在Cisco IOS IPS中配置安全管理器

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>规则</u> 配置 相关信息

<u>简介</u>

思科安全管理器是思科安全管理套件的一部分,该套件为思科自防御网络提供全面的策略管理和实施。思科安全管理器是用于管理安全的行业领先的企业级应用。Cisco Security Manager可跨思科路由器、安全设备和安全服务模块处理防火墙、VPN和入侵防御系统(IPS)安全服务的配置管理。

有关思科安全管理器功能和优势以及3.1版中的新功能的摘要,请参阅思科安全管理器3.1产品手册 ,网址为

<u>http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd</u> <u>8062bf6e.html</u>。您可以从Cisco.com下载Cisco Security Manager 3.1,网址为 <u>http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app</u>(仅限注册客户)。

本文档介绍如何使用Cisco Security Manager 3.1来执行IOS IPS的初始配置。对于已配置IOS IPS的路由器,客户可以直接使用Cisco Security Manager 3.1来执行调配任务。

注意:Cisco Security Manager 3.1仅支持IOS 12.4(11)T2及更高版本的IOS映像,以便配置IOS IPS。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科安全管理器3.1
- 思科IOS 12.4(11)T2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。 有关文档约定的更多信息,请参考 <u>Cisco 技术提示约定。</u>



要配置IOS IPS,请完成以下步骤:

- 1. 从本地PC运行Cisco Security Manager 3.1客户端。
- 2. 从"文件"菜单中选择"新建设备",以便将设备添加到Cisco Security Manager 3.1。

