Cisco ASA with FirePOWER Services

For SMB, Distributed Enterprises, and Industrial Control Systems

Featured products: 5506-X | 5506W-X | 5506H-X | 5508-X | 5516-X

Key Enhancements Over ASA 5505

Category		5505	5506-X
NGFW	Application Visibility & Control	No	Yes
FirePOWER Services	AMP, NGIPS, URL Filtering Subscriptiions	No	Yes
Hardware Security	ACT 2 Hardware Anti-Tamper	**No**	**Yes**
Simplified Purchase Experience	Unlimited User (node) Support	**No**	**Yes**
VPN	Enhanced mobility support	**No**	**Yes**
Additional Features	Throughput	→	Over 2X Firewall Throughput
	Integrated Wireless Access Point	No	Yes (5506W-X variant)

5506-X

MORE SECURE

MORE SCALEABLE

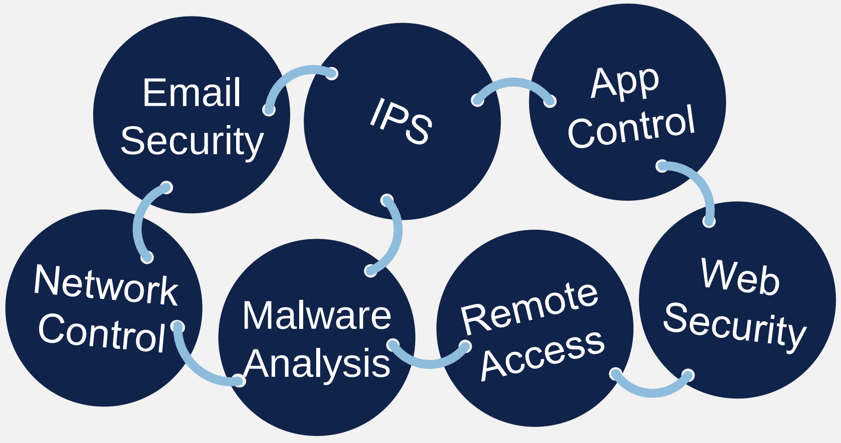
MORE FLEXIBLE

Limited options made it difficult to get the protection you need

Unified Threat Management (UTM)

Stateful Firewall

OR



Multiple Point Solutions

Less Effective

- UTMs are often less effective than components-based systems
- Legacy firewalls and UTM solutions were never designed for protecting against advanced threats

Difficult to Integrate

- Point solutions are difficult to integrate and configure
- Incorrect or incomplete solutions can increase risk

Costly and Time Consuming

- Legacy NGFWs and point solutions are costly and may be impractical-to-administer
- Multiple vendors results in multiple support calls, increasing overall costs

Until now

Cisco ASA with FirePOWER services

Hardware

Security Services

Next-Generation IPS (NGIPS)

Advanced Malware Protection (AMP)

Application Visibility and Control (AVC)

URL Filtering

And Other Next-Generation Firewall Capabilities

Management

Adaptive Security Device Manager (ASDM)

FireSIGHT Management Center

Hardware

Start with the right appliance

	ASA 5506-X	ASA 5506W-X	ASA 5506H-X	ASA 5508-X / ASA 5516-X
	Desktop Model 100% NGFW; best for ASA 5505-X refreshes	**Integrated Wireless AP:** Wireless can be managed locally or through WLC	**Ruggedized** For industrial control and critical infrastructure	**Higher Performance** Value-focused price; 5516 is best for 5512 & 5515 refreshes
Form Factor	**Desktop**	**Desktop**	**Rack Mount or Wall Mount**	**1RU**
CPU	Multicore @ 1.25GHz	Multicore @ 1.25GHz	Multicore @ 1.25GHz	5508: Multicore @ 2GHz 5516: Multicore @ 2.4GHz
Memory – RAM	4GB	4GB	4GB	8GB
Storage	50GB mSata	50GB mSata	50GB mSata tested for heat	5508: 80GB mSata 5516: 100 GB mSata
Flash	8GB	8GB	8GB	8GB
Integrated I/O	8x1G (all L3 interfaces)	8 External, 1 AP	4x1G	8x1G (all L3 interfaces)
Security Context	No	No	No	Yes
FirePOWER Services	Yes	Yes	Yes	Yes

Operating Temperature: -20C to 60C

IP Rating: 40

Cisco Trust Anchor validates the source of the image file and protects against hardware tampering and counterfeiting

To get the performance you need

Features	 ASA 5506-X 5506W-X | 5506H-X	 ASA 5508-X	 ASA 5516-X
Max stateful inspection throughput	750 Mbps	1 Gbps	1.8 Gbps
VPN throughput	100 Mbps	175 Mbps	250 Mbps
Max AVC throughput	250 Mbps	450 Mbps	850 Mbps
Max AVC and NGIPS throughput	125 Mbps	250 Mbps	450 Mbps
AVC or IPS sizing throughput [440B]	90 Mbps	180 Mbps	300 Mbps
Max concurrent sessions	50,000	100,000	250,000
Max connections per second (CPS)	5,000	10,000	20,000

~1.5x to 2x

~1.5x to 2x

Security Services

Add security services to help defend your network

FirePOWER Services

Subscription services that run on the ASA and provide enhanced levels of threat protection and network visibility

- URL Filtering
- Next-Generation Intrusion Prevention System
- Advanced Malware Protection
- ◤ Application Visibility and Control

✚

Foundational Functionality

Built-in firewall services to provide base protection and connect with other security solutions

- Stateful Firewalling
- VPN Capabilities
- Policy Enforcement Point for ISE

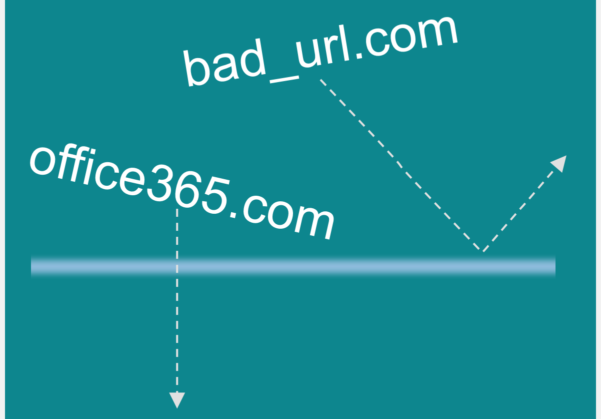
◤ Included by default

Minimize your exposure to web-based threats

Services

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Block specific URLs



Restrict access to specific sites and subsites

Restrict categories of URLs

- ✗ Gambling
- ✓ Social Media
- ✓ Health
- ✗ Gaming
- ✗ Drug Use

Filter out over 280 million URLs based on any of the 80+ categories into which they are grouped; new URLs are added daily

Change policies easily

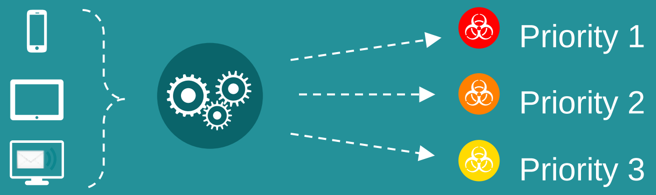
Use the refined user interface to make additions or changes with just a few clicks

Gain unmatched visibility and threat detection

Services

- URL Filtering
- **NGIPS**
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Protect the network more effectively

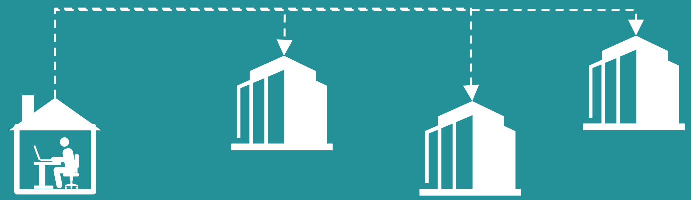


NGIPS automatically correlates information from intrusion events with network assets to prioritize threat investigation

Blended threats and attacks coming through multiple vectors are quickly identified

Reduce IT management burden

Policies can be updated automatically based on vulnerabilities and previous intrusion events



Admins can make adjustments to policies and system settings across locations from a single location, even offsite

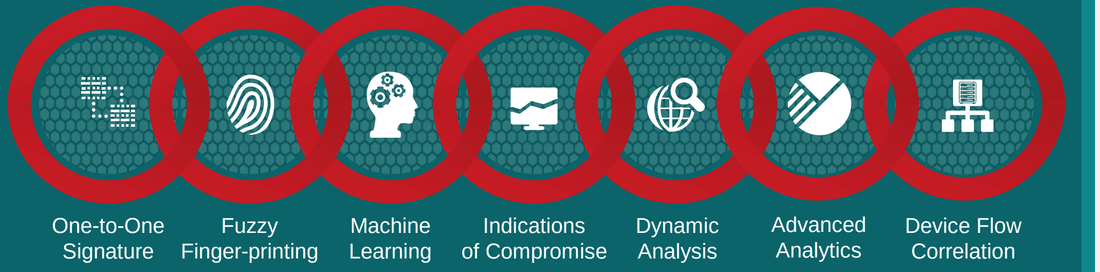
Protect against the most advanced forms of malware and remediate after a breach

Services

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Point-in-time Protection

Identify malware that other solutions miss by analyzing files based on reputation or suspicious behavior. AMP is continuously updated to ensure that it can stop the latest and most advanced forms of malware.



One-to-One Signature

Fuzzy Finger-printing

Machine Learning

Indications of Compromise

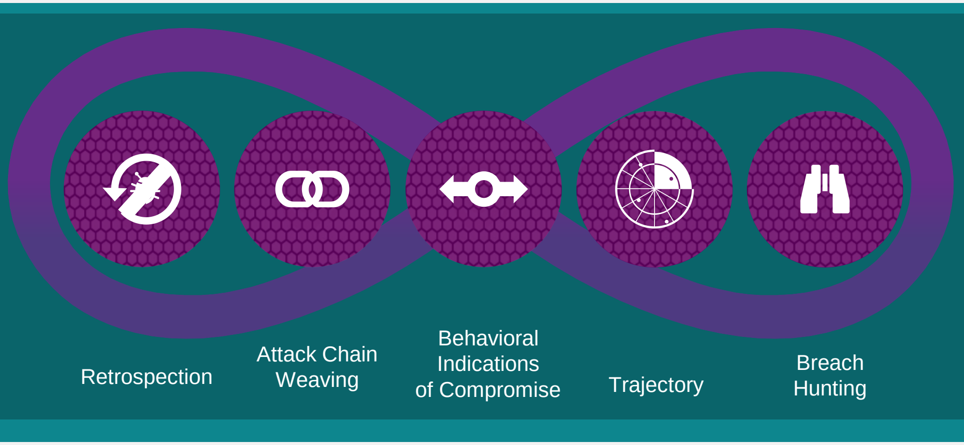
Dynamic Analysis

Advanced Analytics

Device Flow Correlation

Continuous Protection

Defend against attacks even after a file passes the perimeter. AMP tracks files as they move around network; if they turn out to be malicious, you can quickly determine areas of impact and remediate quickly.



