RADIUS を使用した Windows 2008 NPS サーバ (Active Directory)に対する ASA VPN ユーザ 認証の設定例

内容

<u> 概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>設定</u> <u>ネットワーク図</u> <u>設定</u> <u>ASDM の設定</u> <u>CLI での設定</u> <u>Windows 2008 ServerとNPSの構成</u> <u>確認</u> <u>ASA のデバッグ</u> トラブルシュート

概要

このドキュメントでは、RADIUS プロトコルを使用して Microsoft Windows 2008 Network Policy Server (NPS)と通信するように適応型セキュリティ アプライアンス (ASA)を設定する方法を 説明します。これにより、レガシー Cisco VPN Client/AnyConnect/Clientless WebVPN のユーザ が Active Directory に対して認証されます。NPSは、Windows 2008 Serverが提供するサーバーの 役割の1つです。これは、リモートダイヤルインユーザ認証を提供するためのRADIUSサーバの実 装であるWindows 2003 Server, IAS(Internet Authentication Service)に相当します。同様に、 Windows 2008 Serverでは、NPSはRADIUSサーバの実装です。基本的に、ASAはNPS RADIUSサーバへのRADIUSクライアントです。ASAはVPNユーザに代わってRADIUS認証要求を 送信し、NPSはActive Directoryに対してそれらを認証します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

•バージョン9.1(4)が稼働するASA

• Active DirectoryサービスとNPSの役割がインストールされたWindows 2008 R2 Server 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。

設定

注:このセクションで使用されるコマンドの詳細については、<u>Command Lookup Tool(登</u> <u>録ユーザ専用)を使用してください。</u>

ネットワーク図



設定

ASDM の設定

- 1. NPS認証が必要なトンネルグループを選択します。
- 2. [Edit]をクリックし、[Basic]を選択します。
- 3. [Authentication]セクションで、[Manage]をクリックします。

Basic	Name:	TEST	
-Advanced	Aliases:	TEST	
	Authentication		
	Method:	AAA Certificate Both Both Certificate Certificat	~
	AAA Server Group:	LOCAL -	Manage
		Use LOCAL if Server Group fails	\smile
	Client Address Assignment –		
	DHCP Servers:		
		None DHCP Link DHCP Subnet	
	Client Address Pools:	test	Select
	Client IPv6 Address Pools:		Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		
	Group Policy:	DfltGrpPolicy 👻	Manage
	(Following field is an attribu	ute of the group policy selected above.)	
	Enable SSL VPN dien	it protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name: hk.intra	axa	
		m	•
Find:	Ne	xt OPrevious	

- 4. [AAA Server Groups]セクションで、[Add]をクリックします。
- 5. [AAA Server Group]フィールドに、サーバグループの名前(NPSなど)を入力します。
- 6. [プロトコル]ドロップダウンリストから、[**RADIUS**]を選**択します**。
- 7. [OK] をクリックします。

A Server Groups								-
erver Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attes	pts .		Add
XCAL	LOCAL							Edit
nt	00	Match Case	Add AAA Serve AAA Server Group: Protocol: Accounting Node:	r Group NFS RADUIS © Smulta	• recus @ Single			Delete
ivers in the Select erver Name or IP /	ed Group Address Interfa	ce Timeout	Reactivation Modes Dead Time:	Depiet	ion 💮 Timed sinutes		-	Add
			Max Paled Attempt	s: 3				Edit
			🖹 Crable interim a	eccounting ups	date			Delete
			Enable Active D	Wrectory Agen	nt mode			Move Up
			VPII3K Compati	bility Option	n	(8)		Nevre Down
			C	Car	noel Help			Test
nde	00	Match Case						
DAP Attribute I	tap				tool. 0	trans.		(8
				100	HARA H	anser.		

- 8. [Servers in the Selected Group]セクションで、追加したAAAサーバグループを選択し、 [Add]をクリックします。
- 9. [Server Name or IP Address]フィールドに、サーバのIPアドレスを入力します。
- 10. [Server Secret Key]フィールドに秘密キーを入力します。
- 11. サーバが別のポートでリッスンしない限り、[Server Authentication Port]フィールドと [Server Accounting Port]フィールドはデフォルト値のままにします。
- 12. [OK] をクリックします。
- 13. [OK] をクリックします。

