為WLC和Microsoft Windows 2003 IAS Server配 置RADIUS IPSec安全

目錄

簡介 必要條件 需求 採用元件 慣例 IPSec RADIUS組態 設定WLC 配置IAS Microsoft Windows 2003域安全設定 Windows 2003系統日誌事件 無線LAN控制器RADIUS IPSec成功調試示例 Ethreal捕獲 相關資訊

<u>簡介</u>

本指南介紹如何配置WCS和以下WLAN控制器支援的RADIUS IPSec功能:

- •4400系列
- WiSM
- 3750G

控制器RADIUS IPSec功能位於控制器GUI上的**Security > AAA > RADIUS Authentication Servers**部 分下。此功能提供使用IPSec加密控制器和RADIUS伺服器(IAS)之間的所有RADIUS通訊的方法。

必要條件

<u>需求</u>

思科建議您瞭解以下主題:

- LWAPP知識
- 有關RADIUS驗證和IPSec的知識
- 有關如何在Windows 2003 Server作業系統上配置服務的知識

<u>採用元件</u>

若要部署控制器RADIUS IPSec功能,必須安裝和設定以下網路和軟體元件:

- •WLC 4400、WiSM或3750G控制器。此範例使用執行5.2.178.0版軟體的WLC 4400
- 輕型存取點(LAP)。本示例使用1231系列LAP。
- 具有DHCP的交換機
- Microsoft 2003伺服器配置為域控制器,安裝有Microsoft Certificate Authority和Microsoft Internet Authentication Service(IAS)。
- Microsoft域安全
- Cisco 802.11 a/b/g無線客戶端介面卡,帶ADU 3.6版,配置了WPA2/PEAP

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>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

<u>IPSec RADIUS組態</u>

本配置指南未涉及Microsoft WinServer、證書頒發機構、Active Directory或WLAN 802.1x客戶端的 安裝或配置。在部署控制器IPSec RADIUS功能之前,必須安裝和配置這些元件。本指南的其餘部 分介紹如何在以下元件上配置IPSec RADIUS:

- 1. Cisco WLAN控制器
- 2. Windows 2003 IAS
- 3. Microsoft Windows域安全設定

<u>設定WLC</u>

本節介紹如何透過GUI在WLC上設定IPSec。

在控制器GUI上,完成以下步驟。

 在控制器GUI中導覽至Security > AAA > RADIUS Authentication索引標籤,然後新增一個 RADIUS伺服器。

Cisco Systems	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	co
Security	RADIUS	Authenticatio	n Servers				
AAA General	Call Stat	ion ID Type	IP Address	~			
RADIUS Authentication RADIUS Accounting Local Net Users	Credenti	als Caching					
MAC Filtering Disabled Clients	Use AES	Key Wrap					
AP Policies	Network	Managemen	Server	Server Address	5 Port	IPSec	
Access Control Lists	User		Index				
IPSec Certificates		<u>1999</u> 999	1	192.168.30.10	1812	Disabled	
CA Certificate ID Certificate		V	3	192.168.30.105	1812	Enabled	

2. 配置新RADIUS伺服器的IP地址、埠1812和共用金鑰。選中**IPSec Enable**覈取方塊,配置這些 IPSec引數,然後按一下**Apply**。**注意:**共用金鑰既用於對RADIUS伺服器進行身份驗證,又用 作IPSec身份驗證的預共用金鑰(PSK)。

Cisco Systems	MONITOR WLANS	CONTROLL	ER WIRELESS	SECURITY	MANAGEMEN		
Security	Shared Secret		•••]		
AAA General RADIUS Authentication	Confirm Shared Secret		•••				
RADIUS Accounting Local Net Users MAC Filtering	Key Wrap						
Disabled Clients User Login Policies AP Policies	Port Number		1812				
Access Control Lists	Server Status		Enabled 💙				
IPSec Certificates CA Certificate	Support for RFC 35	76	Disabled 💙				
ID Certificate	Retransmit Timeou	ıt	2 seconds				
Wireless Protection	Network User		🖉 Enable				
Policies			EJ ENGDIE				
Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies	Management		🗹 Enable				
	IPSec		Enable				
AP Autoentication	IPsec Parameters						
	IPSec		HMAC SHA1 💌				
	IPSEC Encryption		3DES 💙				
	(Shared Seceret will	be used as t	he Preshared Key)				
	IKE Phase 1		Main 💌				
	Lifetime (seconds)		28800				
	IKE Diffie Hellman G	roup	Group 2 (1024 bits) 🖌			

<u>配置IAS</u>

在IAS上完成以下步驟:

1. 導航到Win2003中的IAS管理器並新增新的RADIUS客戶端。

Elle Action View Help				
⇔ → 🗈 📧 🛍 🚱 😫				
Internet Authentication Service (Local)	Friendly Name	Address	Protocol	Client-Vendor
RADIUS Clients Remote Access Logging	<u>1</u> 4404	192.168.30.2	RADIUS	RADIUS Standar
E 🕎 Remote Access Policies				
Connection Request Processing				

2. 使用控制器上配置的IP地址和共用金鑰配置RADIUS客戶端屬性

04 Properties						?
Settings						
Eriendly name:						
<mark>4404</mark> (1997) (1997)						
Address (IP or DNS):						
192.168.30.2						
Verify						
If you are using remote attribute, specify the ve Client-Vendor:	access endor of	policies ba the RADIU US Standar	ised on IS client	the client t.	vendor's	.
<u>R</u> equest must cont	ain the l	Message A	uthentic	ator attrib	ute	السطي
<u>S</u> hared secret:						
Confirm shared secret:						

3. 為控制器配置新的遠端訪問策略



4. 編輯控制器遠端訪問策略的屬性。確保新增NAS埠型別 — 無線 — IEEE 802.11:

4404 Properties	NAS-Port-Type	<u> </u>
Settings Specify the conditions that connection requests must match. Policy gonditions: NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 OR Wireless Add Edt Bemove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.	Available types: ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110 ISDN Async V.120 ISDN Sync	Selected types: Ethemet Wireless - IEEE 802.11 Wireless - Other
Edit Profile Unless individual access permissions are specified in the user profile, this policy controls access to the network. If a connection request matches the specified conditions:	Color Bin	

5. 按一下Edit Profile,按一下Authentication頁籤,然後選中MS-CHAP v2進行身份驗證

:

Ed	it Dial-in Profile		
Policy <u>c</u> onditions: NAS-Port-Type n	Dial-in Constraints Authentication	IP Encryption whods you want to allow	Multilink Advanced for this connection.
▲	EAP Methods	uthentication version <u>2</u> (MS-CHAP v2)
f connection requ associated profile	User can <u>c</u> hang	ge password after it has (uthentication (MS-CHAF	expired ?)
Edit <u>P</u> rofile	📕 Uger can chang	ge password after it has (expired
Jnless individual Jolicy controls ac	Encrypted authenticat Unencrypted authenticat	ion (CHAP) cation (PAP, SPAP)	
O De <u>n</u> y remote ≀ ● <u>G</u> rant remote √	Onauthenticated access- Allow clients to conne method.	ct without negotiating ar	n authentication

6. 按一下**EAP Methods**,選擇EAP Providers,並將PEAP新增為EAP型別

:

Edit Dial-in Profile		<u>?</u> ×	1	
Dial-in Constraints	IP IP	Multilink		
Authentication	Encryption	Advanced		
Select the authentication	methods you want to allow	for this connection.		
EAP Methods				
Microsoft Encrypt	elect EAP Providers			<u>? ×</u>
🗖 User can <u>c</u>	EAP types are negotiated	in the order in which they	are listed.	
Microsoft Encrypt	EAP types:			
🗖 Uger can c	Protected EAP (PEAP)			Move <u>U</u> p.
Encrypted auther				Move Down
Unencrypted auti				
Unauthenticated acc				
Allow clients to commethod.				
	<u>A</u> dd <u>E</u> dit	<u>R</u> emove	ОК	Cancel
	OK Ca	ncel <u>Apply</u>		

7. 按一下Select EAP Providers上的Edit,然後從下拉選單中選擇與您的Active Directory使用者 帳戶和CA關聯的伺服器(例如tme.tme.com)。新增EAP型別MSCHAP v2:

elect EAP Providers	CCX0-001010101000		?×	PLOXO CROPUCKOSO COSO CINONO KINICIKO KOKO NAMONI CINO KOKOKO	
EAP types are negotiated in the r EAP types:	Protected EAP Prope This server identifies it Select the certificate t	nties self to callers before hat you want it to us	the connection is completed. se as proof of identity.	<u>? ×</u>	
Protected EAP (PEAP)	Certificate (ssued	tme.tme.com			
	Friendly name: Issuer:	wnbu			
	Expiration date:	3/30/2007 3:3 inect	2:22 PM		
<u>A</u> dd <u>E</u> dit	Eap Types Secured password (E/	AP-MSCHAP v2)	EAP MSCHAPy2 Properties		×
UK Cancel		1	Number of authentication retri	es: 2	
	Add	Edit Remo	Allow client to change pass	word after it has exp	ired
			ОК	Cancel	

8. 按一下Encryption頁籤,並檢查遠端訪問的所有加密型別

t Dial-in Profile		1
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
The following encryption is Routing and Remote Accor make sure the encryption If No encryption is the only	evels are supported by se ess. If you use a different levels you select are sup y option selected, then us	ervers running Microsoft remote access server, ported by that software. ers cannot connect by
using data encryption.		
Basic encryption (MF)	PE 40-bit)	
Strong encryption (M	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
☑ No encryption		
	OK 0	Cancel Apply

9. 按一下**Advanced** 頁籤,然後將RADIUS Standard/Framed新增為Service-

Dial-in Profile		
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connect Access server. Attributes:	ion attributes to be retur	ned to the Remote
 Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
•		
Add <u>E</u> dit.	<u>R</u> emove	

Туре:

10. 按一下IP頁籤,然後選中Client may request an IP address。假設交換器或WinServer上啟用

Authoritication	Encruption	1 Advances
Dial-in Constraints	IP	Multilink
IP address assignment (Fram	ned-IP-Address)	
Server must supply an IF	o address	
Client may request an IP	address	
C Server settings determine	e IP address assignme	ent
C Assign a static IP addres	s 255 . 25	5 . 255 . 255
If an IP address assignment overrides these settings.	method is specified in	the user profile, it
IP hiters		
If your remote access server you can define the filters to a	is Microsoft Routing a apply during this conne	and Remote Acces action.
To control the packets this in click Input Filters.	nterface receives,	Input Filters
To control the packets this in Output Filters.	nterface sends, click	<u>O</u> utput Filters

了DHCP。

<u>Microsoft Windows 2003域安全設定</u>

完成以下步驟以配置Windows 2003域安全設定:

1. 啟動預設域安全設定管理器,並為無線網路(IEEE 802.11)策略建立新的安全策略。

http://www.common.com/commons/	
Eile Action View Help	
← → 🗈 🖬 😰 🗟 😫 🎽	
Becurity Settings	Name
🔁 🚰 Account Policies	WLAN Network Policy
🕀 🛃 Local Policies	
🕀 🛃 Event Log	
🗄 🧰 Restricted Groups	
🗄 🤐 System Services	
🗄 🧾 Registry	
🛨 🤷 File System	
Wireless Network (IEEE 802.11) Policies	

 開啟WLAN Network Policy Properties,然後點選Preferred Networks。新增新的首選WLAN並 鍵入您的WLAN SSID的名稱,例如Wireless。按兩下新首選網路,然後按一下IEEE 802.1x選 項卡。選擇PEAP作為EAP型別

:

LAN Network Policy Propertie	?×	
General Preferred Networks	Edit sroller Properties	?
	Network Properties IEEE 802.1x	
Automatically conne below.	Enable network access control using IEEE 802.1x	
	EAPOL-Start message: Transmit	
Networks:	Parameters (seconds)	
Network Name (SSID) IEE	Max start: 3 Start period: 60	
sroller E	Held period: 60 10 10 Authentication period: 30 10 10 10	
	EAP type: Protected EAP (PEAP)	· · · · · · · · · · · · · · · · · · ·
	Authenticate as guest when user or computer information is unavailable	
	Authenticate as computer when computer information is availab	le
A <u>d</u> d <u>E</u> dit	Computer authentication: With user re-authentication	
	ОК	Cancel

3. 按一下PEAP Settings,選中Validate server certificate,然後選擇證書頒發機構上安裝的受信 任的根證書。出於測試目的,取消選中MS CHAP v2覈取方塊「Automatically use my Windows login and password(自動使用我的Windows登入名和密碼)」。

Protected EAP Properties	<u>?×</u>
When connecting:	
☐ ✓ Validate server certificate	
Connect to these servers:	
Trusted <u>R</u> oot Certification Authorities:	
VeriSign Trust Network	
wnbu	
Xcert EZ by DST	
I	
	EAP MSCHAPv2 Properties
Select Authentication Method:	
Secured password (EAP-MSCHAP v2)	When connecting:
Enable Fast Reconnect	Automatically use my Windows logon name an password (and domain if any).
	OK Cancel

4. 在Windows 2003預設域安全設定管理器視窗中,在Active Directory策略上建立另一個新的 IP安全策略,**如4404**。_____

The Default Domain Security Settings Elle Action View Help ← → E III × P III (2) (2) 10 10 10 10 10 10 10 10 10 10 10 10 10	1.0		
Security Settings	Name A	Description	Policy Assigned
Account Policies	1404		Yes
🗄 🤯 Local Policies	Server (Request Secu	For all IP traffic, always req	No
🖻 🚮 Event Log	Client (Respond Only)	Communicate normally (uns	No
Restricted Groups	Secure Server (Requir	For all IP traffic, always req	No
System Services			
🖻 🛄 Registry			
Hie System			
T Wreless Network (IEEE 802.11) Policies			
Public Key Policies			

5. 編輯新的4404策略屬性,然後按一下Rules頁籤。新增新的過濾規則— IP檔案清單(動態);過濾操作(預設響應);身份驗證(PSK);隧道(無)。按兩下新建立的過濾器規則並選擇Security Methods:

404 Prop	berties				?×
Rules	General				
	g Security	rules for commun	icating with oth	er computers	
	,				
	urity rules:				
IP Filt	er List	Filter Actio	n [Authentication.	
₩ <0)ynamic>	Default Re	esponse	Preshared Key	<n< td=""></n<>
Ed	lit Rule Pro	perties			<u>Y</u> ×
	Security Met	hods Authentic	ation Methods		
	Offer these	convitu mathada	when negatist	ing with spaths	
	Uner mese	security methods	; when negotiat	ing with anothe	r computer.
	C				
	Security me	thod preference			
•	Lype	AH Integrity	2DES	ential ES	A <u>d</u> d
	Custom	<none></none>	3DES	ME	Edit
	Custom	<none></none>	DES	SH	·······
	Custom	<none></none>	DES	ME	<u>R</u> emove
	Custom	SHA1	<none></none>	<pre>KN</pre>	
	Lustom	MDO	<inone></inone>	< IN	Move <u>u</u> p
	4			•	Move down
	(and another			Lane.	
	-			(050)	
	Use se:	ssion <u>k</u> ey perfect	forward secrec	y (PFS)	

6. 按一下Edit Security Method,然後按一下Custom Settings單選按鈕。選擇這些設定。注意 :這些設定必須與控制器RADIUS IPSec安全設定匹配。

Edit Security Method	?×Ptraffic, alw	ays req.
Security Method		
 Integrity and encry Data will be encry unmodified. Integrity only Data will be verified encrypted. Qustom Settings 	Determine the settings for this custom security method.	<u>? ×</u>
	Session key settings: Generate a new key every: Generate a new key every: Seconds OK Cancelocation Cancel	ery:

7. 點選Edit Rule Properties下的Authentication Method頁籤。輸入先前在控制器RADIUS設定上 輸入的相同共用密碼。

it Rule Properties		? × ^{P traffic, alwa}
Security Methods Au Authent betwee offered compute	thentication Methods ication methods specify how trust is n computers. These authentication and accepted when negotiating se er.	s established methods are curity with another
Authentication metho	d preference order: Details	A <u>d</u> d
Presnared Ney	CISCO	<u>E</u> dit
-	Detween the computer Active Directory default (Kerberg	rs. os V5 protocol)
(Use a <u>c</u> ertificate from this certific	cation authority (CA):
	 Egolude the CA name from Enable certificate to account 	the certificate request int mapping
6	Use this string (preshared key)	

此時,控制器、IAS和域安全設定的所有配置都已完成。儲存控制器和WinServer上的所有配置,並 重新啟動所有電腦。在用於測試的WLAN客戶端上,安裝根證書並配置WPA2/PEAP。在客戶端上 安裝根證書後,請重新啟動客戶端電腦。所有電腦重新啟動後,將客戶端連線到WLAN並捕獲這些 日誌事件。

注意:要在控制器和WinServer RADIUS之間設定IPSec連線,需要客戶端連線。

Windows 2003系統日誌事件

成功為啟用IPSec RADIUS的WPA2/PEAP配置的WLAN客戶端連線會在WinServer上生成以下系統事件:

😽 Event Viewer							
Eile Action ⊻iew	Help						
← →	• 🗟 🗟 😰						
Event Viewer (Local)	System 22 eve	nt(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Security	Information	4/1/2006	2:52:42 PM	IAS	None	1	N/A

```
User TME0\Administrator was granted access.
Fully-Qualified-User-Name = tme.com/Users/Administrator
NAS-IP-Address = 192.168.30.2
NAS-Identifier = Cisco_40:5f:23
Client-Friendly-Name = 4404
Client-IP-Address = 192.168.30.2
Calling-Station-Identifier = 00-40-96-A6-D4-6D
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = 4404
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)
成功的控制器<> RADIUS IPSec連線在WinServer日誌上生成此安全事件:
```

😫 Event Viewer							
Ele Action View E	<u>H</u> elp						
← → <a>Im	2 🗟 😫						
Event Viewer (Local)	Security 484 ev	ent(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Security System	Success Audit	4/1/2006	2:22:25 PM	Security	Logor/Logoff	541	NETWORK SERVICE

IKE security association established. Mode: Data Protection Mode (Quick Mode) Peer Identity: Preshared key ID. Peer IP Address: 192.168.30.2 Filter: Source IP Address 192.168.30.105 Source IP Address Mask 255.255.255.255 Destination IP Address 192.168.30.2 Destination IP Address Mask 255.255.255.255 Protocol 17 Source Port 1812 Destination Port 0 IKE Local Addr 192.168.30.105 IKE Peer Addr 192.168.30.2 IKE Source Port 500 IKE Destination Port 500 Peer Private Addr Parameters: ESP Algorithm Triple DES CBC HMAC Algorithm SHA AH Algorithm None Encapsulation Transport Mode InboundSpi 3531784413 (0xd282c0dd)

OutBoundSpi 4047139137 (0xf13a7141) Lifetime (sec) 28800 Lifetime (kb) 100000 QM delta time (sec) 0 Total delta time (sec) 0

無線LAN控制器RADIUS IPSec成功調試示例

您可以在控制器上使用debug指令debug pm ikemsg enable以驗證此組態。以下提供範例。

```
(Cisco Controller) >debug pm ikemsg enable
(Cisco Controller) >****** ERR: Connection timed out or error, calling callback
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x0000000000000000
SA: doi=1 situation=0x1
Proposal 0, proto=ISAKMP, # transforms=1, SPI[0]
Transform#=0 TransformId=1, # SA Attributes = 6
EncrAlgo = 3DES-CBC
HashAlgo = SHA
AuthMethod = Pre-shared Key
GroupDescr =2
LifeType = secs
LifeDuration =28800
VID: vendor id[16] = 0x8f9cc94e 01248ecd f147594c 284b213b
VID: vendor id[16] = 0x27bab5dc 01ea0760 ea4e3190 ac27c0d0
VID: vendor id[16] = 0x6105c422 e76847e4 3f968480 1292aecd
VID: vendor id[16] = 0x4485152d 18b6bbcd 0be8a846 9579ddcc
VID: vendor id[16] = 0xcd604643 35df21f8 7cfdb2fc 68b6a448
VID: vendor id[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
VID: vendor id[16] = 0x7d9419a6 5310ca6f 2c179d92 15529d56
VID: vendor id[16] = 0x12f5f28c 457168a9 702d9fe2 74cc0100
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
SA: doi=1 situation=0x1
Proposal 1, proto=ISAKMP, # transforms=1 SPI[0]
Transform payload: transf#=1 transfId=1, # SA Attributes = 6
EncrAlgo= 3DES-CBC
HashAlgo= SHA
GroupDescr=2
AuthMethod= Pre-shared Key
LifeType= secs
LifeDuration=28800
VENDOR ID: data[20] = 0x1e2b5169 05991c7d 7c96fcbf b587e461 00000004
VENDOR ID: data[16] = 0x4048b7d5 6ebce885 25e7de7f 00d6c2d3
VENDOR ID: data[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9644af13 b4275866 478d294f d5408dc5 e243fc58...
NONCE: nonce [16] = 0xede8dc12 c11be7a7 aa0640dd 4cd24657
PRV[payloadId=130]: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6
c67
PRV[payloadId=130]: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b1
378
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9f0420e5 b13adb04 a481e91c 8d1c4267 91c8b486...
NONCE: nonce[20] = 0x011a4520 04e31ba1 6089d2d6 347549c3 260ad104
PRV payloadId=130: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b13
78
PRV payloadId=130: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6c
67
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
```

```
ookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x04814190 5d87caal 221928de 820d9f6e ac2ef809
NOTIFY: doi=1 proto=ISAKMP type=INITIAL_CONTACT, spi[0]
NOTIFY: data[0]
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1b1d1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1, SPI[4] = 0xbb243261
Transform#=1 TransformId=3, # SA Attributes = 4
AuthAlgo = HMAC-SHA
LifeType = secs
LifeDuration =28800
EncapMode = Transport
NONCE: nonce [16] = 0x48a874dd 02d91720 29463981 209959bd
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x2228d010 84c6014e dd04ee05 4d15239a 32a9e2ba
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1 SPI[4] = 0x7d117296
Transform payload: transf#=1 transfId=3, # SA Attributes = 4
LifeType= secs
LifeDuration=28800
EncapMode= Transport
AuthAlgo= HMAC-SHA
NONCE: nonce[20] = 0x5c4600e4 5938cbb0 760d47f4 024a59dd 63d7ddce
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0xcb862635 2b30202f 83fc5d7a 2264619d b09faed2
NOTIFY: doi=1 proto=ESP type=CONNECTED, spi[4] = 0xbb243261
data[8] = 0x434f4e4e 45435431
```

<u>Ethreal 捕獲</u>

以下是Ethreal Capture示例。

```
192.168.30.105 = WinServer
192.168.30.2 = WLAN Controller
192.168.30.107 = Authenticated WLAN client
No. Time Source Destination Protocol Info
1 0.000000 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
2 1.564706 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
3 1.591426 192.168.30.105 192.168.30.2 ESP ESP (SPI=0x7d117296)
4 1.615600 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
5 1.617243 192.168.30.105 192.168.30.2 ESP ESP (SPI=0x7d117296)
6 1.625168 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
7 1.627006 192.168.30.105 192.168.30.2 ESP ESP (SPI=0x7d117296)
8 1.638414 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
```

9 1.639673 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261) 10 1.658440 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296) 11 1.662462 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261) 12 1.673782 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296) 13 1.674631 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261) 14 1.687892 192.168.30.2 192.168.30.105 ESP (SPI=0x7d117296) 15 1.708082 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261) 16 1.743648 192.168.30.107 Broadcast LLC U, func=XID; DSAP NULL LSAP Individual, SSAP NULL LSAP Command 17 2.000073 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003 18 4.000266 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003 19 5.062531 Cisco_42:d3:03 Cisco_42:d3:03 LOOP Reply 20 5.192104 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00> 21 5.942171 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00> 22 6.000242 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003 23 6.562944 192.168.30.2 192.168.30.105 ARP Who has 192.168.30.105? Tell 192.168.30.2 24 6.562982 192.168.30.105 192.168.30.2 ARP 192.168.30.105 is at 00:40:63:e3:19:c9 25 6.596937 192.168.30.107 Broadcast ARP 192.168.30.107 is at 00:13:ce:67:ae:d2

相關資訊

- <u>思科無線LAN控制器組態設定指南5.2版</u>
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。