Ejemplo de Configuración de Túnel IPsec Dinámico entre un ASA Direccionado Estáticamente y un Router Cisco IOS Direccionado Dinámicamente que Utiliza CCP

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Antecedentes Configurar Diagrama de la red Configuraciones Verificación Verificar parámetros de túnel a través de CCP Verifique el estado del túnel a través de la CLI ASA Verifique los parámetros del túnel a través de la CLI del router Troubleshoot Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo de cómo habilitar el PIX/ASA Security Appliance para aceptar conexiones IPsec dinámicas del router Cisco IOS[®]. En este escenario, el túnel IPSec establece cuándo se inicia el túnel desde el extremo del router solamente. ASA no podía iniciar un túnel VPN debido a la configuración de IPSec dinámica.

Esta configuración permite que el dispositivo de seguridad PIX cree un túnel IPsec de LAN a LAN (L2L) dinámico con un router VPN remoto. Este router recibe dinámicamente su dirección IP pública externa de su proveedor de servicios de Internet. El protocolo de configuración dinámica de host (DHCP) proporciona este mecanismo para asignar direcciones IP dinámicamente desde el proveedor. Esto permite que las direcciones IP se vuelvan a utilizar cuando los hosts ya no las necesitan.

La configuración en el router se realiza con el uso de <u>Cisco Configuration Professional</u> (CCP). CCP es una herramienta de administración de dispositivos basada en GUI que le permite configurar routers basados en Cisco IOS. Consulte <u>Configuración básica del router con Cisco</u> <u>Configuration Professional</u> para obtener más información sobre cómo configurar un router con CCP.

Consulte <u>VPN de sitio a sitio (L2L) con ASA</u> para obtener más información y ejemplos de configuración sobre el establecimiento de túnel IPsec que utilizan routers ASA y Cisco IOS.

Consulte <u>VPN de sitio a sitio (L2L) con IOS</u> para obtener más información y un ejemplo de configuración sobre el establecimiento de túnel IPSec dinámico con el uso de PIX y el router Cisco IOS.

Prerequisites

Requirements

Antes de intentar esta configuración, asegúrese de que tanto el ASA como el router tengan conectividad a Internet para establecer el túnel IPSEC.

Componentes Utilizados

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

- Cisco IOS Router1812 que ejecuta Cisco IOS Software Release 12.4
- Software Cisco ASA 5510 versión 8.0.3

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.

Convenciones

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

Antecedentes

En este escenario, la red 192.168.100.0 está detrás del ASA y la red 192.168.200.0 está detrás del router del IOS de Cisco. Se supone que el router obtiene su dirección pública a través de DHCP de su ISP. Dado que esto plantea un problema en la configuración de un peer estático en el extremo de ASA, debe aproximarse al modo de configuración crypto dinámica para establecer un túnel de sitio a sitio entre ASA y el router Cisco IOS.

Los usuarios de Internet en el extremo ASA se traducen a la dirección IP de su interfaz externa. Se supone que NAT no está configurado en el extremo del router del IOS de Cisco.

Estos son los pasos principales que se deben configurar en el extremo ASA para establecer el túnel dinámico:

- 1. Fase 1 Configuración relacionada con ISAKMP
- 2. configuración de exención de Nat
- 3. Configuración dinámica de mapa criptográfico

El router Cisco IOS tiene configurado un mapa criptográfico estático porque se supone que el ASA tiene una dirección IP pública estática. Esta es la lista de pasos principales que se deben configurar en el extremo del router Cisco IOS para establecer un túnel IPSEC dinámico.

- 1. Fase 1 Configuración relacionada con ISAKMP
- 2. Configuración relacionada con el mapa criptográfico estático

Estos pasos se describen en detalle en estas configuraciones.

Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Ésta es la configuración de VPN IPsec en el router VPN con CCP. Complete estos pasos:

 Abra la aplicación CCP y elija Configure > Security > VPN > Site to Site VPN. Haga clic en la pestaña Iniciar la seleccionada.



2. Elija Asistente paso a paso y luego haga clic en



3. Complete la dirección IP del par remoto junto con los detalles de

Site-to-Site VPN Wiza	rd	
VPN Wizard	VPN Connection Information Select the interface for this VPN connection:	FastEthemet1 💽 Details
	Peer Identity Select the type of peer(s) used for this V connection: Enter the IP address of the remote peer.	PN Peer with static P address 💉 209.165.201.2
	Authentication Authentication ensures that each end of t key.	the VPN connection uses the same secret
	Pre-shared Keys pre-shared keys Re-enter Key:	C Digital Certificates
		- Back Next - Firms Cancel Help

autenticación.

4. Elija las propuestas IKE y haga clic en

IKE P IKE p meth devic devic	Proposals inoposals od that is i e. For the ' e should b	specify the en used by this r VPN connecti se configured	cryption algo outer when n on to be esta with at least	rithm, authentical egotiating a VPN blished with the r one of the policie	tion algorithm an connection with t emote device, th s listed below.	d key exchange the remote e remote
Clic	k the Add.	button to add	d more polici	es and the Edit.	button to edit an o	axisting policy Type
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Def
	2	DES	MD5	group2	PRE_SHARE	User Defined
-						
	Add	Edit.	-			

5. Defina los detalles del conjunto de transformación y haga clic en

Site-to-Site VPN Wizor	d			E
VPN Wizard	Transform Set A transform set s data in the VPN to communicate, th one selected bell Click the Add b transform set Select Transform	pecifies the encryption and a unnel. Since the two devices i e remote device must be con ow. utton to add a new transform n Set:	uthentication algorit must use the same figured with the sam set and the Edit bu	hms used to protect the algorithms to re transform set as the ation to edit the specified
11-CO	myset			
	Details of the	specified transform set		
	Name	ESP Encryptic	In ESP Integrity	AH Integrity
	Add	Edit	< Back Next > F	Cancel Help

Siguiente.

6. Defina el tráfico que debe cifrarse y haga clic en

VPN Wizard	IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will b protected by this VPN connection. Other data traffic will be sent unprotected to the rem device. You can protect all traffic between a particular source and destination subnet, i specify an IPSec rule that defines the traffic types to be protected.				
	 Protect all traffic between the following submark 	ets .			
	Enter the IP address and subnet mask of the network where IPSec traffic originates.	Enter the IP Address and Subnet Mask of the destination Network.			
	IP Address:	IP Address:			
	192 168 200.0	192.168.100.0			
	Subnet Mask:	Subnet Mask			
	255.255.255.0 pr 24	255.255.255.0 or 24			
	Create/Select an access-list for IPSec traffic				

7. Verifique el resumen de la configuración IPsec crypto y haga clic en

Wizard	Summary of the O	Configuration		
	Click Finish to de	liver the configurat	ion to the router.	
	pie-snareu key. IKE Policies:			4
	Hash	DH Group	Authentication	Encryption
	MD5 SHA_1	group2 group2	PRE_SHARE PRE_SHARE	DES 3DES
Y	Transform Sets Name.n ESP En ESP Inte Mode:Th	nyset cryption:ESP_DES sgrity:ESP_MD5_H JNNEL	мас	
	IPSec Rule: permit a	II ip traffic from 19:	2.168.200.0 0.0.0.255 to	192.168.100.0 0.0.
	¢			\$ 11
-	Test VPN conr	ectivity after config	uring)	

- Finalizar.
- 8. Haga clic en **Entregar** para enviar la configuración al router VPN.

Deliver Configuration to Router	
Deliver delta commands to the router's running config.	
Preview commands that will be delivered to the router's running configuration.	
crypto ipsec transform-set myset esp-md5-hmac esp-des mode tunnel	^
exit crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to209.165.201.2 set transform-set myset set peer 209.165.201.2 match address 101	
exit interface EastEthernet1	
no crunto men	2
The differences between the running configuration and the startup configuration are lost when the router is turned off.	iever
This operation can take several minutes.	
Deliver Cancel Save to file Help	



9. Click OK.

Configuración de CLI

- <u>Ciscoasa</u>
- Router VPN

Ciscoasa

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
 ip address 209.165.201.2 255.255.254
!
interface Ethernet0/1
nameif inside
 security-level 100
ip address 192.168.100.1 255.255.255.0
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
I
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
   - Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0
no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
```

inspect	h323 ras
inspect	netbios
inspect	rsh
inspect	rtsp
inspect	skinny
inspect	esmtp
inspect	sqlnet
inspect	sunrpc
inspect	tftp
inspect	sip
inspect	xdmcp
!	
service-po	olicy global_policy global
prompt hos	stname context
Cryptoched	cksum:d41d8cd98f00b204e9800998ecf8427e
: end	
ciscoasa(o	config)#

CCP crea esta configuración en el router VPN.

```
Router VPN
VPN-Router#show run
Building configuration...
1
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
1
!
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQ01
1
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
encrypt 3des
 authentication pre-share
group 2
!
crypto isakmp policy 2
hash md5
authentication pre-share
group 2
!
1
crypto isakmp key cisco123 address 209.165.201.2
1
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
1
1
crypto map SDM_CMAP_1 1 IPSec-isakmp
description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
match address 101
1
1
interface BRI0
no ip address
shutdown
!
interface Dot11Radio0
no ip address
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio1
no ip address
 shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
!
interface FastEthernet0
ip address 192.168.200.1 255.255.255.0
 duplex auto
speed auto
1
interface FastEthernet1
ip address dhcp
duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
no ip address
shutdown
!
interface FastEthernet3
no ip address
shutdown
!
interface FastEthernet4
no ip address
shutdown
interface FastEthernet5
no ip address
shutdown
1
interface FastEthernet6
no ip address
shutdown
1
interface FastEthernet7
no ip address
shutdown
!
interface FastEthernet8
no ip address
shutdown
ļ
interface FastEthernet9
no ip address
 shutdown
```

```
interface Vlan1
no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
1
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
privilege level 15
login local
transport input telnet ssh
1
no scheduler allocate
end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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.

- Verificación de los parámetros del túnel a través de CCP
- Verificación del estado del túnel a través de la CLI de ASA
- Verificación de los parámetros del túnel a través de la CLI del router

Verificar parámetros de túnel a través de CCP

 Supervise el tráfico que pasa a través del túnel IPsec.

uplication Help				
Norme 🛞 taafigan 🚮 Nar	🕶 🛠 🔶 🥹	Cisc	o Configur	ation Professional Clar
Select Coversarity Member	ex. Nonitor > Security > VPN State	ui > IFSec Tueseli		
	2 VPH Status			
R (s), Der	Carlor Burners	Park one service sets and Pfler Trend		The Monteres Test Trend
Security	CHONOR TURNOS	Alter and a state of the second		and sources?) Ten inter 1 com
Contrast Stores	-62 PZ 546	Local P Remote P Peer	Tenner States	Belect Ibirn to Monifer
1 181a: Tutenta	CECUPN KenServer	209 185 283 1 2 285 184 281 2 269 185 201 2 900 1	100	Encapeulation Packets
Cotomi Turenti	SSL VPN (All Centexts)			P Decapsulation Packets 12 Sand Error Packets
and have seen berner				P Received Errar Packets
(1) INT 840				1
The last function and				<u>بار</u>
Data press		Turnil Salat		
Barro canya		Vere Hervel Real-late data every 13 cec 🖌		
BALL MAN		Encausion Patients Decausion	in Paciety Sena Ex	Paciety Persived Error Packets
		let let	In In	
		Encaperated see Pasteria	5-17-14-1-T	Becaused at loss Packets.
			172 + +++	
			84	
			e 66	
	0			
		Haldo	12:54:25	
		The [#46/98.55]		Tim (HHMM \$5)
			-	and the second
		Secol Torus Packets		Research from Packets
		Send times Packets		Reserved first Parkets
		Send Taxas Packets		Referred Front Parkets
		bend town Packets		
				Research France Parkets
				Heresed House Packets
				Herese Hrus Pakets
		Derivatives (Sector)		The Joccesi 201

Supervise el estado de la fase I ISAKMP



Verifique el estado del túnel a través de la CLI ASA

Verifique el estado de la fase I ISAKMP SA.

ciscoasa#show crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 209.165.200.12
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE
ciscoasa#
```

Nota: Observe la Función que se va a responder, que indica que el iniciador de este túnel está en el otro extremo, por ejemplo, el router VPN.

```
    Verifique los parámetros de la fase II IPSEC SA.

 ciscoasa#show crypto ipsec sa
 interface: outside
     Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2
       local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
       current_peer: 209.165.200.12
       #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
       #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12
       path mtu 1500, IPSec overhead 58, media mtu 1500
       current outbound spi: E7B37960
     inbound esp sas:
       spi: 0xABB49C64 (2880740452)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0xE7B37960 (3887298912)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
```

Verifique los parámetros del túnel a través de la CLI del router

 Verifique el estado de la fase I ISAKMP SA. 								
	VPN-Router# show	crypto isakmp s	a					
	dst	src	state	conn-id	slot	status		
	209.165.201.2	209.165.200.12	QM IDLE	1	0	ACTIVE		

```
• Verifique los parámetros de la fase II IPSEC SA.
VPN-Router#show crypto ipsec sa
```

```
interface: FastEthernet1
   Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
  current_peer 209.165.201.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
   #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 6, #recv errors 0
    local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
    path mtu 1500, ip mtu 1500
    current outbound spi: 0xABB49C64(2880740452)
    inbound esp sas:
     spi: 0xE7B37960(3887298912)
       transform: esp-des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
       sa timing: remaining key lifetime (k/sec): (4481818/3375)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE
    inbound ah sas:
    inbound pcp sas:
    outbound esp sas:
     spi: 0xABB49C64(2880740452)
       transform: esp-des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
       sa timing: remaining key lifetime (k/sec): (4481818/3371)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE
    outbound ah sas:
    outbound pcp sas:
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

• Derribar las conexiones criptográficas existentes. ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa Utilice los comandos debug para resolver los problemas con el túnel VPN.Nota: Si habilita la depuración, esto puede interrumpir el funcionamiento del router cuando las redes entre redes experimentan condiciones de carga alta.Use los comandos debug con precaución. En general, se recomienda que estos comandos se utilicen sólo bajo la dirección del representante de soporte técnico de su router cuando se intenta resolver problemas específicos.

```
ciscoasa#debug crypto engine
ciscoasa#debug crypto isakmp
ciscoasa#debug crypto IPSec
ciscoasa#
VPN-Router#debug crypto engine
Crypto Engine debugging is on
VPN-Router#debug crypto isakmp
Crypto ISAKMP debugging is on
VPN-Router#debug crypto ipsec
Crypto IPSEC debugging is on
```

VPN-Router#

Consulte debug crypto isakmp en Comprensión y Uso de Comandos debug para obtener más

información sobre los comandos debug. Información Relacionada

- Página de Soporte de IPSec Negotiation/IKE Protocols
- Documentación para Cisco ASA Security Appliance OS Software
- Soluciones de Troubleshooting de VPN IPSEC más comunes
- <u>Solicitudes de Comentarios (RFC)</u>