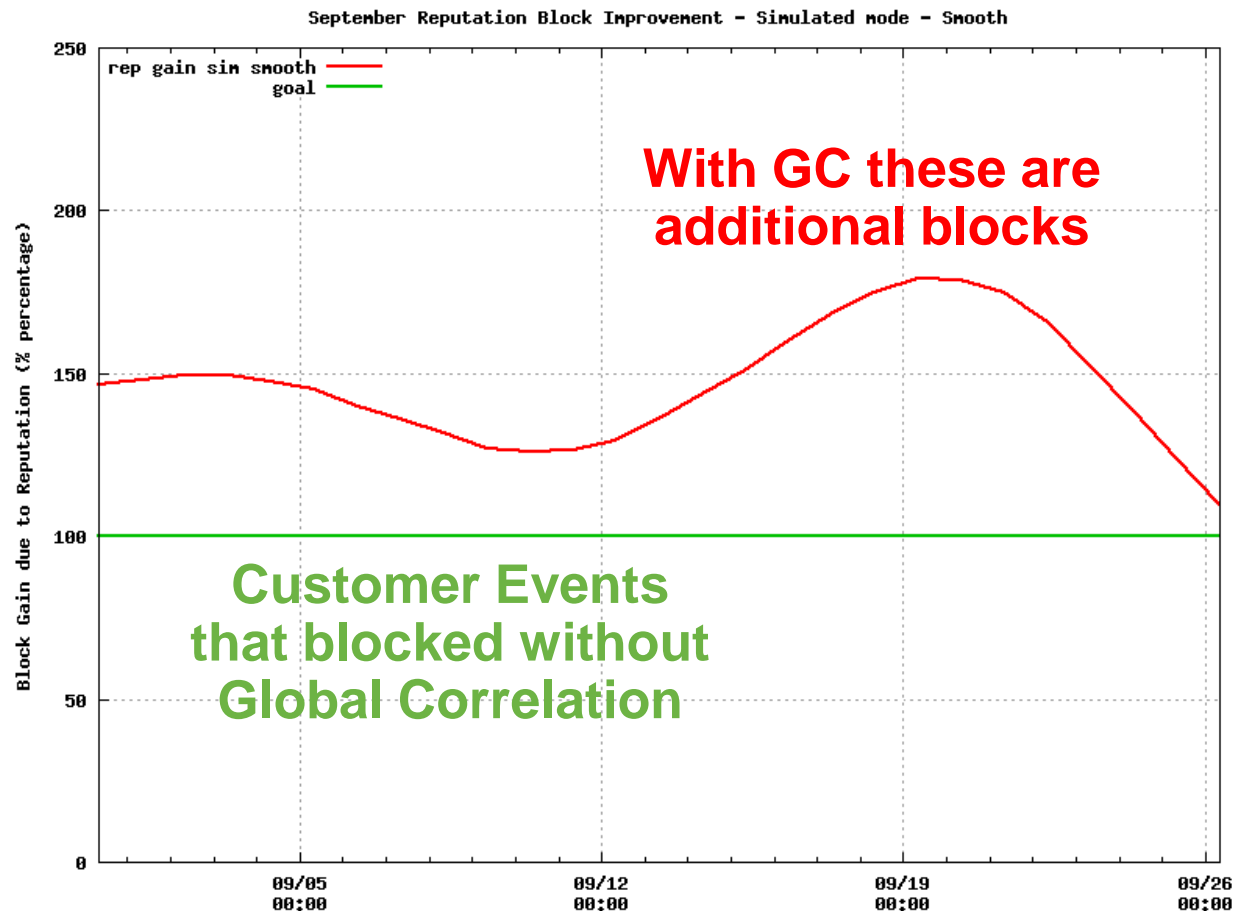
Started in November 2011. finish by February 2012.

Slow roll-out to avoid sudden impacts or customer alarm



Global Correlation Impact

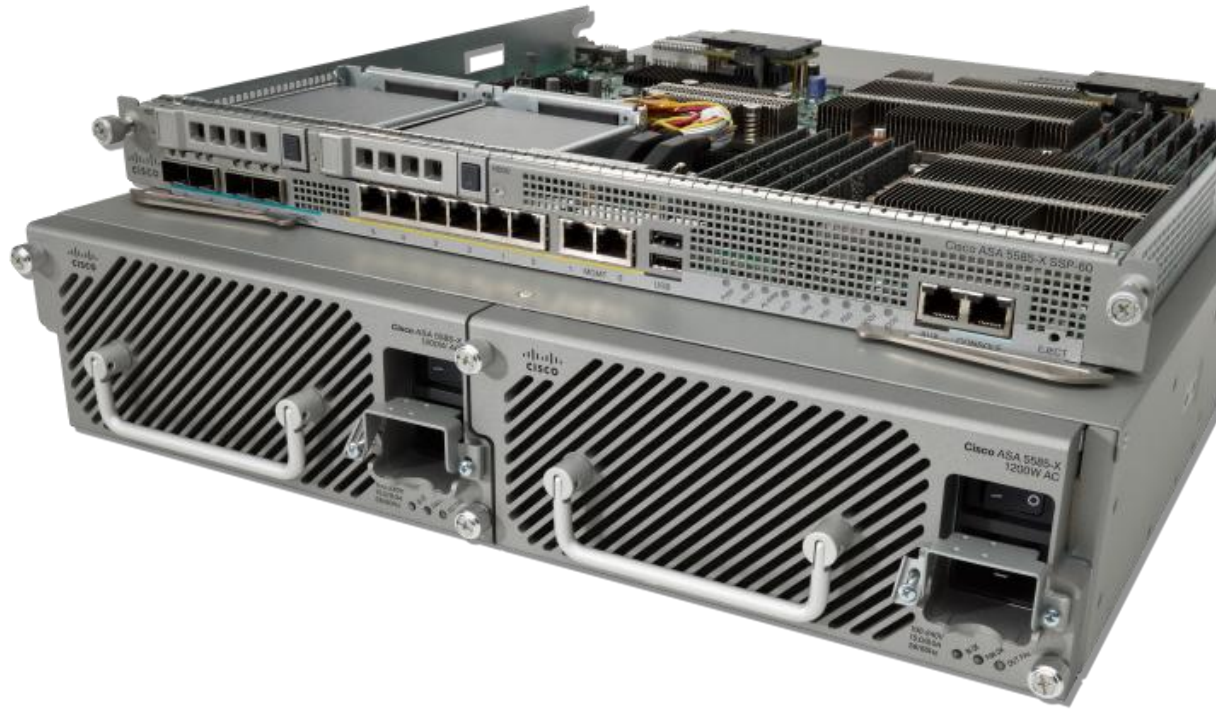
- Impact almost exclusively at Internet Edge
- Hard to prove - Recognize we must find ways to show its relevance



ASA CX

ASA CX

- Context-Aware Firewall
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- Secure Mobility
- SSP-10 and SSP-20



ASA CX – Front View

CX SSP

ASA CX



ASA SSP

Order separate blades or chassis bundle

Requires ASA version 8.4.4

Cisco Prime Security Manager (PRSM)

Build-in

- Configuration, Eventing, and Reporting

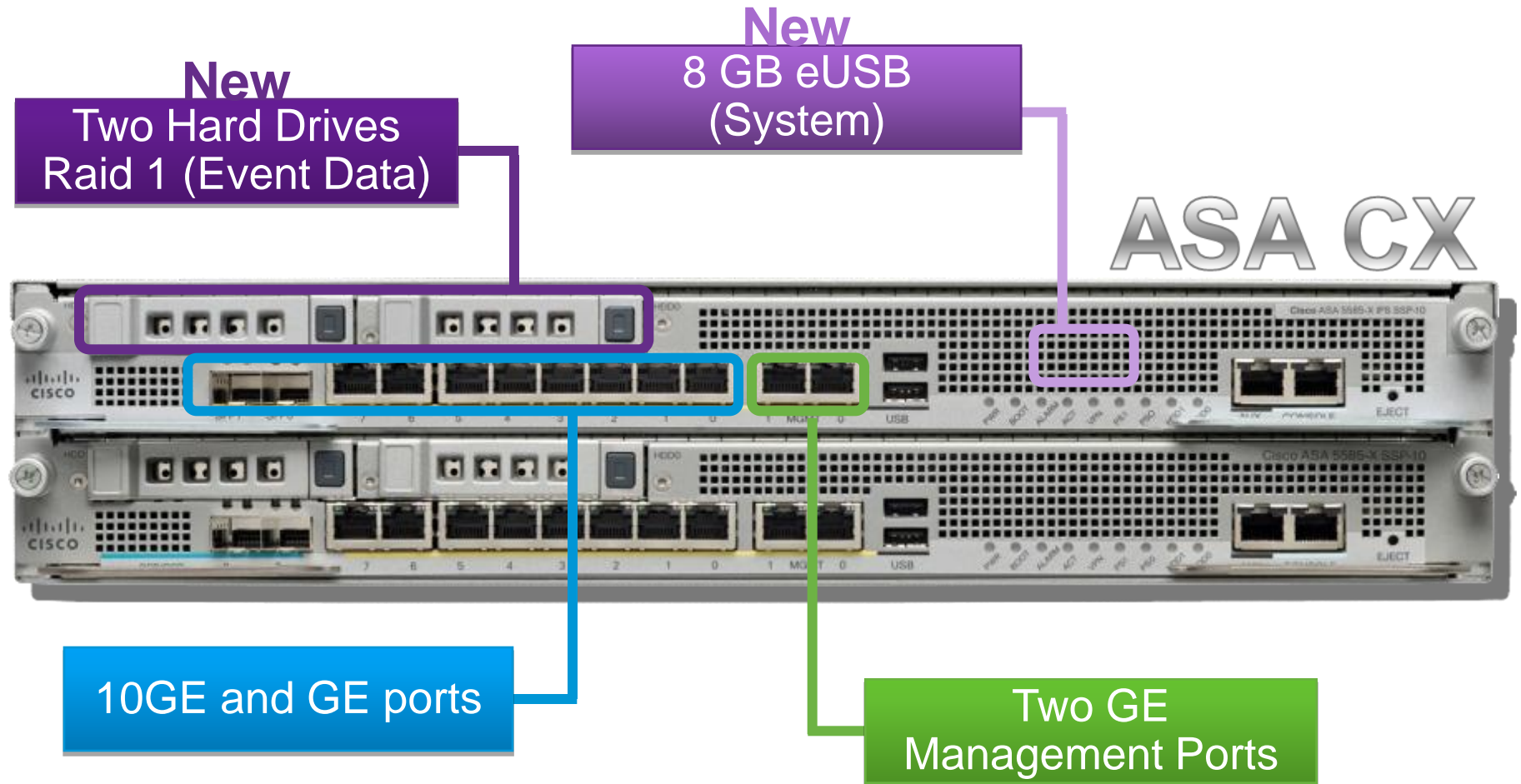
Off-box

- Multi-device Manager for ASA CX
- Supports 25 Chassis (estimate)
- Role Based Access Control
- Virtual Machine or UCS Virtual Appliance

Virtual Machine supports
VMWare ESX 4.1

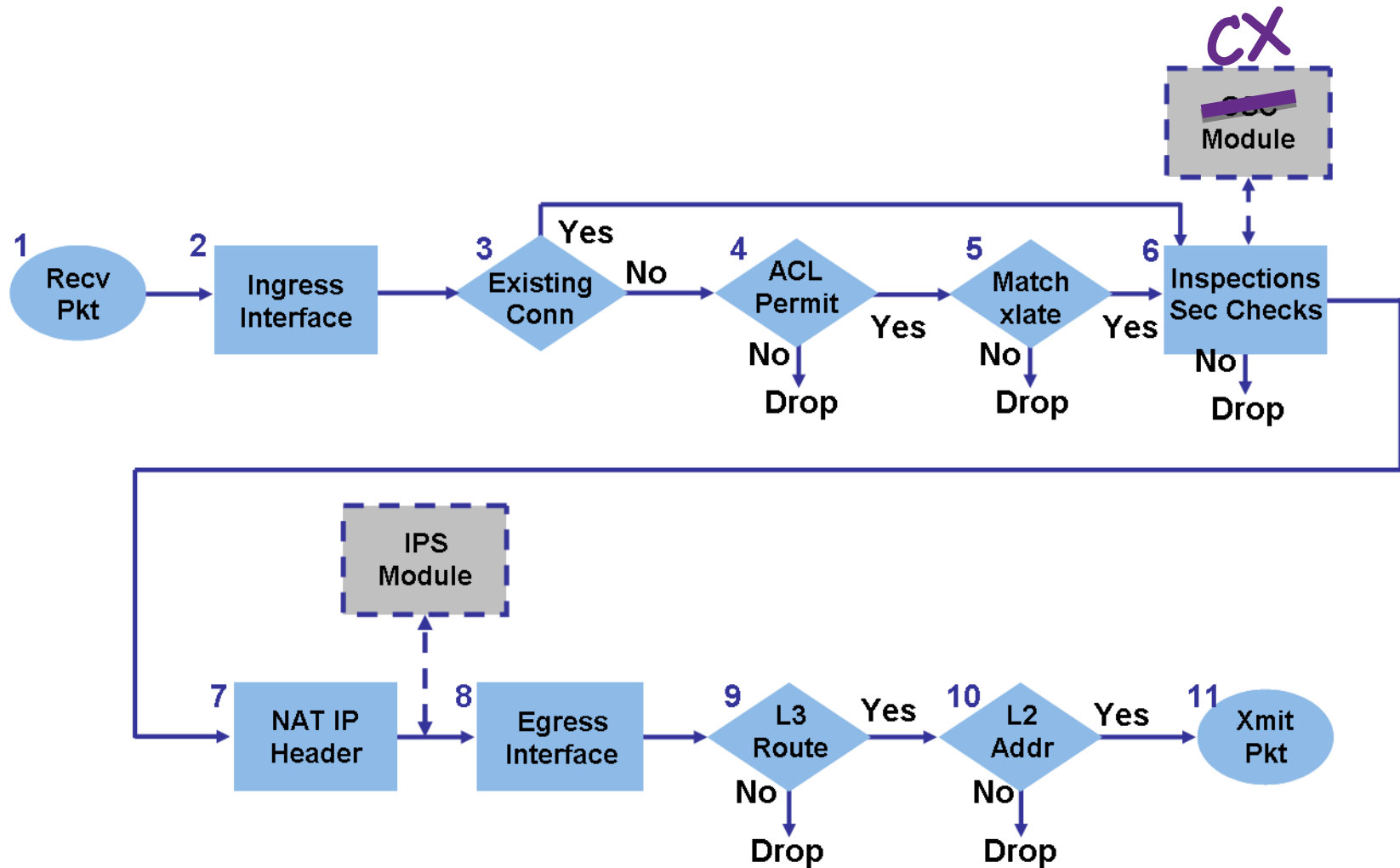


ASA CX – Front View



Packet Processing Flow Diagram

Cisco.com



Send traffic to CX SSP

- Use MPF to direct traffic to the CX blade:

```
policy-map global_policy
  class class-default
    cxsc fail-open auth-proxy

service-policy global_policy global
```

- PRSM Multi-device applies this when connecting to CX:



Policy types

Authentication

- How to identify user?



Decryption

- What to decrypt?



Access




- Allow or Deny?

Policy types - Screenshot

Access

Access

Used by device roles: **default**

Features enabled:   

Policy type: **Access**




Number of Policies: **1**

Source	Destination	Application	Action/Conditions
1 ANY	ANY		Allow

Auth

Authentication

Used by device roles: **default**

Features enabled:   

Policy type: **Authentication**




Number of Policies: **1**

Source	Destination	Action/Conditions
1 ANY	ANY	Use Identity When Available Realm: seclabs

Decryption

Decryption

Used by device roles: **default**

Features enabled:   

Policy type: **Decryption**

Number of Policies: **0**

Source	Destination	Action/Conditions
There are no policies in this policy set		

Authentication Policy

Is identity required?

- **Use identity when available**

Passive Auth only

- **Require identity**

Passive Auth if available,
then Active Auth

- **Require authentication**

Active Auth only

The screenshot shows the 'Action' configuration panel. It has a dropdown menu for 'Action' with the following options: 'Require identity' (selected), 'Use identity when available', 'Require identity', and 'Require authentication'. Below this is a 'Realm' dropdown menu with 'Any' selected. At the bottom, there is a text input field for 'Exclude these user agents' with the value 'Any' and a link 'Create new object'.

How to identify user?

- Basic
- NTLM
- Kerberos

The screenshot shows the 'Action' configuration panel. It has a dropdown menu for 'Action' with the value 'Require identity'. Below this is a 'Realm' dropdown menu with the value 'seclabs'. The 'Authentication type' dropdown menu is open, showing the following options: 'Select the type of input' (selected), 'Basic', 'NTLM', 'Kerberos', and 'Negotiate'. At the bottom, there is a text input field for 'Exclude these user agents'.

Decryption

- Decrypt TLS/SSL traffic across any port
- Self-signed (default) certificate or customer certificate/key
- Based on FQDN, URL Category, User/Group, Device type, IP address, or Port
- FQDN and URL Category are determined using server certificate

Access

- Allow or Deny the transaction based on full context
- Other possible actions:
 - Create Event (on by default)
 - Capture Packets (off by default)
- Also applied to HTTP Traffic:
 - File Filtering Profile

Apply added filtering based on MIME type
 - Reputation Profile

Apply added filtering based reputation score of destination
(default profile drops -6.0 and below and is not active)

Enable policy

On

Policy Action

Allow

Ticket ID

Enter Ticket ID

Tags

Enter keyword tags

▼ **Source**

Any

[Create new object](#)

▼ **Destination**

Any

[Create new object](#)

▼ **Application**

Any

[Create new object](#)

▼ **Profile**

File filtering action profile

Select one File filtering profile

[Create new profile](#)

Web reputation action profile

Select one Web reputation profile

[Create new profile](#)

