ASA VPN User Authentication against Windows 2008 NPS Server (Active Directory) with RADIUS Configuration Example

Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Configurations ASDM Configuration CLI Configuration Windows 2008 Server with NPS Configuration Verify ASA Debugs Troubleshoot

Introduction

This document explains how to configure an Adaptive Security Appliance (ASA) to communicate with a Microsoft Windows 2008 Network Policy Server (NPS) with the RADIUS protocol so that the legacy Cisco VPN Client/AnyConnect/Clientless WebVPN users are authenticated against Active Directory. NPS is one of the server roles offered by Windows 2008 Server. It is equivalent to Windows 2003 Server, IAS (Internet Authentication Service), which is the implementation of a RADIUS server to provide remote dial-in user authentication. Similarly, in Windows 2008 Server, NPS is the implementation of a RADIUS server. Basically, the ASA is a RADIUS client to an NPS RADIUS server. ASA sends RADIUS authentication requests on behalf of VPN users and NPS authenticates them against Active Directory.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ASA that runs Version 9.1(4)
- Windows 2008 R2 Server with Active Directory services and NPS role installed

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Note: Use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) in order to obtain more information on the commands used in this section.

Network Diagram



Configurations

ASDM Configuration

- 1. Choose the tunnel-group for which NPS authentication is required.
- 2. Click Edit and choose Basic.
- 3. In the Authentication section, click **Manage**.

Basic	Name:	TEST	
-Advanced	Aliases:	TEST	
	Authentication		
	Method:	● AAA	
	AAA Server Group:	LOCAL 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.	
		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 🔘 Previous	

- 4. In the AAA Server Groups section, click Add.
- 5. In the AAA Server Group field, enter the name of the server group (for example, NPS).
- 6. From the Protocol drop-down list, choose **RADIUS**.
- 7. Click

OK.

A Server Groups								-
erver Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attem	pts		Add
DCAL	LOCAL							Edit
								Delate
			Add AAA Server	Group		-X-		- COLIC
			AAA Server Group:	NPS				
			Protocol:	RADOUS	-1			
ndt	00	Match Case	Accounting Node:	C Smit	aneous a Sincle			
			Caarts man Made	· Decisi	in . D Tread			
ivers in the Select	ed Group		Nedepotent Proces	in network				_
erver Name or IP A	Address Interfa	ce Timeout	Dead Trise:	10 *	motes			Add
			Max Paled Attempts	- 3				Edit
			Crable interim a	ccorreging rib	ida te			Delete
			E trable Active De	rectory Ager	nt mode			Move Up
			VOUR Compatib	the function				Move Down
			WHON Company	ancy opcies				Test
			OK	Ca	incel Help			TOP
ndt	00	Match Case						
DAP Attribute h	Hap							68
				- C.	Apply R	teet		

- 8. In the Servers in the Selected Group section, choose the AAA Server Group added and click **Add**.
- 9. In the Server Name or IP Address field, enter the server IP address.
- 10. In the Server Secret Key field, enter the secret key.
- 11. Leave the Server Authentication Port and the Server Accounting Port fields at the default value unless the server listens on a different port.
- 12. Click OK.
- 13. Click
 - OK. Edit AnyConnect Connection Profile: TEST 1111 -Advanced TEST Name: Edit AAA Serve - 22 Alapes: TEST Server Group: NPS Authenticator 22 Interface Name: inside + Configure AAA Server Groups Server Name or IP Address: 10.105.130.51 AAA Server Groups 10 seconds Treout: Server Group Protocol Accounting Mode Reactivation Mode Dead Time Add Max Failed Attempts **RADIUS Parameters** LOCA LOCAL Edit Server Authentication Port: 1645 Delete Server Accounting Port: 1646 🔘 🔘 🖂 Match Case Finds Retry Interval: 10 second Server Secret Key: Servers in the Selected Group Common Paesword: Server Name or IP Address Interface Timeout ACL Netmask Convert: Standard Microsoft CHAPv2 Capable: 📝 Delete SDI Messager Message Table 2 Message Name Message Text Hove Do ready-for-sys-pin ACCEPT A SYSTEM GENERATED PIN new-pin-reenter Reenter PIN: Do you want to enter your own pin new PDI with the next card code Enter Next PASSCODE Find: 🗇 🔘 🖂 Match Case new-pin-meth next-ccode-and-reauth LDAP Attribute Map next-code www.pin-eye-ok New PIN Accepted Please remember your new PDN OK Cancel Help www.pin-sup nevi-pin-reg Enter your new Alpha-Numerical PIN (Double-dick in a text cell to make changes.) . Restore default message texts Next Previous Find: OK Cancel Help OK Cancel Help
- 14. From the AAA Server Group drop-down list, choose the group (NPS in this example) added in the previous steps.
- 15. Click

OK.

Basic	Name:	TEST	
Advanced	Aliases:	TEST	
	Authentication		
	Method:	AAA Certificate Both	
	AAA Server Group:	NPS	✓ Manage
		Use LOCAL if Server Group fails	
	Client Address Assignment –		
	DHCP Servers:		
		None O DHCP Link O 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	t protocol	
	Enable IPsec(IKEv2)	dient protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name:		
Find:	O Ne	xt O Previous	

CLI Configuration

```
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

By default, the ASA uses the unencrypted Password Authentication Protocol (PAP) authentication type. This does not mean that the ASA sends the password in plain text when it sends the RADIUS REQUEST packet. Rather, the plaintext password is encrypted with the RADIUS shared secret.

If password management is enabled under the tunnel-group, then ASA uses the MSCHAP-v2

authentication type in order to encrypt the plaintext password. In such a case, ensure that the **Microsoft CHAPv2 Capable** check box is checked in the Edit AAA Server window configured in the ASDM configuration section.

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

Note: The **test aaa-server authentication** command always uses PAP. Only when a user initiates a connection to tunnel-group with password-management enabled does the ASA use MSCHAP-v2. Also, the 'password-management [password-expire-in-days days]' option is only supported with Lightweight Directory Access Protocol (LDAP). RADIUS does not provide this feature. You will see the password expire option when the password is already expired in Active Directory.

Windows 2008 Server with NPS Configuration

The NPS Server Role should be installed and running on the Windows 2008 server. If not, choose **Start > Administrative Tools > Server Roles > Add Role Services**. Choose the Network Policy Server and install the software. Once the NPS Server Role is installed, complete these steps in order to configure the NPS to accept and process RADIUS authentication requests from the ASA:

 Add the ASA as a RADIUS client in the NPS server. Choose Administrative Tools > Network Policy Server. Right-click RADIUS Clients and choose New.

💫 N	etwork Policy	Server						<u>_ 8 ×</u>	Manut
File	Action Vier	w Help							Start
	ءَ 🖄 🛋	? 🖬							
NPS	(Local)		RADIUS Clients						
F F	ADIUS Clients	and Servers		tente alleur una te	on a situation of the sectored sectored	and approx the	t arm tida a a a a a ta		$\mathbf{\Sigma}$
	Remote RA	New	network.	itents allow you to	specify the network acc	cas servers, una	r provide access to	your	
EF	Policies	15xport List							100
5	Connection	View 🕨	Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status		
	Health Polic	Refresh	Cisco Router	10.105.130.69	RADIUS Standard	No	Enabled		
5 M	Vetwork Acces	Hala							
24	Accounting	nep	4						
21	Cilipiates Maria	syement							
3									**
									n P
									2:31 AM
•)	<u> </u>						7/20/2013
Jaw B	Jahungk Accore	Device							

Enter a Friendly name, Address (IP or DNS), and Shared Secret configured on the ASA.

移 Network Policy Server	Cisco Router Properties	×		Start
File Action View Help	Settings Advanced			Start
🗢 🔿 🙋 📅 🛛 🖬	Excite the PADIUS store	1		1
NPS (Local)	P Diable this NADIOS Clerk			-1.00
RADIUS Clients and Servers	Select an existing template:			
RADIUS Clients	×		to your	
Remote RADIUS Server Group				
Connection Request Policies	Name and Address			
Network Policies	Friendly name:			
Health Policies	JUSCO HOUTER			
Network Access Protection	Address (IP or DNS):			
Accounting	10.105.130.69 Verify			
I emplates Management				
	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.			
	Confirm shared secret:			
				**
				The ID
	OK Cancel Apply			12:02 414
• •	<u></u>	_		7/20/2013

Click the **Advanced** tab.From the Vendor name drop-down list, choose **RADIUS Standard**.Click

OK.

RADIUS Clients and Servers	×
Policies Policies Policies Policies Policies Templates Management Policies Templates Management Policies Po	nt Te de

 Create a new Connection Request Policy for VPN users. The purpose of the Connection Request Policy is to specify whether the requests from RADIUS clients are to be processed locally or forwarded to remote RADIUS servers. Under NPS > Policies, right-click
 Connection Request Policies and create a new policy. From the Type of network access server drop-down list, choose
 Unspecified.

Network	test Properties		Start
File Actio	Overview Constructed Com		
(= =) 2	Overview Conditions Settings	1	
NPS (Local)	Policy name:	test	
	- Ostar Osta		$\mathbf{\Sigma}$
Rem	If enabled, NPS evaluates this	s policy while processing connection requests. If disabled, NPS does not evalue this policy.	
Policies			
Conr Netv	Policy enabled		
📔 Heal	Network connection method		
Network	Select the type of network act	cess server that sends the connection request to NPS. You can select either the network access server	
Template	type or Vendor specific, but ne select Unspecified	ather is required. If your network access server is an 802.1X authenticating switch or wireless access poin	
	outor enqueenes.		
	Type of network access s	erver:	
	Unspecified		
	C Vendor specific:		
	10 🚔		
			**
			the P
			12:08 AM
•		OK Creat	7/20/2013
		UK Cancel /	

Click the **Conditions** tab.Click **Add**.Enter the ASA's IP address as a 'Client IPv4 Address' condition.

🚯 Networl	Palieu Consus	-
Ella Activ	test Properties	Start
	Overview Conditions Settings	1
NPS (Local)	Configure the conditions for this network policy.	
	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.	$\mathbf{\Sigma}$
Ren		-
Con	Condition Value	
📑 Net	Client IPv4 Address 10.105.130.69	
📔 Hea		
Network		
Account	11	
Templat	ξ.	
	~	
	Condition description	
	The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS	
	The share in the second s	
	Add Edit Remov	**
		the PD
		17.09 414
•		7/20/2013
	OK Cancel ,	12012015

Click the **Settings** tab.Under Forwarding Connection Request, choose **Authentication**. Ensure the Authenticate requests on this server radio button is chosen.Click **OK**.



3. Add a Network Policy where you can specify which users are allowed to authenticate.For example, you can add Active Directory user groups as a condition. Only those users who belong to a specified Windows group are authenticated under this policy.Under NPS, choose **Policies**.Right-click **Network Policy** and create a new policy.Ensure the Grant access radio button is chosen.From the Type of network access server drop-down list, choose **Unspecified**.

test P	roperties	A7Sta
Ove	rview Conditions Constraints Settings	-
Pol	icy name: Itest	E.
		6
	olicy State f enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	-
F	Policy enabled	C
F	Access Permission	
	f conditions and constraints of the network policy match the connection request, the policy can either grant access or deny	
4	scoess. What is access permission?	
6	Grant access Grant access if the connection request matches this policy	
6	Denviscoes Denviscoes if the connection request matches this policy	
	Jonara usar account dialla presentes	
	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	
5	elect the type of network access server that sends the connection request to NPS. You can select either the network access server type	
s	elect Unspecified.	
	Iype or network access server:	
(Vendor specific:	**
	10 🚔	1
		- 12:1

Click the **Conditions** tab.Click **Add**.Enter the ASA's IP address as a Client IPv4 Address condition.Enter the Active Directory user group which contains VPN users.

	Condtion	Value
192	User Groups	SKP\VPN
	Client IPv4 Address	10.105.130.69
Conc	lition description: Client IP Address conditio	tion specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Click the **Constraints** tab.Choose **Authentication Methods**.Ensure the Unencrypted authentication (PAP, SPAP) check box is checked.Click **OK**.

test Properties		A s
Overview Conditions Constraints Se	ttings	- 1
Configure the constraints for this network If all constraints are not matched by the	k policy. connection request, network access is denied.	6
Contrainte		5
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. EAP Types:	
Called Station ID	MoveUp	
Day and time restrictions	Move Down	
T NAS Port Type		
	Add Edit Remove	
	Less secure authentication methods:	