Retrospection

Attack Chain Weaving

Behavioral Indications of Compromise

Trajectory

Breach Hunting

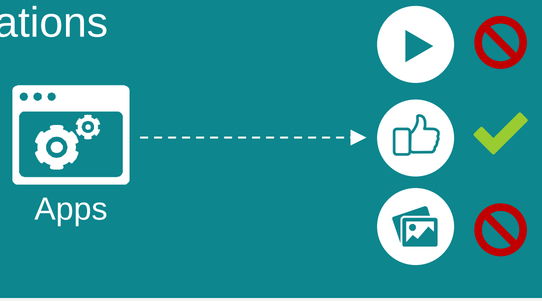
Reduce attack surfaces by controlling application access

Services

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Control port- and protocol-hopping apps that evade traditional firewalls

Enforce acceptable use policies with granular control over applications and micro-applications



Limit the exposure created by social media applications

facebook Google+

twitter LinkedIn

Use custom application detectors / Open App ID

Leverage the proven ASA Firewall capabilities

Services

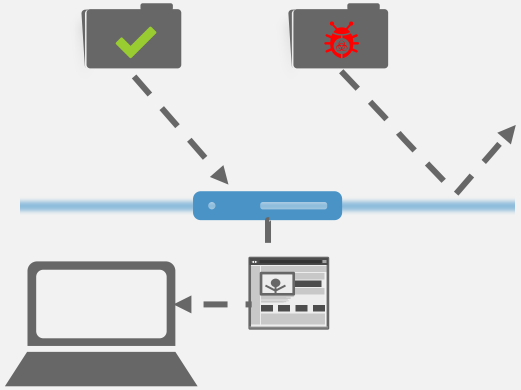
- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Standard Functions

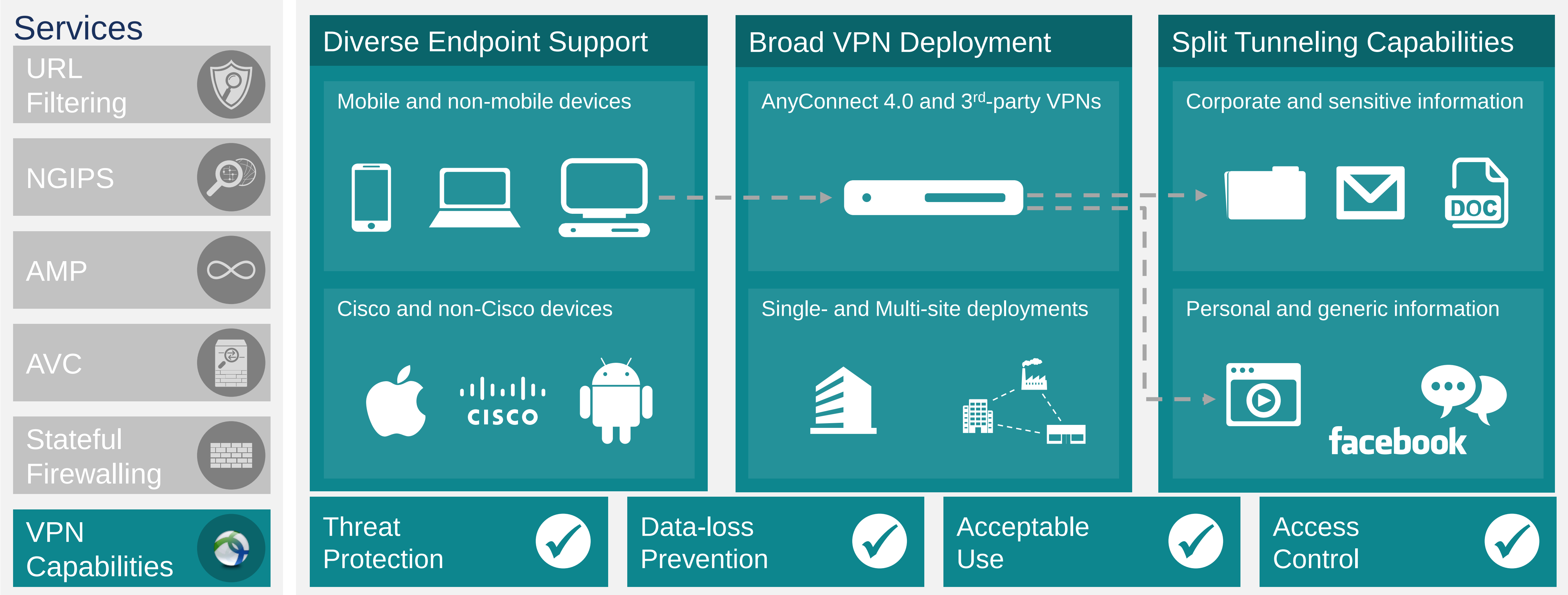
- TCP Normalization
- TCP Intercept
- IP Option Inspection
- IP Fragmentation
- NAT
- Routing
- ACL

New ASA Features

- Clientless tagging, WebVPN support for OWA2013 and XenDesktop7.5
- TLS 1.2
- ECMP Support, IPV6 BGP
- Std. based IKEv2 support. Citrix HTML5 browser support
- VPN Clients Win7, 8.1, 8.1 phone client, iOS8, Knox and Strong Swan
- Full VX LAN support
- Policy-based Routing



Extend protection to off-site users



Services

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Diverse Endpoint Support

Mobile and non-mobile devices

Cisco and non-Cisco devices

Broad VPN Deployment

AnyConnect 4.0 and 3rd-party VPNs

Single- and Multi-site deployments

Split Tunneling Capabilities

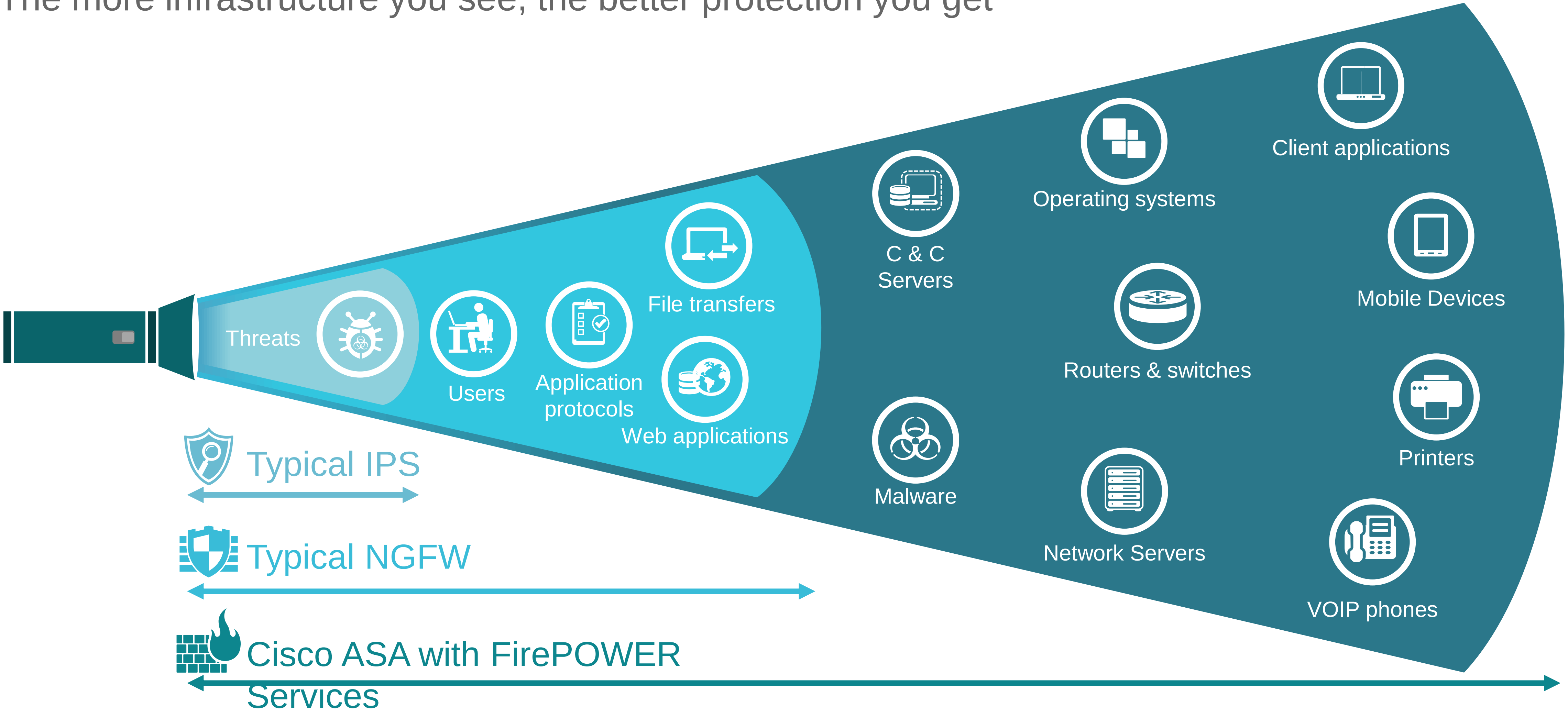
Corporate and sensitive information

Personal and generic information

- Threat Protection ✓
- Data-loss Prevention ✓
- Acceptable Use ✓
- Access Control ✓

No other firewall offers extensive contextual visibility

The more infrastructure you see, the better protection you get



Or is supported by the largest security intelligence and research group

Identify advanced threats quickly with industry-leading threat research

Get industry-specific threat intelligence tailored to your business

Catch advanced threats endpoints miss with Cisco's reverse engineers and threat analysts

Stay protected against the latest threats with regular updates pushed automatically

Talos

- Monitors 35% of the world's email traffic
- Receives 1.1 million incoming malware samples daily

- Performs 4.9 billion AV and web filtering blocks per month
- Processes 100 terabytes of security intelligence daily

Threat Intelligence

Email · Endpoints · Web · Networks · NGIPS · Devices

Research Response

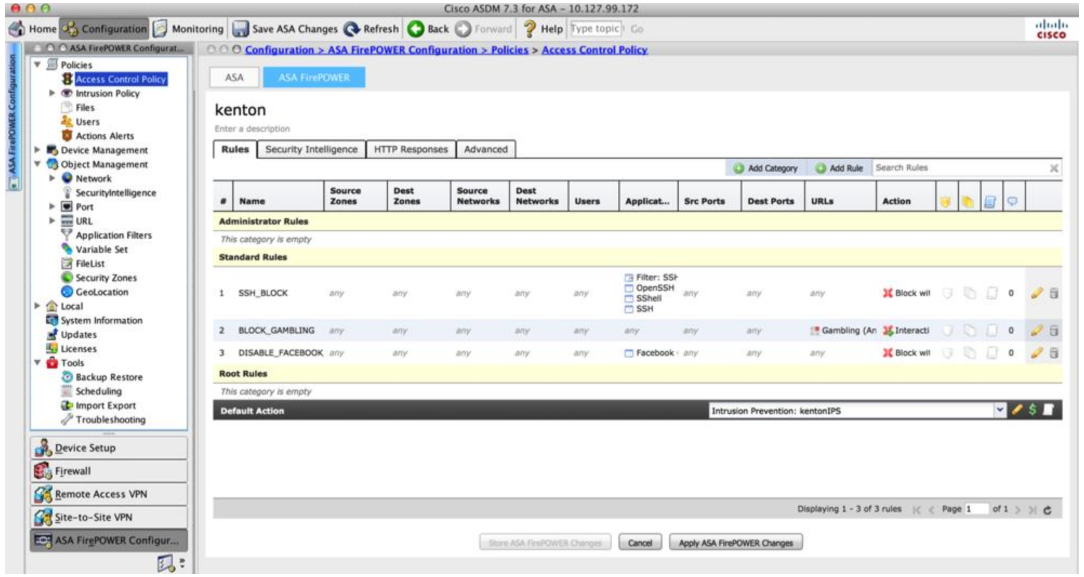
600+ Researchers

24 • 7 • 365 Operations

Management

Cisco offers multiple management solutions

Adaptive Security Device Manager (ASDM) on-box manager



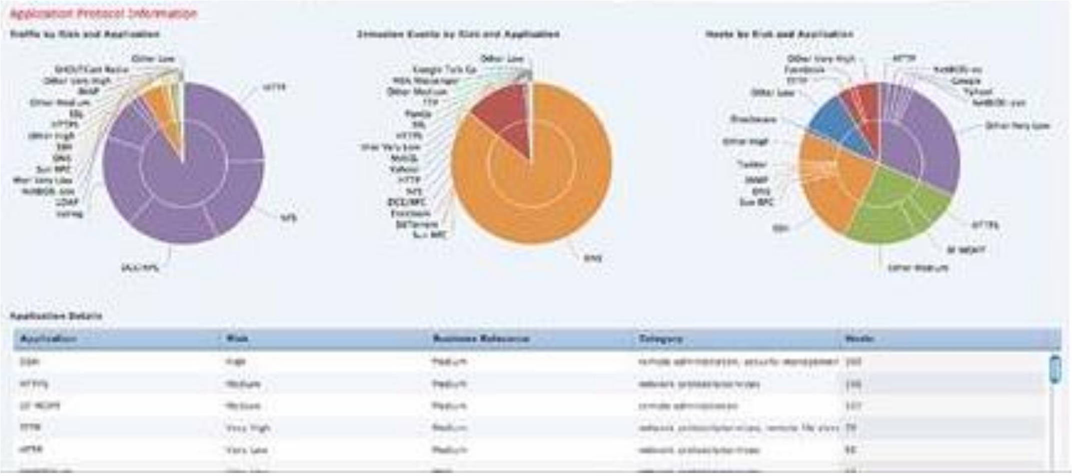
kenton

Enter a description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat...	Src Ports	Dest Ports	URLs	Action					
Administrator Rules																
This category is empty																
Standard Rules																
1	SSH_BLOCK	any	any	any	any	any	Filter: SSH OpenSSH SShell SSH	any	any	any	Block wit				0	
2	BLOCK_GAMBLING	any	any	any	any	any	any	any	any	Gambling (An	Interacti				0	
3	DISABLE_FACEBOOK	any	any	any	any	any	Facebook	any	any	any	Block wit				0	
Root Rules																
This category is empty																
Default Action										Intrusion Prevention: kentonIPS						

Displaying 1 - 3 of 3 rules Page 1 of 1

FireSIGHT Management Center

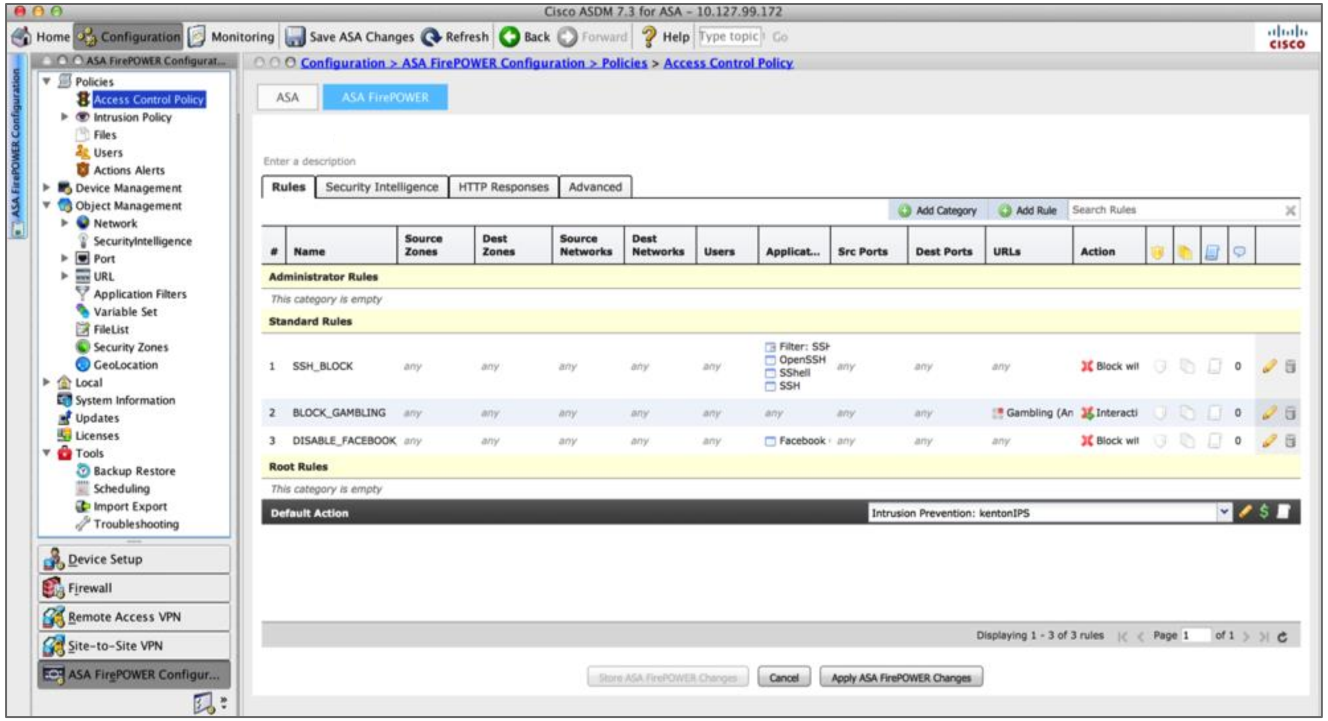

Application Protocol Information
Traffic by Risk and Application
Intrusion Events by Risk and Application
Hosts by Risk and Application
Application Details
Application
Risk
Business Relevance
Category
Hosts

Including integrated, on-box management through Adaptive Security Device Manager

ASDM 7.3.X+ combines control of Access Policy and Advanced Threat Defence Functions

The enhanced UI provides quick views on trends and the ability to drill-down for details

ASDM consolidates management of all stateful and Next-Generation Firewall functions for ease of use

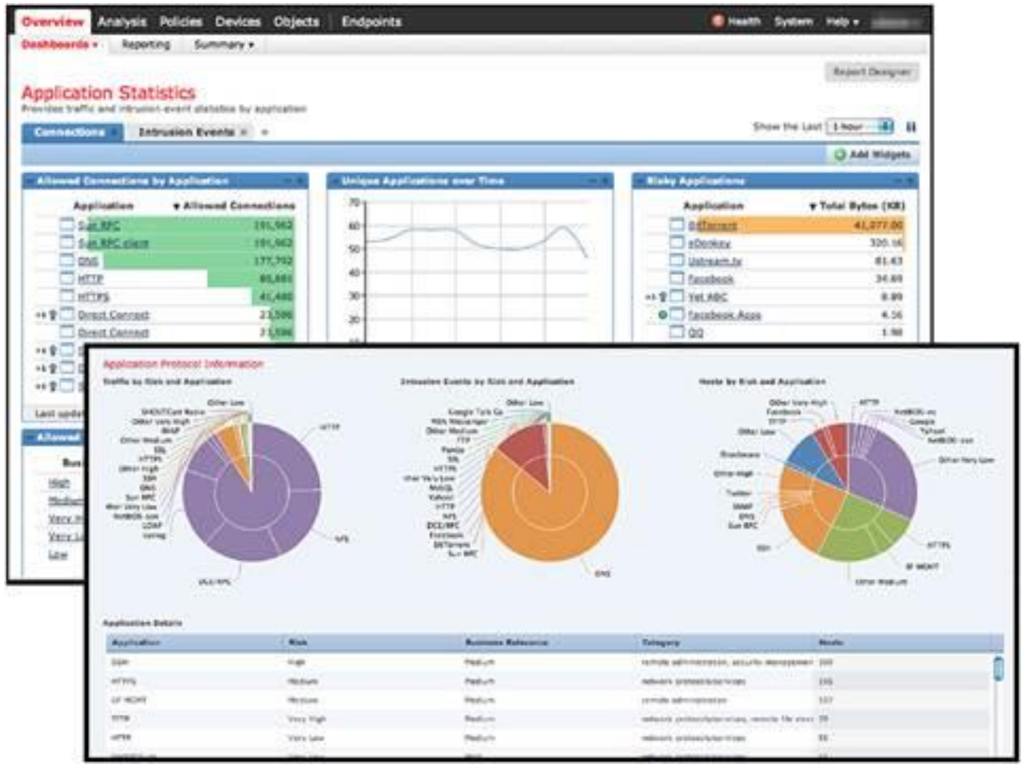


#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat...	Src Ports	Dest Ports	URLs	Action					
Administrator Rules																
This category is empty																
Standard Rules																
1	SSH_BLOCK	any	any	any	any	any	Filter: SSH OpenSSH SShell SSH	any	any	any	Block wit				0	
2	BLOCK_GAMBLING	any	any	any	any	any	any	any	any	Gambling (An	Interacti				0	
3	DISABLE_FACEBOOK	any	any	any	any	any	Facebook	any	any	any	Block wit				0	
Root Rules																
This category is empty																
Default Action											Intrusion Prevention: kentonIPS					

And centralized management for greater control

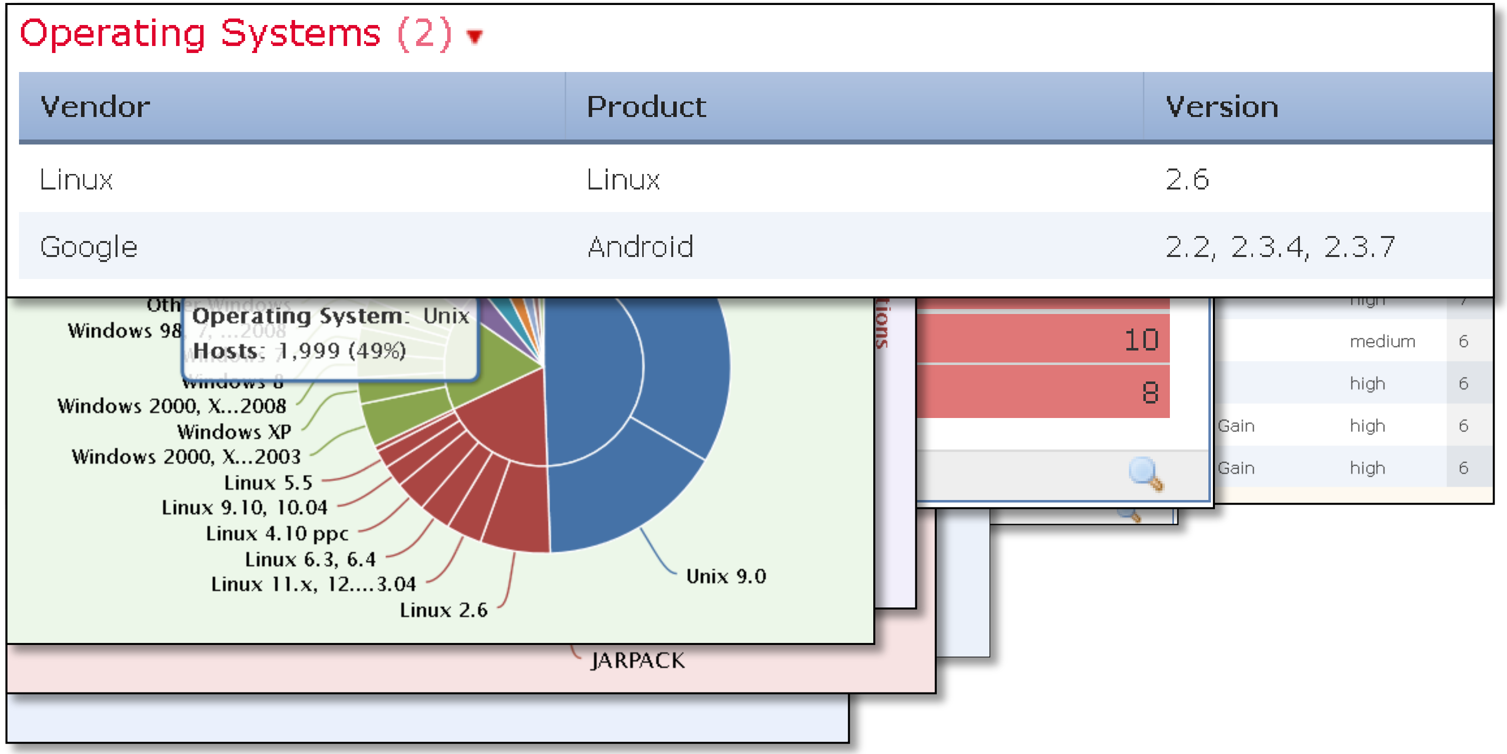
FireSIGHT Management Center and Cisco Security Management (CSM)

- CSM is for ASA, and FireSIGHT Management Center is for FirePOWER Services
- They offer management capabilities across multiple devices
- Centralized management delivers comprehensive visibility and control over the network
- They provide optimal remediation through infection scoping and root cause determination
- FireSIGHT Management Center is offered as a physical appliance or a virtual appliance



With unmatched visibility for accurate threat detection and adaptive defense

	FirePOWER Services
Threats	✓
Users	✓
Web Applications	✓
Application Protocols	✓
File Transfers	✓
Malware	✓
Command & Control	✓
Client Applications	✓
Network Servers	✓
Operating Systems	✓
Mobile Devices	✓



Operating Systems (2)

Vendor	Product	Version
Linux	Linux	2.6
Google	Android	2.2, 2.3.4, 2.3.7

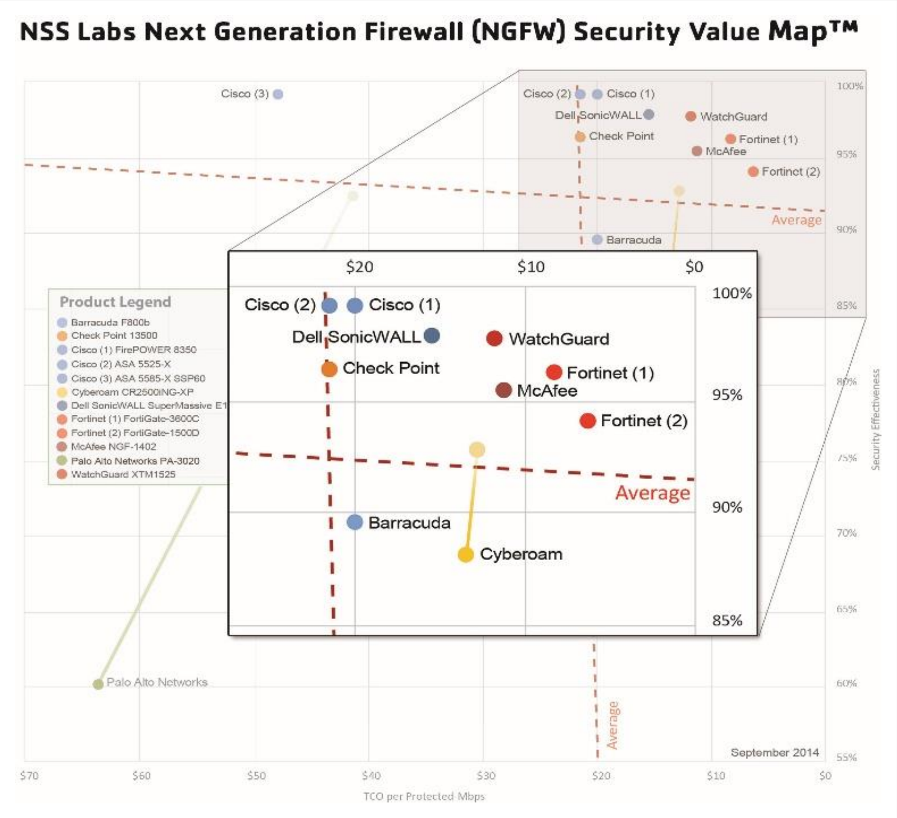
Operating System: Unix
Hosts: 1,999 (49%)

Cisco provides the best protection at a competitive price

NSS Labs:

Next-Generation Firewall Security Value Map

The NGFW Security Value Map shows the placement of Cisco® ASA with FirePOWER Services and the FirePOWER™ 8350 as compared to other vendors. All products achieved 99.2 percent in security effectiveness. Now customers can be confident they’ll get the best protections possible, regardless of deployment.



Source: NSS Labs 2014

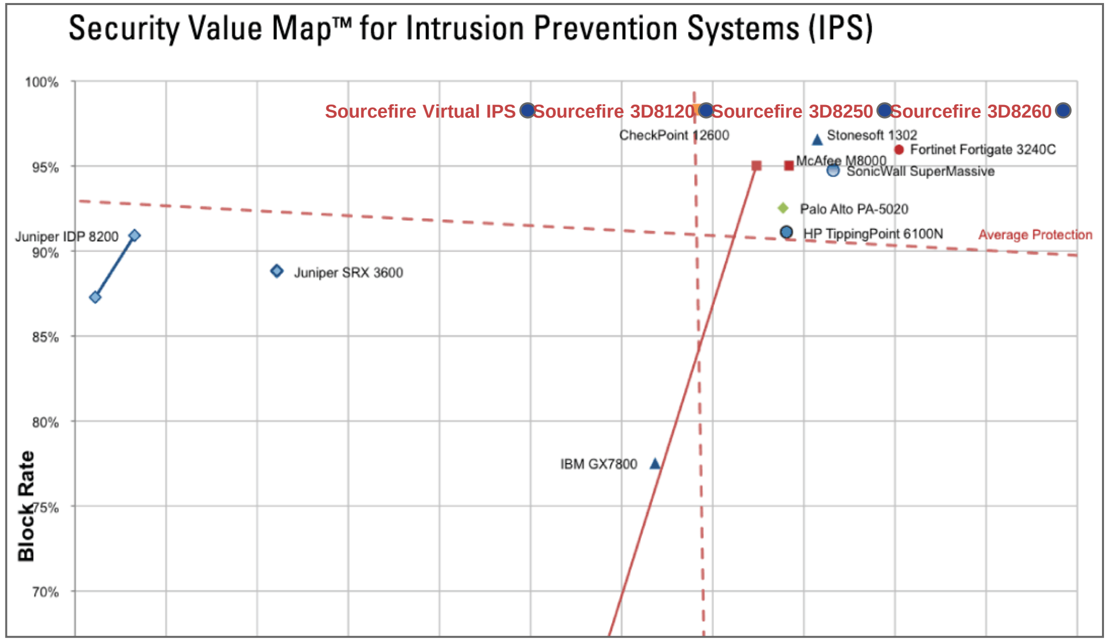
NSS Labs:

Intrusion Prevention Systems Security Value Map

Based on individual and comparative testing of vendors in the IPS market Cisco FirePOWER™ NGIPS* leads the Security Value Map and provides the best protection possible while also leading

the class in total cost of ownership.

* Formerly Sourcefire FirePOWER



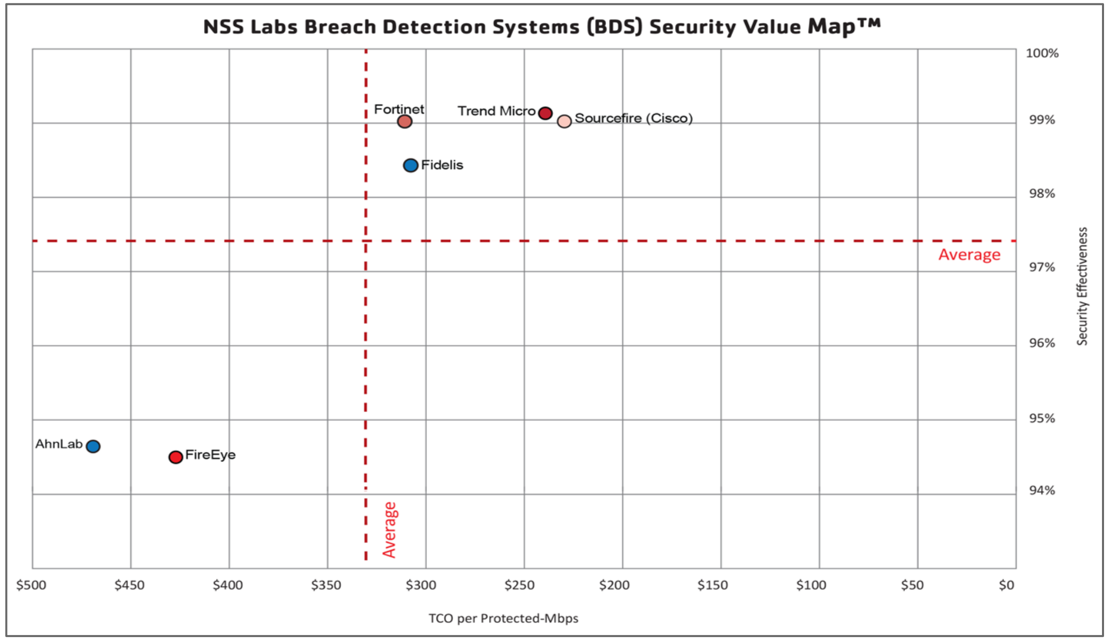
Source: NSS Labs 2014

NSS Labs:

Breach Detection Systems Security Value Map

Cisco® Advanced Malware Protection (AMP) has the lowest TCO of any product tested. It is also a a leader in security effectiveness, achieving detection of 99 percent of all tested attacks.

AMP excelled in time to detection, catching threats faster than competing breach detection systems.



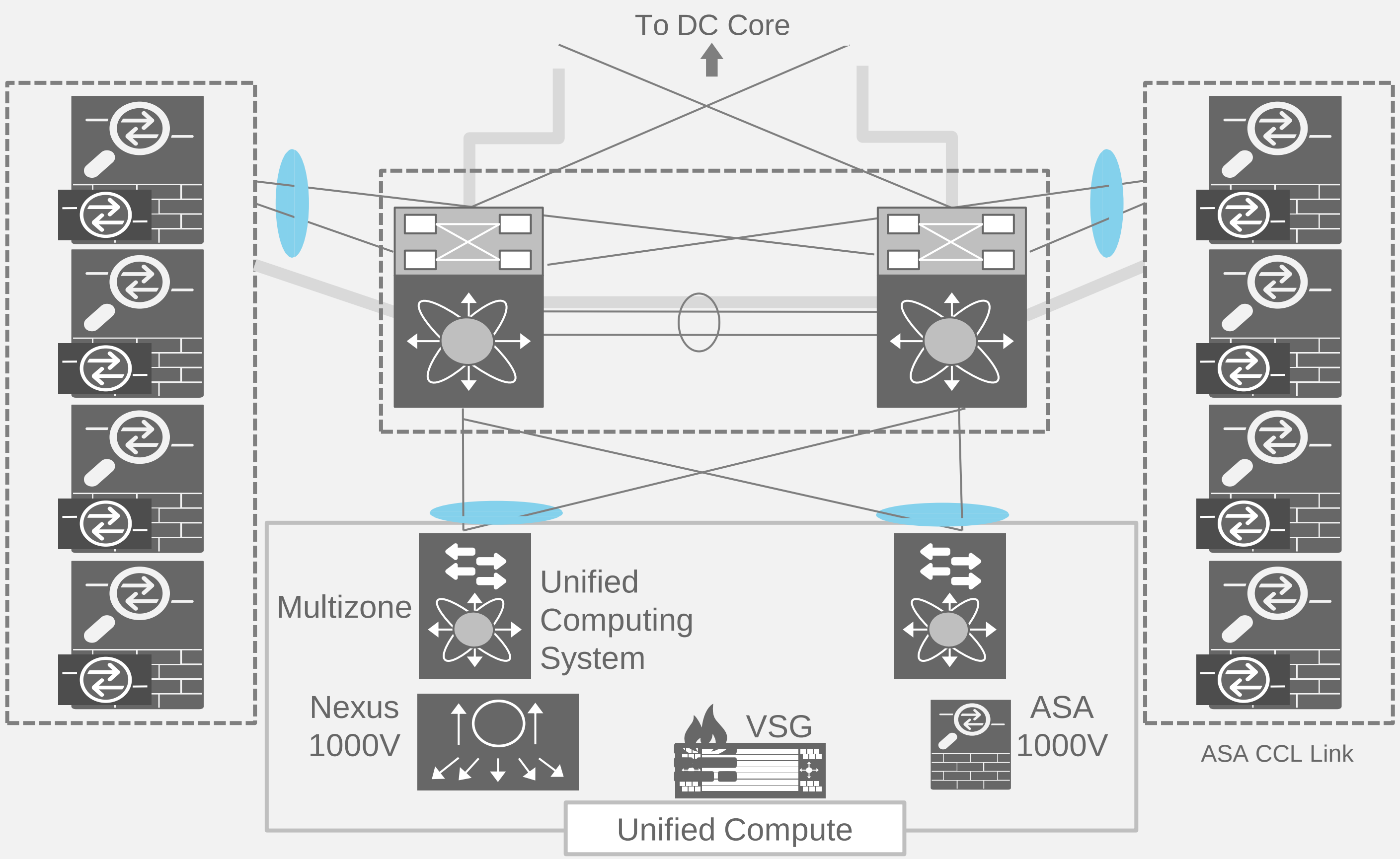
Source: NSS Labs 2014

Cisco offers multiple deployment options

Options include clustering for linear scalability

Deployment Options

- **Linear Scalability Clustering**
- **Multi-context Mode**
- **High Availability**



Supported on 5516-X for 2 node clustering

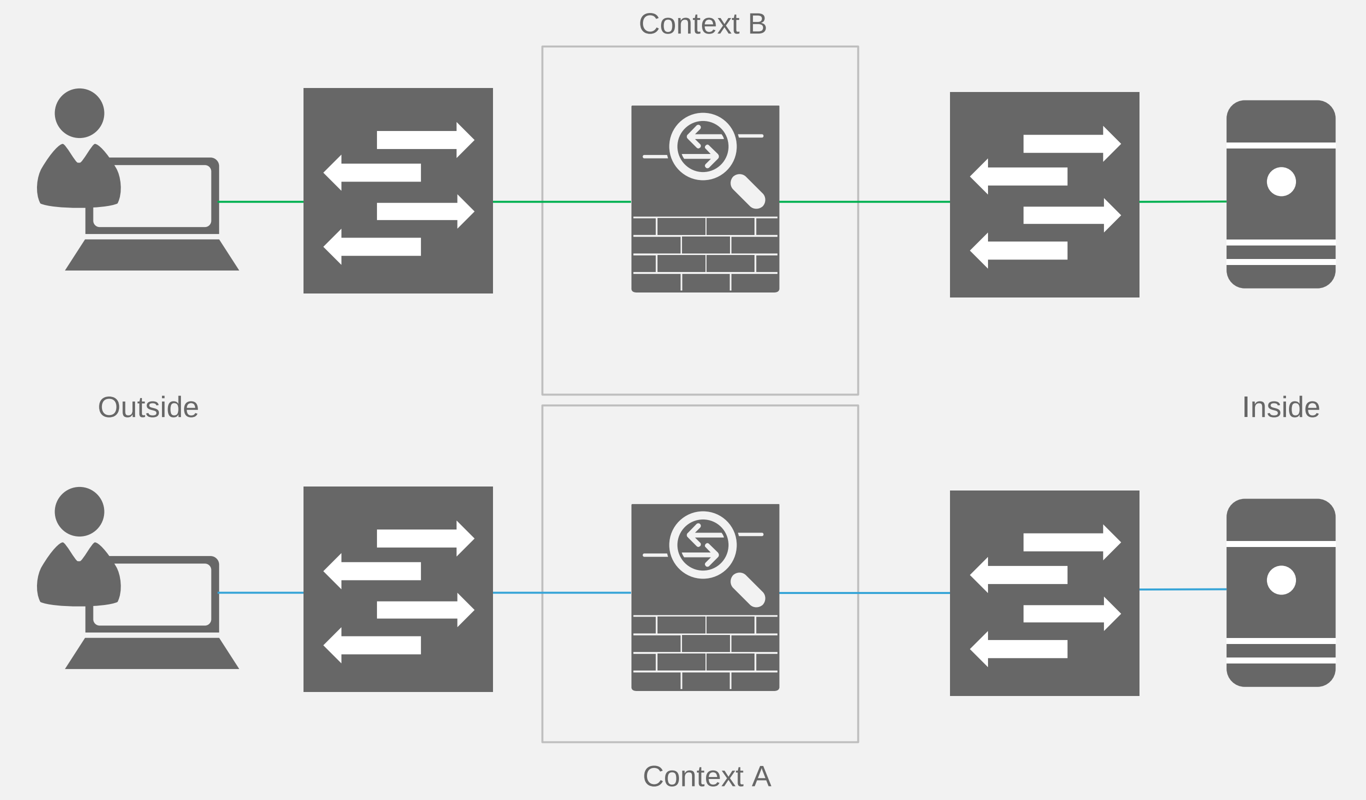
Eliminates asymmetrical traffic issues

Each FirePOWER Services module inspects traffic independently

Multi-context mode for policy flexibility

Deployment Options

- Linear Scalability Clustering
- **Multi-context Mode**
- High Availability



Supported on both the 5508-X and 5516-X models

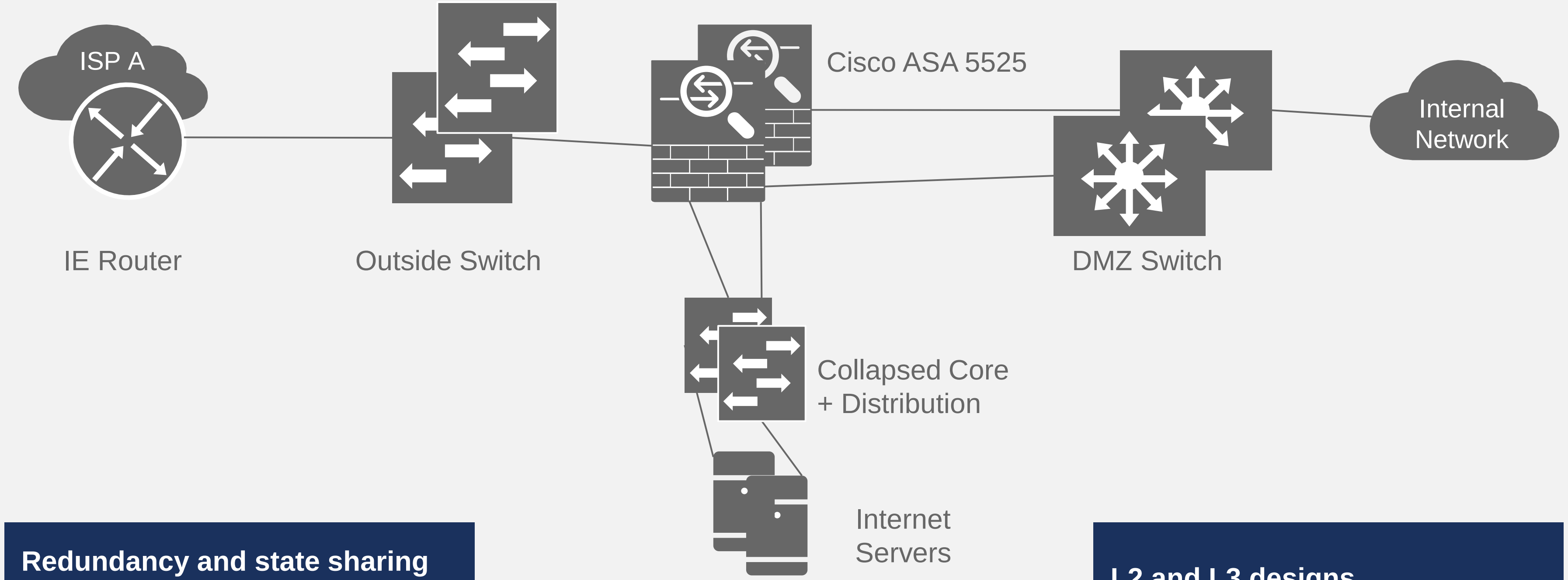
Each interface appears separately to FirePOWER Services module

Allows for granular policy enforcement on both ASA and FirePOWER Services

And high availability for increased redundancy

Deployment Options

- Linear Scalability Clustering
- Multi-context Mode
- **High Availability**



Redundancy and state sharing (A/S and A/A pair)

L2 and L3 designs

FirePOWER can be deployed with ASA in 3 modes

1 **Fail-open**

When FirePOWER services is deployed in fail-open mode, the traffic will not be blocked
in case FirePOWER fails.

2 **Fail-closed**

When FirePOWER services is deployed in fail-closed mode, the traffic will be blocked in case FirePOWER fails.

3 **Monitor Only**

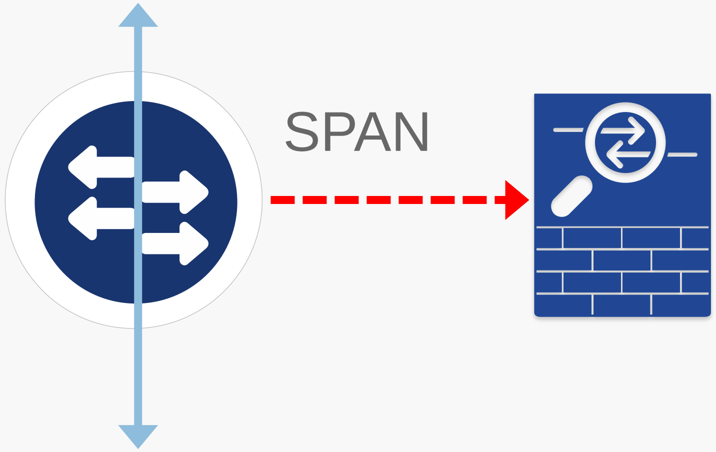
When FirePOWER services deployed in monitor only mode, the traffic from ASA will be copied to FIrePOWER services. The FirePOWER services will not block any traffic. This is usually used for visibility. This mode is also known as “Passive Mode” or “IDS mode.”

With the option to deploy in SPAN port mode (Interface Monitor-only mode)

Considerations for deployment:

- ASA running in transparent mode and single-context mode
- No failover or clustering setup
- SPAN traffic going to FirePOWER Services module in monitor-mode
(CLI command: ‘traffic-forward sfr monitor-only’)
- Traffic forwarding interface must be a physical interface
- Traffic forwarding interface cannot be used for ASA traffic
- ASA version 9.4.1 and FirePOWER version 5.4.1.X
- Other ASA inline interfaces are running ASA functions, but are not forwarding any traffic FirePOWER services module

FirePOWER Services for ASA in Monitor-Only Mode



The default configuration offers easy, first-time setup

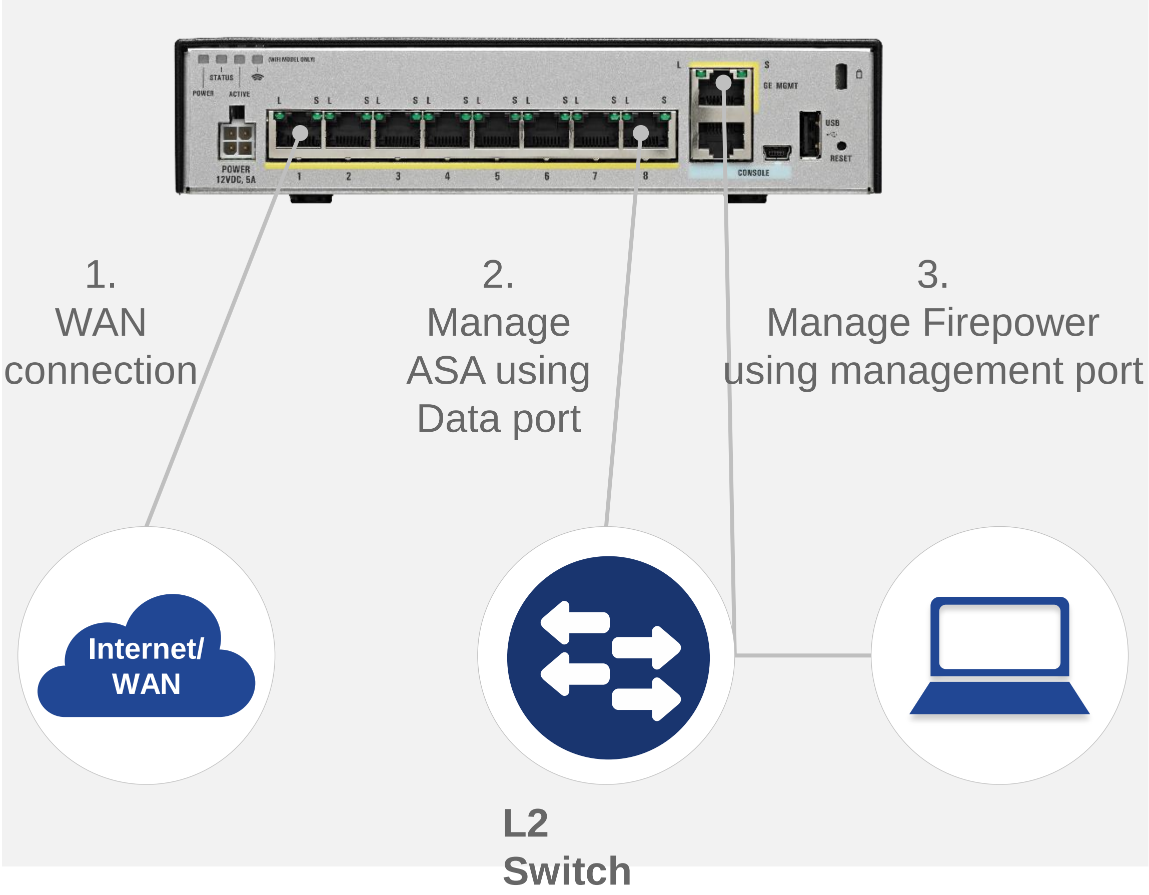
Default Configuration Provides easy Internet connectivity

- There are three steps to provide internet connectivity to laptops

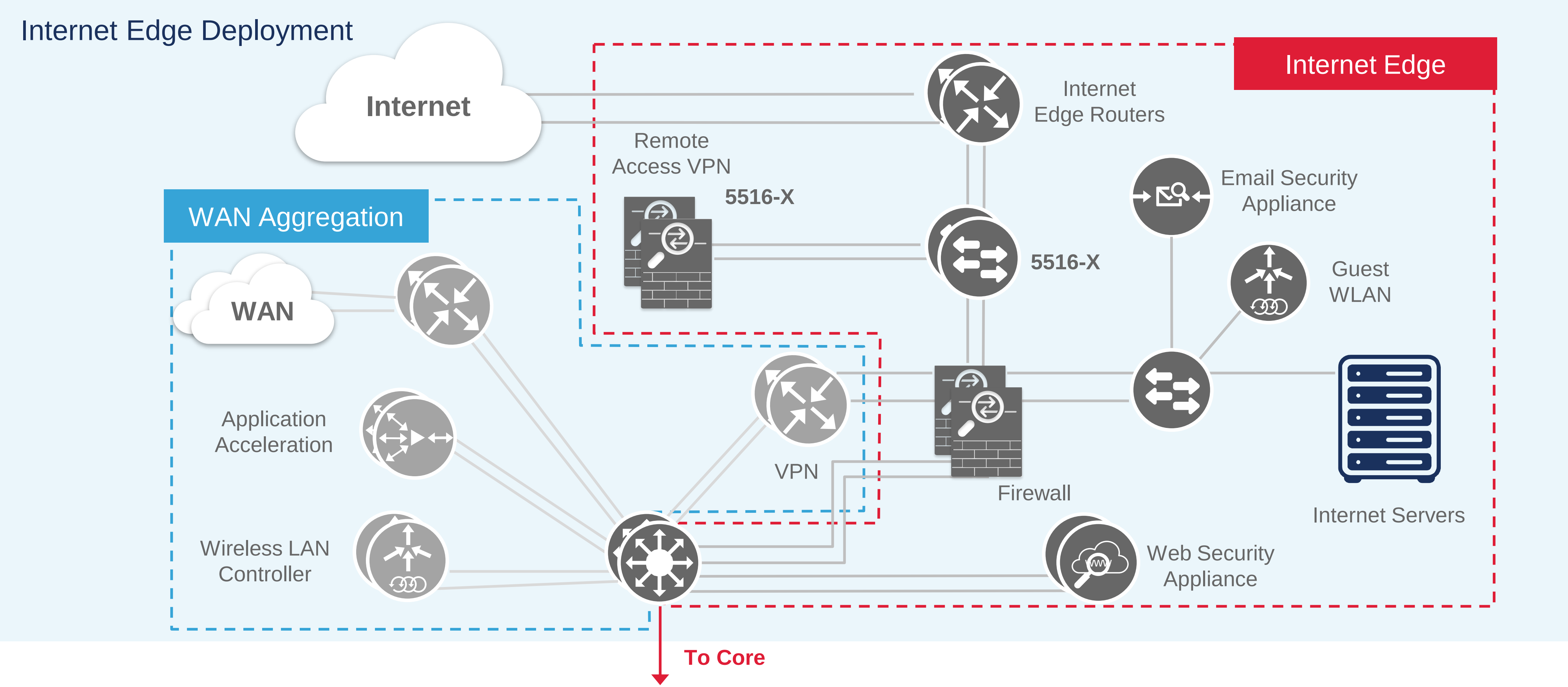
- The WAN port, inside port and management port are already configured

- The WAN port is the outside port that runs DHCP client, the inside port is configured for ASDM management, and the Management port will only be used to manage FirePOWER

- FirePOWER Services can get internet connectivity using L2 switch, L3 switch is not required for SMB deployment

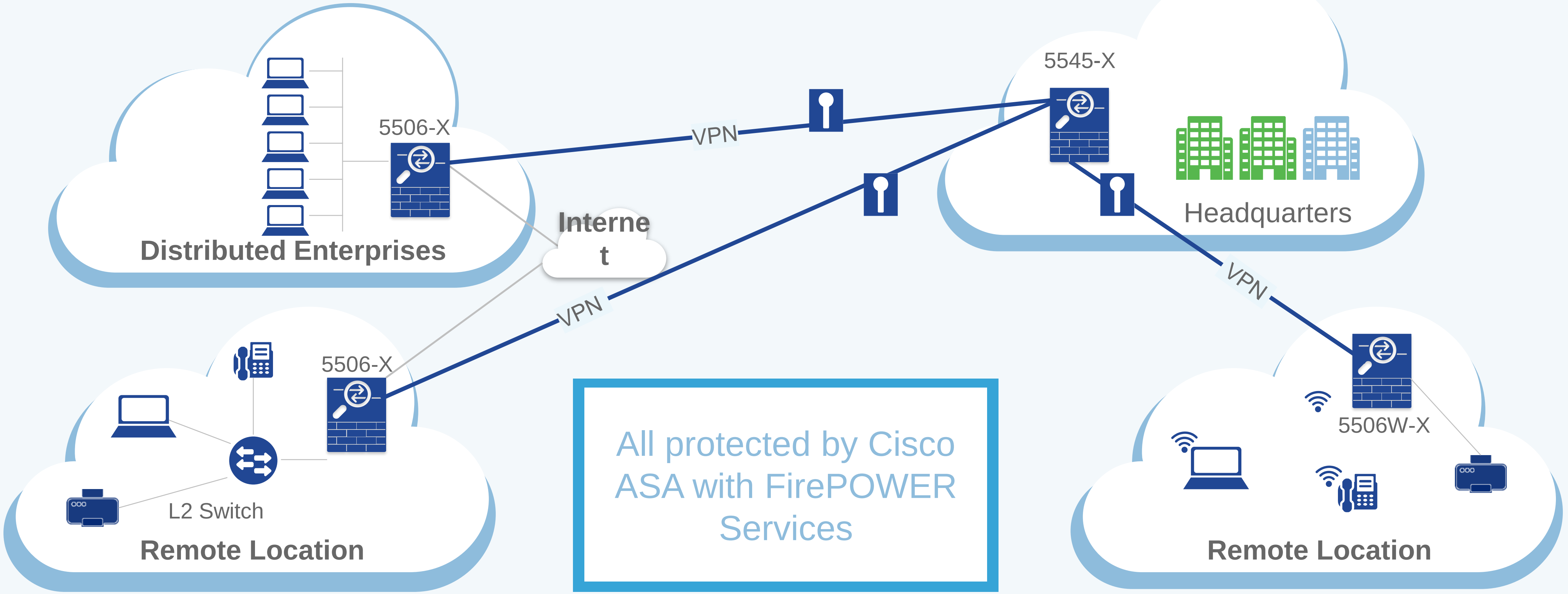


Deploy at the Internet Edge



And protect remote locations

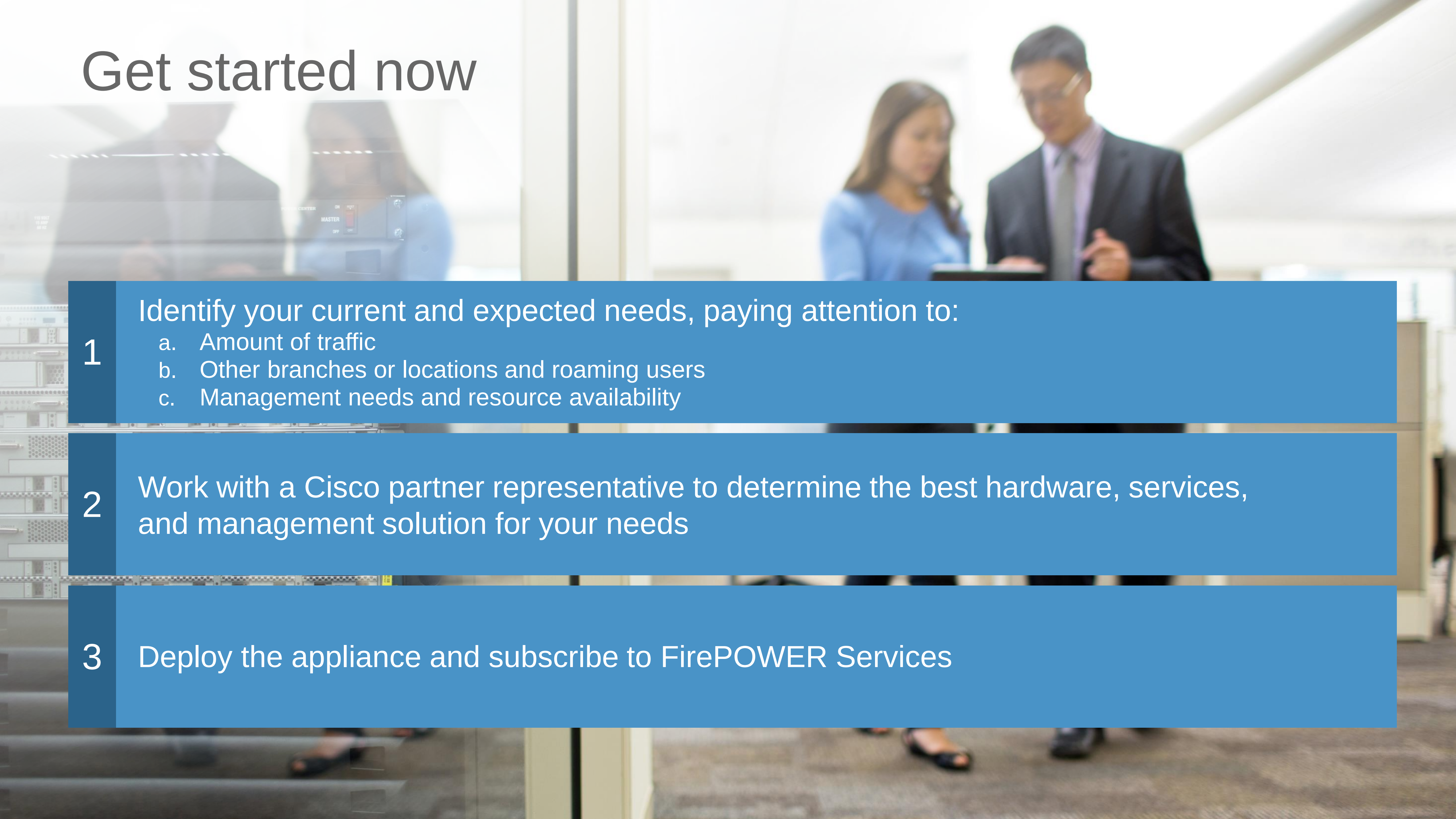
Distributed Enterprises, Remote location/SMB Branch Deployment



All protected by Cisco ASA with FirePOWER Services

Receive this comprehensive protection today

Get started now



1 Identify your current and expected needs, paying attention to:

   a. Amount of traffic
   b. Other branches or locations and roaming users
   c. Management needs and resource availability

2 Work with a Cisco partner representative to determine the best hardware, services, and management solution for your needs

3 Deploy the appliance and subscribe to FirePOWER Services

Check out these additional resources

At-a-Glance

http://www.cisco.com/c/en/us/support/security/asa-5506-x-firepower-services/model.html#At-a-Glance

Data Sheet:

http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html

Cisco Talos Security Intelligence & Research:

http://www.cisco.com/c/en/us/products/security/talos.html

CISCO

TOMORROW starts here.

