Ejemplo de Configuración de ASA/PIX con RIP

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Productos Relacionados Convenciones Antecedentes Configurar Diagrama de la red Configuraciones Configuración de ASDM Configuración de la Autenticación RIP Configuración de Cisco ASA CLI Configuración CLI del router Cisco IOS (R2) Configuración CLI del router Cisco IOS (R1) Configuración CLI del router Cisco IOS (R3) Redistribuir en RIP con ASA Verificación **Troubleshoot** Comandos para resolución de problemas Información Relacionada

Introducción

Este documento explica cómo configurar Cisco ASA para aprender las rutas a través del protocolo de información de routing (RIP), realizar la autenticación y la redistribución.

Consulte <u>PIX/ASA 8.X: Configuración de EIGRP en Cisco Adaptive Security Appliance (ASA)</u> para obtener más información sobre la configuración de EIGRP.

Nota: Esta configuración de documento se basa en la versión 2 de RIP.

Nota: El ruteo asimétrico no se soporta en ASA/PIX.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Cisco ASA/PIX debe ejecutar la versión 7.x o posterior.
- RIP no se admite en modo multicontexto; solo se admite en modo único.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión de software 8.0 y posteriores.
- Software Cisco Adaptive Security Device Manager (ASDM) versión 6.0 y posterior.

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.

Productos Relacionados

La información en este documento también es aplicable al Cisco 500 Series PIX firewall que ejecuta la versión de software 8.0 y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

RIP es un protocolo de ruteo de vector de distancia que utiliza el conteo de saltos como métrica para la selección de trayectoria. Cuando RIP está habilitado en una interfaz, la interfaz intercambia broadcasts RIP con dispositivos vecinos para aprender y anunciar dinámicamente las rutas.

El dispositivo de seguridad admite tanto la versión 1 de RIP como la versión 2 de RIP. RIP versión 1 no envía la máscara de subred con la actualización de ruteo. RIP versión 2 envía la máscara de subred con la actualización de ruteo y admite máscaras de subred de longitud variable. Además, RIP versión 2 admite la autenticación de vecinos cuando se intercambian las actualizaciones de ruteo. Esta autenticación garantiza que el dispositivo de seguridad reciba información de ruteo confiable de un origen de confianza.

Limitaciones:

- 1. El dispositivo de seguridad no puede pasar actualizaciones RIP entre interfaces.
- 2. RIP versión 1 no admite las máscara de subred de longitud variable (VLSM).
- 3. RIP tiene un conteo máximo de saltos de 15. Una ruta con un conteo de saltos mayor que 15 se considera inalcanzable.
- 4. La convergencia RIP es relativamente lenta en comparación con otros protocolos de ruteo.
- 5. Solo puede habilitar un único proceso RIP en el dispositivo de seguridad.

Nota: Esta información se aplica solamente a la versión 2 de RIP:

- 1. Si utiliza la autenticación de vecino, la clave de autenticación y el ID de clave deben ser los mismos en todos los dispositivos vecinos que proporcionan actualizaciones RIP versión 2 a la interfaz.
- 2. Con RIP versión 2, el dispositivo de seguridad transmite y recibe actualizaciones de ruta predeterminadas con el uso de la dirección multicast 224.0.0.9. En el modo pasivo, recibe actualizaciones de ruta en esa dirección.
- 3. Cuando RIP versión 2 se configura en una interfaz, la dirección multicast 224.0.0.9 se registra en esa interfaz. Cuando se quita una configuración RIP versión 2 de una interfaz, esa dirección multicast no se registra.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

<u>Nota:</u> Use el <u>Command Lookup Tool</u> (<u>únicamente</u> clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de ASDM
- <u>Configuración de la Autenticación RIP</u>
- Configuración de Cisco ASA CLI
- Configuración CLI del router Cisco IOS (R2)
- <u>Configuración CLI del router Cisco IOS (R1)</u>
- <u>Configuración CLI del router Cisco IOS (R3)</u>

Configuración de ASDM

Adaptive Security Device Manager (ASDM) es una aplicación basada en navegador que se utiliza para configurar y supervisar el software en dispositivos de seguridad. El ASDM se carga desde el dispositivo de seguridad y luego se utiliza para configurar, supervisar y administrar el dispositivo. También puede utilizar el iniciador ASDM (sólo Windows®) para iniciar la aplicación ASDM más rápido que el applet Java. Esta sección describe la información que necesita para configurar las funciones descritas en este documento con ASDM.

Complete estos pasos para configurar RIP en Cisco ASA:

- 1. Inicie sesión en Cisco ASA con ASDM.
- 2. Elija **Configuration > Device Setup > Routing > RIP** en la interfaz ASDM, como se muestra en la captura de



3. Elija **Configuration > Device Setup > Routing > RIP > Setup** para habilitar el ruteo RIP como se muestra.Elija la casilla de verificación **Enable RIP routing**.Elija la casilla de verificación

Enable RIP version with radio button Version 2.En la pestaña Redes, agregue la red 10.1.1.0.Haga clic en Apply

(Aplicar).



CamposEnable RIP Routing (Activar routing RIP): active esta casilla de verificación para habilitar el routing RIP en el dispositivo de seguridad. Cuando habilita RIP, se habilita en todas las interfaces. Si marca esta casilla de verificación, también se activarán los demás campos de este panel. Desmarque esta casilla de verificación para inhabilitar el ruteo RIP en el dispositivo de seguridad. Habilitar resumen automático: desactive esta casilla de verificación para desactivar el resumen automático de rutas. Margue esta casilla de verificación para volver a habilitar el resumen de ruta automático. RIP versión 1 siempre utiliza el resumen automático. No puede inhabilitar el resumen automático para la versión 1 de RIP. Si utiliza RIP versión 2, puede desactivar el resumen automático si desmarca esta casilla de verificación. Desactive el resumen automático si debe realizar el ruteo entre subredes desconectadas. Cuando se inhabilita el resumen automático, se anuncian las subredes. Habilitar versión RIP: active esta casilla de verificación para especificar la versión de RIP utilizada por el dispositivo de seguridad. Si se desactiva esta casilla de verificación, el dispositivo de seguridad envía actualizaciones de RIP versión 1 y acepta actualizaciones de RIP versión 1 y versión 2. Esta configuración se puede reemplazar por interfaz en el panel de interfaz. Versión 1: especifica que el dispositivo de seguridad sólo envía y recibe actualizaciones de la versión 1 de RIP. Las actualizaciones recibidas de la versión 2 se descartan. Versión 2: especifica que el dispositivo de seguridad sólo envía y recibe actualizaciones de la versión 2 de RIP. Las actualizaciones recibidas de la versión 1 se descartan. Enable default information originate-Marque esta casilla de verificación para

generar una ruta predeterminada en el proceso de ruteo RIP. Puede configurar un route map que se debe cumplir antes de que se pueda generar la ruta predeterminada.Route-map: introduzca el nombre del route map para aplicarlo. El proceso de ruteo genera la ruta predeterminada si se satisface el route map.Red IP a agregar: define una red para el proceso de ruteo RIP. El número de red especificado no debe contener ninguna información de subred. No hay límite en el número de redes que puede agregar a la configuración del dispositivo de seguridad. Las actualizaciones de ruteo RIP se envían y reciben solamente a través de interfaces en las redes especificadas. Además, si no se especifica la red de una interfaz, la interfaz no se anuncia en ninguna actualización RIP.Agregar: haga clic en este botón para agregar la red especificada a la lista de redes. Eliminar: haga clic en este botón para guitar la red seleccionada de la lista de redes.Configure las interfaces como pasivas globalmente: active esta casilla de verificación para establecer todas las interfaces del dispositivo de seguridad en el modo RIP pasivo. El dispositivo de seguridad escucha los broadcasts de ruteo RIP en todas las interfaces y utiliza esa información para rellenar las tablas de ruteo pero no difunde las actualizaciones de ruteo. Utilice la tabla Interfaces pasivas para establecer interfaces específicas a RIP pasivo. Tabla Interfaces pasivas: muestra las interfaces configuradas en el dispositivo de seguridad. Margue la casilla de verificación en la columna Pasivo para las interfaces que desea que funcionen en modo pasivo. Las otras interfaces aún envían y reciben broadcasts RIP.

Configuración de la Autenticación RIP

Cisco ASA admite la autenticación MD5 de las actualizaciones de ruteo del protocolo de ruteo RIP v2. El resumen con clave MD5 en cada paquete RIP evita la introducción de mensajes de ruteo no autorizados o falsos de fuentes no aprobadas. La adición de la autenticación a sus mensajes RIP garantiza que los routers y Cisco ASA sólo acepten mensajes de ruteo de otros dispositivos de ruteo configurados con la misma clave previamente compartida. Sin esta autenticación configurada, si introduce otro dispositivo de ruteo con información de ruta diferente o contraria en la red, las tablas de ruteo de sus routers o Cisco ASA pueden dañarse y puede producirse un ataque de denegación de servicio. Cuando agrega autenticación a los mensajes RIP enviados entre sus dispositivos de ruteo, que incluye el ASA, evita la adición deliberada o accidental de otro router a la red y cualquier problema.

La autenticación de ruta RIP se configura por interfaz. Todos los vecinos RIP en las interfaces configuradas para la autenticación de mensajes RIP deben configurarse con el mismo modo de autenticación y clave.

Complete estos pasos para habilitar la autenticación MD5 RIP en Cisco ASA.

 En ASDM, elija Configuration > Device Setup > Routing > RIP > Interface y elija la interfaz interna con el ratón. Haga clic en Editar.

0	Configur	ation > D)evice Setup > Rou	ting > RIP > Inter	face			
	Config	ure Routi	ng Information Proto	col (RIP) paramet	ers for specific in	terfaces. If sen	d and receive	versions
	are no	t configur	red for an interface t	hen the interface	will show the glo	bally configured	version.	
	Int	erface	Send Version	Rece	ive Version	Auth Type	Auth Ke	Edit
	dmz		2 (Global setting) 2 (Global setting)	2 (Global se 2 (Global se	tting) tting)	text		
	outsid	le	2 (Global setting)	2 (Global se	tting)	text		
2. E	lija la c	asilla E	Enable authentic	ation key y lue	ego ingrese e	el valor Key y	el valor K	еу
	🔂 E	dit RIP	Interface Entry	Y				
		Interfac	te: Inside					
	ſ	Send	Version					
			erride global send	version				
				O Handara O	O Handa	- 1 0 0		
		() version I	C Version 2	C version	n 1 64 Z		
	L							
	ſ	Recei	ve Version					
			verride alobal rece	ive version				
					C. Harris	100		
			C Version 1	C Version 2	C versi	oniekz		
	L							
	[Authe	ntication					
		(🔽 F	nable authenticat	ion key				
			Key:	key‡23				
			Key ID:	1				
		Authe	ntication Mode:	C MD5	C Clear	text		
15			ОК	Cancel	Help			lic on OK y
e	n Appl y	y.					liaya C	ile en Ort y

Configuración de Cisco ASA CLI

Cisco ASA	

```
ciscoasa#show running-config
: Saved
•
ASA Version 8.0(2)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- RIP authentication is
configured on the inside interface. rip authentication
mode md5
rip authentication key
!
!--- Output Suppressed !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0 !-
-- RIP Configuration router rip
network 10.0.0.0
version 2
!--- This is the static default gateway configuration in
!--- order to reach the Internet. route outside 0.0.0.0
0.0.0.0 192.168.1.1 1
```

Configuración CLI del router Cisco IOS (R2)

Router Cisco IOS (R2)

```
interface Ethernet0
ip address 10.1.1.2 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain 1
!
router rip
version 2
network 10.0.0.0
network 172.16.0.0
no auto-summary
```

Configuración CLI del router Cisco IOS (R1)

Router Cisco IOS (R1)

router rip version 2 network 172.16.0.0 no auto-summary

Configuración CLI del router Cisco IOS (R3)

Router Cisco IOS (R3)	
router rip	
version 2	
network 172.16.0.0	
no auto-summary	

Redistribuir en RIP con ASA

Puede redistribuir las rutas de los procesos de ruteo OSPF, EIGRP, estático y conectado en el proceso de ruteo RIP.

En este ejemplo, se muestra la redistribución de las rutas OSPF en RIP con el diagrama de red:



Configuración de ASDM

Complete estos pasos:

 Configuración OSPFElija Configuration > Device Setup > Routing > OSPF en la interfaz ASDM, como se muestra en la captura de pantalla.



Habilite el proceso de ruteo OSPF en la pestaña **Setup > Process Instancias**, como se muestra en la captura de pantalla. En este ejemplo, el proceso OSPF ID es **1**.

	Device Setup □ ₽ ×	Configuration > Device Setup > Routing > OSPF > Setup
Device List	Startup Wizard	Enable at least one OSPF Process Instance and define areas and area network Process Instances Area / Networks Route Summarization Maximum of two OSPF processes can be configured on this device. To rem the checkbox. OSPF Process 1
	Interface Redistribution Static Neighbor Summary Address Virtual Link RIP EIGRP	OSPF Process ID: 1 Advance
	S Device Setup	Enable this OSPF Process
	Firewall	OSPF Process ID: Advanc
	Site-to-Site VPN	
	*	Apply Reset

Haga clic en **Avanzado** en la pestaña **Setup > Process Instancias** para configurar los parámetros opcionales del proceso de ruteo OSPF avanzado. Puede editar la configuración específica del proceso, como la ID del router, los cambios de adyacencia, las distancias de ruta administrativas, los temporizadores y la configuración de origen de la información predeterminada.

🔤 Edit USPH	Process Ad	vanced Pro	perties
-------------	------------	------------	---------

OSPF Process: 1	Route	r ID:	192.168.1.1
Ignore LSA MOSPF (suppress the s syslog messages when router recei MOSPF packets)	ending of ives a LSA	RFC1583 summary (1583)	Compatible (calculate route costs per RFC
Adjacency Changes			
Enable this for the firewall to send a syste when an OSPF neighbor goes up/down.	og message	Enable this fo for each state	r the firewall to send a syslog e change.
Log Adjacency Changes		🔲 Log Adja	cency Change Details
Administrative Route Distances			
Inter Area (distance for all routes from one area to another area) 110	Intra Area (distance within an area) 110	for all routes	External (distance for all routes from other routing domains, learned by redistribution) 110
Timers (in seconds)			
SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)	SPF Hold Time (betw consecutive SPF calo	veen two culations)	LSA Group Pacing (interval at which OSPF LSAs are collected into a group and refreshed)
5	10		240
Default Information Originate			
Configure this to generate default exte	ernal route into an O:	SPF routing do	main.
🔲 Enable Default Information Originat	e	Always a	dvertise the default route
Metric Value: 1	Metric Type: 2	~	Route Map:

Click OK.Después de completar los pasos anteriores, defina las redes e interfaces que participan en el ruteo OSPF en la pestaña **Setup > Area/Networks** . Haga clic en **Agregar** como se muestra en esta captura de pantalla

able at least one OSPF Process	s Instance and define areas	; and area networks.	62	
rocess Instances Area / Netw	orks Route Summarization	1		
Configure the area properties a	and area networks for OSPF	Process		
				\mathbf{C}
Networks	Authentication	Options	Cost	
Networks	Authentication	Options	Cost	
Networks	Authentication	Options		E

Aparece esta pantalla. En este ejemplo, la única red que agregamos es la red externa

(192.168.1.0/24), ya que OSPF sólo se habilita en la interfaz externa.**Nota:** Sólo las interfaces con una dirección IP que se encuentren dentro de las redes definidas participan en el proceso de ruteo

OSPF.

			_	
OSPE Process	1		Area ID:	
Area Type	,			9
Normal				
🔿 Stub	🔽 Summary (allo	iws sending LSAs	into the stub area)	
O NSSA	🔽 Redistribute (imports routes to	normal and NSSA a	reas)
	🔽 Summary (allo	ws sending LSAs	; into the NSSA area))
	🔲 Default Inform	nation Originate	(generate a Type 7 (default)
	Metric Valu	e; 1	Metric Type: 2	~
- Enter IP Ad IP Address:	dress and Mask	Add >>	IP Address 192.168.1.0	255.255.255
Netmask:	255.255.255.0	Delete		
Authenticatio	n		1	
None	C Password	C MD5	Default Cost:	1
			-	

Click OK.Haga clic en Apply (Aplicar).

¢	En Pi	iguration > Devic able at least one C rocess Instances (e Setup > Routin DSPF Process Insta Area / Networks)	i g > OSPF > Se nce and define Route Summariz	tup) areas and area networks. zation		
	(Configure the area	properties and are	a networks for	OSPF Process		
		OSPF Process	Area ID	Area Type	Networks	Authe	Add
	(1	0	Normal	192.168.1.0 / 255.255.255.0	None)
			<u>.</u>				Edit
							Delete

2. Elija Configuration > Device Setup > Routing > RIP > Redistribution > Add para redistribuir las rutas OSPF en

RIF).					
Con	figuration > Device Setu	ıp > Routing > RIP > F	Redistribution			
¢	Configure conditions for red	listributing RIP routes.				
[Protocol	Metric	Match	Route Map		Add
					j	Edit
						Delete

1	Add Redistribution
	Protocol
	○ Static ○ Connected ○ OSPF OSPF ID: 1
	O EIGRP EIGRP ID:
	Metric
	Configure Metric Type
	C Transparent C Value
	Optional
	Route Map:
	Match
	🔽 Internal 🔲 External 1 💭 External 2
	NSSA External 1 🔲 NSSA External 2
3. Haga clic en OK y en Apply.	

Configuración CLI equivalente

```
Configuración CLI de ASA para Redistribuir OSPF en
RIP AS

router rip
network 10.0.0.0

redistribute ospf 1 metric transparent
version 2

!

router ospf 1

router-id 192.168.1.1

network 192.168.1.0 255.255.255.0 area 0

area 0

log-adj-changes
```

Puede ver la tabla de ruteo del router Cisco IOS vecino(R2) después de redistribuir las rutas OSPF en RIP AS.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 4 subnets
        172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1
R
R
       172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1
С
       172.16.1.0 is directly connected, Ethernet1
С
       172.16.2.0 is directly connected, Serial1
     10.0.0/8 is variably subnetted, 2 subnets, 2 masks
       10.1.1.0/24 is directly connected, Ethernet0
С
R
        10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0
     192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0
R
     192.168.2.0/32 is subnetted, 1 subnets
        192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
R
     192.168.3.0/32 is subnetted, 1 subnets
```

R 192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0

!--- Redistributed route advertised by Cisco ASA

Verificación

Complete estos pasos para verificar su configuración:

 Puede verificar la tabla de ruteo si navega a Monitoring > Routing > Routes. En esta captura de pantalla, puede ver que las redes 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 y 172.16.10.0/24 se aprenden a través de R2 (10.1.1.2) con RIP.

oring > Routing >	Routes				
tes					
Each row represent	is one route. AD is	the administrative dista	ance.		
Protocol	Туре	Destination IP	Netmask	Gateway	
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	ins
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	ins
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	ins
RIP	-	172.16.2.0	255.255.255.0	10.1.1.2	ins
CONNECTED	-	10.1.1.0	255.255.255.0	-	ins
CONNECTED	-	10.77.241.128	255.255.255.192	-	dm
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dm
CONNECTED	-	192.168.1.0	255.255.255.0	-	ou
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	ou
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	ou

2. Desde la CLI, puede utilizar el comando **show route** para obtener el mismo resultado.

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route R 172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside

R 172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside

R 172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside

R 172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside

C 10.1.1.0 255.255.255.0 is directly connected, inside

C 10.77.241.128 255.255.255.192 is directly connected, dmz

S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz

C 192.168.1.0 255.255.255.0 is directly connected, outside

0 192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside

0 192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside

```
ciscoasa#
```

Troubleshoot

Esta sección incluye información sobre los comandos debug que pueden ser útiles para resolver problemas OSPF.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

```
    debug rip events: habilita la depuración de eventos RIP

 ciscoasa#debug rip events
 rip_route_adjust for inside coming up
 RIP: sending request on inside to 224.0.0.9
 RIP: received v2 update from 10.1.1.2 on inside
      172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
      172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
      172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
      172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
 RIP: Update contains 4 routes
 RIP: received v2 update from 10.1.1.2 on inside
      172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
      172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
      172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
      172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
 RIP: Update contains 4 routes
 RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142)
 RIP: build flash update entries
         10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
         172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
         172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
         172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
         172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
 RIP: Update contains 5 routes
 RIP: Update queued
 RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1)
 RIP: build flash update entries - suppressing null update
 RIP: Update sent via dmz rip-len:112
 RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142)
 RIP: build update entries
         10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
         172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
```

172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 8 routes RIP: Update queued RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1) RIP: build update entries 10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0 192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 4 routes RIP: Update queued RIP: Update sent via dmz rip-len:172 RIP: Update sent via inside rip-len:92 RIP: received v2 update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP: Update contains 4 routes

Información Relacionada

- Página de Soporte de Cisco 5500 Series Adaptive Security Appliance
- Página de soporte de PIX de la serie 500 de Cisco
- PIX/ASA 8.X: Configuración de EIGRP en Cisco Adaptive Security Appliance (ASA)
- <u>Soporte Técnico y Documentación Cisco Systems</u>