# PIX/ASA:通過ASDM/CLI配置VPN客戶端使用者的Kerberos身份驗證和LDAP授權伺服器組示例

## 目錄

 簡介

 必要條件

 需求

 採用元件

 相關產品

 慣例

 背景資訊

 使用ASDM為VPN使用者配置身份驗證和授權

 配置身份驗證和授權伺服器

 配置VPN隧道組以進行身份驗證和授權

 使用CLI為VPN使用者配置身份驗證和授權

 驗證

 疑難排解

 相關資訊

## <u>簡介</u>

本文檔介紹如何使用Cisco Adaptive Security Device Manager(ASDM)在Cisco PIX 500系列安全裝置上配置Kerberos身份驗證和LDAP授權伺服器組。在本示例中,VPN隧道組的策略使用伺服器組 對傳入使用者進行身份驗證和授權。

## <u>必要條件</u>

### <u>需求</u>

本文檔假定PIX完全可以運行並且配置為允許ASDM更改配置。

注意:請參閱<u>允許ASDM的HTTPS訪</u>問,以便允許ASDM配置PIX。

#### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco PIX安全裝置軟體版本7.x及更高版本
- Cisco ASDM版本5.x及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

#### <u>相關產品</u>

此配置還可以與思科自適應安全裝置(ASA)版本7.x配合使用。

#### <u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

## <u>背景資訊</u>

處理VPN使用者時,並不支援PIX/ASA 7.x軟體中的所有可能的身份驗證和授權方法。下表詳細說明 了哪些方法可用於VPN使用者:

	本	RADIU	TACAC	S	Ν	Kerber	LDA
	地	S	S+	DI	Т	os	Ρ
驗證	是	是	是	是	是	是	否
Authorizati on	是	是	否	否	否	否	是

注意:在本示例中,Kerberos用於身份驗證,LDAP用於VPN使用者的授權。

## 使用ASDM為VPN使用者配置身份驗證和授權

#### 配置身份驗證和授權伺服器

完成以下步驟,以便通過ASDM為VPN使用者配置身份驗證和授權伺服器組。

1. 選擇Configuration > Properties > AAA Setup > AAA Server Groups,然後按一下Add。



2. 定義新身份驗證伺服器組的名稱,並選擇協定。Accounting Mode選項僅適用於RADIUS和 TACACS+。完成後按一下**OK**。

💼 Add AAA Server Group 🔀									
Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.									
Server Group:	my_authent_grp								
Protocol:	Kerberos								
Accounting Mode:	C Simultaneous C Single								
Reactivation Mode:	O Depletion								
Dead Tin	ne: 10 minutes								
Max Failed Attempts:	3								
ОК	Cancel Help								

3. 重複步驟1和2以建立新的授權伺服器組。

🚰 Add AAA Server Group 🛛 🔀									
Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.									
Server Group:	my_author_grp								
Protocol:	LDAP								
Accounting Mode:	O Simultaneous 💿 Single								
Reactivation Mode:	Depletion     O Timed								
Dead Tin	ne: 10 minutes								
Max Failed Attempts:	3								
ОК	Cancel Help								

4. 按一下「Apply」將變更傳送到裝置。



如果裝置已配置為這樣做,裝置現在會預覽新增到運行配置中的命令。

5. 按一下「Send」將命令傳送到裝置。

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 reactivation-mode depletion deadtime 10 max-failed-attempts 3	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	Ă

現在必須使用身份驗證和授權伺服器填充新建立的伺服器組。

6. 選擇Configuration > Properties > AAA Setup > AAA Servers,然後按一下Add。



7. 配置身份驗證伺服器。完成後按一下OK。

Add AAA Server						×
Server Group:		my_authen	it_grp		•	
Interface Name:		inside			•	
Server IP Address:		172.22.1.10	00			
Timeout:		10		seconds		
—Kerberos Parame	ters ———					
Server Port	88					
Retry Interval:	10 second	s			•	
Kerberos Realm:	REALM.CIS	зсо.сом			_	
	,					
					1	
ОК	_┣	Cancel		Help		

Group — 選擇步驟2中配置的身份驗證伺服器組。Interface Name — 選擇伺服器所在的介面 。Server IP Address — 指定身份驗證伺服器的IP地址。Timeout — 指定等待伺服器響應的最 長時間(以秒為單位)。Kerberos引數:伺服器端口 — 88是Kerberos的標準埠。重試間隔 (Retry Interval) — 選擇所需的重試間隔。Kerberos Realm — 輸入Kerberos領域的名稱。這通 常是所有大寫字母的Windows域名。

8. 配置授權伺服器。完成後按一下OK。

🚰 Add AAA Server	×
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:	
ок	Cancel Help
	s

Group — 選擇步驟3中配置的授權伺服器組。Interface Name — 選擇伺服器所在的介面。 Server IP Address — 指定授權伺服器的IP地址。Timeout — 指定等待伺服器響應的最長時間 (以秒為單位)。LDAP引數:伺服器端口 — 389是LDAP的預設埠。基本DN — 在LDAP層次 結構中輸入伺服器在收到授權請求後應開始搜尋的位置。Scope — 選擇伺服器在收到授權請 求後搜尋LDAP層次結構的範圍。Naming Attribute(s)-輸入Relative Distinguished Name(s)屬 性,LDAP伺服器上的條目可依據該屬性進行唯一定義。常用命名屬性包括公用名(cn)和使用 者ID(uid)。登入DN — 某些LDAP伺服器(包括Microsoft Active Directory伺服器)要求裝置通 過身份驗證繫結建立握手,然後才接受任何其他LDAP操作的請求。Login DN欄位定義裝置的 身份驗證特性,這些特性應與具有管理許可權的使用者所對應的身份驗證特性。例如, cn=administrator。對於匿名訪問,請將此欄位留空。Login Password — 輸入登入DN的密碼

- 。Confirm Login Password 確認登入DN的密碼。
- 9. 按一下Apply可在新增所有身份驗證和授權伺服器之後將更改傳送到裝置。如果已經進行了配置, PIX現在將預覽新增到運行配置中的命令。

10. 按一下「Send」將命令傳送到裝置。

### <u>配置VPN隧道組以進行身份驗證和授權</u>

完成這些步驟,將剛才配置的伺服器組新增到VPN隧道組。

 選擇Configuration > VPN > Tunnel Group,然後按一下Add以建立新的隧道組,或按一下 Edit以修改現有組。



2. 在出現的視窗的General頁籤上,選擇之前配置的伺服器組。

💼 Add Tunnel Group
Identity General Client Address Assignment IPSec Advanced
Group Policy: DfltGrpPolicy
Strip the realm from username before passing it on to the AAA server
Strip the group from username before passing it on to the AAA server
To set authentication server group per interface, go to the Advanced tab.
Authentication Server Group: my_authent_grp
Use LOCAL if Server Group fails
Authorization Server Group: my_author_grp
Users must exist in the authorization database to connect
Accounting Server Group:
OK Cancel Help

- 3. 可選: 如果新增新隧道組,請在其它頁籤上配置其餘引數。
- 4. 完成後按一下**OK**。
- 5. 按一下「**Apply**」,以在完成通道組設定後將變更傳送到裝置。如果已經進行了配置,PIX現在 將預覽新增到運行配置中的命令。
- 6. 按一下「Send」將命令傳送到裝置。

# 使用CLI為VPN使用者配置身份驗證和授權

這是適用於VPN使用者的身份驗證和授權伺服器組的等效CLI配置。

安全裝置CLI配置
pixfirewall# <b>show run</b> : Saved
: PIX Version 7.2(2)

```
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
shutdown
no nameif
no security-level
no ip address
1
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
!--- Output is suppressed.
```

## <u>驗證</u>

完成以下步驟,驗證PIX/ASA和AAA伺服器之間的使用者身份驗證:

 選擇Configuration > Properties > AAA Setup > AAA Servers, 然後選擇伺服器組 (my\_authent\_grp)。 然後按一下**測試**以驗證使用者憑據。

	Cisco ASDM 5.0 File Rufes Sea	) for PIX - 10. arch - Options	89.129.147 Tools Wizard	is Help							_10
	Home C	anniguration	Monitoring	Back	Forward	Q Search	Refr	esh Save	<b>?</b> Help		Cisco Syst
	Features	Configuration	n > Features > Pr	caerties >	AAA Setup :	AAA Server	5				
		* <u>*</u> *	127   127   38   abus - ■	84 🛍 🗊	: 范 () () - · · · ·						
	Interfaces	- MAIS	A Server Grou	Add ar	nvers nd configure	AAA servers	for exis	ting AAA server	groups. To c	onfigure server gr	roups
	Security Policy	- Au	th. Prompt	go to t	he <u>AAA Berv</u>	er Groups s	reen.				
	234	E- @Advan	ced ti-Spoofing	Imv	Sever Gro authient	up (Protocol) Carin		Interface inside	Server IP.	Address Time	10
	NAT	- DTC	egment P Options								
	SK VPN	- Contin	necuts Static Table								
	4 <u>2</u> 6	E P DHCF	) pdate 9 Services								Tesi
	Routing	F-∲DH L-∳DH	ICP Server								$\sim$
	Building Blocks	}	Client er								
	提供使用者	■: ■IIII 名稱和容	ःःः	使用者	音名稱 :	測試和	密碼	: 測試)	然後按·	一下 <b>OK</b> 以诸	進行驗證。
	付 Test AA	A Serve	er -172.22	.1.100					×		
	To test	the follow	wing AAA :	server	enter us	sername	and				
	passw	ord.									
	ДДД	Server (	Group: m	iy auth	nent arp	) (Kerbei	os)				
			·	-			ŕ				
	Host	t	17	72.22.1	.100						
	0.	Authoriza	ation 🕻	🖲 Auth	nenticati	on					
	User	rname:		test							
				1001							
	Pass	word:		***							
				,							
			ок			Cancel					
1			in Inf	ormal	tion						>
				orma							ŕ
				•							
				Ų.	Aut	henticati	on te	st to host	172.22.1	.100 is suc	cessful.
								ОК			

3. 您可以看到驗證成功。

# <u>疑難排解</u>

- 身份驗證失敗的一個常見原因是時鐘偏差。確保PIX或ASA上的時鐘與您的身份驗證伺服器同步。當身份驗證因時鐘偏差而失敗時,您會收到以下錯誤消息: 300.此外,還會顯示以下日誌消息:%PIX|ASA-3-113020:Kerberosip\_address300 ip\_address Kerberos伺服器的IP地址。當通過Kerberos伺服器對IPSec或WebVPN使用者進行身份驗證失敗時,會顯示此消息,因為安全裝置和伺服器上的時鐘間隔超過五分鐘(300秒)。發生這種情況時,連線嘗試被拒絕。為了解決此問題,請同步安全裝置和Kerberos伺服器上的時鐘。
- 2. 必須禁用Active Directory(AD)上的預身份驗證,否則可能會導致使用者身份驗證失敗。
- 3. VPN客戶端使用者無法對Microsoft證書伺服器進行身份驗證。出現以下錯誤消息:""14 要解決此問題,請取消選中身份驗證伺服器上的Do not require kerberose preauthentication覈取方塊。

## 相關資訊

- 配置AAA伺服器和本地資料庫
- Cisco ASA 5500系列自適應安全裝置產品支援
- <u>Cisco PIX防火牆軟體</u>
- <u>Cisco Secure PIX防火牆命令參考</u>
- 安全產品現場通知(包括PIX)
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems