و WLCs مداخل RADIUS IPSec نامأ نيوكت Microsoft Windows 2003 IAS

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المكونات المستخدمة <u>الاصطلاحات</u> <u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u> <u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u> <u>اعدادات أمان المجال ل Microsoft Windows 2003</u> <u>أحداث سجل النظام ل Windows 2003 لوحدة تحكم الشبكة المحلية اللاسلكية (RADIUS أسر إثريالي.</u>

<u>المقدمة</u>

يوثق هذا الدليل كيفية تكوين ميزة RADIUS IPSec التي يدعمها WCS ووحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) التالية:

- السلسلة 4400
 - WiSM •
 - 3750G•

توجد ميزة Controller RADIUS IPSec على واجهة المستخدم الرسومية (GUI) لوحدة التحكم **ضمن قسم الأمان >** AAA > **خوادم مصادقة RADIUS**. توفر هذه الميزة طريقة لتشفير جميع إتصالات RADIUS بين وحدات التحكم وخوادم IAS) RADIUS) باستخدام IPSec.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة حول LWAPP
- معرفة مصادقة RADIUS و IPSec
- معرفة كيفية تكوين الخدمات على نظام تشغيل Windows 2003 Server

<u>المكونات المستخدمة</u>

يجب تثبيت مكونات الشبكة والبرامج هذه وتكوينها من أجل نشر ميزة IPSec في بروتوكول RADIUS لوحدة التحكم:

- وحدات التحكم WLC 4400 أو WiSM أو 3750G. يستعمل هذا مثال WLC 4400 أن يركض برمجية صيغة 5.2.178.0
- نقاط الوصول Lightweight (LAPs). يستخدم هذا المثال نقطة الوصول في الوضع Lightweight من السلسلة 1231.
 - التبديل باستخدام DHCP
 - تم تكوين خادم Microsoft 2003 كوحدة تحكم بالمجال مثبتة بواسطة "مرجع شهادات Microsoft" و"خدمة مصادقة إنترنت IAS): (Microsoft).
 - أمان مجال Microsoft
 - مهايئ عميل لاسلكي Cisco 802.11 a/b/g مع ADU الإصدار 3.6 مكون مع WPA2/ PEAP

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>الاصطلاحات</u>

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

تكوين IPSec RADIUS

لا يتناول دليل التكوين هذا تثبيت أو تكوين عميل Microsoft WinServer أو Certificate Authority أو Active Directory أو WLAN 802.1x. يجب تثبيت هذه المكونات وتكوينها قبل نشر ميزة IPSec RADIUS لوحدة التحكم. يوثق الجزء المتبقي من هذا الدليل كيفية تكوين IPSec RADIUS على هذه المكونات:

- 1. وحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco
 - Windows 2003 IAS .2
 - 3. إعدادات أمان Microsoft Windows Domain

<u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u>

يشرح هذا القسم كيفية تكوين IPSec على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال واجهة المستخدم الرسومية (GUI).

من واجهة المستخدم الرسومية (GUI) لوحدة التحكم، أكمل الخطوات التالية.

1. انتقل إلى علامة التبويب **أمان > AAA > مصادقة RADIUS** في واجهة المستخدم الرسومية (GUI) لوحدة التحكم، وأضف خادم RADIUS جديد.

Cisco Systems	MONITOR	WLANE CO			CURITY	MANAGEMENT	s
Security	RADIUS /	Authenticatio	n Servers	MINELESS	JEGONITI	MANAGEMENT	
AAA General	Call Stat	ion ID Type	IP Address	~			
RADIUS Authentication RADIUS Accounting Local Net Users	Credenti	als Caching					
MAC Filtering Disabled Clients User Login Policies	Use AES	Key Wrap					
AP Policies	Network	Management	Server	Server Address	Port	IPSec	
Access Control Lists	User		Index				
IPSec Certificates			1	192.168.30.10	1812	Disabled	
CA Certificate			3	192.168.30.105	1812	Enabled	

2. قم بتكوين عنوان IP، المنفذ 1812، وسر مشترك لخادم RADIUS الجديد. حدد خانة الاختيار I**PSec enable-**، وقم بتكوين معلمات IPSec هذه، ثم انقر فوق **تطبيق**.**ملاحظة:** يتم إستخدام السر المشترك لمصادقة خادم RADIUS وكمفتاح مشترك مسبقا (PSK) لمصادقة IPSec.

