Configurare Security Manager in Cisco IOS IPS

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Informazioni correlate

Introduzione

Cisco Security Manager fa parte di Cisco Security Management Suite, che fornisce l'amministrazione e l'applicazione complete delle policy per Cisco Self-Defending Network. Cisco Security Manager è un'applicazione di classe enterprise leader del settore per la gestione della sicurezza. Cisco Security Manager gestisce la configurazione dei servizi di sicurezza firewall, VPN e Intrusion Prevention System (IPS) su router, appliance di sicurezza e moduli dei servizi di sicurezza Cisco.

Per un riepilogo delle funzionalità e dei vantaggi di Cisco Security Manager, nonché delle nuove funzionalità della versione 3.1, consultare il data sheet di Cisco Security Manager 3.1 all'indirizzo <u>http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd</u> <u>8062bf6e.html</u>. È possibile scaricare Cisco Security Manager 3.1 da Cisco.com all'indirizzo <u>http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app</u> (solo utenti <u>registrati</u>).

In questo documento viene descritto come usare Cisco Security Manager 3.1 per eseguire la configurazione iniziale di IOS IPS. Per i router già configurati con IOS IPS, i clienti possono utilizzare direttamente Cisco Security Manager 3.1 per le attività di provisioning.

Nota: Cisco Security Manager 3.1 supporta solo immagini IOS versione 12.4(11)T2 e successive per configurare IOS IPS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

Completare questa procedura per configurare IOS IPS:

- 1. Eseguire il client Cisco Security Manager 3.1 dal PC locale.
- 2. Per aggiungere un dispositivo a Cisco Security Manager 3.1, scegliere **Nuovo dispositivo** dal menu

=ile.				
🏥 Cisco Security Manager - admin	Connected to '172.25.90.8'			
Ele Edit Yew Balicy Map Iook	Rep			
Sew Device Criefs	3 ?		TRANSFORMER TO AND ADDRESS OF	
gione Device	Device 172.25.90.91 Br	ing RecCodes		
Delete Device				
Sava Cal+S	Prepended PlexConfigs			
View Changes	No.	Name	Street, Street	Description
Yeldate				
Sybrit				
Sugenit and Deploy				
Dępky				
Discard				
Edit Device Groups				
Neg Device Group				
Add Devices to Group				
Bitt Oslap				
E.R., Col+Q				
- PR. (855 #1.865	Appended PlexConfigs			
Dispection Rules	No.	Name	and the second se	Description
E Settings				
Transparent Rules				
Web Pilter Pulles				
CIANT				
G Ste to Ste VEV				
E Remote Access VPN				
E SSL VPN				
S Interfaces				
Platform				
PlexCariligs				
				Values Preview 🔄 🗣 文 📋
				Save

 Nella finestra Nuovo dispositivo, scegliere come si desidera aggiungere il dispositivo. In questo esempio viene aggiunto il dispositivo dalla rete.

Thew 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.	- T	
Add New Device	- 16	
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 Niext F	Insh Cancel H	leip

- 4. Fare clic su Next (Avanti).
- 5. Immettere i dettagli di identità per il dispositivo che si desidera aggiungere. Ad esempio, nome host e indirizzo 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. Fare clic su Next (Avanti).
- 7. Immettere le credenziali primarie, ad esempio il nome utente, la password e la password di abilitazione per il router IOS che si desidera aggiungere.
- 8. Per aggiungere il dispositivo a Cisco Security Manager, fare clic su **Finish** (Fine).**Nota:** nell'esempio si presume che l'utente abbia già un router preconfigurato e possa accedere al router con le credenziali corrette.

Username: cisco1234 Password:* confirm: ******* Enable Password: Confirm: ******* HTTP Credentials Username: Password: Confirm: HTTP Port: 80 HTTPS Port: 443 PS RDEP Mode: HTTPS K Certificate Common Name: Confirm: Confirm:	Primary Credentials			
Password:* ******** Enable Password: Confirm: HTTP Credentials Use Primary Credentials Username: Password: Confirm: HTTP Port: #0 HTTPS Port: #43 IPS RDEP Mode: HTTPS Certificate Common Name: RX-Boot Mode SMP	Username:	cisco1234		
Enable Password: Confirm: HTTP Credentials Use Primary Credentials Username: Password: Confirm: HTTP Port: 80 HTTP Sport: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:	Password:*	******	Confirm:* ******	
HTTP Credentials Username: Password: Confirm: HTTP Port: 80 HTTPS Port: 443 PS RDEP Mode: HTTPS Certificate Common Name: Confirm:	Enable Password:		Confirm:	
Use Primary Credentials Username: Password: Confirm: HTTP Port: 80 HTTP Sport: 91 P43 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SMPL	HTTP Credentials			
Username: Password: Confirm: HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: Confirm:		Use Primary Credentials		
Password: Confirm: HTTP Port: 90 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:		Username:		
HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:		Password:		
HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:		Confirm:		
HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SNMP	HTTP Port:	80		
IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: RX-Boot Mode SNMP	HTTPS Port:	443		
Certificate Common Name: Confirm: RX-Boot Mode SNMP	IPS RDEP Mode:	HTTPS		
RX-Boot Mode SNMP	Certificate Common Name:	1	Confirm:	
RX-Boot Mode SNMP				
	RX-Boot Mode	SMP		

Quando nella finestra Discovery Status viene visualizzato "Discovery completed" (Rilevamento completato), è stata aggiunta una periferica a Cisco Security Manager. Dopo aver aggiunto correttamente un dispositivo a Cisco Security Manager, è necessario assegnare una chiave pubblica per abilitare IPS.

	The second second						
-	100%		_				
Status:	Discovery comple	ted with warn	inos				
Devices to be discovered:	1						
Devices discovered successfully:	1						
Devices discovered with errors:	0						
Discovery Details							
Type Name	Severity	a mananananana	Rate	Innantanananana	Discovered	From	
172.25.90.91	0	Discovery C	ompleted with Warnings	Live Device			
Messages		Severity	Description				
Messages Interfaces wide open for traffic		Severity	Description The following interface ng a new Access-rule	s are wide open for	traffic as there is r	no ACL applied on t	hem. Addi
Messages Interfaces wide open for braffic Policies discovered		Severity	Description The following interface ng a new Access-rule i emission of traffic any ExetEtheoreth	is are wide open for on these interfaces i more:	traffic as there is r reans that there w	no ACL applied on t ill no longer be suc	them. Addi h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused		Severity @ @	Description The following interface ng a new Access-rule i emission of traffic any FastEthernet0 FastEthernet1	is are wide open for on these interfaces i more:	traffic as there is r nears that there w	no ACL applied on t ell no longer be suc	hem. Addi /
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered		Severity (1) (2) (2) (2) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4	Description The following interface ing a new Access-rule i ermission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3	is are wide open for in these interfaces i more:	traffic as there is n nears that there w	no ACL applied on t ill no longer be suc	them. Addi /
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Seventy	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Dualt 10 adu0	is are wide open for on these interfaces i more:	traffic as there is r nears that there w	no ACL applied on t ill no longer be sud	them. Addi /
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Severity (C) (C) (C) (C) (C) (C) (C) (C)	Description The following interface ng a new Access-rule emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5	is are wide open for on these interfaces i more:	traffic as there is n nears that there w	no ACL applied on t ell no longer be suc	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) (2) (2) (2) (2) (2) (3) (3) (4) (4) (5) (4) (5) (4) (5) (4) (5) (5) (5) (5) (5) (5) (5) (5	Description The following interface ing a new Access-rule i emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet6 FastEthernet6 FastEthernet6 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet8 Fa	is are wide open for in these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t ill no longer be suc	them. Addi h implicit p fic. If not, c
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity (i) (i) (i) (i) (i) (i) (i) (i)	Description The following interface ng a new Access-rule of ermission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Point in aduo Action Please verify whether nfigure an access rule	is are wide open for on these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ad to be wide open	no ACL applied on t ill no longer be suc for all types of tra	them. Addi h implicit p fric. If not, o
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Seventy (a) (b) (c) (c) (c) (c) (c) (c) (c) (c	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet6 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet8 F	is are wide open for on these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t ill no longer be suc for all types of tra	them, Add / h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful	•	Sevenity © © @	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 F	is are wide open for in these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t all no longer be suc for all types of tra	them. Add A h implicit p

- 9. Dal menu a sinistra, passare alla schermata di configurazione di FlexConfigs.
- 10. Fare clic sull'interfaccia utente di FlexConfigs sul lato destro dello schermo, quindi fare clic sull'icona

Aggiungi.

Cisco Security Manager - admin	Connected to '172.25.90.8'		
se for new Forch Heb Toos	Reb		
	-3 7		
Devikes 🛃 🔂	Device: 172.25.90.33	takçı: FlexConfigs	
Filter : - none - 🐨	Prepended MexConfig	,	
 Department. Location Al 172.25.90.33 172.25.90.34 	Pio.	Name	Description
AAA Pules Access Rules Access Rules Inspection Rules (i) Settings	Appended FlexConfig	5 Name	Description
Transparent Rules Web Filter Rules Signatures Event Actions General Settings Interface Rules NAT Site to Site VPN			
E Remote Access VPN E S3L VPN E Interfaces E Refigm Precorige			Values Prevlew 🔿 🗢 😥 😭

11. Nell'elenco FlexConfigs selezionati, scegliere IOS_IPS_PUBLIC_KEY, quindi fare clic su OK.

CAT6K_ECLB_portchannel CAT6K_Firewal_multiple_vlan_interfaces IOS_cAgerver IOS_config_not_wireless_station IOS_console_AAA_bypass IOS_console_AAA_bypass IOS_copy_Image IOS_copy_Image IOS_PPM IOS_PPM IOS_PPS_SIGNATURE_CATEGORY IOS_PS_SIGNATURE_CATEGORY IOS_PS_signature IOS_vOIP_advance IOS_VOIP_advance IOS_VOIP_simple IOS_VPN_config_gre_tunnel IOS_VPN_config_gre_tunnel IOS_VPN_set_interface_desc	Filter : 🔄 none 💌			Name No IDS IPS PUBLIC KEY	ninimut
B. LOS VER CHIEDOWD INCIDE INTERTACE	CAT6K_ECLB_portchannel CAT6K_firewall_multiple_vlan_interfaces IOS_add_bridge_interface_desc IOS_CA_server IOS_compress_config IOS_conpress_config IOS_console_AAA_bypass IOS_Copy_Image IOS_Copy_Image IOS_PPM IOS_PPM IOS_PPS_SIGNATURE_CATEGORY IOS_PKI_with_AAA IOS_VOIP_advance IOS_VOIP_advance IOS_VOIP_simple IOS_VPN_set_interface_desc IOS_VPN_sct_interface_desc IOS_VPN_sct_interface_desc		>>		
IOS_VRF_on_vFW	IOS_VRF_on_vFW	~			

- 12. Per salvare le modifiche, fare clic su **Save** (Salva).**Nota:** IOS_IPS_PUBLIC_KEY FlexConfig contiene la configurazione per la chiave pubblica.
- 13. Dal menu a sinistra, scegliere **General Settings** (Impostazioni generali) situato sotto l'intestazione IPS.
- 14. Immettere il percorso di configurazione IPS sul flash. In questa posizione vengono inserite le configurazioni IPS.
- 15. Per salvare le modifiche, fare clic su **Save** (Salva).

Cisco Security Manager - admin	Connected to '172.25.90.8'				
Ele Edit Yew Balicy Map Icols	Help		المنط والمالم المالم المالم الم		Che di
😻 🖉 💽 📚 🖪 🗎 🕯	3 ?				of the local division of the local divisione
Devices 💮 🗇	Device: 172.25.90.33 Policy:	General Settings			
Filter :	Apply Deny Action on:	Block Traffic when IPS en	gine unavailable		
a Location	ragery conty reason on				
- (1) Al	SDEE Properties				
172.25.90.33	Maximum Subscriptions:*	1			
172.25.90.34	Meximum Alerts:*	200			
	Maximum Messages:*	500			
		P			
	IPS Config Location Prope	erties			
	IPS Config Location:	Flash:/ps			
AAA Rules	Max retries:	1			
Access Rules	Timeout seconds between r	etries: D			
Dispection Rules					
E Settings	1				
Transparent Mules					
T 194					
CT Smatures					
E Event Actions					
General Settings					
S Domine & set					
NAT					
Site to Site VPN					
Remote Access VPN					
SSL VPN					
🗄 Interfaces					
Platform					
PlexConligs					
					Save
				and the second	and the second design of the s

Nota: verificare che la directory di posizione sia già stata creata sul flash del router. In caso contrario, utilizzare il comando **mkdir <nome_directory>**per creare la directory di posizione.

- 16. Per abilitare IPS, passare a Regole interfaccia, selezionare la casella di controllo **Abilita IPS** e quindi fare clic su **Aggiungi riga**.
- 17. Nella finestra di dialogo Aggiungi regola IPS immettere un nome per la regola IPS nel campo Nome regola e quindi fare clic su **Aggiungi riga** per includere le interfacce a cui applicare l'IPS.

Cisco Security Manager - admin D File Edit View Policy Map Tools	nonexted to "17223.50.0"
	2
	Device 172.25.90.33 Policy Interface Bules
Denkes E3 (8)	
Filter : - none - v	€ Enable IPS
ig Department	No. Rule Name ACL Name Interface (Direction)
Jacation	
- (3) Al	
172.25.90.33	
1/2.25.90.34	Add/Edit IPS Rule
	Rule Name.* hypel
and the standard sector strength	ACL Name: Select
	Interface (Direction) Direction
C AAA Duint	
Access Bales	
Inspection Rules	
E Settings	
Transparent Rules	
Web Filter Rules	
8 195	Add Row
🔁 Signatures	
Event Actions	OK Cancel Help
General Settings	
C MAY	
Size to Size VPV	
E Remote Access VPN	
SSL VPN	
E Interfaces	
E Platform	
FlexConfigs	
	Save

18. Fare clic sul pulsante di opzione che indica in quale direzione deve essere applicata la regola IPS e quindi fare clic su Seleziona per scegliere le interfacce

-	Adding Pair				×
	Direction:*				
	In	out		Both	
	Interfaces:*			Select	
		[ОК	Cancel	Help
appropriate	<u>.</u>				

19. Selezionare un'interfaccia dall'elenco Selettore di interfaccia e fare clic su

Filter :	none	~	
• 0	ot11Radio0		
₩ F	astEthernet0		
• F	astEthernet1		
E F	astEthernet2		
	astEthernet3		
	ascethernet4		
	Interfaces		
Care I	sternal		
	nternal		
Selected			
Vlan1			
22	J		

20. Per salvare le modifiche, fare clic su **Save** (Salva).



21. Per installare le firme IPS più recenti, scegliere **Strumenti > Applica aggiornamento IPS**.



22. Scegliere il file della firma più recente e fare clic su

Avanti.

