Configure los Cisco VPN 3000 Series Concentrators para Soportar la Función NT Password Expiration con el Servidor RADIUS

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Diagrama de la red Configuración del concentrador VPN 3000 Configuración del grupo **Configuración RADIUS** Configuración del servidor de Cisco Secure NT RADIUS Configuración de una entrada para el concentrador VPN 3000 Configuración de la política de usuario desconocido para la autenticación de dominio NT Prueba de la característica de vencimiento de contraseña de NT/RADIUS Prueba de autenticación de RADIUS. Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña Información Relacionada

Introducción

Este documento incluye instrucciones paso a paso sobre cómo configurar los Cisco VPN 3000 Series Concentrators para soportar la función NT Password Expiration usando el servidor RADIUS.

Consulte <u>Función RADIUS VPN 3000 con vencimiento mediante Microsoft Internet Authentication</u> <u>Server</u> para obtener más información sobre el mismo escenario con Internet Authentication Server (IAS).

Prerequisites

Requirements

- Si el servidor RADIUS y el servidor de autenticación de dominio NT están en dos equipos independientes, asegúrese de que ha establecido la conectividad IP entre los dos equipos.
- Asegúrese de que ha establecido la conectividad IP del concentrador al servidor RADIUS. Si el servidor RADIUS se dirige a la interfaz pública, no olvide abrir el puerto RADIUS en el filtro

público.

 Asegúrese de que puede conectarse al concentrador desde el cliente VPN mediante la base de datos de usuario interna. Si esto no está configurado, consulte <u>Configuración de IPSec -</u> <u>Cisco 3000 VPN Client a VPN 3000 Concentrator</u>.

Nota: La función de caducidad de la contraseña no se puede utilizar con clientes VPN Web o SSL.

Componentes Utilizados

Esta configuración fue desarrollada y probada utilizando las versiones de software y hardware indicadas a continuación.

- Versión 4.7 del software del concentrador VPN 3000
- Versión 3.5 de VPN Client
- Cisco Secure para NT (CSNT) versión 3.0 Microsoft Windows 2000 Active Directory Server para autenticación de usuario

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Notas de diagrama

- 1. El servidor RADIUS en esta configuración está en la interfaz pública. Si este es el caso con su configuración específica, cree dos reglas en su filtro público para permitir que el tráfico RADIUS entre y salga del concentrador.
- 2. Esta configuración muestra el software CSNT y los Servicios de autenticación de dominio NT ejecutándose en la misma máquina. Estos elementos se pueden ejecutar en dos máquinas independientes si así lo requiere la configuración.

Configuración del concentrador VPN 3000

Configuración del grupo

 Para configurar el grupo para que acepte los Parámetros de Vencimiento de Contraseña NT del Servidor RADIUS, vaya a Configuración > Administración de Usuario > Grupos, seleccione su grupo de la lista y haga clic en Modificar Grupo. El siguiente ejemplo muestra cómo modificar un grupo denominado



2. Vaya a la pestaña **IPSec**, asegúrese de que **RADIUS con vencimiento** esté seleccionado para el atributo

Authentication.

Configuration | User Management | Groups | Modify ipsecgroup

Check the Inherit? box to set a field that you want to default to the base group value. Uncheck the Inherit? box and enter a new value to override base group values.

Identity General IPSec	Mode Config Client FW	HW Clier	nt [PPTP/L2TP]		
	IPSec Parameters				
Attribute	Value	Inherit?	Description		
IPSec SA	ESP-3DES-MD5	R	Select the group's IPSec Security Association.		
IKE Peer Identity Validation	If supported by certificate 💌	R	Select whether or not to validate the identity of the peer using the peer's certificate.		
IKE Keepalives	2	R.	Check to enable the use of IKE keepalives for members of this group.		
Reauthentication on Rekey		R	Check to reauthenticate the user on an IKE (Phase-1) rekey.		
Tunnel Type	Remote Access 💌	R	Select the type of tunnel for this group. Update the Remote Access parameters below as needed		
			Remote Access Parameters		
Group Lock	D		Lock users into this group.		
Authentication	RADIUS with Expiry	Ē.	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication.		
IPComp	RADIUS	A.	Select the method of IP Compression for members of this group.		
Mode Configuration	RADIUS with Expiry NT Domain SDI	R	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Altiga/Cisco client are being used by members of this group.		
Apply Cancel	Internal				