Gone Deska Editat Device Sive Sive Sive Verv Qanges Yadda Synk Syn	New Device Colefii C	3 ?		
Differ Davia See Coll+S Yeev Qanges Yadata Sybert	gione Device	Device: 172.25.90.91 Pt	icy: PerCortios	
Save Cold-S Prepended PiercConfigs Vero Opriges No. Name Description Sydaka Sydaw Sydaw Sydaw Sydaw Sydaw Sydaw Sydaw No. Name Description Oprior Edit Device Group Add Devices to Opriop Prepended PiercConfigs Edit Device Group Add Devices to Opriop Prepended PiercConfigs Appended PiercConfigs Max Cold-Q No. Name Description Max No. Name Description Mox Name Description Description Statistics No. Name Description Name Description Description Name Prepended PiercConfigs Name Description Name Prepended Pierco	Delete Device			Second in the second state of the second
Vew Oganges Yakata Sybrit Subart and Deplay Opsizer. Opsizer. Byzende Edit Cevice Group Name Description Statem Rules Process Water Image State Roles Presoner Rules Presoner Rules Brade Description Nati State Roles With Breader Access With Braderan Presoner Access With Braderan	Seve Osl+5	Prepended FlexConfig		
Yildet Sylant Sylant Sylant Sylant Sylant Dippin Dippin <th>View Changes</th> <th>Nip.</th> <th>Name</th> <th>Description</th>	View Changes	Nip.	Name	Description
Sgent	Yakiste			
Skjerk and Deploy Diploy Diployder Group Nag Device Group Add Devices to Group Add Devices to Group Dirt Coll+P Ur Dirt Coll+P Dirt Stations Dirt Stations Dirt Stations Dirt Stations Dirt Stations Dirt Dirt <td>Sj.bmt</td> <td></td> <td></td> <td></td>	Sj.bmt			
Digloy Digloy Digloy Bit Device Group Add Devices to Spep Diff ColleQ Interstances Dispection Rules Settings Transparent Rules Web Pitter Rules Web Pitter Rules PBS NAT Ste to Size VFN Storef Access VFN Storef Access VFN PerConfigs	Submit and Deploy			
Egscad Edt Device groups Neg Device Group Add Devices to Group Bit Dispection Nules Setings Insaparent Rules Web Pitter Rules Web Pitter Rules Bit Set to Size WN Sectors Access VFN Siz VeN Siz VeN Percorers Percorers Percorers	Depky			
Edit Oevice Group Herg Device Group Add Devices to Openc Ditt Onle P Transparent Rules Web Pitter Rules PPS NAT Size to Size WN Size to Size WN Size to Size WN Size to Size WN Dittarfaces PietConfigs	Discard			
Nerg Device Group Brit. Colleg Lit Colleg Appended PlexConfigs No. Name Description PBS NAT Size Ios Size VINI Size Ios Size VINI Size Ios Size VINI Description PrevConfigs Values	ER Device Groups			
Add Devices for Goup Bit Coll+Q Twosen waters Dispection Rules Settings Transperent Rules Web Pfiker Pules P5 NAT Size to Size VPN Remote Access VPN Size to Size VPN Size to Size VPN Size form Pleform Pleform Pleform Pleform Pleform	New Device Group.			
Bitt CodeP Egt CodeP Egt CodeP Egt CodeP Inspecton Rules No. Inspecton Rules No. No. Name Description PS NAT State State VPN Remote Access VPN State Access VPN State Access VPN State Access VPN Patrions Prex.Carchage Values Values	Add Devices to Group			
Control Egit Control Egit Description Settings Transperent Rules Web Pitter Rules Web Pitter Rules Web Pitter Rules PS NAT Ste to Ste VFN Issue to Ste VFN Issue to Ste VFN Issue to Ste VFN Interfaces Pleform PrevCarMps Values Values	Date Contrast to agrigue,	1		
Egit Coll+Q Image: mase mase Draperded PlexConfigs Appended PlexConfigs Inansparent Rules Image: mase mase Web Pitter Rules Image: mase mase Image: mase mase Web Pitter Rules Image: mase mase Image: mase mase mase mase Image: mase mase mase mase Image: mase mase mase mase mase mase mase mase	Oaken Coee			
Inspection Rules Inspection Rules Statings Inspection Rules Web Pitter Rules Web Pitter Rules NAT Ste to Site VPN Remote Access VPN Stations Platform Platform Platform Values Values	Egt Cal+Q	Annuclei Ber Carlos		
Mo. Nerve Description If transparent Rules Web Pitter Rules Web Pitter Rules IPS NAT Site to Site VPN Renote Access VPN Site to Site VPN Interfaced Interfaced Platform Platform PrevConNgs	Inspection Rules	Appended HexCorrigs		
Transparent Rules Web Pitter Rules FPS NAT Size to Size VFN Remote Access VFN Essi VFN Essi VFN Enterfaces Fieldform PievCarMags Values Preview	E Settings	State No. and Street	Narre	Description
Web Piter Pules PFS NAT Size to Size VPN Renote Access VPN Si Siz VPN Disterfaces Filaform PierCorNgs	Transparent Rules			
I PS NAT Ste to Ste VFN Remote Access VFN I SSL VFN I Interfaces I Pleform Ple/Cor/Ng: VolueS Preview Preview Preview Preview	Web Filter Pules			
NAT Size to Size VFN Remote Access VFN Size VFN Size VFN Size VFN Filteraces Filteraces Filteraces Volues Preview	1 195			
Ske to Ske VFN Renote Access VFN SSL VFN SSL VFN Deterfaces Flatform Plev.Car/bgs ValueS Preview	JNAT			
I Remote Access VFN I SSL VFN I Drterfaces I Pleform Plev/Car/Ngc Volues Preview	Site to Site VPN			
I SSL VFN I Diterfaces I Pleform Plei/ConNgc Volues Preview	Remote Access VPN			
I Pistform PievCarMgs Values Preview	SSL VPN			
PerCorNgs] Interfaces			
	9 Platform			
Values Proview 🔿 🔿 🖉 🖊 🖻	J PlexContigs			
				Values Preview 🔶 🗣 🗔 🖊 💼
				Several Sev

3. 在New Device(新设备)窗口中,选择要添加设备的方式。本示例从网络添加设备。

ew Device - Choose Method (Step 1 of)	
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	а
When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.	- I
Add New Device	-
You can add a device that is not yet on the network by specifying the device's identifying information and credentials.	-
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 Prov	Cancel Help

4. 单击 **Next**。

5. 输入要添加的设备的身份详细信息。例如,主机名和IP地址。

Identity		
IP Type:	Static 🗸	
Host Name:		
Domain Name:		
IP Address:	172.25.90.91	
Display Name:*	172.25.90.91	
OS Type:*	v	
	105 - 12.3+	
	105 - Catalyst 6500/7600	
Discover Device Se	ettin PIX	
Discover:	IP5	
	ASA	
	Fixewal Policies	
	DPS Policies	
	RA VPN Policies	
	Discover Policies for Security Contexts	

