## RADIUS サーバを使用して NT のパスワード期 限切れ機能をサポートするための Cisco VPN 3000 シリーズ コンセントレータの設定

### 内容

概要
前提条件
要件
使用するコンポーネント
ネットワーク図
VPN 3000 コンセントレータの設定
グループの設定
RADIUSの設定
Cisco Secure NT RADIUS サーバの設定
VPN 3000 コンセントレータ用のエントリの設定
NT ドメイン認証のための未知のユーザのポリシーの設定
NT ドメイン認証のための未知のユーザのポリシーの設定
NT/RADIUS パスワード有効期限設定機能のテスト
RADIUS認証のテスト
RADIUS プロキシを使用する実際の NT ドメイン認証によるパスワード期限切れ機能のテスト
関連情報

### <u>概要</u>

このドキュメントでは、RADIUS サーバを使用して NT パスワード期限切れ機能をサポートする ために、Cisco VPN 3000 シリーズ コンセントレータを設定する方法について段階的に説明しま す。

Internet Authentication Server(IAS)と同じシナリオについての詳細は、『<u>Microsoft Internet</u> <u>Authentication Serverを使用したVPN 3000 RADIUSの有効期限機能</u>』を参照してください。

## <u>前提条件</u>

#### <u>要件</u>

- ・使用する RADIUS サーバと NT ドメイン認証サーバが別々の2台のマシンである場合は、その2台のマシン間で IP 接続を確立してください。
- また、コンセントレータから RADIUS サーバへの IP 接続も確立する必要があります。
   RADIUS サーバがパブリック インターフェイスに接続している場合は、パブリック フィルタの RADIUS ポートを開いておくことを忘れないでください。

 さらに、内部のユーザ データベースを使用して、VPN クライアントからコンセントレータへ 接続できることを確認してください。この接続が設定されていない場合は、『<u>IPSec の設定 -</u> <u>Cisco 3000 VPN クライアントから VPN 3000 コンセントレータへ</u>』を参照してください。

**注:パスワ**ードの有効期限機能は、Web VPNまたはSSL VPNクライアントでは使用できません 。

#### <u>使用するコンポーネント</u>

この設定の作成とテストは、次のソフトウェアとハードウェアのバージョンで行われています。

- VPN 3000 コンセントレータ ソフトウェア バージョン 4.7
- VPN クライアント リリース 3.5
- Cisco Secure for NT(CSNT)バージョン3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### <u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



#### ダイアグラムノート

- この構成での RADIUS サーバは、パブリック インターフェイスに接続されています。使用 する設定がこれと同じ場合には、パブリック フィルタに 2 つのルールを作成して、RADIUS サーバのトラフィックがコンセントレータに出入りできるようにしてください。
- 2. この設定では、CSNT ソフトウェアと NT ドメイン認証サービスが同一のマシン上で実行されています。これらは、必要な場合には別々のマシンで実行することもできます。

### <u>VPN 3000 コンセントレータの設定</u>

#### <u>グループの設定</u>

1. RADIUSサーバからNT Password Expiration Parametersを受け入れるようにグループを設定 するには、[Configuration] > [User Management] > [Groups]に移動し、リストからグループ を選択して、[Modify Group] をクリックします。次の例では、「ipsecgroup」という名前の グループの設定の変更方法について説明します。

Condiguration | User Management | Groups
Save Needed

2. IPSec タブで、Authentication の属性に RADIUS with Expiry が選択されていることを確認し ます。

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	it 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	N	S.	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	<b>—</b>		Lock users into this group.
Authentication	RADIUS with Expiry		Select the authentication method for members of this group. This parameter does not apply to <b>Individual User</b> 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		

3. この機能を VPN 3002 ハードウェア クライアントでイネーブルにする場合は、HW Client タ ブで、Require Interactive Hardware Client Authentication がイネーブルにされていることを 確認して、Apply をクリックします。

