



Cisco Support Community Expert Series Webcast



Cisco Adaptive Security Appliance (ASA) Lifeline of today's Data Centers

Akhil Behl

Solutions Architect

Author of '*Securing Cisco IP Telephony Networks*'

<http://www.ciscopress.com/title/1587142953>

July 30th 2013

Cisco Support Community – Expert Series Webcast (Presenter and Speaker)

- Today's featured expert is Cisco's Solutions Architect Akhil Behl
- Ask him questions now about Cisco ASA's next Gen Features



Akhil Behl
(Solutions Architect)

Cisco Support Community – Expert Series Webcast (Panel of Experts)



Parminder Pal Singh
(Cisco Technology Trainer)



Sumanta Bhattacharya
(Network Consultant)

Thank You for Joining Us Today

- Today's presentation will include audience polling questions
- We encourage you to participate!



Thank You for Joining Us Today

- If you would like a copy of the presentation slides, click the PDF link in the chat box on the right or go to the following url:



Document url:

<https://supportforums.cisco.com/docs/DOC-35101>

Polling Question 1

What is the most important feature from a Firewall perspective that you would like to have for your organization?

- a) Scalability – I should be able to scale the throughput and processing power on an ongoing basis, as and when required**
- b) Threat protection – I want world class threat protection from various attacks to safeguard my organization's IT assets and information**
- c) Protection of and return on investment – I should be able to leverage new features without replacing the existing hardware**
- d) I think I need all of the above, cannot part with any thing**

Submit Your Questions Now!

Use the Q&A panel to submit your questions. Experts will start responding those





Cisco Support Community Expert Series Webcast



Cisco Adaptive Security Appliance (ASA) Lifeline of today's Data Centers

Akhil Behl

Solutions Architect

Author of '*Securing Cisco IP Telephony Networks*'

<http://www.ciscopress.com/title/1587142953>

Agenda

An introduction to Cisco ASA 5500 / 5500-x series Firewalls

Cisco ASA – Next-Gen Firewall technology for BN

Insight into Cisco ASA Firewall Clustering

Overview of Cisco ASA Web-Security (ScanSafe)

Overview of Cisco ASA TrustSec

Q&A

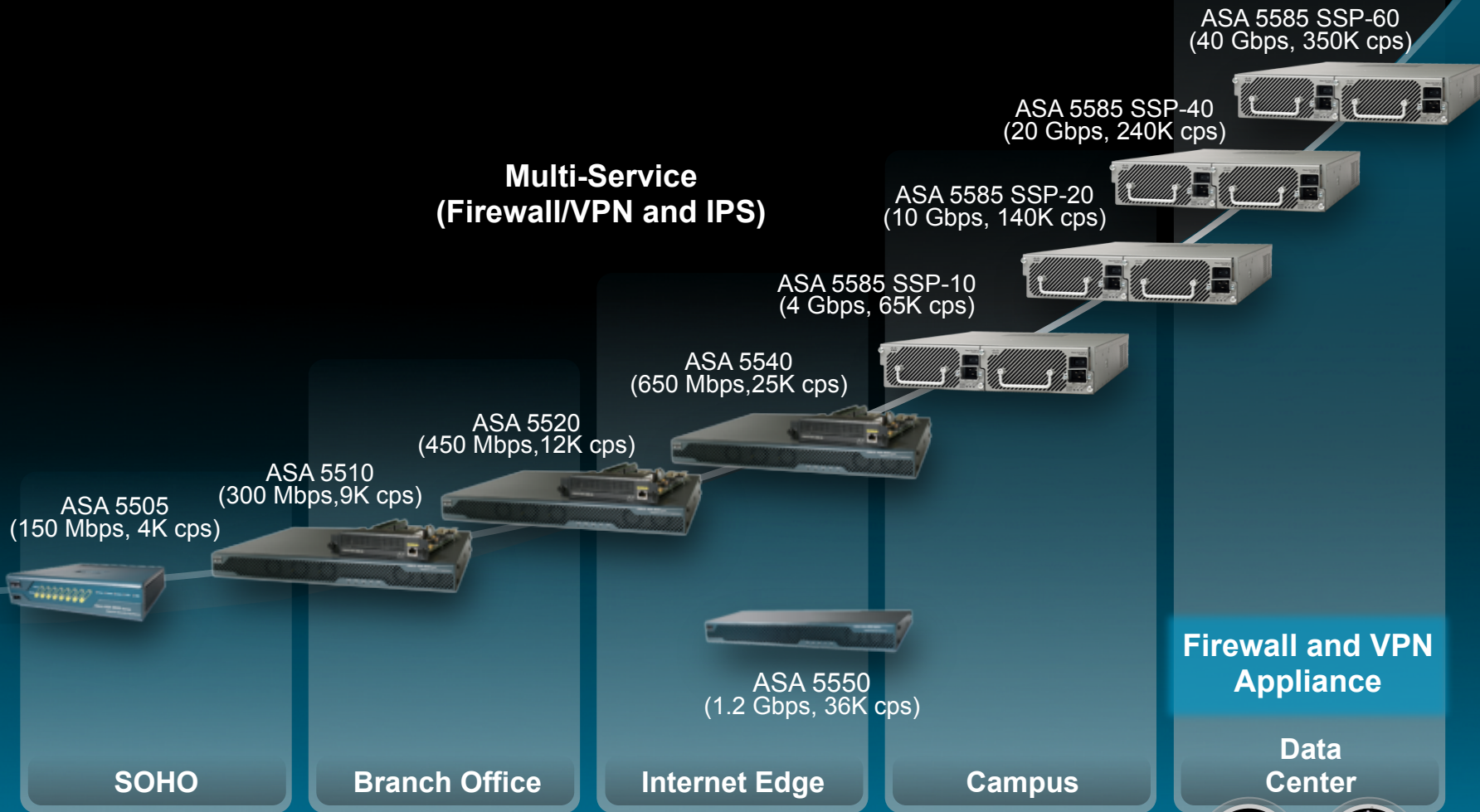


The Cisco ASA 5500 and 5500-X Series Adaptive Security Appliances

Cisco ASA – Serves Wide Range of Solutions

Ranging from SOHO to Enterprise Networks

Performance and Scalability



Adaptive Security Appliance Platform

Enterprise Strength and Scalability

Proven Technology

15+ years of enterprise-class products
Over 1 million ASA units in the market

Extensible / Scalable

Add services to fit growing needs
Multiple security services



World Class Security

Purpose-built for high-performance , highly
scalable security

Software-Centric

Immediate benefits from any software feature
enhancements

Cisco Adaptive Security Appliance Platform

Maximum Uptime, Greater Resiliency

High Availability

- Full-meshed Active/Standby and Active/Active
- Full application state synchronization
- Zero downtime upgrades
- Sub-second failover

Reliability and Resilience

- 2X reliability of a server-based solution
- Cisco ASA MTBF: 100-150K hrs
- Redundant power supplies
- Multi-level resiliency prevents component, link, system failure

The Cisco ASA 5500-X Series Firewalls

Purpose-Built Firewall for Mission-Critical Data Centers

Space

Access

Performance

Compliance

Threats



Elastic Scale

- Fastest connections per second
- Highest number of VPN sessions

Superior Span

- Unprecedented deployment flexibility
- 8X performance density

Leading-Edge Security

- Best of breed firewall, IPS, and VPN
- Includes Cisco guaranteed coverage
- Versatile, always-on remote access

Cisco ASA 5500-X – High End Performance

Delivers MultiScale™ Performance
to Meet the Needs of Mission-Critical Data Centers



- Rapid Connections per Second
- Abundance of Concurrent Sessions
- Accelerated Throughput
- Multiple Security Services
- Span Multiple Platforms and Deployment Scenarios

Polling Question 2

What is primary role of ASA in your Data Center?

