Konfigurationsbeispiel eines Cisco IOS Intrusion Prevention System Security Manager

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Zugehörige Informationen

Einleitung

Cisco Security Manager ist Teil der Cisco Security Management Suite, die eine umfassende Richtlinienverwaltung und -durchsetzung für das Cisco Self-Defending Network bereitstellt. Cisco Security Manager ist eine branchenführende Anwendung der Enterprise-Klasse für das Sicherheitsmanagement. Cisco Security Manager befasst sich mit dem Konfigurationsmanagement von Firewall-, VPN- und IPS-Sicherheitsservices (Intrusion Prevention System) für Cisco Router, Security Appliances und Security Services-Module.

Eine Zusammenfassung der Funktionen und Vorteile von Cisco Security Manager sowie der neuen Funktionen in Version 3.1 finden Sie im Datenblatt zu Cisco Security Manager 3.1 unter http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd 8062bf6e.html. Sie können Cisco Security Manager 3.1 von Cisco.com unter http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app herunterladen (nur http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app

In diesem Dokument wird beschrieben, wie Sie Cisco Security Manager 3.1 zum Durchführen der Erstkonfiguration von IOS IPS verwenden. Für Router, die bereits mit IOS IPS konfiguriert sind, können Kunden Cisco Security Manager 3.1 direkt für Bereitstellungsaufgaben verwenden.

Hinweis: Cisco Security Manager 3.1 unterstützt nur IOS 12.4(11)T2- und spätere IOS-Images, um IOS IPS zu konfigurieren.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Security Manager 3.1
- Cisco IOS 12.4(11)T2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Gehen Sie wie folgt vor, um IOS IPS zu konfigurieren:

- 1. Führen Sie den Cisco Security Manager 3.1-Client von Ihrem lokalen PC aus.
- 2. Wählen Sie **Neues Gerät** im Menü Datei aus, um ein Gerät zum Cisco Security Manager 3.1 hinzuzufügen.

Cisco Security Manager Ladinin Co E. Edit. Yew Rolicy Map Tools 1	innected to '172.25.90.8'		
New Device	2		
gione Device	Paris 170 07 00 64 Pa	and the Contract	
Delete Device	Device: 1/2-25-90.91 Po	ey: Hexcorings	
Save Ox145	Prepended FlexConfigs		
Vew Changes	No.	Name	Description
Yakdate			
Sybrit			
Sugnit and Deploy			
Dgpky			
Discard			
Edit Device Groups			
Neg Device Group			
Add Devices to Group			
Bitt Codep			
E.t 0x1+0			
D HALLEND PLUMOS	Appended PlexConfigs		
Inspection Rules	No.	Name	Description
Settings			
Transparent Rules			
Web Filter Pules			
H IPS			
I MAT			
See to see whe			
2 SQ VDN			
2 Interfaces			
8 Platform			
PlexContros			
			Values Preview 🖨 🗣 🌶 🖊 🛱
			Save

 Wählen Sie im Fenster Neues Gerät aus, wie Sie das Gerät hinzufügen möchten. In diesem Beispiel wird das Gerät aus dem Netzwerk hinzugefügt.

(New Device - Choose Method (Step 1 of)	X
Please choose how you would like to add the device:	
Add Device From Network	
When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.	
Add from Configuration File	
When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.	1
Add New Device	10
You can add a device that is not yet on the network by specifying the device's identifying information and credentials.	4
Add Device From DCR	'
If you are using other CiscoWorks applications and your devices have already been added to the device credentials repository, you can import them into Cisco Security Manager.	
Back Next Pine	th Cancel Help

- 4. Klicken Sie auf Weiter.
- 5. Geben Sie die Identitätsdetails für das Gerät ein, das Sie hinzufügen möchten. Beispiel: Hostname und IP-

Adresse.

Identity		
IP Туре:	Static 🗸	
Host Name:		
Domain Name:		
IP Address:	172.25.90.91	
Display Name:*	172.25.90.91	
OS Type:*	~	
	105 - 12.3+	
	105 - Catalyst 6500/7600	
Discover Device Se	ttin PIX	
Discover:	IP5	
	JASA	
	Fixewall Policies	
	PS Policies	
	RA VPN Policies	
	Discover Policies for Security Contexts	

- 6. Klicken Sie auf Weiter.
- 7. Geben Sie die primären Anmeldeinformationen ein, z. B. Benutzername, Kennwort und Kennwort aktivieren für den IOS-Router, den Sie hinzufügen möchten.
- 8. Klicken Sie auf Fertig stellen, um das Gerät dem Cisco Security Manager hinzuzufügen. Hinweis: In diesem Beispiel wird davon ausgegangen, dass der Benutzer bereits über einen vorkonfigurierten Router verfügt und sich mit den entsprechenden Anmeldeinformationen beim Router anmelden kann.

Primary Credentials	<u></u>			
Username:	cisco1234			
Password:*	******	Confirm:* ********		
Enable Password:	[Confirm:		
NTTP Credentials				
	Use Primary Credentials			
	Username:			
	Password:			
	Confirm:			
HTTP Port:	80			
HTTPS Port:	443			
IPS RDEP Mode:	HTTPS 🔽			
Certificate Common Name:		Confirm:		
RX-Boot Mode	SMP			
		Back Ne	ext Finish	Cancel Help

Wenn im Fenster "Discovery Status" (Erkennungsstatus) "Discovery completed" (Suche abgeschlossen) angezeigt wird, haben Sie dem Cisco Security Manager erfolgreich ein Gerät hinzugefügt. Wenn Sie dem Cisco Security Manager erfolgreich ein Gerät hinzugefügt haben, müssen Sie einen öffentlichen Schlüssel zuweisen, um IPS zu aktivieren.

Status: Dis Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name (%) 172-25.90.91	scovery completed	d with warni	ngs State	Discover	red From
Status: De Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name 172.25.90.91	scovery completed	d with warni	ngs State	Discover	red From
Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name 3 172.25.90.91	Severky © C	iscovery Co	Sate	Discover	red From
Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name 3 172-25.90.91	Severky © C	Ascovery Co	State	Discover	red From
Devices discovered with errors: 0 Discovery Details Type Niame 172-25.90.91	Severiky	Ascovery Co	Rate	Discover	red From
Discovery Details Type Name (7) 172-25.90.91	Severity © C	Ascovery Co	2.ste	Discover	ared From
Type Name 3 172-25.90.91	Severity © C	Ascovery Co	Rate	Discover	red From
(9) 172-25.90.91	0	Ascovery Co	the second second second second		
			impleced with Warnings Live	e Device	
Messages	concernation and a	Severity	Description		
Interfaces wide open for traffic			The following interfaces are ing a new Access-rule on the	e wide open for traffic as there i ese interfaces means that them	is no ACL applied on them. Add e will no longer be such implicit p
Policies discovered		۲	ermission of traffic anymore	80	
Existing policy objects reused		۲	FastEthernet1		
IPS signature policy not discovered.			FastEthernet2 FastEthernet3		
Add Device Successful		۲	FastEthernet4		
		Action			and the state of the file of the
			nfigure an access rule or AC	e interraces need to be wae op 1. accordingly.	pen for all types or trainc, if no
			ľ		

- 9. Navigieren Sie im Menü links zum Konfigurationsbildschirm FlexConfigs.
- 10. Klicken Sie auf der rechten Seite des Bildschirms auf die FlexConfigs-Benutzeroberfläche und anschließend auf das Symbol **Hinzufügen**.

Cinco Security Manager + admin	Connected to '172.25.90.8'	er land and and and and and and and and and	ز امند
Des Eus News Boych Reb Tools	Reb		레이크 및 전 및 전 및 인 및 인 및 인 및 인 및 인 및 인 및 인 및 인
8 9 0 9 8 9 10 1	3 ?		
Devices 🛃 😭	Device: 172.25.90.33 P	alicy: FlawConfigs	
Filter : none 💌	Prepended MexConfig	,	
Compartment Contain Al Societary 172.25.90.39 172.25.90.34	The second	Narke	Description
AAA Rules Access Rules Inspection Rules	Appended FlexConfig		
Transparent Rules Web Pilter Rules B/PS	Peo.	Name	Description
Signatures Event Actions General Settings = Interface Rules			
Site to Site VPN E Remote Access VPN E SSL VPN			
E Interfaces E Platform PresConfep v			Values Provlevi 🖨 🛡 😥 🖀
			Save -

11. Wählen Sie in der Liste "Ausgewählte FlexConfigs" die Option **IOS_IPS_PUBLIC_KEY aus**, und klicken Sie auf **OK**.

			Sector Instant	alianti anatima	Name	a marked and a street of
Filter : none 💉			105	JPS_PUBLI	KEY	
CAT6K_ECLB_portchannel	<u>^</u>					
CAT6K_firewall_multiple_vlan_interfaces						
DIOS_add_bridge_interface_desc						
DIOS_CA_server						
E IOS_compress_config						
105_config_root_wireless_station						
IOS_console_AAA_bypass						
105_Copy_Image	-		_			
105_enable_SSL		>>				
105_FPM	5	<<				
105_IPS_SIGNATURE_CATEGORY	-					
IOS_PKI_with_AAA						
DIOS_set_dock						
105_VOIP_advance						
E IOS_VOIP_simple						
105_VPN_config_gre_tunnel						
105 VPN set interface desc						
IOS_VPN_shutdown_inside_interface						
IOS_VRF_on_vFW						
	¥					
a 🖉						
20						

- 12. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.**Hinweis:** Die IOS_IPS_PUBLIC_KEY FlexConfig enthält die Konfiguration für den öffentlichen Schlüssel.
- 13. Wählen Sie im Menü auf der linken Seite die Option **General Settings (Allgemeine Einstellungen**) unter der Überschrift IPS aus.
- 14. Geben Sie den IPS-Konfigurationsstandort im Flash-Speicher ein. Dies ist der Ort, an dem die IPS-Konfigurationen platziert werden.
- 15. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Clisco Security Manager - admin Co File Foll View Policy Man Tools H	nected to '172.25.90.8'		
	?		
Denkes 😔 🗇	Device: 172.25.90.33 Policy: General Settings		
Fiter: -none v Department Location V AI 172:25:90.30 0 172:25:90.34	Block Traffic when IPS Apply Deny Action on: Ingress Interface SDEE Properties Maximum Subscriptions:* Maximum Alerts:* 200 Maximum Messages:* 200	ingine unavailable	
AAA Rules A Access Rules Dropecton Rules Settings Transparent Rules Web Fiber Rules Dr95 Signatures Exert Actions General Settings NAT Site to Site VPN Remote Access VPN Remote Access VPN Exert Actions Platform Platform Platform	IPS Config Location Properties IPS Config Location: Flash:/ps Max retries: [1 Traeout seconds between retries: 0		
			Save

Hinweis: Stellen Sie sicher, dass das Verzeichnis für den Speicherort bereits im Router-Flash erstellt wurde. Falls nicht, verwenden Sie den Befehl **mkdir <directory_name>**, um das Verzeichnis location zu erstellen.

- 16. Um IPS zu aktivieren, navigieren Sie zu Schnittstellenregeln, aktivieren Sie das Kontrollkästchen **IPS aktivieren**, und klicken Sie dann auf **Zeile hinzufügen**.
- 17. Geben Sie im Dialogfeld IPS-Regel hinzufügen im Feld Regelname einen Namen für die IPS-Regel ein, und klicken Sie dann auf **Zeile hinzufügen**, um die Schnittstellen einzuschließen, auf die IPS angewendet werden soll.

Cisco Security Manager - admin Con	nexted to '172.25.90.8'
ie Edit Yew Balicy Map Ioolis He	p
	? Martin Mart. Mart.
	Darlow 172 25 00 10 Billion Interface Duby
Dences 🔤 🗐	Jerke 17225 90-00 Poky Dikerake Pules
Fiter : - none - w	Tracks WS
	To Deale and Annual Add Innea Statedard (Transford)
Department	Table
a at	
A 172 35 40 31	A00 IPS Rule
C 172 25 90 34	
G mannes	Add/tdt IPS Rule
	Fule Name." (nyod
	AQ Name: Select
	Interface (Direction) Direction
Clause and	
Anna Rules A	
Autorss mars	
E Settings	
C Transport D inc	
Web Filter Rules	
A INS	[Add Dua]
Gisoutures	[mage room]
80 Event Actions	OK Canoel Help
General Settings	
S Interface Rules	
NAT	
Site to Site VPN	
E Remote Access VPN	
B SSL VPN	
E Interfaces	
E Platform	
🖃 FlexConfigs 🔍	

18. Klicken Sie auf das Optionsfeld, das angibt, in welche Richtung die IPS-Regel angewendet werden soll, und klicken Sie dann auf **Auswählen**, um die entsprechenden Schnittstellen

Direction:*				
In	Oout		Both	
Interfaces:*	[Select	
		OK .	Carcel	Help

auszuwählen.

19. Wählen Sie eine Schnittstelle aus der Schnittstellenauswahl-Liste aus, und klicken Sie auf

	Available I	nterfacés:		
	Filter :	none	~	
	D	ot11Radio0		
	S Fi	astEthernet0		
	P F	astEthernet1		
	T F	astEthernet2		
	E Fi	astEthernet3		
	E Fi	astEthernet4		
	V 🖷	ant		
	A	l-Interfaces		
	E	demal		
	I.	ternal		
1	Selected:		 	_
1	vian1			
	41			

20. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Cisco Security Manager - adm	Connected to '172.25.90.8'	x lol.
Elle Edit Yew Bolicy Map Io	i Beb	
* # 🖾 💀 🗗 🕄	3 ?	
	Desire 172 25 30 20 Balay: Interface Dates	
Devices	Device 17223-1035 PolyTakerace Poles	
Fiter : - none - w	To Partie MS	
(the second	No. Bule Name ACI Name	Interface (Paretters)
Department		and duth)
- da Al	1 myter	ard freeda
A 172 15 40 12		
176.45h 70.35		
		a de la d
2 Frend		
AAA Rules		
Access Rules	8	
Inspection Rules		
Settings		
Transparent Rules		
Web Pilter Rules		
E 195		
Signatures		
Event Actions		
E General Settings		
L MAT		
Size to Size VPN		
25 MeHORE ACCESS VPTS		
US JOL VPTN		
E Distant		
100 1001010		

21. Wählen Sie **Extras > IPS-Update anwenden**, um die neuesten IPS-Signaturen zu installieren.



22. Wählen Sie die neueste Signaturdatei aus, und klicken Sie auf

Weiter.

Type: Signatu	re Updates 🐱			Latest Available:	IPS-CS-MGR-sig-S282-req-E1.zip
A STATE OF THE OWNER OWNER OWNER	File	Sig.	Engine	Latest Downloaded:	IPS-CS-MGR-sig-S282-req-E1.zip
IPS-CS-MGR-sig-S	278-req-E1.zip	278	1	Latest Deployed:	IPS-CS-MGR-sig-5282-reg-E1.zp IPS-CS-MGR-sig-5282-reg-E1.zp
IPS-CS-MGR-sig-S	280-req-E1.zip	280	1	Last Checked On:	Apr 19 2007 10:46:37
IPS-CS-MGR-sig-S	282-req-E1.zip	282	1	Last Downloaded On Last Deployed On:	Apr 19 2007 10:45:48 Apr 23 2007 17:56:38
					Check For Updates
					Download Latest Updates
Update Details				1	
File: Description:	IPS-CS-MGR-sig-Si IPS-CS-MGR-sig-Si	282-req-E1.zip 282-req-E1.zip			
Date: Release:	Apr 19 2007 5282	Size: Required Engine Lev	3.8MB vel: E1		

23. Wählen Sie die Geräte aus, auf die das IPS-Update angewendet werden soll, und klicken Sie auf

Select Policies Update will be Applied To	
Apply Updates To:	Devices Assigned to Selected Policies:
Type: Local Signatures Policies 🗸	3 172.25.90.33
Department	-
🗌 🍰 Location	
👻 🗹 🚔 Al	
172.25.90.33	
172 25 90 22	
172.25.90.33	
Select All Decelect All	
Jonet Part Constant Part	
	Back Next Finish Cancel Help

24. Klicken Sie auf **Fertig stellen**, um die Signaturen anzuwenden.

	1000	The local stand strange in the second		Carried Sec.	Ed. In .	Course .	Carlin d	mint
1000	Sub	10 ontions-Red Ontion List	Actions Drock rea Alert	Toformational	Pidesky	Default	true	19
1001	1/16/	IP options-Record Packet Route	Produce Alert	knodemont	1// 601/	Default	11/aBay	10
1002	a	IP options-Timestamp	Produce Alert	Infomiational	100	Default	Ealsa	3
1003	a	IP options Provide s, c, h, tcc	Produce Alert	Infomational	100	Oefault	false	3
1004	0	IP options-Loose Source Route	Produce Alert	Her	100	Oefault	False	100
1095	0	IP options-SATNET ID	Produce Alert	Informational	100/	Oefault	Falsa	(35)
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default	true	100
<								
								1
1005	0	IP options-SATNET ID IP options-Strict Source Route	Produce Alert Produce Alert	Informational High	100	Oefault Default	faise true	111

25. Navigieren Sie zu IPS, und wählen Sie **Signatures (Signaturen)** aus, um die Liste aller Signaturen

Bar David Carry Cart	Trose Geb							
	0 3	?						
Devices		evice: 17	72.25.9	0.33 Policy: Signatures				
FRer : - none		- 18.	r: (no	na -)			C dest	
Department		-	56	Name	×	Santa	E faite	- Consta
Jucation		1000	0	IP antions-Bad Ontion List	Produce Nert	Informational	25	Defailt
Al and the second		(inter	1116	10 million Galari Barlad Barla	11111111111111111111111111111111111111	Addedate 111	11/ 101	(Acced)
G 175-55, 90-30	_	1 Conte	200	IP and inter-Street and	Pinkers Almit	6660000	ten	and
		1000	20	10 optimize Description of a birth	Produce April	and and and a second	100	and
		And a	20	The optimized and the set of the set	Produce reals	1 manual	100	and 1
		1000	20	The operation of the second second	Produce spect	000000	Sec. 1	and a
		19665	16/1	h. abiala Swige (n/ /////////////////////////////////	(/hobros Haur////////////////////////////////////	111 Hiddena	406/11	(balded)
Firemal	^	1005	0	IP options-Strict Source Route	Produce Alert	High	100	Default
AAA Rules		1005	611	Rob cola Bod	() bloghter Helt () () () () ()	111 pholioporte	406/1	(bearder)
Access Rules		1101	0	Unknown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules		1102	0	Impossible IP Packet	Produce Alert	High	100	Default
E Settings		1104	0	IP Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules		110Z	0	RPC 1918 Addresses Seen	Produce Alert	Montainet //	100	(Defect
Web Filter Fulles		1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
Sighabures		1102	1/9	Giaco 305 Interface DoS	Produce Alert	// Medan //	11/18	(hara)
E Event Actions		1102	D X	Girco 305 Interface Do5	Produce Alert	Nedun	1/ 25	Neteo
General Settings		1108	112	Gaco 305 Interface DoS	Produce Alert	Nedun	11/2	Dates
E Interface Rules		1109	112	Gaos 305 Interface DoS	Produce Alert	Nedun	3/10	Default .
NAT		1203	0	IP Frequent Overlap	Denv Packet Inline Produce Alert	monatoral	100	Ortest
Site to Site VPN		1202	0	IP Fragment Overnup - Datagram Too Long	Deny Packet Inline Produce Alert	Hab	100	Defeat
Remote Access VPN		4		a state of the sta	and and an analy and a start			3
JOL VPTS	8 N N	-			and the second	Marco Manda Harrard		m Car
Platform	~					view opdate cever		

26. Wählen Sie **Datei > Senden und Bereitstellen**, um IPS auf dem IOS-Router bereitzustellen.

New Device Col+N	3 ?					
glone Device	Decise 172.0	Can the Country				
Delete Device	Device 172.2	status Parcy signatures				
Save Col+5	- Filter: (- none)	Tenenenenenenen er ander	The state of the second se		
View Changes		×	×	Mathematics and	Apply	Onar
Yekdete	D S	AD Name	Attons	Severar	Fidelity	Source
Sybrit	1000 0	IP options-Bad Option List	Produce Alert	Informational	75	Default
Sugenit and Deploy	1001 0	IP options-Record Pasket Route	Produce Alert	kniskervin /	100	Cutaut
Dgpky	3,002 0	IP options-Timestamp	Produce filert	heckeroict //	100	Outsut
Discard	1003 0	IP options-Fravide s.c.h.tot	Produce sleet	knoteensint ///	100	Catal
Edit Device Groups	1099 0	IP options Loose Source Route	Produce Alert	Hot	100	Outsut
New Device Group	1005 0	IP options-SATNET ID	Produce Alert	knotemotor	100	Outsut
Add Devices to Ggoup	1006 0	IP options-Strict Source Route	Produce Alert	High	100	Default
Str Obi+P	1002 0	111111111/white the set of the se	111111111 trade which 11	Heisteride ////	11/601	/ hickor
tyt Cal+Q	1101 0	Unknown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules	1102 0	Impossible IP Packet	Produce Alert	High	100	Default
E Settings	1104 0	IP Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules	a sute	NFC 1913 Addresses Seen	111111111 Head and 11111111	Meddanieled ////	11/600	/ hickor
Web Filter Pulles	1108 0	IP Pariet with Proto 11	Produce Alert	Hah	100	Defailt
195	10/ 4064	Claim BOS Indestant Dol5	11111111 Sala Shead 11	maan	11116	(hickor)
Signatures +	1100 1	Caro MX Islandara Dat	Burker dard	Contraction (1)	$\mathcal{D}\mathcal{H}$	Sec.
C General Settings	ALMO .	Caro no menarico har	Produce where	and the second s	7.I.U	and a
Interface indes	3196- 2	Cisco Allo anemale poo	PTODACH IDRIT	111 Level	COU.	Carrie
NAT	7105 3	Cado YC2 Weetlade Dd2	Produce Aper	() (parm)	an	carrie
Site to Site VPN	1500 (a)	// he is which contained ////////////////////////////////////	Deny Packet Inine, Produce Alert	11 Jackandord	100/1	(called)
Remote Access VPN	1202 0	IP Fragment Overrun - Datagram Too Long	Deny Packet Inline, Produce Alert	High	100	Default 1
SSL VPN	1			_		>
Interfaces				View Update Level	-	

27. Wählen Sie das Gerät aus, auf dem die Änderungen bereitgestellt werden sollen, und

	2.25.90.33			
1				
	Edit depk	oy method	Add other	devices
		Deploy	Cancel	Help

28. Zeigen Sie den Bereitstellungsstatus an, um zu überprüfen, ob Fehler vorliegen.

		12.15				
Status:		Deployed	d (1 out of 1 devices co	mpleted.)		
Deployment Job Na	me:	admin_jo	b_2007-04-24 10:53:1	0.468		
Devices To be Deplo	oyed:	1				
Devices Deployed 9	With Errors:	0				
eployment Details	(1/1 loaded)				
Device	9	atus	Summary	Method	Config	Transcript
Porce	the summer of the local division of the	Contraction of the local division of the loc	THE PERSON NEW YORK PERSON NEW YOR			
172.25.90.33	SUCCEEDE	D	🔊 Warning: 2	Device	Q2	\$9
172.25.90.33	SUCCEEDE	D	🔊 Warning: 2	Device	ø	ø
172.25.90.33	SUCCEEDE	D	Warning: 2	Device	9	ø
IT2.25.90.33 Mut of Band Change: CL	SUCCEEDE lessages I	D	Severity	Device Description >>>> Difference of file "C:\PR.OG		mp\2007.04.24_10.53. 72 25 90 33 429498
M ut of Band Change: CL peration Successful	SUCCEEDE lessages I	D	Severity	Device Description >>>> Difference of file "C:\PR:OG 15_job_admin_job_2007-04-24 10 7401,dff_archived" and file "C:\PR: 7401,dff_archived" and file "C:\PR:	RA~1\CSCOpx\MDC\te 1_53_10_468\lphase1\1 OGRA~1\CSCOpx\MDC\te DGRA~1\CSCOpx\MDC\te	mpl/2007.04.24_10.53 72_25_90_33_429498 (templ/2007.04.24_10.9
M ut of Band Change: CL peration Successful ig update compilation w	SUCCEEDE lessages 1	D	Severity	Device Description >>>> Difference of file "C:\PR:OG 15_job_admin_job_2007-04-24 10 740\diff_archived" and file "C:\PR:O 15_job_admin_job_2007-04-24 80740\diff_uploaded".	RA~1\(CSCOpx\/MDC\te 053_10_468\\phase1\1 0GRA~1\(CSCOpx\/MDC) 10_53_10_468\\phase1	mp\2007.04.24_10.53 72_25_90_33_429498 [temp\2007.04.24_10.9 [172_25_90_33_42949
M ut of Band Change: CL peration Successful ig update compilation w ig update engine compil	SUCCEEDE lessages I arning lation status	D	Severity	Device Description >>>> Difference of file "C:\PR:OG 15_job_admin_job_2007-04-24 10 740\dff_archived" and file "C:\PR: 3.15_job_admin_job_2007-04-24 80740\dff_uploaded". 9a	RA~1\CSCOpx\MDC\te 1_53_10_468\lphase1\1 0GRA~1\CSCOpx\MDC\ 10_53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_429498 (temp\2007.04.24_10.9 \172_25_90_33_42949
Mut of Band Change: CL peration Successful ig update compilation w ig update engine compil peration Successful	SUCCEEDE lessages I arning lation status	D	Severity	Device Description >>>> Difference of file "C:\PR\OG 15_job_admin_job_2007-04-24 10 740\diff_archived" and file "C:\PR\ 3.15_job_admin_job_2007-04-24 80740\diff_uploaded". -9a >	RA~1\CSCOpx\MDC\te 0_53_10_468\lphase1\1 0GRA~1\CSCOpx\MDC\ 10_53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_429498 (temp\2007.04.24_10.1 \172_25_90_33_42949
M Int of Band Change: CL peration Successful ig update engine compil peration Successful eployment Log	SUCCEEDE lessages I arning lation status	D	Severity	Device Description >>>> Difference of file "C:\PR:OG 15_job_admin_job_2007-04-24 10 740\diff_archived" and file "C:\PR: 3.15_job_admin_job_2007-04-24 80740\diff_uploaded". -9a > Action	RA~1\CSCOpx\MDC\te 1.53_10_468\lphase1\1 0GRA~1\CSCOpx\MDC\te 10_53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_429498 (temp\2007.04.24_10.9 \172_25_90_33_42949
M ut of Band Change: CL peration Successful ig update compilation w ig update engine compil peration Successful eployment Log	SUCCEEDE lessages I arming lation status	D	Severity	Device Description >>>> Difference of file "C:\PR\OG 15_job_admin_job_2007-04-24 10 740\diff_archived" and file "C:\PR\ 3.15_job_admin_job_2007-04-24 80740\diff_uploaded". -9a > Action	RA~1\CSCOpx\MDC\te _53_10_468\lphase1\1 OGRA~1\CSCOpx\MDC\ 10_53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_429498 (temp\2007.04.24_10.1 \172_25_90_33_42949
M Int of Band Change: CL peration Successful ig update engine compil peration Successful eployment Log	SUCCEEDE lessages I arming lation status	D	Severity Severity	Device Description >>>> Difference of file "C:\PR:OG 15_job_admin_job_2007-04-24 10 15_job_admin_job_2007-04-24 30740\diff_uploaded". -9a > kction	RA~1\(CSCOpx\/MDC\te)53_10_468\\phase1\1 0GRA~1\(CSCOpx\/MDC) 10_53_10_468\\phase1 10_53_10_468\\phase1	mp\2007.04.24_10.53 72_25_90_33_429498 (temp\2007.04.24_10.9 \172_25_90_33_42949

Zugehörige Informationen

- <u>Cisco IOS Intrusion Prevention System (IPS) Produkte und Services-Seite</u>
- Erste Schritte mit Cisco IOS IPS mit 5.x-Signaturformat
- Unterstützung für IPS 5.x-Signaturformat und verbesserte Benutzerfreundlichkeit
- <u>Cisco Intrusion Prevention System</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- <u>Technischer Support Cisco Systems</u>