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

al IPSec Mode Config Client FW HW Client PPTP/LZTP Hardware Client Parameters Attribute Value Inherit? Description **Require Interactive Hardware Client** Check to require the hardware client to be interactively authenticated at each connection attempt. Authentication Require Individual User Authentication ч Check to require users behind a hardware client to be authenticated. User Idle Timeout 30 4 Enter the session idle timeout in minutes. Use 0 for no timeout. Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware Cisco IP Phone Bypass 되 lient Apply Cancel

#### <u>RADIUSの設定</u>

1. コンセントレータでRADIUSサーバの設定を行うには、Configuration > System > Servers > Authentication > Addの順に選択します。

Configuration | System | Servers | Authentication

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
	Modify
	Delete
	Move Up
	Move Down
	Test

2. Add 画面で、RADIUS サーバに対応する値を入力して、Add をクリックします。下の例では 、次の値を使用しています。

Server Type: RADIUS

Authentication Server: 172.18.124.96

Server Port = 0 (for default of 1645)

Timeout = 4

Reties = **2** 

Server Secret = cisco123

Verify: cisco123

#### Configuration | System | Servers | Authentication | Add

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 Antonion	Re-enter the secret.
Add Cancel	

### <u>Cisco Secure NT RADIUS サーバの設定</u>

#### <u>VPN 3000 コンセントレータ用のエントリの設定</u>

1. CSNT にログインして、左側のパネルで Network Configuration をクリックします。「AAA Clients」の下にある Add Entry をクリックします。

CISCO SYSTEMS	Vetwork Configu	ration				
Section Sectio	elect					
User Setup	<b>%</b>		1	AAA Clients		?
Setup	AAA Client Host	name	AAA Client IP #	Address	Authenti	cate Using
Components	nsite		172.18.141.40		RADIUS (C	isco IOS/PIX)
Network Configuration System Configuration	<u> </u>		Add Ent	ry .		
Interface Configuration	The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings.					
External User Databases	AAA Servers					
Activity	AAA Server Name	AAA S	erver IP Address	1	AA Server	Туре
Documentation	jazib-pc	172.18	124.96	CiscoSecure	ACS for Wi	ndows 2000/NT
			Add Ent	ry		
			Proxy Distributio	n Table		?
	Character S	tring	AAA S	ervers	Strip	Account
	(Default)	)	jazib-pc		No	Local
			Add Entry S	ort Entries		

2. 「Add AAA Client」の画面で、適切な値を入力して、コンセントレータを RADIUS クライア ントとして追加し、Submit + Restart をクリックします。下の例では、次の値を使用してい ます。

AAA Client Hostname = **133\_3000\_conc** 

AAA Client IP Address = 172.18.124.133

Key = cisco123

CISCO SYSTEMS	Network Configuration				
ամհասութ	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	1 3000)		
External User	🖂 Single Connect TACACS+ AAA Client (Record stop in accounting on failure).				
Databases	🗖 Log Update/Watchdog Packets from this AAA Client				
Activity	🗖 Log RADIUS Tunneling P	ackets from this AAA Client			
Documentation	Submit Submit + Restart Cancel				
使用する 3000 I ます。 <sup>Cisco Systems</sup>	コンセントレータのエン Network Configuratio	トリは、「AAA Clients」 <b>n</b>	セクションの下に表示され		
User	COUCH .				
Group	<b>%</b>	AAA Clie	ents 🤶		
and Security	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			

#### NT ドメイン認証のための未知のユーザのポリシーの設定

1. RADIUS サーバで Unknown User Policy の一部としてユーザ認証を設定する場合は、左側の パネルで External User Database をクリックして、「Database Configuration」へのリンク をクリックします。



2. 「External User Database Configuration」の下にある Windows NT/2000 をクリックします

o

CISCO SYSTEMS	External User Databases	
User Setup	Select	
Shared Profile Components	External User Database Configuration Choose which external user database type to configure	
Network Configuration System Configuration Interface Configuration Administration Control External User Databases External User Databases Reports and Activity Online Documentation	NIS/NIS+ LEAP Proxy RADIUS Server Windows NT/2000 Novell NDS Generic LDAP External ODBC Database RADIUS Token Server AXENT Token Server CRYPTOCard Token Server Safe Word Token Server	
	List all database configurations Cancel	