Turney Clamate	ra i Indahar 🔤			Labort Analablas	100 CE 1000 0000 01
IPS-CS-MGR-sig-S IPS-CS-MGR-sig-S IPS-CS-MGR-sig-S	File 278-req-E1.zp 280-req-E1.zp 282-req-E1.zp	5kg. 278 280 282	Engine 1 1	Latest Available: Latest Downloaded: Latest Applied: Latest Deployed: Last Checked On: Last Downloaded On Last Deployed On:	IPS-CS-MGR-sig-5282-req-E1.2p IPS-CS-MGR-sig-5282-req-E1.2p IPS-CS-MGR-sig-5282-req-E1.2p IPS-CS-MGR-sig-5282-req-E1.2p Apr 19 2007 10:46:37 : Apr 19 2007 10:45:48 Apr 23 2007 17:56:38
Update Details File:	IPS-CS-MGR-sig-	i282-req-£1.zjp			Check For Updates Download Latest Updates
Description: Date: Release:	IPS-CS-MGR-sig- Apr 19 2007 S282	282-req-E1.zip Size: Required Engine Lev	3.6M8 vel: E1]	

23. Selezionare i dispositivi a cui applicare l'aggiornamento IPS e fare clic su Avanti.

Type: Local Signatures Policies	IT2.25.90.33
Department D	
Select All Deselect All	Back Next Finish Cancel Hel

24. Per applicare le firme, fare clic su **Fine**.

			*	<u> </u>	_		Apply	00
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)	122/
1002	0	IP options-Timestamp	Produce Alert	Infomational	100	Catal	(also	12
1003	0	IP options-Provide s, c, h, tcc	Produce Alert	Informational	100	Oefault	(false)	13
1004	0	IP options-Loose Source Route	Produce Alert	Hep	100	Oefault	false	100
1095	0	IP options-SATNET ID	Produce Alert	Informational	100//	Oefault	(also	13/
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default	true	100
<								

25. Passare a IPS e scegliere **Firme** per visualizzare un elenco di tutte le firme

	0.9	2			CONTRACTOR OF CONTRACTOR		-	THE OWNER WHEN THE
Devices	88	Device: 172	.25.90	1.33 Policy: Signatures				
Pitter : none		· FRat	(nor	ne)				
Department	_	-		×			Apply	Cear
Location		D	Sub	distant internet Name (activity)	in international Actions relations	Severity	Fidelity	Source
AL .		1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default
172.25.90.33		1001	112	IP uptons-Record Pecket Route	Produce Alert	Automation#	100	Owner
		1002	0///	IP options Taxestanip	Produce Alert	kroteinolat //	100	Defeid
		1002	11/1	IP options=Provide s, c, h, h:c:	Produce Alert	Anotainoide //	100	Actual
		1005	0	IP optimie-Loose Source Route	Produce Alert	1400	100	Owinit
	_	1005	1/10	IP options SATINET ID	Produce Alert	Informational	100	Datast
	_	1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default
Frend	<u> </u>	1202	1110	Rod and Rod (1111111111111111	(Produce Alert ((((((((((((()	Knoteinovie ///	1/ 60%	the boy
Ann Fulles	- 1	1101	0	Unknown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules		1102	0	Impossible IP Packet	Produce Alert	High	100	Default
10 Settings		1104	0	IP Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules		1/16/1	11/0	RPC (RIR Addressed Seat (111111)	()))))))// telk school	Ministeriore ////	1// 661	(hickor)
Web Filter Rules		1108	0	IP Packet with Proto 11	Produce Alert	Hah	100	Default
1P5		1 4011	1116	Claro MS Interface Dot 1111111	11111111111111111111111111111111111111	makerm	1116	ness
Signatures	1	and	999.	Clara KIS Interface DeS	Produce diast	History	299	and
General Settings		and a	99	rises hit basedara here	Douber dat	and a second	9999	22
Thereface Rules		ALCO I	99		Produce start	and the second s	299	1220
NAT		1440	20	CERCI AUS ARTHUR LADS	human was	11 Labora	1211	(and
Site to Site VPN		1444/	211	The Landburk Conduction (1997)	/ phile here here here here here	111/ Walderland	1400/11	(Iddahd)
Remote Access VPN		1200	0	IP Pragment Overrun - Detagram Too Long	Deny Packet Inline, Produce Alert	High	100	Deraut
SSL VPN	1	I.C.						2
Interfaces						View Update Level		

26. Per distribuire l'IPS sul router IOS, scegliere **File > Invia e** distribuisci.

Open Desks Center Produce Status Stric Center Participant Produce Automs Severity Rodelity Severit			
Delete Device Device Theorem - D State Actions Severity Polatic Very Dynamic Resource Tooly to Understand D Sub Name Actions Severity Polatic Very Dynamic Resource Tooly to Understand D Sub Name Actions Severity Polatic Very Dynamic Resource Resource Tools and Deploy D Sub Name Actions Severity Polatic Submit And Deploy D Sub Name Actions Severity Polatic Deploy Digit of the polarity of	172 25 93 93 Bullou Gaudiana		
State Control Filter: (
View Oproges V V Volume gadata Site Site Name Actorial Seventin Moder Site Spin Dial Site Name Actorial Seventin Moder Site Spin Dial Dial Dial Produce Record Record Record Produce Record	Filter: (- none)		
Synthem D Sub Name Addons Seventy Paddat Seventy Sylper Sub Produce Alert Informational 75 Dele Subprime Subprime Produce Alert Informational 75 Dele Subprime Subprime Produce Alert Informational 100 Ode Deploy Deploy Produce Alert Informational 100 Ode Deploy Deploy Produce Alert Produce Alert <th>×</th> <th>100</th> <th>Y Onar</th>	×	100	Y Onar
Sybrit D000 0 IP options-field Option List Produce Alert Informational 75 Defa Signat, and Deploy D000 0 IP options-field Option List Produce Alert Informational 100 Ode Digstand D000 0 IP options-field Option List Produce Alert Informational 100 Ode Digstand D000 0 IP options-field Option List Produce Alert Informational 100 Ode Digstand D000 0 IP options-field Option List Produce Alert High 100 Ode Digstand D000 0 IP options-field Option List Produce Alert High 100 Ode Digstand D000 0 IP options-field Date Produce Alert High 100 Ode D001 0 IP options-field Date Produce Alert High 100 Ode D002 0 IP options-field Date Produce Alert High 100 Ode D002 0 IP options-field Date Produce Alert High 100 Ode D002 0 IP options-field Date Produce Alert High 100 Ode D004	ID 5.6 Name Adom	s Severity Fidel	ty Source
Subst and Deploy 1001.0 0 IP optime Record Papeter Route Produce Ret Deploy Deploy 1002.0 0 IP optime Record Papeter Route Produce Ret Deploy Deploy Deploy 1002.0 0 IP optime Frevele Struct Struct Produce Ret Deploy Depl	000 0 IP options-Bad Option List Produce Alert	Informational 75	Default
Deploy 3002 0 Proportions-Transitiation Produce ritert Downadcond 100 Outso Edit Device Groups 1002 0 Proportions-Frivable Scill/USC Produce ritert High 100 Outso Mag< Device Groups	01. 0 IP options-Record Paslet Route Produce Alert	Diversitional 100	Catal
Discard 1002 0 IP options-Provide s.r.h.tct Produce Sets Produce Sets Lidt Device Group 1002 0 IP options-Loses Source Rode Produce Sets Produce Sets Neg Device Group 1002 0 IP options-Shift Source Rode Produce Sets Produce Sets Diff Coll-D 1002 0 IP options-Shift Source Rode Produce Sets High 100 Odds Diff Coll-D 1004 0 IP options-Shift Source Rode Produce Alert High 100 Odds Diff Coll-D 1004 0 Unknown IP Protocol Produce Alert High 100 Defie Diff Coll-D Informational TS Defie Informational TS Defie Diff Coll-D Informational TS Defie Informational TS Defie Diff Coll-D Informational State Source Spool Produce Alert High 100 Defie Diff Diff. D Diff. Addresser Seen Produce Alert High 100 Defie Diff. D Diff. D Diff. Addresser Seen Produce Alert High 100 Defie Diff. Diff. D Diff. D	02 0 IP options-Timestamp Produce Alert	201 International 100	Dafaat
Edit Device Group: 100 0 100 0 Meg Device Group: 100 0 100 0 Med Devices to Group: 100 0 100 0 Devices for Quip: 0 100 100 0 Devices for Produce for Produce for	003 0 IP optimis-Fravide s. c.h. tot Produce Alert	001 Americanian 100	(Defail
Marg Dervice Group 1002 0 IP options-SkithTitD Produce Alent high 100 Oaks Mark Dervices to Group 0 IP options-SkithTitD Produce Alent High 100 Oaks Off Oaks 0 IP options-SkithTource Route Produce Alent High 100 Oaks Opt Oaks No Data Data <td>021 0 IP options Loose Source Route Produce Alert</td> <td>High 100</td> <td>Outsut</td>	021 0 IP options Loose Source Route Produce Alert	High 100	Outsut
Add Davies to Ograp D05. 0 IP options-Strikt Source Route Produce Alert High 100 Defensional Strikt Coll+Q D05. 0 IP options-Strikt Source Route Produce Alert Informational 75 Defensional Imponton Rules Informational 70 Defensional 100 Defensional Interpreter Rules Informational 70 Defensional 100 Defensional Interpreter Rules Informational 70 Reference Produce Alert High 100 Defensional Interpreter Rules Interpreter Rules Informational 70 Reference Produce Alert High 100 Defensional Interpreter Rules Interpreter Rules Interpreter Rules Interpreter Rules Produce Alert High 100 Defensional<	05 0 IP options-SATNET ID Produce Next	.001 International 100	Datad
Control Control Control Diversion Rules Intropection Rules Diversion Rules Interface Diversi	06 0 IP options-Strict Source Route Produce Alert	High 100	Default
Coll + Q I 101, 0 Unknown IP Protocol Produce Alert Informational 75 Defa Inspection Rules I 102, 0 Impossible IP Packet Produce Alert High 100 Defa Stattings I 102, 0 Impossible IP Packet Produce Alert High 100 Defa Transparent Rules I 102, 0 IP Locahost Source Spool Produce Alert High 100 Defa Yes I 102, 0 IP Locahost Source Spool Produce Alert High 100 Defa Yes I 102, 0 IP Locahost Source Spool Produce Alert High 100 Defa Yes I 102, 0 IP Packet with Proto II Produce Alert High 100 Defa Yes I 102, 0 Globa JOS Interface DoS Produce Alert High 100 Defa J 102, 1 Claca JOS Interface DoS Produce Alert Medun 75 Defa J 102, 2 Claca JOS Interface DoS Produce Alert Medun 75 Defa J 102, 2 Claca JOS Interface DoS Produce Alert Medun 75	202 8 Bhod over JPv+ ////////////////////////////////////	/ 001 Automatical	/ Hickory
Interction Rules Illigz 0 Impossible IP Packet Produce Alert High 100 Defa Is Settings Illigz 0 Impossible IP Packet Produce Alert High 100 Defa It to be in the settings Illigz 0 IP Locahost Source Spool Produce Alert High 100 Defa It to be in the settings Illigz 0 IP Packet with Proto II Produce Alert High 100 Defa It to be in the settings Illigz 0 IP Packet with Proto II Produce Alert High 100 Defa It to be in the settings Illigz 0 Globa JOS Interface DoS Produce Alert High 100 Defa It to be in the settings Illigz 1 Globa JOS Interface DoS Produce Alert High 75 Defa It to be in the settings Illigz 2 Globa JOS Interface DoS Produce Alert Medun 75 Defa It to be in to settings Illigz 3 Globa JOS Interface DoS Produce Alert Medun 75 Defa It to be in the settings Illigz 3 Globa JOS Interface DoS Produce Alert Medun 75 Defa It to be in the settings Illigz 3 Globa JOS Interface DoS Produce Alert Medun	101. 0 Unknown IP Protocol Produce Nert	Informational 75	Default
B Settings IIID* 0 IP lacahost Source Spoof Produce Alert High 100 Defa IIID* 0 IP lacahost Source Spoof Produce Alert High 100 Defa IIID* 0 IP Packet with Proto II Produce Alert High 100 Defa IIID* 0 IP Packet with Proto II Produce Alert High 100 Defa IIID* 0 Global JOS Interface DoS Produce Alert Medun 75 Defa IIID* 0 Global JOS Interface DoS Produce Alert Medun 75 Defa IIID* 1102 3 Global JOS Interface DoS Produce Alert Medun 75 Defa IIID* 1102 3 Global JOS Interface DoS Produce Alert Medun 75 Defa IIID* 2 Clobal JOS Interface DoS Produce Alert Medun 75 Defa IIID* 3 Global JOS Interface DoS Produce Alert Medun 75 Defa IIID* 3 Global JOS Interface DoS Produce	102 0 Impossible IP Packet Produce Alert	High 100	Default
Transparent Rules 1102 0 RFC 1918 Addresses Seen Produce Alert Informational 100 Data Web Pitter Rules 1102 0 IP Packet with Proto II Produce Alert High 100 Data Signatures 1102 0 IP Packet with Proto II Produce Alert High 100 Data Signatures 1102 0 Gaco JOS Interface DoS Produce Alert Medum 75 Data Signatures 1102 1 Gaco JOS Interface DoS Produce Alert Medum 75 Data Distantace Rules 1102 2 Cleou JOS Interface DoS Produce Alert Medum 75 Data Interface Rules 1102 3 Gaco JOS Interface DoS Produce Alert Medum 75 Data Interface Rules 1102 3 Gaco JOS Interface DoS Produce Alert Medum 75 Data Interface Rules 1102 3 Gaco JOS Interface DoS Produce Alert Medum 75 Data Interface Motes 1202 0 IP Fragment Ovenice	104 0 IP Localhost Source Spool Produce Alert	Hah 100	Default
Web Pitter Pulles Intell Produce Alert High 100 Defa ISS Signatures Intell Produce Alert Medun 75 Defa Signatures Intell Intell Produce Alert Medun 75 Defa Signatures Intell Intell Produce Alert Medun 75 Defa General Settings Intell Intell Produce Alert Medun 75 Defa Intell 2 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 2 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 2 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 3 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 3 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 3 Geno JOS Interface DoS Produce Alert Medun 75 Defa Intell 3 <td< td=""><td>HD 8 EFC 1913 Addresses Gam</td><td>1 Kill Mathematica / / / / / / / / /</td><td>144411</td></td<>	HD 8 EFC 1913 Addresses Gam	1 Kill Mathematica / / / / / / / / /	144411
IPS Index House Next House Next Signatures 1102 0 Caco JOS Interface DoS Produce Next Medun 75 Data Interface Rules 1102 1 Caco JOS Interface DoS Produce Next Medun 75 Data Interface Rules 1102 2 Caco JOS Interface DoS Produce Next Medun 75 Data Interface Rules 1102 3 Caco JOS Interface DoS Produce Next Medun 75 Data Interface Rules 1102 3 Caco JOS Interface DoS Produce Next Medun 75 Data Interface Rules 1102 3 Caco JOS Interface DoS Produce Next Medun 75 Data NAT 1202 3 Caco JOS Interface DoS Produce Next Medun 75 Data NAT 1202 3 Caco JOS Interface DoS Produce Rext Medun 75 Data Star VPN 1202 0 IP Fragment Oversur Datagram Too Long Demy Packet Inline, Produce Alext High 100 Data Star VPN 1202 0 IP Fragment Oversur Datagram Too Long Demy Packet Inline, Produce Alext High 100 </td <td>108 0 19 Pariet with Proto 11 Produce dier</td> <td>Held 100</td> <td>(111111)</td>	108 0 19 Pariet with Proto 11 Produce dier	Held 100	(111111)
Signatures AA22 0 Georgia Statutes Units Produce Hent People 10 Centre © Event Actions 1102 1 Cacuto JOS Interface DoS Produce Hent Medium 75 Data © Event Actions 1102 2 Cacuto JOS Interface DoS Produce Hent Medium 75 Data © Interface Rules 1102 3 Cacuto JOS Interface DoS Produce Alent Medium 75 Data NAT 1202 0 IP fragment Oversize Deny Packet Linke, Produce Alent High 100 Data Stat VPN 1202 0 IP fragment Oversize Deny Packet Inline, Produce Alent High 100 Defa Stat VPN 4 100 Defa 100 Defa	100 / W// Chris MC balanting had ///////////////////////////////////	nummer and and a second	144411
Bit Event Actions 1,022 1 Calco US promotion does tools Produce Name Peoplan 13 Calco Interface Rules 1,102 2 Calco US Interface DoS Produce Name Medium 75 Calco Interface Rules 1,102 3 Calco US Interface DoS Produce Name Medium 75 Calco Interface Rules 1,102 3 Calco US Interface DoS Produce Name Medium 75 Calco State VPN 1,202 0 IP Fragment Oversun - Datagram Too Long Deny Packet Inline, Produce Alert High 100 Defa State VPN 4 Interface Rules Interface Rules <td></td> <td></td> <td>(1922)</td>			(1922)
June I Case Job Job Interface Dos Produce Net Predun 75 Case Interface Rules 1102 3 Gaco Job Interface Dos Produce Net Medium 75 Data Interface Rules 1102 3 Gaco Job Interface Dos Produce Net Medium 75 Data Site to Site VPN 1202 0 IP Fragment Overlac Data Data Produce Alert High 100 Data Site VPN 1202 0 IP Fragment Overlac Deny Packet Inline, Produce Alert High 100 Data Site VPN 4 Interface Produce Alert Inline, Produce Alert High 100 Data	The P CERO FOR REAL PROP HERE	11111111111111111111111111111111111111	(Caland
LLI22 3 Carco JOS Interface Dos Produce Alert Medum 75 Data NAT 1201 0 IP fragment Overlap Deny Packet Inline, Produce Alert Johnstabonal 100 Data Size to Size VPN 1202 0 IP fragment Overlap Deny Packet Inline, Produce Alert High 100 Defe Size VPN 4 Interface Dos Interface Dos Interface Dos Deny Packet Inline, Produce Alert High 100 Defe	The a cado tro beaute boo Produce that	ann an ann an	(Caland)
Site to Site VPN Data Detry Packet Linke, Produce Alert Driversational 100 Outs Remote Access VPN 1202 0 IP Progreent Oversun - Datagram Too Long Deny Packet Linke, Produce Alert High 100 Defendence SSL VPN 4 = <	102 J. GROUICS Intertace DOS Produce Alert	Medun 12	Calant
Remote Access VPN 1202 0 IP Pragment Overnun - Datagram Too Long Deny Packet Inline, Produce Alert High 100 Defa SSL VPN Image: Compare the second	201 0. IP Fragment Overlap: Deny Packet Inline Produ	ku Hert // Jajounakional 100	Culauk
	202 0 IP Fragment Overrun - Datagram Too Long Deny Packet Inline, Produ	xe Alert High 100	Default
			>
View Update Level		View Update Level	2/1

27. Scegliere il dispositivo su cui si desidera distribuire le modifiche e fare clic su

Edit deploy me	thod	Add other devi	ces

28. Visualizzare lo stato della distribuzione per verificare la presenza di errori.

ployment Status Details					
Ratus:	Deployed (1 out of 1 de	vices completi	ed.)		
Deployment Job Name:	admin_job_2007-04-24	10:53:10.468			
Devices To Be Deployed:	1				
Devices Deployed Successfully:	1				
Devices Deployed with Errors:	U				
Deployment Details (1/1 loaded	ກ				
Device S	tatus Sun	mary	Method	Config	Transcript
172.25.90.33 SUCCEEDE	D 🔊 Warnin	g: 2	Device	50	\$
		Descrip	tion		
Messages	Sever	Ry Descrip	Bon Difference of file "C:\/PRO	GRA~1\CSCOpx\MDC\ten	τρ\2007.04.24_10.53.
Messages Out of Band Change: CLI	Sever A	Ry Descrip >>>> 15_job 7401dr	tion Difference of file "C:\PRO _admin_job_2007-04-24 11 f archived" and file "C:\PR	GRA~1\CSCOpx/MDC\ten 0_53_10_468\lphase1\17 10GRA~1\CSCOpx/MDC\t	np\2007.04.24_10.53. 72_25_90_33_4294980 templ2007.04.24_10.5
Messages Out of Band Change: CLI Operation Successful	Sever A O	Ry Descrip >>>> 15_job 740(dr 3.15_	bon Difference of file "C:\PRO _admin_job_2007-04-24 1 f_archived" and file "C:\PR ob_admin_job_2007-04-24	GRA~1\CSCOpx\MDC\ten 0_53_10_468\(phase1\17 tOGRA~1\CSCOpx\MDC\t 10_53_10_468\(phase1\	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 iig update compilation warning	Sever A O A	Ry Descrip >>>> 15_job 740(d/ 3.15_) 807400	Bon Difference of file "C:\PRO _admin_job_2007-04-24 1 f_archived" and file "C:\PP bb_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\lphase1\17 10GRA~1\CSCOpx\MDC\t 10_53_10_468\lphase1\	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 Aig update compilation warning Aig update engine compilation status	Seven A O A O	Ry Descrip >>>> 15_job 740/df 807400 9a	tion Difference of file "C:\PRO _admin_job_2007-04-24 11 f_archived" and file "C:\PR bb_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\lphase1\17 toGRA~1\CSCOpx\MDC\t 10_53_10_468\lphase1\	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 ig update compilation warning ig update engine compilation status Operation Successful	Sever A O A O O	Ry Descrip >>>> 15_job 740(dl 3.15_) 807401 9a >	tion Difference of file "C:\PRO admin_job_2007-04-24 1 F_archived" and file "C:\PR admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\lphase1\17 tOGRA~1\CSCOpx\MDC\t 10_53_10_468\lphase1\	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 Operation Successful Xeployment Log	Sever 2 0 2 0 0 0 0 0 0 0 0 0 0 0 0	Ry Descrip >>>> 15_job 740/df 3.15_ 807401 -9a > Action	tion Difference of file "C:\PRO _admin_job_2007-04-24 1 f_archived" and file "C:\PR ob_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\uphase1\17 tOGRA~1\CSCOpx\MDC\t 10_53_10_468\\phase1\	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 Big update compilation warning Big update engine compilation status Operation Successful Operation Successful	Sever A O A O O O O O O O O	Ry Descrip >>>> 15_job 740/dl 3.15_ 807400 -9a > Action	Bon Difference of file "C:\PRO _admin_job_2007-04-24 1 f_archived" and file "C:\PR ob_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\uphase1\17 tOGRA~1\CSCOpx\MDC\t 10_53_10_468\uphase1\	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 Ag update compilation warning Ag update engine compilation status Operation Successful Operation Successful	Sever (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	Ry Descrip >>>> 15_job 740(d) 3.15_j 80740 -9a > Action	tion Difference of file "C:\PRO _admin_job_2007-04-24 1 f_archived" and file "C:\PR ob_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\lphase1\17 \OGRA~1\CSCOpx\MDC\t 10_53_10_468\lphase1\	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 lig update compilation warning lig update engine compilation status Operation Successful Opeloyment Log	5ever 2 0 2 0 0 0 0 0 0 0	Ry Descrip >>>> 15_job 740/dl 3.15_) 807401 -98 > Action	Bon Difference of file "C:\PRO _admin_job_2007-04-24 1 F_archived" and file "C:\PR ab_admin_job_2007-04-24 diff_uploaded".	GRA~1\CSCOpx\MDC\ten 0_53_10_468\lphase1\17 tOGRA~1\CSCOpx\MDC\t 10_53_10_468\lphase1\	np\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 1.172_25_90_33_42949

Informazioni correlate

- Pagina Prodotti e servizi Cisco IOS Intrusion Prevention System (IPS)
- Guida introduttiva a Cisco IOS IPS con formato della firma 5.x
- Miglioramenti utilizzabilità e supporto del formato della firma IPS 5.x
- <u>Cisco Intrusion Prevention System</u>
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure Intrusion Detection)
- <u>Supporto tecnico Cisco Systems</u>