Configurar o Security Manager no Cisco IOS IPS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Configurar Informações Relacionadas

Introduction

O Cisco Security Manager faz parte do Cisco Security Management Suite, que oferece administração e aplicação abrangentes de políticas para a Cisco Self-Defending Network. O Cisco Security Manager é um aplicativo corporativo líder de mercado para gerenciamento de segurança. O Cisco Security Manager trata do gerenciamento de configuração de serviços de segurança de firewall, VPN e IPS (Intrusion Prevention System) em roteadores, dispositivos de segurança e módulos de serviços de segurança da Cisco.

Para obter um resumo dos recursos e benefícios do Cisco Security Manager, bem como dos novos recursos na versão 3.1, consulte a folha de dados do Cisco Security Manager 3.1 em http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd_8062bf6e.html. Você pode fazer o download do Cisco Security Manager 3.1 do Cisco.com em http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app (somente clientes registrados).

Este documento descreve como usar o Cisco Security Manager 3.1 para executar a configuração inicial do IOS IPS. Para roteadores já configurados com o IOS IPS, os clientes podem usar diretamente o Cisco Security Manager 3.1 para tarefas de provisionamento.

Observação: o Cisco Security Manager 3.1 oferece suporte somente a imagens do IOS 12.4(11)T2 e posteriores para configurar o IOS IPS.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configurar

Conclua estes passos para configurar o IOS IPS:

- 1. Execute o cliente do Cisco Security Manager 3.1 no PC local.
- 2. Escolha **Novo dispositivo** no menu Arquivo para adicionar um dispositivo ao Cisco Security Manager

Cisco Security Manager - admin D le Edit View Policy Map Tools	onnected to '172.25.90.8' Helo	A CONTRACTOR OF THE OWNER	
New Device	2	-	
Gone Device	J 1		
Delete Device	Device: 172.25.90.91 Policy:	: FlexConfigs	
Seve Osl+5	Prepended FlexConfigs		
Vew Changes	No	Name	Description
Yakdate			
Submit			
Submit and Deploy			
Depky			
Discard			
Edt Device Groups			
New Device Group			
Add Devices to Group			
Pirt. Only			
F-2 040			
Carrier Control	Appended PlexConfigs		
Inspection Rules	No.	Name	Description
 Settings 	and the same succession		
Transparent Rules			
Web Filter Pules			
E PS			
NAT			
Distance of the second			
RE SSL VPN			
(i) Interfaces			
E Platform			
PlexCarlings			
			Values Preview 🔶 🔍 😰
			Save

 Na janela Novo dispositivo, escolha como deseja adicionar o dispositivo. Este exemplo adiciona o dispositivo da rede.

New 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	
When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.	
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.	-
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	Pinish Cancel Help

- 4. Clique em Next.
- 5. Insira os detalhes da identidade do dispositivo que deseja adicionar. Por exemplo, nome do host e endereço

IP.

Identity		
IP Type:	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	etting PIX	
Discover:	IP5	
	ASA	
	Pixewal Policies	
	IPS Policies	
	RA VPN Policies	
	Discover Policies for Security Contexts	

- 6. Clique em Next.
- 7. Insira as credenciais principais, como nome de usuário, senha, Enable password (Habilitar senha) para o IOS Router que você deseja adicionar.
- 8. Clique em **Finish** para adicionar o dispositivo ao Cisco Security Manager.**Observação:** este exemplo pressupõe que o usuário já tem um roteador pré-configurado e pode fazer login no roteador com as credenciais apropriadas.

Osername: postori254 Password:* r******* Enable Password: Confirm:* HTTP Credentials Username: Password: Osername: Password: Confirm: HTTP Port: 90 HTTP SPort: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SMMP	Primary Credentials	Firen 1 224		
Password: Confirm: Enable Password: Confirm: HTTP Credentials Use Primary Credentials Username: Password: Password: Confirm: HTTP Port: 80 HTTPS Port: 943 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SNMP	csernane.	CBC01234		
Enable Password: Confirm: Confirm: HTTP Credentials Username: Password: Confirm: Con	Password:*	I	Confirm:*	
HTTP Credentials Use Primary Credentials Username: Password: Confirm: HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:	Enable Password:		Confirm:	
Use Primary Credentials Username: Password: Confirm: HTTP Port: 90 HTTPS Port: 90 HTTPS Port: 91 Exercise Common Name: Confirm: RX-Boot Mode SNMP	NTTP Credentials			
Username: Password: Confirm: HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SNMP		Use Primary Credentials		
Password: Confirm: HTTP Port: 80 HTTPS Port: 943 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:		Username:		
Confirm: HTTP Port: 80 HTTPS Port: 643 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SMMP		Password:		
HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: Confirm: RX-Boot Mode SNMP		Confirm:		
HTTPS Port: [443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: Confirm: RX-Boot Mode SNMP	HTTP Port:	90		
IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: Confirm: RX-Boot Mode	HTTPS Port:	443		
Certificate Common Name: Confirm: Confirm:	IPS RDEP Mode:	HTTPS 💌		
RX-Boot Mode SNMP	Certificate Common Name:		Confirm:	
RAYDOX PROF	DV. Broot Manda	0.00		
	RA-DOOL PRODE	300		

Quando a opção "Descoberta concluída" aparecer na janela Status da descoberta, você adicionou com êxito um dispositivo ao Cisco Security Manager. Depois de adicionar um dispositivo ao Cisco Security Manager com êxito, você deve atribuir uma chave pública para habilitar o IPS.

_	100%		_				
Status:	Discovery complete	ted with warn	ings				
Devices to be discovered:	1						
Devices discovered successfully:	1						
Devices discovered with errors:	0						
Niscovery Details							
Type Name	Severity	-	Rate	nananananana	Discovered	From	
172.25.90.91	0	Discovery Cr	completed with Warnings Li	ve Device			
Messages		Severity	Description				
Messages Interfaces wide open for traffic		Severity	Description The following interfaces a ing a new Access-rule on I	ire wide open for tra	iffic as there is no	o ACL applied on I	them. Addi
Messages Interfaces wide open for traffic Policies discovered		Severity	Description The following interfaces a ing a new Access-rule on emission of traffic anymo	ire wide open for tra these interfaces me tre:	ffic as there is no	o ACL applied on 1 Il no longer be su	them. Addi
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused		Severity (1) (2) (2) (2) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4	Description The following interfaces a ng a new Access-rule on emission of traffic anymo FastEthernet0 FastEthernet1	rre wide open for tra these interfaces me rre:	ffic as there is n ans that there wi	o ACL applied on 1 Il no longer be su	them. Addi ch implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered		Severity	Description The following interfaces a ing a new Access-rule on I emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3	ire wide open for tra these interfaces me ire:	iffic as there is no	o ACL applied on I Il no longer be su	them. Addi ch implicit p
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity	Description The following interfaces a ng a new Access-rule on 1 emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Dat110 adu0	ire wide open for tra these interfaces me ire:	ific as there is n ans that there wi	o ACL applied on 1 Il no longer be su	them. Addi /
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Severity	Description The following interfaces a ng a new Access-rule on I emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Fuelt10 used Action Reserved users to the the the	re wide open for tra these interfaces me re:	ffic as there is n ans that there wi	o ACL applied on 1 Il no longer be sur	them. Addi / A ch implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity (1) (2) (2) (2) (2) (2) (2) (2) (2	Description The following interfaces a ng a new Access-rule on I emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEther	re wide open for tra these interfaces me re: se interfaces need i ACL accordingly.	ffic as there is no ans that there will to be wide open f	o ACL applied on t I no longer be sur for all types of tra	them. Addi / h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity (1) (1) (2) (2) (2) (2) (2) (2) (2) (2	Description The following interfaces a ng a new Access-rule on I emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 PastEthernet4 PastEthernet4 PastEthernet4 Please verify whether the nfigure an access rule or	ire wide open for tra these interfaces me ire: ise interfaces need 1 ACL accordingly.	iffic as there is no ans that there will to be wide open i	o ACL applied on I Il no longer be sur for all types of tra	them. Addi , ch implicit p ffic. If not, c
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Severity	Description The following interfaces a ng a new Access-rule on 1 emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEther	ire wide open for tra these interfaces me ire: ise interfaces need t ACL accordingly.	iffic as there is no ans that there will to be wide open f	o ACL applied on 1 Il no longer be su for all types of tra	them, Addi / ch implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity	Description The following interfaces a ng a new Access-rule on 1 emission of traffic anymo FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEther	re wide open for tra these interfaces me re: ise interfaces need i ACL accordingly.	iffic as there is no ans that there will to be wide open f	o ACL applied on 1 Il no longer be sur for all types of tra	them. Addi A

- 9. No menu à esquerda, navegue até a tela de configuração FlexConfigs.
- 10. Clique na interface do usuário FlexConfigs no lado direito da tela e clique no ícone Add.

Cisco Security Manager - admin	Connected to '172.25.90.8		
ile Edit Yew Bolicy Map Iook	i Help		
	3 ?		
Denkes 😔 🕄	Device: 172.25.90.33	hakey: FlewConfigs	
Filter : none	Prepended PlexConfig	2	
 Department. Location Al 172.25.90.53 172.25.90.34 	Filo.	Name	Description
AAA Rules Access Rules Dispection Rules	Appended RevCon/kg	8	
00 Settings	And No. 111	and an entry Name	provide an object of the state of the Description in an object of the state of the state
Under Dates			
The second secon			
C Smatters			
D Frank Artister			
Consul Setting			
Listerface Dates			
That			
C State State 1014			
ER Remote Access VEN			
ED 00 100			
III Madaras			
C Platform			Values Preview A A Values
Centurin			
			14/01

11. Na lista Seleted FlexConfigs, escolha IOS_IPS_PUBLIC_KEY e clique em OK.

			Silver Incentivity	Name	and a strength
Filter : none v			105_IPS	PUBLIC_KEY	
CAT6K_ECLB_portchannel	^				
CAT6K_firewall_multiple_vlan_interfaces					
105_add_bridge_interface_desc					
105_CA_server					
105_compress_config					
105_config_root_wireless_station					
IOS_console_AAA_bypass					
105_Copy_Image	-		_		
105_enable_SSL		>>			
IOS_FPM	5	<<			
105_IPS_SIGNATURE_CATEGORY	-				
IOS_PKI_with_AAA					
105_set_dock					
IOS_VOIP_advance					
IOS_VOIP_simple					
105_VPN_config_gre_tunnel					
IOS_VPN_set_interface_desc					
IOS_VPN_shutdown_inside_interface					
IOS_VRF_on_vFW					
	*		1		
2					

- 12. Clique em **Salvar** para salvar as alterações.**Observação:** o IOS_IPS_PUBLIC_KEY FlexConfig mantém a configuração para a chave pública.
- 13. No menu à esquerda, escolha **General Settings (Configurações gerais)** localizadas abaixo do cabeçalho IPS.
- 14. Digite o local da configuração do IPS na flash. Esse é o local em que as configurações de IPS são colocadas.
- 15. Clique em **Salvar** para salvar as alterações.

🚉 Cisco Security Manager - admin Co	nected to '172.25.90.8'	
Ele Edit Yew Balicy Map Icols H	+b	
	?	
Devices 😔 🗇	Device: 172.25.90.33 Policy: General Settings	
Fiter: -none v Department Location V () Al () 172:25:90.33 () 172:25:90.33	Block Traffic when IPS engine unavailable Apply Deny Action on: Ingress Interface SDEE Properties Maximum Subscriptions:* 1	
g manual	Maximum Alerts:* 200 Maximum Messages:* 200 IPS Conflig Location Properties	
AAA Rules	IPS Config Location: Flash:/ps Max retries: 1 Timeout seconds between retries: 0	
Settings Transparent Rules Web Filter Rules IPS Signatures		
Concernal Settings		
Ste to Ste VPN Remote Access VPN S SSL VPN S Interfaces Platform		
Disectande A		Save

Observação: verifique se o diretório de local já foi criado na flash do roteador. Caso contrário, use o comando **mkdir <diretory_name>** para criar o diretório de localização.

- 16. Para habilitar o IPS, navegue até Regras de interface, marque a caixa de seleção **Habilitar IPS** e clique em **Adicionar linha**.
- 17. Na caixa de diálogo Adicionar regra de IPS, digite um nome para a regra de IPS no campo Nome da regra e clique em **Adicionar linha** para incluir as interfaces nas quais o IPS deve ser

aplicado.

Cisco Security Manager - admin Conn	exted to '172.25.90.0'	JDI.
Sie Edit View Bolicy Map Iools Help		
	?	
Denkes 🛃 🗇 🗈	evice: 172.25.90.33 Policy: Interface Rules	
Filter : - none - v	I Frankla 185	
Department	No. Rule Name ACL Name Interface (Direction)	
Jucation		
- (3) AL		
172.25.90.33	ADD IPS Rule	
172.25.90.34	Add/Edit IPS Rule	
	Rule Name:* mybol	
	A/I Name	
	Martine Martine	
	Ditertace (Deection) Deection	
AAA Rules		
Access Rules		
Dispection Rules		
Settings		
Transparent Pules		
Web Filter Rules		
	Add Row	
>) Signatures	Car Carel Link	
E Evere Actions	UN UNIT INT	
Citativa Davi		
CINAT		
Ste to Ste VPN		
Remote Access VPN		
B SSL VPW		
E Interfaces		
E Platform		
FlexConfigs		

18. Clique no botão de opção que indica em que direção a regra de IPS deve ser aplicada e clique em Select para escolher as interfaces

Direction:*				
OIn	Out		Both	
Interfaces:*	ſ		Select	
	Г	or	Carcel	Help

19. Escolha uma interface na lista Seletor de interface e clique em

Filter :	none	*	
D	ot11Radio0		
W F	astEthernet0		
• F	astEthernet1		
E F	astEthernet2		
P F	astEthernet3		
	astEthernet4		
	lan1 Listerfacer		
	vternal		
	aternal		
Selected: Vlan1			
₽.)		

20. Clique em **Salvar** para salvar as alterações.



21. Escolha **Tools > Apply IPS Update** para instalar as assinaturas IPS mais recentes.



22. Escolha o arquivo de assinatura mais recente e clique em

Avançar.

Updates Downloade	ed:			Update Status	
Type: Signatu	re Updates 🛛 🗸			Latest Available:	IPS-CS-MGR-sig-S282-req-E1.zip
And the second second	File	Sig.	Engine	Latest Downloaded:	IPS-CS-MGR-sig-5282-req-E1.zip
IPS-CS-MGR-sig-S	278-req-E1.zip	278	1	Latest Applied: Latest Deployed:	IPS-CS-MGR-sig-S282-req-E1.2p IPS-CS-MGR-sig-S282-req-E1.2p
IPS-CS-MGR-sig-S	280-reg-E1.zip	280	1	Last Checked On:	Are 10 2007 10:46:27
				Last Downloaded On:	Apr 19 2007 10:46:37
PS-CS-MGR-SIG-S	282-req-£1.2p	282	1	Last Deployed On:	Apr 23 2007 17:56:38
					Check For Updates
					Download Latest Updates
Update Details				1	
File: Description:	IPS-CS-MGR-sig IPS-CS-MGR-sig	5282-req-E1.zp			
Date:	Apr 19 2007	Size:	3.8MB		
Release:	5282	Required Engine Le	evel: E1]	
			Radi	Next	and Cancel H

23. Escolha os dispositivos nos quais a atualização do IPS deve ser aplicada e clique em **Avancar**.

Type: Local Signatures Policies	Pervices Assigned to belected Policies:
 Department Location All 172.25.90.33 172.25.90.33 	
Select All Deselect All	Back Next Finish Cancel He

24. Clique em **Finish** para aplicar as assinaturas.

			*	×			нррку	0
ID	Sub	Name	Actions	Severity	Fidelity	Source	Enabled	Risk
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default	true	18
1001	0	IP options-Record Packet Route	Produce Alert	Infomiational	100	Cetaut	(also)	1/25/
1002	0	IP options-Timestamp	Produce Alert	Infomiational	100	Default	(also	13
1003	0	IP options Provide s, c, h, tcc	Produce Alert	Informational	100	Oefault	(false)	3
1004	0	IP options-Loose Source Route	Produce Alert	Hep	100	Oefault	(alsa	100
1095	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
<								
								1

25. Navegue até IPS e escolha **Assinaturas** para exibir a lista de todas as assinaturas.

sikes 💽 🗄	Device: 17						
HT 1 - DODA - 14		2.25.9	1.33 Policy: signatures				
a	· FRe	r: (no	ne)				1
g Department		5.6	· ·	×	Gart	PCCH	Con a
Jucation	1000	0	IP antique Bad Ontion List	Produce Next	Informational	75	Default
	1000	1110		11111111144444	111/22/22/2017	11/100	TACKA
172.25.90.33	1 and	20	Contraction and Contraction of Contr	Produce Amer	1992 Carlos	and li	1220
	1000	211	Is about anesand	Produce April	monadora	100	Carry
	10502	611	Propriors-Provide scondic	Produce wert	managar	100	Conser
	1002	8	JP options-Loose Source Route	Produce Apert	11442	100	Conser.
	1002	6/1	16 abrous 24 WELTD	[Produce Amrt]]]]]]]	11/ pulouingoug	106/1	Galara
interest A	1905	0	IP options-Strict Source Route	Produce Alert	High	100	Default
AAA Rules	1002	0/1	IPv6 over IPv4	Produce Alert	hronistord	100	Detail
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 Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules	Safe	1/1	RPC INTR Addresses Seen	Produce Alert	Anoteenote //	100	hieros)
Web Filter Rules	1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
7 Sectors	1104	111	Gaco 305 Interface DoS	(Produce Alert () () () () ()	11 mbs (1)	1118	Acres 1
E Event Actions	1109	112	Girco 305 Interface DoS	Produce Alert	Hedun	11 al	Defeat
General Settings	1104	112	Girco 305 Interface Do5	Produce Nert	Hedun	31/20	Owland
Interface Rules	1109	397	Gion 305 Interface Do5	Prinduce diert	Hedan	200	Ortest
NAT	Test 1	20	10 Francest Charles	Denis Partiel Inline Doublese Alert	And and and a second	m	and
Site to Site VPN	1202	000	ID Resmant Courses to Dataset and Long	Dany Parket John Dook on Alert	mann	100	CULLER !!
Remote Access VPN	1000		Pringham Orenan's bacagrain nos cong	neid verver simelvinnere weir		100	1000
SSL VPTN	12.000						

26. Escolha **File > Submit and Deploy** para implantar o IPS no roteador IOS.

Sew Device Col+N	3	?						
Delete Device	1	Nevice: 1	72.25.9	3.33 Policy: Signatures				
Saun Oulus	П	- Filte	r ((m)				
Ven Changes		-			~		Acoly	Oner
Validate		ID.	Sub	Nane	Adtons	Severky	Fidelity	Source
Submit		1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default
Submit and Depkoy	H.	1000	1116	IP options Record Packet Route	() Produce Alert () () () () ()	kniskiering ///	1// 605	Auto)
Depky	11	1002	112	IP options-Timestamp	Produce filert	herothererold	100	Outaut
Discard	н	1003	0	P options-Fravide s.c.h.tct	Produce diert	Informational	100	Cufault
Edit Device Groups		1004	18	IP options Loose Source Route	Produce Alert	Hot	100	Ordent
leg Device Group		1005	211	IP options GATNET ID	Produce filert	Informational	100	Outsut
Add Devices to Ggoup		1006	000	P options-Shirt Sauce Raite	Produce Alert	Hoh	100	Default
39% ObleP		1007	1116	Bedder Bed (11111111111111111	unnin hall all all all all all all all all al	Sectements (111)	11/606	1 seco
tyt Col+Q		1101	000	Unincen IP Protocol	Produce Alert	Informational	14000	Defailt
Temestes Rules	1	1102	0	Incossile & Parket	Produce Alert	Hab	100	Defail
E Settinos	1	1104	0	Disrabat Sagra Sagra	Drockute Alert	Herb.	100	Colard
Transparent Rules		(state	in	11111111111111111111111111111111111111	11111111111111111111111111111111111111	1111 Jackardala	11166	1ALLAN
Web Filter Rules		1100	1600	in the state of the second sec	Inder Mat	mand	166011	(mm)
195		1198	in	Prese were berling	Produce rear	1111 MALLING	Sum	(alles)
Signatures	11	TTAG	EU.	CBO ICS INSERTION DOS	HODICE MALE	all and the	COU	Carson
Event Actions		7105	20	Caso Jus aneerace pes	Produce Here	1 bear	am	Caland
T Interface Rules		1105	199	cisco pro asseriace pos	Produce siert	() (seared))	BUI	Carrie .
NAT		7705	12	Carco Jus Interface Dos	Produce April	() Noaru ()	200	Caland
Site to Site VPN	1	1500	1611	The Extension Contactor () () () () () () () () () (Deny Packet Inine, Produce Alert	11 papalingoorg	100	Calant
Remote Access VPN		1202	0	IP Fragment Overrun - Datagrain Too Long	Deny Packet Inline, Produce Alert	High	100	Default 1
SSL VPN		<		-				>
Interfaces						View Update Level		

27. Escolha o dispositivo no qual deseja implantar as alterações e clique em

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

28. Visualize o status da implantação para verificar se há erros.

pioyment status Details					
			_		
	12.00	de la facterat die La ethet Hat Helen 11			
Status:	Deployed (1	1 out of 1 devices co	mpleted.)		
Deployment Job Name:	admin_300_2	2007-04-24 10:53:10	3.468		
Devices Deployed Successfully	. 1				
Devices Deployed With Errors:	0				
Deployment Details (1/1 load	ed)				
Device	Status	Summary	Method	Config	Transcript
172.25.90.33 SUCCEE	DED	Warning: 2	Device	5	50
Massanas		Caucardiu	escription		
Messages Dut of Band Change: CLI		Severity	escription >>>> Difference of file "C:\/PR/OGRA-	1\CSCOpx/MDC\ten	pl2007.04.24_10.53.
Messages Dut of Band Change: CLI Deperation Successful		Severity	escription >>>> Difference of file "C:\PROGRA~ 5_job_admin_job_2007-04-24 10_53_ 40\diff_archived" and file "C:\PROGR/	1\CSCOpx/MDC\ten 10_468\\phase1\17 A~1\CSCOpx\MDC\t	p\2007.04.24_10.53, 2_25_90_33_4294980 emp\2007.04.24_10.5
Messages Out of Band Change: CLI Operation Successful Sq update compilation warning		Severity	escription >>>> Difference of file "C:\PROGRA- 5_job_admin_job_2007-04-24 10_53 /40\diff_archived" and file "C:\PROGR/ 1.15_job_admin_job_2007-04-24 10_5 00740\diff_uploaded".	1\CSCOpx\MDC\tem 10_468\\phase1\17 A~1\CSCOpx\MDC\t 3_10_468\\phase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\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 statu	5	Severity	escription >>>> Difference of file "C:\PROGRA~ 5_job_admin_job_2007-04-24 10_53 40\diff_archived" and file "C:\PROGR/ 1.15_job_admin_job_2007-04-24 10_5 0740\diff_uploaded".	1\CSCOpx\/MDC\ten 10_468\\phase1\17 A~1\CSCOpx\/MDC\t 3_10_469\\phase1\	p\2007.04.24_10.53; 2_25_90_33_4294980 emp\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 statu Deerwition Successful	5	Severity	escription >>>> Difference of file "C:\PROGRA 5_job_admin_job_2007-04-24 10_53 40\dff_archived" and file "C:\PROGRJ 1.15_job_admin_job_2007-04-24 10_5 0740\dff_uploaded". -9a	1\CSCOpx\MDC\ten 10_468\lphase1\17 A~1\CSCOpx\MDC\t 3_10_468\lphase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\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 statu Operation Successful Declarament Los	15	Severity Severity Severity	escription >>>> Difference of file "C:\PROGRA- 5_tob_admin_tob_2007-04-24 10_53 40\dff_archived" and file "C:\PROGR/ 1.15_tob_admin_tob_2007-04-24 10_5 0740\dff_uploaded". -9a > ction	1\CSCOpx\/MDC\tem 10_468\\phase1\17 A~1\CSCOpx\/MDC\t 3_10_468\\phase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\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 statu Operation Successful Deployment Log	5	Severity C C C C C C C C C C C C C	escription >>>> Difference of file "C:\PROGRA~ 5_job_admin_job_2007-04-24 10_53 40\diff_archived" and file "C:\PROGR/ 15_job_admin_job_2007-04-24 10_5 0740\diff_uploaded". -9a - ction	1\CSCOpx\/MDC\ten 10_468\\phase1\17 A~1\CSCOpx\/MDC\t 3_10_468\\phase1\	p\2007.04.24_10.53, 2_25_90_33_4294980 emp\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 statu Operation Successful Xeployment Log	5	Severity	escription >>>> Difference of file "C:\PROGRA- 5_job_admin_job_2007-04-24 10_53 40\dff_archived" and file "C:\PROGRA 1.15_job_admin_job_2007-04-24 10_5 0740\dff_uploaded". -9a ction	1\CSCOpx\MDC\ten 10_468\lphase1\17 A~1\CSCOpx\MDC\t 3_10_468\lphase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\2007.04.24_10.5 172_25_90_33_42949
Messages Out of Band Change: CLI Operation Successful Rig update compilation warning Rig update engine compilation statu Operation Successful Operation Successful	5	Severity Severity Severity	escription >>>> Difference of file "C:\PROGRA- 5_job_admin_job_2007-04-24 10_53 /40\diff_archived" and file "C:\PROGRA 1.15_job_admin_job_2007-04-24 10_5 0740\diff_uploaded". -9a > ction	1\CSCOpx\MDC\ten 10_468\uphase1\17 A~1\CSCOpx\MDC\t 3_10_469\uphase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\2007.04.24_10.5 172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Big update compilation warning Big update engine compilation statu Operation Successful Deployment Log	5	Severity C Severity C S S S S S S S S S S S S S	escription >>>> Difference of file "C:\PROGRA- 5_job_admin_job_2007-04-24 10_53 40\diff_archived" and file "C:\PROGR/ 1.5_job_admin_job_2007-04-24 10_5 10740\diff_uploaded". -9a ction Refrect	1\CSCOpx\/MDC\ten 10_468\\phase1\17 A~1\CSCOpx\/MDC\t 3_10_468\\phase1\	p\2007.04.24_10.53. 2_25_90_33_4294980 emp\2007.04.24_10.5 172_25_90_33_42949

Informações Relacionadas

- Página de produtos e serviços do Sistema de prevenção de intrusão (IPS Intrusion Prevention System) do Cisco IOS
- Introdução ao Cisco IOS IPS com formato de assinatura 5.x
- Suporte ao formato de assinatura IPS 5.x e aprimoramentos de usabilidade
- <u>Cisco Intrusion Prevention System</u>
- Avisos de campo do produto de segurança (incluindo CiscoSecure Intrusion Detection)
- <u>Suporte Técnico Cisco Systems</u>