Authentication Configure AAA Server Groups AAA Server Groups AAA Server Group AAA Server Group Server Group Prever Group COAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL L	-Advanced	Name: Alapes:	TEST				ń	Edit AAA Server		
Configure AAA Server Groups 23 AAA Server Group Protocol AAA Server Group Protocol Accounting Mode Reactivation Mode LOCAL LOCAL LOCAL LOCAL Best Balata Server Accounting Protocol 10 Server Accounting Protocol 1645 Server Name or IP Address 1646 Nore Up 1646 Nore Up 1646 Nore Up 1647 Server Name or IP Address 1646 Server Name or IP Address 1646 <t< th=""><th></th><th>Authenticatio</th><th>n</th><th></th><th></th><th></th><th></th><th>Server Group:</th><th>NPS</th><th></th></t<>		Authenticatio	n					Server Group:	NPS	
AAA Server Groups Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Pailed Attempts Add ICOAL LOCAL ICOAL ICOAL ICOAL ICOAL ISO PAULIES Server Name or IP Address: 10.105.100.51 Innout: 30 seconds EAAC ISS Parameters EAAC ISS P	Configure AAA Se	iver Groups		an i sertion i	-		23	Interface Name:	inside +	
Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Pailed Attempts Add LOCAL LOCAL Brannetics RADILIS Parameters Edit Datable Finds Servers in the Selected Group Server Name or IP Address Interface Timeout 10:055:130:31 reacter 33 Server Name or IP Address Interface Timeout 10:055:130:31 reacter 33 Common Passion'd: Common Passion'd: Common Passion'd: Server Name or IP Address Interface Timeout Toat Finds IDAP Attribute Hap OK Cancel Help New Ellip Move Up Move Data Move Up Move Up Move Data Move Up Move Data Move Up Move Move Message Table Message Table Message Table Move Up Move Data Move Move Move Deated Move Data Move D	AAA Server Groups							Server Name or IP Address:	10.105.130.51	
LOCAL LOCAL NSS RADILS Res RADILS Res RADILS Res Radit Res Res Res	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Nex Failed Attempts	Add	Tineout:	10 seconds	
155 RADUUS Genge Besieton 10 3 Colt Finds Original Delete Berver Austentrication Port: 164.6 Finds Original Delete Berver Austentrication Port: 164.6 Server Name or IP Address Interval: 30 accords: - Server Name or IP Address Interval: 30 accords: - Server Name or IP Address Interval: 30 accords: - Server Secret Key: Onescenter Server Secret Key: - - Server Secret Key: Onescenter Server Secret Key: - - Server Secret Key: Server Secret Key: - - - Server Secret Key: Server Secret Key: - </td <td>LOCAL</td> <td>LOCAL</td> <td></td> <td></td> <td></td> <td></td> <td>-</td> <td>RADIUS Parameters</td> <td></td> <td></td>	LOCAL	LOCAL					-	RADIUS Parameters		
Delete Pind: Pind: Server Name or P Address Server Name or P P E Address Server Name or P P E Address Server Name	NPS	RADIUS	Single	Depletion	10	3	Eat	Server Authentication Ports	1645	
Pinds Match Case Servers in the Selected Group Server Name or IP Address Server Name or IP Address Interface Timeout Move Up Move Up Move Up Move Up Move Up Message Table Interface Move Up Message Table Message Table Message Name Message Text mst Meth Case Move Up Message Text Message Name Message Name Message Text Message Name Message Name Message Text							Delete	Server Accounting Port:	1646	
Servers in the Selected Group Servers in the Selected Group Servers in the Selected Group Server Name or IP Address Interface Timeout ID 105 130.51 Inside III Delete ID 201 ID 2	Finds	000	Match Case					Retry Interval:	10 seconds	
Servers in the Selected Group Servers in the Servers Server in the Servers Servers Servers Servers Servers Servers Servers Servers Servers Servers Servers Serv								Course Coursel Vann		
Server Name or IP Address Interface Timeout Add Add Add Add Add Add Add Add Add Ad	Servers in the Select	ed Group				/		JO TO JOJE KNET		_
AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard AC, Netmask Convert: Standard								Common Paesword:		
Delete Delete Delete Delete More Up More Up More Up More Up More Down Test Test Resage Table More Down Resage Table More Down Test Test Delete Downet Up More Down Test Delete More Down Resage Table	Carneter Name or 12	Address Interform	Treesed				Add			
Delete Microsoft Crawy, Coppeter: W Delete Nove Up Nove Up Hessage Table Howe Down Test Test Nove Up IDAP Attribute Hap Or you want to enter your on new Philis on enter your on the Philis on the Next Philis on enter your on new Philis on enter your on the Philis on the P	Server Name or IP	Address Interface	Timeout			<u> </u>	Add	ACL Netmask Convert:	Standard	
Nove Up Hessage Table Find: Image: Sol Message Text Find: Image: Sol Message Text IDAP Attribute Map Resenter PIN: IDAP Attribute Map Image: Sol Message Text Image: Sol Message Text Resage Text Image: Sol Message: Sol Message Text Resage Text Image: Sol Message: Sol Message Text Resage Text Image: Sol Message: Sol Message: Sol Message Text Resage Text Image: Sol Message: Sol	Server Name or IP 10,105,130,51	Address Interface	Timeout 31				Add	ACL Netmask Convert:	Standard	•]
Move Up Hove Up Hove Down Test Test DAP Attribute Map OK Cancel Help Imd: Imd: Imd: Imd: Imd: Previous	Server Name or IP 10.105-130.51	Address Interface	Timeout 18				Add Edit	ACL Netmask Convert: Microsoft CHAPv2 Capable:	Standard	•]
Heve Down Test Test Test Test Test Test Test Test	Server Name or IP 10.105/130.51	Address Interface Inside	Timeout 13				Add Edit Delete	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages	Standard	•]
Test Test Find: Image: Second Sec	Server Name or IP 10.105.130.51	Address Interface	Timeout 30				Edit Delete Move Up	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table	Standard	•
Find: Image: Spin-reenter Reenter PIN: IDAP Attribute Map Image: Spin-reenter Do you want to enter your on new PDIN with the next code on new point-reenter or new PDIN accepted on the pin-reenter or new point-reenter or new point-re	Server Name or IP 10:105:130.51	Address Interface	Timeout 33				Add Edit Delete Nove Up Hove Down	ACI, Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Hessage Name	Standard	•]
Find: Image: Match Case LDAP Attribute Map Image: Match Case OK Cancel Help Image: Match Case Image: Match Case Image: Match Case OK Cancel Help Image: Match Case Image: Match Case Image: Match Case OK Cancel Help Image: Match Case Image: Match Case Image: Match Case Image: Match Case Match Case <	Server Name or IP	Address Interface	Timeout 33				Add Edit Delete Nove Up Move Down	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name redy-for-sys on	Standard	•
	Server Name or IP 10:105:130:51	Address Interface	Timeout 30				Add Edit Delete Move Up Hove Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name ready-for-sys-pin new-pin-remter	Standard Message Text ACCEPT A SYSTEM GE Reenter PIN:	•]
Image: Comparison of the second of the se	Server Name or IP 10, 105, 100, 51 Find:	Address Interface	Timeout 33 Match Case				Add Edit Delete Move Up Move Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SCI Messages Message Table Message Name ready-for-sys-pin new-pin-reenter new-pin-reenter new-pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter	•) INERATED P2 your own pin
OK Cancel Help Inter gin-spic-ck New gin-spic-ck N	Server Name or IP 10:105:130:51 Find:	Address Interface	Timeout 33 Match Case				Add Edit Delete Nove Up Nove Dp Nove Down Test	AC, Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name ready-for-sys-pin new pin-reenter new pin-reenter new pin-reenter new pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the next	VERATED P3 your own pin t card code
OK Cancel Hdp Please remember your new Apha-Alumer * * * * ind: * * *	Server Name or IP 20:105:130:51 Find: LDAP Attribute	Address Interface roots	Timeout 33 Match Case				Add Edit Delete Nove Up Nove Up Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name ready for sys spin new spin neth next-code and-reauth next-code	Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the neod Enter Next PASSCOOL	• INERATED PIP your own pin t card code t
	Server Name or IP 10:105:130:51 Find: LDAP Attribute	Address Interface	Timeout 33 Match Case				Add Edit Delete Move Up Hove Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SCI Messages Message Table Message Name ready-for-sys-pin new-pin-center new-pin-meth next-code and-reauth next-code new-pin-sys-ok	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the ned Enter Invest PIASCOOL New PIN Accepted	VERATED PIP your own pin t card code t
	Server Name or IP 10:105:130:51 Find: LDAP Attribute	Address Interface rests	Timeout 31 Match Case	Cancel	Help		Add Edit Delete Move Up Hove Down Test	AC, Netmask Convert: Microsoft CHAPv2 Capable: SCI Messages Hessage Table Message Name ready-for-sys-cin new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter	Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: De you want to enter new PIN with the next Enter Next PASSCOOL New PIN Accepted Please remember your	VERATED PJ your own pin t card code t r new PIN
Ind: Restore default message texts	Server Name or IP 10:105:130:51 Find: LDAP Attribute	Address Interface rests	Timeout 31 Match Case	Cancel	Help		Add Edit Delese Nove Up Hove Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name ready for sys oin new pin-reenter new pin-reenter new pin-reenter new pin-reenter new pin-reenter new pin-sys-ok new pin-sys-ok	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the need Enter Next PASSCOOL New PIN Accepted Please nemember your Enter your new Alpha	NERATED PD your own pin t card code c r new PDN -Pumerical PD
Pind: Previous	Server Name or P 10.105/130151 Find: LDAP Attribute	Address Interface roots	Timeout 31 Match Case	Cancel	Hdp		Add Edit Delese Nove Up Hove Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Name ready for sys ofin new pin-meth new pin-meth new pin-meth new code and reauth new code and reauth new code and reauth new pin-sys-ok new pin-sys-ok new pin-sys-ok new pin-sys-ok	Standard Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the netod Enter Next PASSCOOL New PIN Accepted Please nemember your Enter your new Alpha to make changes.)	vour own pin t card code e r new PIN -Numerical PD
	Server Name or IP 10.005:120.51 Find: LDAP Attribute	Address Interface reads	Timeout 33 Match Case	Cancel	Help		Add Eait Delete Move Up Move Down Test	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Difference Hessage Table Hessage Name ready-for-sys-spin new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-sys-ok new-pin-sys-o	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the next Enter Next PASSCOOL New FIN Accepted Please nonember your Enter your new Alpha to make changes.) e default message texts	your own pin t card code t r new PIN -Numerical PD
	Server Name or IP 10.105:120.51 Find: LDAP Attribute	Address Interface	Match Case	Cancel	Help		Add EGI Delete Nove Up Hove Down Teat	ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages Message Table Message Tabl	Standard Standard Message Text ACCEPT A SYSTEM GE Reenter PIN: Do you want to enter new PIN with the next Inter Next PASSCOOL New FIN Accepted Please nemember you Enter your new Alpha to make changes.) d default message texts	vour own pin t card code t r new PDN -Numerical PD

- 14. [AAA Server Group]ドロップダウンリストから、前の手順で追加したグループ(この例で はNPS)を選択します。
- 15. [OK] をクリックします。

asic	Name:	TEST	
dvanced	Aliases:	TEST	
	Authentication		
	Method:	AAA Certificate Both	
	AAA Server Group:	NPS -	Manage.
		Use LOCAL if Server Group fails	
	Client Address Assignment –		
	DHCP Servers:		
		None DHCP Link DHCP Subnet	
	Client Address Pools:	test	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	DfltGrpPolicy 🗸	Manage.
	(Following field is an attribu	ute of the group policy selected above.)	
	Enable SSL VPN clien	it protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name:		
		m	_
51			

CLI での設定

aaa-server NPS protocol radius aaa-server NPS (inside) host 10.105.130.51 key ***** tunnel-group TEST type remote-access tunnel-group TEST general-attributes address-pool test authentication-server-group (inside) NPS tunnel-group TEST webvpn-attributes group-alias TEST enable

ip local pool test 192.168.1.1-192.168.1.10 mask 255.255.255.0 デフォルトでは、ASAは暗号化されていないパスワード認証プロトコル(PAP)認証タイプを使用 します。これは、ASAがRADIUS REQUESTパケットを送信するときにプレーンテキストでパス ワードを送信することを意味するものではありません。プレーンテキストのパスワードは、 RADIUS共有秘密で暗号化されます。

トンネルグループでパスワード管理が有効になっている場合、ASAはプレーンテキストのパスワ ードを暗号化するためにMSCHAP-v2認証タイプを使用します。このような場合、ASDM設定セク ションで設定した[Edit AAA Server]ウィンドウで[**Microsoft CHAPv2 Capable**]チェックボックスが オンになっていることを確認します。

tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management

注:test aaa-server authenticationコマンドは、常にPAPを使用します。ユーザがパスワー ド管理が有効なトンネルグループへの接続を開始した場合にのみ、ASAはMSCHAP-v2を使 用します。また、'password-management [password-expire-in-days]'オプションは Lightweight Directory Access Protocol(LDAP)でのみサポートされます。RADIUSにはこの機 能はありません。Active Directoryでパスワードの有効期限が既に切れている場合は、 [password expire]オプションが表示されます。

Windows 2008 ServerとNPSの構成

NPSサーバーの役割がインストールされ、Windows 2008サーバーで実行されている必要があり ます。そうでない場合は、[Start] > [Administrative Tools] > [Server Roles] > [Add Role Services]を選択します。ネットワークポリシーサーバを選択し、ソフトウェアをインストールし ます。NPSサーバーの役割がインストールされたら、次の手順を実行して、ASAからの RADIUS認証要求を受け入れて処理するようにNPSを構成します。

1. ASAをNPSサーバーのRADIUSクライアントとして追加します。 [管理ツー**ル] > [ネットワー** クポリシーサーバ]を選択します。[RADIUS Clients]を右クリックし、[New]を選択します。

Network Policy Server						_ 비즈 _ 스	Start
File Action View Help							June
🗢 🔿 🖄 📅 🚺 🖬							
NPS (Local)	RADIUS Clients						-
RADIUS Clients and Servers	RADIUS	clients allow you to	specify the network acc	cess servers, that	t provide access to	o your	2
Remote RA New	t network.						
Connection		ID Address	Derive Marchater	NUDCON	0		6-6
Network Pc	Cisco Router	10.105.130.69	RADIUS Standard	No No	Enabled		
Health Polic Refresh							
Accounting Help							
Templates Management							
10							
							1 D
							2-31 AM
•							7/20/2013
Jew Network Access Device							

ASAで設定されているフレンドリ名、アドレス(IPまたはDNS)、および共有秘密を入力し ます。



[Advanced] タブをクリックします。[ベンダー名]ドロップダウンリストから、[**RADIUS Standard**]を**選択します**。[OK] をクリックします。

NPS (Local)	RADIUS Clients	New RADIUS Client	x
RADIUS Clients Remote RADIUS Server G Policies Network Access Protection Accounting Templates Management	Friendly Name	Settings Advanced Vendor Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list. Vendor name: FADIUS Standard FADIUS Standard • Additional Options • Access-Request messages must contain the Message-Authenticator attribute RADIUS client is NAP-capable OK	
	4		

 VPNユーザの新しい接続要求ポリシーを作成します。接続要求ポリシーの目的は、 RADIUSクライアントからの要求をローカルで処理するか、リモートRADIUSサーバに転送 するかを指定することです。 [NPS] > [ポリシー]で、[接続要求ポリシー]を右クリックし、新 しいポリシーを作成します。[Type of network access server]ドロップダウンリストから、 [Unspecified]を選択します。

🤣 Network	test Properties	Ctart
File Actio		Jun
	Overview Conditions Settings	
MPS (Local)	Policy name: test	
RADIUS		
RAD	Policy State	
Rem	If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.	
Policies		
Netv	I ✓ Policy enabled	
📔 Heal	No. 1	
So Network	Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server	
Accounti	type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access poin	
Template	select Unspecified.	
	Type of network access server:	
	C Vendor specific:	
	10	
		**
		the IDa
		12:08 414
•		7/20/2013
	OK Cancel	

[条件]タブを**クリック**します。[Add] をクリックします。ASAのIPアドレスを[Client IPv4 Address]条件として入力します。

Network	Deline Common	
Eile Actio	test Properties	A Start
	Overview Conditions Settings	
NPS (Local)	Configure the conditions for this network policy.	
RADIUS	If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.	$\mathbf{\Sigma}$
E Policies		
Conr	Condition Value	
Netv	Client IPv4 Address 10.105.130.69	
📔 Heal		- 🛩
Network		
Accounti		
Template		
	N	
	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR OFTA C	
		_
	Condition description:	
	The client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
	Add Edit R	emov «
		12:09 414
•		7/20/2013
	OK Cancel	1 2012010

[設定]タブを**クリック**します。[Forwarding Connection Request]で、[**Authentication**]を選択 します。[Authenticate requests on this server]オプションボタンが選択されていることを確 認します。[OK] をクリックします。



 認証を許可するユーザを指定できるネットワークポリシーを追加します。たとえば、Active Directoryユーザグループを条件として追加できます。指定されたWindowsグループに属する ユーザーのみが、このポリシーで認証されます。[NPS]で[ポリシー]を選択します。[ネット ワークポリシー]を右クリックし、新しいポリシーを作成します。[Grant access]オプション ボタンが選択されていることを確認します。[Type of network access server]ドロップダウン リストから、[Unspecified]を選択します。

Overview Conditions Constraints Settings	
Policy name: test	- Million
Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?	
 Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. 	
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type	
Vendor specific, but neither is required. It your network access server is an SU2.1X authenticating switch or wireless access point, select Unspecified. Type of network access server:	

[条件]タブを**クリック**します。[Add] をクリックします。ASAのIPアドレスを[Client IPv4 Address]条件として入力します。VPNユーザを含むActive Directoryユーザグループを入力し ます。

conr	nection request, NPS skip	ps this policy and evaluates other policies, if additional policies are configured.	
	Condition	Value	
22	User Groups	SKP\VPN	
1	Client IPv4 Address	10.105.130.69	

[拘束]タブを**クリック**します。[**Authentication Methods**]を選択します。[Unencrypted authentication (PAP, SPAP)]チェックボックスがオンになっていることを確認します。[OK] をクリックします。

Overview Conditione Constraints	tione	-
Configure the constraints for this network If all constraints are not matched by the o	policy. connection request, network access is denied.	
Constraints Constraints Authentication Methods Session Timeout Called Station ID Day and time restrictions	Allow access only to those clients that authenticate with the specified methods. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up	
2 NAS Port Type	Add Edit Remove Less secure authentication methods: Image: Complete Authentication version 2 (MS-CHAP-v2) Image: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) Image: Microsoft Encrypted Authentication (MS-CHAP) Image: Microsoft Encrypted Authentication (CHAP) Image: Microsoft Encrypted Authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication method Image: Microsoft Encrypted Authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication (PAP, SPAP)	
		- 12

NPS RADIUSサーバーからグループポリシー属性(属性25)を渡す

グループポリシーをNPS RADIUSサーバーでユーザーに動的に割り当てる必要がある場合は、グ ループポリシーのRADIUS属性(属性25)を使用できます。

ユーザにグループポリシーを動的に割り当てるためにRADIUS属性25を送信するには、次の手順 を実行します。

1. ネットワークポリシーを追加したら、必要なネットワークポリシーを右クリックし、[設定]]タブを**クリック**します。



2. [**RADIUS Attributes**] > [**Standard**]を選択します。[Add] をクリックします。[Access type]は [All]のままにします。

Retwork Policy Server		
File Action Utest Proper Image: Strength Proper Overview Overview Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper Image: Strength Proper	Conditions Constraints Settings	the policy grants access, settings are applied Add Standard RADIUS Attribute
Conne C	S Attributes Index Specific Advacess Protection P Enforcement anded State g and Remote Access Nink and Bandwidth scalion Protocol (SAP) Filere snybion Settings Add.	To add an attribute to the settings, select the attribute, and then click Add. To add a custom or predefined Vendor Specific attribute, close this draing and select Vendor Specific, and then click Add Access type Attributes: Attributes: Name AccelentationInterval Caliback-Rumber Cleve Bised FramedAppleTak-Link FramedApple
		Add Dose

 [Attributes]ボックスで、[Class]を選択し、[Add]をクリックします。属性値、つまりグループ ポリシーの名前を文字列として入力します。この名前のグループポリシーは、ASAで設定す る必要があることに注意してください。これは、ASAがRADIUS応答でこの属性を受信した 後、VPNセッションに割り当てるためです。

Network Policy	y Server test Properties		
File Action () () () () () () () () () () () () () () (Dverview Conditions Constraints Settle Configure the settings for this network poli If conditions and constraints match the co	ngs sy nnection request and t	The policy grants access, sattings are applied.
Renot	Settings:	100	Add Standard RADUIS Attribute
E Folcies	RADIUS Attributes	To send addition	
Conne	Standard	then click Edit. I	To add an attribute to the settings, select the attribute, and then click Add.
Netwo	Vendor Specific	your RADIUS di	To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click
E Network A	Natwork Assass Induction		Add.
Accounting	NAP Externation		Access type:
🖽 🛒 Templates	3 Nar Enorcement	Attributes	Al
	Extended State	Name	
	Routing and Remote Access	Framed+hotoc	Abbules
	Multilink and Bandwidth	Confidentype	Name
	ID Share		AcctineiroInterval
	W IF FIXEIS		Lalbeck-Number
	🔒 Encryption		Filed
	🚜 IP Settings		Framed AppleT alk-Link
		Add	Framed-AppleTaik-Network
			Fransel-OrnhaTalk-Zenna
			Description:
			Specifies the classification of accounting records.
•			Add Dave
			DK Concel L Arch
Shetwork Polic	y Server		
Network Polic File Action Vi	n Server Lest Properties		
Network Polic File Action Vi	y Server Test Properties Dverview Conditions Constraints Sett	ings	
File Action Vi 4 - Action Vi 1 - A	Vervier Lest Properties Diverview Conditions Constraints Sett Contigue the settings for his network poli	ings CV	
Network Polici File Action Image: State of the st	 Server Lest Properties Dverview Conditions Constraints Setting Configure the settings for this network pole If conditions and constraints match the conditions 	ings Cy rimection request and (The policy grants access, settings are applied
Network Polic File Action Vi Action Vi Policies NPS (Locol) RADIUS CI RADIUS RADIUS RADIUS RADIUS	 Server Lest Properties Dverview Conditions Constraints Setting Configure the settings for this network pole If conditions and constraints match the co Settings: 	ngs cy nnection request and (The policy grants access, settings are applied
Piet Acton Vi Pie Acton Vi Pie Acton Vi Piet Act	Server Test Properties Overview Conditions Constraints Sett Configue the settings for this network poli If conditions and constraints match the co Settings RADIUS Attributes	ngs cy meetion request and t	Ithe policy grants access, settings are applied Add Standard RADIUS Attribute
Piet Acton Vi Acton Vi Pie Acton Vi Piet Acton V	Server Test Properties Overview Conditions Constraints Set Configue the settings for this network pol If conditions and constraints match the co Settings RADIUS Attributes Standard	ngs 9) metion request and t Pren cick Edit rem Edit Edit rem Edit (Dit S edit	The policy grants access, settings are applied Add Standard RADIUS Attribute X To add an attribute to the satisfue, select the attribute, and then click Add. X
File Acton Vi File Acton Vi Pros (Local) RADIUS (Local) RADIUS (Local) RADIUS RA	Server Lest Properties Overview Conditions Constraints Set Configue the settings for this network pol If conditions and constraints match the co Settings FADIUS Attributes Standard Ziendor Specific	ngs gy meetion request and t To send additor Pren citik Edi 1 your FIADIUS di	Ithe policy grants access, settings are applied Add Standard RADIUS Attribute To add an attribute to the sattings, select the attribute, and then plick Add. To add a custom or precisined Vendor Sneedilin Attribute, close this dialon and select Vendor Sneedilic, and then plick Add
File Acton Vi File Acton Vi Protection RADIUS (Local) RADIUS (Local) RADIUS (Local) RADIUS RADI	Server Test Properties Overview Conditions Constraints Sett Configue the settings for this network pol If conditions and constraints match the co Settings RADIUS Attributes Standard Ziendor Specific Network Access Protection	ngs gy meetion request and t To send additor Hen cick Edi I your FIADIUS di	Add Standard RADIUS Attribute Image: Select the attribute select Wender Specific Attribute select Wend
File Acton Vi File Acton Vi Provide State RADIUS (Local) RADIUS (Local) RADIUS (Local) RADIUS R	Server Test Properties Overview Conditions Constraints Set Configue the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Standard Zer Vendor Specific Network Access Protection NAP Enforcement	ngs Synnection request and t To send additor Pren cick Edi I your FIADIUS di Attributor:	
File Acton Vi File Acton Vi Pros (Local) RADDUS (Local) RA	Server Test Properties Overview Conditions Constraints Sett Configue the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Extended State	ngs Synnection request and t To send additor Pren cick Edi I your FIADIUS di Athibutes:	Add Standard RADIUS Attribute Image: Second Standard RADIUS Attribute To add an attribute to the sattings, select the attribute, and then click Add. To add a custom or precisioned Vendor Specific Attribute close this dialon and select Vendor Specific attribute information Add Attribute Information Access type: Attribute name: Class
File Acton Vi File Acton Vi Pros (Local) RADDUS CI RADDUS CI RADDUS CI RETURN Return k Accounting Return k Templatas	Server Test Properties Overview Conditions Constraints Setting Configue the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Doutling and Remote Access	ngs Synnection request and the Hen cick Edi I your FADIUS di Attributes: Name Framed Protoc	Add Standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or precisioned Vendor Specific Attribute X Add Attribute Information Access type: Attribute nome: Al Class Attribute nomber: X
File Acton Vi File Acton Vi Produces RADIUS CI RADIUS CI RADIUS CI Retwork A Metwork A Accounting Retwork A Templetes	Server Test Properties Overview Conditions Constraints Setting Configue the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Settings Produc Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access Mittick and Exclusive	ngs (y) To send additor Hen click Edi I your FIADIUS di Athibutes: Name Framed Protoc Service Type	Add Standard RADIUS Attribute X Add Standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or predefined Vendor Sneeting, saled the attribute, and then click Add. X Add add a custom or predefined Vendor Sneeting, saled the attribute, and then click Add. X Add add a custom or predefined Vendor Sneeting, saled the attribute, and then click Add. X Add add add add attribute Information X Access type: Attribute name: Class Attribute number: 25
File Acton Vi File Acton Vi Pile Acton Vi Pile State Pile Stat	Server Test Properties Overview Conditions Constraints Setting Configure the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Settings Produc Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access Multink and Bandwidth Adcester Protection[34P]	ngs Oy meetion request and the Hen click Edi I your FIADIUS di Athibutes: Name FramedProtoc Service-Type	Add Standard RADIUS Attribute X Add Standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or precisined Vendor Sneeting, saled the attribute, and then click Add. X Add data attribute Information X Attribute Information X Attribute name: Class Attribute number: 25 Name Attribute formation
File Acton Vi File Acton Vi Part Constant Part C	Server Test Properties Overview Conditions Corligue the satings for this network poli if conditions and constraints match the co- settings: RADIUS Attributes Standard Yendor Specific Network Access Protection NAP Enforcement NAP Enforcement Extended State Routing and Remote Access Multink and Bandwidth Accelen Protocol (BAP) IP Filers	ngs (y median request and the hen cick Edi I your FIADIUS di Athibutes: Name FramsdPratec Service-Type	Add Standard RADIUS Attribute X Add Standard RADIUS Attribute X To add an attribute to the settings, select the attribute, and then click Add. X To add a custom or predefined Vendor Sneeting, and then click Add. X Add data attribute Information X Access type: Attribute name: Class Attribute number: 25 Name Attribute format: Octoback-Number: Astribute format: Catback-Number Attribute format: Octoback-Number
File Acton Vi File Acton Vi Part Constant Part C	Server Test Properties Overview Conditions Constraints Set Configue the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Settings Produc Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access Multink and Bandwidth Access Photos (BAP) Theres Encyclips	ngs (y median request and the Hen click Edi I your FIADIUS di Attributes: Name FramedProtoc Service-Type	Add Standard RADIUS Attribute X Add standard RADIUS Attribute X To add an attribute to the satilitys, saled the attribute, and then click Add. X To add a custom or predefined Vendor Sneeting, and then click Add. X Add Add Attribute Information X Access type: Attribute name: All Class Attribute number: 25 Name Attribute format: Access trineimInterver CetString Caliback-Number Enter the attribute value in:
File Acton Vi File Acton Vi Acton Vi File Acton Vi File Acton Vi File Acton Vi File Acton File	Server Test Properties Overview Conditions Constraints Setting Configure the settings for this network poli If conditions and constraints match the co Settings FADIUS Attributes Settings PADIUS Attributes Padius	ngs (y median request and the Hen cick Edi I your FIADIUS di Athibutes: Name FramedProtoc Service-Type	Add Standard RADIUS Attribute X Add Standard RADIUS Attribute X To add an attribute to the satilitys, saled the attribute, and then click Add. X To add a custom or predefined Vendor Sneeting attribute, and then click Add. X Add Add Attribute Information X Access type: Attribute name: Class X Attribute number: 25 Name Attribute format: October Vendor Sneeting Attribute number: 25 Name Attribute format: October Vendor Sneeting Calbert Vendor Calbert Vendor Sneeting
File Acton Vi File Acton Vi File Acton Vi File Acton Vi File Acton Vi File Acton Vi File Acton File Acton	Second Test Properties Overview Conditions Constraints Setting Configure the settings for this network poli If conditions and constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Settings: Standard If conditions and constraints match the constraints Settings: RADIUS Attributes Standard Settings: FADIUS Attributes If conditions and constraints match the constraints Settings: RADIUS Attributes Standard Standard Standard If constraints Settings: Report Protoconstraints NAP Enforcement Settended State Routing and Remote Access Multilink and Bandwidth Alocelien Photopol (BAP) Files Enceryption Settings	ngs Over the send addition Hen cick Edi I your FIADIUS di Athibutes: Name Framed Protoc Service-Type	Add Standard RADIUS Attribute X Add standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or predefined Vendor Sneeting attribute, and then click Add. X Add access type: Attribute Information Attribute Information X Access type: Attribute nome: All Class Attribute nombe: 25 Name Attribute format: Calback-Number Calback-Number Calback-Number Celsting Fined-depiel dw C Sting Fined-depiel dw C Sting Fined-depiel dw C Sting Fined-depiel dw Hestocicinal
File Acton Vi	Server Test Properties Overview Conditions Constraints Setting Configure the settings for this network poli If conditions and constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Settings: FADIUS Attributes Standard Standard Yendor Specific Network Access Protection NAP Enforcement NAP Enforcement Extended State Fouting and Remote Access Multink and Bandwidth Access Photos (J&P) Y IP Filers Encryption W IP Setlings IP Setlings	ngs (y median request and the Hen click Edi I your FIADIUS di Attributes: Name FramedProtoc Service-Type Add	Add Standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or precisined Vendor Sneeting, saled the attribute close this dialon and select Vendor Sneeting, and then click Add. X To add a custom or precisined Vendor Sneeting, and then click Add. X Add Add Attribute Information X Access type: Attribute nome: All Class Attribute nombe: 25 Name Attribute format: Calbeck/Number Calbeck/Number Calbeck/Number Calbeck/Number Finend/opteTalk; Ching Finend/opteTalk; Hesadecinal
File Acton Vi	Server Test Properties Overview Conditions Constraints Setting Configure the settings for this network politic conditions and constraints match the conditions and constraints match the conditions Settings: FADIUS Attributes Standard If conditions Standard If vendor Specific Network Access Protection NAP Enforcement Setting and Remote Access Multink and Bandwidth Access Induct (BAP) If Pilets Encryption If Piletings If Piletings	ngs (y meetion request and the Hen click Edi I your FIADIUS di Attributes: Name FramedPhotoc Service-Type Add	Add Standard RADIUS Attribute Image: Select the attribute, and then click Add. To add an attribute to the sattings, select the attribute, and then click Add. Image: Select the attribute close this dialon and select Vendin Sinenific, and then click Add. To add a custom or precisioned Vendin Sinenific, and then click Add. Image: Select the attribute close this dialon and select Vendin Sinenific, and then click Add. To add a custom or precisioned Vendin Sinenific. Attribute Information Add Attribute Information Access type: Attribute nomber. All Class Attribute nomber. 25 Name Attribute format: Calback-Number Celefsting Calback-Number Celefsting Calback-Number Celefsting Finend-AppleTake Feared close this Finend-AppleTake Feared close take Filed Feared close take
File Acton Vi File Acton Vi Acton Vi Acton Vi Acton Vi Repose Re	Server Test Properties Overview Conditions Constraints Setting Configure the settings for this network politic conditions and constraints match the conditions and constraints match the conditions Settings: FADIUS Attributes Standard If conditions Standard If vendor Specific Network Access Protection NAP Enforcement Setting and Remote Access Multink and Earctwidth Alocation Protocol (BAP) IP Filters Encryption IP Settings	ngs Synnection request and the Hen clock Edi I your PiADIUS di Attributes: Name Framed Photoc Service-Type Add	Add Standard RADIUS Attribute Image: Second sec