- 6. 单击 **Next**。
- 7. 输入要添加的IOS路由器的主要凭证,如用户名、密码、启用密码。
- 8. 单击**Finish**将设备添加到Cisco Security Manager。**注意:**本示例假设用户已经预配置了路由器,并且可以使用适当的凭证登录路由器。

Primary Credentials			
Username:	cisco1234		
Password:*	*******	Confirm:* *******	
Enable Password:		Confirm:	
HTTP Credentials			
	Use Primary Credentials		
	Username:		
	Password:		
	Confirm:		
HTTP Port:	80		
HTTPS Port:	443		
IPS RDEP Mode:	HTTPS		

当"发现状态"窗口中显示"发现已完成"时,您已成功将设备添加到思科安全管理器。成功将设 备添加到思科安全管理器后,必须分配公钥才能启用IPS。

Status: Discovery comple Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name Severity Operation Severity Operatin the severity Severity	ted with warn	nings State Discovered From Completed with Warnings Live Device
Status: Discovery comple Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Discovery Details Type Name Severity 172-25.90.91 ©	ted with warn	nings State Discovered From Completed with Warnings Live Device
Status: Discovery comple Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0 Xiscovery Details Type Name Severity 172-25.90.91 Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	ted with warn	Trings State Discovered From Completed with Warnings Live Device
Devices to be discovered: 1 Devices discovered successfully: 1 Devices discovered with errors: 0	Discovery Co	State Discovered From Completed with Warnings Live Device
Devices discovered successfully: 1 Devices discovered with errors: 0 Niscovery Details Type Name Severity Type Name Severity T22.25.90.91 Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Discovery Co	State Discovered From Completed with Warnings Live Device
Devices discovered with errors: 0 Discovery Details Type Name Severity 172-25.90.91 Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Discovery Co	State Discovered From Completed with Warnings Live Device
Discovery Details Type Name Severity Type Name Severity Interfaces wide open for traffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Discovery Co	State Discovered From Completed with Warnings Live Device
Type Name Severity Type Name Severity 172.25.90.91 © Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Discovery Co	State Discovered From Completed with Warnings Live Device
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Discovery C	Completed with Warnings Live Device
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful		
Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful	Security	Description
Policies discovered Existing policy objects reused IPS signature policy not discovered. Add Device Successful		The following interfaces are wide open for traffic as there is no ACL applied on them. Add on a new Access-rule on these interfaces means that there will no longer be such implicit on
Existing policy objects reused IPS signature policy not discovered. Add Device Successful		ernission of traffic anymore:
IPS signature policy not discovered. Add Device Successful	۲	FastEthernet1
Add Device Successful	۸	FastEthernet2 FastEthernet3
	۲	FastEthernet4
		Action
		Please verify whether these interfaces need to be wide open for all types of traffic. If not nfigure an access rule or ACL accordingly.

- 9. 从左侧的菜单中,导航至FlexConfigs配置屏幕。
- 10. 单击屏幕右侧的FlexConfigs用户界面,然后单击"添加"**图**标。

Cisco Security Manager + admin	Connected to '172.25.90.8		
Elle Edit Yew Bokcy Map Icols	i Reb		
*****	3 ?		
Devices 🔮 🕄	Device: 172.25.90.33	hakcy: FlexConfigs	
Filter : none	Prepended PlexConfig	2	
 Department Location Al 172.25.90.30 172.25.90.34 	Táo.	Name	Description
AAA Rules Access Rules Inspection Rules (i) Settings	Agoended RexConfig	1	
Transparent Rules Web Pitter Rules BPS Signatures Event Actions General Settings NAT Site to Site VMI E Remote Access VMI EX Site VMI EX Site VMI			
B Exteriaces B Pietlam PresCorigo			Velues) Preview 🔿 🔿 🎯 🖉
			Save

