Autenticação de usuário ASA VPN no Windows 2008 NPS Server (Ative Diretory) com exemplo de configuração RADIUS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Diagrama de Rede Configurações Configuração do ASDM Configuração de CLI Windows 2008 Server com configuração de NPS Verificar Depurações do ASA Troubleshoot

Introduction

Este documento explica como configurar um Adaptive Security Appliance (ASA) para se comunicar com um Microsoft Windows 2008 Network Policy Server (NPS) com o protocolo RADIUS para que os usuários legados do Cisco VPN Client/AnyConnect/Clientless WebVPN sejam autenticados no Ative Diretory. O NPS é uma das funções de servidor oferecidas pelo Windows 2008 Server. É equivalente ao Windows 2003 Server, IAS (Internet Authentication Service), que é a implementação de um servidor RADIUS para fornecer autenticação de usuário de discagem remota. Da mesma forma, no Windows 2008 Server, o NPS é a implementação de um servidor RADIUS para um servidor NPS RADIUS. O ASA envia solicitações de autenticação RADIUS em nome de usuários de VPN e o NPS os autentica no Ative Diretory.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA com versão 9.1(4)
- Windows 2008 R2 Server com serviços Ative Diretory e função NPS instalada

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.

Configurar

Note: Use a <u>Command Lookup Tool (somente clientes registrados) para obter mais</u> informações sobre os comandos usados nesta seção.

Diagrama de Rede



Configurações

Configuração do ASDM

- 1. Escolha o grupo de túneis para o qual a autenticação NPS é necessária.
- 2. Clique em Editar e escolha Básico.
- 3. Na seção Autenticação, clique em Gerenciar.

Basic	Name:	TEST	
-Advanced	Aliases:	TEST	
	Authentication		
	Method:	AAA O Certificate Both	\frown
	AAA Server Group:	LOCAL	▼ Manage
		Use LOCAL if Server Group fails	\smile
	Client Address Assignment -		
	DHCP Servers:		
		None O DHCP Link O 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 dien	t protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name: hk.intra	axa	
Find:	O Ne	xt O Previous	
		•	

- 4. Na seção Grupos de servidores AAA, clique em Adicionar.
- 5. No campo AAA Server Group (Grupo de servidores AAA), digite o nome do grupo de servidores (por exemplo, NPS).
- 6. Na lista suspensa Protocolo, escolha 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	ten (1) Tend			
ivers in the Select	ed Group		NEOCONDIGN PROC	. Depier				_
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 F	Hap							68
				- C.	Apply R	teet		

- 8. Na seção Servidores no Grupo selecionado, escolha o Grupo de servidores AAA adicionado e clique em **Adicionar**.
- 9. No campo Nome do servidor ou Endereço IP, insira o endereço IP do servidor.
- 10. No campo Chave secreta do servidor, digite a chave secreta.
- 11. Deixe os campos Server Authentication Port e Server Accounting Port no valor padrão, a menos que o servidor ouça em uma porta diferente.
- 12. Click OK.
- 13. Click
 - OK.

hannad	Name:	TEST				-	G	
Contraction of the second	Alapes:	TEST					Edit AAA Server	and the second se
	Authenticat	on					Server Group:	WPS
onfigure AAA Ser	wer Groups		a contan i	-		22	Interface Name:	inside -
A Server Groups							Server Name or IP Address:	10.105.130.51
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Tree	May Failed Attempts	Add	Timeout:	10 seconds
CAL COULD	LOCAL	necounting rives	INCOLUTION IT TAKE	Dean mile	Har I alco Hildigio		RADIUS Parameters	
8	RADIUS	Single	Depietion	10	3	Edit	Server Authentication Port	1645
						Delete	Server Accounting Port:	1646
Vnd:	001	Match Case					Retry Interval:	10 seconds
rvers in the Select	ted Group				-		server secret key:	
antar Name or 12	Address Interfer	Trend			(Add	Common Password:	
evenane or pr	AUD 035 2100100	e integrat				_	ACL Netmask Convert:	Standard -
0.105.130.51	(rade	10				Edit		-
						Oulute	Plicrosoft CHAPV2 Capable	
						Contra I	SDI Messages	
						Nove Up	Hessage Table	
						Hove Down	Message Name	Message Text
						Hove Down	Message Name ready-for-sys-pin	Message Text ACCEPT A SYSTEM GENERATED PIN
						Hove Down Test	Message Name ready-for-sys-pin new-pin-reenter	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN:
ind:	0 01	Match Case				Hove Down Test	Message Name ready-for-sys-pin new-pin-reenter new-pin-meth	Message Text ACCEPT A S1STEM GENERATED PIN Reenter PIN: Do you want to enter your own pin
ind:	001	Match Case				Hove Down Test	Hessage Name ready-for-sys-pin new-pin-reenter new-pin-meth next-ccode-and-reauth	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code
ind: LDAP Attribute I] © () Hap	Match Case				Hove Down Test	Nessage Name ready-for-sys-pin new-pin-reenter new-pin-meth next-ccode-and-reauth next-ccode	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE
ind: LDAP Attribute N	0 0 1 Hap	Match Case				Nove Down Test	Hessage Name ready-for-sys-pin new-pin-meth next-code-and-reauth next-code new-pin-eys-ok	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE New PIN Accepted
ind: LDAP Attribute N	0 0 I	Match Case	Cance +	telp		Nove Down Test	Hessage Name ready-for-sys-pin new-pin-reenter new-pin-meth next-code and-reauth next-code and-reauth next-code new-pin-sys-ok new-pin-sys-ok	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE Herw PIN Accepted Please remember your new PIN Enter PIN Accepted
ind: LDAP Attribute P	0 0 ! Hap	Match Case	Cancel	telp		Nove Down Test	Hessage Name ready-for-sys-pin new pin-neether new pin-neether new pin-neether new code and-reauth new con-sys-ok new pin-sys-ok new pin-sep	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODIE New PIN Accepted Please remember your new PIN Enter your new Alpha-Akmenical PIN
ind:] © ©] Hap	Match Case	Cancel	telp		Hove Down Test	Hessage Name ready-for-sys-pin new pin-meth new coole-and-reauth next-code new pin-sys-ok new pin-sys-ok new pin-sys-ok new pin-sys-ok new pin-sys-ok new pin-sys-ok	Message Text ACCEPT A SYSTEM GENERATED PID Reenter PIN: Do you want to enter your own pin new PID with the next card code Enter Next PASSCODE Here PID Accepted Please remember your new PID Enter your new Alpha-Humerical PID to make changes.)
ind:	001 Map	Match Case	Cancel +	telp		Hove Down Test	Hessage Name ready-for-sys-pin new-pin-meth new-pin-meth new-code-and-reauth new-pin-sys-ok new-pin-sys-ok new-pin-sys-new Double-dick in a text cell Restor	Message Text ACCEPT A SYSTEM GENERATED PIN Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODI Here PIN Accepted Please remember your new PIN Enter your new Alpha-Akmerical PID to make changes.) e default message texts

- 14. Na lista suspensa Grupo de servidores AAA, escolha o grupo (NPS neste exemplo) adicionado nas etapas anteriores.
- 15. Click

C)	Κ
1	,	N

Basic	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 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 attrib	ute of the group policy selected above.)	
	Enable SSL VPN dier	nt protocol	
	Enable IPsec(IKEv2)	dient protocol	
	DNS Servers: 10.40	.3.10	
	WINS Servers:		
	Domain Name:		
Find:	O Ne	ext Previous	
		· · · · · · · · · · · · · · · · · · ·	

Configuração de CLI

```
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

Por padrão, o ASA usa o tipo de autenticação PAP (Password Authentication Protocol) não criptografado. Isso não significa que o ASA envie a senha em texto simples quando envia o pacote RADIUS REQUEST. Em vez disso, a senha em texto simples é criptografada com o segredo compartilhado RADIUS.

Se o gerenciamento de senha estiver habilitado no grupo de túneis, o ASA usará o tipo de autenticação MSCHAP-v2 para criptografar a senha de texto simples. Nesse caso, verifique se a caixa de seleção **Microsoft CHAPv2 Capable** está marcada na janela Edit AAA Server configurada na seção de configuração do ASDM.

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

Note: O comando **test aaa-server authentication** sempre usa PAP. Somente quando um usuário inicia uma conexão com um grupo de túneis com o gerenciamento de senha habilitado o ASA usa o MSCHAP-v2. Além disso, a opção 'password-management [password-expire-in-days]' só é suportada com o Lightweight Diretory Access Protocol (LDAP). RADIUS não fornece este recurso. Você verá a opção password expire quando a senha já tiver expirado no Ative Diretory.

Windows 2008 Server com configuração de NPS

A função de servidor NPS deve ser instalada e executada no servidor Windows 2008. Caso contrário, escolha **Start > Administrative Tools > Server Roles > Add Role Services**. Escolha o Network Policy Server e instale o software. Depois que a função de servidor NPS for instalada, faça o seguinte para configurar o NPS para aceitar e processar solicitações de autenticação RADIUS do ASA:

 Adicione o ASA como um cliente RADIUS no servidor NPS. Escolha Ferramentas Administrativas > Servidor de Políticas de Rede.Clique com o botão direito do mouse em RADIUS Clients e escolha New.

🞭 Network Policy	Server					<u>_ 8 ×</u>	Mana
File Action View	w Help						Start
💠 🄿 📶	2 🖬						
NPS (Local)		RADIUS Clients					
RADIUS Clients a	and Servers		tente allevenerate	and the sectored and	and the state of the	t any file access to your	$\mathbf{\Sigma}$
Remote RA	New	network.	ients allow you to	specify the network acc	ess servers, that	at provide access to your	-
Policies	Sxport List						
Connection	View +	Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status	
Health Polic	Defrech	Cisco Router	10.105.130.69	RADIUS Standard	No	Enabled	
Network Acces	Refreat						
Accounting	Help						
Templates Manag	gement						
163							**
							(b P
	Elect.	1					2:31 AM
							7/20/2013
Vew Network Access	Device						

Insira um nome amigável, um endereço (IP ou DNS) e um segredo compartilhado configurados no

ASA.

Network Policy Server	Cisco Router Properties	×		Ctart
File Action View Help	Settings Advanced			Jun
		1		
	Enable this RADIUS client			
NPS (Local)	Select as existing template:			
RADIUS Clients and Servers			to your	2
Remote RADIUS Server Group	<u> </u>		to your	
Policies	- Name and Address			
Connection Request Policies	Friendly name:			-D=D
Network Policies	Gaas Paster			
Health Policies	Jusco Router			
Network Access Protection	Address (IP or DNS):			
Accounting	10.105.130.69 Verify			
Templates Management				
	Shared Secret			
	Select an existing Shared Secrets template:			
	None			
	To manually type a shared secret Slick 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:			
	••••			
				**
		_		(h P
	OK Cancel Apply			12:02 414
1 F	P			7/20/2013

Clique na guia Advanced.Na lista suspensa Nome do fornecedor, escolha **RADIUS Standard**.Click **OK**.

NPS (Local)	RADIUS Clients	New RADIUS Client
RADIUS Clients and Servers 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: Image: Client standard RADIUS Standard Image: Client standard Additional Options Image: Access-Request messages must contain the Message-Authenticator attribute RADIUS client is NAP-capable Image: Client is NAP-capable DK Cancel

2. Crie uma nova Política de Solicitação de Conexão para usuários de VPN. A finalidade da Política de Solicitação de Conexão é especificar se as solicitações de clientes RADIUS devem ser processadas localmente ou encaminhadas para servidores RADIUS remotos. Em NPS > Policies, clique com o botão direito do mouse em Connection Request Policies e crie uma nova política.Na lista suspensa Tipo de servidor de acesso à rede, escolha Não especificado.

Network	test Properties	Start
File Actio	Overview Construct Service	
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	In enabled, hit o evaluates the policy while processing connection requests. In deabled, hit o does not evalue the policy.	
Conr	Policy enabled	
Heal		- 👽
Network	Network connection method	
Accounti	type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access po	in
Template	select Unspecified.	
	Type of network access server;	
	C Vendor specific:	
	10 🔶	
		-
		**
		de Do
		12:08 44
•		7/20/2013
	OK Cancel	/

Clique na guia **Condições**.Clique em Add.Digite o endereço IP do ASA como uma condição 'Endereço IPv4 do cliente'.

Network	alter Comme	
Ella Actio	test Properties	Start
	Overview Conditions Settings	3
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.	$\mathbf{\Sigma}$
Policies		
Conr	Condition Value	
📔 Netv	Client IPv4 Address 10.105.130.69	
📔 Heal		
Network		
Accounti		
Template		
	Condition description;	
	The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
	Add Edit Remov	
2		10 P
		12:08 AM
•		7/20/2013
	OK Cancel ,	

Clique na guia **Configurações**.Em Forwarding Connection Request, escolha **Authentication**. Verifique se o botão de opção Autenticar solicitações neste servidor está selecionado.Click **OK**.



3. Adicione uma política de rede onde você possa especificar quais usuários têm permissão para autenticar.Por exemplo, você pode adicionar grupos de usuários do Ative Diretory como uma condição. Apenas os usuários que pertencem a um grupo especificado do Windows são autenticados sob esta política.Em NPS, escolha Polícies.Clique com o botão direito do mouse em Política de rede e crie uma nova política.Verifique se o botão de opção Conceder acesso está selecionado.Na lista suspensa Tipo de servidor de acesso à rede, escolha Não especificado.

	X
Overview Conditions Constraints Settings	
Policy name: Itest	
- Dila Data	
If enabled, NPS evaluates this policy while performing authorization. If d	lisabled, NPS does not evaluate this policy.
I Policy enabled	
Access Permission	
If conditions and constraints of the network policy match the connect	tion request, the policy can either grant access or deny
access. what is access permission?	
G Grant appears Grant appears if the connection rap and matches this a	adies.
G D D D C D C C C C C C C C C C C C C C	concy.
 Deny access. Deny access if the connection request matches this p 	oicy.
I Ignore user account dial-in properties.	tion to the set of the
authorization with network policy only; do not evaluate the dial-in pro-	perties of user accounts .
Network connection method	
Select the type of network access server that sends the connection rec	juest to NPS. You can select either the network access server type
or Vendor specific, but neither is required. If your network access serve select Unspecified.	ar is an 802.1X authenticating switch or wireless access point,
Type of network access server:	
Unspecified	
C Vendor specific:	
C Vendor specific:	

Clique na guia **Condições**.Clique em Add.Insira o endereço IP do ASA como condição de endereço IPv4 do cliente.Insira o grupo de usuários do Ative Diretory que contém usuários de

VPN.

if co	nditions match the conne tection request NPS skir	ction request, NPS uses this policy to authorize the connection request. If	conditions do not match the	
	action respects, in a sep	a na poroj a la craduce con poroce, a dadevita poroce de coniga		
	Condition	Value		
12	User Groups	SKP\VPN		
	Client IPv4 Address	10.105.130.69		
Conc	lition description: Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the conne	ection request to NPS.	

Clique na guia **Restrições**.Escolha **Métodos de Autenticação**.Verifique se a caixa de seleção Autenticação não criptografada (PAP, SPAP) está marcada.Click **OK**.

Overvew Conditions Constraints Constraints are not matched by the connection request, network access is denied. Constraints: Constraints Authentication Methods Image: Colled Station ID Image: Cole Colled	Operational Constraints I Constraints I Constraints		N 5
Constraints: Constraints Allow access only to those clents that authenticate with the specified methods. Authentication Methods EAP types are negotiated between NPS and the client in the order in which they are lated. Called Station ID Day and time restrictions Table NAS Port Type Move Up Move Down Move Down Add Edit Bemove Less secure authentication methods: Microsoft Encrypted Authentication (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (PAP, SPAP) Allow clents to connect without negotiating an authentication method Perform machine heath check only	Configure the constraints for this network if all constraints are not matched by the o	tings : policy, connection request, network access is denied.	
Authentication Methods Image: Session Timeout Session Timeout Called Station ID Day and time restrictions NAS Port Type Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication (MS-CHAP-v2) Image: User can change password after it has expired Microsoft Encrypted authentication (CHAP) User can change password after it has expired Image: Change password after it has expired Im	Constraints:		_ 4
Idle Timeout Session Timeout Called Station ID Day and time restrictions NAS Port Type Add Edit Bemove Less secure authentication methods: Microsoft Encrypted Authentication (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (CHAP) User can change password after it has expired Microsoft Encrypted authentication (CHAP) User can change password after it has expired Microsoft Encrypted authentication (CHAP) User can change password after it has expired Allow clients to connect without negotisting an authentication method Perform machine health check only	Authentication Methods	Allow access only to those clients that authenticate with the specified methods.	6
Called Station D Pay and time restrictions NAS Port Type Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) Ver User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) Ver User can change password after it has expired Encrypted authentication (MS-CHAP) Ver User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) Ver User can change password after it has expired How clients to connect without negotiating an authentication method Perform machine health check only	Session Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:	_
Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) Image: Wear can change password after it has expired Image: Microsoft Encrypted Authentication (MS-CHAP) Image: Wear can change password after it has expired Image: Microsoft Encrypted Authentication (MS-CHAP) Image: Wear can change password after it has expired Image: Microsoft Encrypted authentication (MS-CHAP) Image: Wear can change password after it has expired Image: Microsoft Encrypted authentication (MS-CHAP) Image: Wear can change password after it has expired Image: Microsoft Encrypted authentication (CHAP) Image: Wear can change password after it has expired Image: Microsoft Encrypted authentication (PAP, SPAP) Image: Microsoft Encrypted Authentication (PAP	Day and time restrictions NAS Port Type	Move Up Move Down	
Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Unencrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only		Add Edit Remove	
 ✓ User can change password after it has expired ✓ 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 		Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)	
Vincosot Enclypted Admentication (NISCHAP) Viscosot Enclypted Admentication (CHAP) Viscosot Enclypted authentication (CHAP) Vincosot Enclypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only		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		User can change password after it has expired	
Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only		Encrypted authentication (CHAP)	
Perform machine health check only		Unencrypted authentication (PAP, SPAP)	
α		Perform machine health check only	_
			**
			12.

Pass Group-policy Attribute (Atributo 25) do Servidor NPS RADIUS

Se a política de grupo precisar ser atribuída ao usuário dinamicamente com o servidor NPS RADIUS, o atributo RADIUS da política de grupo (atributo 25) poderá ser usado.

Conclua estes passos para enviar o atributo RADIUS 25 para atribuição dinâmica de uma política de grupo ao usuário.

 Depois que a Diretiva de rede for adicionada, clique com o botão direito do mouse na Diretiva de rede necessária e clique na guia Configurações.



2. Escolha **Atributos RADIUS > Padrão**. Clique em Add. Deixe o tipo de acesso como Todos.

10000	
Network Policy Server	
File Action Vi	A
Image: Settings Overview Conditions Constraints Settings Image: Settings Image: Setting	and the policy grants access, settings are applied.
Remot BADIUS Attributes	Add Standard RADIUS Attribute
Conne Standard To tend ad	fion 1 To add en attribute to the settings, select the attribute, and then click Add.
Contraction Specific Jour RADIU	S di To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click
🗷 🌺 Network A Network Access Protection	Add
Accountin: NAP Enforcement Attributes:	Access type
Extended State Name	
Routing and Remote Access FramedPr	doc Ambutes:
Multiink and Bandwidth Service-Ty Alexander Default (240)	Name A
The store of the s	AppHrterinHinterval
	Class
- Entryption	FilerId
and the sounds	Framed AppleTak-Link
Add	Epimed Anniel Sk. Zava
	Description
	Specifies the length of the interval (in seconds) between each interim update that the NAS sends.
	AddClass
	OK Cencel Apply

3. Na caixa Atributos, escolha Classe e clique em Adicionar. Digite o valor do atributo, ou seja, o nome da política de grupo como uma string. Lembre-se de que uma política de grupo com esse nome deve ser configurada no ASA. Isso significa que o ASA o atribui à sessão VPN após receber esse atributo na resposta RADIUS.

Network Policy Server		
File Action V	(s)	
NPS (Local) Contigue the settings for this network policy		
RADIUS CI Conditions and constraints match the com	lection request and 0	the poncy grants access, saturigs are appred.
Remot BADIUS Attributes	Transfertier	Add Standard RADIUS Attribute
Conne Standard	then click Edit. I	To add an attribute to the settings, select the attribute, and then click Add
Health Zendor Specific	yeur radius ei	To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.
Ketwork A Network Access tolection		Access type:
E Templates State	Attributes	A
Routing and Remote Access	Framed-Protoc	Albènter
Multink and Bandwidth	Service-Type	Name
P files		AccHinterim Interval
🔒 Encryption		
🚜 IP Sellings		Frened-AppleTalk-Link
	Add	Frened-AppleT dik-Network EgenerationaleT dik-Zene
		Description:
		Specifies the diastification of accounting records
<		Att Dree
		DK Cancel Apply
SiNetwork Policy Server		
File Action Vi	1	×
Byetyeek Conditions Constraints Setting	25	
RADIUS (I Contigue the sattings to this network policy Reptus (I Contigue the sattings to this network policy If conditions and constraints match the contigue	nection request and (the policy grants access, settings are applied.
RADU Settings		Add Standard RADIUS Attribute
Policies RADIUS Attributes	To send addition from click Exit 1	To add an attribute to the settings, select the attribute, and then click Add.
Netwo	your RADIUS cli	To add a custom or predefined Vendor Specific Attribute, close this dialog and select Vendor Specific, and then click
E S Retwork A Network Access Projection		Add Attribute Information
Accountin; SAP Enforcement	Athibutes:	Access upe: Ambute name:
Extended State	Name	Antibute number
A Multink and Bandwidth	Service-Type	Alliquiss 20
Allocation Protocol (BAP)		Acchine interve OctetString
Encryption		Class Enter the attribute value in:
🚜 IP Sellings		Fiter-Id 🕞 String
	Add	Fremed-AppleTak-
		lect 1
		Description
		N OK Caned
		Specifies the classific
×1		Specifies the classific
<u>×1</u>		Specifies the classific Cancel Add Close

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Depurações do ASA

Ative debug radius all no 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: 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)..... |A.....~m.... 01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 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 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
                                             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) = 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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Verifique se a conectividade entre o ASA e o servidor NPS está boa.Aplique capturas de pacotes para garantir que a solicitação de autenticação saia da interface ASA (de onde o servidor pode ser alcançado). Confirme se os dispositivos no caminho não bloqueiam a porta UDP 1645 (porta de autenticação RADIUS padrão) para garantir que ela chegue ao servidor NPS. Mais informações sobre capturas de pacotes no ASA podem ser encontradas no <u>ASA/PIX/FWSM: Exemplo de Captura de Pacotes usando CLI e ASDM Configuration</u>.
- Se a autenticação ainda falhar, verifique o visualizador de eventos no NPS do Windows. Em Visualizador de Eventos > Logs do Windows, escolha Segurança. Procure eventos associados ao NPS por volta da hora da solicitação de autenticação.

File Action View Help								
Event Viewer (Local)	Security Number of	f events: 93 (!) New events ave	ilable				Actions	•
E S Windows Logs	Keywords	Date and Time	Source	Event 3D	Task Category		Security	-
Application	Audit Success	2/10/2014 1:37:43 PM	Microso	4634	Logoff		open Saved Log	
Security	Audit Success	2/10/2014 1:37:43 PM	Microso	4624	Logon	- 11	Tranto Custon Bour	
Setup	Audit Success	2/10/2014 1:37:43 PM	Microso	4672	Special Logon	- 11	Y Create Custom Rev	
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 Policy Server		Clear Lon	
Applications and Services Logs	Audit Success	2/10/2014 1:37:28 PM	Microso	4634	Logoff			
Subscriptions	Audit Success	2/10/2014 1:37:28 PM	Microso	4624	Logon		Pilter Current Log	
	Audit Success	2/10/2014 1:37:28 PM	Microso	4648	Logon		Properties	
	Audit Success	2/10/2014 1:37:28 PM	Microso	4776	Credential Validation		.00 mil	
	Audit Success	2/10/2014 1:37:24 PM	Microso	4634	Logoff		Hind	
	Audit Success	2/10/2014 1:37:11 PM	Microso	4624	Logon		Save All Events As	
	Audit Success	2/10/2014 1:37:11 PM	Microso	4672	Special Logon		Attach a Tack To this Is	
	Audit Success	2/10/2014 1:36:43 PM	Microso	4634	Logoff			
	Audit Success	2/10/2014 1:36:43 PM	Microso	4624	Logon		View	•
	Audit Success	2/10/2014 1:36:43 PM	Microso	4672	Special Logon		Refresh	
	Audit Failure	2/10/2014 1:35:47 PM	Microso	6273	Natwork Policy Server	. 11		
	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	Attach Task To This Event			
	Audit Success	2/10/2014 1:35:47 PM	Microso	4648	L Copy		Event 6273, Microsoft Wi	m 🔺
	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 Eve	
	General Details				Help +		Сору	
						-	Save Selected Events	£

Depois de abrir as Propriedades do evento, você poderá ver o motivo da falha, como mostrado no exemplo. Neste exemplo, PAP não foi escolhido como o tipo de autenticação na política de rede. Portanto, a solicitação de autenticação falha.

```
Log Name: Security
Source: Microsoft-Windows-Security-Auditing
            2/10/2014 1:35:47 PM
Date:
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 Network Policy Server administrator for more information.
User:
  Security ID:
                       SKP\vpnuser
  Account Name:
                        vpnuser
  Account Domain:
                         SKP
  Fully Qualified Account Name: skp.com/Users/vpnuser
Client Machine:
  Security ID:
                       NULL SID
  Account Name:
                        _
  Fully Qualified Account Name:
  OS-Version:
                       _
  Called Station Identifier:
  Calling Station Identifier:
NAS:
  NAS IPv4 Address:
                        10.105.130.69
  NAS IPv6 Address:
                         _
  NAS Identifier:
  NAS Port-Type:
NAS Port:
                         Virtual
                    0
RADIUS Client:
  Client Friendly Name:
                             vpn
  Client IP Address:
                             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.