مداخ لباقم ASA VPN مدختسملا ةقداصم Windows 2008 NPS (Active Directory) لااثم عم نيوكت RADIUS

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>التكوين</u> <u>التكوينات</u> <u>محوين واجهة سطر الأوامر (CLI)</u> <u>تكوين واجهة سطر الأوامر (CLI)</u> <u>تصحيح أخطاء MNS مع تهيئة NPS</u> <u>تصحيح أخطاء محالاحها</u>

المقدمة

يشرح هذا المستند كيفية تكوين جهاز أمان متكيف (ASA) للاتصال بخادم نهج الشبكة (NPS) لنظام التشغيل Microsoft Windows 2008 مع بروتوكول RADIUS حتى تتم مصادقة مستخدمي Cisco VPN مو أحد أدوار الخادم التي يوفرها Active Directory. NPS المتواردين مقابل Active Directory. NPS هو أحد أدوار الخادم التي يوفرها Windows 2008 Server. وهو مكافئ ل Windows 2003 Server، IAS (خدمة مصادقة الإنترنت)، وهو تنفيذ خادم RADIUS لتوفير مصادقة مستخدم الطلب الهاتفي عن بعد. وعلى نحو مماثل، في NPS RADIUS، وهو تنفيذ يمثل RADIUS تنفيذ خادم RADIUS. أساسا، ASA هو عميل RADIUS لخادم Server. يرسل ASA طلبات مصادقة عنوبة عن مستخدمي VPN و NPS هو عميل RADIUS، لحادم RADIUS.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA الذي يشغل الإصدار 4)9.1
- Windows 2008 R2 Server المثبت عليه خدمات Active Directory ودور NPS

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



التكوينات

تكوين ASDM

- 1. أختر مجموعة النفق التي يلزم لها مصادقة NPS.
 - 2. طقطقة **يحرر** واخترت **أساسي**.
 - 3. في قسم المصادقة، انقر على **إدارة**.

Jasic	Name:	TEST	
Advanced	Aliases:	TEST	
	Authentication		_
	Method:	AAA O Certificate Both	\sim
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	\bigcirc
	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	ite of the group policy selected above.)	
	Enable SSL VPN dient	t protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name: hk.intra	axa	
	•	m	•

- 4. في قسم مجموعات خادم AAA، انقر فوق **إضافة**.
- 5. في حقل مجموعة خوادم AAA، أدخل اسم مجموعة الخوادم (على سبيل المثال، NPS).
 - 6. من القائمة المنسدلة للبروتوكول، أختر RADIUS.
 - 7. وانقر فوق
 - .OK

rd: COL COL CAL Case Coup Coup Packet Case Coup Coup Coup Coup Coup Coup Coup Coup	en en Group	Destand	Accounting Mode	Descrituation Mode	Dead Time	May Enlard Attempt			- (Add
nd Add AAA Server Group AAA Server Group Protectel P	ICAL .	LOCAL	Peccenter g 1 look	TOESCOTO BOTT FORE	Dictard Titles	Park I back Hotelage				
nd: 🗍 🗇 🗇 🕅 Match Case	nd: vers in the Select rver Name or IP	ed Group Address Interfa	Match Case	Add AAA Server AAA Server Group: Protocol: Accounting Nocie: Reactivation Mode: Dead Time: Max Pailed Attempts Dirable interim ac Emable Active Dir VPHSR Compatib CK	Group RADOUS Smult Depict 10 = 3 Sounding up rectory Agen elity Optice	neous @ Single son @ Timed sinules date stracke no noel Help	•			Add Edit Delete Move Up Move Down Test
	ndt	00	Match Case							
DAP Attribute Hap	DAP Attribute	Hap			_					(8

- 8. في قسم الخوادم في المجموعة المحددة، أختر مجموعة خوادم AAA التي تمت إضافتها وانقر فوق **إضافة**.
 - 9. في حقل اسم الخادم أو عنوان IP، أدخل عنوان IP الخاص بالخادم.
 - 10. في حقل "مفتاح سر الخادم"، أدخل المفتاح السري.
- 11. أترك منفذ مصادقة الخادم وحقول منفذ محاسبة الخادم عند القيمة الافتراضية ما لم يستمع الخادم إلى منفذ مختلف.
 - 12. وانقر فوق **OK**.
 - 13. وانقر فوق
 - .OK

Advanced	Name:	TEST				- A	The Local Add Summer		
	Alapes:	TEST					Server Gran	MPK	
	Authenticato	on —				82	Interface Name:	inside -	
configure AAA Se	rver Groups		-	-			Securitizes or Th Address	10 105 130 51	
AAA Server Groups							Terest	10. Iox iox sq	
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Pailed Attempts	Add	meouc	10 seconds	
LOCAL	LOCAL					Edt	RADIUS Parameters		
NRS .	RADIUS	Single	Depletion	10	5		Server Authentication Port	1645	
						Delete	Server Accounting Port:	1646	
Pind:	001	Match Case					Retry Interval:	10 seconds +	1
							Server Secret Key:		1
lervers in the Selec	ted Group				/				
							Commence in the second de		
Server Name or IP	Address Interfac	e Timeout			(Add	Common Password:		
Server Name or IP 10, 105, 130, 51	Address Interfac	e Timeout	4		(Add	Common Password: ACL Netmask Convert:	Standard -	1
Server Name or IP 10.105.130.51	Address Interfac	e Tineout			(Add	Common Paesword: ACL Netmask Convert: Microsoft CHAPv2 Capable:	Standard -	
Server Name or IP 10.105-130.51	Address Interfac roste	e Timeout			C	Add Edit Delete	Common Paesword: ACI, Netmask Convert: Microsoft CHAPv2 Capable:	Standard •	
Server Name or IP 10.105-130.51	Address Interfac	e Timeout			C	Add Edit Delete Nove Up	Common Pastword: ACL Netmask Convert: Microsoft CHAPv2 Capable: SDI Messages	Standard -	
Server Name or IP 10, 105, 130, 51	Address Interfac resde	e Timeout			(Add Edit Delete Nove Up	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table	Standard •	
Server Name or IP 10:105:130:51	Address Interfac	e Timpout				Add Edit Delete Nove Up Move Down	Common Password: ACL Netmaak Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Name	Standard •	
Server Name or IP 10.105.130.51	Address Interfaci reside	e Timeout 30				Add Edit Delese Nove Up Hove Down Test	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Hessage Table Hessage Table Hessage Name ready-for-sys-pin	Standard •	(8) ED PIN
Server Name or IP	Address Interface	e Timeout				Add Edit Delete Nove Up Move Down Test	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Name ready-for-sys-pin new-pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM GENERATE Reporter PIN:	(2) ED PIN
Server Name or IP 10.105.130.51 Find:	Address Interfact	e Timeout 33 Match Case				Add Edit Deline Move Up Move Down Test	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Name ready dur-sys-pin new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reenter	Standard Standard Message Text ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your own we EIN with the new for your own	(S ED PIN wn pin
Server Name or IP 10:105:130.51 Find:	Address Interfactor	e Timeout 23 Match Case				Add Edit Delete Nove Up Move Down Test	Common Passion de ACL Netmaak Convert: Microsoft CHAPv2 Capable SEI Messages Hessage Table Hessage Name ready dor sigs pin new pin neeth new pin neeth new pin neeth new pin neeth new pin neeth new pin neeth	Standard Standard Kessage Text ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your ow new PIN with the next card or Enter Next PASSCOOT	(2) ED PIN wn pin ode
