Configurer la sécurité IPSec RADIUS pour les WLC et le serveur IAS Microsoft Windows 2003

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Conventions Configuration IPSec RADIUS Configurer le WLC Configurer le WLC Configuration de l'IAS Paramètres de sécurité du domaine Microsoft Windows 2003 Événements du journal système Windows 2003 Exemple de débogage de réussite du contrôleur LAN sans fil RADIUS IPSec Capture Éthréenne Informations connexes

Introduction

Ce guide explique comment configurer la fonctionnalité RADIUS IPSec prise en charge par WCS et les contrôleurs WLAN suivants :

- Gamme 4400
- WiSM
- 3 750 G

La fonctionnalité Controller RADIUS IPSec est située sur l'interface graphique du contrôleur sous la section **Security > AAA > RADIUS Authentication Servers**. La fonctionnalité fournit une méthode pour vous de chiffrer toutes les communications RADIUS entre les contrôleurs et les serveurs RADIUS (IAS) avec IPSec.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances sur le LWAPP
- Connaissances sur l'authentification RADIUS et IPSec
- Connaissances sur la configuration des services sur le système d'exploitation Windows 2003 Server

Composants utilisés

Les composants réseau et logiciels suivants doivent être installés et configurés afin de déployer la fonctionnalité Controller RADIUS IPSec :

- Contrôleurs WLC 4400, WiSM ou 3750G. Cet exemple utilise le WLC 4400 qui exécute la version logicielle 5.2.178.0
- Points d'accès légers (LAP). Cet exemple utilise le LAP de la gamme 1231.
- Commutateur avec DHCP
- Serveur Microsoft 2003 configuré en tant que contrôleur de domaine installé avec Microsoft Certificate Authority et Microsoft Internet Authentication Service (IAS).
- Sécurité du domaine Microsoft
- Adaptateur client sans fil Cisco 802.11 a/b/g avec ADU version 3.6 configuré avec WPA2/PEAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configuration IPSec RADIUS

Ce guide de configuration ne traite pas de l'installation ou de la configuration de Microsoft WinServer, de l'autorité de certification, d'Active Directory ou du client WLAN 802.1x. Ces composants doivent être installés et configurés avant le déploiement de la fonctionnalité RADIUS IPSec du contrôleur. Le reste de ce guide explique comment configurer IPSec RADIUS sur ces composants :

- 1. Contrôleurs WLAN Cisco
- 2. IAS Windows 2003
- 3. Paramètres de sécurité du domaine Microsoft Windows

Configurer le WLC

Cette section explique comment configurer IPSec sur le WLC via l'interface graphique utilisateur.

Àpartir de l'interface utilisateur graphique du contrôleur, procédez comme suit.

 Accédez à l'onglet Security > AAA > RADIUS Authentication dans l'interface graphique du contrôleur, et ajoutez un nouveau serveur RADIUS.

CISCO SYSTEMS	MONITOR	WLANs C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	s co
Security	RADIUS A	uthenticatio	n Servers				
AAA General	Call Stati	on ID Type	IP Address	~			
RADIUS Authentication RADIUS Accounting	Gredenti	als Caching					
MAC Filtering Disabled Clients	Use AES I	Key Wrap					
AP Policies	Network User	Management	Server Index	Server Address	s Port	IPSec	
IDSec Certificates			1	192.168.30.10	1812	Disabled	
CA Certificate			3	192.168.30.105	1812	Enabled	

2. Configurez l'adresse IP, le port 1812 et un secret partagé du nouveau serveur RADIUS. Cochez la case IPSec Enable-, configurez ces paramètres IPSec, puis cliquez sur Apply.Remarque : le secret partagé est utilisé à la fois pour authentifier le serveur RADIUS et comme clé prépartagée (PSK) pour l'authentification IPSec.