File Acton Vi File Acton Vi Acton Vi Acton Vi File Acton Vi Acton RADUS CI RADUS CI Remot Conne C	Server Test Properties Overview Conditions Constraints Setting Contigues the settings for this network politic conditions and constraints match the conditions and constraints match the conditions Settings: FADIUS Attributes Standard It conditions Standard It conditions Network Access Protection NAP Enforcement Standard State Routing and Remote Access Multink and Bandwidth Allocation Protocol (BAP) It P Filers Encryption It P Settings It P Settings	ngs Synnection request and the Pren cick Edi I your FIADIUS di Attributes: Name Framed Protoc Service-Type Add	Add Standard RADIUS Attribute Image: Standard RADIUS Attribute Add Standard RADIUS Attribute Image: Standard RADIUS Attribute To add an attribute to the sattings, saled the attribute, and then click Add. Image: Standard RADIUS Attribute Information To add a custom or precisional Vender Sneeting Attribute Information Image: Standard RADIUS Attribute Information Add Attribute Information Image: Standard RADIUS Attribute Information Add a custom or precision Attribute name: Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: All Attribute Information Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: All Attribute name: Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: All Class Attribute name: Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: All Class Attribute name: Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: Callback-Number Class Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: Callback-Number Class Image: Standard RADIUS Attribute name: Image: Standard RADIUS Attribute name: Callback-Number Image: Standard RADIUS Attribute name: <t< td=""></t<>
File Acton Vi File Acton Vi Acton Vi Acton Vi RADLIS CI RADLIS CI RADLIS CI REPORTES Conne Conne Conne Conne Reportes Conne Conn	Server Test Properties Overview Conditions Constraints Setting Contigues the settings for this network politic conditions and constraints match the conditions and constraints match the conditions Settings: FADIUS Attributes Standard Standard Vendor Specific Network Access Protection NAP Enforcement Standard State Fouting and Remote Access Multilink and Banckath Alocation Protocol (BAP) IP Filters Encryption IP Settings IP Settings	ngs Synnection request and the Hen cick Edi I your PADIUS di Attributes: Name Framed Protoc Service-Type Add	Ithe policy grants access, settings are applied Add Standard PADIUS Attribute To add an attribute to the sattings, saled the attribute, and then plick Add. To add a custom or precisional Vendor Specific Attribute close this diation and select Vendor Specific Attribute Information Add Add Add Attribute Information Add Attribute Information Attribute Information Attribute Information Attribute Information Attribute Information Attribute name: All Class Attribute name: Calback Number Class Premed AppleTake Premed AppleTake <
Network Police File Acton Vi Image: State of the sta	Server Test Properties Overview Conditions Constraints Settings Contigues the settings for this network politic conditions and constraints match the constraints match the constraints Settings FADIUS Attributes Standard Image: Projectics Network Access Projection Image: Rest Access Projection NAP Enforcement Image: Extended State Routing and Remote Access Image: Image: Projection Multilink and Banckvidth Allocation Prolocol (BAP) Image: Image: Image: Image: Projection Image: Projection Image: Image: Image: Projection Image: Projection Image: Projection Image: Projection Image: Projection Image: Projection Image: Projection Image: Projection Image: Image: Projection Image: Projection Image: Projection Image: Projection Image: Image: Projection Image: Projection Image: Projection Image: Projection <t< td=""><td>ngs (y) To send additor Hen cick Edi I your PADIUS di Attributes: Name Framed Protoc Service-Type Add</td><td>If the policy grants access, settings are applied. Add Standard RADIUS Attribute To add an attribute to the sattings, saled the attribute, and then click Add. To add a custom or precisioned Vendor Streeting attribute close this dation and select Vendor Streeting, and then click Add. To add a custom or precisioned Vendor Streeting attribute close this dation and select Vendor Streeting, and then click Add. Access type: Attribute Information Access type: Attribute name: All Class Attribute number: 25 Attribute number: 25 Attribute number: 25 Caback-Number Enter the attribute value in: Precedd Figure 4domed Table Precedd Figure Table Headeclined Precedd Figure Table East the attribute value in: Precedd Figure Table Headeclined Precedd Figure Table Headeclined Precedd Figure Table Headeclined Precedd Figure Table Headeclined <t< td=""></t<></td></t<>	ngs (y) To send additor Hen cick Edi I your PADIUS di Attributes: Name Framed Protoc Service-Type Add	If the policy grants access, settings are applied. Add Standard RADIUS Attribute To add an attribute to the sattings, saled the attribute, and then click Add. To add a custom or precisioned Vendor Streeting attribute close this dation and select Vendor Streeting, and then click Add. To add a custom or precisioned Vendor Streeting attribute close this dation and select Vendor Streeting, and then click Add. Access type: Attribute Information Access type: Attribute name: All Class Attribute number: 25 Attribute number: 25 Attribute number: 25 Caback-Number Enter the attribute value in: Precedd Figure 4domed Table Precedd Figure Table Headeclined Precedd Figure Table East the attribute value in: Precedd Figure Table Headeclined Precedd Figure Table Headeclined Precedd Figure Table Headeclined Precedd Figure Table Headeclined <t< td=""></t<>
	Server Test Properties Overview Conditions Constraints Setting Contigue the settings for this network public conditions and constraints match the constraints match the constraints Settings FADIUS Attributes Standard Image: Standard Yendor Specific Network Access Protection NAP Enforcement Image: Extended State Fourting and Remote Access Image: Multink and Bandwidth Alcoston Photosol (BAP) Image: Finance access Image: Protocol (BAP) Image: Photosol (BAP) Image: Photosol (BAP) Image:	ngs (y) rmetion request and the free cick Edi I pour FIADIUS eli Attributes: Name Framed Protoc Service-Type Add	Add Standard RADIUS Attribute X Add Standard RADIUS Attribute X To add an attribute to the sattings, saled the attribute, and then click Add. X To add a custom or preteined Vender Streeting attribute, and then click Add. X To add a custom or preteined Vender Streeting attribute, and then click Add. X Access type: Attribute Information X Access type: Attribute name: X Altributes 25 X Name Attribute name: X Caleack Number CatelString X Caleack Number CatelString Headecinal Fremed Apple Lake Headecinal Headecinal Specifies the classify Catel Catel X Add. Does Add.
Network Police File Action Vi Image: Action Vi Image: Action Vi Image: Action Image: Action Vi Image: Action Vi Image: Action Image:	Server Test Properties Dverview Conditions Constraints Setting Configure the settings for this network public conditions and constraints metch the constraints metch the constraints Settings: RADIUS Attributes Standard Image: Standard Yendor Specific Network Access Protection NAP Enforcement Image: Extended State Routing and Remote Access Image: Interpret Protection Multilink and Bandwidth Alcoelish Photopol (BAP) Image: IP Files Encryption Image: IP Settings IP Settings	ngs (y) Intertion request and (then cick, Edi I jour FIADIUS eff Attributes: Name Framed-Protoc Service-Type Add	It is all x Add Standard RADIUS Attribute To add an attribute to the astringe, select the attribute, and then click Add. To add a attribute to the astringe, select the attribute, and then click Add. To add a custom or precisioned Vender Specific attribute close this frains and select Vender Specific, and then click Add. To add a custom or precisioned Vender Specific attribute close this frains and select Vender Specific, and then click Add. Add Add Attribute Information Attribute Information Attribute name: All Calcask Number Calcask Numb

確認

ここでは、設定が正常に機能しているかどうかを確認します。

注:debug コマンドを使用する前に、「<u>デバッグ コマンドの重要な情報」を参照してくだ</u> <u>さい。</u>

ASA のデバッグ

ASAでdebug radius allを有効にします。

ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds) radius mkreq: 0x80000001 alloc_rip 0x787a6424 new request 0x80000001 --> 8 (0x787a6424) got user 'vpnuser' got password add_req 0x787a6424 session 0x80000001 id 8 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) _____ Raw packet data (length = 65)..... 01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f | ...A....~m... 40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28 @P.6..vpnuser..(c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04 | .h....Z.oC. 06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00 ..i...=... 05 | . Parsed packet data..... Radius: Code = 1 (0x01)Radius: Identifier = 8 (0x08)Radius: Length = 65 (0x0041)Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836 Radius: Type = 1 (0x01) User-Name Radius: Length = 9 (0x09)Radius: Value (String) = 76 70 6e 75 73 65 72 vpnuser Radius: Type = 2(0x02) User-Password Radius: Length = 18 (0x12)Radius: Value (String) = Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x0Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5send pkt 10.105.130.51/1645 rip 0x787a6424 state 7 id 8 rad_vrfy() : response message verified rip 0x787a6424 : chall_state '' : state 0x7 : reqauth: c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36 : info 0x787a655c session_id 0x8000001 request_id 0x8 user 'vpnuser' response '***' app 0

reason 0 skey 'cisco' sip 10.105.130.51 type 1

RADIUS packet decode (response)

-----Raw packet data (length = 78).... 02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37N...Kv+..7 bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 02 | ..lL....... 19 2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a |j 2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf ,....<..n...@.. 1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03 .:.0........ Parsed packet data.... Radius: Code = 2 (0x02)Radius: Identifier = 8 (0x08)Radius: Length = 78 (0x004E)Radius: Vector: E8884B7620B6AAD30D2B9437BF9A6C4C Radius: Type = 7 (0x07) Framed-Protocol Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x1 Radius: Type = 6 (0x06) Service-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x2Radius: Type = 25 (0x19) Class Radius: Length = 46 (0x2E)Radius: Value (String) = 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf |j,. 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a<...n...@....: 18 6f 05 81 00 00 00 00 00 00 00 03 .0..... rad_procpkt: ACCEPT RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0x787a6424 session 0x80000001 id 8 free_rip 0x787a6424 radius: send queue empty INFO: Authentication Successful

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- ASAとNPSサーバ間の接続が良好であることを確認します。パケットキャプチャを適用して、認証要求が(サーバが到達可能な場所から)ASAインターフェイスを離れるようにします。UDPポート1645(デフォルトのRADIUS認証ポート)がパス内のデバイスによってブロックされていないことを確認し、NPSサーバに到達するようにします。ASAでのパケットキャプチャの詳細については、『ASA/PIX/FWSM:CLI および ASDM を使用したパケットのキャプチャの設定例.
- それでも認証が失敗する場合は、Windows NPSのイベントビューアで確認します。[イベント ビューア] > [Windowsログ]で、[セキュリティ]を選択します。認証要求時にNPSに関連するイ ベントを探します。

Vent Viewer (Local)	Security Number of	events: 93 (1) New events ave	lable			Actions
Custom Views	Keywords	Date and Time	Source	Event 3D	Task Category	Security
Webdaws Logs Application Security Setup Softem Forwarded Events Applications and Services Logs Subscriptions	Audit Success Audit Sucees Audit Success Audit Success Audit Success Audit Success Aud	2/10/2014 11:37:43 PM 2/10/2014 11:37:43 PM 2/10/2014 11:37:43 PM 2/10/2014 11:37:43 PM 2/10/2014 11:37:26 PM 2/10/2014 11:37:26 PM 2/10/2014 11:37:26 PM 2/10/2014 11:37:26 PM 2/10/2014 11:37:26 PM 2/10/2014 11:37:21 PM 2/10/2014 11:37:11 PM 2/10/2014 11:37:11 PM 2/10/2014 11:36:43 PM 2/10/2014 11:36:43 PM 2/10/2014 11:36:43 PM 2/10/2014 11:36:47 PM 2/10/2014 11:36:47 PM 2/10/2014 11:36:47 PM 2/10/2014 11:36:47 PM	Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso	9634 4624 4627 6279 6272 4634 4624 4624 4674 4672 4634 4672 5278 4624 4672 5278 4654 4672 5278	Logoff Logof Special Logon Special Logon Network Policy Server Network Policy Server Logoff Logon Credential Validation Logoff Logon Special Logon Network Bit Server Logoff Logon Special Logon Network Bit Server L Copy Save Selected Events Refresh Help	Open Saved Log Open Saved Log Oreate Custom View Import Custom View Olear Log Properties Properties Find Save All Events As Attach a Task To this Log Wew Refresh Pip Event Properties Sevent Properties

[Event Properties]を開くと、次の例に示すように、失敗の理由が表示されます。この例では、ネットワークポリシーの下で認証タイプとしてPAPが選択されていません。したがって、認証要求は失敗します。

Log Name:	Security						
Source:	Microsoft-Windows-Security-Auditing						
Date:	2/10/2014 1:35:47 PM						
Event ID:	6273						
Task Category:	Network Policy Server						
Level:	Information						
Keywords:	Audit Failure						
User:	N/A						
Computer:	win2k8.skp.com						
Description:							
Network Policy	Server denied access to a user.						
Contact the Net							
Contact the Net	work poincy server administrator for more information.						
User:							
Security ID	: SKP\vpnuser						
Account Name	e: vpnuser						
Account Doma	ain: SKP						
Fully Quali	fied Account Name: skp.com/Users/vpnuser						
Oliont Marbina							
Security ID	NULL SID						
Account Name							
Fully Qualit	led Account Name: -						
OS-Version:	- 						
Called Stat:	lon identifier: -						
Calling Stat	cion identifier: -						
NAS:							
NAS IPv4 Ado	dress: 10.105.130.69						
NAS IPv6 Ado	lress: -						
NAS Identif:	ier: -						
NAS Port-Typ	pe: Virtual						
NAS Port:	0						
RADIUS Client:							
Client Frier	ndly Name: vpn						
Client IP Ad	ldress: 10.105.130.69						

Authentication Details: Connection Request Policy Name: vpn Network Policy Name: vpn Authentication Provider: Windows Authentication Server: win2k8.skp.com Authentication Type: PAP EAP Type: -Account Session Identifier: -Logging Results: Accounting information was written to the local log file. Reason Code: 66 Reason: The user attempted to use an authentication method that is not enabled on the matching network policy.