▼ **Policy properties**

Eventing

On

Capture packets

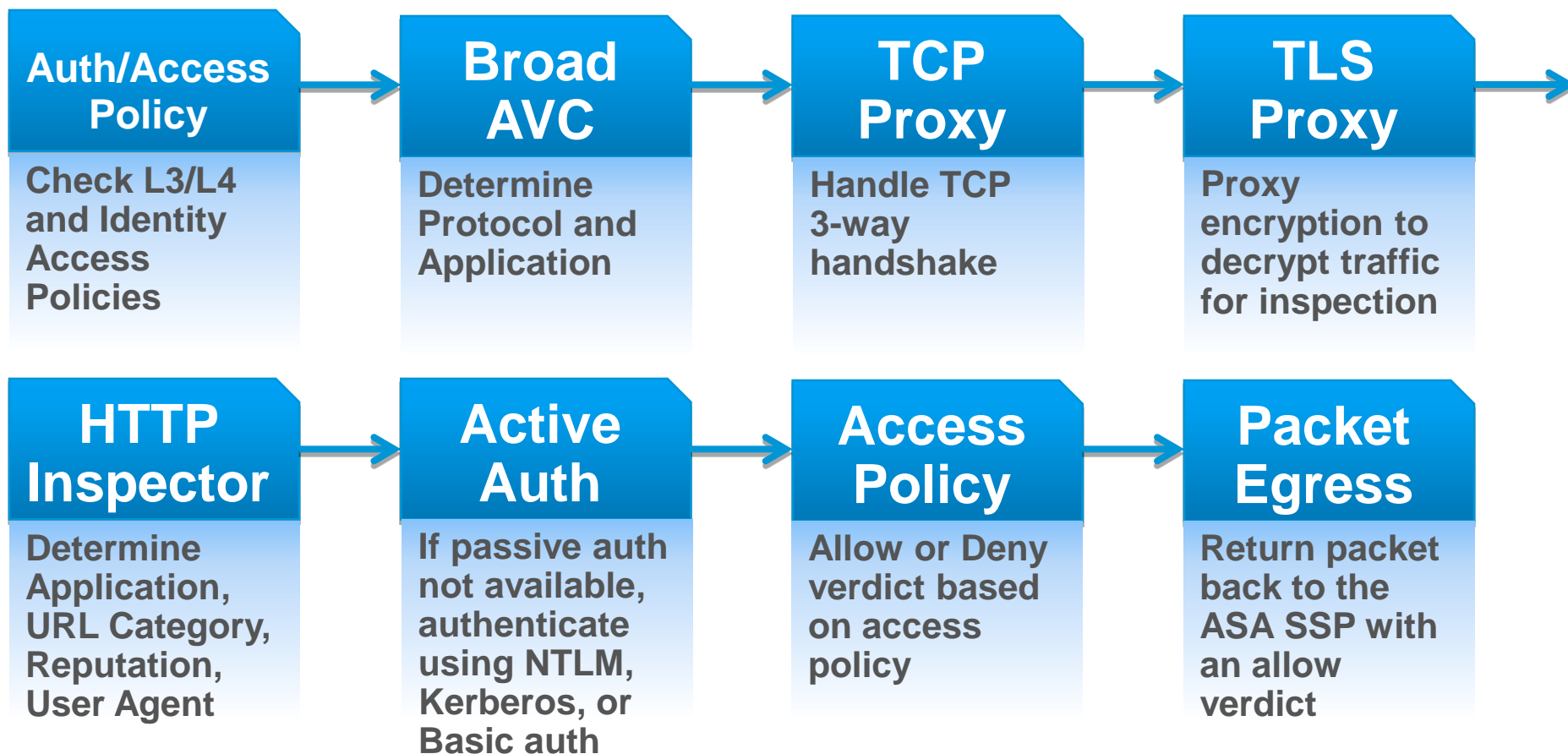
Off

Save policy

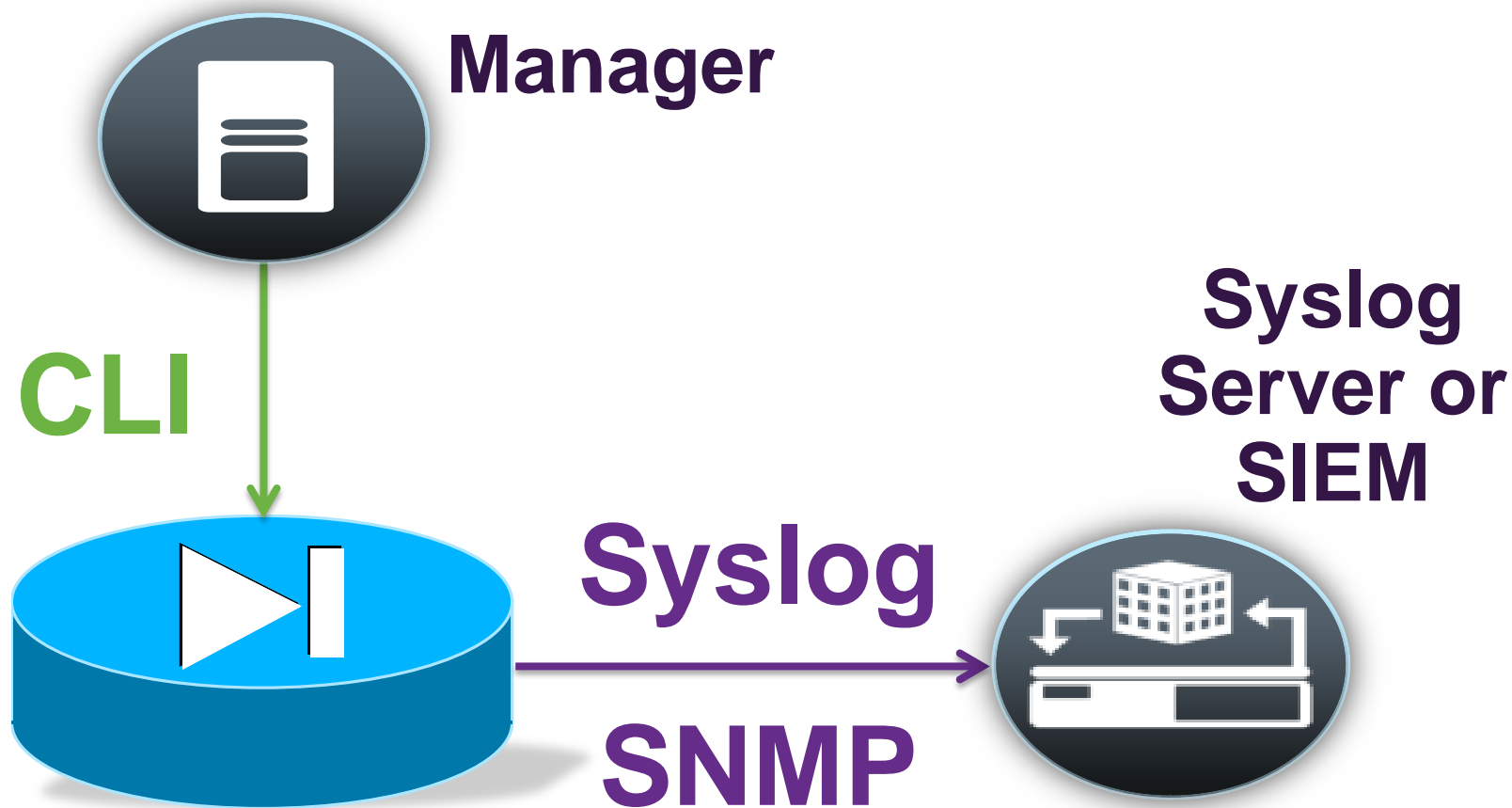
Cancel

Day-in-the-life of a packet

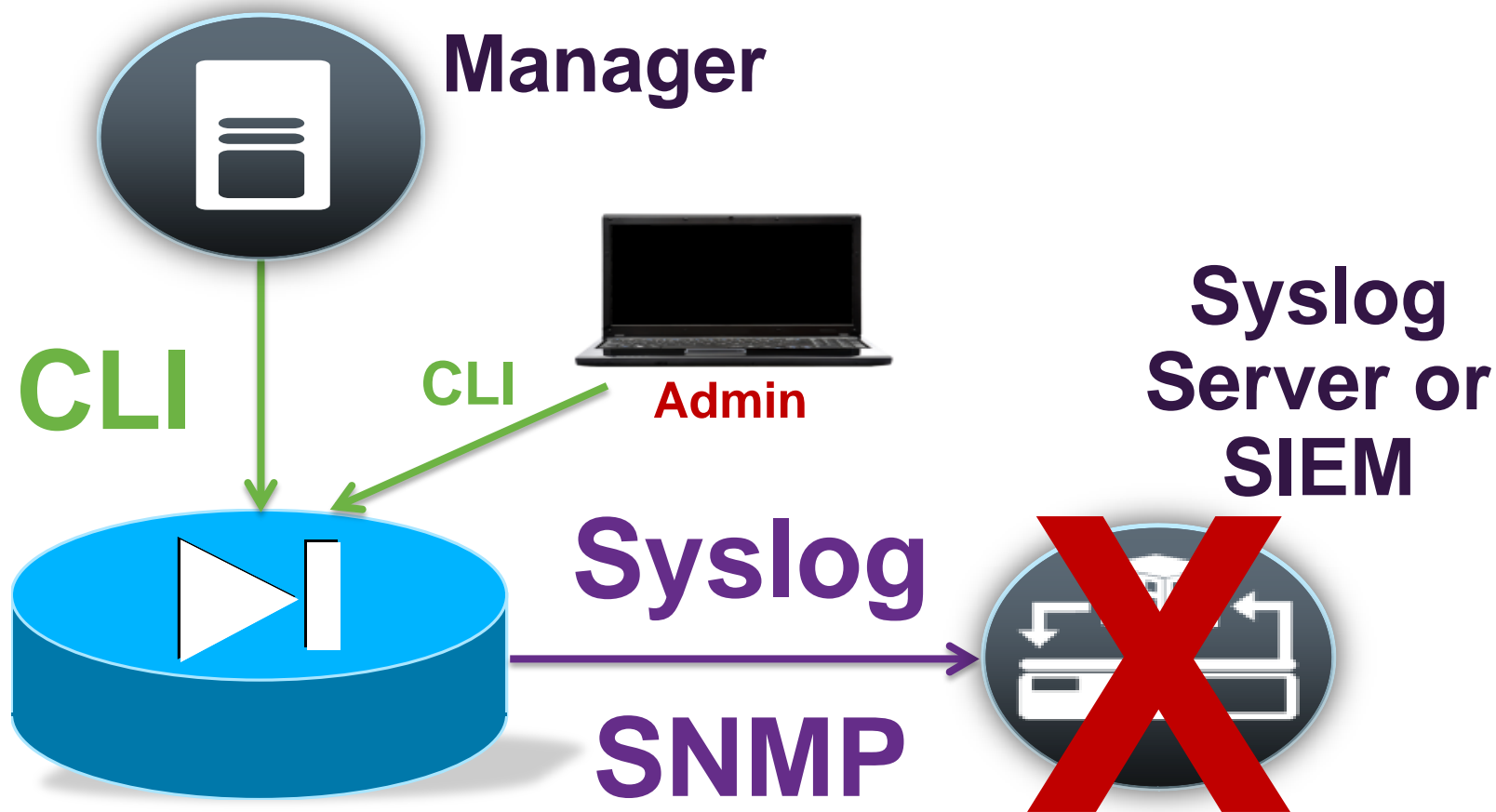
(One possible flow. May be different for other traffic.)



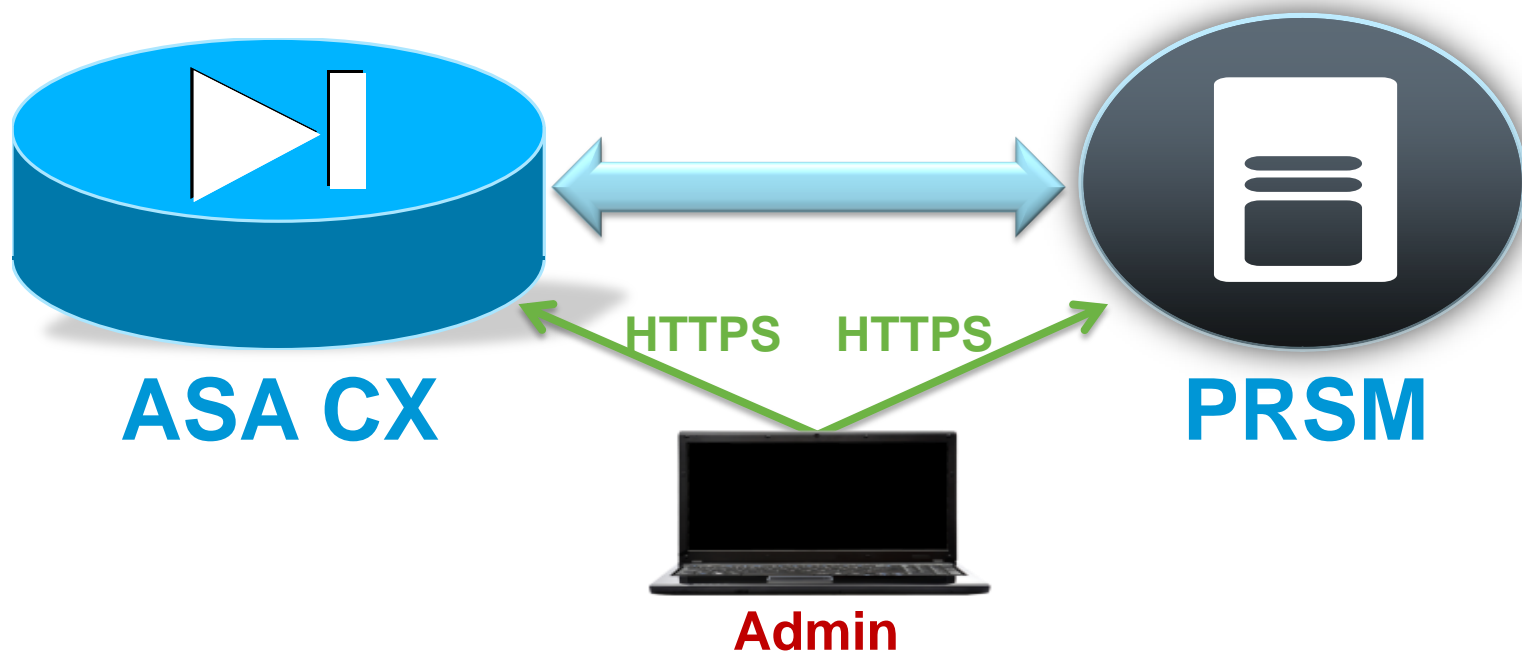
Management Architecture - Today



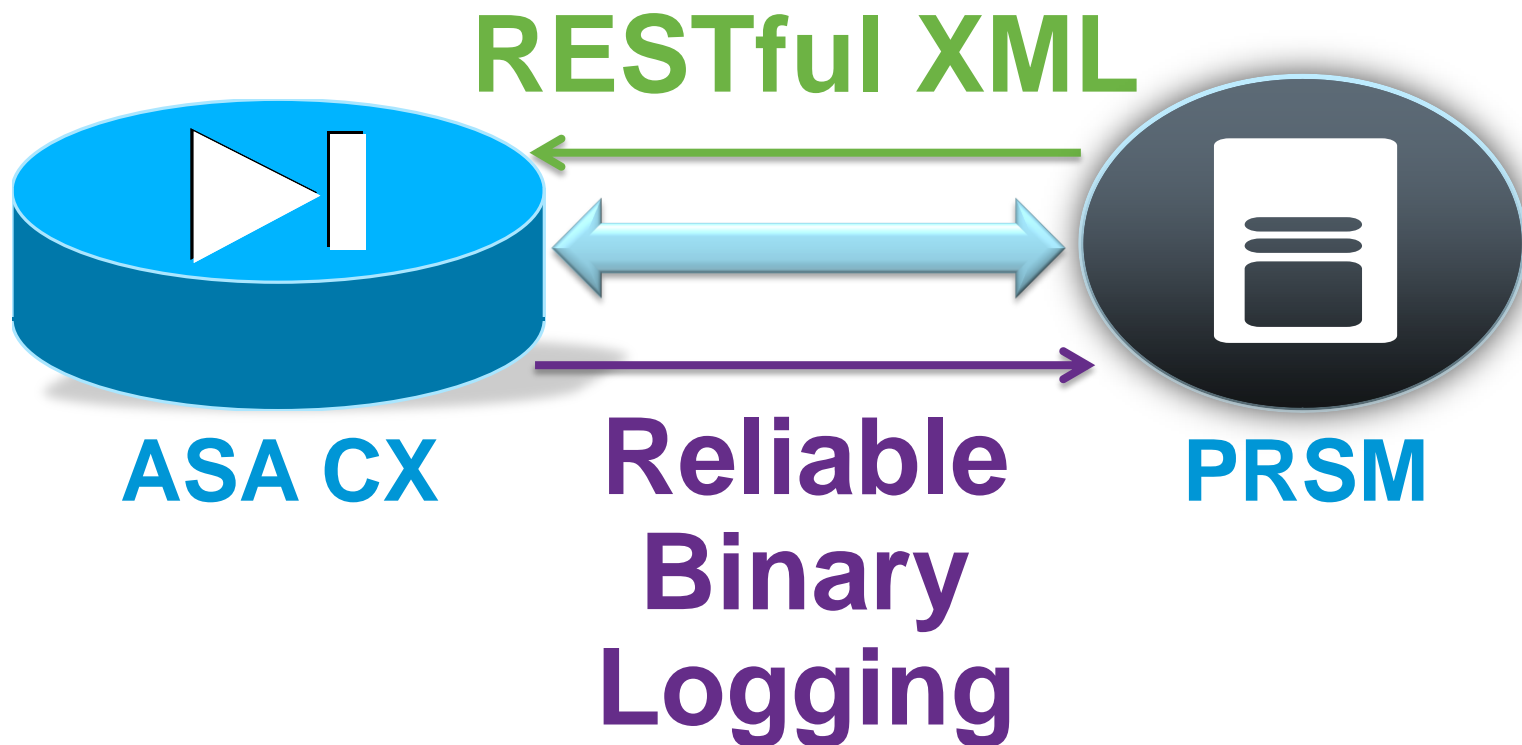
Management Architecture - Today



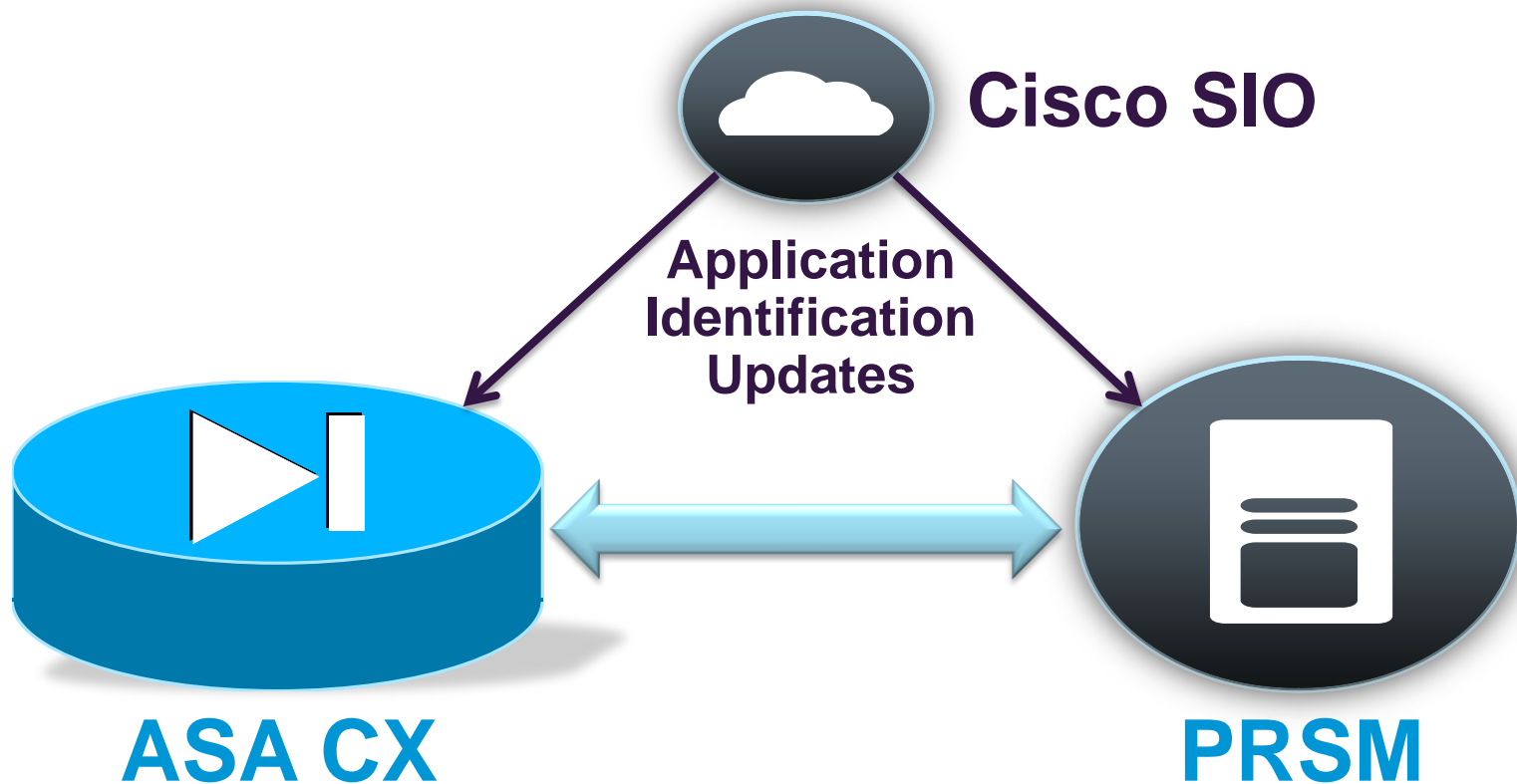
Management Architecture – ASA CX/PRSM



Management Architecture – ASA CX/PRSM



Management Architecture – ASA CX/PRSM





Cisco ASA 1000V Cloud Firewall

Virtual Security: Evolving Security Concerns

Additional Need to Secure Virtual Networks

Hybrid security portfolio for end-to-end security

Consistency across physical and virtual security solutions

Solution scale, span, and simplicity

Extend established best practices to the new virtual and cloud environments

Physical, Virtual, Cloud: End-to-End Security

PHYSICAL

PHYSICAL APPLIANCES AND MODULES

Multi-scale™ data center-class ASA devices



**Cisco ASA
5585-x**



**ASA SM for
Catalyst 6500**

- Scalable in-line performance
- Data center edge security policies
- Flexible deployment options

VIRTUAL & CLOUD

CLOUD FIREWALL

Enhanced cloud security



**Cisco Virtual
Security Gateway
(VSG)**



Cisco ASA 1000V

- Proven firewall to secure your cloud
- Tenant-edge to VM-specific policies
- Automated, policy-based provisioning

Virtual Security Portfolio

Virtual Security Gateway

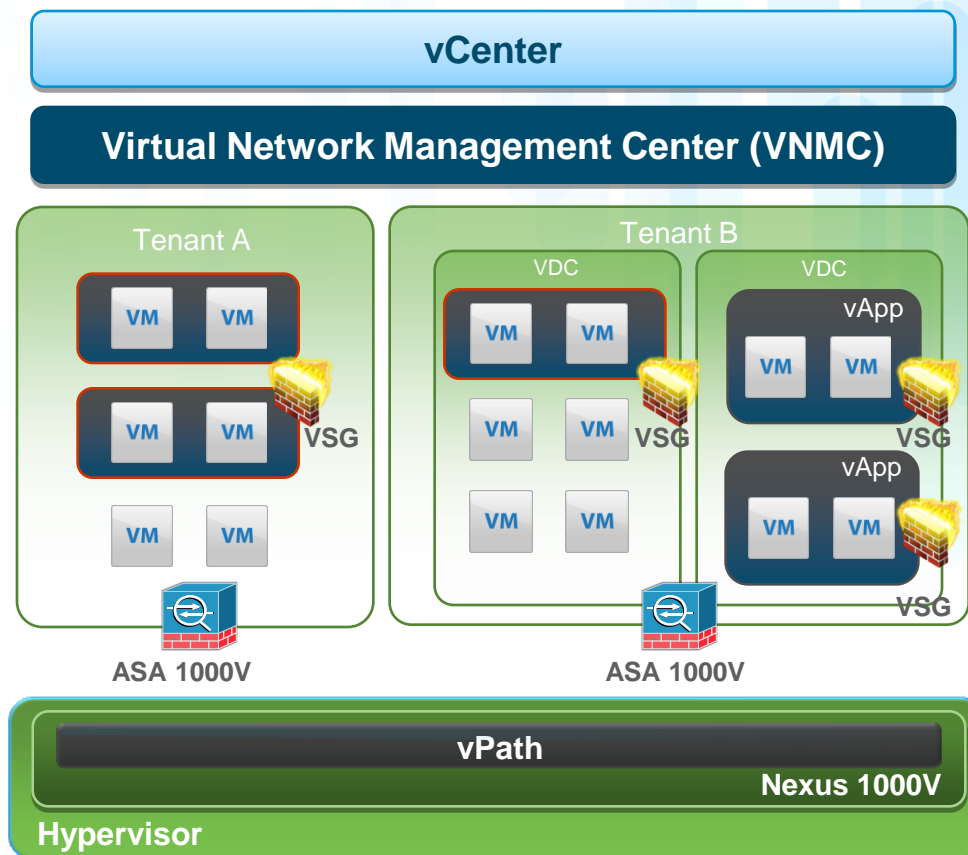
Zone based intra-tenant
segmentation of VMs

ASA 1000V

External / multi-tenant edge
deployment

Securing Tenant Edge with ASA 1000V

- Proven Cisco Security...Virtualized Physical – virtual consistency
- Collaborative Security Model
VSG for intra-tenant secure zones
ASA 1000V for tenant edge controls
- Seamless Integration
With Nexus 1000V & vPath
- Scales with Cloud Demand
Multi-instance deployment for horizontal scale-out deployment



ASA 1000V: Solution Features and Capabilities

Default Gateway

Site-to-Site VPN

NAT

DHCP

Attack Prevention

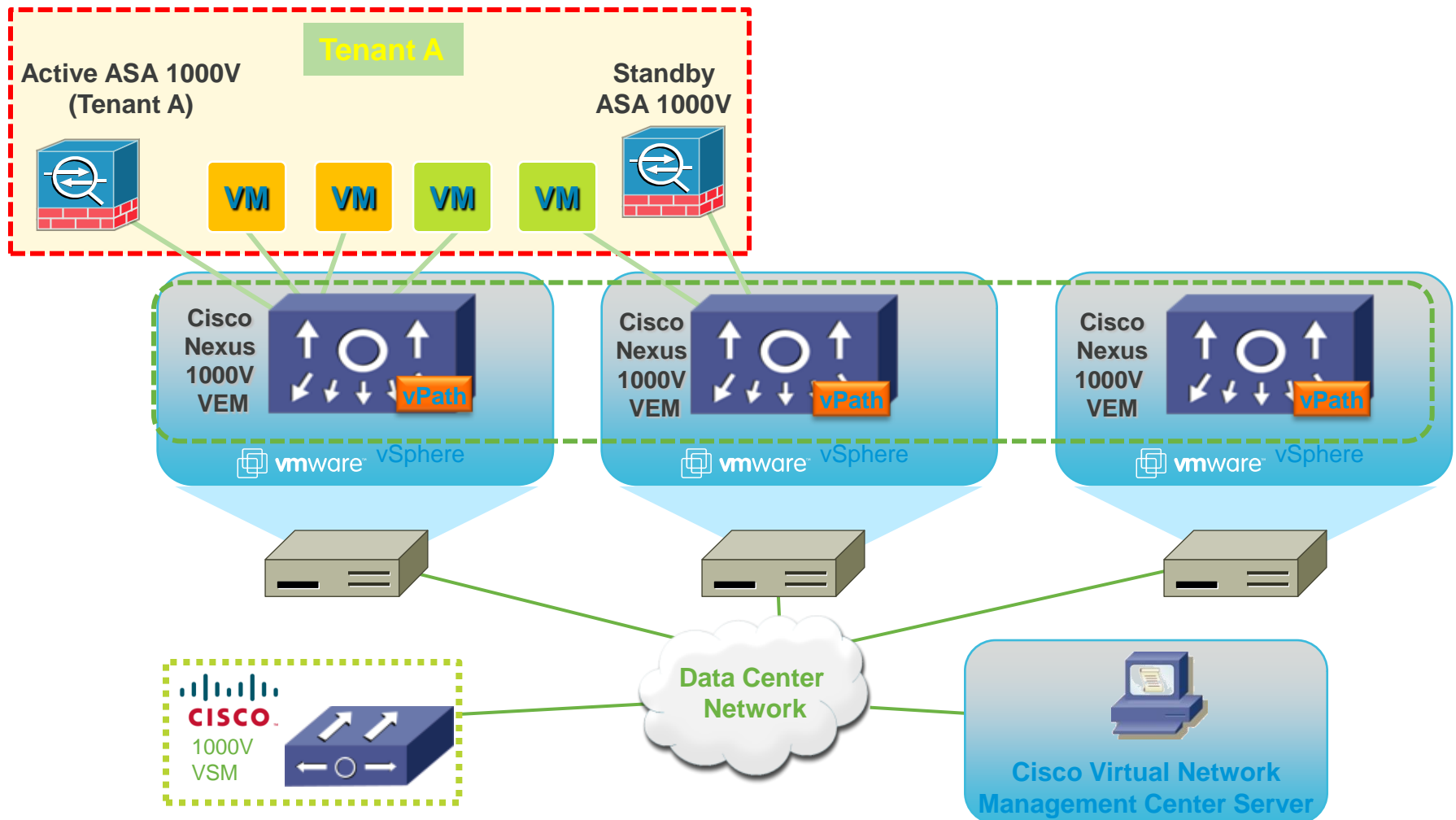
Proven Firewall

Enhanced Flexibility &
Operational Efficiency

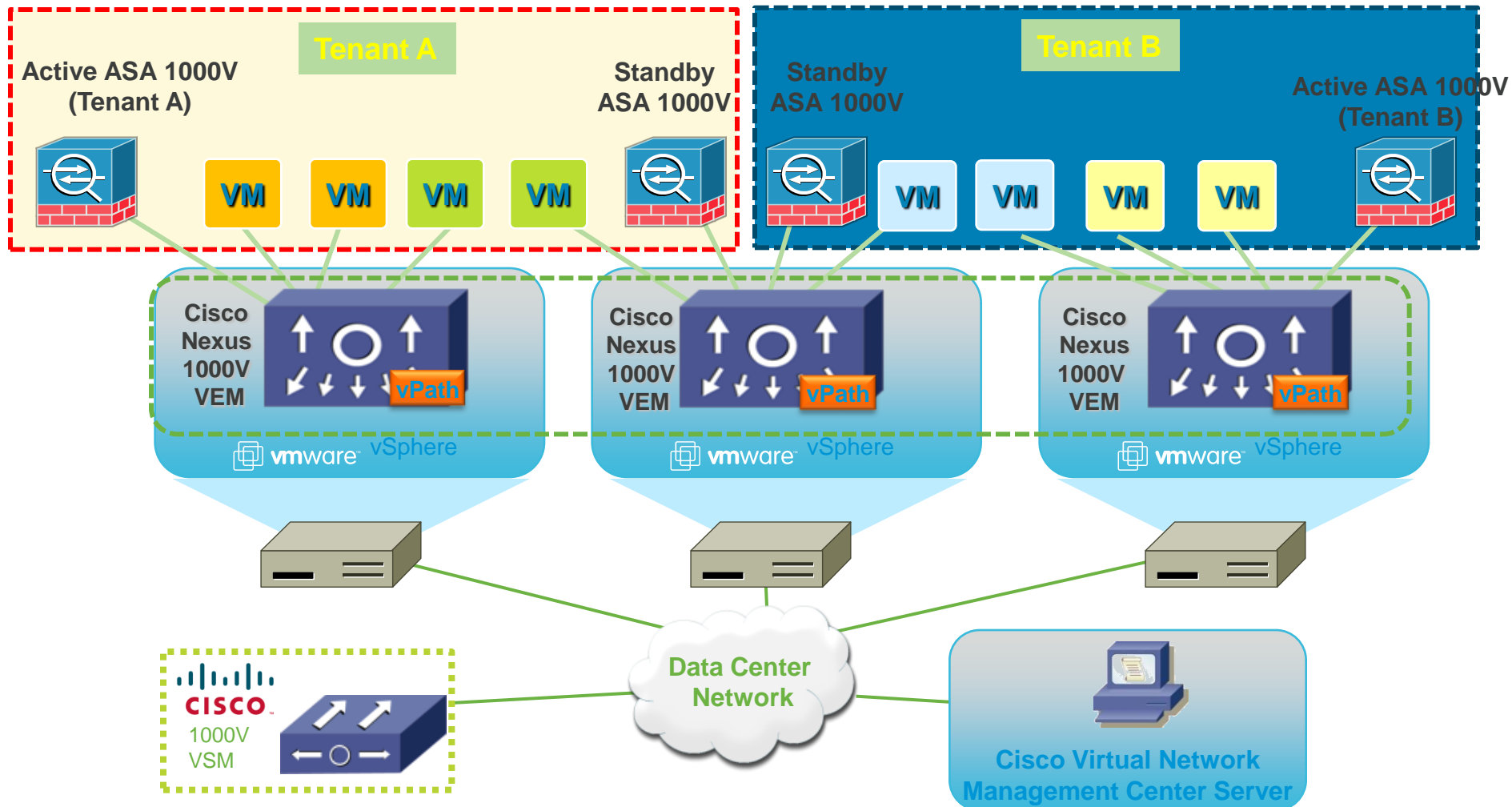
Address new virtualization
workflows

Not just an ASA in a VM... But, part of a solution containing vPath

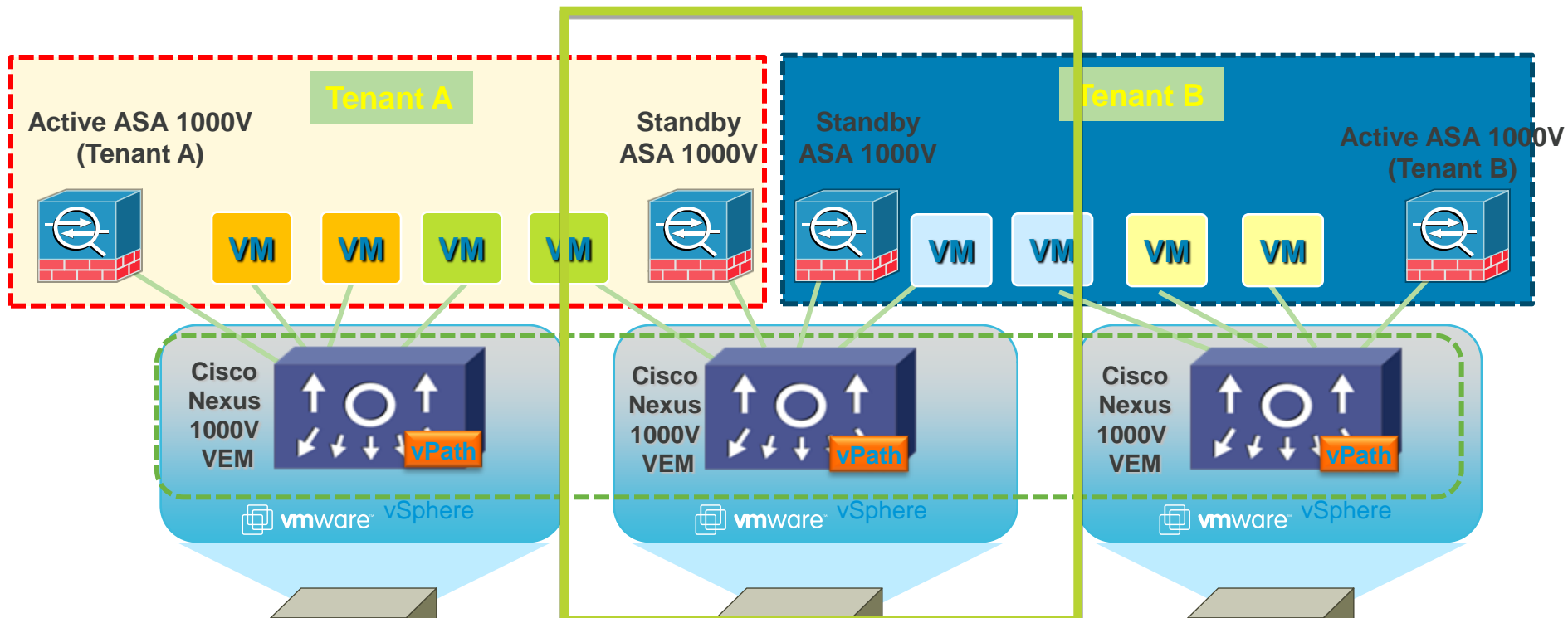
Deployment in Multitenant Environment



Deployment in Multitenant Environment

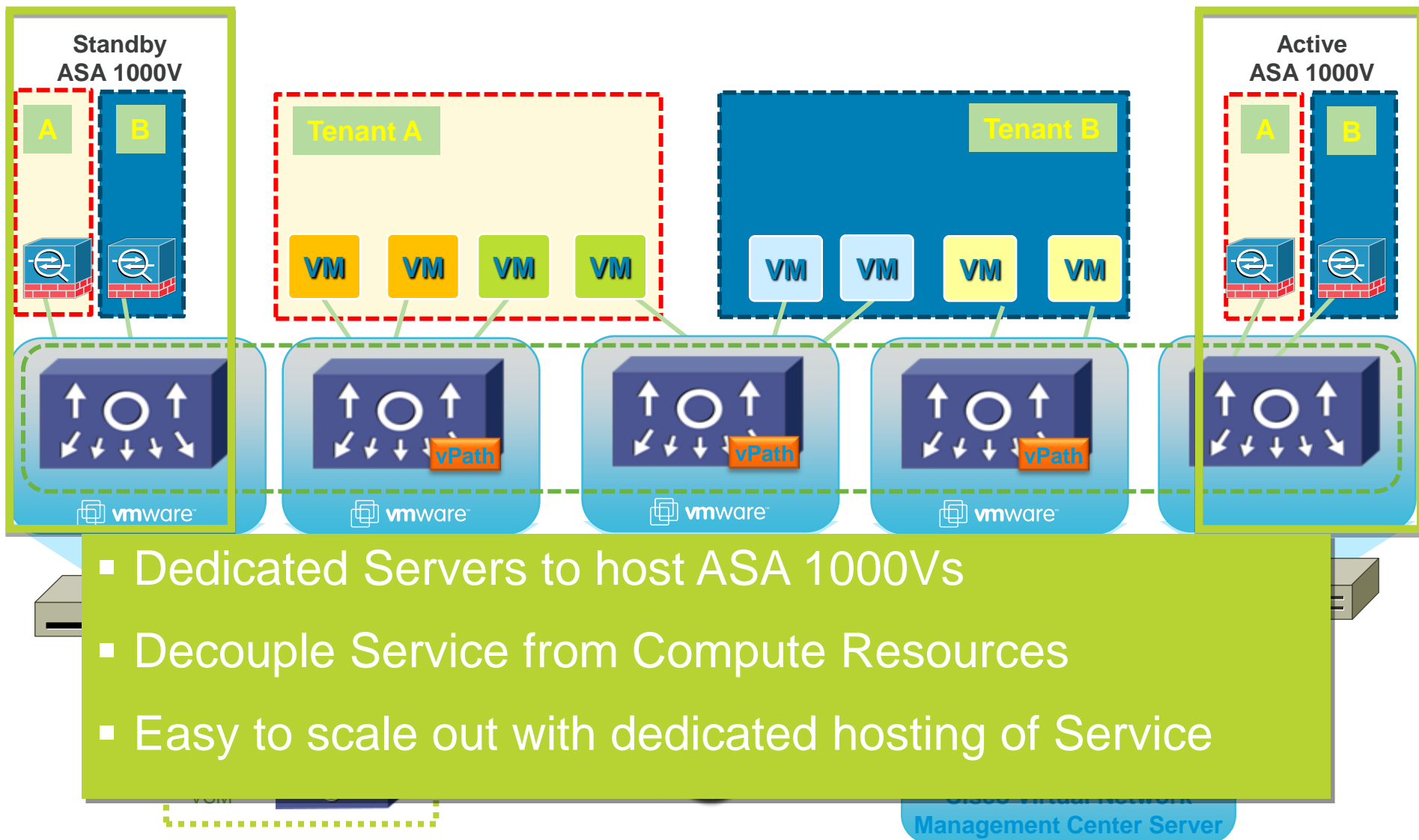


Deployment in Multitenant Environment