Cisco Systems	MONITOR WLANS O	ONTROLLER	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	Server Status	181 En:	abled 🔽		
Access Control Lists					
IPSec Certificates CA Certificate	Support for RFC 3576	Dis	abled 💙		
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	V	Enable		
AP Authentication	IPsec Parameters				
	IPSec	HM	AC SHA1 🔽		
	IPSEC Encryption	3D	ES 🗸		
	(Shared Seceret will be	used as the P	reshared Key)		
	IKE Phase 1	Ma	in 🔽		
	Lifetime (seconds)	288	800		
	IKE Diffie Hellman Grou	Jp Gro	oup 2 (1024 bits) 🗸	

Configuration de l'IAS

:

Complétez ces étapes sur le SAI :

1. Accédez au gestionnaire IAS dans Win2003 et ajoutez un nouveau client RADIUS.

Internet Authentication Service				
Elle Action View Help				
	0		- ,	
Internet Authentication Service (Local)	Friendly Name	Address	Protocol	Client-Vendor
RADIUS Clients Remote Access Logging	<u>]</u> 4404	192.168.30.2	RADIUS	RADIUS Standard
🕀 💐 Remote Access Policies				
Connection Request Processing				

2. Configurez les propriétés du client RADIUS avec l'adresse IP et le secret partagé configurés sur le contrôleur

04 Properties				11
Settings				
Eriendly name:				
4404				
Address (IP or DNS	5):			
192.168.30.2				
Verifu				
If you are using ren			al and the allowed the	ndor's
attribute, specify th	note access p le vendor of ti	he RADIUS	client.	
attribute, specify th	note access p le vendor of ti RADIU	bolicies base he RADIUS S Standard	a on the client ve client.	
Client-Vendor:	note access p ie vendor of th RADIU: contain the M	oolicies base he RADIUS S Standard essage Auth	a on the client ve client. nenticator attribute	
Client-Vendor:	note access p le vendor of th RADIU: contain the M	S Standard essage Auth	a on the client ve client. nenticator attribute	
attribute, specify th Client-Vendor: Image: Request must of shared secret: Shared secret: Confirm shared sec	note access p le vendor of th RADIU: contain the M	S Standard essage Auth	a on the client ve client. nenticator attribute	
attribute, specify th Client-Vendor: <u>B</u> equest must of <u>S</u> hared secret: Confirm shared sec	note access p le vendor of th RADIU: contain the M	S Standard essage Auth	a on the client ve client. henticator attribute	
Tribute, specify th Client-Vendor: <u>R</u> equest must of <u>S</u> hared secret: Confirm shared sec	note access p le vendor of th RADIU: contain the M	S Standard essage Auth	a on the client ve client. henticator attribute	

3. Configurez une nouvelle stratégie d'accès à distance pour le contrôleur

🐤 Internet Authentication Service		
Ele Action Yiew Help		
← → 💽 🖬 🛃 🛃 😰		
Internet Authentication Service (Local)	Name	Order
ADIUS Clients Remote Access Logging	\$\$ 4404	1
Remote Access Policies Connection Request Processing		

4. Modifiez les propriétés de la stratégie d'accès à distance du contrôleur. Veillez à ajouter le type de port NAS - Sans fil - IEEE 802.11

Settings	Augilable turger		Calastad himes:
Specify the conditions that connection requests must match. Policy gonditions: NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 OR Wireless Add Edt Edt Emove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.	ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.120 ISDN Async V.120	<u>A</u> dd >> << <u>R</u> emove	Ethernet Writeless - IEEE 80211 Writeless - 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: O Degy remote access permission G Grant remote access permission OK Cancel Apply	Contraction Recycle Bin		

5. Cliquez sur **Edit Profile**, cliquez sur l'onglet **Authentication**, et vérifiez MS-CHAP v2 for Authentication

:

Ed Specify the condit	t Dial-in Profile	3
Policy <u>c</u> onditions: NAS-Port-Type n	Dial-in Constraints IP M Authentication Encryption Ad Select the authentication methods you want to allow for this co	Aultilink Ivanced nnection.
	EAP Methods	
A <u>d</u> d	Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP)	v2)
f connection requassociated profile	User can change password after it has expired <u>Microsoft Encrypted Authentication (MS-CHAP)</u>	
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)	
f a connection re © De <u>n</u> y remote a	- Unauthenticated access	
Grant remote .	Allow clients to connect without negotiating an authentic method.	ation

6. Cliquez sur **Méthodes EAP**, sélectionnez Fournisseurs EAP et ajoutez PEAP comme type EAP

:

Edit Dial-in Profile			2	×I		
Dial-in Constraints Authentication	IP Encryption		Multilink Advanced	1		
Select the authentication	methods you want to	o allow for this	connection.			
EAP Methods						
Microsoft Encrypt	Select EAP Provide	ers				<u>?×</u>
🔲 User can <u>c</u>	EAP types are nego	otiated in the c	rder in which they	y are listed.		
Microsoft Encrypt	EAP types:					
🗖 Uger can c	Protected EAP (PE	AP)				Move <u>U</u> p
Encrypted auther						Move Down
Unencrypted auti						
Unauthenticated acc						
Allow clients to content method.						
	<u>A</u> dd	<u>E</u> dit	<u>R</u> emove		ОК	Cancel
	OK	Cancel	Apply	J		

7. Cliquez sur **Edit** sur Select EAP Providers et choisissez dans le menu déroulant le serveur associé à vos comptes d'utilisateurs Active Directory et à votre autorité de certification (par exemple, tme.tme.com). Ajoutez le type EAP MSCHAP v2

:

Select EAP Providers			? ×		
EAP types are negotiated in the r	Protected EAP Prope	ities		<u> ? ×</u>	
EAP types:	This server identifies it Select the certificate th	self to callers befor hat you want it to u	e the connection is completed. use as proof of identity.		
HOIECIEU EAF (FEAF)	Certificate (ssued	tme.tme.com	1		
	Friendly name:				
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:	32:22 PM		
Add 1 549	Enable Fast Recon	nect			
	Secured password (E/	AP-MSCHAP v2)	EAP MSCHAPy2 Properties		×
OK Cancel			Number of authentication retri	ies: 2	
	Add	Edit Rem	Allow client to change pass	sword after it has exp	pired
			[ОК	Cancel	

8. Cliquez sur l'onglet Encryption, et vérifiez tous les types de cryptage pour l'accès à distance

it Dial-in Profile		?)
Dial-in Constraints	IP.	Multilink
Authentication	Encryption	Advanced
The following encryption le Routing and Remote Acce make sure the encryption I	evels are supported by se ess. If you use a different evels you select are supp	rvers running Microsoft remote access server, ported by that software.
If No encryption is the only using data encryption.	option selected, then us	ers cannot connect by
I ■ Basic encryption (MP)	PE 40-bit)	
Strong encryption (Mf	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
☑ No encryption		
	1 1	
	OK C	ancel Apolu

9. Cliquez sur l'onglet Advanced, et ajoutez RADIUS Standard/Framed en tant que Service-

it Dial-in Profile		?)>
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connection Access server. Attributes:	n attributes to be return	ned to the Remote
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
•	4	•
A <u>d</u> d <u>E</u> dit	<u>R</u> emove	
	OK (Cancel Apply

Type :

10. Cliquez sur l'onglet IP et cochez la case Client may request an IP address. Cela suppose que DHCP est activé sur un commutateur ou un serveur

onder met er onne		
Authentication	Encryption	Advance
Dial-in Constraints	IP	Multilini
IP address assignment (Fr	amed-IP-Address)	
Server must supply an	IP address	
Client may request an	IP address	
C Server settings determ	ine IP address assignr	ment
Assign a static IP addr	ess 255 . 3	255 . 255 . 255
If an IP address assignmer overrides these settings.	nt method is specified	in the user profile, it
IP filters		
If your remote access serv you can define the filters to	er is Microsoft Routing o apply during this con	g and Remote Acce: inection.
To control the packets this click Input Filters.	s interface receives,	Input Filters
To control the packets this Output Filters.	s interface sends, click	Cutput Filters

WinServer."

Paramètres de sécurité du domaine Microsoft Windows 2003

Complétez ces étapes afin de configurer les paramètres de sécurité du domaine Windows 2003 :

1. Lancez le gestionnaire des paramètres de sécurité du domaine par défaut et créez une nouvelle stratégie de sécurité pour les stratégies de réseau sans fil (IEEE

Eile Action View Help	
← → 1 🖸 🚺 🛃 😰 1 🏠	
Security Settings	Name
🔁 🚰 Account Policies	WI AN Network Policy
🗄 🛃 Local Policies	
🗄 🛃 Event Log	
🗄 🧰 Restricted Groups	
🗄 🧰 System Services	
E 🔁 Registry	
File System	
Wireless Network (TEEE 802 11) Dolicies	1