Cisco Systems			
All the second sec	MONITOR WLANS COI	NTROLLER WIRELESS	SECURITY MANAGEMEN
Security	Shared Secret	•••	
AAA General RADIUS Authentication	Confirm Shared Secret	•••	
RADIUS Accounting Local Net Users	Key Wrap		
Disabled Clients User Login Policies	Port Number	1812	
AP Policies Access Control Lists	Server Status	Enabled 💙	
IPSec Certificates CA Certificate	Support for RFC 3576	Disabled 💌	
ID Certificate	Retransmit Timeout	2 seconds	
Web Auth Certificate			
Wireless Protection Policies	Network User	🗹 Enable	
Trusted AP Policies Rogue Policies	Management	🗹 Enable	
Custom Signatures Client Exclusion Policies	IPSec	🗹 Enable	
AP Authentication	IPsec Parameters		
	IPSec	HMAC SHA1 🔽	
	IPSEC Encryption	3DES 💙	
	(Shared Seceret will be us	ed as the Preshared Key)	
	IKE Phase 1	Main 🖌	
	Lifetime (seconds)	28800	
	IKE Diffie Hellman Group	Group 2 (1024 bits)	V



أتمت هذا steps على ال IAS:

1. انتقل إلى مدير IAS في Win2003 وأضف عميل RADIUS

جديدا.

Internet Authentication Service				_101 >
Eile 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 Standard
Kemote Access Policies Connection Request Processing				

2. قم بتكوين خصائص عميل RADIUS باستخدام عنوان IP والسر المشترك الذي تم تكوينه على وحدة

4 Properties		? ×
ettings		
Friendly name:		
1404 ·		
ddress (IP or DNS):		
92.168.30.2		
⊻erify		
f you are using remote attribute, specify the v	e access policies based on the client vendor's vendor of the RADIUS client.	
Cli <u>e</u> nt-Vendor:	RADIUS Standard	•
<u>R</u> equest must cor	ntain the Message Authenticator attribute	
hared secret:	XXXXXXXX	
onfirm shared secret	******	
	OK Cancel Ap	ply
		••••••

3. تكوين نهج وصول عن بعد جديد لوحدة التحكم:

🎾 Internet Authentication Service		
Ele Action View Help		
← → 🗈 🖬 🚱 🚱 😫		
Internet Authentication Service (Local)	Name	Order
RADIUS Clents Remote Access Logging Remote Access Policies	S 4404	1
E Connection Request Processing		

4. تحرير خصائص نهج الوصول عن بعد لوحدة التحكم. تأكد من إضافة نوع منفذ NAS - لاسلكي - IEEE 802.11:

4404 Properties	NAS-Port-Type	<u> </u>
Settings Specify the conditions that connection requests must match.	Agailable types: ADSL-CAP - Asymmetri ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Asses Modema	Selected types: Ethemet Wireless - IEEE 80211
Policy gonditions: NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 OR Wireless Add Edt Edt Eemove If connection requests match the conditions specified in this policy, the	Async (wodelin) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110 ISDN Async V.120 ISDN Sync	Wileiess - Other
Associated profile will be applied to the connection. 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: Degy remote access permission OK Cancel Apply	Recycle Bn	

5. انقر على **تحرير ملف التعريف**، وانقر فوق علامة التبويب **المصادقة**، ثم تحقق من MS-CHAP V2 للمصادقة:

4404 Properties	201 ? ×
Settings	
Specify the condit	dit Dial-in Profile 🔹 🔀 🔀
Policy <u>c</u> onditions: NAS-Port-Type m	Dial-in Constraints IP Multilink Authentication Encryption Advanced
A <u>d</u> d	EAP Methods Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP v2)
If connection requ associated profile	User can <u>change</u> password after it has expired Microsoft Encrypted Authentication (MS-CHAP)
Edit <u>P</u> rofile	User can change password after it has expired
Unless individual - policy controls ac:	Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP)
If a connection re C De <u>n</u> y remote a	Unauthenticated access
<u>G</u> rant remote	Allow clients to connect without negotiating an authentication method.
	OK Cancel Apply

6. انقر على **أساليب EAP**، وحدد مزودي EAP، واضيف PEAP كنوع EAP:

Edit Dial-in Profile			? ×]	
Dial-in Constraints	I IP	1	Multilink		
Authentication	Encryption	1. 1	Advanced		
Select the authentication	i methods you want to	allow for this	connection.		
EAP Methods					
Microsoft Encrypt	Select EAP Provide	:rs			<u>?×</u>
🗖 User can <u>c</u>	EAP types are nego	tiated in the or	der in which they	are listed.	
Microsoft Encrypt	EAP types:				
🗖 Uger can c	Protected EAP IPE	AP)			Move <u>U</u> p.
Encrypted auther					Move Down
Unencrypted aut					
Unauthenticated acc					
Allow clients to ci method.					
	Add	<u>E</u> dit	<u>R</u> emove	ОК	Cancel
	ОК	Cancel	Apply		

7. انقر على **تحرير** في تحديد موفري EAP واختر من القائمة المنسدلة الخادم المقترن بحسابات مستخدمي Active Directory و CA (على سبيل المثال، tme.tme.com). إضافة نوع EAP MSCHAP v2:

Select EAP Providers			?×	CORRECT CORREC	
EAP tupes are peoplisted in the s	Protected EAP Prope	ties		<u> 1 × </u>	
EAP types: EAP types: Protected EAP (PEAP)	This server identifies it: Select the certificate th	self to callers befor hat you want it to u	e the connection is completed. se as proof of identity.		
	Certificate (ssued	tme.tme.com			
	Friendly name:				
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:3	32:22 PM		
	Enable Fast Recon	nect			
<u>A</u> dd <u>E</u> dit	Eap Types Secured password (EA	P-MSCHAP v2)			.
OK L Cancel			CAP MSCHAPY2 Propercies		~
			Number of authentication retrie	s: 2	
	Add	Edit Rem	Allow client to change passi	word after it has expired	
			OK	Cancel	

8. انقر فوق علامة التبويب **التشفير**، وفحص جميع أنواع التشفير للوصول عن

Dial-in Profile		<u>? ×</u>
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
The following encryption le Routing and Remote Acce make sure the encryption I If No encryption is the only	evels are supported by ser ess. If you use a different r evels you select are supp option selected, then use	vers running Microsoft emote access server, orted by that software. ers cannot connect by
using data encryption.		
Basic encryption (MP	PE 40-bit)	
Strong encryption (MI	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
☑ No encryption		
	ОК С	ancel <u>A</u> pply

9. انقر فوق علامة التبويب **خيارات متقدمة**، وقم بإضافة RADIUS Standard/Framed كنوع

Dial-in Profile		?×
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connection Access server.	attributes to be return	ned to the Remote
Attri <u>b</u> utes:		
Name	Vendor	Value
•		Þ
▲ <u>dd</u> <u>E</u> dit	<u>R</u> emove	

10. انقر فوق علامة التبويب **IP**، وتحقق من **إمكانية طلب العميل لعنوان I**P. هذا يفترض أن أنت تتلقى DHCP يمكن على مفتاح أو

Authentication Encryption Advanced
Dial-in Constraints IP Multilink
address assignment (Framed-IP-Address)
Server must supply an IP address
Client may request an IP address
Server settings determine IP address assignment
Assign a static IP address 255 . 255 . 255 . 255
n IP address assignment method is specified in the user profile, it rrides these settings.
ilters
our remote access server is Microsoft Routing and Remote Access, can define the filters to apply during this connection.
control the packets this interface receives, <u>Input Filters</u>
control the packets this interface sends, click <u>O</u> utput Filters
OK Cancel Apply
OK Cancel <u>Apply</u>

إعدادات أمان المجال ل Microsoft Windows 2003

أكمل الخطوات التالية لتكوين إعدادات أمان مجال Windows 2003:

1. قم بتشغيل مدير إعدادات أمان المجال الافتراضية، وقم بإنشاء سياسة أمان جديدة لنهج الشبكة اللاسلكية (IEEE

🚡 Default Domain Security Settings	
Eile Action Yiew 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	

.(802.11

2. افتح خصائص نهج شبكة WLAN، وانقر فوق **الشبكات المفضلة**. أضف شبكة WLAN جديدة مفضلة واكتب اسم WLAN SSID، مثل . انقر نقرا مزدوجا على الشبكة المفضلة الجديدة ثم انقر على علامة التبويب **IEEE** B**02.1**x. أختر PEAP ليكون هو النوع EAP:

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

3. انقر على **إعدادات PEAP**، وتحقق من **التحقق من شهادة الخادم**، وحدد شهادة الجذر الموثوق بها المثبتة على المرجع المصدق. لأغراض الاختبار، قم بإلغاء تحديد مربع MS CHAP V2 لاستخدام تسجيل الدخول إلى Windows وكلمة المرور الخاصة بي تلقائيا.

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

4. في إطار إدارة إعدادات أمان المجال الافتراضية ل Windows 2003، قم بإنشاء نهج أمان IP جديدة أخرى على نهج Active Directory، مثل 4404.

🚡 Default Domain Security Settings							
Eile Action View Help							
Security Settings	Name A	Description	Policy Assigned				
E 🛃 Account Policies	111	ALL PROPERTY AND A DESCRIPTION	Yes				
E	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				
U System Services							
Wireless Network (IEEE 802.11) Policies							
Public Key Policies							
🔄 🧰 Software Restriction Policies							
IP Security Policies on Active Directory (tme.com)							

5. قم بتحرير خصائص نهج 4404 الجديدة، وانقر فوق علامة التبويب **قواعد**. إضافة قاعدة تصفية جديدة - قائمة ملفات IP (ديناميكية)؛ إجراء التصفية (الاستجابة الافتراضية)؛ المصادقة (PSK)؛ النفق (بلا). انقر نقرا مزدوجا على قاعدة المرشح التي تم إنشاؤها حديثا وحدد طرق

s Te	General General	rules for commun	icating with other cor	nputers		
Sec	urity rules:					
P Filt	ter List	Filter Actio	on Authe	entication.	Tu	
2 <[Dynamic>	Default R	esponse Presh	hared Key	<n< th=""><th></th></n<>	
Ec	dit Rule Prop	perties				? X
	Security Meth	hods Authentic	ation Methods			
		I. Institution				
	011 1	5 JL I				
	Offer these	security methods	s when negotiating wi	ith anothe	r computer.	
	Offer these	security methods	s when negotiating wi	ith anothe	r computer.	
	Offer these <u>S</u> ecurity me	security methods thod preference	s when negotiating wi order: ESP Confidential.	ith anothe	r computer. Add	1
	Offer these <u>S</u> ecurity me Type Custom	security methods thod preference AH Integrity <none></none>	s when negotiating wi order: ESP Confidential. 3DES	ith anothe ES SH	r computer.	
	Offer these Security me Type Custom Custom	security methods thod preference AH Integrity <none> <none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES	ith anothe <u>ES</u> SH ME	r computer.	
	Offer these Security me Type Custom Custom	security methods thod preference AH Integrity <none> <none> <none></none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES	ith anothe ES SH ME SH	r computer. A <u>d</u> d	
	Offer these Security me Type Custom Custom Custom Custom	security methods thod preference <u>AH Integrity</u> <none> <none> <none> <none></none></none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES DES	ith anothe <u>ES</u> SH MC SH MC SH	r computer. A <u>d</u> d Edit	
-	Offer these Security me Type Custom Custom Custom Custom	security methods thod preference AH Integrity <none> <none> <none> <none> SHA1</none></none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES DES SES SES	ith anothe SH ME SH ME KH	r computer. A <u>d</u> d Edit <u>R</u> emov	•
	Offer these Security me Type Custom Custom Custom Custom Custom Custom	security methods thod preference AH Integrity <none> <none> <none> <none> SHA1 MD5</none></none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES DES <none> <none></none></none>	ith anothe <u>ES</u> SH MC SH MC <n <n< td=""><td>r computer. A<u>d</u>d Edit <u>R</u>emov</td><td>e</td></n<></n 	r computer. A <u>d</u> d Edit <u>R</u> emov	e
	Offer these Security me Type Custom C	security methods thod preference AH Integrity <none> <none> <none> SHA1 MD5</none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES DES <none> <none></none></none>	ith anothe SH ME SH ME <n <n< td=""><td>r computer. A<u>d</u>d Edit <u>R</u>emov Move <u>u</u></td><td>e wn</td></n<></n 	r computer. A <u>d</u> d Edit <u>R</u> emov Move <u>u</u>	e wn
	Offer these Security me Type Custom C	security methods thod preference AH Integrity <none> <none> <none> SHA1 MD5</none></none></none>	s when negotiating wi order: ESP Confidential. 3DES 3DES DES DES <none> <none></none></none>	ith anothe SH ME SH ME <n <n< td=""><td>r computer. A<u>d</u>d Edit <u>R</u>emov Move <u>u</u></td><td>e wn</td></n<></n 	r computer. A <u>d</u> d Edit <u>R</u> emov Move <u>u</u>	e wn

6. انقر **تحرير أسلوب التأمين**، وانقر زر انتقاء **الإعدادات المخصصة**. أخترت هذا عملية إعداد.**ملاحظة:** يجب أن تتطابق هذه الإعدادات مع إعدادات أمان IPSec الخاصة بوحدة التحكم RADIUS.

Edit Security Method	? × P trattic, alway	s req
Security Method		
C Integrity and encry	ption	
Data will be encry unmodified.	Custom Security Method Settings	? ×
C Integrity only	Specify the settings for this custom security method.	
Data will be verific encrypted.	Data and address integrity without encryption (AH) Integrity algorithm:	
O Custom	MD5	
<u>S</u> ettings	Data integrity and encryption (ESP): Integrity algorithm: SHA1	
	Encryption algorithm:	
	Session key settings:	
	Generate a new key every: Generate a new key every	r.
	100000 Kbytes 28800 seconds	
	OK Cancel	

7. انقر فوق علامة التبويب **أسلوب المصادقة** ضمن خصائص قاعدة التحرير. أدخل نفس السر المشترك الذي أدخلته سابقا في تكوين RADIUS لوحدة التحكم.

Edit Rule Propertie	s	? >	C P traffic, always rec
Security Methods	Authentication Methods		
Auti betv offe com	nentication methods specify how veen computers. These authentic red and accepted when negotiati puter.	trust is established ation methods are ing security with another	
Authentication me	thod preference order:		
Preshared Key	cisco	<u>Aga</u>	
		<u>E</u> dit	
E	dit Authentication Method P	roperties	?×
	Authentication Method	on method specifies how tru nputers.	ist is established
	C Active Directory default (K)	erberos V5 protocol)	
	C Use a certificate from this (certification authority (CA):	
	_		Browse
	Exclude the CA name	from the certificate request account mapping	
	cisco		<u>^</u>

وعند هذه النقطة، يتم إكمال جميع التكوينات الخاصة بإعدادات وحدة التحكم و IAS وأمان المجال. قم بحفظ جميع التكوينات على كل من وحدة التحكم ونظام التشغيل WinServer وإعادة تمهيد جميع الأجهزة. على عميل WLAN الذي يتم إستخدامه للاختبار، قم بتثبيت الجذر والتكوين ل WPA2/PEAP. بعد تثبيت شهادة الجذر على العميل، أعد تشغيل جهاز العميل. بعد إعادة تمهيد جميع الأجهزة، قم بتوصيل العميل بالشبكة المحلية اللاسلكية (WLAN) والتقاط أحداث السجل هذه.

ملاحظة: يلزم اتصال عميل لإعداد اتصال IPSec بين وحدة التحكم و WinServer RADIUS.

أحداث سجل النظام ل Windows 2003

يقوم اتصال عميل شبكة WLAN الناجح الذي تم تكوينه ل WPA2/PEAP مع تمكين IPSec RADIUS بتوليد حدث النظام هذا على WinServer:

😽 Event Viewer							
Eile Action View	Help						
⇔ → 🗈 🖬 🖆	• 🖬 🗔 😭						
Event Viewer (Local)	System 22 eve	nt(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Security System	Information	4/1/2006	2:52:42 PM	IAS	None	1	N/A

```
.User TMEO\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
```

يقوم اتصال IPSec الخاص بوحدة التحكم الناجحة <> بإنشاء حدث الأمان هذا على سجلات WinServer:

😫 Event Viewer							
Ele Action View H	telp						
⇔ ⇒ 🗈 🖬 😭	2 🗟 😫						
Event Viewer (Local)	Security 484 ev	ent(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Security	Success Audit	4/1/2006	2:22:25 PM	Security	Logon/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

<u>مثال تصحيح أخطاء نجاح IPSec لوحدة تحكم الشبكة المحلية اللاسلكية RADIUS</u>

يمكنك إستخدام الأمر debug **pm ikemsg enable** على وحدة التحكم للتحقق من هذا التكوين. فيما يلي مثال.

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 = secsLifeDuration =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 5d87caa1 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>أسر إثريالي</u>

هنا عينة إلتقاط ثري.

WinServer = 192.168.30.105 WLAN Controller = 192.168.30.2 Authenticated WLAN client = 192.168.30.107 No. Time Source Destination Protocol Info .Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf 0.000000 1 Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003 (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.564706 2 (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.591426 3 (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.615600 4 (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.617243 5 (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.625168 6 (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.627006 7 (ESP ESP (SPI=0x7d117296 192.168.30.2 192.168.30.2 1.638414 8

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

<u>معلومات ذات صلة</u>

- <u>دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 5.2</u>
 - الدعم التقني والمستندات Cisco Systems

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