Server Name or IP 10:105-130.51 Find: LDAP Attribute	Address Interface reside	e Timeout 33 Match Case				Add Edit Delete Nove Up Hove Down Test	Common Password: ACL, Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Table Message Name ready-for-sys-pin new-pin-reember new-pin-meth newt-coole-and-reauth next-coole-and-reauth next-coole-and-reauth next-coole-and-reauth	Standard Standard Kessage Text ACCEPT A SYSTEM GENERATI Reenter PIN: Do your own new PIN with the next card oo Inter Next PASSCOOL New PIN Adcested	(2) ED PIN wn pin ode
Server Name or 19 00.105.130.51 Find: LDAP Attribute	Address Interface reside	e Timeout 33 Match Case				Add Edit Delete Move Up Move Down Test	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Name ready-dor-sys-pin new-pin-meth new-pin-meth new-pin-meth new-pin-meth new-pin-dimeth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth next-code-and-reauth	Standard Standard Message Text ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your ow new PIN with the next card or Enter Next PASSCODE New PIN Accepted Please remember your new PIN Accepted Please remember your new PIN	(2) ED PIN orde
Server Name or IP 50:105:120:51 Find: LDAP Attribute	Address Interfact reside	e Timeout 30 Match Case	Cancel	Help		Add Edit Delete Move Up Move Down Test	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Name ready-dor-sys-pin new-pin-meth new-pin-meth new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter new-pin-readter	Standard Standard Kessage Text ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your ow new PIN with the next card co finder Next PASSCOOL New PIN Accepted Please remember your new PI Stater your new Alpha-Namedi	(8 ED P3N vn pin ode cal P3N cal P3N
Server Name or IP 10: 105: 130: 51 Find: LDAP Attribute	Address Interfact reade	e Timeout 30 Match Case	Cancel	Help		Add Edit Delete Move Up Move Down Teat	Common Password: ACL Netmask Convert: Microsoft CHAPv2 Capable SDI Messages Message Table Message Table Message Name ready-for-sys-pin new-pin-meth	Standard Standard Standard Kensage Text ACCEPT A SYSTEM GENERATE ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your ow new PIN with the next card co finder Next PASSCOOL New PIN Accepted Please remember your new PI Enter your next Apta-Named to make changes.)	(8 ED P3N wn pin ode an cal P3N
Server Name or IP to 105 130.51 Find: LDAP Attribute	Address Interfac	e Timeout 33 Match Case	Cancel	Heip		Add Edit Delete Move Up Move Down Test	Common Password: ACL Netmaak Convert: Microsoft CHAPv2 Capable SEC Messages Hessage Table Message Name ready-dor-sys-pin new-pin-reeth new-pin-reeth new-pin-rep-ok new-pin-rep-ok new-pin-rep-ok new-pin-rep-ok new-pin-rep-ok new-pin-rep-ok new-pin-rep-ok new-pin-rep (Double-click in a text cel Restor	Standard Standard Kessage Text Message text Standard Message text Message text	(£ ED PIN vn pin cale N cal PIN
Server Name or IP 10: 105: 130, 51 Find: IDAP Attribute	Address Interfactor	e Timeout 23 Match Case OK	Cancel I	нар		Add Edit Delese Nove Up Move Down Test C	Common Password: ACI, Netmaak Convert: Microsoft CHAPv2 Capable SEI Messages Hessage Table Message Name ready-for-sigs-pin new-pin-reenter new-pin-reenter new-pin-reenter new-pin-reep (Double-dick in a text cell Restore	Standard Standard Kessage Text Message Text ACCEPT A SYSTEM GENERATE Reenter PIN: Do you want to enter your ow new PIN with the next card o Enter Next PASSCOOL New PIN Accepted Please remember your new PI Enter your new Alpha-Numeri Ito make changes.) e default message texts	ED P3h en pin ode

- 14. من القائمة المنسدلة لمجموعة خوادم AAA، أختر المجموعة (مصادر الشبكة (NPS) في هذا المثال) التي تمت إضافتها في الخطوات السابقة.
 - 15. وانقر فوق **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 DHCP Link DHCP Subnet	
	Client Address Pools:	test	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	DfltGrpPolicy 🗸	Manage
	(Following field is an attribu	te of the group policy selected above.)	
	Enable SSL VPN client	t protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name:		
			-
	•	III	+
Find:	Ne:	xt OPrevious	

تكوين واجهة سطر الأوامر (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
ويشكل افتراضي، يستخدم ASA نوع مصادقة بروتوكول مصادقة كلمة المرور (PAP) غير المشفر. لا يعني ذلك أن ال
ويشكل افتراضي، يستخدم ASA نوع مصادقة بروتوكول مصادقة كلمة المرور (PAP) غير المشفر. لا يعني ذلك أن ال
ASA يرسل الكلمة في نص عادي عندما يرسل هو ال radius due radius
```

إذا تم تمكين إدارة كلمة المرور ضمن مجموعة النفق، فعندئذ يستخدم ASA نوع مصادقة MSCHAP-V2 لتشفير كلمة مرور النص العادي. في مثل هذه الحالة، تأكد من تحديد خانة الاختيار **قدرة Microsoft CHAPv2** في نافذة Edit AAA Server التي تم تكوينها في قسم تكوين ASDM.

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

ملاحظة: يستخدم أمر **مصادقة AAA-Server** دائما PAP. لا يستخدم ASA MSCHAP-V2 إلا عندما يقوم المستخدم بتهيئة اتصال بمجموعة النفق مع تمكين إدارة كلمة المرور. أيضا، ال 'كلمة إدارة [كلمة مرور-تنتهي في يوم]' ساندت خيار فقط مع خفيف وزن دليل منفذ بروتوكول (LDAP). لا يوفر RADIUS هذه الميزة. سترى خيار انتهاء صلاحية كلمة المرور عندما تكون كلمة المرور منتهية الصلاحية بالفعل في Active Directory.

Windows 2008 Server مع تهيئة NPS

يجب تثبيت "دور خادم NPS" وتشغيله على خادم Windows 2008. إذا لم تكن هناك مساحة، أختر **ابدأ > أدوات إدارية > أدوار الخادم > إضافة خدمات الأدوار**. أختر "خادم نهج الشبكة" وقم بتثبيت البرنامج. بمجرد تثبيت دور خادم NPS، أكمل الخطوات التالية لتكوين NPS لقبول طلبات مصادقة RADIUS ومعالجتها من ASA:

1. إضافة ASA كعميل RADIUS في خادم NPS. أختر **أدوات إدارية > خادم نهج الشبكة.**انقر بزر الماوس الأيمن فوق **عملاء RADIUS** واختر

								جديد.
Network Policy	Server						<u>_ 8 ×</u>	Start
File Action View	w Help							
🗇 🏟 🙎 📰	?							
NPS (Local)		RADIUS Clients						
RADIUS Clients a	and Servers							
RADIUS Clim	New	RADIUS cl	ients allow you to	specify the network acc	cess servers, that	t provide access to	your	
Policies	Sxport List							
Connection	Minu	Friendly Name	IP Address	Device Manufacturer	NAP Canable	Statue		
Network Pc	view P	Cisco Router	10,105,130,69	RADIUS Standard	No	Enabled		
Health Polic	Refresh							
Network Acces	Help							
Templates Mana	oement							
10								**
								n D
	[]]]	•						2:31 AM 7/20/2013
Network Access	Device							
ALT HELINA & ALLESS				- 1 <i>-</i> . 1	(DNIO	i ida i		

أدخل اسما مألوفا وعنوانا (IP أو DNS) وسرا مشتركا تم تكوينه على ASA.

😂 Network Policy Server	Cisco Router Properties	×		Start
File Action View Help	Settings Advanced			June
🗢 🔿 🔰 🖬 🛛 🖬	Enable this BADUUS start	1		1
NPS (Local)	enable this RADIOS clent			1
RADIUS Clients and Servers	Select an existing template:			
RADIUS Clients			to your	4
Remote RADIUS Server Group				
Policies	Name and Address			-
Connection Request Policies	Friendly name:			
Network Policies	Cisco Router			
Health Policies				
Protection Network Access Protection	Address (IP or DNS):			
Accounting	10.105.130.69 Verify			
remplates 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:			
	••••			
				**
				10 P
	UK Lancel Apply			12:02 AM
H F	1-1	_		7/20/2013

انقر فوق علامة التبويب **خيارات متقدمة**.من القائمة المنسدلة اسم المورد، أختر **معيار RADIUS**.وانقر فوق OK.

NPS (Local)	RADIUS Clients No	w RADIUS Client	×
 NPS (Local) RADIUS Clients and Servers Remote RADIUS Server G Policies Network Access Protection Accounting Templates Management 	RADIUS Clients RADIUS	Settings Advanced Vendor Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list. Vendor name: Image: Client Standard Additional Options Image: Client is NAP-capable	×