3. 「Database Configuration Creation」画面で、Create New Configuration をクリックします

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

4. プロンプトが表示されたら、NT/2000 認証のための名前を入力して、Submit をクリックし ます。次の例では、「Radius/NT Password Expiration」という名前を使用しています。

Cisco Systems	External User Databases	
tlltmtlltm	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. Configure をク	リックして、ユーザ認証用のドメイン名を設定します。 External User Databases Edit	
User Setup	External User Database Configuration	?

	Configuration
6.	「Available Domains」から NT ドメインを選択し、右矢印ボタンをクリックして、これを「
	Domain List」に追加します。 「MS-CHAP Settings」で、Permit password changes using
	MS-CHAP version 1 と version 2 のオプションが選択されていることを確認します。設定が
	終了したら、[Submit] をクリックします。

| Shared Profile | Components

Network Configuration

System Configuration

4

Configure

Choose what to do with the Windows NT/2000 database.

Delete

?



7. 左側のパネルで External User Database をクリックし、次に「Database Group Mappings」 へのリンクをクリックします(この例を参照してください)。 先に設定した外部データベ ースのエントリが表示されます。次の例では、先ほど設定したデータベースである「 Radius/NT Password Expiration」のエントリが表示されています。

CISCO SYSTEMS	External User Databases		
autiliturautilitura	Select		
User Setup			
Group Setup	Unknown User G	roup Mappings 🎅	
Shared Profile Components	Choose the External User Database for which you want to configure the group mappings.		
Network Configuration	Name	Туре	
System Configuration	Radius/NT Password Expiration	Windows NT/2000	
Interface Configuration			
Administration Control	Ca	ancel	
Databases			

8. 「Domain Configurations」画面で、New configuration をクリックして、ドメイン設定を追

加します。 Cisco Systems	External User Databases	
Ratilinanatilina.	Edit	
User Setup		
Group Setup	Domain Configurations	2
Shared Profile Components		
Network Configuration	<u>\DEFAULT</u>	
System Configuration	New configuration	

9. 「Detected Domains」のリストから使用するドメインを選択して、Submit をクリックしま す。次の例では、「JAZIB-ADS」という名前のドメインを示しています。

Cisco Systems	External User Databases
User Setup	Edit
Group Setup	Define New Domain Configuration
Shared Profile Components	JAZIB-ADS
Network Configuration	Detected Domains:
Configuration	
Administration Control	Domain :
External User Databases	Submit Cancel

10. 使用するドメイン名をクリックして、グループのマッピングを設定します。次の例では、 ドメイン「JAZIB-ADS」が表示されています。

CISCO SYSTEMS	External User Databases	
الاستينالاس	Edit	
User Setup		
Group Setup	Denvis Conferentian	9
Shared Profile Components	Domain Configurations	1
Network Configuration	JAZIB-ADS \DEFAULT	
System Configuration	New configuration	
Configuration		

11. Add mapping をクリックして、グループのマッピングを定義します。

CISCO SYSTEMS	External User Databases		
hatilinaantiina.	Edit		
User Setup			
Group Setup	Group Mappin	gs for Domain : JAZIB-ADS	?
Shared Profile Components	NT groups	CiscoSecure group	
Configuration	- 1	no mappings defined -	
Interface Configuration		Add mapping	
Administration Control		elete Configuration	
Databases			

12. 「Create new group mapping」画面で、NT ドメイン上のグループを、CSNT RADIUS サ ーバ上のグループにマップして、Submit をクリックします。次の例では、NT グループ「 Users」を RADIUS グループの「Group 1」にマップしています。

		/ •/		
CISCO SYSTEMS	External	User	Database	S

Group   Setup	Create new group mapping for Domain : JAZIB-ADS	
Shared Profile Components	Define NT mean set	
-I Network	Denne 141 group set	
Configuration	Administrators	
Sustem	Guests	
Configuration	Backup Operators	
Linterface	Server Operators	
Configuration	Account Operators	
LAdministration		
Control	Add to selected Remove from selected	
External User	Selected	
Databases	Users	
Reports and		
Activity		
Online		
Documentation		
	Up Down	
	<u>.</u>	
	CiscoSecure group: Group 1	

13. 左側のパネルで External User Database をクリックし、次に「Unknown User Policy」への リンクをクリックします(この例を参照してください)。 Check the following external user databases のオプションを選択します。右矢印ボタンをクリックして、先に設定した 外部データベースを「External Databases」のリストから「Selected Databases」のリスト



### NT/RADIUS パスワード有効期限設定機能のテスト

コンセントレータには、RADIUS 認証をテストする機能があります。この機能を正しく使用する には、次の手順を慎重に行ってください。

#### RADIUS認証のテスト

1. [Configuration] > [System] > [Servers] > [Authentication] に移動します。使用する RADIUS サーバを選択して、Test をクリックします。

Configuration | System | Servers | Authentication

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

You should have a properly 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. プロンプトが表示されたら、NT ドメインのユーザ名とパスワードを入力して、OK をクリ ックします。次の例では、パスワード「cisco123」を使用している、NT ドメイン サーバで Configuration | System | Servers | Authentication | Test

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

		User Name jfrahim
		Password Anternation
OK Cancel		
3. 認証が正しく設定されると、	「Authentication Successful」とい	<i>い</i> うメッセージが表示されま
Success		
Continue	Successful	

す。

上記以外のメッセー

ジが表示された場合は、設定や接続に問題があります。このドキュメントで説明されている 設定手順やテスト手順を繰り返して、すべての設定が正しく行われていることを確認してく ださい。また、デバイス間の IP 接続も確認してください。

# RADIUS プロキシを使用する実際の NT ドメイン認証によるパスワード期限切れ機能のテスト

 ドメイン サーバ上にユーザがすでに定義されている場合は、そのプロパティを変更して、 そのユーザが次にログオンするときにパスワードを変更するメッセージが表示されるように します。ユーザのプロパティのダイアログ ボックスの「Account」タブを表示して、User must change password at next logon のオプションを選択し、OK をクリックします。

Console Window Hel	p	tory osers and t	polibities Paxo belaxiorecorout l'axiorecorout osers1
Action View Eavorites	⇔ ⇒ €	× 🗗 🙆 😫	<u>1</u> 2 2 2 1 1 2 4 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. cis DinsUpdat Domain S Domain C Domain C Domain C Domain C Domain Us Domain Us Enterprise Group Poli Group Poli.	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	Dial-in       Environment       Sessions       Remote control       Terminal Services Profile         General       Address       Account       Profile       Telephones       Organization       Member Of         User logon name:       [ftrahim       @jazib.cisco.com       •         User logon name       (pre-Windows 2000):       [JAZIB-ADS\       •         JAZIB-ADS\       [ftrahim        Log On To         Logon Hours       Log On To        Account is locked out.         Account options:            Viser cannot change password at next logon           Viser cannot change password            Account expires            Store password using reversible encryption           Account expires            Mever             OK       Cancel       Apply

2. VPN クライアントを起動して、コンセントレータへのトンネルの確立を試みます。

nn	Jser Authentication for lab
9	Enter Username and Password.
	Username:
	ifrahim
	Password:
niti	******
Cor	🗖 Save Password
	Domain:
	JAZIB-ADS
	OK Cancel

3. ユーザ認証の際に、パスワードの変更が要求されます。

User Au	uthentication for la	ab
٩	Your password expi	red
New F	assword:	
Confir	n Password:	
	ОК	Cancel

### <u>関連情報</u>

- <u>Cisco VPN 3000 シリーズ コンセントレータ</u>
- IPSec
- <u>Cisco Secure Access Control Server for Windows</u>
- RADIUS
- Requests for Comments (RFCs)