# 使用RADIUS对Windows 2008 NPS服务器(Active Directory)进行ASA VPN用户身份验证配置示例

## 目录

<u>简介</u> 先决条件 要求 使用的组件 配置 网络图 配置 ASDM 配置 CLI 配置 Vindows 2008服务器,带NPS配置 验证 ASA调试 故障排除

# 简介

本文档介绍如何配置自适应安全设备(ASA)以使用RADIUS协议与Microsoft Windows 2008网络策略 服务器(NPS)通信,以便对传统Cisco VPN客户端/AnyConnect/无客户端WebVPN用户进行Active Directory身份验证。NPS是Windows 2008 Server提供的服务器角色之一。它相当于Windows 2003 Server, IAS(Internet身份验证服务),即RADIUS服务器的实施,提供远程拨入用户身份验证。 同样,在Windows 2008服务器中,NPS是RADIUS服务器的实施。基本上,ASA是NPS RADIUS服 务器的RADIUS客户端。ASA代表VPN用户发送RADIUS身份验证请求,NPS根据Active Directory对其进行身份验证。

## 先决条件

要求

本文档没有任何特定的要求。

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行版本9.1(4)的ASA
- 安装了Active Directory服务和NPS角色的Windows 2008 R2服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

## 配置

**注意**:使用命令查找工具(仅限注册用户)可获取有关本部分所使用命令的详细信息。

#### 网络图



#### 配置

#### ASDM 配置

- 1. 选择需要NPS身份验证的隧道组。
- 2. 单击"**编辑"**,然后选择"基本"。
- 3. 在"身份验证"部分,单击管理。

Aliases:		
	TEST	
Authentication		-
Method:	AAA      Certificate      Both     Both     Certificate     South     South	$\frown$
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	te of the group policy selected above.)	
Enable SSL VPN dient	t protocol	
Enable IPsec(IKEv2)	client protocol	
DNS Servers: 10.40.	3.10	
WINS Servers:		
Domain Name: hk.intra	axa	
•	III	•
Ne:	xt 🔘 Previous	
	Method: AAA Server Group: Client Address Assignment – DHCP Servers: Client Address Pools: Client IPv6 Address Pools: Client IPv6 Address Pools: Default Group Policy Group Policy: (Following field is an attribu I Enable SSL VPN clien I Enable IPsec(IKEv2) DNS Servers: Domain Name: hk.intra	Method: <ul> <li>AAA</li> <li>Certificate</li> <li>Both</li> </ul> AAA Server Group:       LOCAL         Use LOCAL if Server Group fails         Client Address Assignment         DHCP Servers: <ul> <li>None</li> <li>DHCP Link</li> <li>DHCP Subnet</li> </ul> Client Address Pools:       test         Client IPv6 Address Pools:       IPv6 address pool is only supported for SSL.         Default Group Policy <ul> <li>Group Policy:</li> <li>DflfGrpPolicy</li> <li>(Following field is an attribute of the group policy selected above.)</li> <li>IPv6 Enable IPsec(IKEv2) client protocol</li> <li>INS Servers:</li> <li>Domain Name:</li> <li>Hk.intraxa</li> </ul> IVINS Servers:       ID         Domain Name:       Hk.intraxa

- 4. 在AAA Server Groups部分,单击**Add**。
- 5. 在AAA Server Group字段中,输入服务器组的名称(例如,NPS)。
- 6. 从Protocol下拉列表中,选择**RADIUS**。
- 7. Click

OK.

VA Server Groups									-
ierver Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Atte	npts			Add
DCAL	LOCAL								Edit
									Coluin
			Add AAA Server	Group		X			UDELE
			AAA Server Group:	NPS					
			Protocol:	RADOUS	•		L		
indi	00	Match Case	Accounting Mode:	C Smult	rreous 💩 Single				
			Reactivation Mode:	Depiet	ion (1) Timed				
ivers in the Select	ed Group		DealThe	10 -	diaster.		-		
erver Name or IP /	Address Interfa	ce Timeout	Max Enderi Allerent		a cons				A00
			File all states	- 2					Edit
			Chable ritennia	ccounting up	Galle				Delete
			Enable Active D	rectory Agen	nt mode				Move Up
			VOUR Compati	alley Onting		(8)			Mevie Down
			WHON Compati	ancy opcies					Test
			OK	Ca	noel Hel	p			1691
indt	00	Match Case							
DAP Attribute I	Han								68
the secondates	- ap								
				-	Annly 1	honot			

- 8. 在Selected Group部分的Servers中,选择已添加的AAA Server Group,然后单击Add。
- 9. 在服务器名称或IP地址字段中,输入服务器IP地址。
- 10. 在Server Secret Key字段中,输入密钥。
- 11. 除非服务器侦听不同的端口,否则将服务器身份验证端口和服务器记帐端口字段保留为默认 值。
- 12. Click **OK**.
- 13. Click
  - OK.

1000	Name:	TEST					^ I			
Advanced	Alapes:	TEST				i (		dit AAA Server		
	Authenticator	n				-	Ser	ver Group:	NPS	
Configure AAA Se	rver Groups		an i cardhan i	-		22	Int	erface Name:	inside -	
AA Server Groups							Ser	ver Name or IP Address:	10.105.130.51	
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add	In	eout	10 seconds	
OCAL	LOCAL						RA	DIUS Parameters		
NPS	RADIUS	Single	Depletion	10	3	con	1	erver Authentication Port	1645	
						Delete		erver Accounting Port:	1646	
Pind:	000	Match Case						etry Interval:	10 seconds	
								erver Secret Kev:		
ervers in the Selec	teel Carnam									
	and aroup							Common Reserves de		
Server Name or IP	Address Interface	Timeout			6	Add		ommon Password:		
Server Name or IP	Address Interface	Timeout			- (	Add		Common Paesword: ICL Netmask Convert:	Standard	•
Server Name or IP 10.105-130.51	Address Interface	Timeout			9	Add Edit		Common Password: ICL Netmask Convert: ficrosoft CHAPv2 Capable:	Standard	•
Server Name or IP 10.105.130.51	Address Interface	Timeout 30			•	Add Edit Delete		Common Paesword: ICL Netmask Convert: ficrosoft CHAPv2 Capable:	Standard	•
Server Name or IP 00.005-130.51	Address Interface	Timeout 30			•	Add Edit Delete Nove Up	5	ionmon Password: ICL Netnask Convert: forosoft CHAPv2 Capable: Messages Message Table	Standard V	•
Server Name or IP 10: 105: 130: 51	Address Interface	Timeout 25			(	Add Edit Delete Nove Up Hove Down	sci	ionmon Password: IQ, Netmaak Convert: torosoft CHAPv2 Capable: Messages Message Table Pessage Name	Standard	-
Server Name or IP 10:105:130:51	Address Interface	Timeout 20			(	Add Edit Delete Nove Up Move Down	SD	ionmon Paesword: ICL Netmask Convert: Istrosoft CHAPv2 Capable: Messages Message Table Plessage Name ready-for-sus-cin	Standard V Message Text ACCEPT A SYSTEM G	•
Server Name or IP 10.105.130.51	Addreas Interface	Timeout 20				Add Edit Delete Nove Up Move Down Test	9 9 90	iommon Paesword: CL, Netmaak Convert: Isrosoft CHAPv2 Capable: Messages Message Table Message Name ready-for-sys-pin ready-for-sys-pin meav-pin-reenter	Standard :	•
Server Name or IP to: 105 130 51 Finds	Address Interface	Timeout 30 Match Case				Add Edit Delete Move Up Move Down Test	9 9 90	iommon Paseword: ICI, Netmaak Convert: Isrosoft CHAPv2 Capable: Messages Message Table Message Name ready for -sys spin new-pin-reenter new-pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM 6 Reenter PTN: Do you want to enter	enerated PJ
Server Name or IP to tots 130.51 Finds	Address Interface	Timeout 30 Match Case				Add Edit Delete Nove Up Nove Up Test	SD	ommon Paesword: CC, Netmaak Convert: torosoft CHAPv2 Capable Messages Message Table Message Name ready-for-sys-pin new-pin-meth new-pin-meth new-pin-meth new-pin-meth	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ente new PIN with the ne	ENERATED P3
Server Name or IP 10: 105: 130: 51 Find: IDAP Attribute	Address Interface roote	Timeout 30 Match Case				Add Edit Delete Move Up Move Down Test	SD	ommon Paesword: CC, Netmaak Convert: torosoft CHAPv2 Capable Messages Message Table Nessage Name ready-dor-sys-pin new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ente new PIN with the ne Enter Next PASSCOL	enerated P3 s your own pin xt card code of
Server Name or IP to 105 130 51 Find: LDAP Attribute	Address Interface Inside	Timeout 30 Match Case				Add Edit Delete Nove Up Move Down Test	50	ommon Paesword: CC, Netmaak Convert: torosoft CHAPv2 Capable Messages Message Table Message Name ready dor sys pin new pin-reenter new pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ento new PIN with the ne Chern Next PASSCOO New PIN Accepted New PIN Accepted New PIN Accepted	ENERATED P3
Server Name or IP 10: 105: 130: 51 Find: LDAP Attribute	Address Interface Inside	Timeout 33 Match Case	Cancel	Hdp		Add Edit Delete Move Up Move Down Test	SCO	ommon Paesword: CC, Netmaak Convert: Krosoft CHAPv2 Capable Messages Message Table Message Name ready-flor-sig-pin new-pin-reenter new-pin-meth new-pin-meth new-conde-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth new-pin-sign-req	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to enter Enter Next PASCOO New PIN Accepted Pinase remember you Enter your new Alph	• ENERATED P3 s your own pin st card code 26 ur new P1N a-Numerical P3
Server Name or IP 10: 105: 130: 51 Find: IDAP Attribute	Address Interface Inside	Timeout 32 Match Case	Cancel	Hdp		Add Edit Delete Move Up Move Down Test	50	ommon Paesword: CC, Netmaak Convert: torosoft CHAPv2 Capable Hessages Hessage Table Ressage Name ready dor sys pin new pin-reenter new pin-reenter new pin-reenter new pin-reenter new pin-reenter new pin-sys pin new pin new pin-sys pin new pin new pin new pin new pin new pin new pin new pin new pin new	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ente new PIN Accepted Please remember you Enter your new Alph to make changes.)	everated P3 s your own pin st card code 28 ur new P1N a Aumetical P1
Server Name or IP 10:105-130-51 Find: LDAP Attribute	Address Interface Inste Map	Timeout 32 Match Case	Cancel	Help		Add Edit Delete Move Up Move Down Test	504	Iommon Paesword: ICI, Nichmaek Convert: Istrosoft CHAPv2 Capable Messages Message Table Nessage Table Nessage Name ready-for-sys-pin new-pin-sechen new-pin-sechen new-pin-sep- new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep new-pin-sep	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ente new PIN with the new Enter Next PASSCOOL New PIN Accepted Please ensember you Enter your new Alph to make changes.) e default message texts	everated P3 s your own pin xt card code of ur new PDN a-Numerical P1
Server Name or IP 10: 105 130:51 Find: LDAP Attribute d:	Address Interface Inside	Match Case	Cancel	Help		Add Edit Delete Move Up Move Down Test	50	ommon Paesword: CC, Netmaak Convert: Icrosoft CHAPv2 Capable Messages Message Table Nessage Table Nessage Name ready dro sys pin new pin-reenter new pin-reenter new pin-reenter new pin-sys pin new-pin-sys pin-sys pin new-pin-sys pin new-p	Standard Standard Message Text ACCEPT A SYSTEM G Reenter PIN: Do you want to ente new PIN with the ne Enter Next PASSCO Hew PIN Accepted Pinase remember you Enter your new Alph Ito make changes.) e default message texts	eNERATED P2 y your own pin st card code of ur new PDN a-furmerical P0

- 14. 从AAA Server Group下拉列表中,选择在前面的步骤中添加的组(本例中为NPS)。
- 15. Click
  - OK.

lasic	Name:	TEST	
Advanced	Aliases:	TEST	
	Authentication		
	Method:	AAA O Certificate O 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 Pool	s:	Select
	Default Group Policy		
	Group Policy:	DfltGrpPolicy	<ul> <li>Manage.</li> </ul>
	(Following field is an attr	ibute of the group policy selected above.)	
	Enable SSL VPN die	ent protocol	
	Enable IPsec(IKEv	2) dient protocol	
	DNS Servers: 10.4	0.3.10	
	WINS Servers:		
	Domain Name:		
	<	m	
. [		Next Devices	

#### CLI 配置

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 默认情况下,ASA使用未加密的密码身份验证协议(PAP)身份验证类型。这并不意味着ASA在发送 RADIUS REQUEST数据包时以明文形式发送密码。相反,明文密码使用RADIUS共享密钥加密。

如果在隧道组下启用密码管理,则ASA使用MSCHAP-v2身份验证类型来加密明文密码。在这种情况下,请确保在ASDM配置部**分配置的"编辑AAA服**务器"窗口中选中"支持Microsoft CHAPv2"复选框

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

**注意**:test aaa**-server authentication命令始**终使用PAP。只有当用户启动与启用了密码管理 的隧道组的连接时,ASA才使用MSCHAP-v2。此外,"密码管理[密码过期天数]"选项仅受轻量 级目录访问协议(LDAP)支持。RADIUS不提供此功能。当密码在Active Directory中已过期时 ,您将看到密码过期选项。

#### Windows 2008服务器,带NPS配置

NPS服务器角色应安装并运行在Windows 2008服务器上。否则,请选择开**始>管理工具>服务器角 色>添加角色服务**。选择网络策略服务器并安装软件。安装NPS服务器角色后,请完成以下步骤 ,以便将NPS配置为接受和处理来自ASA的RADIUS身份验证请求:

1. 将ASA添加为NPS服务器中的RADIUS客户端。 选择Administrative Tools > Network Policy Server。右键单击RADIUS Clients并选择New。



输入在ASA上配置的友好名称、地址(IP或DNS)和共享密钥。

Network Policy Server	Cisco Router Properties	×		Chart
File Action View Help	Settings Advanced			Start
(= =) 🔰 🖬 🛛 🖬		-1		1
NPS (Local)	Iv Enable this RADIUS client			
RADIUS Clients and Servers	Select an existing template:			
RADIUS Clients			to your	
Remote RADIUS Server Group				
Policies	Name and Address	- 11		-
Connection Request Policies	Friendly name:			
Network Policies	Cisco Router			
Health Policies				
Accounting	Address (IP or DNS):			
Templates Management	10.105.130.69 Venty			
	Shared Secret			
	Select an existing Shared Secrets template:			
	None			
	To manually type a shared secret click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case sensitive.			
				**
		-		n D
	OK Cancel Apply			12:02 414
				7/20/2013

单击 Advanced 选项卡。从供应商名称下拉列表中,选择RADIUS标准。Click OK.

NPS (Local)	RADIUS Clients	New RADIUS Client	×
<ul> <li>RADIUS Clients and Servers</li> <li>RADIUS Clients</li> <li>Remote RADIUS Server G</li> <li>Policies</li> <li>Network Access Protection</li> <li>Accounting</li> <li>Templates Management</li> </ul>	Friendly Name	Settings       Advanced         Vendor       Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.         Vendor name:       Image: Client is the second s	

 为VPN用户创建新的连接请求策略。连接请求策略的用途是指定是本地处理来自RADIUS客户端的请求还是转发到远程RADIUS服务器。 在NPS > Policies下,右键单击Connection Request Policies并创建新策略。从Type of network access server下拉列表中,选择 Unspecified。

🤣 Network	test Properties	Start
File Actio		John
🗇 🔿 💈	Overview Conditions Settings	
NPS (Local)	Policy name: test	
RADIUS		$\mathbf{\Sigma}$
RAD	Policy State If enabled NPS evaluates this policy while processing connection requests if disabled NPS does not evalue this policy	
Policies	a chabed, hi o chabated and policy hine proceeding connection requested, hi o dece hit chabe and policy.	
Conr	V Policy enabled	
Heal		
Setwork	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	
- remplate	select Unspeched.	
	Type of network access server:	
	Unspecified	
	C Vendor specific:	
	10	
		**
		10 P
•		12:08 AM
	OK Cancel /	12012013

## <u>单击"条件**"选**项卡。单击 Add</u>。输入ASA的IP地址作为"客户端IPv4地址"条件。

Network	test Properties		Start
File Actio	Overview Conditions Settin	igs	
	Configure the conditions for th	nie network policy	
NPS (Local)	Conligate the conditions for a		
RAD	connection request, NPS skip	ection request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.	2
Rem Rem			
Conr	Condition	Value	
Netv	👰 Client IPv4 Address	10.105.130.69	
Heal			
Accounti			
🛒 Templati			
		12	
		v	
			_
	Condition description:		
	The Client IP Address condition	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
		Add Edit Remo	v «
2			
			12:08 AM
		OK Cancel	7/20/2013

单击"设**置"**选项卡。在Forwarding Connection Request(转发连接请求)下,选择 Authentication。确保选择Authenticate requests on this server单选按钮。Click



3. 添加网络策略,在该策略中可以指定允许哪些用户进行身份验证。例如,可以添加Active Directory用户组作为条件。只有属于指定Windows组的用户才会在此策略下进行身份验证。在 NPS下,选择Policies。右键单击Network Policy并创建新策略。确保已选择Grant access单选 按钮。从Type of network access server下拉列表中,选择Unspecified。

Oven	view Conditions Constraints Settings
Poli	cy name: test
F F	olicy State enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. 7 Policy enabled
A	ccess Permission conditions and constraints of the network policy match the connection request, the policy can either grant access or deny ccess. <u>What is access permission?</u>
с С	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
N	authorization with network policy only; do not evaluate the dial-in properties of user accounts . etwork connection method elect 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. If your network access server is an 802.1X authenticating switch or wireless access point, lect Unspecified
G	Type of network access server:
	Vendor specific:
C	10 🚖

单击"条件**"选**项卡。单击 Add。输入ASA的IP地址作为客户端IPv4地址条件。输入包含VPN用 户的Active Directory用户组。

			configured.	
_				
450	Condition	Value		
	User Groups	5KP\VPN		_
L .				
Cond	tion description:			
Cond The (	tion description: Jient IP Address conditio	on specifies the IP address of the RADIUS client that forwarded th	e connection request to NPS.	
Cond The (	tion description: Jient IP Address conditio	on specifies the IP address of the RADIUS client that forwarded th	e connection request to NPS.	
Cond The (	tion description: Jient IP Address conditio	ion specifies the IP address of the RADIUS client that forwarded th	e connection request to NPS.	

单击"约束**"(Constraints**)选项卡。选择**Authentication Methods**。确保选中Unencrypted authentication(PAP, SPAP)复选框。Click **OK**.

Overview Conditions Constraints Set	tings	
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	Allow access only to those clients that authenticate with the specified methods.	
Julie Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed.	
Called Station ID	Move Up	
Day and time restrictions	Move Down	
T NAS Port Type		
	Add Edit Remove	
	Less secure authentication methods:	
	✓ Motosoft Encrypted Authentication Version 2 (MSCHAP-V2)	
	Microsoft Encrypted Authentication (MS-CHAP)	
	User can change password after it has expired	
	Encrypted authentication (CHAP)	
	Unencrypted authentication (PAP, SPAP)	
	Allow clients to connect without negotiating an authentication method	
	I_ Perform machine health check only	E
		1
		f I

从NPS RADIUS服务器传递组策略属性(属性25)

如果需要使用NPS RADIUS服务器将组策略动态分配给用户,则可以使用组策略RADIUS属性(属 性25)。

完成以下步骤,以便向用户发送RADIUS属性25,以便动态分配组策略。

1. 添加网络策略后,右键单击所需的网络策略,然后单击"设置"选项卡。



2. 选择RADIUS属性>标准。单击 Add。将"访问"类型保留为"全部"。

Network Policy Server	
File Action Vitest Properties	
Image: Section of the sectio	uest and the policy gravits access, settings are applied
Remot	Add Standard RADIUS Attribute
E Policies RADIUS Attributes To ser	the second secon
Conne 🚯 Standard then o	ick Edi. I is add an appole to the settings, select the appole, and then click Add.
Health Vendor Specific	ADIOS (a) To add a custom or predefined Vendor Specific altibule, close this dialog and select Vendor Specific, and then click
🗷 🐜 Network A 💦 Network Access Protection	AG
📲 Accounting 🐘 NAP Enforcement	Access (pe
🗄 🛃 Templates 🥔 Attribut	es:
Nam Evended state	t at Poster
Houting and Remote Access Service	Allibutes:
Allocation Protocol (BAP)	Name A
TP Files	College & Colleg
C Formite	Clers
	FitsHd
A IP Settings	Framed AppleTalk-Link
A	dd Framed AppleTalk-Network
	kamedonnel su, com
	Description
	Specifies the length of the interval (in seconds) between each interim update that the NAS sends.
	Add Dava
	Sur. Lus
	OK Cancel Apply

3. 在"属性"框中,选择"类"并单击"添加"。输入属性值,即作为字符串的组策略名称。请记住,必须在ASA中配置具有此名称的组策略。这样,ASA在RADIUS响应中收到此属性后将其分配给 VPN会话。



## 验证

使用本部分可确认配置能否正常运行。

注意:使用 debug 命令之前,请参阅有关 Debug 命令的重要信息。

#### 在ASA上启用debug radius all。

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: 0x8000001 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) = 28 c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 (.h....Z.oC 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 : regauth: 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).... | ....N...Kv .....+..7 02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37 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) = 0x1Radius: Type = 6 (0x06) Service-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x2Radius: Type = 25 (0x19) Class Radius: Length = 46 (0x2E)Radius: Value (String) = 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a 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

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

- 确保ASA和NPS服务器之间的连接正常。应用数据包捕获,确保身份验证请求离开ASA接口 (从可访问服务器的位置)。确认路径中的设备不会阻止UDP端口1645(默认RADIUS身份验 证端口),以确保其到达NPS服务器。有关ASA上数据包捕获的详细信息,请参阅 <u>ASA/PIX/FWSM:使用 CLI 和 ASDM 进行数据包捕获的配置示例.</u>
- 如果身份验证仍然失败,请查看Windows NPS上的事件查看器。在"事件查看器">"Windows日志"下,选择"安**全"。**查找在身份验证请求期间与NPS关联的事件。

Event Vewer (Local)	Security Number of events: 93 (1) New events available					Actions	
Custom Views     Windows Loos	Keywords	Date and Time	Source	Event ID	Task Category	Security	-
Wendows Copy Security Security Setup System Porwarded Events Applications and Services Logs Subscriptions	Audit Success Audit Suceess Audit Suceess Audit Suceess Audit Suceess Audit Suceess Au	2/10/2014 1:37:43 PM 2/10/2014 1:37:43 PM 2/10/2014 1:37:43 PM 2/10/2014 1:37:43 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:21 PM 2/10/2014 1:37:21 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:47 PM	Microso Microso	4634 4624 4672 6270 4634 4624 4624 4624 4674 4672 4634 4672 4634 4672 4634 4672 4672 4672 4672 4672 4672 4673	Logoff Logon Special Logon Network Policy Server Network Policy Server Logoff Logon Logon Credential Validation Logoff Logon Special Logon Special Logon Logoff Logoff Logoff Logoff Logon Logoff Logo	Open Saved Log     Open Saved Log     Create Custom View     Import Custom View     Olear Log     Properties     Properties     Find     Save All Events As     Attach a Task To this Log     View     Refresh     Properties     Event Properties     Event Properties     Event Properties     Attach Task To This Event     Event Properties     Attach Task To This Event     Event Properties     Copy	····

#### 打开事件属性后,您应该能够看到失败的原因,如示例所示。在本示例中,未在网络策略下选 择PAP作为身份验证类型。因此,身份验证请求失败。

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	twork Policy 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					
Client Markins						
Client Machine						
Security ID	: NULL SID					
Account Name						
Fully Quali:	fied Account Name: -					
OS-Version:	-					
Called Stat:	ion Identifier: -					
Calling Stat	tion Identifier: -					
NAS:	10 105 120 60					
NAS IPV4 Add	aress: 10.105.130.69					
NAS IPV6 Add	aress: -					
NAS Identii:	ler: -					
NAS Port-Typ	pe: Virtual					
NAS Port:	0					
DADTUS Clicat.						
Cliont Eric	ndly, Namo, yon					
Client TD A	$\frac{101}{1000}$					
CITEUR IN VO	AULESS: 10.103.130.09					

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.