Configurare i Cisco VPN serie 3000 concentrator per supportare la funzione di scadenza password di NT con il server RADIUS

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Esempio di rete Configurazione di VPN 3000 Concentrator Configurazione gruppo **Configurazione RADIUS** Configurazione di Cisco Secure NT RADIUS Server Configurazione di una voce per il concentratore VPN 3000 Configurazione del criterio utente sconosciuto per l'autenticazione del dominio NT Test della funzionalità di scadenza delle password NT/RADIUS Test di autenticazione RADIUS Autenticazione del dominio NT effettiva tramite proxy RADIUS per verificare la funzionalità di scadenza password Informazioni correlate

Introduzione

In questo documento vengono fornite istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator in modo da supportare la funzione di scadenza della password NT con il server RADIUS.

Per ulteriori informazioni sullo stesso scenario con il server di autenticazione Internet (IAS, Internet Authentication Server), fare riferimento alla <u>VPN 3000 RADIUS con funzionalità di</u> <u>scadenza</u> che<u>utilizza</u> il server di autenticazione Internet (Internet Authentication Server).

Prerequisiti

Requisiti

- Se il server RADIUS e il server Autenticazione dominio NT si trovano su due computer distinti, accertarsi di aver stabilito la connettività IP tra i due computer.
- Accertarsi di aver stabilito la connettività IP tra il concentratore e il server RADIUS. Se il server RADIUS è rivolto verso l'interfaccia pubblica, non dimenticare di aprire la porta

RADIUS sul filtro pubblico.

 Accertarsi di poter connettersi al concentratore dal client VPN utilizzando il database degli utenti interni. Se non è configurata, consultare il documento sulla <u>configurazione di IPSec -</u> <u>Cisco 3000 VPN Client su VPN 3000 Concentrator</u>.

Nota: non è possibile usare la funzione di scadenza password con client VPN Web o SSL.

Componenti usati

Questa configurazione è stata sviluppata e testata utilizzando le versioni software e hardware riportate di seguito.

- VPN 3000 Concentrator Software versione 4.7
- VPN Client release 3.5
- Cisco Secure for NT (CSNT) versione 3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Note diagramma

- 1. Il server RADIUS in questa configurazione si trova nell'interfaccia pubblica. In questo caso, creare due regole nel filtro pubblico per consentire al traffico RADIUS di entrare e uscire dal concentratore.
- 2. Questa configurazione mostra il software CSNT e i servizi di autenticazione di dominio NT in esecuzione sullo stesso computer. Questi elementi possono essere eseguiti su due computer separati se richiesto dalla configurazione.

Configurazione di VPN 3000 Concentrator

Configurazione gruppo

 Per configurare il gruppo in modo che accetti i parametri di scadenza password NT dal server RADIUS, andare a Configurazione > Gestione utente > Gruppi, selezionare il gruppo dall'elenco e fare clic su Modifica gruppo. Nell'esempio seguente viene illustrato come modificare un gruppo denominato

 "ipsecgroup".
 Condiguration [User Management] Groups
 Save Needed 2

 This section lets you configure groups. A group is a collection of users treated as a single entity.
 Click the Add Group button to add a group, or select a group and thick Delete Group or Modify Group. To modify other group parameters, thick Modify Auth. Servers, Modify Act. Servers Modify Address Pools or Modify Client Update.

 Current Groups
 Actions

 Modify Address Pools
 Modify Address Pools

 Modify Client Update
 Delete Group

2. Andare alla scheda IPSec e verificare che per l'attributo Authentication sia selezionato RADIUS con

scadenza.