- a) Cisco ASA is heart and sole of my Data Center and I leverage it's next gen threat protection capabilities in addition to standard firewall features
- b) It's used as a Unified Threat Management (UTM) Appliance protecting my network against a host of threats
- c) It's used as a basic perimeter firewall for filtering traffic
- d) I don't have Cisco ASA as of yet in my Data Center however, plan to have it's world-class protection for my network soon



Cisco ASA Next-Gen Firewall Technology for Borderless Networks

Business Imperatives

Growing Number
and Range of
Devices



Sensitive Information
from Different
Sources



Prevalence of
Data Theft



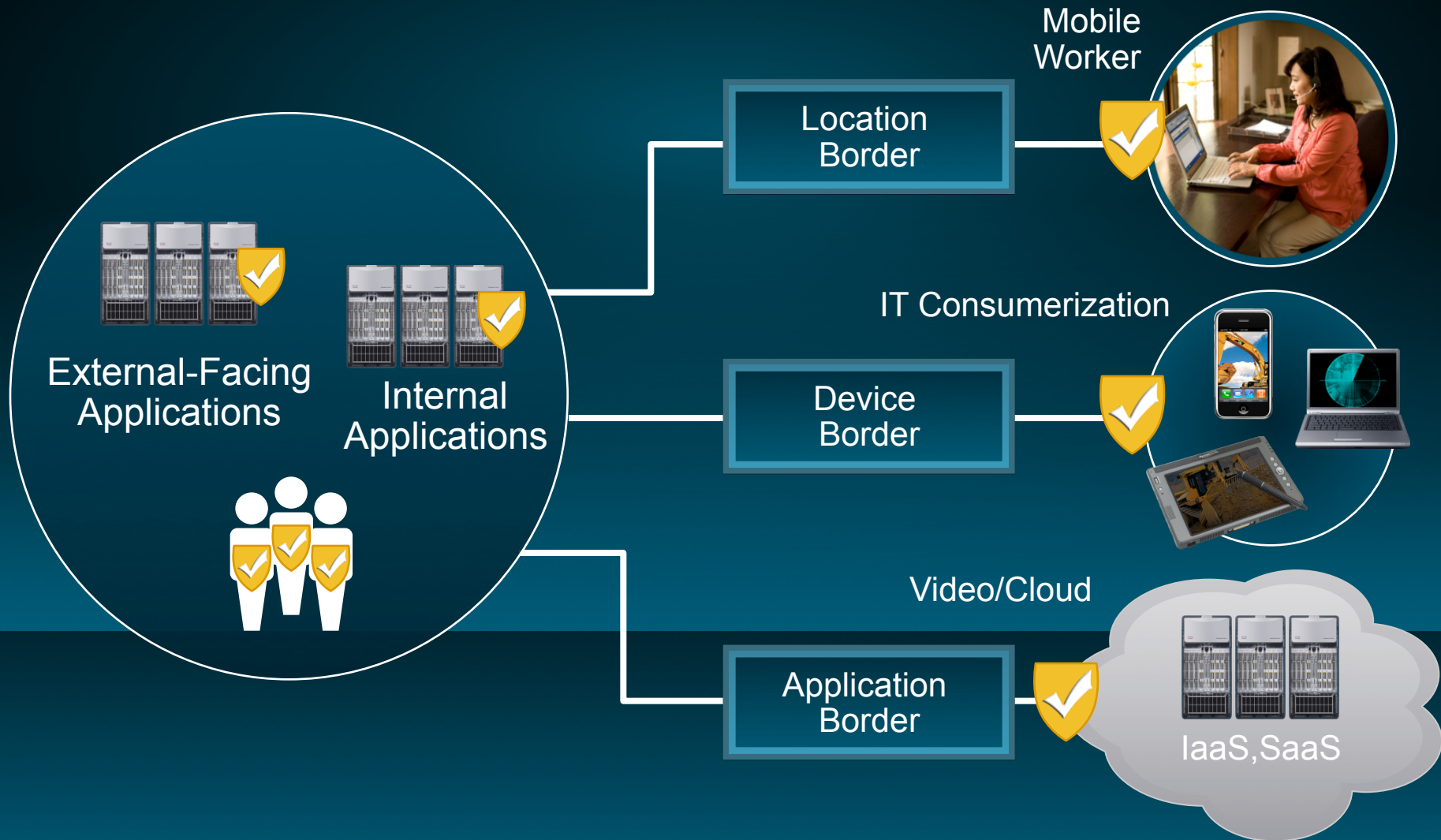
Simplify
Security for the User,
the Business, and for
the Operations