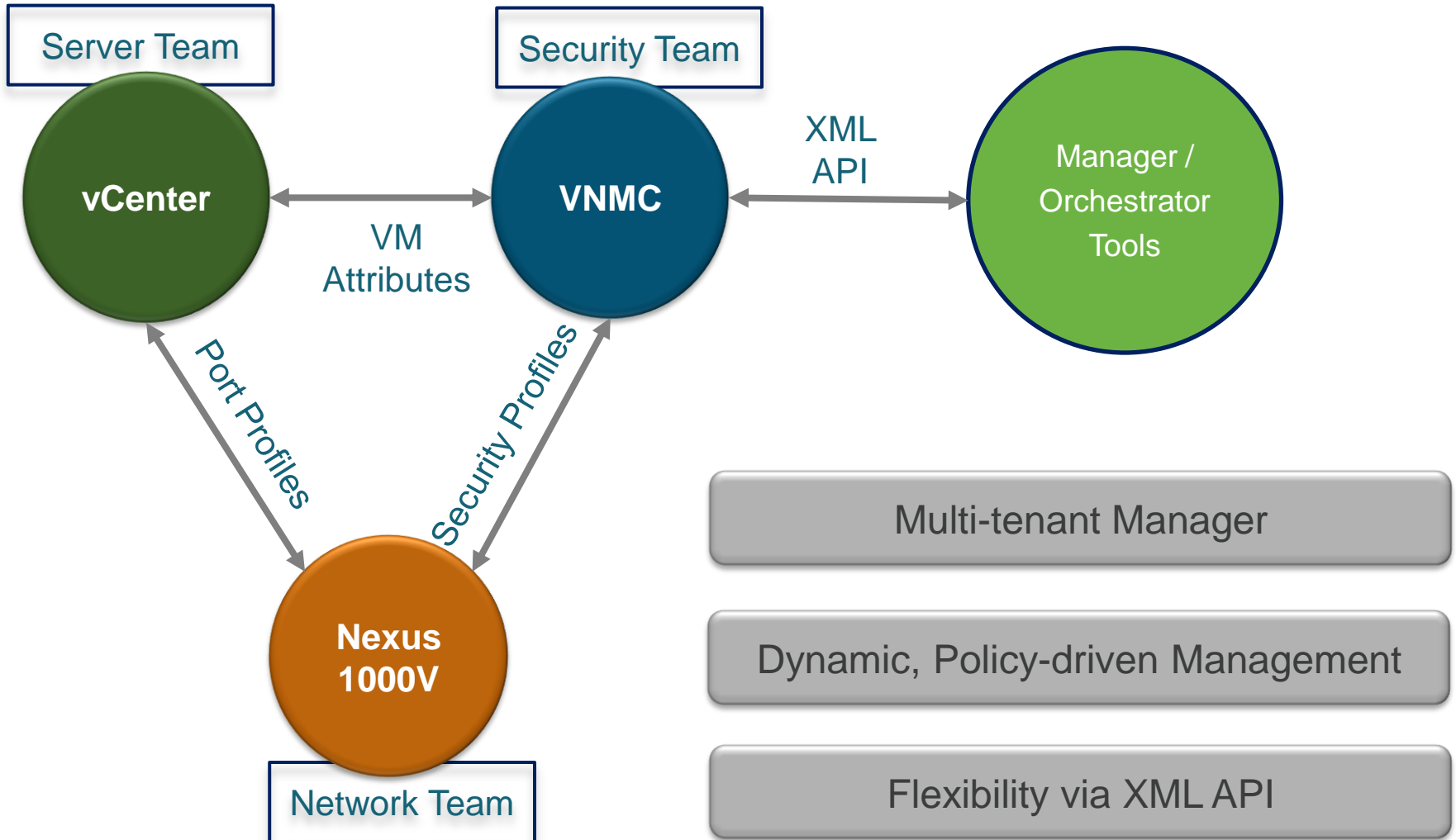


- Security policies enforced on shared compute environment
- Multitenant aware vPath
- Active and Standby ASA 1000Vs on different physical hosts

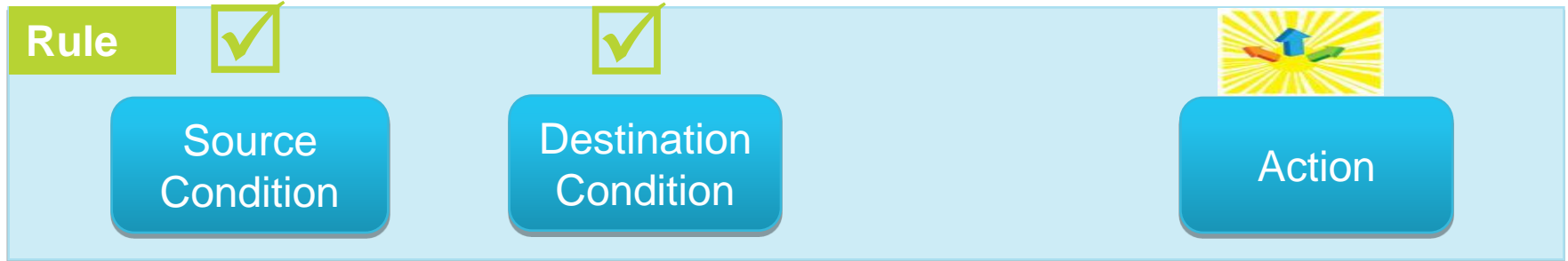
Deployment on Dedicated Host



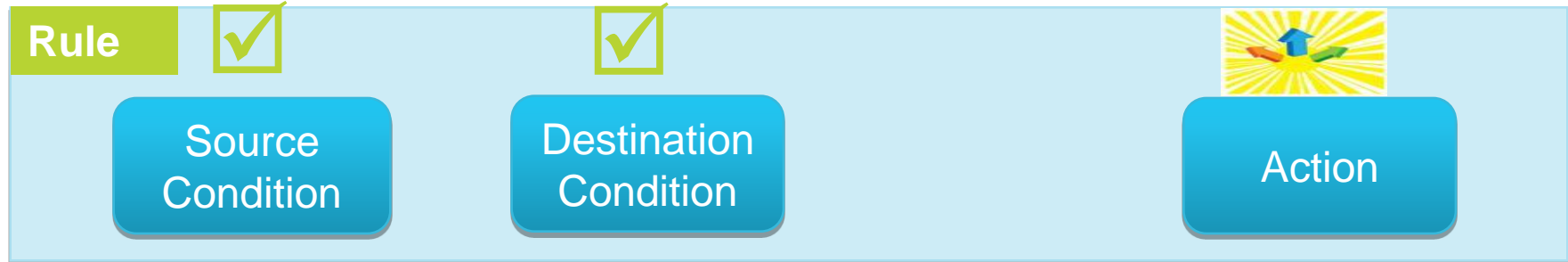
Non-disruptive Operations



VM Attribute Based Policy Creation (Future)



VM Attribute Based Policy Creation (Future)



Condition

Attribute Type :

Network ▼

Attribute Type

Network

VM

User Defined

vZone

Expression

Attribute Name :