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	S.	Select the group's IPSec Security Association.		
IKE Peer Identity Validation	It supported by certificate 💌	R	Select whether or not to validate the identity of the peer using the peer's certificate.		
IKE Keepalives	R	4	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 💌	E.	Select the type of tunnel for this group. Update the Remote Access parameters below as needed		
			Remote Access Parameters		
Group Lock	—		Lock users into this group.		
Authentication	RADIUS with Expiry	ŗ.	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication.		
IPComp	PADIUS	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				

 Se si desidera abilitare questa funzionalità sui client hardware VPN 3002, passare alla scheda Client hardware, verificare che Richiedi autenticazione client hardware interattivo sia abilitato, quindi fare clic su Applica. 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

entity General IPSec Mode Config Client FW HW Client PPTP/L2TP					
Hardware Client Parameters					
Attribute	Value	Inherit?	Description		
Require Interactive Hardware Client Authentication	R		Check to require the hardware client to be interactively authenticated at each connection attempt.		
Require Individual User Authentication		E.	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

Configurazione RADIUS

Apply Cancel

1. Per configurare le impostazioni del server RADIUS sul concentratore, selezionare Configurazione > Sistema > Server > Autenticazione > Aggiungi.

Configuration

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. Nella schermata Aggiungi, immettere i valori che corrispondono al server RADIUS e fare clic su Aggiungi.Nell'esempio seguente vengono utilizzati i valori seguenti. 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	vetom Sorvore	Authentication Add
configuration (a	ystem Servers	Muurenucauun Muu

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 Antonian	Re-enter the secret.
Add Cancel	

Configurazione di Cisco Secure NT RADIUS Server

Configurazione di una voce per il concentratore VPN 3000

1. Accedere a CSNT e fare clic su **Configurazione di rete** nel pannello sinistro. In "Client AAA", fare clic su **Add Entry** (Aggiungi voce).

Select	indition				
%		A	AAA Client	ts	
AAA Client Host	name A/	AA Client IP A	Address	Authenti	icate Using
nsite	172.	18.141.40		RADIUS (C	lisco IOS/PIX
		Add Ent	Ŋ		
The current conf	iguration h	ias been cha	nged. Re	start ACS in	n "System
Configuration:So	ervice Cont	rol" to ado	pt the new	w settings.	
Configuration:Se	ervice Cont	rol" to ado	pt the new	w settings.	
Configuration:So AAA Server Name	ervice Cont	rol'' to ado A r IP Address	pt the new	w settings. 's AAA Server	Туре
Configuration:So AAA Server Name	AAA Serve	rol" to ado A r IP Address 96	pt the new AA Server CiscoSecu	w settings. s AAA Server re ACS for Wi	Type ndows 2000/1
Configuration:Se AAA Server Name jazib-pc	AAA Serve	A The second sec	AA Server CiscoSecu	w settings. s AAA Server re ACS for Wi	Type indows 2000/1
Configuration:Se AAA Server Name jazib-pc	AAA Serve 172.18.124.	A r IP Address 96 Add Ent xy Distributio	AA Server CiscoSecu	w settings. 's AAA Server re ACS for Wi	Type indows 2000/1
Configuration:So AAA Server Name jazib-pc	AAA Serve 172.18.124 Pro	A r IP Address 96 Add Ent xy Distributio	AA Server CiscoSecu	w settings. s AAA Server re ACS for Wi Strip	Type indows 2000/1 Account

 Nella schermata "Add AAA Client" (Aggiungi client AAA), immettere i valori appropriati per aggiungere il concentratore come client RADIUS, quindi fare clic su Submit (Invia) + Riavvia (Riavvia).Nell'esempio seguente vengono utilizzati i valori seguenti. 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+	AAA Client (Record stop in accounting on failure).
Reports and Activity	Log RADIUS Tunneling Pac	kets from this AAA Client
Documentation	Subr	it Submit + Restart Cancel

Nella sezione "Client AAA" verrà visualizzata una voce relativa al concentratore 3000.

CISCO SYSTEMS	Network Configuration				
hallinaatiina.	Select				
Setup	\$	AAA Clie	ents 🤶		
an I Shared Profile	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/PEX)		
System Configuration		Add Entry			

Configurazione del criterio utente sconosciuto per l'autenticazione del dominio NT

1. Per configurare l'autenticazione utente sul server RADIUS come parte del criterio utente sconosciuto, fare clic su **Database utente esterno** nel riquadro sinistro, quindi fare clic sul collegamento **Configurazione database**.



2. In "Configurazione database utenti esterni", fare clic su Windows NT/2000.

CISCO SYSTEMS	External User Databases	
tillutillu	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	LEAP Proxy RADIUS Server	
Contiguration	Windows NT/2000	
Configuration	Novell NDS	
- Administration	Generic LDAP	
Control	External ODBC Database	
External User	RADIUS Token Server	
Databases	AXENT Token Server	
Activity	CRYPTOCard Token Server	
and Online	SafeWord Token Server	
Documentation	SDI SecurID Token Server	
	List all database configurations	
	Cancel	

3. Nella schermata "Creazione della configurazione del database", fare clic su Crea nuova configurazione.

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

4. Quando richiesto, digitare un nome per l'autenticazione NT/2000 e fare clic su Invia. Nell'esempio seguente viene illustrato il nome "Radius/NT Password Expiration" (Scadenza password 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 Radius/NT Password Expiration	
System Configuration	Submit Cancel	

5. Fare clic su **Configura** per configurare il nome di dominio per l'autenticazione utente.

CISCO SYSTEMS	External User Databases	
	Edit	
Setup		i.
Group Setup	External User Database Configuration	and the second se
Shared Profile Components	Choose what to do with the Windows NT/2000 database.	
Network Configuration	Configure Delete	
System Configuration		
Configuration		Transferration of the local distribution of

6. Selezionare il proprio dominio NT da "Domini disponibili", quindi fare clic sul pulsante freccia destra per aggiungerlo all'elenco dei domini. In "MS-CHAP Settings" (Impostazioni MS-CHAP) verificare che le opzioni per Permit password changes using MS-CHAP version 1 and version 2 (Consenti modifiche password utilizzando MS-CHAP versione 1 e versione 2) siano selezionate. Al termine, fare clic su Submit (Invia).



7. Fare clic su Database utente esterno nel pannello a sinistra, quindi fare clic sul collegamento per i mapping dei gruppi di database (come mostrato nell'esempio). Verrà visualizzata una voce per il database esterno configurato in precedenza. L'esempio seguente mostra una voce per "Radius/NT Password Expiration", il database appena configurato.



8. Nella schermata "Domain Configurations" (Configurazioni dominio), fare clic su **New configuration** (Nuova configurazione) per aggiungere le configurazioni di dominio

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

 Selezionare il proprio dominio dall'elenco "Domini rilevati" e fare clic su Invia. Nell'esempio seguente viene illustrato un dominio denominato "JAZIB-ADS".

CISCO SYSTEMS	External User Databases	
User Setup		
Setup	Define New Domain Configuration	2
Shared Profile Components	JAZIB-ADS	
Network Configuration		
System Configuration	Detected Domains:	
Configuration	Clear Selection	
Administration Control	Domain :	
Databases		
Reports and Activity	Submit Cancel	

 Fare clic sul nome di dominio per configurare i mapping dei gruppi. Nell'esempio viene mostrato il dominio "JAZIB-ADS".

CISCO SYSTEMS	External User Databases	
ومتلكل التسمينا التسا	Edit	
User Setup		
Group Setup	1	Tabatan C
Shared Profile	Domain Configurations	?
Network	JAZIB-ADS	
	<u>\DEFAULT</u>	
Configuration	New configuration	
Configuration		

11. Fare clic su **Aggiungi mapping** per definire i mapping dei

gruppi.	External User Databases	
User Setup	Edit	
Group Setup	Group Mappings for Domain : JAZIB-ADS	?
Shared Profile Components Net work Configuration	NT groups CiscoSecure group - no mappings defined -	
System Configuration	Add mapping	
Administration Control	Delete Configuration	

12. Nella schermata "Crea nuova mappatura gruppo", mappare il gruppo sul dominio NT a un gruppo sul server RADIUS CSNT, quindi fare clic su **Invia**. Nell'esempio seguente il gruppo NT "Users" viene mappato al gruppo RADIUS "Group 1".

CISCO SYSTEMS	External User Databases
ամինտանինութ	Edit
User Setup	
Group Setup	Create new group mapping for Domain : JAZIB-ADS 🔗
Shared Profile Components	Define NT group set
Configuration	NT Groups
System Configuration	Guests Backup Operators Replicator
Configuration	Account Operators Print Operators
Administration Control	Add to selected Remove from selected
Databases	Selected
Reports and Activity	
Online Documentation	
	Up. Down
	CiscoSecure group: Group 1
	Submit Cancel

13. Fare clic su **Database utenti esterni** nel pannello a sinistra, quindi fare clic sul collegamento per **Criteri utente sconosciuti** (come illustrato in questo <u>esempio</u>). Assicurarsi che l'opzione **Controlla i seguenti database utenti esterni** sia selezionata. Fare clic sul pulsante freccia destra per spostare il database esterno configurato in precedenza dall'elenco "Database esterni" all'elenco "Database selezionati".



Test della funzionalità di scadenza delle password NT/RADIUS

Il concentratore offre una funzione per testare l'autenticazione RADIUS. Per verificare correttamente questa funzionalità, eseguire la procedura descritta di seguito.

Test di autenticazione RADIUS

1. Andare a **Configurazione > Sistema > Server > Autenticazione**. Selezionare il server RADIUS e fare clic su





 Quando richiesto, digitare il nome utente e la password di dominio NT e quindi fare clic su OK. L'esempio seguente mostra il nome utente "jfrahim" configurato sul server di dominio NT con "cisco123" come password.



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

User Name jfrahim Password

OK Cancel

3. Se l'autenticazione è configurata correttamente, dovrebbe essere visualizzato il messaggio "Autenticazione



riuscita".

Se si riceve un

messaggio diverso da quello mostrato sopra, si è verificato un problema di configurazione o connessione. Ripetere i passaggi di configurazione e test descritti in questo documento per verificare che tutte le impostazioni siano state eseguite correttamente. Verificare inoltre la connettività IP tra i dispositivi.

Autenticazione del dominio NT effettiva tramite proxy RADIUS per verificare la funzionalità di scadenza password

 Se l'utente è già definito nel server di dominio, modificare le proprietà in modo che all'utente venga richiesto di modificare la password al successivo accesso. Nella scheda Account della finestra di dialogo delle proprietà dell'utente, selezionare l'opzione Cambiamento obbligatorio password all'accesso successivo, quindi fare clic su OK.

🛅 Console1 - [Console Roo	ot\Active Direc	tory Users and	Computers [jazib-pc.jazib.cisco.com]\jazib.cisco.com\Users]
Console Window Help	0		
Action View Eavorites	← →	🗙 🗗 🔂 🖄	2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Tree Favorites	Name	Туре	Jazib Frahim Properties
Console Root	Administra Cert Publis disco c. cls DrsAdmins DrsUpdat Domain A Domain A Domain C Domain G Domain G Domain Us Enterprise Group Poli Guest IUSR_JAZI Jazb Frahim krbtgt NetShow RAS and I Schema A TsInternet	User Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro User User User User User User Security Gro User Security Gro User Security Gro User Security Gro User Security Gro User User User User User User User User	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 Logon Hours Log On To • Account is locked out Account options: • Ø User rannot change password at next logon • Ø User cannot change password • • Password never expires • Store password using reversible encryption • Account expires • Never • • • Never • • •
			OK Cancel Apply

2. Avviare il client VPN, quindi provare a stabilire il tunnel per il

	ISCO SYSTEMS
0	Enter Username and Password. Username:
	jírahim
	Password:
niti Cor Autl	Save Password
	JAZIB-ADS
	OK Cancel

concentratore.

3. Durante l'autenticazione utente, verrà richiesto di modificare la

Jser A	uthentication for lab
A	Your password expired
New	Dassimord.
	assmola.
Confir	m Password:
	OK Cancel

password.

Informazioni correlate

- <u>Cisco VPN serie 3000 Concentrator</u>
- IPSec
- <u>Cisco Secure Access Control Server per Windows</u>
- <u>RAGGIO</u>
- RFC (Requests for Comments)