11. 在Selected FlexConfigs列表中,选择IOS_IPS_PUBLIC_KEY,然后单击OK。

CAT6K_ECLB_portchannel CAT6K_firewall_multiple_vlan_interfaces CAT6K_firewall_multiple_vlan_interfaces IOS_add_bridge_interface_desc IOS_CA_server	-	
 IOS_compress_config IOS_config_root_wireless_station IOS_console_AAA_bypass IOS_Copy_Image IOS_enable_SSL IOS_PPM IOS_IPS_SIGNATURE_CATEGORY IOS_PKI_with_AAA IOS_set_clock IOS_VOIP_advance IOS_VOIP_aimple IOS_VPN_config_gre_tunnel IOS_VPN_set_interface_desc IOS_VPN_shutdown_inside_interface IOS_VRF_on_vFW 	>>	

- 12. 单击Save以保存更改。注意:IOS_IPS_PUBLIC_KEY FlexConfig保留公钥的配置。
- 13. 从左侧的菜单中,选择IPS标**题下方**的General Settings。
- 14. 在闪存上输入IPS配置位置。这是IPS配置的放置位置。
- 15. 单击Save以保存更改。

🏦 Cisco Security Manager – admin Ce	onnected to '172.25.90.8'			
Elle Edit View Balicy Map Iools I	Aelo			
	3 ?			
Devkes 😔 🗇	Device: 172.25.90.33 Policy: Gen	eral Settings		
Filter : - none w	D	lock Traffic when IPS er	ngine unavaliable	
Department	Apply Deny Action on: Ing	ess Interface	×	
v (MAL	SDEE Properties			
172.25.90.33	Maximum Subscriptions:* 1			
172.25.90.34	Maximum Alerts:* 20	D		
	Maximum Messages:* 20	0		
	IPS Config Location Propertie			
	IPS Config Location:	Flash:/ps		
AAA Rules	Max retries:	1		
Access Rules	Timeout seconds between retrie	e 0		
Dispection Rules	· · · · · · · · · · · · · · · · · · ·			
Transparent Bules				
Web Filter Rules				
8 195				
🗇 Signatures				
E Event Actions				
General Settings				
CINAT				
Ste to Ste VPN				
Remote Access VPN				
SSL VPN				
Interfaces				
Platform				
Prescarings v				
				Save

注意:确保已在路由器闪存上创建位置目录。否则,请使**用mkdir <directory_name>**命令创 建位置目录。

- 16. 要启用IPS,请导航至Interface Rules,选中Enable IPS复选框,然后单击Add Row。
- 17. 在Add IPS Rule对话框的Rule Name字段中,输入IPS规则的名称,然后单击**Add Row**以包括 必须应用IPS的接口。



18. 单击指示IPS规则必须应用到哪个方向的单选按钮,然后单击**选择**以选择适当的接口。

Direction:*				
OIn	Oout		Both	
Interfaces:*	· · · · · · · · · · · · · · · · · · ·		Select	
	,			
		OK	Cancel	Help

19. 从接口选择器列表中选择接口,然后单击确定。

Interface Selector		
Available Interfaces:		
Filter : none	~	
Dot11Radio0		
FastEthernet0		
FastEthernet1		
FastEthernet2		
FastEthernet3		
FastEthernet4		
Vlant Vlant		
All-Interfaces		
External		
Linternal		
Selected:		
Vlan1		
2		
	Caprel	elo
		οφ.

20. 单击Save以保存更改。



21. 选择Tools > Apply IPS Update以安装最新的IPS签名。

le Edit Yew Balky Map	Look	e Reib			
Derikes	0	Device Properties Pglicy Object Manager Site-To-Site VPN Manager	ace Rules		
Filter : - none - v	•	Deployment Manager Policy Digcovery Status	ACL Name	Interface (Direction)	
Jucation		Show Containment		Wan1 (both)	
👻 🎒 Al	12	Inventory Status			
172.25.90.33	2	Catalyst Summary Info			
172.25.90.34		Device Manager			
	10	IPS Event Vieger			
	<	Apply IPS Lodete			
		Preview Configuration			
		Device OS Management			
AAA Rules	13	Audit Beport			
Access mars		Change Reports			
E Settions		Configuration Archive			
Transparent Rules	-	Backup			
Web Filter Rules	-	Constant Manager Planmadics			
E PS	-	Security Hanager Cragnostics			
Signatures	114	Security Magager Administration			
Event Actions					
General Settings	. 85				
Dinterface Rules					
NAT					
Site to Site VPN					
Revote Access VPN					
SSL VPN					
E Interfaces					
E Platform					
- FlexConfigs					

22. 选择最新的签名文件,然后单击Next。

Ipdates Download	led:			Update Status	
Type: Signat	ure Updates 👻			Latest Available:	IPS-CS-MGR-sig-S282-req-E1.zip
Alassistan investigation	File	Sig.	Engine	Latest Downloaded:	IPS-CS-MGR-sig-5282-req-E1.zip
IPS-CS-MGR-sig-S278-req-E1.zip		278	1	Latest Applied: Latest Deployed:	IPS-CS-MGR-sig-5282-req-E1.zp IPS-CS-MGR-sig-5282-req-E1.zip
IPS-CS-MGR-sig-	5280-req-E1.zip	280	1	Last Checked On:	Apr 19 2007 10:46:37
IPS-CS-MGR-sig-	PS-CS-MGR-sig-S282-req-E1.zp		1	Last Downloaded On: Apr 19 2007 10:45:48 Last Deployed On: Apr 23 2007 17:56:38	
					Check For Updates
					Download Latest Updates
Update Detail	5			1	
File: Description:	IPS-CS-MGR-si IPS-CS-MGR-si	g-5282-req-E1.zip g-5282-req-E1.zip			
Date: Release:	Apr 19 2007 5282	Size: Required Engine Le	3.8MB evel: E1		
			Back	Next	Finish Cancel H

23. 选择必须应用IPS更新的设备,然后单击**Next**。

Type: Local Signatures Policies	3 172.25.90.33
 □ Department □ De	
Select All Deselect All	Back Next Finish Cancel H

24. 单击Finish以应用签名。

m	64	Selected and Marrie Sciences	Artinor	Savartu	Fidality	Saure	Feabled	Dirk
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default	true	18
1001	1/0/	IP options-Record Packet Route	Produce Alert	knoideimorini ///	1// 601/	Default	1/ 1000	1/2/
1092	0	IP options-Timestamp	Produce Alert	Informational	100	Default	Eala	5
1003	0	IP options Provide s, c, h, tcc	Produce Alert	Infomational	100	Oefault	false	3
1004	0	IP options-Loose Source Route	Produce Alert	11/1004/11	100	Oefault	Ealse	100
1005	0	IP options-SATNET ID	Produce Alert	Informational	100/	Oefault	(also	25
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default	true	100
<								

25. 导航到IPS,然后选择**Signatures**以查看所有签名的列表。

Devices	2 🗇	Device: 1	72.25.9	0.33 Policy: Signatures				
Filter : - none 😿		· FRe	r: (no	ne)				
Department		m	SA	Name	×	Ganty	Future	Same
Jucation		1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default /
Al and a second	- 1	1001	116	10 optimum Gar and Partial Durite	111111111111111	Addedite 111	11/001	1 hered
California (140-02)	_	Sec.	20	IP animum Constants	Pinkere Alert	and and a second	001	and a
	_	Sec.	20	10 optimes December 2 h http://	Produce filmt	and and and and and	100	and a
		222	200	1D estimated and Calara Brade	Produce dant	Ser and	100	Sec.
	- 1	1000	20	IP optimized and the state	Constant and	and and a second	See.	1222
		1446	16/11	In the day and the second seco	III. MARTINE IN INCOMENTING	Ull Haldelak	146/11	11990
Frenal	^	1000		The obstacle-party some hanse	Produce wert	rign .	100	Derauk
AAA Rules		frees	16/1	The bear and	Produce Hels	11/ Wednesday	406/1	(baland)
Access Rules		1101	0	Unknown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules		1102	0	Impossible IP Packet	Produce Alert	High	100	Default
8 Settings		1104	0	IP Locathost Source Spool	Produce Alert	High	100	Default
Transparent Rules		11az	0	RPC INTR Addresses Seen	Produce Alert	Anotempini //	100	(Nickel)
Web Filler Hules	- 1	1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
Signatures.	141	1102	1/1	Gaco 305 Interface DoS	Produce Alert	() maden ())	11/18	history !
E Event Actions		1122	112	Gado 305 Jacentace DoS	Produce Alert	Nedun	1/25	Defect
General Settings		1104	112	Gaco 305 Interface DoS	Produce Aiert	Nedun	21/2	Dated
Dinterface Rules		1109	112	Glock 305 Interface DoS	Produce Alert	Nedun	11/20	Orfest
NAT		1203	0	IP fragment Overlag	Denv Packet Inline Produce Aert	monatory	100	Ortest
Site to Site VPN		1202	0	IP Pragment Overrup - Datagram Too Long	Deny Packet Inine Produce Alert	Hab	100	Defeat .
Remote Access VPN	- 1	1			and a sea seat and a seat			3
totarfares		-				Mars 1 Made to 1 mart		
Distions						view Opdate Level		

26. 选择File > Submit and Deploy以在IOS路由器上部署IPS。

New Device Col+N	3 ?				100	
gone Device	Device: 172.25	5.90.33 Policy: Signatures				
Delete Device						
Save Col+2	· Filter: (-	-none)			Look	1000
New Changes	I I I I I	A line line line line line line line line		- Country	Entelley	Energ
Terose	1000 0	R entires-fied Ontion List	Produce Net	Informational	75	Colorit.
Schert and Parks	101 660	111111466666666666	annon a second	Nelskiller III	11166	racen
Sugrit and Leptoy	And a	The observation of the second statement of the second	House Here	Luning	100	Cane !!
Discard	Aller a	in the other constraints	Contract and	Maria a	1 Carl	Canal .
Edit Canalas Canalas	1000 0	In declarationage a c'utrat	Produce spect	(managara	100	(out and
New Device Group	3092 0	IP sptore-Louise source Route	Produce Apert	Her	100	Datacit
Add Devices to Group	5000/6/	// IS abraux-EVINELID	() biodrife where () () () () () () () () () () () () ()	1 soloungoorg	106//	Capatal
Pare Codus	1006 0	IP options-Strict Source Route	Produce Alert	High	100	Default
ta odvo	2002 0	The onto The	Produce Alert	historiational	100	Dataut
County	1101 0	Unknown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules	1102 0	Inpossible IP Packet	Produce Alert	High	100	Default
Settings	1121 0	IP Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules	1192 0	RFC 1918 Addresses Seen	Produce Alert	herioteensint //	100	Dutait
Web Piller Pulles	1105 0	IP Packet with Proto 11	Produce Alert	High	100	Default
C Scoubures	10/ 2011	Claco JOS Interface DoS	Produce Alert	//man///	11/3	history !
Event Actions	1 2011	Gaco IOS Interface DoS	Produce Alert	Medun	S.C.	Outest
General Settings	1109 2	Cisco 305 Interface DoS	Produce filert	Nedan	All	Owfault
Diterface Rules	1109 3	Geo JOS Interface DoS	Produce Ame	Man	11/20	Defect
NAT	1201 0	IP fragment Overlag	Deny Packet Initie, Produce Mert	brokerow.	100	Outsit
Size to Size VPN	1202 0	IP Fragment Overrun - Datagram Too Long	Deny Packet Inline, Produce Alert	High	100	Default
CRL VENI	2					3
Interfaces	-		r	View Literate Level		
Platform				and obview caner		2000

27. 选择要在其上部署更改的设备,然后单击**Deploy**。

	vices		
172.25.9	0.33		
Edit	deploy method	Add oth	er devices
Edit	deploy method	Add oth	er devices