		OK Cancel	

2. إنشاء نهج جديد لطلب الاتصال لمستخدمي VPN. الغرض من نهج "طلب الاتصال" هو تحديد ما إذا كانت الطلبات من عملاء RADIUS ستتم معالجتها محليا أو إعادة توجيهها إلى خوادم RADIUS البعيدة. تحت NPS > السياسات، انقر بزر الماوس الأيمن فوق **نهج طلب الاتصال** وقم بإنشاء سياسة جديدة.من نوع القائمة المنسدلة لخادم الوصول إلى الشبكة، أختر **غير محدد**.

Network		1
Eile Actio	test Properties	Start
	Overview Conditions Settings Policy name: test	-
NPs (Local) RADIUS RAD RAD RAD Rem Policies Conr Netv Heal	Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled 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 poin select Unspecified. Type of network access server: Unspecified Vendor specific: 10 2	
		« () [) [) 12:08 AM
•	OK Cancel ,	7/20/2013

انقر على علامة التبويب **الشروط**.انقر فوق **إضافة (Add)**.أدخل عنوان IP الخاص ب ASA كشرط 'عنوان IPv4 للعميل'.

File Actio	test Properties	Start
File Actio		
NPS (Local) RADIUS RAD RAD RAD Rem Rem Rem	Overview Conditions Settings 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.	
Conr	Condition Value	
Netv	Client IPv4 Address 10.105.130.69	
📔 Heal		
So 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 Remo	w € 12:08 AM 7/20/2013

انقر على صفحة **الإعدادات**.أختر **المصادقة** تحت طلب إعادة توجيه الاتصال. تأكد من إختيار طلبات المصادقة على زر الخيار للخادم.وانقر فوق OK.



3. إضافة نهج شبكة حيث يمكنك تحديد المستخدمين المسموح لهم بالمصادقة.على سبيل المثال، يمكنك إضافة مجموعات مستخدمي Active Directory كشرط. تتم مصادقة أولئك المستخدمين الذين ينتمون إلى مجموعة Windows محددة فقط بموجب هذا النهج.تحت NPS، أختر **السياسات**.انقر بزر الماوس الأيمن فوق **نهج الشبكة** وقم بإنشاء نهج جديد.تأكد من إختيار الزر "منح حق الوصول".من نوع القائمة المنسدلة لخادم الوصول إلى الشبكة، أختر **غير محدد**.

Ja He	test Properties	Start
File	Overview Conditions Constraints Settings	
(2) (Policy name: test	
NPS (
- International	Folicy state If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
E P	E Peter secold	
2		
	Access Permission	
	If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?	
🛒 T		
	Grant access. Grant access if the connection request matches this policy.	
	C Deny access. Deny access if the connection request matches this policy.	
	Ignore user account dial-in properties.	
	authorization with network policy only; do not evaluate the dial-in properties of user accounts .	
	Network connection method	
	Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but network access server is an 802.1X authenticating switch or wireless access point.	
	select Unspecified.	
	Type of network access server:	
	Unspecified	
	C Vendor specific:	
	10 🚔	10 P
		12:11 AM
	OK Cancel Apply	

انقر على علامة التبويب **الشروط**.انقر فوق **إضافة (Add)**.أدخل عنوان IP الخاص ب ASA كحالة عنوان IPv4 للعميل.أدخل مجموعة مستخدمي Active Directory التي تحتوي على مستخدمي VPN.

🐌 No	test Properties		Pro. 1
File	Quarian Constitues Con	And a second sec	Start
(.	Overview Considerins Con	istrants Settings	
NDC	Configure the conditions for	this network policy.	5
R	If conditions match the conr connection request, NPS sk	nection request, NPS uses this policy to authorize the connection request. If conditions do not match the kips this policy and evaluates other policies, if additional policies are configured.	$\mathbf{\Sigma}$
-	Condition	Value	1 mil
7	Liser Groups	SKP\VPN	
	Client IPv4 Address	10.105.130.69	
	Condition description: The Client IP Address cond	Ition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
		Add Edit Remove	«
•		OK Cancel Apply	7/20/2013

انقر فوق علامة التبويب **القيود**.أختر **طرق المصادقة**.تأكد من تحديد خانة الاختيار المصادقة غير المشفرة (،PAP SPAP).وانقر فوق

.OK

🥬 Ne	test Properties	Start
File	Overview Conditions Constraints Settings	-
()	Configure the constraints for this network policy.	
NPS	If all constraints are not matched by the connection request, network access is denied.	
	Constraints:	
	Constraints Allow access only to those clients that authenticate with the specified methods.	
	Idle Timeout EAP types are negotiated between NPS and the client in the order in which they are listed. Session Timeout EAP types are negotiated between NPS and the client in the order in which they are listed.	
A I	Called Station ID Move Up	
-	Day and time restrictions Image: Second s	
	Add Edit Remove	
	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 (PAP, SPAP)	
	Allow clients to connect without negotiating an authentication method	
	Perform machine health check only	
		"
		10 P
		12:13 AM
•	OK Cancel <u>Apply</u>	7/20/2013

تمرير سمة نهج المجموعة (السمة 25) من خادم NPS RADIUS

إذا كان نهج المجموعة بحاجة إلى تعيينه للمستخدم بشكل ديناميكي باستخدام خادم NPS RADIUS، يمكن إستخدام سمة RADIUS لنهج المجموعة (السمة 25).

أكمل هذه الخطوات لإرسال سمة RADIUS 25 للتعيين الديناميكي لنهج المجموعة للمستخدم.

1. بعد إضافة "نهج الشبكة"، انقر بزر الماوس الأيمن فوق "نهج الشبكة" المطلوب وانقر فوق علامة التبويب **إعدادات**.

🚯 Network Policy Server					
File Action View Help			the second se		
🗢 🔿 🙍 📅 🛛 🖬	test Pronerties			×	
Accounting Templates Management	est Properties Descriptions Constraints Settings Configure the settings for this network policy. It conditions and constraints match the connel Settings: RADIUS Attributes Setting Condox Specific Network Access Protection Settended State Routing and Remote Access Multimk and Bandwidth Allocation Protocol (BAP) FIFTers Encepption FIP Settings	ngs and the policy grants access, settings are applied To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes. Attributes: Name Value Framed Protocol PIP Service-Type Framed			
		Add.	Edit. Remove	iy.	

2. أختر **خصائص RADIUS > قياسية**. انقر فوق **إضافة (A**dd). أترك نوع الوصول "الكل".

			العل
🚯 Network Policy	Server		
File Action VI	Overview Conditions Conditionts Softings Configure the settings for this network policy. If conditions and constraints match the connec Settings:	tion request and t	the policy graves access, settings are applied.
Polities Conne Polities Polities Polities Network A Accountin; Templates	RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access Multilink and Bandwidth Multilink and Bandwidth Protection (BAP) IP Filtere Encryption IP Settings	To rend additor then click Edit I your PADIUS di Attributes: Name FranschProtoc Service-Type Add.	To add an attribute to the settings, select the attribute, and then click Add. To add a custom or predefined Vendor Specific attribute, close this delog and select Vendor Specific, and then click Add. Access type Attributes: Attributes: Attributes: Attributes: Attributes: Description: Description: Specific attribute, close this delog and select Vendor Specific, and then click Add. Caliback-Number Clears FiberId Fiamed AppleTak-Link Fiame
			OK Cencel Apply

3. في مربع الخصائص، أختر **فئة** وانقر **إضافة**. أدخل قيمة السمة، أي اسم نهج المجموعة كسلسلة. تذكر أنه يجب تكوين سياسة مجموعة بهذا الاسم في ASA. هذا حتى أن ASA يقوم بتعيينه إلى جلسة VPN بعد أن يستلم هو هذه السمة في إستجابة RADIUS.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر **debug**.

تصحيح أخطاء ASA

مكنت 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: 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 = 65c4 lb ab la e3 7e 6d 12 da 87 6f 7f |A.....~m 41 00 08 01)..a8 36 01 09 76 70 6e 75 73 65 72 02 12 28 @P.6..vpnuser 50 40 .c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04 | .h.....Z.oC=.....0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00 | ..i 06 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 6e 75 73 65 72 **vpnuser** 70 76 Radius: Type = 2(0x02) User-Password (Radius: Length = 18 (0x12) = (Radius: Value (String c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 | (.h.....Z.oC 28 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 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 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37 | ...N..Kv+.7 00 08 02bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 00 02 | ..lL ..@...2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf / ,....<le 3a 18 6f 05 81 00 00 00 00 00 00 00 03 .:.0Parsed 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 |7....j :...@....3c 84 Of 6e f5 95 d3 40 01 cf 1e 3a |<..n 00 00 00 006f 05 81 00 00 00 00 00 00 00 03 .0 18 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

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- تأكد من أن الاتصال بين خادم ASA و NPS جيد.تطبيق التقاط الحزم لضمان أن يترك طلب المصادقة واجهة ASA (من حيث يمكن الوصول إلى الخادم). تأكد من أن الأجهزة الموجودة في المسار لا تمنع منفذ UDP 1645 (منفذ مصادقة RADIUS الافتراضي) لضمان وصوله إلى خادم NPS. يمكن العثور على مزيد من المعلومات حول التقاط الحزم على ASA في ASA/PIX/FWSM: التقاط الحزم باستخدام CLI ومثال تكوين ASDM.
- في حالة إستمرار فشل المصادقة، ابحث في عارض الأحداث على NPS ل Windows. تحت عارض الأحداث > سجلات Windows، أختر **التأمين.** ابحث عن الأحداث المقترنة ب NPS في وقت طلب المصادقة.

Event Viewer								. 6 ×
File Action View Help								
🗢 🔿 🖄 🖬 📓 🛅								
Event Viewer (Local)	Security Number of	events: 93 (1) New events ava	iable				Actions	
Custom Views	Keywords	Date and Time	Source	Event 1D	Task Category		Security	-
E Mindows Logs	Audit Success	2/10/2014 1:37:48 PM	Microso	4634	Lopoff	22	Coren Saved Lon	
Security	Audit Success	2/10/2014 1:37:43 PM	Microso	4624	Legen		gen surce tog	
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 Policy Server		during	-
🗄 🔚 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		Piber 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	
	Audit Success	2/10/2014 1:37:24 PM	Microso	4634	Logoff		Find	
	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		All ach a Task To this I a	
	Audit Success	2/10/2014 1:36:43 PM	Microso	4634	Logoff		Addach a Task To this Lo	/9
	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		Refrech	
	Audit Failure	2/10/2014 1:35:47 PM	Microso	6273	Notwork Policy Server	_	M Herresh	
	Audit Success	2/10/2014 1:35:47 PM	Microso	4624	L Event Properties		👔 Help	•
	Audit Success	2/10/2014 1:35:47 PM	Microso	4672	AStach Task To This Event			
	Audit Success	2/10/2014 1:35:47 PM	Microso	4648	L Copy	•	Event 6273, Microsoft Wi	n 🔺
	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	m
	General Details				Help		Copy	
						-	Save Selected Events	1

بمجرد فتح "خصائص الحدث"، يجب أن تكون قادرا على رؤية سبب الفشل كما هو موضح في المثال. في هذا المثال، لم يتم إختيار PAP كنوع مصادقة ضمن نهج الشبكة. وبالتالي، يفشل طلب المصادقة.

Log Name: Security Microsoft-Windows-Security-Auditing Source: 2/10/2014 1:35:47 PM Date: Event ID: 6273 Task Category: Network Policy Server Information Level: Keywords: Audit Failure User: N/A win2k8.skp.com Computer: :Description .Network Policy Server denied access to a user .Contact the Network Policy Server administrator for more information :User Security ID: SKP\vpnuser vpnuser Account Name: 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: Virtual NAS Port: 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 :ЕАР Туре -- :Account Session Identifier .Logging Results: Accounting information was written to the local log file Reason Code: 66 The user attempted to use an authentication method that is Reason: .not enabled on the matching network policy

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما