# Router IOS: Autenticación de proxy de autenticación entrante con ACS para configuración de IPSec y cliente VPN

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Diagrama de la red Configuración Configuración de VPN Client 4.8 Configuración del servidor TACACS+ mediante Cisco Secure ACS Configuración de la función de reserva Verificación Troubleshoot Información Relacionada

### Introducción

La función de proxy de autenticación permite a los usuarios iniciar sesión en una red o acceder a Internet a través de HTTP, con sus perfiles de acceso específicos recuperados y aplicados automáticamente desde un servidor TACACS+ o RADIUS. Los perfiles de usuario están activos sólo cuando hay tráfico activo de los usuarios autenticados.

Esta configuración está diseñada para activar el explorador Web en 10.1.1.1 y dirigirlo a 10.17.17.17. Debido a que el cliente VPN está configurado para pasar por el punto final del túnel 10.31.1.111 para llegar a la red 10.17.17.x, el túnel IPSec está construido y el PC obtiene la dirección IP del conjunto RTP-POOL (ya que se realiza la configuración de modo). A continuación, el router Cisco 3640 solicita la autenticación. Luego de que el usuario ingresa un nombre de usuario y una contraseña (almacenados en el servidor TACACS+ en 10.14.14.3), la lista de acceso transmitida desde el servidor es agregada a la lista de acceso 118.

# Prerequisites

### Requirements

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- Cisco VPN Client se configura para establecer un túnel IPSec con el Cisco 3640 Router.
- El servidor TACACS+ está configurado para el proxy de autenticación. Consulte la sección

"Información Relacionada" para obtener más información.

#### **Componentes Utilizados**

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

- ¿IOS de Cisco? Versión de software 12.4
- Cisco 3640 Router
- Cisco VPN Client para Windows versión 4.8 (cualquier VPN Client 4.x y posterior debería funcionar)

**Nota:** El comando **ip auth-proxy** se introdujo en la versión 12.0.5.T del software del IOS de Cisco. Esta configuración se probó con Cisco IOS Software Release 12.4.

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Configurar

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

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la <u>Command Lookup Tool</u> (sólo clientes registrados).

#### Diagrama de la red

En este documento, se utiliza esta configuración de red:



#### Configuración

```
Router 3640
Current configuration:
1
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
1
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass
!--- Enable AAA. aaa new-model
!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
server 10.14.14.3
!
!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode
aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHC$R/07uQ44E2JgVuCsOUWdG1
enable password ww
1
ip subnet-zero
1
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
```

^C ip auth-proxy auth-cache-time 10 ip auth-proxy name list\_a http ip audit notify log ip audit po max-events 100 cns event-service server ! !--- Define ISAKMP policy. crypto isakmp policy 10 hash md5 authentication pre-share group 2 !--- These commands define the group policy that !--- is enforced for the users in the group RTPUSERS. !--- This group name and the key should match what !--- is configured on the VPN Client. The users from this !--group are assigned IP addresses from the pool RTP-POOL. crypto isakmp client configuration group RTPUSERS key cisco123 pool RTP-POOL !--- Define IPSec transform set and apply it to the dynamic crypto map. crypto ipsec transform-set RTP-TRANSFORM esp-des esp-md5-hmac 1 crypto dynamic-map RTP-DYNAMIC 10 set transform-set RTP-TRANSFORM 1 !--- Define extended authentication (X-Auth) using the local database. !--- This is to authenticate the users before they can !--- use the IPSec tunnel to access the resources. crypto map RTPCLIENT client authentication list userauth !--- Define authorization using the local database. !---This is required to push the 'mode configurations' to the VPN Client. crypto map RTPCLIENT isakmp authorization list groupauth crypto map RTPCLIENT client configuration address initiate crypto map RTPCLIENT client configuration address respond crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC interface FastEthernet0/0 ip address 10.31.1.111 255.255.255.0 ip access-group 118 in no ip directed-broadcast !--- Apply the authentication-proxy rule to the interface. ip auth-proxy list\_a no ip route-cache no ip mroute-cache speed auto half-duplex !--- Apply the crypto-map to the interface. crypto map RTPCLIENT interface FastEthernet1/0 ip address 10.14.14.14 255.255.255.0 no ip directed-broadcast speed auto half-duplex

```
--- Define the range of addresses in the pool. !--- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list
118 permits communication !--- between the TACACS+
server and the 3640 router to enable !--- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host
10.31.1.111
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
!
end
```

#### Configuración de VPN Client 4.8

Complete estos pasos para configurar el VPN Client 4.8:

- 1. Elija Inicio > Programas > Cisco Systems VPN Client > VPN Client.
- 2. Haga clic en **Nuevo** para iniciar la ventana Crear nueva entrada de conexión VPN.

🍰 status: Disconnected	VPN Client - Version 4.8.0	1.0300	
Connection Entries Status	Certificates Log Options H	Help	
Connect New	Import Modify	) Delete	CISCO SYSTEMS
Connection Entries Certific	cates Log		
Connection Entry	$\nabla$	Host	Transport
•			
Not connected.			

3. Introduzca el nombre de la entrada de conexión junto con una descripción. Introduzca la dirección IP externa del router en el cuadro Host (Host). A continuación, introduzca el nombre y la contraseña del grupo VPN y haga clic en

Dennistan [			
Description: J			
Host: 1	0.31.1.111		
Authentication	Transport   Backup	Servers Dial-Up	
Group Authent	ication	C Mutual Group	p Authenticatio
Name:	RTPUSERS		
Password:	******		
Confirm Passwo	rd: 🔤		
C Certificate Auth	nentication		
Name:		*	
C Send CA Ca	ertificate Chain		

#### Guardar.

4. Haga clic en la conexión que desea utilizar y haga clic en **Connect** desde la ventana principal de VPN

Client.

👌 status: Di	sconne	cted   VPN C	lient - Version ·	4.8.01.0300	);	×
Connection Er	ntries SI	tatus Certific	ates Log Optio	ins Help		
Connect	ter New	v Impo	a 🏹 rt Modify	) Delete		CISCO SYSTEMS
Connection E	intries	Certificates	Log			
	Conne	ction Entry	2		Host	Transport
	vpn				10.31.1.111	IPSec/UDP
.1						
-						
Not connected	d,					

5. Cuando aparezca el mensaje, ingrese la información de su nombre de usuario y contraseña para Xauth y haga clic en OK (Aceptar) para conectarse a la red remota.

👌 status: Disconnected   VPN	Client - Version 4.8.01.030		
Connection Entries Status Certi	ficates Log Options Help		
Cancel Connect New	mport Modify Dele	ete	CISCO SYSTEMS
Connection Entries Certificates	Log		
Connection Entry	Δ	Host	Transport
vpn		10.31.1.111	IPSec/UDP
1	The server has requested the authentication. CISCO SYSTEMS Usernar	following information to complete ne: cisco rd: management OK	the user
Authenticating user			

El cliente VPN se conecta con el router en el sitio central.

👌 status: Co	nnected   VPN Client - Version 4.8.01.0300		- 🗆 ×
Connection En	tries Status Certificates Log Options Help		
Disconnect	New Import Modify Delete		CISCO SYSTEMS
Connection Er	ntries Certificates Log		
	Connection Entry	Host	Transport
0	vpn	10.31.1.111	IPSec/UDP
•			
Connected to '	"vpn"	Connected Time: 0 day(	s), 00:09.44 🔻 //

#### Configuración del servidor TACACS+ mediante Cisco Secure ACS

Complete estos pasos para configurar TACACS+ en un Cisco Secure ACS:

1. Debe configurar el router para localizar Cisco Secure ACS para verificar las credenciales del usuario.Por ejemplo:

3640(config)#
aaa group server tacacs+ RTP
3640(config)#
tacacs-server host 10.14.14.3 key cisco

 Elija Network Configuration a la izquierda y haga clic en Add Entry para agregar una entrada para el router en la base de datos del servidor TACACS+. Elija la base de datos del servidor según la configuración del router.

CISCO SYSTEMS			
	Select		
User Setup			
Group Setup	<b>%</b> Q	AAA Client	s 🤶
Shared Profile Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using
Network Configuration	<u>3640</u>	10.14.14.14	TACACS+ (Cisco IOS)
Configuration	PIX-A	172.16.1.85	RADIUS (Cisco IOS/PIX)
Administration Control	<u>VPN3000</u>	172.16.5.2	TACACS+ (Cisco IOS)
External User Databases	WLC	172.16.1.31	RADIUS (Cisco Aironet)
Reports and Activity	WLC Main	172.16.1.50	RADIUS (Cisco Aironet)
Online Documentation	-	Add Entry Sear	ch

3. La clave se utiliza para autenticar entre el router 3640 y el servidor Cisco Secure ACS. Si desea seleccionar el protocolo TACACS+ para la autenticación, elija TACACS+ (Cisco IOS) en el menú desplegable Authenticate Using.

CISCO SYSTEMS	Network Configuration	
antillinaantillina -	Edit	
User Setup		
Group Setup	Ad	d AAA Client
Shared Profile Components	AAA Client Hostname	3640
Network Configuration	AAA Client IP	10.14.14.14
System Configuration	Address	<b></b>
Interface Configuration	Key	cisco123
Administration Control	Authenticate Using	TACACS+ (Cisco IOS)
Databases	□ Single Connect TA accounting on failur	CACS+ AAA Client (Record stop in re).
Reports and Activity	🗖 Log Update/Watch	ndog Packets from this AAA Client
Online Documentation	🗖 Log RADIUS Tum	neling Packets from this AAA Client
	□ Replace RADIUS Client	Port info with Username from this AAA
	Submit	Submit + Restart Cancel

4. Ingrese el nombre de usuario en el campo Usuario en la base de datos de Cisco Secure y luego haga clic en **Agregar/Editar**.En este ejemplo, el nombre de usuario es rtpuser.

CISCO SYSTEMS	User Setup
antiiliinaantiiliina -	Select
User Setup	
Group Setup	User: rtpuser
Shared Profile Components	Find Add/Edit
Network Configuration	
System Configuration	List users beginning with letter/number: A B C D E F G H I J K L M
Interface Configuration	N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9
Administration Control	List All Users
Databases	
Reports and Activity	Back to Help
Online Documentation	

 En la siguiente ventana, introduzca la contraseña para el explorador. En este ejemplo, la contraseña es rtpuserpass. Si lo desea, puede asociar la cuenta del usuario a un grupo. Cuando haya finalizado, haga clic en Submit (Enviar).

CISCO SYSTEMS	User Setup
User Setup	Supplementary User Info 🙎
Group Setup Setup Components	Real Name rtpuser Description
Network Configuration	User Setup
Interface Configuration	Password Authentication: CiscoSecure Database
Administration Control	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
Databases	Confirm
Online Documentation	Password Separate (CHAP/MS-CHAP/ARAP)
	Confirm Password Password
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is
	Submit Delete Cancel

#### Configuración de la función de reserva

Cuando el servidor RADIUS primario deja de estar disponible, el router conmutará por error al siguiente servidor RADIUS de respaldo activo. El router continuará utilizando el servidor RADIUS secundario para siempre incluso si el servidor primario está disponible. Por lo general, el servidor principal es de alto rendimiento y el servidor preferido. Si el servidor secundario no está disponible, la base de datos local se puede utilizar para la autenticación mediante el comando <u>aaa</u> <u>authentication login default group RTP local</u>.

# Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

Establezca un túnel IPSec entre el PC y el router Cisco 3640.

Abra un explorador en el PC y apunte a **http://10.17.17.17**. El router Cisco 3640 intercepta este tráfico HTTP, activa el proxy de autenticación y le solicita un nombre de usuario y una contraseña. El Cisco 3640 envía el nombre de usuario/contraseña al servidor TACACS+ para la autenticación. Si la autenticación es correcta, debería poder ver las páginas web en el servidor web en 10.17.17.17.

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

 <u>show ip access-lists</u> —Muestra las ACL estándar y extendidas configuradas en el router de firewall (incluye entradas de ACL dinámicas). Las entradas de ACL dinámicas se agregan y eliminan periódicamente en función de si el usuario se autentica o no.Esta salida muestra la lista de acceso 118 antes de que se activara auth-proxy:

3640**#show ip access-lists 118** 

```
Extended IP access list 118
10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```

Esta salida muestra la lista de acceso 118 después de que se activó auth-proxy y el usuario autentica correctamente:

```
3640#show ip access-lists 118
   Extended IP access list 118
   permit tcp host 10.20.20.26 any (7 matches)
   permit udp host 10.20.20.26 any (14 matches)
   permit icmp host 10.20.20.26 any
   10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
   20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
   30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```

Las primeras tres líneas de la lista de acceso son las entradas definidas para este usuario y descargadas del servidor TACACS+.

show ip auth-proxy cache — Muestra las entradas del proxy de autenticación o la configuración del proxy de autenticación en ejecución. La palabra clave cache para enumerar la dirección IP del host, el número del puerto de origen, el valor de tiempo de espera para el proxy de autenticación y el estado para las conexiones que utilizan el proxy de autenticación. Si el estado del proxy de autenticación es ESTAB, la autenticación de usuario es correcta.
 3640#show ip auth-proxy cache

```
Authentication Proxy Cache
Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

### Troubleshoot

Para ver los comandos de verificación y depuración, junto con otra información de troubleshooting, consulte <u>Resolución de problemas del Proxy de Autenticación</u>.

**Nota:** Antes de ejecutar un comando **debug**, consulte <u>Información Importante sobre Comandos</u> <u>Debug</u>.

### Información Relacionada

<u>Configuración del Proxy de Autenticación</u>

- Configuraciones de Proxy de Autenticación en Cisco IOS
- Implementación del Proxy de Autenticación en Servidores TACACS+ y RADIUS
- Página de soporte para cliente Cisco VPN
- <u>Página de soporte de firewall de IOS</u>
- Página de soporte de IPSec
- <u>Página de soporte de RADIUS</u>
- <u>Solicitudes de Comentarios (RFC)</u>
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- <u>Soporte Técnico Cisco Systems</u>