Backup Slides

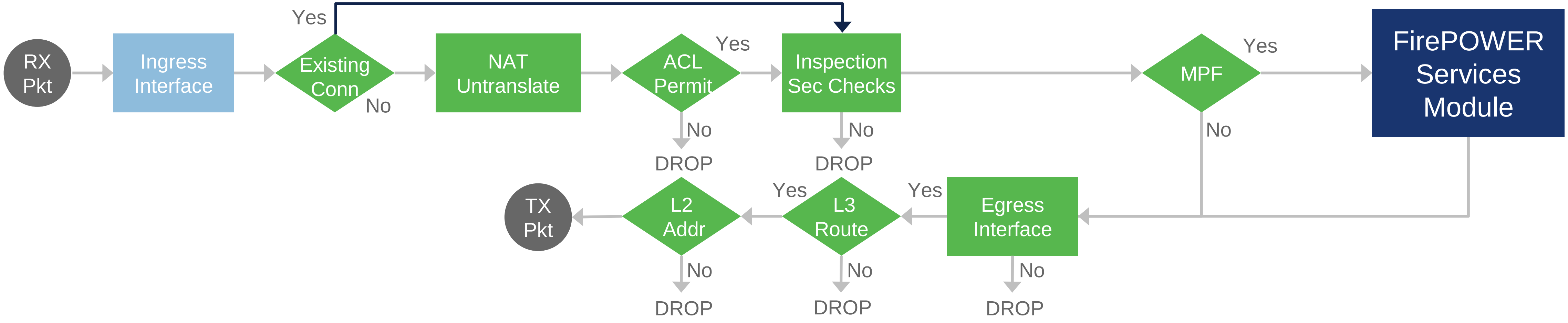
Packet Processing Order of Operations

1. ASA Module processes all ingress packets against ACL, Connection tables, Normalization and CBAC before traffic is forwarded to the FirePOWER Services module

2. ASA provides flow normalization and context-aware selection/filtering to the FirePOWER Services

3. Clustered ASA provides flow symmetry and HA to the FirePOWER Services

4. Packets and flows are not dropped by FirePOWER Services
   - Packets are marked for Drop or Drop with Reset and sent back to ASA
   - This allow the ASA to clear the connection from the state tables and send resets if needed



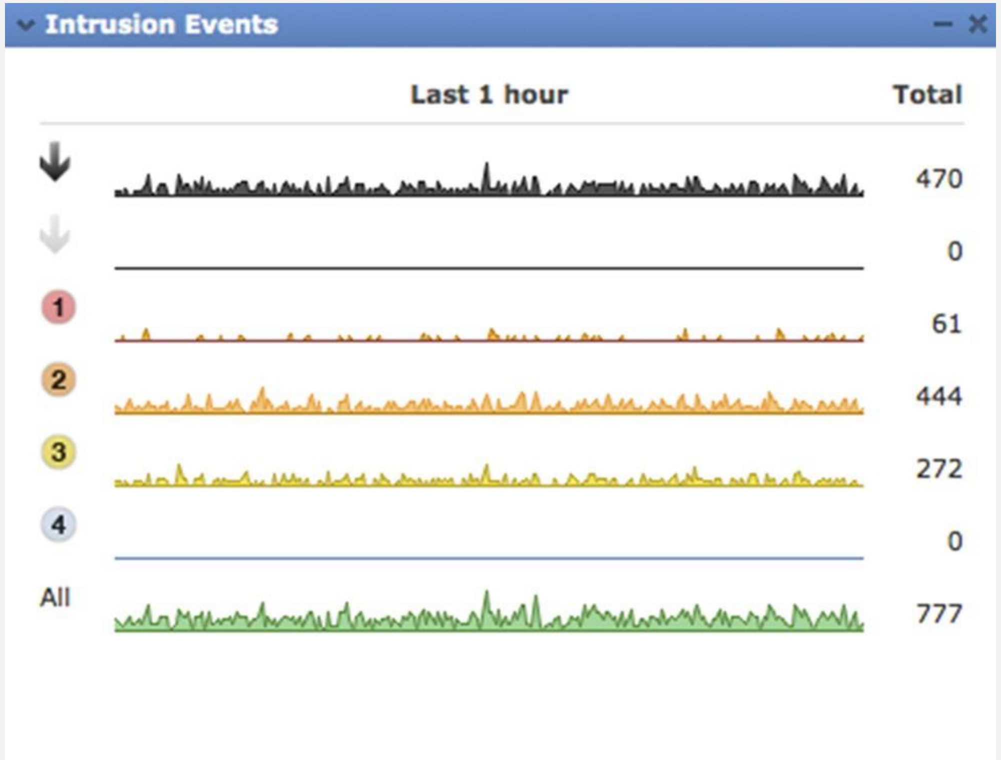
Key Enhancements Over ASA 5505

5506-X
MORE SECURE
MORE SCALEABLE
MORE FLEXIBLE

Category	Sub-Category	5505	New ASA with FirePOWER Services
NGFW — FirePOWER Services	**Application Visibility & Control**	No	Yes
	AMP, NGIPS, URL Filtering Subscriptiions	No	Yes
Hardware Security	**Trust Anchor Module** **Hardware Anti-Tamper**	No	Yes
Simplified Purchase Experience	**Unlimited User (node) Support**	No	Yes
VPN	**Enhanced mobility support**	No	Yes
Additional Features	**Throughput**	→	Over 2.5X Steteful Performance
	Integrated Wireless Access Point	No	Yes (5506W-X variant)
	Ruggedized Option	No	Yes (5506H-X variant)
	POE	Yes	No

Stay focused on what’s important

Impact Assessment



Intrusion Events

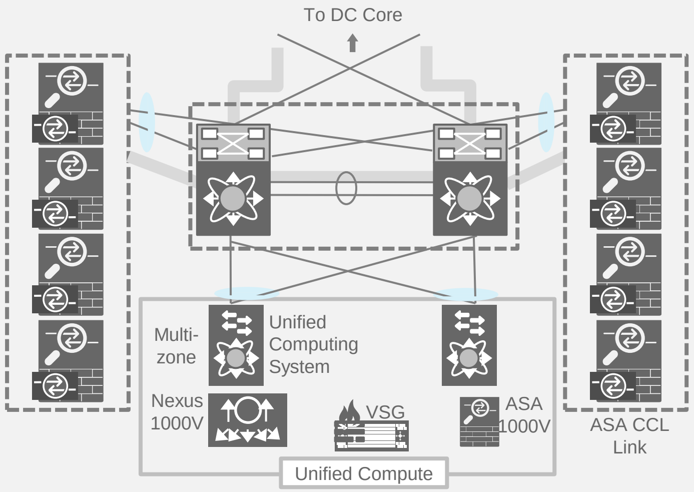
	Last 1 hour	Total
↓		470
↓		0
1		61
2		444
3		272
4		0
All		777

Correlates all intrusion events with an impact of the attack against the target

Impact Flag	Administrator Action	Why
1	Act Immediately; Vulnerable	Event corresponds with vulnerability mapped to host
2	Investigate; Potentially Vulnerable	Relevant port open or protocol in use, but no vulnerability mapped
3	Good to Know; Currently Not Vulnerable	Relevant port not open or protocol not in use
4	Good to Know; Unknown Target	Monitored network, but unknown host
5	Good to Know; Unknown Network	Unmonitored network

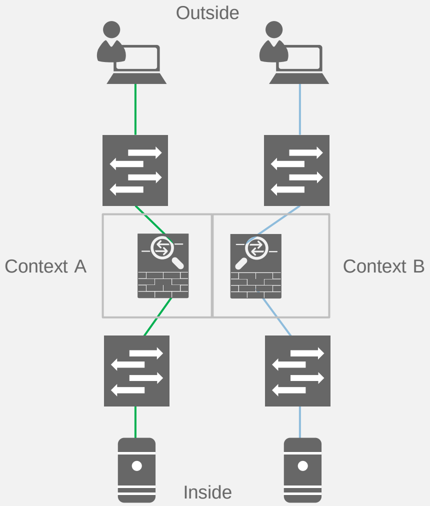
FirePOWER Services support all current ASA deployment models

Clustering for linear scalability



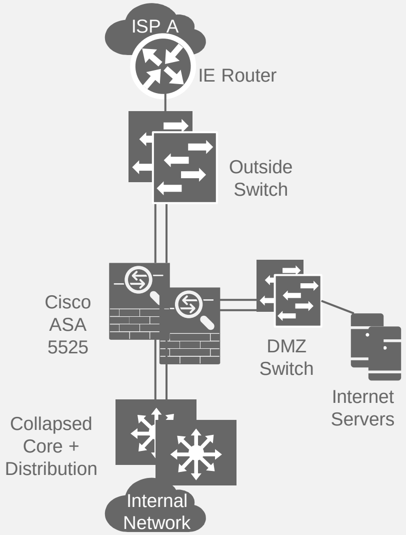
- Up to 16x ASA in cluster
- Eliminates Asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently

Multi-context mode for policy flexibility



- Each ASA Interface appears as a separate interface to FirePOWER Services module
- Allows for granular policy enforcement on both ASA and FirePOWER services

High availability for increased redundancy



- Redundancy and state sharing (A/S & A/A pair)
- L2 and L3 designs

*State sharing does not occur between FirePOWER Services Modules