 Si desea que esta función se habilite en los clientes de hardware VPN 3002, vaya a la pestaña HW Client, asegúrese de que Require Interactive Hardware Client Authentication esté habilitado y haga clic en Apply. Check the Inherit? box to set a field that you want to default to the base group value. Uncheck the Inherit? box and enter a new value to override base group values

Identity General	IPSec Mode Config	Client FW HW Client	PPTPAZTP

Hardware Client Parameters				
Attribute	Value	Inherit?	Description	
Require Interactive Hardware Client Authentication	Я		Check to require the hardware client to be interactively authenticated at each connection attempt.	
Require Individual User Authentication		P.	Check to require users behind a hardware client to be authenticated.	
User Idle Timeout	30	R	Enter the session idle timeout in minutes. Use 0 for no timeout.	
Cisco IP Phone Bypass		R	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.	
Apply Cancel				

Configuración RADIUS

1. Para configurar la configuración del servidor RADIUS en el concentrador, vaya a Configuration > System > Servers > Authentication > Add.

Configuration | System | Servers | Authenti

This section lets you configure parameters for servers that authenticate users.

You should have a property configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and add users to the internal database.

Click the Add button to add a server, or select a server and click Modify, Delete, Move, or Test.



2. En la pantalla Add, escriba los valores que corresponden al servidor RADIUS y haga clic en Add.El ejemplo siguiente utiliza los valores siguientes. Server Type: RADIUS

Authentication Server: 172.18.124.96 Server Port = 0 (for default of 1645) Timeout = 4Reties = 2 Server Secret = cisco123

Verify: cisco123

Configuration S	stom Convore	Authontication Add
configuration (a	ystem Servers	Autientication Aut

Configure and add a user authentication server.

Server Type RADIUS	Selecting Internal Server will let you add users to the internal user database.
Authentication Server 172.18.124.96	Enter IP address or hostname.
Server Port 0	Enter 0 for default port (1645).
Timeout 4	Enter the timeout for this server (seconds).
Retries 2	Enter the number of retries for this server.
Server Secret	Enter the RADIUS server secret.
Verify	Re-enter the secret.
Add Cancel	

Configuración del servidor de Cisco Secure NT RADIUS

Configuración de una entrada para el concentrador VPN 3000

 Inicie sesión en CSNT y haga clic en Configuración de red en el panel izquierdo. En "Clientes AAA", haga clic en Agregar entrada.

Network Configu	iration				
\$		A	AA Client	s	
AAA Client Host	name A	AA Client IP A	ddress	Authenti	icate Using
nsite	172	. 18. 141.40		RADIUS (C	isco IOS/PIX)
		Add Ent	y		
The current conf	iguration	has been cha	nged. Re	start ACS in	a "System
Configuration:So	ervice Con	trol" to ado	pt the new	v settings.	
Configuration:So	ervice Con	trol" to ado	pt the new	w settings.	
Configuration:So	AAA Serve	itrol'' to ado A er IP Address	pt the new	w settings. s AAA Server	Туре
Configuration:So AAA Server Name	AAA Serv 172.18.124	trol'' to ado A er IP Address	AA Server CiscoSecu	w settings. s AAA Server re ACS for Wi	Type ndows 2000/P
Configuration:So AAA Server Name jazib-pc	AAA Serv 172.18.124	atrol" to ado A er IP Address .96 Add Ent	AA Server CiscoSecu	s AAA Server re ACS for Wi	Type ndows 2000/P
Configuration:So AAA Server Name jazib-pc	AAA Serv 172.18.124	A er IP Address 96 Add Ent	AA Server CiscoSecu	w settings. s AAA Server re ACS for Wi	Type ndows 2000/f
Configuration:So AAA Server Name jazib-pc	AAA Servi 172.18.124 Pro	Add Ent	AA Server CiscoSecu y	w settings. s AAA Server re ACS for Wi	Type indows 2000/P

2. En la pantalla "Add AAA Client" (Agregar cliente AAA), escriba los valores adecuados para agregar el concentrador como RADIUS Client y, a continuación, haga clic en Submit + Restart.El ejemplo siguiente utiliza los valores siguientes. AAA Client Hostname = 133_3000_conc

AAA Client IP Address = 172.18.124.133

Key = cisco123

Authenticate using = RADIUS (Cisco VPN 3000)

CISCO SYSTEMS	Network Configuration	
	Edit	
User Setup		
Group Setup		Add AAA Client
Shared Profile Components	AAA Client Hostname	133_3000_conc
Network Configuration	AAA Client IP Address	172.18.124.133
Configuration	Key	cisco123
Administration Control	Authenticate Using	RADIUS (Cisco VPN 3000)
External User Databases	 Single Connect TACACS+. Log Update/Watchdog Pack Log RADIUS Tunneling Pace 	AAA Client (Record stop in accounting on failure). .ets from this AAA Client kets from this AAA Client
Documentation	Subr	it Submit + Restart Cancel

Aparecerá una entrada para su concentrador 3000 en la sección "**Clientes AAA**".

CISCO SYSTEMS	Network Configuration	n	
User Setup		AAA Clie	ents
La Setup	AAA Client Hostname	AAA Client IP Address	Authenticate Using
Components	133 3000 conc	172.18.124.133	RADIUS (Cisco VPN 3000)
Network Configuration	nsite	172.18.141.40	RADIUS (Cisco IOS/PIX)
System Configuration		Add Entry	

Configuración de la política de usuario desconocido para la autenticación de dominio NT

1. Para configurar la autenticación de usuario en el servidor RADIUS como parte de la política de usuario desconocida, haga clic en **Base de datos de usuario externa** en el panel izquierdo y luego haga clic en el enlace **Configuración de base de datos**.



2. En "Configuración de base de datos de usuario externa", haga clic en Windows NT/2000.

CISCO SYSTEMS	External User Databases	
	Select	
User Setup		
Group Setup	External User Database Configuration	?
Shared Profile Components	Choose which external user database type to configure.	
Network Configuration	NIS/NIS+	
System Configuration	LEAP Proxy RADIUS Server	
1 contrigue action	Windows NT/2000	
Configuration	Novell NDS	
	Generic LDAP	
Control	External ODBC Database	
External User	RADIUS Token Server	
J Valabases	AXENT Token Server	
Activity	CRYPTOCard Token Server	
and Online	SafeWord Token Server	
Documentation	SDI SecurID Token Server	
	List all database configurations	
	Cancel	

3. En la pantalla "Database Configuration Creation" (Creación de la configuración de la base de datos), haga clic en **Create New Configuration (Crear nueva configuración)**.

CISCO SYSTEMS	External User Databases	
and the and the second	Edit	
User Setup		
Group Setup	Database Configuration Creation	?
Shared Profile Components	Click here to create a new configuration for the Windows NT/2000 database.	
Sustem Configuration	Create New Configuration	
Administration	Cancel	

 Cuando se le solicite, escriba un nombre para la autenticación NT/2000 y haga clic en Enviar. El siguiente ejemplo muestra el nombre "Expiración de contraseña de Radius/NT".

Cisco Systems	External User Databases	
	Edit	
User Setup	Create a new External Database Configuration	?
Shared Profile Components	Enter a name for the new configuration for Windows NT/2000	
Network Configuration System Configuration	Radius/NT Password Expiration Submit Cancel	
Configuration		

5. Haga clic en **Configurar** para configurar el nombre de dominio para la autenticación de usuario.

CISCO SYSTEMS	External User Databases	
adillinadillina.	Edit	
User Setup		
Group Setup	External User Database Configuration	?
Shared Profile Components	Choose what to do with the Windows NT/2000 database.	
Network Configuration	Configure Delete	
System Configuration	Configure Defete	
Configuration		

6. Seleccione su dominio NT en "Available Domains" (Dominios disponibles) y, a continuación, haga clic en el botón de flecha derecha para agregarlo a la "Domain List" (Lista de dominios). En "MS-CHAP Settings," asegúrese de que las opciones para Permit password changes using MS-CHAP version 1 y version 2 estén seleccionadas. Haga clic en Enviar cuando haya terminado.



7. Haga clic en Base de datos de usuario externa en el panel izquierdo y, a continuación, haga clic en el vínculo para Asignaciones de grupo de base de datos (como se muestra en este <u>ejemplo</u>). Debería ver una entrada para su base de datos externa configurada previamente. El siguiente ejemplo muestra una entrada para "Expiración de contraseña de RADIUS/NT", la base de datos que acabamos de configurar.



8. En la pantalla "Domain Configurations" (Configuraciones de dominio), haga clic en **New configuration** para agregar las configuraciones de dominio

CISCO SYSTEMS	External User Databases	
	Edit	
User Setup		
Group Setup		
Shared Profile Components	Domain Configurations	2
Network Configuration	DEFAULT	
System Configuration	New configuration	

 Seleccione su dominio de la lista de "Dominios detectados" y haga clic en Enviar. El siguiente ejemplo muestra un dominio llamado "JAZIB-ADS".

CISCO SYSTEMS	External User Databases			
االانسىياالانسا	Edit			
User Setup				
Group Setup	Define New Domain Configuration	?		
Shared Profile Components	JAZIB-ADS			
Network Configuration				
System Configuration	Detected Domains:			
Configuration	Clear Selection			
Administration Control	Domain :			
Databases				
Reports and Activity	Submit Cancel			

10. Haga clic en su nombre de dominio para configurar las asignaciones de grupo. Este ejemplo muestra el dominio "JAZIB-

ADS". Cisco Systems	External User Databases	
User Setup	Edit	
Sroup Setup	Domain Configurations	?
Net work Configuration	JAZIB-ADS VDEFAULT	
System Configuration	New configuration	

11. Haga clic en **Agregar asignación** para definir las asignaciones de grupo.

CISCO SYSTEMS	External User Databases		
halling and the s	Edit		
User Setup			
Group Setup	Group Mappi	ngs for Domain : JAZIB-ADS 🔋	
Shared Profile Components	NT groups	CiscoSecure group	
Network Configuration	-	no mappings defined -	
System Configuration			
Configuration		Add mapping	
Administration Control		Delete Configuration	
External User Databases		Selete Configuration	

12. En la pantalla "Crear asignación de grupo nuevo", asigne el grupo en el dominio NT a un grupo en el servidor RADIUS CSNT y, a continuación, haga clic en **Enviar**. El siguiente ejemplo asigna el grupo NT "Users" al grupo RADIUS "Group

1". Cisco Systems	External User Databases	
antillitura tillitura -	Edit	
User Setup		
Group Setup	Create new group mapping for Domain : JAZIB-ADS	?
Shared Profile Components	Define NT group set	
Configuration	Administrators	
System Configuration	Guests Backup Operators	
Interface Configuration	Replicator Server Operators Account Operators Print Operators	
Administration Control	Add to selected Remove from selected	
External User Databases	Selected	
Reports and Activity		
Documentation		
	Up	
	CiscoSecure group: Group 1	
	Submit Cancel	

13. Haga clic en Base de datos de usuario externa en el panel izquierdo y, a continuación,

haga clic en el vínculo **Política de usuario desconocida** (como se muestra en este <u>ejemplo</u>). Asegúrese de que la opción para **Verificar las siguientes bases de datos de usuario externas** esté seleccionada. Haga clic en el botón de flecha hacia la derecha para mover la base de datos externa configurada previamente de la lista "Bases de datos externas" a la lista "Bases de datos



Prueba de la característica de vencimiento de contraseña de NT/RADIUS

El concentrador ofrece una función para probar la autenticación RADIUS. Para probar esta función correctamente, asegúrese de seguir estos pasos con cuidado.

Prueba de autenticación de RADIUS.

 Vaya a Configuration > System > Servers > Authentication. Seleccione su servidor RADIUS y haga clic en Test. This section lets you configure parameters for servers that authenticate users.

You should have a property configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and add users to the internal database.

Click the Add button to add a server, or select a server and click Modify, Delete, Move, or Test.

Authentication Servers	Actions
Internal (Internal)	Add
172.18.124.96 (Radius)	Modify
	Delete
	Move Up
	Move Down
	Test

 Cuando se le solicite, escriba su nombre de usuario y contraseña de dominio NT y, a continuación, haga clic en Aceptar. El siguiente ejemplo muestra el nombre de usuario "jfrahim" configurado en el servidor de dominio NT con "cisco123" como contraseña.

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.





3. Si la autenticación está configurada correctamente, debe recibir un mensaje que diga "Autenticación



correcta".

Si recibe algún

mensaje que no sea el que se muestra arriba, hay algún problema de configuración o conexión. Repita los pasos de configuración y prueba descritos en este documento para asegurarse de que todos los parámetros se hayan realizado correctamente. Compruebe también la conectividad IP entre los dispositivos.

<u>Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña</u>

 Si el usuario ya está definido en el servidor de dominio, modifique las propiedades para que se le pida al usuario que cambie la contraseña en el próximo inicio de sesión. Vaya a la ficha "Cuenta" del cuadro de diálogo de propiedades del usuario, seleccione la opción para El

usuario debe cambiar la contraseña en el siguiente inicio de sesión y haga clic en Aceptar.

Console1 - [Console Root	Active Direct	tory Users and (Computers [jazib-pc.jazib.cisco.com]\jazib.cisco.com\Users]
📸 Console Window Help			
Action View Eavorites	🗢 🔿 🗈 💽	🗙 💼 🙆 😫	2000 10 7 400
Action Yew Eavorites I Tree Favorites I Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Console Root Image: Consot Image: Console Root	 Administra Administra Cert Publis Cert Publis Cort Publis Cort Publis DonsUpdat Donain A Domain C Domain C Domain G Domain G Domain Us Coup Poll Group Poll Group Poll Group Poll Group Poll Group Poll INAM_JAZ Jazb Frahim Krbtgt NetShow NetShow S RAS and I TsInternet 	Ver Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro User User User User User Security Gro Security Gro User Security Gro User Security Gro User Security Gro User Security Gro User	Jazib Frahim Properties ? × Dial-in Environment Sessions Remote control Terminal Services Profile General Address Account Profile Telephones Organization Member Of User logon name: [frahim @jazib.cisco.com • User logon name (pre-Windows 2000): JAZIB-ADS\ [frahim Log On Hours Log On To • Account is focked out Account options: • Ver cannot change password at next logon • • Ver cannot change password • • Account expires • • • Store password using reversible encryption • • Account expires • • • • Never • • • • • OK Cancel Apply •

2. Inicie el cliente VPN y luego intente establecer el túnel al

C onne	ISCO SYSTEMS
0	Enter Username and Password.
	Username:
	ifrahim
	Password:
Initi	******
Cor	Save Password
	Domain:
	JAZIB-ADS
	OK Cancel

3. Durante la autenticación de usuario, se le solicitará que cambie la

L	Jser Authentication for lab
	Your password expired
	New Password:
	Confirm Password:
contraseña	OK Cancel

Información Relacionada

- <u>Concentrador Cisco VPN serie 3000</u>
- IPSec
- <u>Cisco Secure Access Control Server para Windows</u>
- RADIUS
- Solicitudes de Comentarios (RFC)