	Microsoft Encrypted Authentication version 2 (MS-CHAP-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	
	Perform machine health check only	_
		**
		Ch
		12:1
	OK Cancel Ann	7/20

Pass Group-policy Attribute (Attribute 25) from the NPS RADIUS Server

If the group-policy needs to be assigned to the user dynamically with the NPS RADIUS server, the group-policy RADIUS attribute (attribute 25) can be used.

Complete these steps in order to send the RADIUS attribute 25 for dynamic assignment of a group-policy to the user.

1. After the Network Policy is added, right -click the required Network Policy and click the **Settings**

tab.



2. Choose **RADIUS Attributes > Standard**. Click **Add**. Leave the Access type as All.

/ \11.			
Notwork Policy	Server est Properties		
File Action Ville			
(= =) 🖄 📅	Overview Conditions Constraints Settings	1	
😝 NPS (Local) 🖂 🔛 RADIUS CI	Configure the settings for this network policy. If conditions and constraints match the connect	tion request and t	he policy grante access, settings are applied
RACOU	0		
Remot	settings		Add Standard RADIUS Attribute
🖻 🧾 Policies	BADIUS Altributes	To send additor	
Conne 🔛	🚯 Standard	then click Edit. I	To add an attribute to the settings, select the attribute, and then click Add.
🖾 Netwo	- Under Casse Xe	your RADIUS di	To add a custom or medalined Vendor Snecilic altibute close this dialog and select Vendor Snecilic, and then dick
📑 Health	Vendor specific		Add.
🗄 🋬 Network A	Network Access Protection		
Accountin;	NAP Enforcement	64.3. to	Access (be
🗄 📑 Templates	The state of the state	Antibures:	A1 T
	Evended state	Name	
	Routing and Remote Access	FramedProtoc	Attributes:
	💑 Multiink and Bandwidth	Service-Type	Name
	Allocation Protocol (BAP)		Apphinteriminterval
	TP Files		Calbeck-Number
	Counting		Clara
	thorypaon 💼		Fibeld
	💑 IP Settings		Framed Annie Tak-Link
			Framed Apple Talk Network
		P.00	Figmed AppleT alu Zono
			Description
			Specifies the length of the interval (in seconds) between each interim update that the NAS sends
4			
	1		Add. Dave
			UN Lance A000

3. In the Attributes box, choose **Class** and click **Add**. Enter the attribute value, that is, the name of the group-policy as a string. Remember that a group-policy with this name has to be configured in the ASA. This is so that the ASA assigns it to the VPN session after it receives this attribute in the RADIUS response.

Network Polic	y Server test Properties						
File Action W	Dverview Conditions Constraints Settin	ve)					
NP5 (Local)	Configure the settings for this network polic	- I 9					
E RADIUS CI	If conditions and constraints match the con	rection request and t	policy grants access, settings are applied.				
Remot	Sellings		Add Standard RADIUS Attribute				
E E Folces	Standard	To send addition then click Edit. I	To add an attribute to the settings, select the attribute, and then click Add				
Contraction Network	Z Vendor Specific	your RADIUS of	To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click				
🗄 🌺 Network A	Network Accessorolection		Adde				
E Templates	S NAP Enforcement	Athibutes	A				
	Extended State	Name Examed-Exator					
	Multink and Bandwidth	Service-Type	Abbules Abbules				
	Allocation Protocol (BAP)		Acctivitationinterval				
	A Encusion						
	💑 IP Sellings	-	FileNd FramesblopdeT elbilink				
		Add	Framed-AppleTalk-Network				
			France Greeke Tab. Zena				
			Description:				
			Specifies the classification of accounting records.				
-							
		1	Add Dose				
			DK Carriel Arch				
-							
Network Polic	v Server test Properties						
File Action Vi	v Server test Properties Dverviex Conditions Constraints Setti	ngs					
Network Polic File Action Vi (+	v Server Test Properties Overview Conditions Constraints Setti Configue the settings for this network place Discretiging and settings for this network the set	ngs 3/					
Network Polic File Action View 2 NPS (Lecel) RADDUS Cl RADDUS Cl	v Server Lest Properties Dverviex Conditions Constraints Setti Configue the settings for this network pole If configure and constraints match the con Settings	ngs % mection request and (the policy grants access, settings are applied				
Network Polic File Actor Vi NPS (Local) RADIUS CI RADIUS	v Server Lest Properties Dverview Conditions Constraints Settin Configue the satings for this network pole If conditions and constraints match the con Settings: RADIUS Attributes	nas) 9) median request and t	the policy grants access, sellings are applied.				
	v Server Lest Properties Dverview Conditions Constraints Setti Contigue the settings for this network pole If conditions and constraints match the con Settings RADIUS Attributes Standard	ngs Winnection request and f To send addition them citick Edit 1 wow PADUS citi	the policy grants access, settings are applied. Add Standard RADIUS Attribute To add an attribute to the astringe, select the attribute, and then slick Add.				
File Action Vi File Action Vi Professional Control RADIU RADI	v Server Lest Properties Overview Conditions Constraints Settin Configure the settings for this network pole If conditions and constraints match the con Settings: FADIUS Attributes Standard Vendor Specific	nss) 9 median request and f 1 To send addiar Pien cick Edit I peur RADIUS cli	Add Standard RADIUS Attribute Add Standard RADIUS Attribute To add an attribute to the estings, ested the attribute, and then click Add. To add an attribute to the settings, ested the attribute, and then click Add. To add a custom or precisioned Vender Specific Attribute classe this finite workselect Vender Specific, and then click Add Attribute Information				
Network Police File Action Vi Action Vi Police RADDUS Cl RADDUS Cl RADDUS Cl RADDUS Cl Remot Re	Server Lest Properties Derview Conditions Constraints Settin Configue the satings for this network pole If conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection NoP Enjacement	nas) median request and t To send additor men olok Edit 1 yeur PADIUS di	Imit xi X Add Standard RADIUS Attribute To add an attribute to the astrings are applied. To add an attribute to the astrings, select the attribute, and then blok Add. To add a custom or predefined Vender Specific attribute, close this dialon and select Vender Specific, and then blok Add Attribute Information Access type: Attribute name:				
	Server test Properties Overviex Conditions Constraints Settin Corligue the settings for this network pole If conditions and constraints match the con Settings FADIUS Attributes Standard Vendor Specific Network Access Protection MAP Enforcement Kelended State	nss) y To send additor here clock Edit 1 peur PIADIUS cli Athibutes: Name					
File Acton Vi File Acton Vi Policical RADUS CI RADUS RADUS Remot	Itest Properties Diverview Conditions Constraints Settin Configure the settings for this network pole If conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection Network Access Protection Network Access Protection NAP Enforcement Settended State Routing and Remote Access	y median request and t To send addiar frem cick Edit I jour FIADIUS cli Attributes: Name Framed Protoc					
Network Police He Acton V Acton V Ple	Server Lest Properties Overview Conditions Constraints Settin Configue the satings for this network pole If conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection M P Enforcement Setting and Remote Access Multink and Remote Access	y mection request and to mection request and to free clock Edit 1 year PADIUS cli Attributes: Name FramedProtoc Service-Type					
File Acton Vi File Acton Vi Physical Cool RADUS CI RADUS CI R	Itest Properties Overview Conditions Constraints Setting Contigue the settings for this network polic if conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Standard Yendor Specific Network Access Protection NAP Enforcement NAP Enforcement Number of Benotic Access Multink and Benote Access Multink and Benote Access Whiles and Benote Access Prices	y median request and t To send additor hen cick Edi 1 peur PADIUS di Athibutes: Name Framed Protoc Service-Type					
He twork Polic Fie Actor Vi Police() RADUS CI RADUS Polices Polices Network Network Recoverka Recoverka Recoverka Recoverka Recoverka	Itest Properties Derives Conditions Constraints Settin Configue the settings for this network pole If conditions and constraints match the con- Settings: RADIUS Attributes Standard Wendor Specific Network Access Protection Not Work Access Protection NAP Enforcement Set Extended State Routing and Remote Access Multink and Remote Access Receiver Protocol (BAP) The Prices Encryption	y median request and t To send additor frem cick Edi I pour FIADIUS cli Attributes: Name FramedProtoc Service-Type					
Network Police File Action Vi Police Republic Conne	Itest Properties Dverview Conditions Constraints Setting Configure the settings for this network pole if conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: RADIUS Attributes Standard Iterative Access Protection Iterating and Remote Access Multink and Remote Access Iterating and Remote Access Iterating and Remote Access Iterating and Remote Access Iterations Iteratinetee	y mection request and to mection request and to free clock Edit 1 year PADIUS cli Attributes: Name FramedProtoc Service-Type					
Fie Acton Vi	Verticer Itest Properties Overview Conditions Constraints Setting Contigues the settings for this network polic It conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Standard Iteration Specific Network Access Protection NAP Enforcement NAP Enforcement Noting and Remote Access Multink and Bandwidth Alocelion Protocol (BAP) IP Filers Encorption IP Settings	y median request and t hen clok Edi I yeur PADIUS di Attributes: Name Framed Photoc Service-Type Add					
Network Polic File Actorn Vi Res RADUS CI RADUS CI Renes Renes Retwork Retwork Retwork Recounting Retwork Recounting	Itest Properties Derivest Conditions Constraints Settin Configue the settings for this network pole It conditions and constraints match the con- Settings: FADIUS Attributes Standard Standard Specific Network Access Protection Mark Access Protection Setting and Remote Access Routing and Remote Access Multink and Bandwith Alocation Protocol (BAP) T IP Files Encryption M IP Settings	y mection request and the free cick Edit I your FIADIUS of Attributes: Name FramedProtoc Service-Type Add.	Add Standard RADIUS Attribute To add an attribute to the settings are applied Add standard RADIUS Attribute To add an attribute to the settings, select the attribute, and then click Add. To add a custom or preteined Vender Severith Attribute close this dation and select Vender Severith Attribute Information Add Add Add Add at custom or preteined Vender Severith Attribute, and then click Add. Add Add Add Add Add Add Attribute Information Attribute number: Attribute format: OctedString Class Attribute format: OctedString Class Premed/AppleTaky Fremed/AppleTaky Fremed/AppleTaky Premed/AppleTaky Premed/AppleTaky <tr< td=""></tr<>				
Network Police Fie Acton Vi Pie Acton Pie A	Itest Properties Overview Conditions Constraints Setting Conditions and constraints match the constraints Settings: PADIUS Attributes Standard Image: Standard Image: Vendor Specific Network Access Protection Standard Image: Extended State Pouting and Remote Access Multink and Bandwidth Access Protection (BAP) IP Files Image: Encryption Image: Files Image: Encryption Image: Files Image: Encryption Image: Files Image: Encryption Image: Files	y mection request and to mection request and to men clock Edit 1 peur PADIUS cli Attributes: Name Framed-Protoc Service-Type Add					
Fie Acton Vi Fie Acton Vi Pie Acton Vi RADUS CI RADUS CI RADU	Vertice: Dverview Conditions Constraints Setting Contigue the settings for this network polic it conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Standard Wendor Specific Network Access Protection NAP Enforcement NAP Enforcement Noting and Remote Access Multink and Bandwith Alocation Protocol (BAP) P IP Files Encorption IP Settings	y median request and the hencick Edi I peur PADIUS di Attributes: Name Framed Protoc Service-Type Add	Add Standard RADIUS Attribute X Add standard RADIUS Attribute X To add an attribute to the astlings, asked the attribute, and then slick Add. X To add a custom or precisional Vendro Specific attribute, close this finion and select Vendro Specific, attribute close this finion and select Vendro Specific, and then slick Add. To add a custom or precisional Vendro Specific attribute, close this finion and select Vendro Specific, and then slick Add. Add Access type Attribute name: All Attribute name: All Attribute format: Abstitute format: 25 Name Attribute format: Abstitute format: Calleack Number Calleack Number Sting Fremed/key lei Take, Fremed/key lei T				
Network Police File Action Vi Pile Action Vi	Vertices Dverview Conditions Constraints Setting Conditions and constraints match the conditions and constraints match the conditions and constraints match the conditions Settings: FADIUS Attributes Standard Image: Product Specific Network Access Protection NAP Enforcement Image: Extended State Pouting and Remote Access Roceine Proteol (BAP) Image: IP Filers Image: Encryption Image: IP Settings	y mection request and the merchak Edit I yeur RADIUS di Attributes: Name FramedProtoc Service-Type Add	Add standard RADIUS Attribute Image: Select the attribute, and then blok Add. To add an attribute to the settings, select the attribute, and then blok Add. Image: Select the attribute, and then blok Add. To add a custom or preferred Vencior Scorelin, attribute, and then blok Add. Image: Select the attribute, and then blok Add. To add a custom or preferred Vencior Scorelin, attribute, and then blok Add. Image: Select the attribute formation Add Attribute Information Image: Select the attribute value in: Attribute format: Class Image: Select the attribute value in: Fiered Select the classifier Ensembles: Image: Select the classifier Freed Select the classifier Image: Select the classifier Image: Select the classifier Description: Image: Select the classifier Image: Select the classifier Description: Image: Select the classifier Image: Select the classifier Specifier Image: Select the classifier Image: Select the classifier				
Network Police File Action With Structure Image: Structure Image: Structure <td>Server Lest Properties Overview Conditions Constraints Setting Contigue the settings for this network pole if conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Standard It constraints Standard Note that Access Protection NAP Enforcement NAP Enforcement Noting and Remote Access Multink and Bandwidth Alocelion Protocol (BAP) P IP Filers Encorption IP Settings</td> <td>y median request and the hencick Edi I yeur PADIUS di Attributes: Name Framed Photoc Service-Type Add</td> <td>Imit xi Imit xi Add Standard RADIUS Attribute To add an attribute to the astrings, asled the attribute, and then slick Add. To add an attribute to the astrings, asled the attribute, and then slick Add. To add a custom or predefined Vendor Specific attribute, all then slick Add. Access type Attribute number: Attribute number:</td>	Server Lest Properties Overview Conditions Constraints Setting Contigue the settings for this network pole if conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: FADIUS Attributes Standard It constraints Standard Note that Access Protection NAP Enforcement NAP Enforcement Noting and Remote Access Multink and Bandwidth Alocelion Protocol (BAP) P IP Filers Encorption IP Settings	y median request and the hencick Edi I yeur PADIUS di Attributes: Name Framed Photoc Service-Type Add	Imit xi Imit xi Add Standard RADIUS Attribute To add an attribute to the astrings, asled the attribute, and then slick Add. To add an attribute to the astrings, asled the attribute, and then slick Add. To add a custom or predefined Vendor Specific attribute, all then slick Add. Access type Attribute number: Attribute number:				

Verify

Use this section to confirm that your configuration works properly.

Note: Refer to <u>Important Information on Debug Commands</u> before you use **debug** commands.

ASA Debugs

Enable debug radius all on the ASA.

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 7fA.....~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 0x80000001 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 37 | ...N..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
| .:.o.....
1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03
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) = 0x2
Radius: 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 | ....<
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- Ensure the connectivity between the ASA and the NPS server is good.Apply packet captures to ensure the authentication request leaves the ASA interface (from where the server is reachable). Confirm that the devices in the path do not block the UDP port 1645 (default RADIUS authentication port) in order to ensure it reaches the NPS server. More information on packet captures on the ASA can be found in <u>ASA/PIX/FWSM: Packet Capturing using CLI and ASDM Configuration Example</u>.
- If the authentication still fails, look in the event viewer on the windows NPS. Under Event Viewer > Windows Logs, choose Security. Look for events associated with NPS around the time of the authentication request.

Event Viewer						S_X
File Action View Help						
💠 🔿 🖄 📅 📓 📅						
Event Viewer (Local)	Security Number of	Actions				
Custom Views Worknus Loos	Keywords	Date and Time	Source	Event ID	Task Category	Security 🔺
	Audit Success	2/10/2014 1:37:43 PM	Microso	4634	Logoff	S Open Saved Log
Security	Audit Success	2/10/2014 1:37:43 PM	Microso	4624	Logon	
Setup	Audit Success	2/10/2014 1:37:43 PM	Microso	4672	Special Logon	Treate Custom View
System	Audit Success	2/10/2014 1:37:28 PM	Microso	6278	Network Policy Server	Import Custom View
Forwarded Events	Audit Success	2/10/2014 1:37:28 PM	Microso	6272 Network Pol	Network Policy Server	Charles
🗉 📇 Applications and Services Logs	Audit Success	2/10/2014 1:37:28 PM	Microso	4634	Logoff	Clear Log
Subscriptions	Audit Success	2/10/2014 1:37:28 PM	Microso	4624	Logon	Piter Current Log
	Audit Success	2/10/2014 1:37:28 PM	Microso	4648	Logon	Properties
	Audit Success	uccess 2/10/2014 1:37:28 PM Microso 4776 Credential Validation	Credential Validation			
	Audit Success	2/10/2014 1:37:24 PM	Microso	io 4634 Logoff		He Find
	Audit Success	2/10/2014 1:37:11 PM	Microso	4624	Logon	Save All Events As
	Audit Success	ss 2/10/2014 1:37:11 PM Microso 4672 SpedalLogon ss 2/10/2014 1:36:43 PM Microso 4634 Logoff	Special Logon	Attach a Tack To this Log		
	Audit Success		Microso	4634 Logoff		Addenta rask to dits cog
	Audit Success	2/10/2014 1:36:43 PM	Microso	4624	Logon	View F
	Audit Success	2/10/2014 1:36:43 PM	Microso	4672	Special Logon	Refrech
	Audit Failure	2/10/2014 1:35:47 PM	Microso	6273	Network Policy Server	Nerresti
	Audit Success	2/10/2014 1:35:47 PM	Microso	4624	L Event Properties	👔 Heip 🕨 🕨
	Audit Success	2/10/2014 1:35:47 PM	Microso	4672	Ktach Task To This Event	
	Audit Success	2/10/2014 1:35:47 PM	Microso	4648	L Copy	Event 6273, Microsoft Win A
	Audit Success	2/10/2014 1:35:47 PM	Microso	4769	K Save Selected Events	Event Properties
	Event 6273, Microsof	ft Windows security auditing			Refresh	💿 Attach Task To This Even
	General Details				Help +	Copy 🕨
	Decails					Save Selected Events
					<u> </u>	CI STATE TO LET TO LA TO

Once you open Event Properties, you should be able to see the reason for failure as shown in the example. In this example, PAP was not chosen as the authentication type under Network policy. Hence, the authentication request fails. Log Name: Security

policy. Herice,	the authenti	cation rec	quest ialis. I	og Name:	Security				
Source:	Microsoft-W	indows-Se	curity-Audit:	ing					
Date:	2/10/2014 1:35:47 PM								
Event ID:	vent ID: 6273								
Task Category:	Task Category: Network Policy Server								
Level:	Information								
Keywords:	Audit Failure								
User:	N/A								
Computer:	win2k8.skp.	COM							
Description:									
Network Policy	Server deni	ed access	to a user.						
Contact the Ne	twork Policy	Server a	dministrator	for more in	nformation.				
User:									
Security ID	:	SKP\vpnu	ser						
Account Name:		vpnuser							
Account Dom	ain:	SKP							
Fully Quali	fied Account	Name:	skp.com/Use:	rs/vpnuser					
Client Machine	:								
Security ID	:	NULL SID							
Account Name	e:	-							
Fully Quali	fied Account	Name:	-						
OS-Version:		-							
Called Stat	ion Identifi	er:	-						
Calling Sta	tion Identif	ier:	-						
NAS:									
NAS IPv4 Ad	dress:	10.105.	130.69						
NAS IPv6 Ad	dress:	-							
NAS Identif	ier:	_							
NAS Port-Ty	pe:	Virtua	1						
NAS Port:	0								
RADIUS Client:									
Client Frie	ndly Name:	vpn							
Client IP A	ddress:	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.