Maintain Regulatory
Compliance and
Manage Risk Well

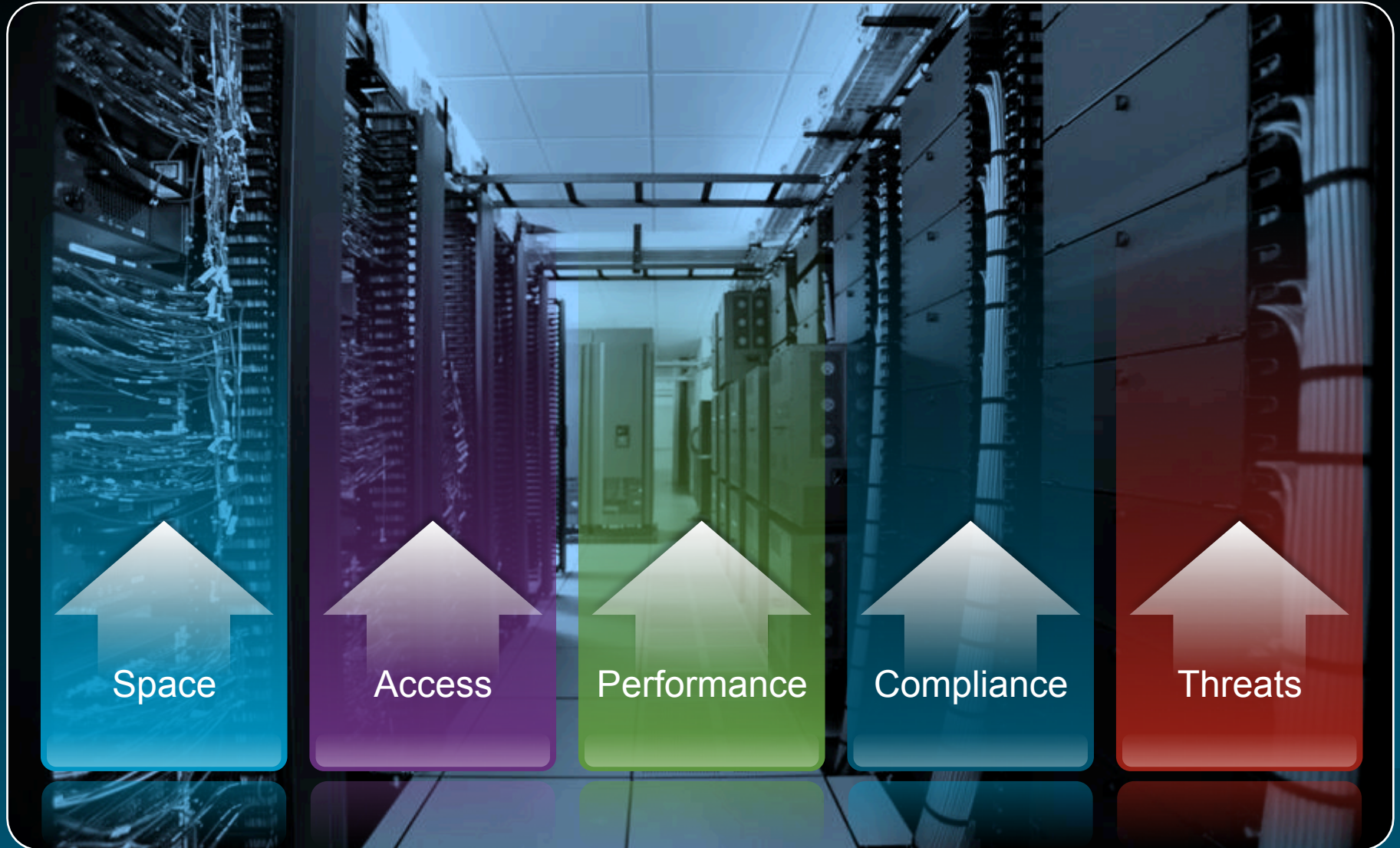
Design and Defend
for Unpredictable
Threats

Security Imperatives

Changing Environment - Shifting Borders



Today's Data Center Challenges



Space

Access

Performance

Compliance

Threats

Superior Scalability

Up to **350,000** connections per second

Up to **8** million connections

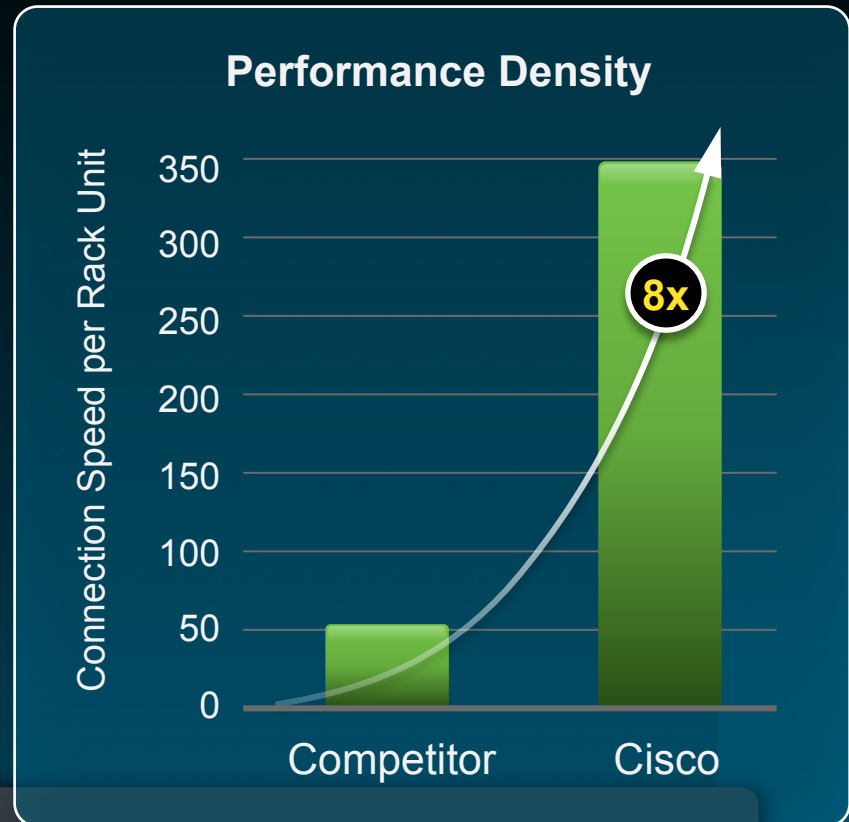
Up to **35** Gbps multi-protocol throughput

Clustering up to 8 firewalls

Lower power consumption

Lower cooling costs

All this in just **2** Rack Units



8X the Performance Density of Competitive Firewalls

Superior Span Across Security Verticals

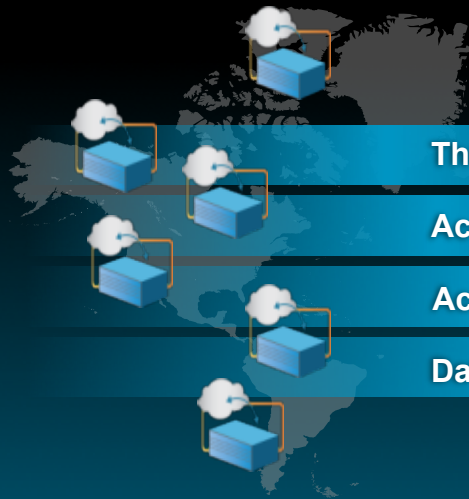
Network or Cloud Enforcement

- Consistent **Security**
- Consistent **Management**
- Consistent **Visibility**



Intelligent Traffic Routing Client

Broad OS Platform Support
Minimal Device Requirements



Threat Protection

Acceptable Use

Access Control

Data Loss Prevention

Platform Agnostic Security – BYOD Support



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 ASA Firewall Clustering

Why Clustering?



- Scaling to **100+ Gbps** of traffic through a cluster of Cisco ASA appliances
- Ease of **On-going** management
- Achieve **Deployment** Simplicity
- High **Availability** and **Investment** Protection

Data Centers Require Better Methods to Deliver Secure, High Performance Connectivity

Cisco ASA – Clustering Highlights

Scaling Factor

- Total throughput equals N times single node throughput times scaling factor
- Linear scaling factor regardless of N

N-to-N High Availability

- All units are active
- Seamless traffic redistribution in the event of node failure

Manageability

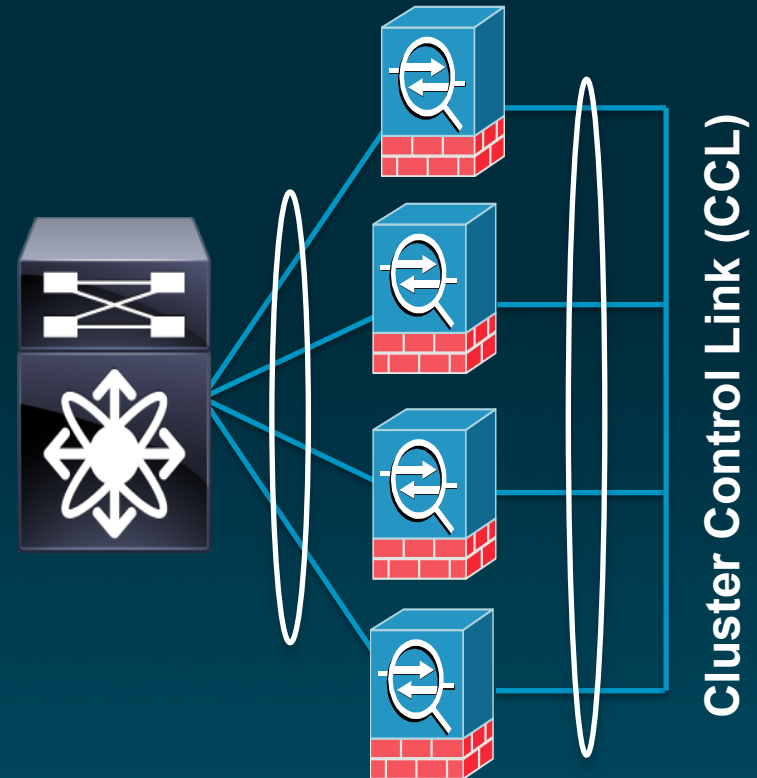
- Single configuration and automatic configuration synchronization across the cluster
- Cluster-wide resource usage statistics

Same Level of Redundancy

- Every traffic flow has a backup within the cluster

Clustering Overview

- **Cluster up to eight ASA appliances**
- **Load-balancing approach**
 - Stateless load balancing by external switch (Ether Channel load balancing [ECLB] or Router (Equal Cost Multipath [ECMP] or Cisco® Policy Based Routing [PBR])
 - Load balance within cluster over proprietary Cluster Control Protocol
- **In-cluster high availability via Cluster Control link (CCL)**
- **Hitless upgrade for Production Environments**

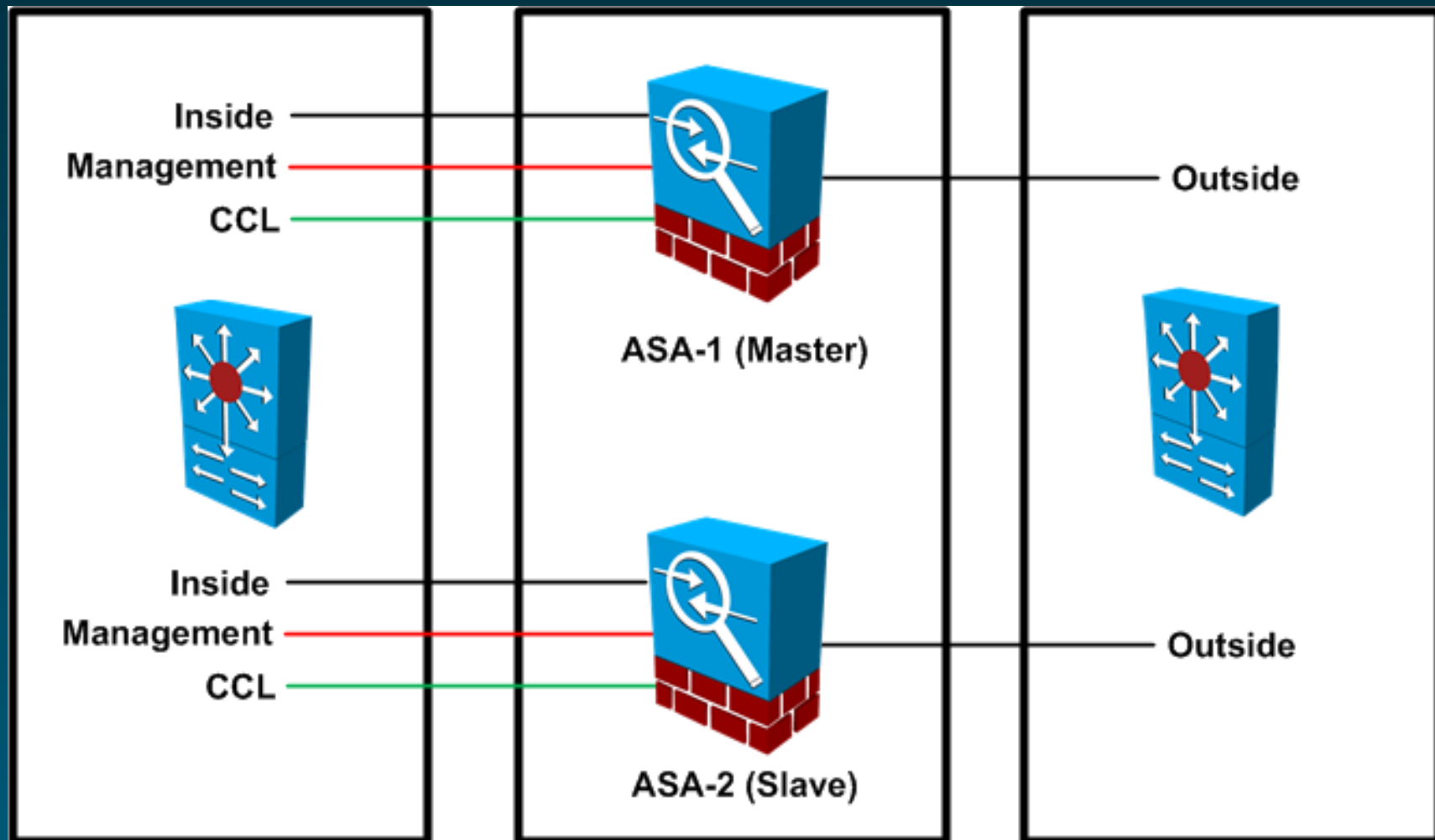


Clustering: High Availability

- All the units in the cluster are active and are passing traffic
- Clustering can be configured in **Individual mode** or **Spanned mode**
- All the units in the cluster are either owner or backup on a session by session basis
- In case of a node failure, the backup unit(s) take over the session
- Use of LACP allows neighboring switches to stop sending traffic over the failed link.
- Single Configuration console and Automatic Configuration Sync across the Cluster
- Remote Command Execution to any node
- Cluster-wide resource usage statistics

Cisco ASA Clustering Configuration

Live Demonstration (Topology)



Clustering Limitations

- Not all inspection engines are available in clustered mode
- Remote Access VPN is not available in clustered mode
- Site-to-Site VPN is centralized to one node
- Unified Communications is not supported in clustered mode



Cisco ASA ScanSafe

Cisco ASA – The Best In Class

**Best in Class Network
Security**



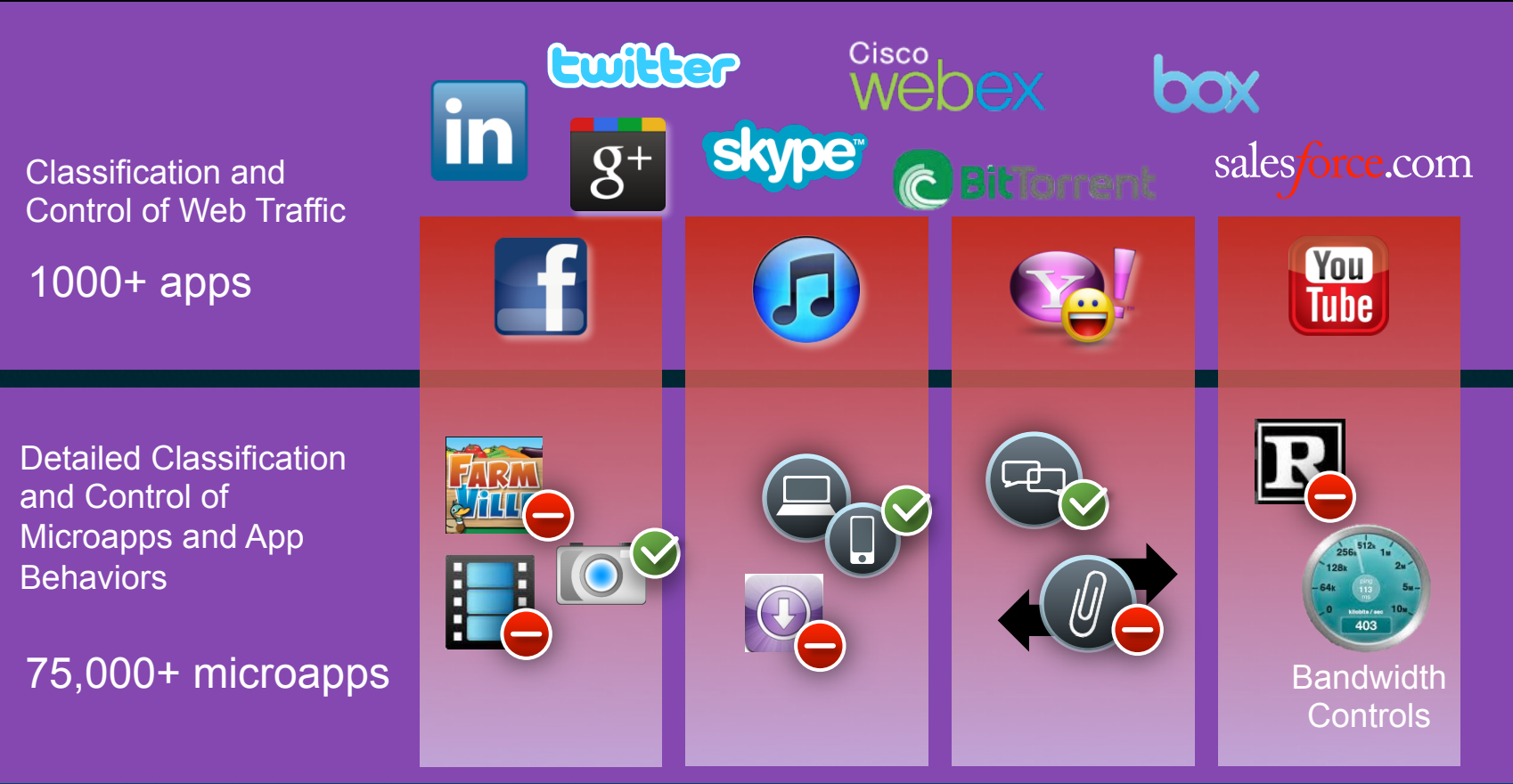
**Best in class Cloud web
security**



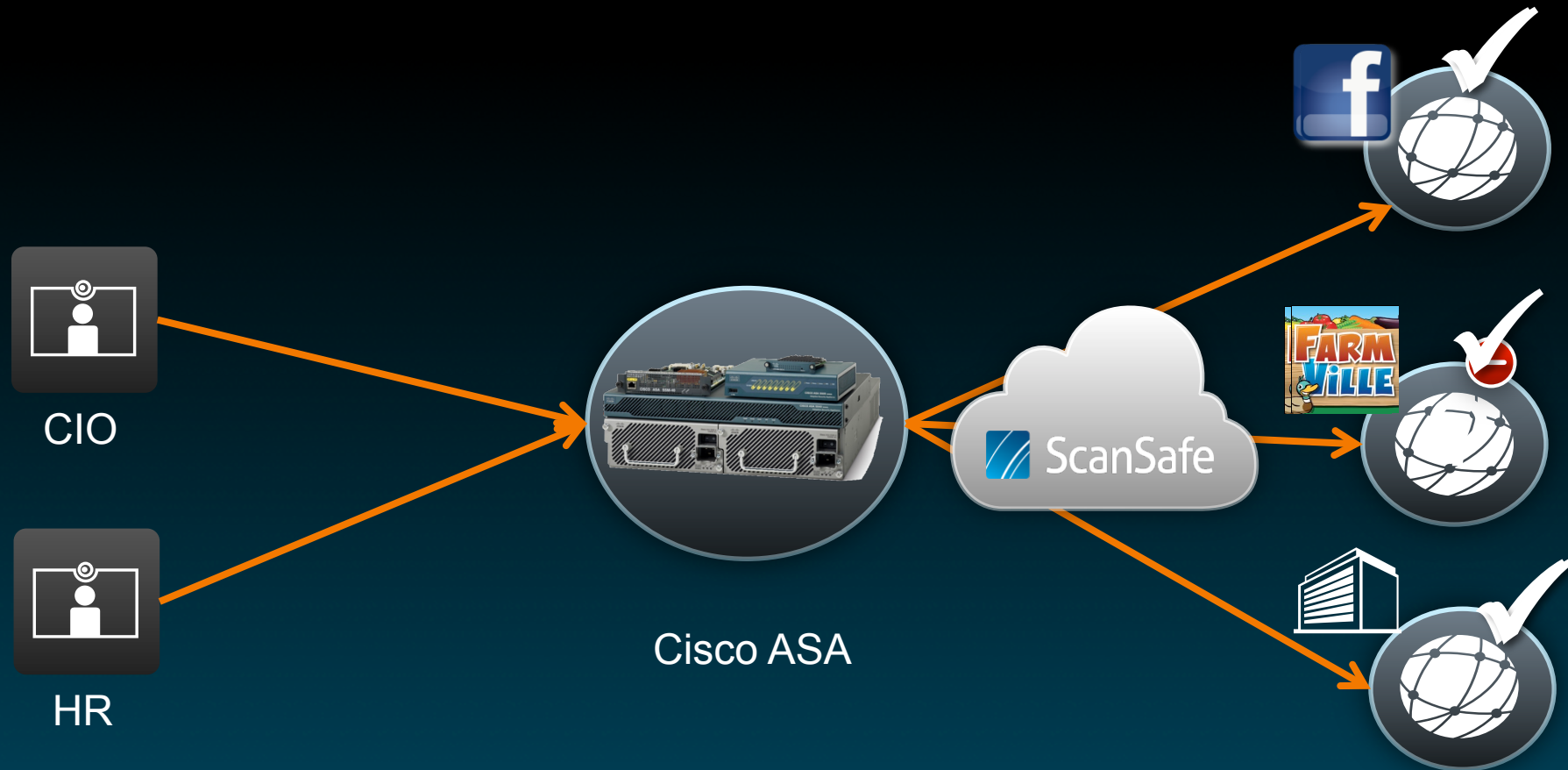
ScanSafe Overview



ScanSafe – Web Applications Visibility and Control



Flexible Policy Enforcement



- Identity aware cloud based web security
- Supports per context ScanSafe redirection
- Multiple AV engines and Web-content Scanlets

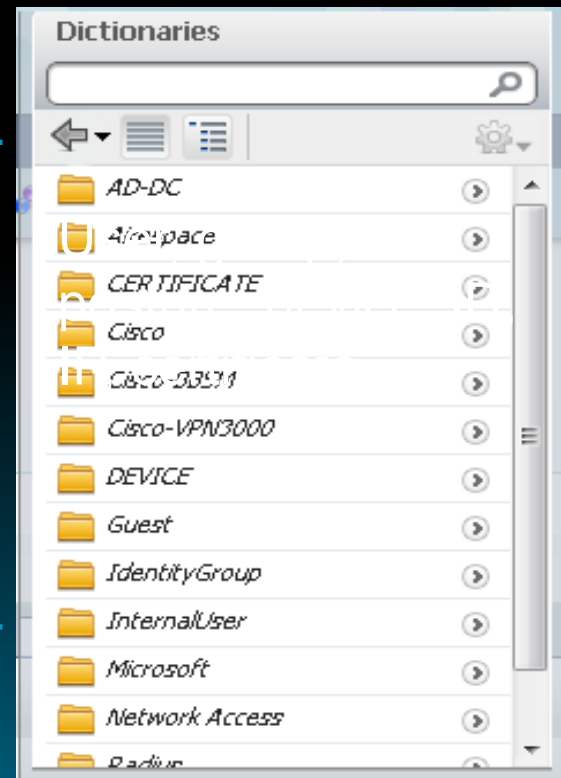


Cisco ASA TrustSec

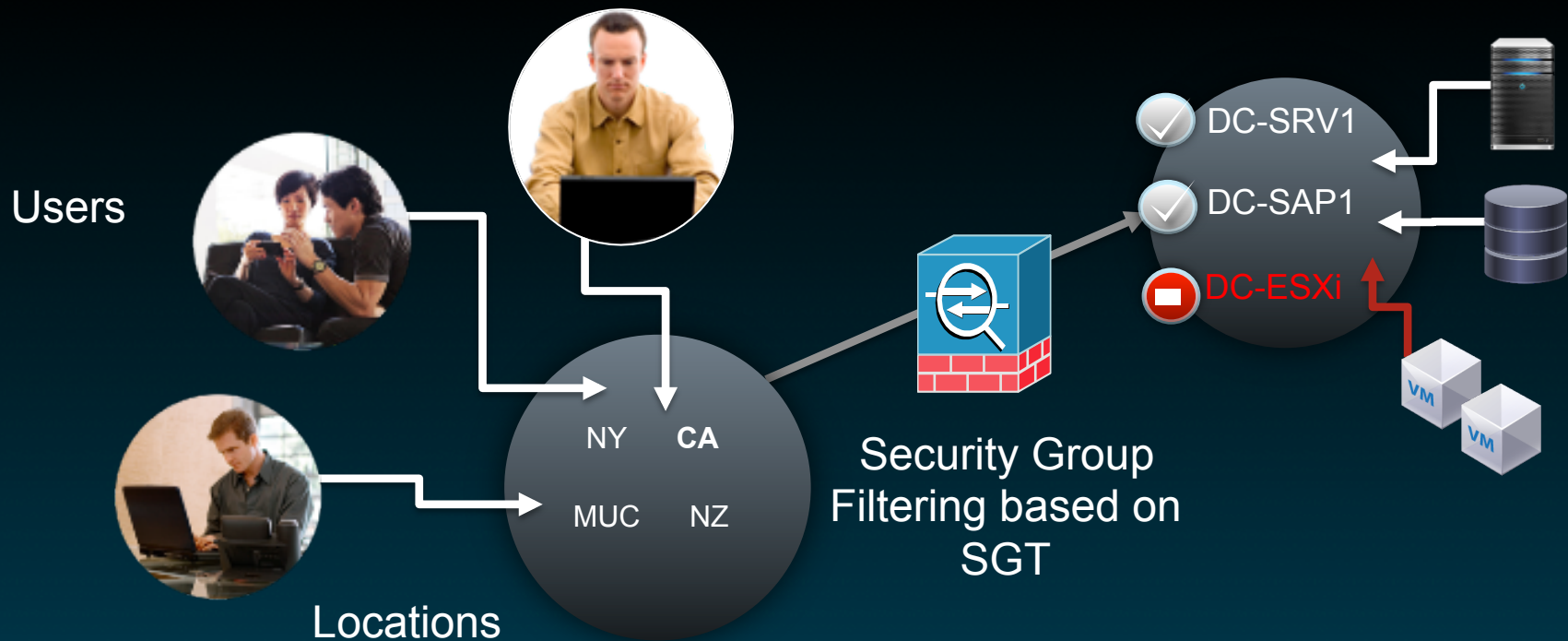
What is Cisco TrustSec?

Covers anything having to do with Identity:

- IEEE 802.1X (Dot1x)
- Profiling Technologies
- Guest Services
- Secure Group Access (SGA)
- Access Control Server (ACS)
- Identity Services Engine (ISE)



Cisco ASA TrustSec Overview



- Cisco Security Group Tags (TrustSec and ASA) helps reduced >500,000 firewall rules to 50 rules
- SGT can be a function of one or many attributes; allows complex policy rules
- ASA Access Policies can be a combination of SGT and 5-tuple rules

Policy definition – ISE Egress Policy Matrix

CISCO Identity Services Engine ise admin Logout Feedback

Home Operations Policy Administration Task Navigator

Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

Egress Policy Network Device Authorization

Source Tree Destination Tree Matrix

Egress Policy (Matrix View)

Edit Add Clear Mapping Configure Push Monitor All Dimension 6X10 Show Policy-View-1

Destination Source	Web_Servers (7 / 0007)	Time_Card_Server (10 / 000A)	Manager_Portal (9 / 0009)	Employee_Portal (8 / 0008)	CreditCard_Server (11 / 000B)
Unregist_Dev_SGT (3 / 0003)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP
Management_SGT (5 / 0005)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP
Employee_SGT (4 / 0004)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP
CC_Scanner_SGT (6 / 0006)	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP

Default Enabled SGACLs : Permit IP Description : Default egress rule

Policy Enforcement – Cisco ASA

Cisco ASDM 6.7 for ASA - 10.1.201.2

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

type topic to search Go

CISCO

Device List

Find: 10.1.201.2

10.1.201.2

10.1.66.2

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity By TrustSec
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging	Time	Descript
		Source	User	Security Group	Destination	Security Group						
inside (1 incoming rule)												
1	<input checked="" type="checkbox"/>	any			any		ip	Permit	TOP 10 ...			
outside (9 incoming rules)												
1	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit	0			
2	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny	0			
3	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit	0			
4	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny	0			
5	<input checked="" type="checkbox"/>	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit	0			
6	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	Deny	0			
7	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Time_Card_Ser...	https	Permit	0			Time Card Application
8	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser...	https	Deny	0			Time Card Application
9	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	CreditCard_Ser...	https	Permit	0			Credit Card Scan Communication
Global (1 implicit rule)												
1		any			any		ip	Deny				Implicit rule

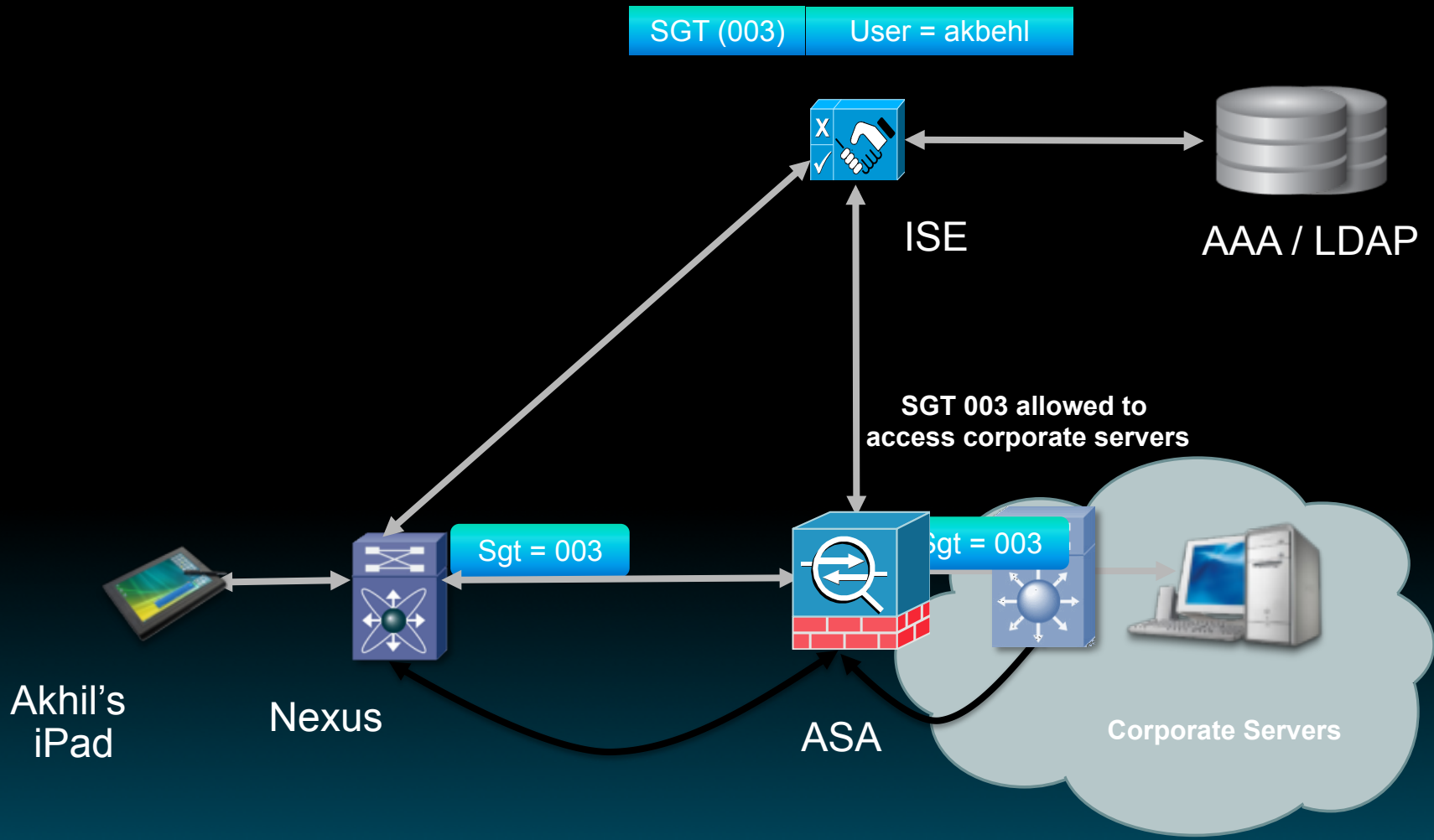
Apply Reset Advanced...

Configuration changes saved successfully.

<admin> 15

5/31/12 11:53:50 PM PDT

Cisco ASA TrustSec in Action



Cisco ASA TrustSec – Use Case(s)

User=akbehl

Authenticates from a **corporate asset (laptop)**, gets assigned **SGT = 007/Quarantine**

It turns out that **AV** was turned **OFF**

Once AV is turned on akbehl gets assigned 008/Compliant

On ASA: { if SGT = 008; allowfull_access to enterprise_servers }

User=Guest

Authenticates from **guest_iPad**

Gets assigned to SGT = 100/Guest

On ASA: { if SGT = 100; allow internet_only access }

Polling Question 3

Do you leverage Cisco ASA's next gen security features such as – Clustering, ScanSafe or TrustSec?

- a) I leverage all three features in my Data Center environment and am realizing the benefits**
- b) I intend to / leverage all / some of these features for maximizing the throughput and scalability, reliable web filtering and BYOD policy implementation and hope these will help me bring down TCO and increase ROI**
- c) I'm not sure if these features will be useful in my environment and need further information to make a conscious decision**
- d) I do not intend to use any of these features in near future**

Further Reading and References

- Cisco ASA Product Portfolio

www.cisco.com/go/asa

- Cisco ASA Startup and Basic Configuration

<http://www.firewall.cx/cisco-technical-knowledgebase/cisco-firewalls/964-cisco-asa5500-startup.html>

- Securing Cisco IP Telephony Networks

<http://www.amazon.com/dp/1587142953>

- Cisco ASA Configuration Guides

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html



Submit Your Questions Now!

Use the Q&A panel to submit your questions. Experts will start responding those



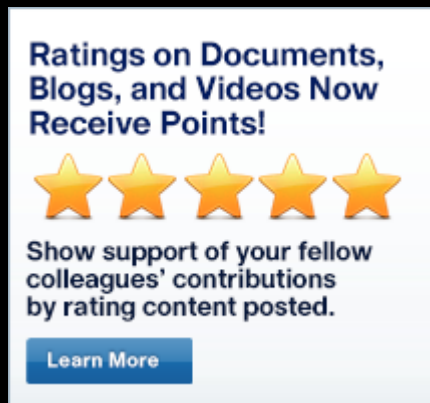
Trivia Question

- **How is Cisco Adaptive Security Appliance (ASA) making your new car safer?**
 - a) Cisco ASA is part of the infrastructure for NCCAR an organization that assist in the testing of safety of new cars
 - b) Cisco ASA is part of the NASCAR circuit
 - c) Cisco ASA came out in 2004 as part of a national safety initiative for new cars

Follow-up **Ask the Expert** Event

- **If you have additional questions, you can ask them to Akhil, Sumanta & Parminder. They will be answering from July 30 to August 9.**
- <https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>
- **You can watch the video or read the Q&A, 5 business days after the event at**
- <https://supportforums.cisco.com/community/netpro/ask-the-expert/webcasts>

Rate content in the Cisco Support community.



Now, when you rate, authors get points!!...

Now you can help the great content to be more easily found and for the ratings you provide to videos, blogs and videos, the authors get the points.

<https://supportforums.cisco.com/community/netpro/idea-center/cafe/blog/2013/06/07/ratings-extended-to-documents-blogs-and-videos>

Now you can access the non-English communities from the new version of the mobile app (iPhone, iPad, or Android)



If you speak Spanish, Portuguese, Japanese, Russian, or Portuguese, you can access the communities on these languages from your mobile device.

Visit : <https://supportforums.cisco.com/docs/DOC-34844>



Expert Corner

Engage, Collaborate, Co-Create and Share with Experts!

Live interactive events, blogs and much more on the Cisco Support Community

Visit:

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

Next Expert Series Webcast in Portuguese

Cisco IOS XR Software: Fundamentals, Configuration, and Troubleshooting

Wednesday Aug 7, at

11 a.m. Brasilia City time (UTC-3 hours)

9 a.m. PDT San Francisco (UTC -7 hours),

10 a.m. EDT New York (UTC-4 hours)

Join Cisco Expert **Rodrigo Delgado**



Learn basic concepts about Cisco IOS XR Software and have an overview of the Cisco IOS XR Software architecture

Register for this live Webcast @

[http://tools.cisco.com/gems/cust/customerQA.do?
METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S186
84&PRIORITY_CODE](http://tools.cisco.com/gems/cust/customerQA.do?METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S18684&PRIORITY_CODE)

Ask the Expert Events – English

Current



Topic: RF Gateway 1 (RFGW1)

Join Cisco Expert: **Ron Hanson**

Learn and ask questions about all aspects of the RF Gateway 1 (RFGW1) including Installation, operation, configuration, and troubleshooting.



Topic: Cisco Cloud Web Security – Transparent Solution

Join Cisco Expert: **Jennifer Halim**

Learn and ask questions regarding true transparent experience with Cisco Cloud Web Security using your existing Cisco devices (WSA Connector, ASA Connector, ISRG2 Connector).

Join the discussion for these Ask The Expert Events at:

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

Check out CiscoLive365.com

Watch over 600 sessions from Cisco Live Orlando, download PDFs, visit partners, and more!

The screenshot shows the Cisco Live 365 website interface. At the top right, there are links for "Cisco Live", "Live Support", "Help", and "Login". The main navigation bar includes "Session Catalog", "Agenda", "Social Networking", "Solutions Center", and "Prize Center", along with a search bar labeled "Search Catalog".

The main content area is split into two columns. The left column features a "Welcome" heading, social media icons for Facebook, Twitter, LinkedIn, Google+, and Email, and a login section. The login section includes the text "Log in to access thousands of sessions on cloud, BYOD, data center, and more!", an input field for "Email or Username", an input field for "Password", a "Forgot Your Username or Password?" link, and a green "Login" button. Below the login section is a "Not a Member?" section with the text "Join now to access free content from global Cisco Live conferences." and a green "Register Now" button.

The right column features a large image of John Chambers, the CEO of Cisco. To the right of the image, the text reads "Watch the Cisco Live Orlando Keynote With John Chambers". Below the image is a "View Now" button with a right-pointing arrow and four small square icons.

At the bottom of the page, there is a "Live Events" section with a sub-section for "Orlando 2013". Below this, there is a text box that says "View the agenda for the extended agenda and more information about each session." and a "Broadcast and Twitter Chat" button.

We have communities in other languages

If you speak **Spanish, Portuguese, Japanese, Polish or Russian**, we invite you to ask your questions and collaborate in your language:

- **Spanish** → <https://supportforums.cisco.com/community/spanish>
- **Portuguese** → <https://supportforums.cisco.com/community/portuguese>
- **Japanese** → <https://supportforums.cisco.com/community/csc-japan>
- **Polish** → <https://supportforums.cisco.com/community/etc/netpro-polska>
- **Russian** → <https://supportforums.cisco.com/community/russian>

We invite you to actively collaborate in the Cisco Support Community and social media

<https://supportforums.cisco.com>



<http://www.facebook.com/CiscoSupportCommunity>



http://twitter.com/#!/cisco_support



<http://www.youtube.com/user/ciscosupportchannel>



<https://plus.google.com/110418616513822966153?prsrc=3#110418616513822966153/posts>



<http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8>



https://play.google.com/store/apps/details?id=com.cisco.swtg_android



<http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019>



Newsletter Subscription: https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES

Trivia Answer

- **How is Cisco Adaptive Security Appliance (ASA) making your new car safer?**
 - a) Cisco ASA is part of the infrastructure for NCCAR an organization that assist in the testing of safety of new cars
 - b) Cisco ASA is part of the NASCAR circuit
 - c) Cisco ASA came out in 2004 as part of a national safety initiative for new cars

Thank You for
Your Time



Please Take a Moment to Complete the Evaluation