ا ققداصم مداوخ تاعومجم Kerberos ققداصم مداوخ تاعومجم LDAP ضيوفتو ربع VPN ليمع يمدختسمل ASDM/CLI نيوكت لاثم

المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المكونات المستخدمة</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> معلومات أساسية تكوين المصادقة والتفويض لمستخدمي VPN باستخدام ASDM تكوين مجموعة نفق VPN للمصادقة والتفويض تكوين المصادقة والتفويض لمستخدمي VPN باستخدام CLI التحقق من الصحة واستكشاف الأخطاء وإصلاحها معلومات ذات صلة

<u>المقدمة</u>

يصف هذا المستند كيفية إستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco لتكوين مصادقة Kerberos ومجموعات خادم تفويض LDAP على جهاز الأمان Cisco PIX 500 Series Security Appliance. في هذا المثال، يتم إستخدام مجموعات الخوادم بواسطة نهج مجموعة أنفاق VPN لمصادقة المستخدمين الواردين وتخويلهم.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

يفترض هذا المستند أن PIX قيد التشغيل الكامل وتم تكوينه للسماح ل ASDM بإجراء تغييرات التكوين.

ملاحظة: راجع <u>السماح بوصول HTTPS ل ASDM</u> للسماح بتكوين PIX بواسطة ASDM.

<u>المكونات المستخدمة</u>

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

- برنامج جهاز أمان PIX من Cisco الإصدار x.7 والإصدارات الأحدث
 - Cisco ASDM، الإصدار x.5 والإصدارات الأحدث

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.

<u>المنتجات ذات الصلة</u>

كما يمكن إستخدام هذا التكوين مع جهاز الأمان القابل للتكيف (ASA) من Cisco، الإصدار x.7.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>معلومات أساسية</u>

لا يتم دعم جميع طرق المصادقة والتفويض الممكنة المتوفرة في برنامج PIX/ASA 7.x عند التعامل مع مستخدمي VPN. يوضح هذا الجدول الطرق المتوفرة لمستخدمي الشبكة الخاصة الظاهرية (VPN):

LDAP	Ker bero s	NT	SDI	TA CA CS +	RA DI US	محلي	
لا	نعم	نعم	نعم	نعم	نعم	نعم	المصا دقة
نعم	لا	ע	ע	لا	نعم	نعم	الاعتم اد

ملاحظة: يتم إستخدام Kerberos للمصادقة ويستخدم LDAP لتفويض مستخدمي VPN في هذا المثال.

<u>تكوين المصادقة والتفويض لمستخدمي VPN باستخدام ASDM</u>

تكوين خوادم المصادقة والتفويض

أكمل هذه الخطوات لتكوين مجموعات خوادم المصادقة والتفويض لمستخدمي VPN من خلال ASDM.

1. أختر **تكوين > خصائص > إعداد AAA > مجموعات خوادم AAA**، وانقر **إضافة**.



2. قم بتحديد اسم لمجموعة خوادم المصادقة الجديدة، واختر بروتوكولا.يكون خيار وضع المحاسبة ل RADIUS و TACACS+ فقط. انقر فوق موافق عند

薩 Add AAA Server Gro	oup X
Configure AAA server applicable for RADIUS	group. The Accounting Mode attribute is only 3 and TACACS+ protocols.
Server Group:	my_authent_grp
Protocol:	Kerberos
Accounting Mode:	C Simultaneous 💿 Single
Reactivation Mode:	 Depletion C Timed
Dead Tin	ne: 10 minutes
Max Failed Attempts:	3
ОК	لانتهاء.

^{3.} كرر الخطوات 1 و 2 لإنشاء مجموعة خوادم تخويل

藬 Add AAA Server Gro	pup	×	
Configure AAA server (applicable for RADIUS	group. The Accounting and TACACS+ protoco	Mode attribute is only Is.	
Server Group:	my_author_grp		
Protocol:	LDAP	Ē	
Accounting Mode:	C Simultaneous	 Single 	
Reactivation Mode:	 Depletion 	C Timed	
Dead Tin	ne: 10	minutes	
Max Failed Attempts:	3		
ОК	Cancel	Help	جديدة
		وق تطبيق لإرسال التغييرات إلى	، انقر ف
			الجهاز



إذا قمت بتكوينه للقيام بذلك، فإن الجهاز يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله. 5. طقطقة **يرسل** in order to أرسلت الأمر إلى

الأداة.

The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the PIX, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

aaa-server my_authent_grp protocol kerberos aaa-server my_authent_grp protocol kerberos reactivation-mode depletion deadtime 10 max-failed-attempts 3 aaa-server my_author_grp protocol Idap aaa-server my_author_grp protocol Idap reactivation-mode depletion deadtime 10 max-failed-attempts 3	*
Send Cancel	j –
ء مجموعات الخوادم التي تم إنشاؤها حديثا الآن بخوادم المصادقة والتخويل.	يجب ملء

6. أُختر **تكوين > خُصائص > َإعداد AAA > خوادم AAA،** وانقر َ إضافة.

X

📬 Cisco ASDM 5.0	0 for PIX - 10.89.129.147		_ O ×
File Rules Sea	arch Options Tools Wizards	Help	
Home C	anfiguration Monitoring	Sack Forward Search Refresh Save Help	Cisco Systems
Features	Configuration > Features > Pro	rerties > AAA Setup > AAA Servers	
Hterfaces	⊕ ⊕ ₩ ■ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Add and configure AAA servers for existing AAA server groups. To configure se go to the <u>AAA Berver Groups</u> screen.	rver groups
NAT VPN	- Sont-Spoofing - Fragment - TCP Options - OTimeouts - RP Static Table		Edit
Routing Routing	P DHCP Services P DHCP Server P DHCP Relay DHCP Relay DHCP Relay P DNS Client		1651
Administration	History Metrics History Metrics P Audit P Audit Policy P Audit Signatur Cogging P Logging Setup P Event Lists Cogging Filters		
Wizards /	Syslog Setup	Apply Reset	
Configuration cha	inges saved successfully.	cisco NA (15) 🚔 🔂	1/19/06 10:46:23 PM UTC

7. قم بتكوين خادم مصادقة. انقر فوق موافق عند

Server Group:		my authent or	1	-
conter oroup.		Intra annual gir	r 	
Interface Name:		inside		•
Server IP Address:		172.22.1.100		
Timeout:		10	seconds	
– Kerberos Parame	ters — —			
Server Port:	88			
Server Port: Retry Interval:	88 10 second	ls		•
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	ds ISCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	ds ISCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	ds ISCO.COM		
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	ds ISCO.COM		
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	ds ISCO.COM		
Server Port: Retry Interval: Kerberos Realm: OK	88 10 second REALM.CI	ds ISCO.COM	Help	

يتواجد عليها الخادم.**عنوان IP للخادم**—حدد عنوان IP الخاص بخادم المصادقة.**المهلة**— حدد الحد الأقصى للوقت، بالثواني، للانتظار إستجابة من الخادم.**معلمات Kerberos:منفذ الخادم**—88 هو المنفذ القياسي ل Kerberos.**الفاصل الزمني لإعادة المحاولة**— أختر الفاصل الزمني لإعادة المحاولة المطلوب.**عالم Kerberos**—أدخل اسم عالم Kerberos. غالبا ما يكون هذا هو اسم مجال Windows في كافة الأحرف الكبيرة.

8. قم بتكوين خادم تفويض. طقطقة **ok** عندما

Server Group:	my_author_grp
Interface Name:	inside 💌
Server IP Address:	172.22.1.101
Timeout:	10 seconds
LDAP Parameters	
Server Port:	389
Base DN:	ou=cisco
Scope:	One level beneath the Base DN
Naming Attribute(s):	uid
Login DN:	
Login Password:	
Confirm Login Password:	
	,

ة الخوادم—أختر مجموعة خوادم التخويل التي تم تكوينها في الخطوة 3.ا**سم الواجهة**— أختر الواجهة التي يتواجد عليها الخادم.**عنوان IP للخادم**—حدد عنوان IP الخاص بخادم التخويل.**المهلة**— حدد الحد الأقصى للوقت، بالثواني، للانتظار إستجابة من الخادم.**معلمات LDAP منفذ الخادم**—389 هو المنفذ الافتراضي ل LDAP.**Base DN**—أدخل الموقع في التدرج الهرمي ل LDAP حيث يجب أن يبدأ الخادم في البحث بمجرد أن يستلم طلب تخويل.**النطاق**—أختر المدى الذي يجب أن يبحث فيه الخادم في التدرج الهرمي ل LDAP بمجرد أن يستلم طلب تفويض.**سمة (سمات) التسمية**- أدخل سمة (سمات) الأسماء المميزة ذات الصلة التي يتم من خلالها تعريف الإدخالات الموجودة على خادم LDAP بشكل فريد. سمات التسمية الشائعة هي الاسم الشائع (cn) تعريف الإدخالات الموجودة على خادم LDAP—تنطلب بعض خوادم PDAL، بما في ذلك خادم IDAP مومعرف المستخدم (uid).**تسجيل الدخول ND**—تنطلب بعض خوادم PDAL، بما في ذلك خادم IDAP ومعرف المستخدم (uid). معرف المستخدم (uid) معان التصمية المحال بعض خوادم LDAP، بما في ذلك خادم Microsoft أخرى. يحدد حقل ND الخاص بتسجيل الدخول حصائص مصادقة الجهاز، والتي يجب أن تنطابق مع خصائص أخرى. يحدد حقل ND الخاص بتسجيل الدخول خصائص مصادقة الجهاز، والتي يجب أن تنطابق مع خصائص أخرى. يحدد حقل ND الخاص بنسجيل الدخول خصائص مصادقة الجهاز، والتي يعب أن تنطابق مع خصائص أخرى. يحدد حقل ND الخاص بتسجيل الدخول خصائص مصادقة الجهاز، والتي يعب أن تنطابق مع خصائص أخرى. يحدد حقل ND الخاص بتسجيل الدخول خصائص مصادقة الجهاز، والتي يوب أن تنطابق مع خصائص أخرى. يحدد حقل ND الخاص بتسجيل الدخول حصائص مصادقة الجهاز، والتي يوب أن تنطابق مع خصائص مستخدم لديه امتيازات إدارية. على سبيل المثال، cn=administrator. فارغا.**كلمة مرور تسجيل الدخول**- أدخل كلمة المرور ل ND تسجيل الدخول.**قم بتأكيد كلمة مرور تسجيل** الد**خول**— فريما بلاحول. أدخل كلمة المرور ل ND تسجيل الدخول.قم بتأكيد كلمة مرور تسجيل الد**خول**— قم بتأكيد كلمة المرور ل ND الخاص بتسجيل الدخول.قم بتأكيد كلمة مرور تسجيل 9. انقر فوق **تطبيق** لإرسال التغييرات إلى الجهاز بعد إضافة جميع خوادم المصادقة والتخويل.إذا قمت بتكوينه للقيام بذلك، فإن PIX يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله. 10. طقطقة **يرسل** in order to أرسلت الأمر إلى الأداة.

تكوين مجموعة نفق VPN للمصادقة والتفويض

أتمت هذا steps in order to أضفت النادل مجموعة أنت فقط شكلت إلى VPN نفق مجموعة.

1. أخترت **تشكيل > VPN > مجموعة نفق**، وطقطقة **يضيف** in order to خلقت جديد نفق مجموعة، أو **يحرر** in order to عدلت مجموعة

					موجود.
📬 Cisco ASDM 5	.0 for PIX - 10.89.129.147				
File Rules B	earch Options Tools Wizard	is Help			
💰 Home	Configuration Monitoring	Back Forward Search	Refresh Save	? Help	CISCO SYSTEMS
Features	Configuration > Features > VP	'N > General > Tunnel Group			
Hterfaces Hterfaces Security Policy NAT NAT Security Policy NAT Security Policy NAT Security Policy NAT		Kanage VPN tunnel group Manage VPN tunnel group IPSec connections. Name Default(RAGroup Default(L2L Group	os. A VPN tunnel group n Type Ipsec-ra Ipsec-121	epresents a connection sp Group Policy DftIGrpPolicy DftIGrpPolicy	ecific record for Add Edit Delete
Administration Administration Properties Wizards /	Provis	Specify the delimiter to be are received when tunnels Group Delimiter: - No	e used when parsing tun s are being negotiated. one Roply	nel group names from the Reset	user name that
			cisco NA (15)	🚽 🔤 🖬 🛛 🖻	1/19/06 10:48:03 PM UTC

2. في علامة التبويب "عام" للنافذة التي تظهر، حدد مجموعات الخوادم التي تم تكوينها مسبقا.

🕵 Add Tunnel Group		×
Identity General Client Address A	ssignment IPSec Advanced	
Group Policy: DfltGrpPolicy	T	
🗖 Strip the realm from usernan	ne before passing it on to the AAA server	
Strip the group from username	ne before passing it on to the AAA server	
To set authentication server grou	p per interface, go to the Advanced tab.	
Authentication Server Group:	my_authent_grp	
Use LOCAL if Server Gr	oup fails	
Authorization Server Group:	my_author_grp	
🗌 Users must exist in the	authorization database to connect	
Accounting Server Group:	None	
<u>ок</u>	Cancel Help	

- 3. *إختياري:* قم بتكوين المعلمات المتبقية في علامات التبويب الأخرى إذا قمت بإضافة مجموعة نفق جديدة.
 - 4. انقر فوق موافق عند الانتهاء.
- 5. انقر فوق **تطبيق** لإرسال التغييرات إلى الجهاز بعد اكتمال تكوين مجموعة النفق.إذا قمت بتكوينه للقيام بذلك، فإن PIX يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله.
 - 6. طقطقة **يرسل** in order to أرسلت الأمر إلى الأداة.

تكوين المصادقة والتفويض لمستخدمي VPN باستخدام CLI

هذا هو تكوين CLI المكافئ لمجموعات خوادم المصادقة والتفويض الخاصة بمستخدمي VPN.

تكوين واجهة سطر الأوامر (CLI) عبر جهاز الأمان

pixfirewall#show run Saved : : (PIX Version 7.2(2)

```
I
                                    hostname pixfirewall
                     domain-name default.domain.invalid
             enable password 8Ry2YjIyt7RRXU24 encrypted
                                                   names
                                                       !
                                     interface Ethernet0
                                               shutdown
                                              no nameif
                                      no security-level
                                          no ip address
                                                       !
                                     interface Ethernet1
                                          nameif inside
                                     security-level 100
                 ip address 172.22.1.105 255.255.255.0
                                                       !
   Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU ---!
 encrypted ftp mode passive dns server-group DefaultDNS
  domain-name default.domain.invalid pager lines 24 mtu
  inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
      is suppressed. aaa-server my_authent_grp protocol
                                                kerberos
            aaa-server my_authent_grp host 172.22.1.100
                        kerberos-realm REALM.CISCO.COM
                 aaa-server my_author_grp protocol ldap
             aaa-server my_author_grp host 172.22.1.101
                                  ldap-base-dn ou=cisco
                                    ldap-scope onelevel
                             ldap-naming-attribute uid
                                      http server enable
                            http 0.0.0.0 0.0.0.0 inside
                                no snmp-server location
                                 no snmp-server contact
    snmp-server enable traps snmp authentication linkup
                                      linkdown coldstart
         tunnel-group DefaultRAGroup general-attributes
            authentication-server-group my_authent_grp
              authorization-server-group my_author_grp
                                                       ļ
```

.Output is suppressed ---.

<u>التحقق من الصحة</u>

أكمل هذه الخطوات للتحقق من مصادقة المستخدم بين خادم PIX/ASA و AAA:

1. أختر **تكوين > خصائص > إعداد AAA > خوادم AAA**، وحدد مجموعة الخوادم (my_authent_grp). ثم انقر على **إختبار** للتحقق من مسوغات المستخدم.



2. قم بتوفير اسم المستخدم وكلمة المرور (على سبيل المثال، اسم المستخدم: الاختبار وكلمة المرور: الاختبار)، وانقر **موافق** للتحقق من

🚰 Test AAA Server -172.	22.1.100	ا شخص ش	
To test the following AA password.	A server enter username and		
AAA Server Group:	my_authent_grp (Kerberos)		
Host:	172.22.1.100		
${f C}$ Authorization	O Authentication		
Username:	test		
Password:	***		
ок	Cancel		الم حة
			أينايد

3. يمكنك أن ترى أن المصادقة



استكشاف الأخطاء وإصلاحها

- 2. يجب تعطيل المصادقة المسبقة في Active Directory (AD)، أو قد يؤدي ذلك إلى فشل مصادقة المستخدم.
- 3. يتعذر على مستخدمي عميل شبكة VPN المصادقة مقابل خادم شهادات Microsoft. تظهر رسالة الخطأ هذه: ا
- ِّ (14) لحل هذه المشكلة، قم بإلغاء تحديد خانة الاختيار **لا تتطّلب** مصادقة **مسبقة لُ kerberose** على خادم المصادقة.

<u>معلومات ذات صلة</u>

- <u>تكوين خوادم AAA وقاعدة البيانات المحلية</u>
- <u>دعم منتجات أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco م</u>
 - برنامج جدار حماية <u>Cisco PIX</u>
 - <u>مراجع أوامر جدار حماية PIX الآمن من Cisco</u>
 - <u>الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)</u>
 - <u>طلبات التعليقات (RFCs)</u>
 - <u>الدعم التقني والمستندات Cisco Systems</u>

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