Esempio di autenticazione utente VPN ASA su server dei criteri di rete Windows 2008 (Active Directory) con configurazione RADIUS

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Configurazioni Configurazione ASDM Configurazione CLI Windows 2008 Server con configurazione Server dei criteri di rete Verifica Debug dell'ASA Risoluzione dei problemi

Introduzione

In questo documento viene spiegato come configurare un'appliance ASA (Adaptive Security Appliance) per comunicare con un server dei criteri di rete (NPS) di Microsoft Windows 2008 tramite il protocollo RADIUS in modo che gli utenti Cisco VPN Client/AnyConnect/WebVPN senza client legacy vengano autenticati in Active Directory. Server dei criteri di rete è uno dei ruoli server offerti da Windows 2008 Server. Equivale a Windows 2003 Server, IAS (Internet Authentication Service), ovvero all'implementazione di un server RADIUS per l'autenticazione remota degli utenti connessi tramite connessione remota. Analogamente, in Windows 2008 Server dei criteri di rete è l'implementazione di un server RADIUS. In pratica, l'appliance ASA è un client RADIUS collegato a un server RADIUS Server dei criteri di rete. ASA invia richieste di autenticazione RADIUS per conto di utenti VPN e Server dei criteri di rete le autentica in Active Directory.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA con versione 9.1(4)
- Server Windows 2008 R2 con i servizi Active Directory e il ruolo Server dei criteri di rete installati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento</u> <u>di ricerca dei comandi (solo utenti registrati).</u>

Esempio di rete



Configurazioni

Configurazione ASDM

- 1. Scegliere il gruppo di tunnel per il quale è richiesta l'autenticazione di Server dei criteri di rete.
- 2. Fare clic su Modifica e scegliere Base.
- 3. Nella sezione Autenticazione fare clic su **Gestisci**.

ation rver Group: ress Assignment ervers: ddress Pools:	TEST AAA Certificate Both LOCAL Use LOCAL if Server Group fails Use LOCAL if Server Group fails One DHCP Link DHCP Subnet	Manage
ation ver Group: ress Assignment ervers: ddress Pools:	AAA Certificate Both LOCAL Use LOCAL if Server Group fails None DHCP Link DHCP Subnet	Manage
: rver Group: ress Assignment ervers: ddress Pools:	AAA Certificate Both LOCAL Use LOCAL if Server Group fails None DHCP Link DHCP Subnet	Manage
rver Group: ress Assignment ervers: ddress Pools:	LOCAL Use LOCAL if Server Group fails One ODHCP Link ODHCP Subnet	Manage
ress Assignment ervers: ddress Pools:	Use LOCAL if Server Group fails None O DHCP Link O DHCP Subnet	
ress Assignment ervers: ddress Pools:	None DHCP Link DHCP Subnet	
ervers: ddress Pools:	None DHCP Link DHCP Subnet	
ddrees Pools:	None OHCP Link OHCP Subnet	
ddress Pools		
dureas roots.	test	Select
v6 Address Pool		Select
	IPv6 address pool is only supported for SSL.	
oup Policy		
olicy:	DfltGrpPolicy	✓ Manage
ng field is an attri	bute of the group policy selected above.)	
nable SSL VPN die	ent protocol	
nable IPsec(IKEv	2) client protocol	
Servers: 10.4	0.3.10	
Servers:		
our reror		
	v6 Address Pools oup Policy olicy: ng field is an attril nable SSL VPN clie nable IPsec(IKEv2 servers: 10.40	IPv6 address pool is only supported for SSL. oup Policy olicy: DfltGrpPolicy ng field is an attribute of the group policy selected above.) nable SSL VPN client protocol nable IPsec(IKEv2) client protocol ervers: 10.40.3.10

- 4. Nella sezione Gruppi di server AAA, fare clic su Aggiungi.
- 5. Nel campo Gruppo server AAA immettere il nome del gruppo di server (ad esempio, Server dei criteri di rete).
- 6. Dall'elenco a discesa Protocollo, scegliere RADIUS.
- 7. Fare clic su OK.

								-
rver Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts			Add
CAL	LOCAL							Edit
			Add AAA Serve	r Group				Delete
			AAA Server Group: Protocol:	NFS RADOUS	•			
ndt	00	Match Case	Accounting Node:	O Smult	meous 🕘 Single			
vers in the Selec	ted Graup		Reactivation Modes	Depiet	ion 💮 Timed			
rver Name or IP	Address Interfac	re Timeout	Dead Titse:	10 =	inutes			Add
			Max Failed Attempt	s: 3				Edit
			🖻 Onable interim a	eccounting up	date			Delete
			E trable Active D	krectory Agen	nt mode			Move Up
			VPII 3K Compati	bility Option		8		Move Down
			ОК		noel Help			Test
				-				
nde	00	Match Case						
DAP Attribute	Нар							(8
				-				

- 8. Nella sezione Server del gruppo selezionato, scegliere il gruppo di server AAA aggiunto e fare clic su **Aggiungi**.
- 9. Nel campo Nome server o Indirizzo IP immettere l'indirizzo IP del server.
- 10. Nel campo Chiave privata server immettere la chiave segreta.
- 11. Lasciare i campi Porta di autenticazione server e Porta accounting server sul valore predefinito a meno che il server non sia in ascolto su una porta diversa.
- 12. Fare clic su OK.
- 13. Fare clic su
 - OK.

dvanced	Name:	TEST				ń	Edit AAA Server	
	Alapes:	161						
	Authenticatio	an					Server Group:	insida
onfigure AAA Se	rver Groups						Street and the second second	in the second
AA Server Groups							Server Name or IP Address:	10.105.130.51
	Destand	A converting Marcia	Parasthustics Made	David Tree	Max Railed Messale	Add	Timeout:	10 seconds
verver Group	Protocol	Accounting Ploate	Reactivation Plode	Lead time	Max Falled Attempts		RACE IS Parameters	
AA.	RADUS	Sinde	Depletion	10	1	Edit	Carvar Authantication Dout	1646
	- Internet					Delete	Server source and and the o	
	10.0						Server Accounting Port:	1646
ind:	0 0 1	Match Case					Retry Interval:	30 seconds •
							Server Secret Key:	
rvers in the Select	ted Group				/		Commun Damanut	
erver Name or IP	Address Interfac	e Timeout			(Add	Lonmon Passwore:	
0.105.130.51	route	10					ACL Netmask Convert:	Standard -
	Je bros					Edt	Microsoft CHAPv2 Capable	: [7]
					6	Delete		
							SDI Messages	
						Move Up	Message Table	(
						Hove Down	Message Name	Message Text
					-		ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN
						Test		
					h	Test	new-pin-reenter	Reenter PIN:
ind:	0 01	Match Case			la	Test	new-pin-reenter new-pin-meth	Reenter PIN: Do you want to enter your own pin
ind:	0 0 z	Match Case] i	Test	new-pin-reenter new-pin-meth next-coode-and-reauth	Reenter PIN: Do you want to enter your own pin new PIN with the next card code
ind: DAP Attribute I) © () [Hap	Match Case			1	Test	new-pin-reenter new-pin-meth next-coole-and-reauth next-code	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE News EN Accepted
ind: LDAP Attribute I	0 0 I Hap	Match Case] li	Test	new-pin-reenter new-pin-meth next-ccode-and-reauth next-ccode new-pin-sys-ok	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE New PIN Accepted Blasse semantics war new PIN
ind: DAP Attribute I	0 0 I Map	Match Case	Cancel	Help] is	Test	new-pin-reenter new pin-meth next-coole-and-reauth next-coole new-pin-eyp-ok new-pin-eyp new-pin-eyp	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE New PIN Accepted Please remember your new PIN Enter your new PIN
ind: DAP Attribute I) O O I Map	Match Case	Cancel	Help]		Test	new pin-reenter new pin-meth next-code and-reauth next-code new pin-sys-ok new pin-sys-ok new pin-sep	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE New PIN Accepted Please remember your new PIN Enter your new Apha-Numerical PID
ind: DAP Attribute I	Map	Match Case	Canod	Help		Test	new pin-mether new pin-meth new coole and-reauth new coin-arp-ok new pin-arp-ok new pin-arp new pin-req (Double-dick in a text cel	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCOOL New PIN Accepted Please ensember your new PIN Enter your new Alpha-Numerical PIP to make changes.)
nd: DAP Attribute I) © © E Hap	Match Case	Cancel	Help] i	Test	new pin-reenter new pin-meth next-code-and-reauth new-code-and-reauth new pin-app new pin-app new pin-req (Double-dick in a text cel Restor	Reenter PIN: Do you want to enter your own pin new PIN with the next card code Enter Next PASSCODE Here PIN Accepted Please remember your new PDN Enter your new Alpha-Numerical PID to make changes.) e default message texts

- 14. Dall'elenco a discesa Gruppo server AAA, scegliere il gruppo (Server dei criteri di rete in questo esempio) aggiunto nei passaggi precedenti.
- 15. Fare clic su

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 attribution	ute of the group policy selected above.)	
	Enable SSL VPN clien	it protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name:		
Find:	Ne	xt Previous	

Configurazione 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

Per impostazione predefinita, l'ASA usa il tipo di autenticazione PAP (Password Authentication Protocol) non crittografato. Ciò non significa che l'ASA invii la password in testo normale quando invia il pacchetto RADIUS REQUEST. Al contrario, la password in testo normale viene crittografata con il segreto condiviso RADIUS.

Se la gestione delle password è abilitata nel gruppo di tunnel, l'appliance ASA usa il tipo di autenticazione MSCHAP-v2 per crittografare la password in testo normale. In tal caso, verificare che la casella di controllo **Funzionalità CHAPv2 Microsoft** sia selezionata nella finestra Modifica server AAA configurata nella sezione Configurazione ASDM.

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

Nota: Il comando **test aaa-server authentication** utilizza sempre il protocollo PAP. Solo quando un utente avvia una connessione a un gruppo di tunnel con gestione password abilitata, l'ASA utilizza MSCHAP-v2. Inoltre, l'opzione 'gestione password [giorni di scadenza password]' è supportata solo con il protocollo LDAP (Lightweight Directory Access Protocol). RADIUS non fornisce questa funzione. L'opzione relativa alla scadenza della password verrà visualizzata quando la password è già scaduta in Active Directory.

Windows 2008 Server con configurazione Server dei criteri di rete

Il ruolo Server dei criteri di rete deve essere installato e in esecuzione nel server Windows 2008. In caso contrario, scegliere **Start > Strumenti di amministrazione > Ruoli server > Aggiungi servizi ruolo**. Scegliere Server dei criteri di rete e installare il software. Una volta installato il ruolo Server dei criteri di rete, completare la procedura seguente per configurare il Server dei criteri di rete per accettare ed elaborare le richieste di autenticazione RADIUS dall'appliance ASA:

 Aggiungere l'appliance ASA come client RADIUS nel Server dei criteri di rete. Scegliere Strumenti di amministrazione > Server dei criteri di rete. Fare clic con il pulsante destro del mouse su Client RADIUS e scegliere Nuovo.

🞭 Network Policy	Server					<u>_ 8 ×</u>	
File Action View	w Help						Start
💠 🔿 🔁 📅	2 🖬						
NPS (Local)		RADIUS Clients					
RADIUS Clients : RADIUS Clients : Remote RA	New	RADIUS cl network.	ients allow you to	specify the network acc	cess servers, that	t provide access to your	
Policies	15xport List	-					
Connection	View 🕨	Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status	
Health Polic	Refresh	Cisco Router	10.105.130.69	RADIUS Standard	No	Enabled	
Network Acces Accounting	Help						
							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
							() P
	15.1	1					2:31 AM
							7/20/2013
New Network Access	Device						

Immettere un nome descrittivo, un indirizzo (IP o DNS) e un segreto condiviso configurati sull'appliance

ASA.

Network Policy Server	Cisco Router Properties	× -	
File Action View Help	Settinger   Advanced		start
	Settings   Advanced		1
	Enable this RADIUS client		
NPS (Local)			
RADIUS Clients and Servers	Select an existing template:		
RADIUS Clients	V	to your	
Remote RADIUS Server Group			
Polices	Name and Address		
Network Policies	Friendly name:		
Health Policies	Cisco Router		
Network Access Protection	Address (ID DNIC).		
Accounting	Address (IP of DNS):		
Templates Management	10.105.130.69		
	Shared Secret		
	Select an existing Shared Secrets template:		
	None		
	Indie		
	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:		
			**
	OK Cancel Apply		12:02 AM
1	<u> </u>		7/20/2013

Fare clic sulla scheda **Avanzate**.Dall'elenco a discesa Nome fornitore scegliere **RADIUS Standard**.Fare clic su **OK**.

RADIUS Clients and Servers       RADIUS Clients and Servers         RADIUS Clients       Remote RADIUS Server G         Policies       Policies         Network Access Protection       Friendly Name         Friendly Name       Friendly Name         Policies       Vendor         Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.         Vendor name:         RADIUS Standard	NPS (Local)	RADIUS Clients	New RADIUS Client	x
Additional Options Access-Request messages must contain the Message-Authenticator attribute RADIUS client is NAP-capable OK Cancel	<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: Provide the RADIUS Standard         Image: RADIUS Standard       Image: Provide the RADIUS Standard         Image: RADIUS Standard       Image: Provide the RADIUS Standard         Image: RADIUS Standard       Image: Provide the RADIUS Standard         Image: RADIUS Client is NAP-capable       Image: Provide the RADIUS client is NAP-capable         Image: OK       Cancel	

2. Crea un nuovo criterio di richiesta di connessione per gli utenti VPN. Lo scopo del criterio di richiesta di connessione è specificare se le richieste dei client RADIUS devono essere elaborate localmente o inoltrate ai server RADIUS remoti. In Server dei criteri di rete > Criteri fare clic con il pulsante destro del mouse su Criteri di richiesta di connessione e creare un nuovo criterio.Dall'elenco a discesa Tipo di server di accesso alla rete scegliere Non specificato.

🤣 Network	test Properties	Start
File Actio	Quanting los must be must	
	Conditions Settings	
NPS (Local)	Policy name: test	
RADIUS		$\sum$
RAD	Policy State	_
Policies	ir enabled, NFS evaluates this policy while processing connection requests. It disabled, NFS does not evalue this policy.	
Conr	✓ Policy enabled	
Netv Heal		-   👀
Network	Network connection method	
Accounti	Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access poly	n
🛒 Templati	select Unspecified.	
	C Type of network access server	
	C Vendor specific:	
	10	
		-
		**
		10 P
1		12:08 AM
	OK Cancel	12012013

Fare clic sulla scheda **Condizioni**.Fare clic su **Add**.Immettere l'indirizzo IP dell'ASA come condizione 'Indirizzo IPv4 client'.

a N	letwork	Deline Courses		alvi	
File	Actio	test Properties		A	Start
	AC00	Overview Conditions Settings	rk policy.	-[	1
	RADIUS RADIUS RAD	If conditions match the connection red connection request, NPS skips this po	uest, NPS uses this policy to authorize the connection request. If conditions do not match the licy and evaluates other policies, if additional policies are configured.	e	2
E	Policies				
	Conr	Condition Valu			
	Netv	Client IPv4 Address 10.1	05.130.69		
	Network				
2	Accounti				
4	Template				
			R. C.		
			- 0		
		Condition description:			
		The Client IP Address condition specif	ies the IP address of the RADIUS client that forwarded the connection request to NPS.		
			Add Edit	Remov .	x
				4	200
•					2:08 AM
			OK Cancel		2072013

Fare clic sulla scheda **Impostazioni**. In Inoltro richiesta di connessione scegliere **Autenticazione**. Accertarsi che il pulsante di opzione Autentica richieste sul server sia selezionato. Fare clic su **OK**.



3. Aggiungere un criterio di rete in cui è possibile specificare gli utenti autorizzati all'autenticazione.Èad esempio possibile aggiungere gruppi di utenti di Active Directory come condizione. Solo gli utenti che appartengono a un gruppo di Windows specificato vengono autenticati in base a questo criterio.In Server dei criteri di rete scegliere Criteri.Fare clic con il pulsante destro del mouse su Criteri di rete e creare un nuovo criterio.Assicurarsi che sia selezionato il pulsante di opzione Concedi accesso.Dall'elenco a discesa Tipo di server di accesso alla rete scegliere Non specificato.

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	
-	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:	
	Unspeched	
(	Vendor specific:	**
	10 🚔	1
		- 12:1

Fare clic sulla scheda **Condizioni**.Fare clic su **Add**.Immettere l'indirizzo IP dell'ASA come condizione dell'indirizzo IPv4 del client.Immettere il gruppo di utenti di Active Directory che contiene gli utenti

VPN.

wen	view Cohilitions Const	traints Settings			
Con	figure the conditions for th	his network policy.			
lf con	anditions match the conne nection request, NPS skip	ection request, NPS uses this policy to authorize the connection ps this policy and evaluates other policies, if additional policies a	request. If condition re configured.	ons do not match th	e
_					
400	Condition	Value			
15	Giser Groups	SKP\VPN			_
-3	Client IPV4 Address	10.103.130.63			
Con	dition description: Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded	the connection re	quest to NPS.	
Con	dition description: Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded	I the connection re Add	quest to NPS.	Remove
Con	dition description: : Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded	I the connection re Add	quest to NPS.	Remove

Fare clic sulla scheda **Vincoli**.Scegliere **Metodi di autenticazione**.Assicurarsi che la casella di controllo Autenticazione non crittografata (PAP, SPAP) sia selezionata.Fare clic su **OK**.

Configure the constraints for this network policy.         F all constraints are not matched by the connection request, network access is denied.         Constraints:         Constraints         Authentication Methods         Image:	Overview Conditions Constraints Se	Hinns	175
Constraints         Authentication Methods         Image: Called Station ID	Configure the constraints for this network If all constraints are not matched by the	connection request, network access is denied.	
Idle Timeout   Session Timeout   Called Station ID   Day and time restrictions   NAS Port Type     Add   Edt.   Bemove   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   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   How cients to connect without negotisting an authentication method   Perform machine health check only	Constraints Constraints Authentication Methods	Allow access only to those clients that authenticate with the specified methods.	
Called Station ID   Pay and time restrictions   Image: NAS Port Type     Add     Edit     Remove     Less secure authentication methods:     Image: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)   Image: Microsoft Encrypted Authentication (MS-CHAP)   Image: Microsoft Encrypted authentication (CHAP)   Image: Microsoft Encrypted authentication (PAP, SPAP)   Image: Microsoft Encrypted Authenticati	Idle Timeout     Session Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:	
Add       Edt       Remove         Less secure authentication methods: <ul> <li>Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)</li> <li>User can change password after it has expired</li> <li>Microsoft Encrypted Authentication (MS-CHAP)</li> <li>User can change password after it has expired</li> <li>Encrypted authentication (CHAP)</li> <li>Unencrypted authentication (PAP, SPAP)</li> <li>Allow clients to connect without negotiating an authentication method</li> <li>Perform machine health check only</li> <li>Image: Second Second</li></ul>	Day and time restrictions     NAS Port Type	Move Up Move Down	
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) 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     Encrypted authentication (CHAP)     Unencrypted authentication (PAP, SPAP)     Allow clients to connect without negotiating an authentication method     Perform machine health check only		Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)     User can change password after it has expired     Microsoft Encrypted Authentication (MS-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 Encrypted authentication (CHAP)	
		Unencrypted authentication (FAP, SPAP)     Allow clients to connect without negotiating an authentication method     Perform machine health check only	
		OK Cancel App	12: y 7/2

#### Passa l'attributo Criteri di gruppo (attributo 25) dal server RADIUS Server dei criteri di rete

Se il criterio di gruppo deve essere assegnato dinamicamente all'utente con il server RADIUS Server dei criteri di rete, è possibile utilizzare l'attributo RADIUS del criterio di gruppo (attributo 25).

Completare questa procedura per inviare l'attributo RADIUS 25 per l'assegnazione dinamica di un criterio di gruppo all'utente.

 Dopo aver aggiunto il criterio di rete, fare clic con il pulsante destro del mouse sul criterio di rete desiderato e scegliere la scheda Impostazioni.



2. Scegliete Attributi RADIUS > Standard. Fare clic su Add. Lasciare il tipo di accesso Tutto.

🚯 Network Polic <u>y Server</u>	
File Action Vi test Properties	<u>×</u>
👍 🖦 👘 👾 Överview Conditions Constraints Settings	
RADUS C     R	d the policy grants access, settings are applied.
Remet Settings	Add Standard RADIUS Attribute
E Policies RADIUS Altributes To cend addition	²⁷ To add as with the to the collision calculates with a width or with 6.44
Conne Standard then click Edit	I a sas en atribute to the terango, telect the atribute, and then block Acts.
Health Z Vendor Specific	To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click
🕞 💺 Network A Network Access Protection	Ada
Accounting NAP Enforcement	Access type
🗄 🛃 Templates 🦉 🐴 Christeenen 🖉 Attributes:	Al Contractor and a second sec
19 Extended State Name	
Routing and Remote Access FramedProt	Ambutes:
Multilink and Bandwidth Service-Type	Name 🔺
Allocation Protocol (SAP)	ApptVintermInterval
TP Files	Calback-Number
🔒 Encryption	Cless
- IP Settings	Filer-Id
44 · · · · · · · · · · · · · · · · · ·	Transdopperaktink
Add	France Appendix Appendix
	4 () ·
	Description
	Specifies the length of the interval (in seconds) between each interim update that the NAS sends
<b>•</b>	
	Add. Dore
	OK Cencel Apply

 Nella casella Attributi, scegliere Classe, quindi fare clic su Aggiungi. Immettere il valore dell'attributo, ovvero il nome del criterio di gruppo come stringa. Tenere presente che i criteri di gruppo con questo nome devono essere configurati nell'appliance ASA. In questo modo, l'ASA la assegna alla sessione VPN dopo aver ricevuto l'attributo nella risposta 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 distalication 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	Attributes:	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

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Nota: consultare le <u>informazioni importanti sui comandi di debug prima di usare i comandi di</u> debug.

### Debug dell'ASA

Abilitare il raggio di debug su tutte le appliance 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).....
01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f
                                              | ...A....~m...
40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28
                                                @P.6..vpnuser..(
c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04
                                               | .h.....Z.oC.
06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00
                                               ..i...=...
05
                                                | .
Parsed packet data....
Radius: Code = 1 (0x01)
Radius: Identifier = 8 (0x08)
Radius: Length = 65 (0x0041)
Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
76 70 6e 75 73 65 72
                                                vpnuser
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
send 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) = 0x2Radius: Type = 25 (0x19) Class Radius: Length = 46 (0x2E)Radius: Value (String) = 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf | .....j,. 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a | ....<..n..@....: 18 6f 05 81 00 00 00 00 00 00 00 03 .0..... rad_procpkt: ACCEPT RADIUS_ACCESS_ACCEPT: normal termination RADIUS DELETE remove_req 0x787a6424 session 0x80000001 id 8 free_rip 0x787a6424 radius: send queue empty INFO: Authentication Successful

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Verificare che la connettività tra l'appliance ASA e il Server dei criteri di rete sia corretta.Applicare le acquisizioni dei pacchetti per assicurarsi che la richiesta di autenticazione lasci l'interfaccia ASA (da cui è raggiungibile il server). Confermare che i dispositivi nel percorso non blocchino la porta UDP 1645 (porta di autenticazione RADIUS predefinita) per garantire che raggiunga Server dei criteri di rete. Per ulteriori informazioni sull'acquisizione dei pacchetti sull'appliance ASA, consultare il documento <u>ASA/PIX/FWSM:</u> <u>Acquisizione di pacchetti mediante CLI e ASDM</u>.
- Se l'autenticazione ha ancora esito negativo, controllare il Visualizzatore eventi in Server dei criteri di rete di Windows. In Visualizzatore eventi > Registri di Windows scegliere Protezione.
   Cercare gli eventi associati a Server dei criteri di rete nel periodo di tempo della richiesta di autenticazione.

Event Viewer						<u>_ 5 ×</u>
File Action View Help						
Event Viewer (Local)	Security Number of	events: 93 (1) New events ave	stable			Actions
Custom Views	Kenavords	Date and Time	Source	Event 1D	Task Category	Security 🔺
E Windows Logs	Audit Success	2/10/2014 1:32:48 PM	Microso	4634	Loooff	Anna Saundian
Appleation	Audit Success	2/10/2014 1:37:43 PM	Microso	4624	10000	go open saved bog
Sehun	Audit Success	2/10/2014 1:37:43 PM	Microso	4672	Secolal Lease	Treate Custom View
Sustem	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	
H P Applications and Services Logs	Audt Success	2/10/2014 1:37:28 PM	Microso	4634	Lonoff	Clear Log
Subscriptions	Audit Success	2/10/2014 1:37:28 PM	Microso	4624	Lopop	Piter Current Log
	Audit Success	2/10/2014 1:37:28 PM	Microso	4648	Legen	E annut
	Audit Success	2/10/2014 1:37:28 PM	Microso	4776	Credential Validation	Propercies
	Audit Success	2/10/2014 1:37:24 PM	Microso	4634	Locoff	👯 Find
	Audit Success	2/10/2014 1:37:11 PM	Microso	4624	Legen	Save All Events As
	Audit Success	2/10/2014 1:37:11 PM	Microso	4672	Special Lopon	in sere receiver and
	Audit Success	2/10/2014 1:36:43 PM	Microso	4634	Lopoff	Attach a Task To this Log
	Audit Success	2/10/2014 1:36:43 PM	Microso	4624	Legen	View F
	Audit Success	2/10/2014 1:36:43 PM	Microso	4672	Special Lopon	2
	Audt Falure	2/10/2014 1:35:47 PM	Microso	6273	Network Policy Server	G Refresh
	Audit Success	2/10/2014 1:35:47 PM	Microso	4624	Event Properties	👔 Heip 🕨 🕨
	Audit Success	2/10/2014 1:35:47 PM	Microso	4672	<ul> <li>AStach Task To This Event</li> </ul>	-
	Audit Success	2/10/2014 1:35:47 PM	Microso	4648	L Copy	Event 6273, Microsoft Win 🔺
	Audit Success	2/10/2014 1:35:47 PM	Microso	4769	g Save Selected Events	Event Properties
	E	5 M C - 4			Defeat	
	Evenc 6273, Microsof	t windows security auditing.			Kareso	Attach Task To This Even
General Density				Heb +	E Copy	
	Decano					Save Selected Events
					1	in save search Events

Dopo aver aperto Proprietà evento, dovrebbe essere possibile visualizzare il motivo dell'errore come illustrato nell'esempio. Nell'esempio riportato sotto, il tipo di autenticazione PAP non è stato scelto in Criteri di rete. La richiesta di autenticazione ha pertanto esito negativo.

```
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
            N/A
User:
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
                         SKP
  Account Domain:
  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:
                         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.