2. Ouvrez Propriétés de la stratégie de réseau WLAN, puis cliquez sur Réseaux préférés. Ajoutez un nouveau WLAN préféré et tapez le nom de votre SSID WLAN, tel que Wireless. Double-cliquez sur ce nouveau réseau préféré, puis cliquez sur l'onglet IEEE 802.1x. Sélectionnez PEAP comme type d'EAP

Disferred Mehuarka	Edit sroller Properties	21
eneral Treferred Networks	Network Properties IEEE 802.1x	
Automatically conne	Enable network access control using IEEE 802.1x	
	EAPOL-Start message: Transmit	
Networks:	Parameters (seconds)	
Network Name (SSID) IEE	Max start: 3 2000 Start period: 60 2000	
🗼 sroller E	Held period: 60 10 10 Authentication period: 30 10 10 10	
	CAF WPE. [Protected EAP (PEAP)	
	EAF WPe. [Protected EAP (PEAP)	
	Authenticate as guest when user or computer information is	
	EAF WPe. [Protected EAP (PEAP) Settings. Settings. Authenticate as guest when user or computer information is unavailable Authenticate as computer when <u>computer information is available</u>	
A <u>d</u> d <u>E</u> dit	Authenticate as guest when user or computer information is unavailable Authenticate as computer when <u>computer</u> information is available Computer authentication: With user re-authentication	

3. Cliquez sur **PEAP Settings**, cochez **Validate server certificate**, et sélectionnez le certificat racine de confiance installé sur l'autorité de certification. À des fins de test, décochez la case MS CHAP v2 pour Utiliser automatiquement mon identifiant et mon mot de passe

Windows.

Protected EAP Properties	?×	
When connecting:		
Validate server certificate		
Connect to these servers:		
Trusted <u>R</u> oot Certification Authorities:		
VeriSign Trust Network		
🛄 wnbu		
	EAP MSCHAPy2 Properties	
Select Authentication Method:		
Secured password (EAP-MSCHAP v2)	When connecting:	
Enable Fast Reconnect	Automatically use my Wind password (and domain if a	lows logon name and ny).
		Cancel

 Dans la fenêtre Gestionnaire des paramètres de sécurité du domaine par défaut de Windows 2003, créez une autre stratégie de sécurité IP sur la stratégie Active Directory, telle que 4404.



Modifiez les nouvelles propriétés de la stratégie 4404, puis cliquez sur l'onglet Règles.
 Ajouter une nouvelle règle de filtre : IP Filet List (Dynamic); Filter Action (Default Response);

Authentication (PSK); Tunnel (None). Double-cliquez sur la règle de filtre nouvellement créée et sélectionnez Méthodes de sécurité

33	Security i	rules for commun	icating with oth	ier compute	IS	
IP Sec	urity rules:					-
IP Fil	ter List	Filter Actio	n	Authentica	tion T	u
. ≤	Dynamic>	Default Re	esponse	Preshared	Key <	N E
	Offer these	security methods	when negotia	ting with an	other com	nputer.
	Offer these Security me	security methods whod preference	when negotia order:	ting with an	other com	nputer.
•	Offer these <u>S</u> ecurity me Type Custom	security methods thod preference AH Integrity <none></none>	order: SDES	ting with and ential E	other com	nputer. A <u>d</u> d
	Offer these Security me Type Custom Custom	security methods thod preference AH Integrity <none> <none></none></none>	order: BSP Confid 3DES 3DES	ting with and ential E: SI	other com	Add
	Offer these Security me Type Custom Custom Custom	security methods whod preference AH Integrity <none> <none> <none></none></none></none>	order: ESP Confid 3DES 3DES DES	ting with and ential E SI M SI		Add
	Offer these Security me Type Custom Custom Custom Custom	security methods whod preference AH Integrity <none> <none> <none> <none> <none> <none></none></none></none></none></none></none>	order: ESP Confid 3DES 3DES DES DES CS (None)	ting with and ential E SI M SI M 21		A <u>d</u> d <u>E</u> dit
	Offer these <u>Security me</u> <u>Type</u> Custom Custom Custom Custom Custom Custom Custom	security methods whod preference AH Integrity <none> <none> <none> <none> SHA1 MD5</none></none></none></none>	order: ESP Confid 3DES 3DES DES DES <none> <none></none></none>	ting with and ential E SI M SI A SI		A <u>d</u> d Edit
	Offer these <u>Security me</u> <u>Type</u> Custom Custom Custom Custom Custom Custom Custom	security methods thod preference AH Integrity <none> <none> <none> <none> SHA1 MD5</none></none></none></none>	order: ESP Confid 3DES 3DES DES DES <none> <none></none></none>	ting with and ential E SI M SI SI SI SI		A <u>d</u> d <u>E</u> dit <u>B</u> emove
	Offer these <u>Security me</u> <u>Type</u> Custom Custom Custom Custom Custom Custom	security methods thod preference AH Integrity <none> <none> <none> SHA1 MD5</none></none></none>	order: ESP Confid 3DES 3DES DES DES <none> <none></none></none>	ting with and ential E SI M SI A SI A SI		A <u>d</u> d Edit Bemove Move <u>up</u> ove d <u>o</u> wn

 Cliquez sur Edit Security Method, puis sur la case d'option Custom Settings. Sélectionnez ces paramètres. Remarque : ces paramètres doivent correspondre aux paramètres de sécurité du contrôleur RADIUS IPSec.

Edit Security Method	?×	/s req
Security Method		
 Integrity and encry Data will be encry unmodified. Integrity only Data will be verific encrypted. <u>C</u>ustom <u>S</u>ettings 	Determine the settings for this custom security method.	<u>? ×</u>
	Session key settings: Generate a new key every: Generate a new key every: 28800 Seconds Seconds OK Cance	у.

7. Cliquez sur l'onglet **Authentication Method** sous Edit Rule Properties. Entrez le même secret partagé que celui que vous avez entré précédemment dans la configuration RADIUS du contrôleur.

Rule Properties ecurity Methods Aut	nentication Methods	1×
Authenti between offered a compute	cation methods specify how trust is established computers. These authentication methods are ind accepted when negotiating security with anol r.	ther
Authentication <u>m</u> ethod Method Preshared Key	l preference order: Details Add cisco	
Edit (<u>Edit</u>	
	The authentication method specifies between the computers.	how trust is established
	Active Directory default (Kerberos V5 protocol)	(04)
	Use a certificate from this certification authority	<u>B</u> rowse
	Esclude the CA name from the certificate in Enable certificate to account mapping	request
•	Use this <u>s</u> tring (preshared key)	
	cipac.	

Àce stade, toutes les configurations des paramètres de contrôleur, IAS et de sécurité du domaine sont terminées. Enregistrez toutes les configurations sur le contrôleur et WinServer et redémarrez toutes les machines. Sur le client WLAN utilisé pour le test, installez le certificat racine et configurez pour WPA2/PEAP. Une fois le certificat racine installé sur le client, redémarrez l'ordinateur client. Après le redémarrage de toutes les machines, connectez le client au WLAN et capturez ces événements de journal.

Remarque : une connexion client est requise pour configurer la connexion IPSec entre le contrôleur et WinServer RADIUS.

Événements du journal système Windows 2003

Une connexion client WLAN configurée pour WPA2/PEAP avec IPSec RADIUS activé génère cet événement système sur le serveur WinServer :

192.168.30.105 = WinServer 192.168.30.2 = WLAN Controller

😽 Event Viewer							
Eile Action View	Help						
← → 💽 💽 🖆	1 🗟 🔹						
Event Viewer (Local)	System 22 eve	nt(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Socurity	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)
```

Une connexion RADIUS IPSec du contrôleur <> réussie génère cet événement de sécurité dans les journaux WinServer :

😫 Event Viewer							
Ele Action View	Help						
⇔ ⇒ 🗈 🖬 🖀	6 🗟 😫						
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
```

Exemple de débogage de réussite du contrôleur LAN sans fil RADIUS IPSec

Vous pouvez utiliser la commande debug **debug pm ikemsg enable** sur le contrôleur afin de vérifier cette configuration. Voici un exemple.

```
(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=0x00000000000000000
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] = 0xcf0bbdlc 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 = TransportNONCE: 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

Capture Éthréenne

Voici un exemple de capture éthique.

```
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=0xbb243261)
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=0xbb243261)
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=0xbb243261)
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 (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 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
```

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 5.2
- Assistance et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.