IP Address

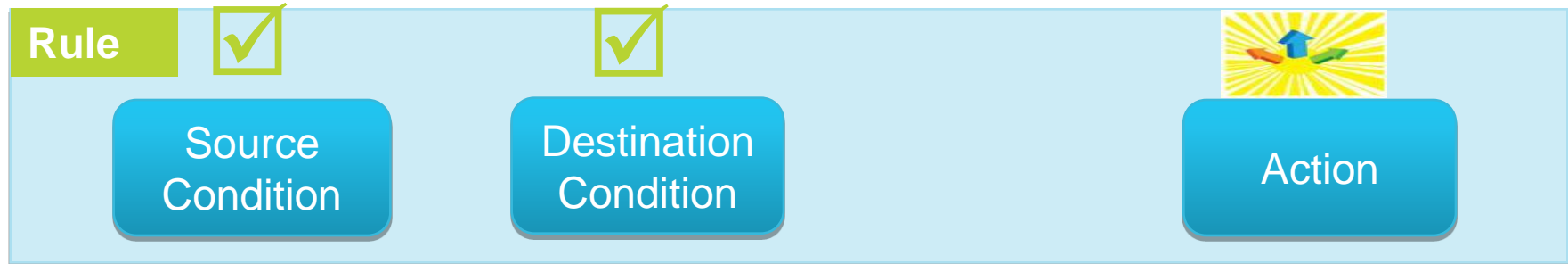
Operator :

eq ▼

Attribute Value :

192 . 168 . 1 . 2

VM Attribute Based Policy Creation (Future)



Condition

Attribute Type :

Network ▼

Expression

Attribute Name :

IP Address

Operator :

eq ▼

Attribute Value :

192 . 168 . 1 . 2

Attribute Type

Network

VM

User Defined

vZone

VM Attributes

VM Name

Guest OS full name

Resource Pool

Parent App Name

Port Profile Name

Cluster Name

VM DNS Name

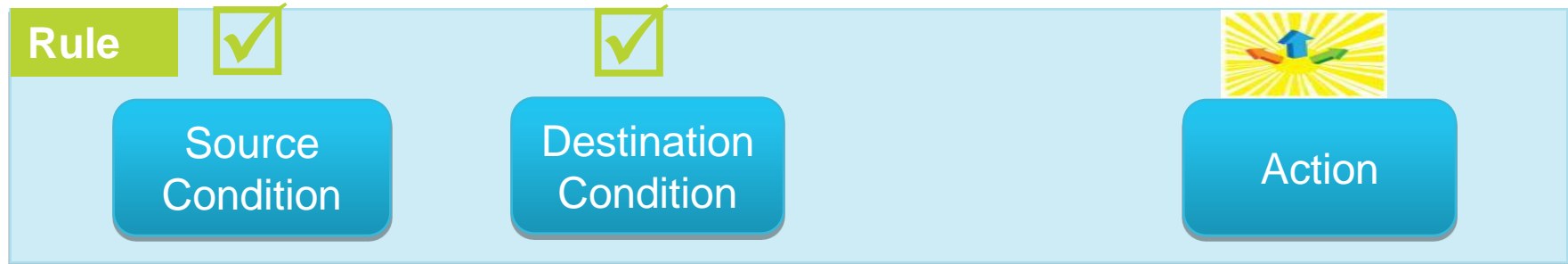
Hypervisor Name

Network Attributes

IP Address

Network Port

VM Attribute Based Policy Creation (Future)



Condition

Attribute Type : ▼

Expression

Attribute Name : Operator : Attribute Value :

Attribute Type

- Network
- VM
- User Defined
- vZone

VM Attributes

- VM Name
- Guest OS full name
- Resource Pool
- Parent App Name
- Port Profile Name
- Cluster Name
- VM DNS Name
- Hypervisor Name

Network Attributes

- IP Address
- Network Port

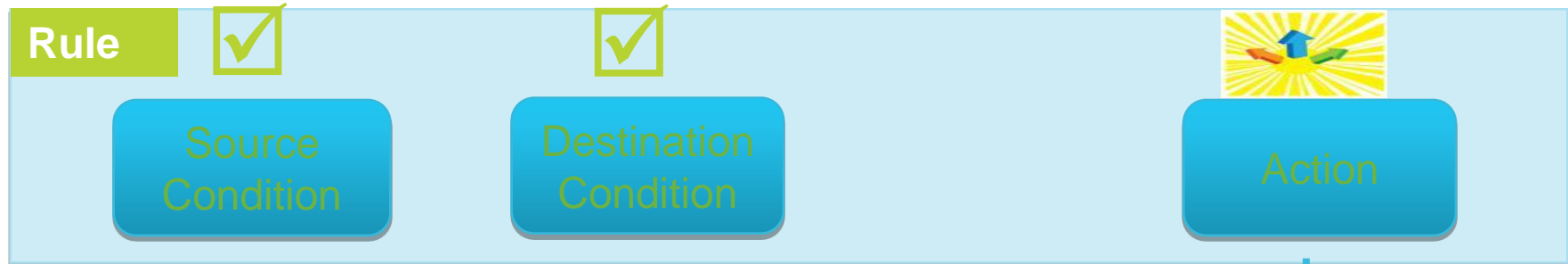
Operator

- eq
- neq
- gt
- lt
- range
- Not-in-range
- Prefix

Operator

- member
- Not-member
- Contains

VM Attribute Based Policy Creation (Future)



Condition

Attribute Type :

Network ▼

Expression

Attribute Name :

IP Address ▼

Operator :

eq ▼

Attribute Value : 192 . 168 . 1 . 2

☒ drop ☐ permit ☐ reset

☐ log

VM Attributes

Instance Name

Guest OS full name

Zone Name

Parent App Name

Port Profile Name

Cluster Name

Hypervisor Name

Network Attributes

IP Address

Network Port

Operator

eq

neq

gt

lt

range

Not-in-range

Prefix

Operator

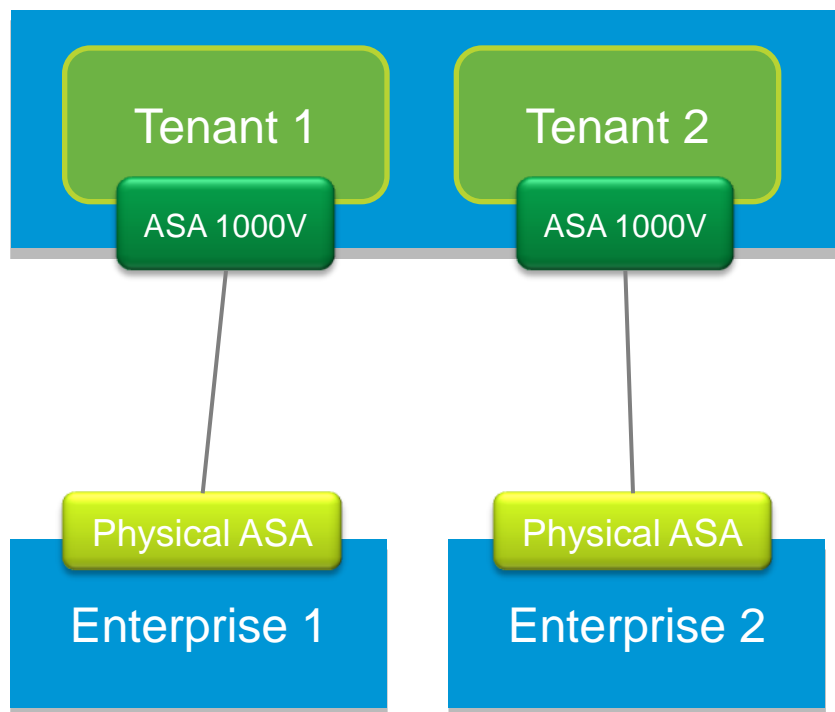
member

Not-member

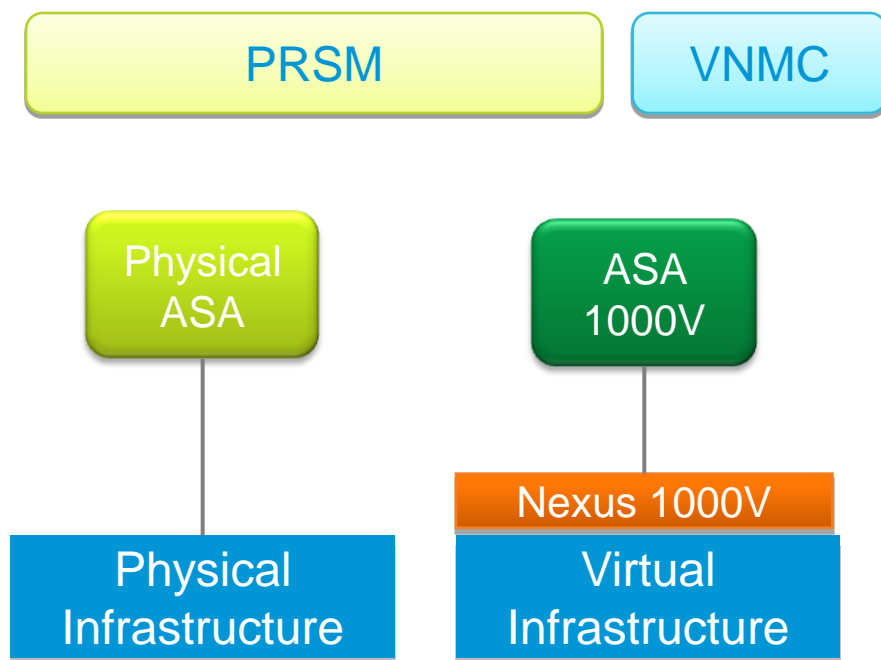
Contains

Target Customer Segments

Cloud Service Providers



Enterprises with hybrid infrastructure



Thank you.

