TOMORROW starts here.

11 11 11 CISCO



Cisco Security Management

BRKSEC-2060

Sanjay Agarwal Product Line Manager Security Management





© 2014 Cisco and/or its affiliates. All rights reserved.

What is not Covered

- Prime Infrastructure
- Cisco VNC
- Cisco ISE
- Cisco Meraki
- Cisco ScanSafe
- Cisco WAS



Current Security Management Portfolio



Cisco Security Management Portfolio



© 2014 Cisco and/or its affiliates. All rights reserved.

CSM Operational Use Case Medium and Large Enterprise

- CSM for enterprise deployments
- Customers looking to manage complete ASA management
- Customers looking for Enterprise class features:
 - Security Dashboard and Health Status
 - Large Complex Policy Management
 - Policy Approval
 - Policy Sharing and Validation
 - Device Configuration
 - Visibility and Events
 - Upgrades and Alerts



CSM in Action Security Admin

Day in the life of Security Administrator





@ Office

Day in the life of Security Administrator

8 AM 9 AM 11 AM 12 PM Lunch 3 PM 5 PM 9 PM 12 AM

Quick Security Dashboard and health view

Challenges

- Did the changes I made yesterday create any problem? Is there anything wrong?
- Is there a possibility of a threat, which I should address immediately?
- What configuration tasks do I need to perform to address my issues?
- Did CSM backup go through successfully last night?



CSM Solution

CSM Dashboard

Your starting point to perform detailed check

- 360 degree view of what's happening on your network
- Cross launches any CSM application at a click of a button
- Personalise only see what you want to see about your network
- Easy drill down capability to start and investigate security problems

gCisco Security Manager - Dashboard - rakesh Connected to '10	.142.52.123'			User: rakesh Server: 10.142.52
cisco Security Manager		🍄 Configuration Manager 🚑 Event Viewer	🍯 Health and Performance Monito	r 🛛 🍓 Image Manager 🗧 🌆 Report Mana
Summary × Health and Performance				📑 🧮 Show Gadgets
Device Health Summary Last updated on Jun	-11, 03:03 PM Top Signatures	Last updated on Jun-11, 02:24 PM	Top Malware Sites	Last updated on Jun-11, 02:24 P
Group by Category - 🔍 Type to Search	🗉 🖨 Signatures	Last 24 Hours 👻	IP Address	Last 24 Hours
🖏 Device Down	0 Back Door PC Invader	(9445.1) 72.88 K	malware.com (192.20.20.20)	501.92
🗰 Interface Down	3 IPv6 Options Padding Too Long	(1716.0) 61.7 K	malware.com (172.30.30.30)	501.92
😡 Overall Device Health	6 Back Door PC Invader	(9445.2) 61.65 K		
😭 High CPU Utilization	0 TCP Drop - Bad SACK Allow	(1330.8) 50 K		
High Memory Utilization	2 Invalid IPv6 Header Flow Label Field	(1707.0) 47.77.K		
LIPS - High Inspection Load	2	View more		
Level IPS - High Missed Packets	1 Top Attackers	Last undated on 3 in-11 07-24 PM	Ton Sources	Last undated on 3 in-11 07-24
🔔 IPS - Bypass Mode	2 Attackers	Last 24 Hours V	Sources	Last 24 Hours
	20.20.20.2	20.00 K	102 20 20 20	752
	20 20 20 1	69.62 K	152.20.20.20	102.
	10 10 10 1	59.38 K		
	10.10.10.100	57.9 K		
	20.20.20.2	55.66 K		
		View more		
P Intelligence	Top Victims	Last updated on Jun-11, 02:24 PM	Top Destinations	Last updated on Jun-11, 02:24
Enter IPv4 Address	Victims	Last 24 Hours 👻	Destinations	Last 24 Hours
	3.3.3.1	80.75 K	172.30.30.30	752.9
	3.3.3.8	58.49 K		
	2.2.2.2	57.9 K		
	2.2.2.1	56.42 K		
	3.3.3.2	55.66 K		
		View more		
p Infected Hosts Last updated on Jun	-11, 02:24 PM IPS License		Deployment	
fected Hosts Last	24 Hours • Q Type to Search		C Type to Search	
192.20.20.20(Inside)	501.92 K 🗉 🌍 10.106.135.62	😣 Expired	admin_job_2013-06-11 08:4	19:05.656 🥝
	€ 🧐 10.142.52.199	🙁 Expired		
	H 🗐 10.77.208.139	🔞 Expired		
	⊞ 🧐 10.106.160.103	😣 Expired		



Landing Page

Cisco Security Manager - Dashboard - rakesh Connected to '10.142.52.12

Device HPM

Cross Launches

Create Dashboard

Image: Control of the con		aer				User: rakesh Server: 10.142.52		
Senser Sensenser Senser Senser <th>cisco</th> <th></th> <th>🛛 🍑 Config</th> <th>uration Manager 🍓 Event Viewer</th> <th> 🖝 Health and Performance Monitor</th> <th> 🝓 Image Manage 🖓eport Manager</th> <th></th> <th></th>	cisco		🛛 🍑 Config	uration Manager 🍓 Event Viewer	🖝 Health and Performance Monitor	🝓 Image Manage 🖓eport Manager		
Device the difference with the second of the seco	Summary × Health and Performance					📅 😹 Show Gadgets 🧉	-	
Group Volume Impairs Sector Signation Lots 2 Hours Impairs Control Sector Impa	Device Health Summary	Last updated on Jun-11, 03:03 PM	Top Signatures	Last updated on Jun-11, 02:24 PM	Top Malware Sites	Last updated on Jun-11, 02:24 PM		
Implementation Implementation Implementation Imple	Group by Category - 🔍 Type to Sea	arch 🗈 🖻	Signatures	Last 24 Hours 👻	IP Address	Last 24 Hours 👻		
I model and a construction boown Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digetons besing The Long (1716.9) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Second (172.8) 9.15K I work for CPU Unitation Pet digeton the Se	🖏 Devic 🚬 …n	0	Back Door PC Invader (9445.1)	72.88 K	malware.com (192.20.20.20)	501.92 K		
Image: Control Device Headth	🗉 🔚 Interface Down	3	IPv6 Options Padding Too Long (1716.0)	61.7 K	malware.com (172.30.30.30)	501.92 K		
Import CPU Utilization 0 Import High Hender Utilization 2 Import High Hender He	🗉 🔬 Overall Device Health	6	Back Door PC Invader (9445.2)	61.65 K				
Differ High Monory Ultration Diffe	High CPU Utilization	0	TCP Drop - Bad SACK Allow (1330.8)	<u>50 K</u>				
IP S- High Hispectol Load Image:	🗉 🗮 High Memory Utilization	2	Invalid IPv6 Header Flow Label Field (1707.0)	47.77.K				
Image: Big : High Hillsond Packets 1 Image: Big : High Hillsond Packets 2 Image: Big : High Hillsond Packets 2 Image: Big : High Hillsond Packets 1 Image: Big : High Hillsond Packets 2 Image: Big :	🗉 🔔 IPS - High Inspection Load			View more				
a) PS - Bypass Mode 2 b) Lackors Lackors Lackors Lackors Strengen Lackors Lackors Lackors Lackors Lackors Lackors Lackors Lackors </th <th>🗉 🔔 IPS - High Missed Packets</th> <th>1</th> <th>Top a skers</th> <th>Last updated on Jun-11, 02-24 PM</th> <th>Top Sources</th> <th>Last updated on Jun-11, 02:24 PM</th> <th></th> <th></th>	🗉 🔔 IPS - High Missed Packets	1	Top a skers	Last updated on Jun-11, 02-24 PM	Top Sources	Last updated on Jun-11, 02:24 PM		
Image: construction of the start of the	🗉 🔔 IPS - Bypass Mode	2	Attackers	Last 24 Hours *	Sources	Last 24 Hours		
10 Interdependent losts 10 Vectors Last updated on June 11, 02240 100 Vectors 100 Vectors <th></th> <th></th> <th></th> <th></th> <th></th> <th>770.0 //</th> <th></th> <th></th>						770.0 //		
in the Boy A defined in Sum-11, 0224PR in the Boy A defined in Sum-11, 0224PR infected Hosts tast updated on Sum-11, 0224PR infected Host infected Host infected Host infected			20.20.20.3	89.06 K	192.20.20.20	752.9 K		
1000000000000000000000000000000000000			10 10 10 1	59.38 K				
12 Intelligence Top Victims Last updated on Jun 11, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Line Componential PV-4 Address Top Line Componential PV-4 Address Destinations Last updated on Jun 12, 0224PRI State PV-4 Address Top Line Componential PV-4 Address Destinations			10.10.100	57.9 K				
Image: Construction of the series			20.20.20.2					
Image: Depintence Top Victims Last updated on 3un-11, 0224PM Victims Last 20 Hours Top Destinations Last 20 Hours A3.3.1 98.75K 172.39.39.20 752.9K A3.3.2 98.75K 172.39.39.20 752.9K A3.3.3.2 98.75K 172.39.39.20 752.9K Destinations Last 20 Hours Device Health Summary View more View more Device Health Summary Top Infected Hosts Last 24 Hours FS Locense Group by Category 192.20.20 20(Inside) S01.9K 91.0106.135.62 Expired Group by Category Group by Category Group by Category Group by Category Group by Category 192.20 20 20(Inside) S01.9K 91.0106.160.103 Expired Fspired Fspired B admin_job_2013.06.110 Bit49:05.656 Group by Category Group by Category Group by Category Group by Device B admin_job_2013.06.110 Bit49:05.656 Fspired Fspired Fspired Fspired B admin_job_2013.06.110 Bit49:05.656 Group by Category Group by Device Group by Device Group by Device Group				View more				
Interfact of the first interfact of the sector Interfact of the sector Interfact of the sector	TP Intelligence		Ton Victims	Last undated on Jun-11, 02:24 PM	 Top Destinations	Last updated on Jun-11, 02:24 PM		
122.02.02.0(nside) 501.927 192.20.20.20(nside) 501.927 101.06.166.0.103 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.013 101.061.060.01	C Enter IPv4 Address		Victims	Last 24 Hours 👻	Destinations	Last 24 Hours 👻		
1333.8. 184.4 <			3.3.3.1	80.75 K	172.30.30.30	752.9 K		
192 20 20 (Inside) 501,224 Statuped to Lot 10,212,494 Statuped to Lot 10,212,494 Statuped to Lot 10,212,494 Image: Statuped to			3.3.3.8	58.49 K				
Image: State of the state			2.2.2.2	57.9 K			1	
Infected Hosts Last updated on Jun-11, 02:24 PM Infected Hosts Deployment Group by Category 192.20.20.20(Inside) 501:92K © 10.104.135.62 © Expired © Type to Search © Group by Category Group by Category 192.20.20.20(Inside) 501:92K © 10.104.135.62 © Expired © Group by Category Group by Category 192.20.20.20(Inside) © 10.104.135.62 © Expired © Group by Category Group by Category 192.20.20.20(Inside) © 10.104.135.62 © Expired © Group by Category Group by Category 192.20.20.20(Inside) © 10.104.135.62 © Expired © Group by Category Group by Category Group by Device			2.2.2.1	56.42 K				
Infected Hosts Last updated on Jun-11, 02:24PW IPS License Deployment Group by Category 192.20.20.20(Inside) 501.92 K © 10.106.135.62 © Expired © Type to Search © Type to Search © Group by Category 192.20.20.20(Inside) 501.92 K © 10.106.135.62 © Expired © Group by Category 192.20.20.20(Inside) 501.92 K © 10.106.103 © Expired © Group by Category 192.20.20.20(Inside) 501.92 K © 10.106.103 © Expired © Group by Category			3.3.3.2	55.66 K				_
Top Infected Hosts Last updated on Jun-11, 02:24PM PS License Deployment Group by Category Infected Hosts Last 24 Hours Type to Search Type to Search Type to Search Group by Category Group by Category 192.20.20.20(Inside) 501.92 K S01.02 K S01.02 K S01.02 K S01.02 K Group by Category Group by Category 192.20.20.20(Inside) 10.106.103 Expired Group by Category Group by Category 192.20.20.20(Inside) 10.106.103 Expired Group by Category Group by Category Group by Device Group by Technology Group by Technology Group by Technology				View more		Devie	te Health Summa	ry
Infected Hoats Last 24 Hours Type to Search Type to Search Type to Search Group by Alert 192.20.20.20(Inside) 19.10.106.135.62 Expired admin_job_2013-06-11.08:49:05.656 Group by Category 19.20.20.20(Inside) 10.106.103 Expired Group by Category Group by Device 19.20.20.20(Inside) 10.106.103 Expired Group by Category Group by Device	Top Infected Hosts	Last updated on Jun-11, 02:24 PM	IPS License		Deployment	Group	by Category	-
192.20.20 (Inside) 501.92 K 9 10.106.135.62 Sepired 9 10.102.52.199 Sepired 9 10.102.6130 Sepired 9 10.106.103 Sepired 9 10.106.103 Sepired 9 10.106.103 Sepired 9 10.106.100 Sepired 9 10.106	Infected Hosts	Last 24 Hours 👻	C Type to Search		C Type to Search		Complex Mark	
	192.20.20.20(Inside)	501.92 K		🔕 Expired	admin_job_2013-06-11 08:49	:05.656	Group by Alert	
			10.142.52.199	😣 Expired		~	Group by Category	
B @ 10.106.160.103 C Expired Group by Device Group by Technology Group by Technology				Expired			Group by Device	
Group by Technology			⊞	😣 Expired			Group by Device	
							Group by Technolog	JУ
		-						15-

Landing Page - Gadgets



Landing Page – Details

	User: rakesh Server: 1	0.142.52.123
cisco Security Manager	🚱 Configuration Manager 🦺 Event Viewer 🐻 Health and Performance Monitor 🝓 Image Manager 🏭 Re	port Manager
Summary × Health and Performance	📰 🐹 Show	Gadgets 🧃
Device Health Summary		◇ ⊕ ×
Group by Category		
🗞 Device Down		0
🗆 🥅 Interface Down		3
S 10.106.160.53		
Interface 'outside': Protocol Down (Protocol: down, Status: down)		
First Seen: Jun-10, 12:18 PM	Last Seen: Jun-11, 11:43 AM	1
Severity: Critical	State: Active	
Acknowledged By: None		
Cleared By: None		
SP 10,106.161.200		
Interface 'inside': Protocol Down (Protocol: down, Status: down)		
First Seen: Jun-10, 12:18 PM	Last Seen: Jun-11, 11:43 AM	1
Severity: Critical	State: Active	_
Acknowledged By: None		
Uleared By: None		
SP 10.77.208.171		
Interface 'Test': Protocol Down (Protocol: down, Status: down)		
First Seen: Jun-10, 12:18 PM	Last Seen: Jun-11, 11:43 AM	1
Severity: Critical	State: Active	_
Acknowledged By: None		
Lleared By: None		
		6
😭 High CPU Utilization		0
🗉 🗱 High Memory Utilization		2
🗉 🔔 IPS - High Inspection Load		2
🗉 🔔 IPS - High Missed Packets		1
🗉 🔔 IPS - Bypass Mode		2



Device Health Summary

Device Health Summary	La	st updated on Jan-02, 0	1:44 PM IST		
Group by Category 🔹 👻	🔍 Type to Searc	:h			
🗉 🔌 Device Not Reachable	e		2		
🗉 🐺 Interface Down			7		
🗉 🔬 Overall Device Health	Alerts		4		
🎟 High Memory Utilizati	on		0		
🕅 Firewall - High CPU U	🔔 Alert			8	
IPS - High Inspection	🌍 ips-nyk 🔞 Missed Packets a	re 7%			
🗉 🍈 IPS - High Missed Pac	First Seen: Dec-16, 11:3	6 AM IST			
() ips-nyk	Severity: Critical Acknowledged By: None	街 Device Summary			8
Missed Packets are 7	Acknowledge Comment	🎯 ips-nyk		🔌 Conn	ected
Severity: Critical Acknowledged By: None Cleared By: None	Clear Comments: Add Notes:	Cisco IPS 4260 Sensor (IPS) Target OS Version: 7.0 Running OS Version: 7.0(1)E4 Address: 192.168.135.3 Ovmer: Report Card Connected Connected Device Health Inspection Load Simissed Packets IPS in Bypass Mode Commory Usage Last Deployment: Unknow) S574∨1.4 n		View Health Summary View Events
		License expires in 570 da	ys #IST		View Image Manager
		Last updated, Jan-02, 01:46 Ph	01101		🙁 Close
					-

- Brings HPM Alerts information to Dashboard
- Can group Alerts by Category, Alert-Type, Device and Technology
- Add comments, Acknowledge or Clear Alert
- View Device Summary



© 2014 Cisco and/or its affiliates. All rights reserved.

HPM All Device View & Details



@ Office

Day in the life of Security Administrator

8 AM 12 PM Lunch 3 PM 5 PM 9 AM 11 AM Challenges Change **Request &** What needs to change in the network? ٠ **Security Policy** Who needs to approve?

> Will it create any problem?

How can it be deployed?



Review

Why is this change required?

9 PM

12AM

Cisco

CSM Solution

CSM Configuration Manager

Unified Security Policy & Change Management

- Device Discovery and modelling
- Policy Management and validation
- Policy sharing and bundling
- Policy approval workflow
- Policy Object and Services

💐 Cisco Security Manager - Configu	ration Manage	er - admin (Connected	l to 'madagasca	r-beta'									_ 0 >
File Edit View Policy Map Mar	nage Tools L	aunch He	0											halle
Bevice 🔀 Map 🗊 Policy 🖴 Po	licy Bundle 🛛 🥥) 🌮 🗟	🕄 🐴	2 🗶 🖪	💐 🔯 🛅	🖲 🍓 🍓 🚳 I	0				Q Search Al	Categories	•	(ISCO)
Devices 🔮 👻	Device: asa-l Policy Assigne	live d: <u> local -</u>	_			Policy: Access Rule Assigned To: local of	es (Unified) levice			Inherits From: -	none			
Filter : none 💌	☆ Filter: (r	none)												BB
Department	Permit				▼ is		•				v	Apply	Cle	ar
			1		Sources		1		Destinations					
ASA-cluster	NO.	Permit	1	Network	Security Grou	up User		Networ	rk	Security Group	- Service	HitCount		Ŷ
asa-duster-1	🛕 🗉 🗐 La	ocal (18 Rule	:)											_
asa-live		V	10.0.	0.0/255.0.248.0	no tags -	no user	📑 All-Ac	dresses		no tags	tcp/old	0	Never	
asa-multi-live		V	📑 All-Ac	idresses	no tags -	no user	📑 All-Ac	dresses		no tags	tcp/old/1-65535	0	Never	
- 🖃 asa-multi-live_admin	B 3	V	All-Ac	idresses	no tags -	no user	📑 All-Ac	dresses		no tags	🧊 try	0	Never	
	8 4	V	All-Ac	idresses	no tags -	no user	📑 All-Ac	dresses		no tags	क्रि try1	0	Never	
asa-mult-live_CIX2	B 5	v	4.5.6	.9	no tags -	no user	📑 All-Ac	dresses		no tags	🗩 ТСР	0	Never	
asa-trans	6	v	Al-Ac	idresses	no tags -	no user	9.9.9	.9		no tags	🗩 UDP	0	Never	
	@ 7	V	8.9.7	.8	no tags -	no user	📑 All-Ac	dresses		no tags	👮 ТСР	0	Never	
(S) ips-nyk	@ 8	v	8.9.7	.8	no tags -	no user	5.5.5	.5		no tags	🗩 TCP	0	Never	- 1
indiciosa	a 9	V	Al-Ac	dresses	no tags -	no user	10.3.	4.5		no tags	TCP	0	Never	
	10	1	Al-Ac	Idresses	no taos -	no user	10.5.	6.7		no tags	D ICMP	0	Never	
Policies											A	^		<u>الا</u> لح
😑 Firewall					-1						1 limi			
AAA Rules (Unified)	Enable co	onflict detecti	on _	Generate Report	t					Refresh Hit Count	Query #1	$\uparrow \forall$	#	1
Inspection Rules (Unified)	(1) ASA 8.3 or	nwards the d	evice uses F	Real IP(pre-natted	IP) in firewall ruk	es.Use Real IP address	25.							
Botnet Traffic Filter Rules														Save
⊕-Settings	Policy Object	Manager												đΧ
Web Filter Rules	4 🛨 Favor	ites		📑 Networks	/Hosts 🛛 🗹	Referenced 🔍 🖪	🖻 😹 🕜							
	a Id	ientity User (roup	× Filter: (non	e)						Q+ Type	to Search		
		etworks/Hosl	s	*	Name 🔨	Conte	nt	Туре	Category	Overrides		Description		
Per-Session NAT Rules	20 Se	ecurity Group		1		1.1.2.3	ŀ	lost		1				*
H-Remote Access VPN	🖉 🦻 Se	ervices		2		2.2.2.2	ł	lost		1				
🗐 Interfaces				4.3.2.1		6.6.66.6	ł	lost		×				
Identity Options	A Recent	t Objects		4.3.2.1har	rsha	4.3.2.1	1	lost		1				
-TrustSec		YINDEC		4001::1		4001::1	ł	lost		~				
SXP Connection Peers	🕨 þ 📷 All Ob	ject Types		4011::1		22::22	ł	lost		1				
🗄 Platform				4011::1_e	qfjqwhfrhqj :	22::22	1	lost		1				
FlexConfigs				A-10.105.	191.70	10.105.191.70	(Group		1				
				A-10.109.6	50.192	10.109.60.192	(Group		1				_
				4										<u> </u>
				Displaying: 155	0 of 1550 object	ts							÷ /	2
< >														



Docked Policy Object Manager

(;	3. Launo	ch													
	Po	olicy Ob	ject	evice: ny-asa olicy Assigned:	local			Policy: Assign	Access Rules ed To: local device			Inherits From:	none			
Cisco Security Manager -		Manage	er	E Filter: (no	ne)											
File Edit View Policy Map	Mana	age Tools	н	No.	Permit	S	ource	User	Destination	Se	rvice	Interface	Dir.	Options	Category	
	C Dolic		20 3		al (23 Rule:	s)										<u> </u>
		y banaic	G- 0	1	0	en any		THREAT DLABS (MKtg	DataCenter-1	₩ IP		Giobal in	1		None	
Dev	合	Device: ny-asa		2	0	any		THREAT DLABS \\MKtg	DataCenter-2			Global in	1		None	
1. Select		Policy Assigned:	: local	3	0	any		THREATDLABS\WKtg	DataCenter-3	AI 🕰		Global in	1		None	
				4	0	any		THREATDLABS\\Mktg	CSM-Server	P IP		Global in	1		None	
NY-ASA		+ Filter: (n	one)	5	0	any any		THREATDLABS\\Br	DataCenter-1	₩ IP		Global in	1		None	
		No.	Permi	6	0	any any		THREATDLABS\\Br	DataCenter-2	₩ IP		Global in	1		None	▼
-ins		□ <u></u> [Lo	cal (23 Ri													
		1	0	🔽 Enable Aut	Conflict D	etection	Generate Re	eport		licy O	hiert		Stoo 🎇	ls 🔻 🥱		
ny-asa-ssm		2	0	†ASA 8.3 onw	ards the de	evice uses Re	al IP(pre-natted IP) in firewall rules.Use R			Dject					
sf-asa		3	0						Manac	aer is c	locke	d				Save
			0	Policy Object Ma	nager						- D -					а
		4		A 🔶 Favorites			- Port Lists	Referenced	below	Acces	is ku	e				
		5	0	Ag Iden	ity User Gr	roup	+ Filter: (none	-)						Q- Type to	Search	
Delision		6		V ⁶ Netw	orks/Hosts	TPv6	Name		Content	Category	Overrides		Descriptio	on		Last Ti
Policies		7	0	-C Port	Lists	4	£50554	50554			×	Shared License Port				
- Firewall		8	0	🔗 Servi	ces	q	ALLPORTS	0-65535			×					
AAA Rules		0	0	Recent O	hiecto	4	EDefault Range	1-65535			×	Default/Any Port Range	2			
Access Rules		, ,		- Gracento	bjeeta	4	EHTTPS	443			×	HTTPS Port				
Access Rules		10		👂 👌 All Object	Types	4	EWEBPORTS	3128,443,80,800	0,8080		2	WEBPORTS				
2 Salact			~													
Z. Select																
Access							c]									Þ
, 190000							Displaying: 5 of 5	objects							÷	1 🗎
				ĮI.												



ACL Hit Count

Cisco Security Manager - admin connected to "172.25	.80.215"					
File Edit View Policy Map Tools Help						
💱 💋 🗊 💽 🎓 💽 🗟 🖓 🤗						
Hit Count Query Results		Rule	HitCount			_
Info		Local - Default 1	1318			
Salach Davies: Cataluck#200 [sc] Defeats Mt Count		Local - Deradic_1	1310	App	ly Remo	/e
Select Device: Calarystocol V		Local - Default_2	215	Service	Dir. I	nte
Selected Access Rules Pula Hit/Gunt Permit Source Dectination Ser	ic Interface Dir	Land Defeult 0	245	tcp/8877	IN	
Local - Default_1 1318 V M any M any State	P-Dat outside in	Local - Derault_3	215			_
Local - Default_2 215 🗸 📲 👘 any 🍠 IPS	ec-AH outside in	Default/300 None	10.2.2.2	tcp/1720	in	out
Local - Default_3 215 V Bany Buny 27 IPS	ec-ESP in	Default/300 None	E Test2	tcp/Web_Service	in	out
			10.1.1.100	tcp/80	in	out
			📑 any	🔛 ICMP-Echo-Reply	in	out
			📑 any	🤝 Zorgan	in	out
Thoose: Expand			📑 any	udp/138	in	out
			10.5.3.4	tcp/22	in	out
Rule Hit Count Permit Service Interfaces Direction	Source Addre Source Port Dest Addr	esses Destination Port ACL Name	any 📑	udp/53	in	out
Local - Defaul 0 🖌 🎓 gre 🕞 outside in 👔	🛱 0.0.0.0/0 🌆 0.0.0.	0/0 acl_mdc_outs	any 📑	tcp/53	in	out
			Aue 🚎	(te\$+\$9	/m//////	oùt
			📑 any	tcp/443	in	out
		OK	any 📑	tcp/139	in	out =
E Settings			10.2.2.0/24	tcp/21	in	out
E NAT	.4 🚫 None	Test2	10.2.2.0/24	tcp/23	in	out
	.5 🖌 None	Test2	10.2.2.0/24	tcp/80	in	out
∫ FlexConfigs	.6 🖌 None	ing any	E Test	IPSec.prot.prot	in	out
	7 🗸 None	any	Test	udp/IPSec.udp.udp	in	out
	.8 🗸 None	ee any	10.2.3.0/24	tcp/Web_Service	in	out
			Query			
						Save

Check if an access rule is encountering hits on live device



© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Drag-and-drop Objects to Policy

+ Filt	ter: (nor	ne)									
	No.	Permit	Source	User		Destination	Service	Interfac	e Dir.	Options	Category
	10	0	📑 any	THREATDLABS	\\Engg 🧕	DataCenter-2	→ IP	🜐 Global	in		None 🔺
	11	0	📑 any	THREATDLABS	\\Engg	DataCenter-3	→ IP	🜐 Global	in		None
	12	0	📑 any	THREATDLABS	\\Engg 📮	CSM-Server	→ IP	🌐 Global	in		None
	13	0	📑 any	no user		7.7.7	€ IP	🌐 Global	in		None
®	14	~	📑 any	THREATDLABS	\\Sales	8.8 8.8	→ IP	🌐 Global	in		None
©'	15	*	👺 Engineering_Net	THREATDLABS	\\Engg _	FataCenter-1	🗭 IP	🕞 Global	in		None
©	16	~	🚜 Engineering_Net	THREATDLABS	\\Engg 🛓	DataCenter-2	⇒ IP	(🖶 Global	in		None
<pre> • • • • • • • • • • • • • • • • • • •</pre>	Enable Autr	o Conflict E eards the de nager s	etection Gener	ate Report	s.Use Rep 1P addr 2. ok	bject to a			Tools		► C C C C C C C C C C C C C C C C C C C
eci ork	Enable Auto	o Conflict E ards the de nager s tity User G vorks/Hosts	etection Gener	ate Report tted IP) in firewall rules rks/Hosts rone)	S.Use Real TP addr 2. Ok	^{esses.} Drag an oject to a rule's		[Tools	Search	Save
<pre> • • • • • • • • • • • • • • • • • • •</pre>	mable Auto	o Conflict E ards the de nager s tity User G vorks/Hosts vorks/Hosts	etection Gener evice uses Real IP(pre-nat oup IPv6 IB Filter: (r IBany	ate Report tted IP) in firewall rules rks/Hosts none) Vahie 0.0.0.0	S.Use Real TP addr 2. Ok	esses. Drag an oject to a rule's stination	Category	Overrides Refer	enced	Type to Search efined any network	Description
ect ork	inable Autr A 8 3 onw rites Ident Netw CE Port I Servi	o Conflict E ards the de nager s tity User G vorks/Hosts Lists Lists ices	etection Gener evice uses Real IP(pre-nat oup IPv6 I Filter: (r IPv6	ate Report tted IP) in firewall rules rks/Hosts none –) Nafriè 0.0.0.0 ownloads.c.m megad	s.Use Real IP addr 2. ok feer ok 0/0 fowrloads.com	esses. Drag an oject to a rule's stination Group	Category	Overrides Refer ×	enced	Type to Search	E P C C
ectork	inable Auto t Man rites Iden V Netw -CE Port I	o Conflict E ards the de nager s tity User G tity User G vorks/Hosts Lists ices	etection Gener	ate Report tted IP) in firewall rules rks/Hosts none) Nathie 0.0.0.0 ownloads.c.m megad	s. Use Real TP addr 2. Ok offer 0/0 coverloads.com	esses. Drag an oject to a rule's stination Group FQDN FQDN	Category	Overrides Refer × (× (enced	Type to Search efined any network	Description
eci ork ts	inable Auto Mar Intes Identive Via Network CE Port I Recent O	o Conflict D ards the de nager s tity User G vorks/Hosts vorks/Hosts Lists ices	etection Gener evice uses Real IP(pre-nat oup IPv6	ate Report tted IP) in firewall rules rks/Hosts none) Nahie 0.0.0.0 ownloads.com megad www.a www.a	s. Use Real TP addr 2. Ok offer 0/0 formioads.com apple.com cisco.com	esses. Drag an oject to a rule's stination Group FQDN FQDN FQDN	Category	Overrides Refer × (× (× (enced	Type to Search efined any network	Description
eci ork ts	inable Auto A & 3 onw t Man Netw Servi Recent O All Object	o Conflict D mager s tity User G vorks/Hosts vorks/Hosts Lists lices bjects t Types	etection Gener	ate Report tted IP) in firewall rules rks/Hosts none) Naĥić 0.0.0.0 ownloads.c.m megad www.a www.a	s. Use Real TP addr 2. Ok offer 0/0 cownloads.com apple.com cisco.com erver.threatdlabs.	esses. Drag an oject to a rule's stination Group FQDN FQDN FQDN FQDN FQDN	Category	Overrides Refer × (× (× (× (× (enced Prede	Type to Search efined any network	Description
ectork	inable Auto A & 3 onw t Main Netw B Netw Porti Recent O All Object	o Conflict D mager s tity User G works/Hosts works/Hosts ices ices torks/Hosts trypes	etection Gener evice uses Real IP(pre-nat oup IPv6	ate Report tted IP) in firewall rules rks/Hosts one) Naĥie 0.0.0.0 ownloads.c.m megad www.a www.a csm-se -1 10.10.	s. Use Real TP addr 2. Ok ferr 0k 0/0 comloads.com apple.com cisco.com erver.threatdlabs. 10.0/24	esses. Drag an oject to a rule's stination Group FQDN FQDN FQDN FQDN Ktest FQDN Networ	Category	Overrides Refer X (X (X (X (L ())	enced Controls	Type to Search efined any network	Description
eci ork ts	inable Auto A & 3 onw t Marites Metwork Porti Recent O All Object	o Conflict D mager s tity User G works/Hosts works/Hosts Lists lices bjects t Types	etection Gener evice uses Real IP(pre-nat oup IPv6 € Filter: (r gany Cisco.com CSM-Server @DataCenter @DataCenter	ate Report tted IP) in firewall rules rks/Hosts one) Naĥie 0.0.0.0 ownloads.c.m megad www.a www.a csm-se -1 10.10. -2 172.16	s. Use Real TP addr 2. Ok offer 0/0 comioads.com apple.com cisco.com erver.threatdlabs. 10.0/24 5.10.0/24	esses. Drag an oject to a rule's stination Group FQDN FQDN FQDN FQDN test FQDN Networ Networ	Category	Overrides Refer X (X (X (L (L (L (C (C (C (C (C (C (C (C	enced Prede	Q+ Type to Search	Description

BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Policy Sharing and Inheritance



- Take any device policy/setting and save it for sharing
- Shared policies can be assigned to multiple devices

BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Ciscolin

Global Objects Search & Find-Usage

ration Manager - admin Connecte	d to '172 16 1 10'						
age Tools Launch Help							
icy Bundle 💽 🐎 🗟 🗟 🕰	0 0 4	ũ 🛛 🖓				ataCenter-1	CISCO.
Device: ny-asa Policy Assigned: <u> local</u>		Policy: Access Rules Assigned To: local device		(1. Search for	:	
Filter: (none)					DataContor_		71
No. Permit	Global Search				DataCenter		ategory
🗆 🗾 Local (23 Rules)	Search All Categories	DataCenter-1				Search	û
1 🛇 🖷 any	⁹ 5 results found for DataCent	er-1 in All Categories (0.22 se	conds)			0	lone
2 🛇 📑 any	Click on any of the categories list	ed below to view the search result	7				lone
3 🚫 🖷 any	Results	🖻 😓					lone
⁴ 2 Select	Policies	Filter: (none)					lone
5 2. 00.000	Policy Objects	Scope Rule	Permit	Source	User	Destination	lone
	Networks/Hosts (1)	💭 ny-asa - Local 1	0	📑 any	THREATDLABS\\Mktg	DataCenter-1	lone
		😪 ny-asa - Local 5	0	any	THREATDLABS\\Branch	DataCenter-1	
Enable Auto Conflict Detection		📯 ny-asa - Local 9	0	any any	THREATDLABS\\Engg	DataCenter-1	
†ASA 8.3 onwards the device uses	8	Signation in the second	×	🐝 Engineering	THREATDLABS\\Engg	DataCenter-1	Save
Policy Object Manager	3. Right-click	and					
Favorites	select "Go To'	'. This					
Identity User Group	will show rule	that					
Networks/Hosts-IPv6	will show rule						ription
-CE Port Lists	matches th	nis					
Services	object's us	ano					
腸 Recent Objects	Object 3 us	age					
All Object Types							
		•]	
	Global Search Index Last Updated Displaying: 23 of 23 objects	on 26 Jan 2012 10:18 AM PST					
BRKSEC-2060	© 2014 Cis	co and/or its affiliates. All righ	ts reserved		Cisco Public		

Auto-Conflicts Detection



Create & Manage Policy Bundle

2. Select this to display all shared policies	ration Manager - admin Con Manage Tools Launch Dicy Bundle Delicy Bundle Con Policy Type: All Shared Policies Policy All	Shared Policies	x. isco.
Al Shared Policies	Details Shared Policies Firewall Access Rules Global FW Policy Botnet Traffic Filter Rules Global BTF Policy Global BTF Policy	Type Access Rules Inspection Rules Botnet Traffic Filter Rules	
3. Add new policy bundle	Global IDFW Settings	Identity Options	ave



Assign Policy Bundle to Devices





Policy Bundle Assignment

Cisco Security Manager		nin Conn	ected to '172.16.1.1	.0'			
File Edit View Policy 1.	Select	aunch H	Help				al al a
Device Dev	vice View	3) 🐴 🗖 🔳		?	🔍 Search All Ca	cisco.
Devices	Device: la-asa Policy Assigned: <u>Gl</u> Policy Bundle Assign	lobal FW P ned: ASA I	<u>Policy</u> Policy Bundle	Policy: Access Rules Assigned To: <u>3 Devices</u>	Inheri	ts From: <u> none -</u>	
Department	• Filter: (none	:)		3. Validate			
All	No. Pe	ermit S	Source	Policy Bundle	Destination	Service	Interfa
dc-asa	🗆 河 Global	FW Policy	- Mandatory (21 Ru	io oppigned			
kc-asa	1	× 1	Engineering_Net		🜉 DataCenter-1	穿 IP	I DM
la-asa	2	× 1	Engineering_Net	THREATDLABS\\Engg	🜉 DataCenter-2	穿 IP	🗰 DM 🗉
my-asa	3	\checkmark	Engineering_Net	THREATDLABS\\Engg	💂 DataCenter-3	穿 IP	DM
y-asa-ssm	4	0	📑 any	THREATDLABS\\Mktg	DataCenter-1	🗩 IP	(te) Glo
	5	0	📑 any	THREATDLABS\\Mktg	DataCenter-2	🗩 IP	(te) Glo
Policies	6	0	📑 any	THREATDLABS\\Mktg	DataCenter-3	P IP	(Bo
Firewall	7	0	📑 any	THREATDLABS\\Mktg	CSM-Server	De IP	(Bo
AAA Rules	8	0	📑 any	THREATDLABS\\Branch	👰 DataCenter-1	🗩 IP	🕀 Glo
Access Rules	2 Select					<u> </u>	
Botnet Traffic Filter Ru	assigned policy	t Det devi	tection Ger	nerate Report	P addresses.	Tools 🔻 😽	Save



@ Office

Day in the life of Security Administrator



- How should I submit ticket for approval
- Have I completed all my tickets?



approval

Workflow

What Is It?

 Provides multiphase workflow for deployment with approvals at each stage

Example

- All policy changes need to be approved
- Deployment to the network must be during the change window

Benefit

- Enables teamwork and collaboration between NetOps and SecOps
- Provides scope of control



- Who Can Modify Device Configs?
- Who Can View Changes?
- Who Can Approve Changes?
- Who Can Deploy Changes to Devices?
 Cisco

© 2014 Cisco and/or its affiliates. All rights reserved.

Activity Model

- Robust approval workflow can be turned on or off
- Tied to privileges and rollbased model to enable admin controls through job creation and deployment
- Multiple users can be active at same time, and work in separate "activities"
- Activities can be opened for editing or submission later and deployed

tivity Manager				
Activity	State	Use	r Last Action	
admin_U5.12.U5_14:58:15	Approved	admin	Activity approved	^
admin_05.12.05_15:01:42	Approved	admin	Activity approved	
admin_05.12.05_15:02:46	Approved	admin	Activity approved	
admin_05.12.05_15:04:04	Approved	admin	Activity approved	
admin_05.12.05_15:07:00	Approved	admin	Activity approved	=
admin_05.12.05_15:20:09	Approved	admin	Activity approved	~
Create	Open Close	Validate Submit /	Approve Reject Discard	Refresh
tivity Details Activity History	Workflow			
System				
Device Communication		a		
♦ General	worl	criow Lontrol		
Device Parameters		able Workflow		
Token Management		Require Activity Approval		
Device Groups		Require Deployment Approval		
 Licensing 	Defa	ult Approvers		
Preferences	Activit	y Approval Email: admin@	Pdomain.com	
 Customize Desktop 	Job 0	proval Email:	Delomain com	
 Configuration Archive 	500 A	provarenan. jaaning	paomain.com	
 Deployment 	Worl	dlow History		
 Discovery 	Кеери	Activity for: 30	days Purge Now	
FlexConfig				
♦ Logs	Keep .	Job for: 30	days Purge Now	
◆ Policy				
Policy Management		Save	Recet Restore To Factor	ory Defaults
♦ Workflow				any bordards
 Application Security 				
Take Over User Session				

Cisco Public

Activity Report What Fields Changed: What Objects Changed

Activity Change Report

cisco

User:adminSession started on:13-Nov-2006 13:46:01Current state:Edit OpenReport created on:13-Nov-2006 17:45:30

Devices

🥗 mypix.cisco.com

Access Rule

🗏 Access Rule

Operation	No.	Mandatory	Permit	Source	Destination	Service	Interface	Dir.	Category	Enabled
Add	1	true	permit	any,	any,	HTTP, HTTPS, FTP	All-Interfaces	in	None	true
Add	2	true	deny	any,	any,	IP	All-Interfaces	in	None	true

[©] 10.89.33.138

Device was discovered

Shared Policies

 ■ IPS-IpsEASetting

_IpsEASetting:	10.89.33.138_lpsEASetting_1
5	163454688687 (Added)

Inherits From	None
Affected Devices	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138
New Assignments	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138

IpsEASetting

Operation	Global -deny -timeout
Add	3609

IPS-IpsAnomalyDetection



@ Office

Day in the life of Security Administrator

8 AM	9 AM	11 AM	12 PM	Lunch	3 PM	5 PM	9 PM	12AM	
llongo	•								

Challenges

- Where there any company violations?
- How many changes do I need to submit?
- How should I submit ticket for approval
- Have I completed all my tickets?

Events



CSM Solution

CSM Event Viewer

View and Troubleshoot all Security Events

- Real time event management and troubleshooting
- Cross linkages between events and configurations
- Customisable views for monitoring selected devices
- Admin configured objects can be seen in the events (ASA+IPS)
- Tools such as ping, traceroute, and packet tracer for further troubleshooting

All Device Events X View Settings Search within results: Q - Type have to search Ottak Bestine Time Search View Type Area to be and the time					
View Sections Search within results: Q- Type here to search Otatt Search Within Tesults: Q- Type here to search Otatt					
Search within results: Q- Type here to search 🕥 last					
Bacalua Time Severity W Event Tume To W Event Nam	1 day 🔹 🔛 Save 🔹 🐌 Start 📖 🔅	er dear			
Receive nine Severky Everk rype to Everk nam	e Device 💌	Reputation 💌 Source	Source Service	💌 Destination 💌	Destination 5
6/15/10 1:21:41 AM 1 Informational 302015 # Buik UD	P 💮 A5A-13	10.130.1.1	3 udp/514	10.130.1.30	udp/514
6/15/10 1:21:41 AM 🔒 Informational 302015	P \$\$454-13	10.130.1.1	3 udp/514	10.130.1.31	udp/514
6/15/10 1:21:41 AM 1 Informational 302016 Teardown U	OP @ A5A-13	10.130.1.30	0 udp/514	10.130.1.13	udp/514
6/15/10 1:21:41 AM a Informational 302016 Teardown U	DP SA-13	10.130.1.3	udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM 👔 Informational 302015	P SA5A-13	10.130.1.1	udp/514	10.130.1.30	udp/514
6/15/10 1:19:40 AM 1 Informational 302015 #0 Built UD	P SA5A-13	10.130.1.13	3 udp/514	10.130.1.31	udp/514
6/15/10 1:19:40 AM 4 Informational 302016 Teardown U	DP SA5A-13	10.130.1.3	0 udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM 4 Informational 302016 Teardown U	DP SP 45A-13	10.130.1.3	udp/514	10.130.1.13	udp/514
6/15/10 1:17:39 AM 1 Informational 302010 Connection	USAGE ASA-13				
6/15/10 1:15:43 AM 1 Informational 302015 # Built UD	P \$ 454-13	10.130.1.13	3 udp/514	10.130.1.30	udp/S14
6/15/10 1:15:43 AM 4. Informational 302015 At Built UD	P @ ASA-13	10.130.1.13	3 udp/514	10.130.1.31	udp/514
6/15/10 1:15:43 AM 🕴 Informational 302016 Teardown U	DP 945A-13	10.130.1.30	0 udp/514	10.130.1.13	udp/514
6/15/10 1:15:43 AM 4. Informational 302016 Teardown U	DP SASA-13	10.130.1.3	udp/514	10.130.1.13	udp/514
6/15/10 1:13:41 AM 1 Informational 302015	P SA5A-13	10.130.1.13	3 udp/514	10.130.1.30	udp/514
6/15/10 1:13:41 AM 1 Informational 302015 M Built UD	P SA5A-13	10.130.1.13	3 udp/514	10.130.1.31	udp/514
6/15/10 1:13:41 AM 4 Informational 302016 Teardown U	DP SASA-13	10.130.1.3	0 udp/514	10.130.1.13	udp/514
6/15/10 1:13:41 AM 🔥 Informational 302016 Teardown L	DP 945A-13	10.130.1.3	udp/514	10.130.1.13	udp/514
6/15/10 1:11:40 AM 1 Informational 302015	P SASA-13	10.130.1.13	3 udp/514	10.130.1.30	udp/514
6/15/10 1:11:40 AM 1 Informational 302015 AB Bulk UD	P @ ASA-13	10.130.1.1	3 udp/514	10.130.1.31	udp/514
6/15/10 1:11:40 AM 4. Informational 302016 Teardown L	OP SASA-13	ASA-13 10.130.1.30	0 udp/S14	10.130.1.13	udp/S14
6/15/10 1:11:40 AM 🔒 Informational 302016 Teardown U	DP SA-13	10.130.1.3	udp/514	10.130.1.13	udp/514
6/15/10 1:09:39 AM 👔 Informational 302015 💏 Buik UD	P \$ A5A-13	10.130.1.13	0 udp/514	10.130.1.30	udp/514
6/15/10 1:09:39 AM 1 Informational 302015 # Built UD	P SA5A-13	10.130.1.13	3 udp/S14	10.130.1.31	udp/514
6/15/10 1:09:39 AM 4 Informational 302016 Teardown L	DP SASA-13	10.130.1.3	0 udp/514	10.130.1.13	udp/514
<					
		1			



Event Viewer Detail

🙀 CSM - Event Viewer											
<u>File View H</u> elp											cisco
Views 9	Event Monitoring										
🗣 New 📝 Edit 🏢 Delete	🛛 🛃 All Device Events 🔾	<									4 🕨 🗉
Predefined Views	Settings				n n						۲
Firewall Traffic Ever	Search within results: Qr Typ	e here to search	👸 last 1	day 🔹 🔛 Sa	we 🔹 👂 Start 🔳 Sto	🗐 📋 Clear					3,620
Firewall Denied Eve	Receive Time Severity	💌 Event Type ID	Event Name		🕆 Device 💌	Reputation 💌 Source	~	Source Service	Destination	🛛 Destination	n Service 💌 🔳
NAT Events	6/15/10 1:25:44 AM 🔥 Inform	national 302015	💏 Buik UDP		S ASA-13	10.130.	1.13	udp/514	10.130.1.30	udp/514	^
	6/15/10 1:25:44 AM 🔒 Inform	national 302015	🙀 Buit UDP		SP A5A-13	10.130.	1.13	udp/514	10.130.1.31	udp/514	-
- 🧱 IPSec VPN Events	6/15/10 1:25:44 AM 👍 Inform	national 302016	Teardown UD	P	SP ASA-13	10.130.	1.30	udp/514	10.130.1.13	udp/514	
SSL VPN Events	6/15/10 1:25:44 AM 🔥 Inform	national 302016	Teardown UD	P	A5A-13	10.130.	1.31	udp/514	10.130.1.13	udp/514	
Failover Events	6/15/10 1:23:42 AM 🔥 Inform	national 302015	🙀 Built UDP		A5A-13	10.130.	1.13	udp/514	10.130.1.30	udp/514	
All IPS Events	6/15/10 1:23:42 AM 👍 Inform	national 302015	A Buit UDP		ASA-13	10.130.	1.13	udp/514	10.130.1.31	udp/514	
IPS Phonty Alerts	6/15/10 1:23:42 AM 🔥 Inform	national 302016	Teardown UD	P	S A5A-13	10.130.	1.30	udp/514	10.130.1.13	udp/514	
IDS Status Events	6/15/10 1:23:42 AM 🔥 Inform	national 302016	Teardown UD	P	S ASA-13	10.130.	1.31	udp/514	10.130.1.13	udp/514	
IPS Error Events	6/15/10 1:21:41 AM 🔥 Inform	national 302015	ALC BUILTOP		S ASA-13	10.130	1.13	udp/514	10.130.1.30	udp/514	
B IN Views	6/15/10 1:21:41 AM	vational 302015	ALD Built LIDP		SA54-13	10.130	1.13	udp/S14	10,130,1,31	udp/514	
- III Test IPS	6/15/10 1:21:41 AM 🔥 Inform	ational 302016	Teardown UD	P	S ASA-13	10.130	1.30	udp/514	10,130,1,13	udp/514	
	6/15/10 1:21:41 AM	national 302016	Teardown UD	P	SA54-13	10.130	1.31	udp/514	10.130.1.13	udo/514	
- 📴 Last 1 Day botnet e	6(15(10.1:19:40 AM A Toforn	vational 302015	AR Built LIDP		SP ASA-13	10.130	1.13	udp/514	10.130.1.30	udp/514	
	6/15/10 1:19:40 AM	ational 302015	A But UDD		S ASA-13	10.130	1.13	udp/514	10,130,1,31	udp/514	
Last 1 day All Even	6/15/10 1:19:40 AM	lational 302016	Teardown UD	P	SP A5A-13	10.130	1.30	udp/514	10 130 1 13	udp/514	
Errors Only ASA	6/15/10 1:19:40 AM	ational 302016	Teardown UD	P	ASA-13	10.130	1.21	udo/514	10,130,1,13	udp/514	
mark test	chicker 17 co 10 6 - 7		2 P 10		ADA-13	10.130.	1.01	000014	10,100,1,10	000/014	Y
1 Jarry IDS view	<										>
BitTorreptActivity	5						1				
- III AT View											
AAA Events-Spivey											
	2:00 AM 4:00 AM	6:00 AM	8.00 AM 1	0:00 AM	12:00 PM 2:00 PI	M 400 PM	6:00 P	M 8:00 PM	10:00 PM	12:00 AM	مر مر
	🗉 Event Details										0
	Receive Time	6/15/10 1:23:42 AM		Severity	Informatio	nal	^	Event Type ID	30201	5	
	Event Name	Built UDP	R.	Device	ASA-13			Reputation			
	Source	10.130.1.13		Source Serv	rice udp/514		-	Destination	10.130	0.1.30	
	Destination Service	udp/514		Action	built			Risk Rating			
	Destination Interface	inside		Description	bult outbo 29201543 (10.130.1	und udp connection for inside:10.130.1.30/51 30/514) to	4				
	Displayed Fields Details	Explanation Related Th	reats (Recommen	ded Action (Trig	gger Packet Context Pack	ket /					
< >	P										

Ciscolive!

BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

Real-Time Event Viewer

<u> </u>	II Device Events ×									4 14 1
🔅 View	Settings									*
Search wit	thin results: Q- Type here to	search	10:12:22	AM - 10:7		Save 🔹 🕨 S	Start 🔳 Stop 📋	Clear		70
No.	Receive Time	Severity 👻	Device 👻	Source	. Locate	r Identity	✓ Protocol ✓	Source 🔻	Destin 👻	Event Name
24	1/26/12 10:32:14 AM	🔥 Informational	🔗 ny-asa	172. ev	ents from		udp	udp/31784	172.16	H Built UDP
25	1/26/12 10:32:14 AM	🔥 Informational	🤗 ny-asa	172.				37455		SSLHandsha
26	1/26/12 10:32:14 AM	🔥 Informational	🦃 ny-asa	172.	Sales-PC			37455		SSL handsh
27	1/26/12 10:32:13 AM	🔥 Informational	🦃 ny-asa	172. 10. 1.			TCP> tcp	tcp/37455	204.15	Built TCP
28	1/26/12 10:32:13 AM	🔥 Informational	🦃 ny-asa	172.16			udp 🗤	udp/18701	172.16	Built UDP
29	1/26/12 10:32:09 AM	🔥 Informational	🦃 ny-asa	SALE C	THREATDLA	BS\sales-user	TCP> tcp	tcp/51403		PAT teardown
30	1/26/12 10:32:08 AM	🔥 Informational	💭 ny-asa	SALES-PC	THREATDLA	BS\sales-user	TOP top	tcp/51401		PAT teardown
31	1/26/12 10:32:08 AM	🔥 Informational	🦃 ny-asa	SALES-PC	THREATDLA	BS\sales-user	TCP> tcp	tcp/51410		PAT teardown
32	1/26/12 10:32:08 AM	🔥 Informational	🦃 ny-asa	SALES-PC	THREATDLA	BS\sales-user	TCP> tcp	tcp/51402		PAT teardown
33	1/26/12 10:32:08 AM	🔥 Informational	🦃 ny-asa	SALES-PC	THREATDLA	BS\sales-user	TCP> tcp	tcp/51411		PAT teardown
34	1/26/12 10:32:08 AM	🔥 Informational	💭 ny-asa	SALES-PC	THREATDLA	BS\sales-user	TCP> tcp	tcp/51400		PAT teardown
35	1/26/12 10:32:05 AM	🔥 Informational	💭 ny-asa	74.125.53.139			TCP> tcp	tcp/80	RY-PC2	Teardown TCF
36	1/26/12 10:32:05 AM	🔥 Informational	🦃 ny-asa	74.125.224.71			TCP> tcp	tcp/80	RY-PC2	Teardown TCF
37	1/26/12 10:31:48 AM	🔥 Informational	🦃 sf-asa	172.16.1.90			udp 🗤	udp/514	172.16	Built UDP
38	1/26/12 10:31:48 AM	🔥 Informational	🦃 sf-asa	172.16.1.10			udp 🗤	udp/514	172.16	Teardown UDF
39	1/26/12 10:31:39 AM	🔥 Informational	🔗 ny-asa	72.247.64.170			TCP> tcp	tcp/80	SALES-PC	Teardown TCF
40	1/26/12 10:31:38 AM	🔥 Informational	🦃 ny-asa	SALES-PC	THREATDLA	BS\sales-user 🔪	TCP> tcp	tcp/51415	74.125	Built TCP
41	1/26/12 10:31:38 AM	🔥 Informational	🔗 ny-asa	SALES-PC	THREATDLA	BS\sales-user	tcp	tcp/51415		PAT created
42	1/26/12 10:31:38 AM	🔥 Informational	🤗 ny-asa	72.247.64.170				tcp/80	SALES-PC	Teardown TCF
43	1/26/12 10:31:38 AM	🔥 Informational	🤗 ny-asa	72.247.64.170		(SALES-PC	Teardown TCF
44	1/26/12 10:31:38 AM	🛓 Informational	🤗 ny-asa	72.247.64.170			2. LOOKS	s tor AD	SALES-PC	Teardown TCF
45	1/26/12 10:31:38 AM	🔥 Informational	🤗 ny-asa	72.247.64.170					SALES-PC	Teardown TCF
46	1/26/12 10:31:38 AM	🔥 Informational	🤗 ny-asa	SALES-PC	THREATDLA	BS\sales-user	user n	lames	74.125	Built TCP
47	1/26/12 10:31:38 AM	 Informational 	🕝 nv-asa	SALES-PC	THREATDLA	RS\sales-user	aalaa			PAT created
<u> </u>							Sales	-usei		
2				Λ	ΛΛ					Y 😔 (
-	Λ									
0	/ \							$ _ \land _$		
	10:14 AM 10:16	6 AM 10:18 A	M 10:2	20 AM 10:22	2 AM 10:24 AM	10:26 AM	1 10:28 A	M 10:30	AM	10:32 AM 🌮 🦉
+ Even	t Details									

© 2014 Cisco and/or its affiliates. All rights reserved.

Jump to Policy from Events

🎲 CSM - Event Viewer									- 🖻 🔀					
File View Help							_		ulu –					
Views P	Event Monitoring							CI	sco					
🗣 New 🗹 Edt 🏢 Delete	All Device Events ×								4 1 1					
- II Predefined Views	Settings								(*)					
All Device Events	Found with the second of Co-Trans have be second	Million Laborard Direct		land 1	6						_	_		-
Firewall Traffic Eve	Bearch within results: Q+ Type here to search	🕑 last 1 day 🔹 🔛 Sav	a • p start 🌆 stop 🔲 Ci	lear	Cisco Security Manager - adm	in Conner	cted to	10.130.1.30						
- AAA Events	Receive Time Severity ⊻ Event Type ID	Event Name	Device ⊻ Reputatio	on 🚩 Source	the for new Forth Tot Co	e Geb								
NAT Events	6/15/10 12:55:40 A Informational 302015	🙀 Buil: UDP	S ASA-13	10.130.1		Denire Al	64.17		Deless Arrest	e Rudae			_	-
Botnet Events	6/15/10 12:55:40 🔥 Informational 302015	🙀 Buit UDP	SP ASA-13	10.130.1	Devices 😥 🖄	Policy Assi	aned: A5	A-13 Local Rules - Orio	ainal Assigned To:	L Device	Inherits Pi	rom: Corp Pol	KY.	
SSI VPN Events	6/15/10 12:55:40 🔥 Informational 302016	Teardown UDP	SP ASA-13	10.130.1	Filter : none 👻	FRet	(- none	-)						
Failover Events	6/15/10 12:55:40 A Informational 302016	Teardown UDP	ASA-13	10.130.1	- Albah al	(Constraint)	Constanting of the		~				Acoly	Cear
🗑 All IPS Events	6/15/10 12:53:39 A Informational 302015	(A) Built UDP	ASA-13	10.130.1	Boston Univ	No.	Pernit	Source	Destination	Service	Interface	DV.	Options	Cati
🙀 IP5 Priority Alerts	6/15/10 12:53:39 A Informational 302015	grag Built UDP	BP A5A-13	10.130.1	B B Demo	* EG	orp Policy	- Mandatory (E Rule)						
- 0 IP5 Alert Events	6/15/10 12:53:39 1 Informational Sozote	Teardown UDP	SP A5A-13	10.130.1	E Live Devices	8 ØA	SA-13 Los	al Rules - Original - Mand	atory (7 Rules)					
IP5 Status Events	6/15/10 12:53:37 A Informational 302016	A Public	SP ASA-13	10.130.1		100	SM	att ()))	10.130.3-0/24	(BP)	outside //	(In)		SILL
My Views	6/15/10 12:51:38 A Telementional 302015	AS RUBUDD	ASA 12	10.130.1	-S 195-21_DM2	2	*	👼 inside-network	any any	₽P	🝓 Global	in		N
- Test IPS	6/15/10 12:51:38 A Informational 302016	Teardown LIDP	S ASA-13	10.130.1	- @ ny-asa	3	v	any any	anakerver	SMTP	🍓 Global	in		N
	6/15/10 12:51:38 A Informational 302016	Teardown UDP	@ A5A-13	10.130.1	Sec. 1		V	any any	webserver1	P HTTP	🝓 Global	in		N
- 🕕 Last 1 Day botnet	6/15/10 12:49:37 Informational 30/2015	At Buit LIDP	SP ASA-13	10.130.1	(Policies)	5	V	B DMZ_Servers	DB_server1	top/1521	🍓 Global	in		N
- III botnet	6/15/10 12:49:37 A Informational 302015	Fiker This Value		10.130.1	Frend	6	V	ary ary	D8_server1	tcp/8080	😪 Global	in		N
East 1 day All Even	6/15/10 12:49:37 A Informational 302016	Teardow Either Not This V	(alue)	10.130.1	AAA Rules	7	×	1.2.3.4	any any	PP	😪 Global	in		N
mark test	6/15/10 12:49:37 🛦 Informational 302016	Teardow Custom Titles		10.130.1	- Fill Inspection Rules	ELA	5A-13 Los	al Rules - Original - Defa	it (Expty)					
- GY View	6/15/10 12:47:35 🔒 Informational 302010	Connect			Botnet Traffic Filter Rule	= 610	orp Policy	- Default (1 Rule)						
	6/15/10 12:47:33 4. Informational 302015	A Buil: Clear This Filter		10.130.1	Web Filter Rules	-								
- III BitTorrentActivity	6/15/10 12:47:33 🔒 Informational 302015	H Bult Clear Al Filters		10.130.1	H NAT									
AT View	6/15/10 12:47:33 🔥 Informational 302016	Teardow Filter this flow		10.130.1	Translation Options					R				
testrov	⁹ 6/15/10 12:47:33 🔒 Informational 302016	Teardow Create Filter fr	om Event	10.130.1										
	6/15/10 12:45:32 🧘 Informational 302015	A Buit		10.130.1	Remote Access VPN GT Configuration Waard									
	6/15/10 12:45:32 🤱 Informational 302015	Buil: Show All Details	5	10.130.1	- 🗍 ASA Cluster Load Balanc									
	6/15/10 12:45:32 🔥 Informational 302016	Teardow Re Copy Cell		10.130.1	Dynamic Access									
	N	Real Copy Selected	Event(s)		Gobal Settings									
		Res CODY AL ROWS			Public Key Infrastructure	4						A		3
					PSec VPN						Tq	ols 🕶 🞯	* * 🛃	ノ血
		Save Selected	Event(s) as HTML	400.011	S. (2)	1 A5A 8.3	crovards	the device uses Real IP(p	re-natted IP) in firewall rul	is Use Real IP addresses.				
	2.00 AM 4.00 AM 0.00 AM	Save All Events	; as HTML	4.00 F.84										5010
<	Event Details	Save Selected I	Event(s) as CSV						0					
		Save All Events	as CSV											
🐉 start 🔰 🔗 🔞	🗃 🔤 📸 👘 🙈 Cisco Security Manag 🛛 🍇 C	SM - Event Vie Go TorPolicy						339.8	1:31 AM					
									and the second					



Jump to Events from Policy

- A new right click menu item 'Show Events'
- When clicked, Event Viewer is launched with filters like Device, Source, Destination, Source/Destination Service, Source User Identity, Action and Source/Destination Security Group Tag/Name.

🕞 🗐 Best_sane_rule - Mandatory (20 Rules)

0	1	 Image: A second s	4.5.	Edit Sources			11.1.1	no tags	👮 ТСР
	2	\checkmark	📑 All-A	Show Source Copter	ote		🛃 All-Ad	no tags	🔗 IP
	3	Ś	📑 All-A	Create Network Ohi	iect from Cell Contents.		🚇 All-Ad	no tags	tcp/old/1-65535
	4	V	📑 All-A	Add Row		•	🚇 All-Ad	no tags	🔊 try
®	5	\checkmark	📑 All-A	Edit Row		Ctrl+E	10.1.1	no tags	🦻 try 1
S	6	V	📑 All-A 😭	😭 Delete Row		Ctrl+D	9.9.9.9	no tags	穿 UDP
®	7	\checkmark	8.9. 。	🐇 Cut		Ctrl+X	📑 All-Ad	no tags	穿 тср
®	8	V	8.9.	🛅 Сору		Ctrl+C	5.5.5.5	no tags	穿 тср
®	9	\checkmark	🚜 All-A 🖺	Paste		Ctrl+V	10.3.4.5	no tags	穿 тср
0	10	V	🚅 All-A	Move Row Up		Ctrl+Up	10.5.6.7	no tags	DICMP
®	11	V	🚅 All-A 💐	Move Row Down		Ctrl+Down	🎒 NETOBJ1	no tags	👮 ТСР
ø	12	V	🥵 neto	Include in New Secti	ion		🛃 All-Ad	no tags	De TCP
G	13	\checkmark	🖷 All-👩	Disable			notobj10	no tags	👮 ТСР
G	14	\checkmark	🖷 All-	Show Events		۱.	Realtime	no tags	👮 ТСР
6	15	V	📲 All-A	Show MARS Events		•	Historical	no tags	sicmpthingy
6	16	v	All-A	Import Rules				no tags	tcp/serOG2
0	17	<i>√</i>	🚅 All-Ass	Combine Rules	no tago	10 0301	📲 All-Ad	no tags	🔗 ICMP6-Router-Ad
0	18	<i>√</i>	🛋 All-Add	Iresses	no tags	no user	All-Ad	no tags	😴 тср
	19	V	🚚 All-Add	Iresses	no tags	no user	All-Ad	no tags	₩ P
	20	1	All-Add	Iresses	no tags	no user	All-Ad	no tags	₩ P
	20			•					**



@ Office

Day in the life of Security Administrator

8 AM	9 AM	11 AM	12 PM	Lunch	3 PM	5 PM	9 PM	12AM	

Challenges

- Are the policies deployed earlier working?
- Trouble shooting existing policies?
- Setting up alerts for critical assets
- Have I completed all my tickets?

SW updates image management


CSM Solution

CSM Image Manager

All ASA Software Upgrades Taken Care

- Consolidated view of all ASA images that will matter for your n/w
- Validates jobs and hardware requirements before upgrade
- Notifications post image upgrades to provide the job status
- Reduces manual errors by doing all requisite checks before and after upgrades
- It can be done in batch.
- There is no requirement to re-discover the device back (except for NAT if moving from pre 8.3 to post 8.3). This is a great benefit from CSM perspective since the complete policy structure is maintained.

Cisco Security Manager - Image e Launch Help	Manager	r - admin Connected	to 'jthakre-demo	,					_ 🗆 ×
🔄 🔂 🍊 I 🗈 😤 I 🤗 📃								Q-	cisco
	٠	🔛 Install Image	Release Note	s			Not up	dated. Click this button to start up	date. 🛛 🏀
Images	All In	ages							
Repository Images	٢	Image		Туре 👻	Version	Location	▼ Size ▼	Description	Commen
Bundles 💠 💥 🌣	×	anyconnect-linux-k9-	2.2.0128.pkg	AnyConnect Image	2.2.0128	🕎 Repository	3.5 MB	AnyConnect Image	*
Bundles	×	csd_3_6_181-3.6.18	l.pkg	Cisco Secure Desktop Image	3.6.181	🙀 Repository	25.5 MB	📄 Cisco Secure Desktop Image	
🔤 asa-asdm	×	anyconnect-macosx-p	owerpc-k9-2.2.0	AnyConnect Image	2.2.0128	🕎 Repository	3.2 MB	AnyConnect Image	
Devices 🎗	×	anyconnect-macosx-i	386-2.2.0140-k9	AnyConnect Image	2.2.0140	🞇 Repository	3.2 MB	AnyConnect Image	
Device Groups	×	anyconnect-linux-64-	3.0.0629-k9-3.0	AnyConnect Image	3.0.0629	🞇 Repository	6.3 MB	AnyConnect Image	
	×	anyconnect-linux-2.2	.0140-k9-2.2.01	AnyConnect Image	2.2.0140	🎇 Repository	3.5 MB	AnyConnect Image	
MRBAC	×	anyconnect-macosx-p	owerpc-2.3.201	AnyConnect Image	2.3.2016	🎇 Repository	4.1 MB	AnyConnect Image	
	×	securedesktop_asa-k	9-3.3.0.118.pkg	Cisco Secure Desktop Image	3.3.0.118	🔯 Repository	4.5 MB	📄 Cisco Secure Desktop Image	
asa5540-seed	×	anyconnect-macosx-i	386-2.4.1012-k9	AnyConnect Image	2.4.1012	🎇 Repository	4.6 MB	AnyConnect Image	
ASA_MULTI_CTX	×	rdp-plugin-1.0.2.jar		Remote Access Plugin	1.0.2	🔯 Repository	850.2 KB	📑 Remote Access Plugin	
ASA_VPN_SIM_SINGLE	×	anyconnect-win-2.3.3	2016-k9-2.3.201	AnyConnect Image	2.3.2016	🔯 Repository	2.5 MB	AnyConnect Image	
BLR-ASA	×	anyconnect-linux-3.0	.0629-k9-3.0.06	AnyConnect Image	3.0.0629	🔯 Repository	8.2 MB	AnyConnect Image	
BLR-ASA-IM	×	anyconnect-macosx-i	386-2.5.2006-k9	AnyConnect Image	2.5.2006	🔯 Repository	6.1 MB	AnyConnect Image	
HQ-ASA-IM	×	csd-3.4.0373.pkg		Cisco Secure Desktop Image	3.4.0373	🔯 Repository	8.5 MB	📄 Cisco Secure Desktop Image	
HQ-ASA-IM-1	×	anyconnect-linux-2.5	2006-k9-2.5.20	AnyConnect Image	2.5.2006	🔯 Repository	6.3 MB	AnyConnect Image	
SF-ASA	×	securedesktop-asa_k	9-3.2.0.136.pkg	Cisco Secure Desktop Image	3.2.0.136	🞇 Repository	3.0 MB	📑 Cisco Secure Desktop Image	
Jobs	×	csd_3_5_2001-3.5.20	001.pkg	Cisco Secure Desktop Image	3.5.2001	🔯 Repository	11.8 MB	📄 Cisco Secure Desktop Image	
Install Jobs	×	anyconnect-linux-2.4	1012-k9-2.4.10	AnyConnect Image	2.4.1012	🔯 Repository	4.9 MB	AnyConnect Image	
	×	anyconnect-win-2.5.2	2006-k9-2.5.200	AnyConnect Image	2.5.2006	🔯 Repository	4.4 MB	AnyConnect Image	
	×	csd_3_5_2008-3.5.20	008.pkg	Cisco Secure Desktop Image	3.5.2008	🞇 Repository	12.3 MB	📑 Cisco Secure Desktop Image	
	×	csd_3_4_2048-3.4.20)48.pkg	Cisco Secure Desktop Image	3.4.2048	🔯 Repository	9.6 MB	Cisco Secure Desktop Image	
	×	anyconnect-macosx-p	owerpc-2.4.101	AnyConnect Image	2.4.1012	🞇 Repository	4.6 MB	AnyConnect Image	
	×	anyconnect-macosx-p	owerpc-2.5.200	AnyConnect Image	2.5.2006	🕎 Repository	6.1 MB	AnyConnect Image	
	×	csd_3_5_841-3.5.84	L.pkg	Cisco Secure Desktop Image	3.5.841	🔯 Repository	11.5 MB	📑 Cisco Secure Desktop Image	
						~		1	-



Launch ASA Image Manager



Assign Images to Devices



Configure Image Update Job

Install images on selected devices Assign Images for installation on devices Assign images to device by clicking Add button. Righ Assignments Schedule Properties	t dick on assignments in the l	pelow table and delete as required. Validation Complete. Start Val	Install images of Assign Image Assign image Idation Assignments	n selected devices es for installation s to device by clicking Scheduk	n on dev Add	3. Select Schedule tab	he below table a	and delete as required	
Device Image	Validation	1 Click	44 4			January 2012			b b b
🖃 🦃 sf-asa		T. CIICK	Sun	Mon	Tue	Wed	Thu	Fri	Sat
securedesktop_asa_k9-3.3.0.151.pkg	Warning	Start	1	2	3	4	5	6	7
Warnings		Validation	8	9	10	11	12	13	14
to view			15	16	17	18	19	20	21
Device dirty			22	23	24	25	26	²⁷ 4 S	elect
Description: Device is marked dirty			29	30	31	1	2	fut	
Cause: There are config changes pending to be deployed to	o the device		5	6	7	8	9		ure
to prevent inconsistent behaviour	Assign Images for it Assign images to devic Assignments Schedu Name: Image Description: Image	Installation on devices e by dicking Add button. Right dick on ass Properties Install Job - 26 Jan 2012 14:29:54 Install Job added at 26 Jan 2012	signments in the below table i	and delete as required.		Now		Install	Cancel
5. Adjust other parameters	In Error Stop Installation Continue Install	Backup Current Image Install in C Yes C Par ation C No C Seq	nages to devices in G Ins allel G Ins juential G Onl	iall image and reboot de iall image, but do not re y copy image onto devic	evice eboot device ices	1. C St Valid	Click art ation		
BRKSEC-2060	Add Assignment	© 2014 Cisco and/or its am	liates. All rights reser	Install Ved.	Cancel	Cisco Public		c	isco <i>livi</i>

Review Image Update Job Status





Review Device Installed Images & Status



BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

@ Office

Day in the life of Security Administrator

8 AM 9 AM 11 AM 12 PM Lunch 3 PM 5 PM 9 PM 12AM

Challenges

- Are the policies deployed earlier working?
- Trouble shooting existing policies?
- Setting up alerts for critical assets
- Have I completed all my tickets?



Deployment

Scalable Distributed Deployment

What Is It?

 Simplified distributed deployment method for 1000s remote devices

Example

- Update large numbers of remote firewalls, which may have dynamic addresses, intermittent links, or NAT addresses
- Update both configurations and software images
- Devices self updated whenever they come online
- Scales through Web technologies

Benefit

 Helps customers with 1000s of teleworkers and remote locations with minimal technical staff at the remote site





Deployment Manager

- Deployment choices: deploy to file, device, token server, AUS, etc.
- Schedule job deployments with notification and approval
- Lets users select devices to deploy and provides deployment report

Deployment Manager				
Deployment Job Table (5/5 loaded)				
Name	Last Action 🔺	Status	Changed By	Description
admin_job_2005-12-05 15:07:4	05-Dec-2005 15:08:04	Deployed	admin	Auto Created Deployment Job i
admin_job_2005-12-05 15:04:2	05-Dec-2005 15:04:27	Failed	admin	Auto Created Deployment Job i
admin_job_2005-12-05 15:02:0	05-Dec-2005 15:02:08	Failed	admin	Auto Created Deployment Job i
admin_job_2005-12-05 15:00:0	05-Dec-2005 15:01:21	Failed	admin	Auto Created Deployment Job i
admin_job_2005-12-05 14:56:2	05-Dec-2005 14:57:05	Failed	admin	Auto Created Deployment Job i
		Deploy	Refresh Redeploy	Abort Rollback
Summary Details Deployment Job Name: Deployment Status: Progress Status: Number Of Devices To Be Deployed: Number Of Devices Deployed Successfully: Number Of Devices Deployed With Errors:	admin_job_2005-12-05 15:07:4: Deployed 4 3 0	3.718 4 devices completed. (75%)		
				Close Help



CSM Solution

CSM Report Manager

Standard Reports with Drilldown Capabilities

- Out of box systems reports for FW, IPS, and VPN
- Ability to export reports to most commonly used formats
- Users can define and save custom views of standard reports
- Drill down from reports to relevant data points through the application





Sample Drill Down Report





Cisco Public

Some More....

Generate Report 🚽 🕞 Pr <mark>int 🕞 Export 🔹</mark> Chart Type : Pie 💌									
Duration : Dec 6, 2013 3:00:00 as PDF 6, 2013 4:00:00 PM									×
		📓 Top Victims (Sig	nature ID=9445.1)						۲
		Chart Table							
	Drill down		,		,	If IP Intel data is no	present, the data may	not be available or time	out would have occurred 🔺
	Table view	Rank	Victim Address	Count	Reverse DNS Name	Country	City	Region	Percentage
		1	3.3.3.5 1	1121	n003-000-000-000	. United States	Fairfield	Connecticut	33.23
	9445.1	2	3.3.3.6 1	1059	n003-000-000-000	. United States	Fairfield	Connecticut	31.4
	9445.0	3	3.3.3.1 2	228	n003-000-000-000	. United States	Fairfield	Connecticut	6.76
	9445.2	4	3.3.3.7 2	220	n003-000-000-000	. United States	Fairfield	Connecticut	6.52
	1716.0	5	3.3.3.8 2	216	n003-000-000-000	. United States	Fairfield	Connecticut	6.4
	1407.0	Top Attackers (Signature ID=9445	1)					
	1330.8	Chart Table	Signatare 10-3443.	•••					w.
	1717.0					If IP Intel data is no	present, the data may	not be available or time	out would have occurred 🔺
	1707.0	Rank	Attacker Address	Count	Reverse DNS Name	Country	City	Region	Percentage
	1403.0	1	20.20.20.9 1	1409		United States	Falls Church	Virginia	42.53
		2	20.20.20.8	344		United States	Falls Church	Virginia	10.38
		3	20.20.20.6 3	336		United States	Falls Church	Virginia	10.14
		4	20.20.20.3 2	270		United States	Falls Church	Virginia	8.15
		5	20.20.20.2 2	211		United States	Falls Church	Virginia	6.37
		Ľ.						-	
								Genera	ted on Dec 5, 2013 4/03/37 P
Rank	Signature ID	Signature Name	•		Count			Percentage	
1 9445.1	Back Door PC In	wader		3711			13.26		4
2 9445.0	Back Door PC In	wader		3150			11.26		
3 9445.2	Back Door PC In	wader		3134			11.2		
4 1716.0	IPv6 Options Pa	idding Too Long		3110			11.12		
5 1407.0	Teredo Destinat	ion Port		2610			9.33		
6 1401.0	IPIP Encapsulati	ion		2588			9.25		



Send Report via Email

Security Manager Notification: Schedule ff run successful on Wed Dec 11 20:00:13 CET 2013

Wednesday,	December 11, 2013 8:00:43 PM 🎤
From	admin@domain.com
То	gacs@budlabsec.com
Attachments	1day fw_Report-ff-admin.pdf

Dear User,

Schedule $f\!f$ succeeded in generating $1day~f\!w$ report on Wed Dec 11 20:00:13 CET 2013

Attached:pdf



173 37 95 213

Ciscolive

kujoprod14.cisco.com 0.02

@ Office



Day in the life of Security Administrator

8 AM	9 AM	11 AM	12 PM	Lunch	3 PM	5 PM	9 PM	124	AM	
									sleep	



Cisco Prime Security Manager







- Primarily for Cisco NG firewall or called "CX"
- Focus on easy to use simple deployments
- Basic ASA management
- Focus on NGFW features
 - L7 Applications
 - URL filtering
 - NGIPS
 - Basic ASA management



PRSM

In Action (Operations)

- Dashboard
- New Policy Model
- Events
- Reports



PRSM in Action Security Admin



Day in the life of Security Administrator





Quick Security Snap Shot



8 AM							\sum	\geq	\geq	
Quick Security Snap Shot	User and Application Activity Review	Change Request	Report Request	Security System Alerts	New Software Update Arrives	Sleep at ease				

To be added



User and Application Activity Review

Top 25 applications by transactions

02 Feb 2014, 03:30:39 AM (UTC) to 03 Feb 2014, 03:30:39 AM (UTC)

		Trar	sactions			Bytes		Top 5 by transactions			
	Application	Total	Allowed	Denied	Total	Sent	Received	Users		Web destinations	
1	HyperText Transfer Protocol	99.0 H	96.0 K	2.0 K	2.0 GB	29.0 MB	2.0 GB	ADR\\Ranj Sharma ADR\\Vikram Kulkami ADR\\Dilbert Geek ADR\\Ami Kurosawa ADR\\Sean Darrell	9.0 K 8.0 K 8.0 K 8.0 K 8.0 K	www.best-of-web.com www.mars.com www.hollywoodtuna.com updates.ironport.com www.northamericanwhitetail.com	535 493 438 420 404
2	SharePoint	2.0 K	2.0 K	8	81.0 MB	793.0 KB	81.0 MB	ADR\\Jane Radcliff ADR\\Ira Blue ADR\\Vikram Kulkarni ADR\\Harry Houdini ADR\\Ranj Sharma	488 370 207 200 195	www.nsc.org www.sru.edu www.health.nsw.gov.au www.rightathome.com www.northern.edu	270 257 178 168 158
3	Generic Search Engine Traffic	871	838	33	11.0 MB	227.0 KB	11.0 MB	ADR\\Jane Radcliff ADR\\Ira Blue ADR\\Sean Darrell ADR\\Vicki Dustin ADR\\Harry Houdini	117 105 86 74 66	www.korea.net www.cowboy.com www.tom.com www.thefreesite.com www.yam.com	85 84 74 72 61
4	Transport Layer Security Protocol	698	602	96	3.0 MB	1.0 MB	2.0 MB	ADR\\Jane Radcliff ADR\\Ira Blue ADR\\Ranj Sharma ADR\\Nina Chemski ADR\\Rita Meter	110 103 62 54 54	www.cisco.com news-tags.cisco.com cisco-tags.cisco.com www.static-cisco.com	26 6 6 2
5	Domain Name System	536	536	0	119.0 KB	18.0 KB	100.0 KB	ADR\\Rita Meter 172.16.1.240 172.16.1.100	301 207 28		
6	SSL	501	501	0	496.0 MB	1.0 MB	494.0 MB	172.16.1.80 172.16.1.120	251 250		
7	eBay	223	205	18	4.0 MB	78.0 KB	4.0 MB	ADR\\Rita Meter ADR\\Vikram Kulkarni ADR\\Ranj Sharma ADR\\Ira Blue ADR\\Sean Darrell	209 5 5 1 1	i.ebayimg.com ir.ebaystatic.com srx.main.ebayrtm.com rtm.ebaystatic.com www.ebay.com	143 18 16 14 10
8	Binary over HTTP	176	69	107	2.0 MB	37.0 KB	2.0 MB	ADR\\Nina Chemski ADR\\Harry Houdini ADR\\Jane Radcliff ADR\\Dilbert Geek ADR\\Sean Darrell	46 44 17 14 14	download.registrysmart.com download.errorsmart.com carlo20.dyndns.org banner.cdpoker.com Imon2web.org	8 6 6 5
9	Flash Video	140	140	0	40.0 MB	38.0 KB	40.0 MB	ADR\\Sean Darrell ADR\\Ira Blue ADR\\Jane Radcliff ADR\\Ami Kurosawa ADR\\Vikram Kulkarni	17 16 16 14 13	www.cyberbee.com www.yamaha.com www.lostvectors.com www.learningplanet.com www.groovygirls.com	18 6 4 4 4





PRSM New Policy Model







8 AM	10 AM	11 AM	12 PM	Lunch 3 PM			
Quick Security Snap Shot	User and Application Activity Review	Change Request	Repor Reque	rt Security st System Alerts	New Software Update Arrives	Sleep at ease	

Receive Time 01/23/2013 23:37:38	Event Type HTTP Complete	Device LA-ASA-CX	Username vicki dustin	Source vicki dustin	Destination Host www.facebook.com	Destination Port 80	Application Facebook Ge	Reputation Score 5.9	Web Category Social Networking
01/23/2013 23:37:35	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:33	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:33	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:32	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:25	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:25	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443	Facebook Ge	4.0	Social Networking



Cisco Prime Security Manager in Action

						1.1	Receive Time	Event Type	Device	Username	Sou
							01/23/2013 23:37:	8 HTTP Complete	LA-ASA-CX	vicki dustin	n vick
Dag	hhoard						01/23/2013 23:37:	35 HTTP Complete	LA-ASA-CX	vicki dustin	n vick
Das	sinuaru						01/23/2013 23:37:	33 HTTP Complete	LA-ASA-CX	vicki dustin	n vick
							01/23/2013 23:37:	33 HTTP Complete	LA-ASA-CX	vicki dustin	n vick
dara (Hereinge	A Basarbos (141)						01/23/2013 23:37:	32 HTTP Complete	LA-ASA-CX	vicki dustin	n vici
	Verifield Negliational July	97.5	TRabes				01/23/2013 23:37:	7 HTTP Complete	LA-ASA-CX	vicki dustin	n vici
F98.0.401=	14.311 hospitalismi di an	172K	MecCi.				01/02/0012 22:27	1077D Complete	14.484.07	stati dunkin	
	Temphelines and	23 K	Pol Linux	1			01723/2013 23.37.	Complete	DAMBACA	VICKI DOSLIN	90.9
	Top destination						01723/2013 23:37:	25 HTTP Complete	LA-ASA-CX	vicki dustin	n vica
tere (strange (At	View non Web categories	Verane B	Tab destinations	1.4. h= 101			01/23/2013 23:37:	25 HTTP Complete	LA-ASA-CX	vicki dustin	n vick
AL AGE OF	17.6.1 Date Date of the local	19.1 X 5.5 X	control facebook cont	10.24							
	2100	53.6	www.chara.com	444							
	Applications Facility of a	10	lgafication (gene u Produkt	10 - 500 10 - 50 - 50	C	on	trol	C.	G	P Constitute (Event) D: 10	9401425
	Applications Frances (Nr. 20) Frances (Nr. 20)		light after types under the second se	9-102 - 12-4 - 13-4	C	on	trol	C.	HTT	IP Complete (Event ID: 10 HTTP transaction passed p	0401425 volicy constrain
	And the second s	100 miles	Augusta la seconda de la secon	90 808 • 10 4 • 10 4	C	on	trol	C.	HIT	P Cerepiele (Event ID: 1) HTTP bunkaction passed p Event details	9401425 olicy constrain
	And the second s			in out ■ 0.0 ⇒ 0.0 → 0.0	C	on	trol	C.	HET	IP Correlate (Event ID: 10 HTTP transaction passed po Event details Source	946142) oricy constrain
	Application Appli				C	on	trol	ŭ		Processies (Event D- 15) HTTP transaction passed pr Event details Source User v	0401425 rolicy constrain kki dustin
	ar (finite)				C	on	trol	ŭ	HET Aut	PCerretete (Eventilo 10 HTTP bunnaction passed p Event details Source Usar VI Roym k P a down 5	0401425 colicy constituit kki dualin kcopital iso 52.0.10
Ma		nts to			C	on	trol	ŭ	HET	IP Complete (Event D: 10 HTTP Instanction parent p Source Outer V Room In Pactores S Part S	046142) ohity constraint kki dualin kcoptili isiasa to isiasa to
Ma	b Eve	nts to	Policie		C	on	trol	u		IP Complete (Event Dr. 10 HTTP Instruction passed pr F Event details Source User V Royam A P actives S Herafo B Herafo B	040142) olicy constrain kki dualin toophili toophili toophili fo fo
Ma		nts to Application Service		Install on	C	ON	trol	et capture	HE	IP Corport HTP Surraction passed p F Event details Source Uses V Use V Source Port Source Port Source Port Source Port Source S	0x01422 colicy constrain kbi duatin ccopital (00502 corres 40
Ma Source theodese (1.54)	an the second se	nts to Application/Service	Policie	Install on	C Iterface role	ON	trol	et capture	HET Aa	P Complete (Event Dr. 10 HTP Parameter parent p Event details Source User W Royan h Partons S Port 6 Vert 7 Vert 7	0401422 colleg constraint kkild dualitin hecophil (4052 terve 40
Source ck policies (1-14)	er er al Appled DE Eve Destination	Application/Service	Policie	Install on	therface role	ON	Eventing Pack	et capture	H	BP Censions (Ivent D 11) HTTP Instruction passed po Town (Ivent O 444)) Starts User W Partial Sector	0401425 któl duellin któl duellin któl duellin któl duellin któl duellin któl duellin któl któl któl któl któl któl któl któl
Maa Source ck policies (1-14) Rolicies created from		nts to Applications Service		Install on	Interface role	ON	Eventing Pack	et capture	HI	Comparison Construction Con	0401425 któl dvallen któl dvallen ktorphil ktorp na któl dvallen ktorphil k
Source ck policies (1-14) Policies created from		Application Service	Policie Policie Actoricottor	Install on	Merface role	ON Ht count	Eventing Pack OFF OFF	et capture		PCereptine (Ivent Dr. 15 Provide Comparison passed p Port Observation passed p Port S Por	0.0011422 onlicy constraint icophia icos on 10 f4052 icome ico
Source ck policies (1-14) Policies created from 1 Engineering	Appled Territory of the second	nts to Application Service		Install on Al devices	Inside Inside	ON Htt count	Eventing Pack OFF OFF	et capture	H	BP Competence (Event Ch 10) HTP Parameterio passes pro- Bywent detable Source Wards with a second se	khi duatin hotoyi namalirahi koopital ka asa na koopital ka asa na koopital ka asa na koopital ka asa na koopital ka asa ka a asa ka a asa ka a as a a asa as
Source ck policies (1-14) Policies created from 1 Engineering	Aphine Control of the second s	Applications Service NPP NPP	Protection of the second secon	Install on Ail dealcos	Interface role	Ht count	Eventing Pack OFF OFF	et capture		PC Cençular E (Event Ch 1) HTTP Instruction passes por Event details Source Usas Via Portante Sea Source Source Construct Source Construct Source	0401425 ohicy construint kcbi duality cooptial texts in to 16052 com 40
Source ck policies (r-t4) Policies created from 1 Engineering	April and April Ap	Applications Service	Protection of the second secon	Install on All devices	Merface role	Ht count	Eventing Pack OFF OFF OFF OFF	et capture	HI As	PCension (Investion 10:10 HTTP Investicity processing pro- Twent details States Uname Market	Ald State Ald State
Maria Contraction of the second secon	Destination Desti	Appletites Service	Policical Policical Activational Memory Memo	Install on All devices All devices	Inside Inside Inside	ON Ht count	Eventing Pack OFF OFF OFF OFF	t capture		Proved (e) (iver10) (i) (iver10) (i) (iver10) (i) (i) (i) (i) (i) (i) (i) (i) (i) (i	kild susta kild susta song on shurri kild susta song on to forse for for for for for for for for for for
Source policies (1-14) licies created from Engineering	Destruction Destr	Application Service	Protocology PODICICS Actions Conditions Actions (2015) Actions (2015) Act	Install on Al deaces	Mertace role Inside Inside	Htt count Htt count List List Sin List List Sin List List Sin	Eventing Pack GFF GFF GFF GFF	et capture		Borner (Inset) Control (Inset) Co	0481425 antor constraint kki dualle coopta lasos no koopta forme 46

Navigate Down to Events

ce	Destination Host	Destination Port	Application	Reputation Score	Web Category
dustin	www.facebook.com	80	Facebook Ge	6.9	Social Networking
dustin	www.facebook.com	443		4.0	Social Networking
dustin	www.facebook.com	443		4.0	Social Networking
dustin	www.facebook.com	443		4.0	Social Networking
dustin	www.facebook.com	443		4.0	Social Networking
i dustin	www.facebook.com	443		4.0	Social Networking
dustin	www.facebook.com	443		4.0	Social Networking
i dustin	www.facebook.com	443		4.0	Social Networking
dustin	www.facebook.com	443	Facebook Ge	4.0	Social Networking

Terro starup: West 23 Jan 2013, 19:37 Pt

View Event

Key Benefits

- Greater visibility and control
- Enhanced threat response
 and mitigation
- Unified management for core ASA firewall and NGFW services
- Straightforward migration to ASA 5500-X NGFW
- Intuitive, easy-to-use GUI



Cisco/Sourcefire Product Portfolio





FireSIGHT Sees "Everything"

CATEGORIES	EXAMPLES	SOURCEFIRE NGIPS & NGFW	TYPICAL IPS	TYPICAL NGFW
Threats	Attacks, Anomalies	 ✓ 	~	 ✓
Users	AD, LDAP, POP3	v	×	v
Web Applications	Facebook Chat, Ebay	 ✓ 	×	
Application Protocols	HTTP, SMTP, SSH	v	×	4
File Transfers	PDF, Office, EXE, JAR	v	×	4
Malware	Conficker, Flame	¥	×	×
Command & Control Servers	C&C Security Intelligence		*	×
Client Applications	Firefox, IE6, BitTorrent	<i>v</i>	×	×
Network Servers	Apache 2.3.1, IIS4		×	×
Operating Systems	Windows, Linux	v	×	×
Routers & Switches	Cisco, Nortel, Wireless	 ✓ 	×	×
Mobile Devices	iPhone, Android, Jail	¥	×	×
Printers	HP, Xerox, Canon	v	×	×
VoIP Phones	Avaya, Polycom	 ✓ 	×	×
Virtual Machines	VMware, Xen, RHEV		×	×
Information Supe	© 2014 Cisco and/or its affiliates. All rights reserved.	Contextual Awareness		Ciscoliv

FireSIGHT Enables Automation



IT Insight Spot rogue hosts, anomalies, policy violations, and more



Automated Tuning Adjust IPS policies automatically based on network change



Impact Assessment

Threat correlation reduces actionable events by up to 99%



User Identification Associate users with security and compliance events **Ci**

Cisco Public



BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

FireSIGHT Management Centre v5 Benefits



Innovative Admin Experience

Inte	mesting Use Cases															
	Save Cancel	Save and	d Apply						O AM	Category Q Add Rule Search Rules						
-	ce Tacoete: A devices															
	ce rangeon gracticas	Route	Dest	Ren	Dest	_							_	_	_	
	Name	Zones	Zones	Net	Net	VLA	U	Applications	Services	URLa	Action	•				
Ad	ministrator Rules		_													
724	's callegory is emply.	_	_	_	_	_	_		_		_	_	-	_	-	
50	indard Rules	_	_	_	_	_										
,	Mobile Security 1	sintern 🍕	any	any	@ Ten	1000	-	Diackberry browser Mobile Safari	any	any	K Block			1	1	Ę
2	Read Only Facebook	🤹 intern	S Extern	ary	arry.	2014	arry	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game: Fit	2017 y	any	K Block			0	-	ę
а	Web Block List	sintern 🕫	Stern	шу	ary	2014	any	any	<i>my</i>	Adult and Pornography (Any Reputation) Bot Nets (Any Reputation) Confirmed SPAM Sources (Any Reputation) (13 mores)	Rinck			۰	,	5
4	Block All P2P	4 intern	S Extern	any	any	any	any	Categories: peer to peer	any	any	× Block			0	0	1
5	Inbound Email	Sector:	Sintern	any	arry	any	any	SMTP	SMTP	any	Altow			0	1	1
6	Outbound Web Browsing	S Exten	S Intern	anty	arry	any	any	HTTP	any	any	Allow			0	0	18
Ro	ot Rules															
725	s category is empty.												-		-	-
De	fault Action									Access Control: Block All Traffic					~	

Simplified Policy Model



New Reporting Engine



Flexible Report Creator



FireSIGHT Management Centre v5 Benefits

Top Events by So		$- \times$	
Country Na	me	•	Count
United State	5		162
Germany	Initiator IP ×	Initiator Location ×	Responder IP ×
China China			
Iapan	76.100.209.66	SA USA	10.4.32.112
France	10.4.10.131		10.4.32.112
Russia			
📧 North Korea	10.4.10.131		10.4.32.112
C Pakistan	10.4.33.95		10.5.32.206
Iraq	-		-
Iran	89.188.101.82	ISR	10.5.32.206
Last updated 1 min	200.189.215.85	SRA BRA	10.4.33.44
	10.4.31.237		10.5.32.206
	10.4.11.216		10.5.39.206

Geolocation in Events & Dashboards

Darkie Total Runkers NAT 20 Exercer \$1.10 - Front Interfaces Virtual Runkers NAT 30 Exercer \$1.20 - Front Interfaces Interfaces NAT 30 Exercer \$1.20 - Front Interfaces Interfaces Nature Rear Management Interfaces 10 Mark Nangement 11 Markement Nangement 12 Mark Nangement 13 Markement Nangement 13 Markement Nangement 13 Markement Nangement 13 Markement Nangement 14 Yata Paster 15 Markement Nangement 14 Yata Paster 15 Paster Paster 16 Yata Paster	Help + admin								
levie Interface Industries Verbust werkens Verbust Revere NAT 23 Sensor 24 42 - Front Industriase 24 Sensor 24 42 - Front Industriase 25 Sensor 24 42 - Front Industriase 26 Sensor 24 42 - Front Industriase 27 Sensor 24 42 - Front Industriase 28 Sensor 24 42 - Front Industriase 29 Sensor 24 42 - Front Industriase 20 Sen									
Image: Second File Image: Second File Image: Second File Image: Second File <th></th>									
Note Type Note Note <th< th=""><th colspan="9"></th></th<>									
Max Max <th></th>									
Constraint of the second									
Not Part Record 2 data C effort Assegment C effort Assegment C tip Parkine									
Kerr Hassgement Interface(s) Image: model <	101010000								
Mat Pat Name/Patents Asseptement 0 401 Management 0 101 Management 0 101 Management 0 101 Management 0 102 Management 0 103 Management	Rear Management Interface(s)								
Link Name Type NameWy Zones Assignment 0 400 Management Assignment 0 stp1 Passive Passive 0 stp2 Passive Passive 0 stp3 0 stp4									
Unit Name Type Namework Assignment 0 401 Management Assignment 0 101 Management Factors 0 102 Management Factors 0 103 Management Factors 0 104 Factors Factors	Add Interface								
of Management v 1g1 Passive Passive v 1g2 Passive Passive v 1g3 v 1g3 V	Actions								
O 11 Pactory Factory 0 112 Pactory Pactory 0 113 Pactory Pactory 0 113 Pactory Pactory	1								
\$12 Passive # Passive # Passive # Passive # Passive # Passive	1								
0 stp3 0 stp4	1								
0 xtp4	1								
	1								
() s2p1	1								
6202	1								

New Device Management

Overview Analysis Policies Devices		Health System	n Help + admin +
	Local + User Management	Updates Licenses P	fonitoring • Tools •
User Roles			
Users User Roles Login Authentication			
		Configure Permission Escalation	Create User Role
User Role		Enabled	Actions
Access Admin Sourcefire Provided			l / 🖻 🖻 🕫
Administrator Sourcefire Provided			🕘 🥒 📭 💿 🖻
External Database User Sourcefire Provided			🗏 🥒 🖻 🖉
Intrusion Admin Sourcefire Provided			🕘 🥒 📭 💿 🖻
Maintenance User Sourcefire Provided			🕘 🥒 🖻 🖉
Network Admin Sourcefire Provided) / 🗠 🗠 🛛
Reporting Admin Sourcefire Provided			🗏 🥒 📭 💿
Security Approver Sourcefire Provided			🕘 🥒 📭 💿
Security Event Analyst Sourcefire Provided			- n n s
Security Event Analyst (Read Only) Sourcefire Provided			- 🖬 🖌 🗧

Security & Network Admin Roles

erview	Analysis	Policies	Devices		•	Health	/stem
			Local + User Manag	gement	Updates	Licenses	Monii
Jser F	lole Edit	tor					
Users	User Role	ss Logi	Authentication				
	N 0 1	ame escription 1enu Base 9 Dici 9 Polici 9 Polici 9 Col 0 Col 9 Co	def Permissions arches arches	105			*
			Save Can	cel			

Admin Role Editor



Context Explorer

- Visualisation
- Explore Large Volumes of Security Data
- Identify Risky Hosts and Applications
- See Low Productivity and Bandwidth Misuse
- Acquire Actionable Intelligence





Geolocation

✓ Top Events by Source Country	— ×		Initiator	
Country Name	- Count	Initiator IP ×	Location ×	Responder IP ×
Country Name	Count	76,100,209,66	usa	10.4.32.112
United States	162		<u>0011</u>	
Germany	36	10.4.10.131		in <u>10.4.32.112</u>
China China	18	10 4 10 121		10 4 33 113
Japan	13	<u>10.4.10.131</u>		10.4.32.112
France	11	10.4.33.95		10.5.32.206
Russia	4	B 89 188 101 82		10 5 32 206
😂 North Korea	2	<u></u>	<u>13R</u>	<u>10.5.52.200</u>
C Pakistan	1	200.189.215.85	S BRA	10.4.33.44
Iraq	1	10.4.31.237		10.5.32.206
🔤 Iran	1			
		10.4.11.216		10.5.39.206
Last updated 1 minutes ago	Q, 1	_		



 Visualise and map countries, cities of hosts, events



Devices Supported by CS Manager

- Security Appliances
 - PIX 500 Series
 - ASA 5500 Series w/ AIP-SSM
 - IPS 4200 Series Sensors
- IOS Routers
 - 70, 90, 800, 1600, 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7300, 7500, 7600 Series
 - NM-CIDS
- Catalyst 6500/7600 Services Modules
 - FWSM
 - IDSM-2
 - VPNSM
 - VPN SPA
- Catalyst 6500 Series Switches



ASA/CX Installation Workflow

New customers buying ASA and CX

- Manufacturing installs CX completely before shipping
- CX is booted automatically when ASA is started
- Login to CX console from ASA CLI and setup management IP
- Configure CXSC redirection on ASA for traffic redirection
- Customers who already own an ASA
 - Install one or two SSDs on ASA depending on the model*
 - Copy **9.1.1 ASA image** which supports CX onto flash filesystem
 - CX uses 3GB space on ASA flash filesystem, so ensure we have more than 3GB free space on ASA flash
 - Reload ASA with **9.1.1 version**
 - Follow the bootstrapping steps



ASA Support Supported OS & Models





Ciscolive,

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

PRSM Offerings Virtual & Appliance

Intel Dual Core 8GB RAM, 500 GB HDD, ESXi 4.0, 5.0

Starting at \$ 3,000

100 Devices (ASA/CX) max: 5000 policies, 10000 objects, 15K eps

2.47 Ghz, 16GB RAM, 6TB HDD





PRSM Appliance

PRSM Virtual

BRKSEC-2060

© 2014 Cisco and/or its affiliates. All rights reserved.

FireSIGHT Management Centre Appliances



	DC750	DC1500	DC3500
Max. Devices Managed*	10	35	150
Max. IPS Events	20M	30M	150M
Event Storage	100 GB	125 GB	400 GB
Max. Network Map (hosts / users)	2k / 2k	50k / 50k	300k / 300k
High Availability Features	Lights-out Management (LOM)	RAID 1, LOM, High Availability pairing (HA)	RAID 5, LOM, HA, Redundant AC Power

* Max number of devices is dependent upon sensor type and event rate



Ciscolive!



Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site <u>www.ciscoliveaustralia.com/mobile</u>
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



##