28. 查看部署状态以验证是否存在错误。

ployment Status Details				
proyment status pecans				
Status:	Deployed (1 out of 1 device	s completed.)		
Devices To Be Deployed:	admin_000_2007-04-24 10:5	3:10.400		
Devices Deployed Successfully:	1			
Devices Deployed With Errors:	0			
Deployment Details (1/1 loaded	n			
Device S	tatus Summar	y Method	Config	Transcript
172 25 90 33 SUCCEEDE	A		17	F 2
Transo Jordebe	D warning: 2	Device	\$0	\$
112123-20120	D (J) Warning: 2	Device	99	¢,
172123-20133 SOCIEC	ω <u>(1</u> 2 werning: 2	Device	¢,	Q
Messages	Severity	Description	9	Q
Messages Dut of Band Change: CLI	Severity	Description >>>> Difference of file "C:I/PRO 15 job admin job 2007-04-24	\$0 DGRA~1\CSCOpx\MDC\ter 10 53 10 468\[phase1\1]	\$0 mp\2007.04.24_10.53. 72 25 90 33 4294960
Messages Dut of Band Change: CLI Operation Successful	Severity	Device Description >>>> Difference of file "C:\PR(15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\P	90 DGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\)1 ROGRA~1\CSCOpx\MDC\ 40.63 10_53_10_468((phase1))	mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5
Messages Dut of Band Change: CLI Operation Successful Sig update compilation warning	Severity A D A	Description >>>> Difference of file "C://PRO 15_job_admin_job_2007-04-24 740(jdff_archived" and file "C://P 3.15_job_admin_job_2007-04-2 80740(dff_uploaded".	90 DGRA~1\CSCOpx/(MDC)ter 10_53_10_468\(phase1\)1 ROGRA~1\CSCOpx/(MDC) 4 10_53_10_468\(phase1	\$0 np\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Out of Band Change: CLI Operation Successful Sig update compilation warning Sig update engine compilation status	Severity	Description Descr	90 DGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\1 ROGRA~1\CSCOpx\MDC\ 4 10_53_10_468\(phase1)	************************************
Messages Dut of Band Change: CLI Operation Successful Sig update compilation warning Sig update engine compilation status Operation Successful	D A warning: 2 Severity A 0 A 0 0 0 0	Description Descr	SGRA~1\CSCOpx/MDC(ter 10_53_10_468\\phase1\1 ROGRA~1\CSCOpx/MDC\ 4 10_53_10_468\\phase1'	<pre>%</pre> mp\2007.04.24_10.53, r2_25_90_33_4294980 temp\2007.04.24_10.5 (172_25_90_33_42949)
Messages Dut of Band Change: CLI Operation Successful Sig update engine compilation status Operation Successful Operation Successful Operation Successful	Seventy Seventy () () () () () () () () () () () () ()	Description Descr	SGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\1 ROGRA~1\CSCOpx\MDC\ 4 10_53_10_468\(phase1)	\$0 mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Sig update compilation warning Sig update engine compilation status Operation Successful Deployment Log	Severity Severity (1) (2) (2) (2) (2) (2) (2) (2) (3) (3) (3) (3) (3) (3) (3) (3) (3) (3	Description Descr	SGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\1 ROGRA~1\CSCOpx\MDC\ 4 10_53_10_468\(phase1)	% mp\2007.04.24_10.53, 72_25_90_33_4294980 temp\2007.04.24_10.5 (172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Sig update compilation warning Sig update engine compilation status Operation Successful Deployment Log	Severity A (1) (2) (2) (2) (2) (3) (3) (3) (3) (3) (3)	Description Descr	SGRA~1\CSCOpx/MDC(iter 10_53_10_468\\phase1\1 ROGRA~1\CSCOpx/MDC\ 4 10_53_10_468\\phase1'	<pre>%</pre> mp\2007.04.24_10.53, r2_25_90_33_4294980 temp\2007.04.24_10.5 (172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Sig update engine compilation status Operation Successful Deployment Log	Seventy A () () () () () () () () () () () () ()	Description >>>> Difference of file "C:\PRO 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\P 3.15_job_admin_job_2007-04-2 80740\diff_uploaded". 9a > Action	SGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\1 ROGRA~1\CSCOpx\MDC\ 4 10_53_10_468\(phase1)	\$0 mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Sig update compilation warning Sig update engine compilation status Operation Successful Deployment Log	Severity A (1) (2) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	Description Descr	90 DGRA~1\CSCOpx\MDC\ter 10_53_10_468\(phase1\1 ROGRA~1\CSCOpx\MDC\ # 10_53_10_468\\phase1 4 10_53_10_468\\phase1	<pre>%</pre>

相关信息

- Cisco IOS入侵防御系统(IPS)产品和服务页
- <u>采用 5.x 签名格式的 Cisco IOS IPS 入门</u>
- IPS 5.x签名格式支持和可用性增强
- <u>Cisco Intrusion Prevention System</u>
- <u>安全产品的问题信息通告 (Field Notice) (包括CiscoSecure Intrusion Detection)</u>
- <u>技术支持 Cisco Systems</u>