RADIUS IPSec-beveiliging voor WLC's en Microsoft Windows 2003 IAS-server configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configuratie van IPSec RADIUS De WLC configureren De IAS configureren Microsoft Windows 2003 domeinbeveiligingsinstellingen Windows 2003-systeemloggebeurtenissen Draadloze LAN-controller voor RADIUS en IPSec-succes bij debugvoorbeeld Ethreal Capture Gerelateerde informatie

Inleiding

Deze handleiding beschrijft hoe de RADIUS IPSec-functie moet worden geconfigureerd die wordt ondersteund door WCS en deze WLAN-controllers:

- 4400 Series
- WiSM
- 3750G

De functie Controller RADIUS IPSec bevindt zich op de Controller GUI onder de sectie **Security > AAA > RADIUS-verificatieservers**. Deze voorziening biedt u een methode om alle RADIUScommunicatie tussen controllers en RADIUS-servers (IAS) te versleutelen met IPSec.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis over LWAPP
- Kennis van RADIUS-verificatie en IPSec
- Kennis over het configureren van services op het besturingssysteem Windows 2003 Server

Gebruikte componenten

Deze netwerk- en softwarecomponenten moeten worden geïnstalleerd en geconfigureerd om de controller RADIUS IPSec-functie te kunnen implementeren:

- WLC 4400, WiSM of 3750G controllers. In dit voorbeeld wordt WLC 4400 gebruikt, dat softwareversie 5.2.178.0 uitvoert
- Lichtgewicht access points (LAP's). In dit voorbeeld wordt de 1231-serie LAP gebruikt.
- Switch met DHCP
- Microsoft 2003-server geconfigureerd als een domeincontroller die is geïnstalleerd met Microsoft Certificate Authority en met Microsoft Internet Verification Service (IAS).
- Microsoft Domain Security Appliance
- Cisco 802.11 a/b/g draadloze clientadapter met ADU versie 3.6 geconfigureerd met WPA2/PEAP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Configuratie van IPSec RADIUS

Deze configuratiehandleiding is niet van toepassing op de installatie of configuratie van Microsoft WinServer, Certificate Authority, Active Directory of WLAN 802.1x-client. Deze componenten moeten voorafgaand aan de implementatie van de controller IPSec RADIUS-functie worden geïnstalleerd en geconfigureerd. De rest van deze handleiding legt uit hoe IPSec RADIUS op deze componenten moet worden geconfigureerd:

- 1. Cisco WLAN-controllers
- 2. Windows 2003 IAS
- 3. Beveiligingsinstellingen Microsoft Windows-domein

De WLC configureren

Deze sectie verklaart hoe u IPSec op de WLC kunt configureren via de GUI.

Voltooi deze stappen vanuit de controller-GUI.

 Navigeer naar het tabblad Security > AAA > RADIUS-verificatie in de Controller GUI en voeg een nieuwe RADIUS-server toe.

Cisco Systems							
alia alia	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	СС
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	Management	Server	Server Address	s Port	IPSec	
Access Control Lists	- Oser		Index	100 110 00 10	1010		
IPSec Certificates		1.1.1.1.1.1. 1.1 .1.1.1.1	· · · 1 · · · · · · · · · · · · · · · ·	192,168,30,10	1812	Disabled	
CA Certificate ID Certificate		V	3	192.168.30.105	1812	Enabled	

 Configureer het IP-adres, poort 1812 en een gedeeld geheim van de nieuwe RADIUS-server. Controleer het vakje Inschakelen-controle van IPSec, configureer deze IPSec-parameters en klik vervolgens op Toepassen.Opmerking: het gedeelde geheim wordt gebruikt voor de verificatie van de RADIUS-server en als de vooraf gedeelde sleutel (PSK) voor IPSecverificatie.

CIECO SYSTEME	MONITOR WLANS (CONTROLLI	ER WIRELESS	SECURITY	MANAGEMEN
Security	Shared Secret	ſ	•••		
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		Enabled		
Access Control Lists					
IPSec Certificates	Support for RFC 357	6 [Disabled 💌		
ID Certificate	Retransmit Timeout		2 seconds		
Web Auth Certificate					
Wireless Protection Policies	Network User		🗹 Enable		
Rogue Policies Standard Signatures	Management		🗹 Enable		
Custom Signatures Client Exclusion Policies	IPSec		Enable		
AP Authentication	IPsec Parameters				
	IPSec	[HMAC SHA1 🔽		
	IPSEC Encryption		3DES 💙		
	(Shared Seceret will be	e used as th	ne Preshared Key)		
	IKE Phase 1		Main 🔽		
	Lifetime (seconds)		28800		
	IKE Diffie Hellman Gro	up	Group 2 (1024 bits) 🗸	

De IAS configureren

Voltooi de volgende stappen in de IAS:

1. Navigeer naar de IAS-beheerder in Win2003 en voeg een nieuwe RADIUS-client toe.

Internet Authentication Service				
Elle Action View Help				
⇔ → 🗈 🔳 💼 🕑 🖳 🔗				
Internet Authentication Service (Local)	Friendly Name	Address	Protocol	Client-Vendor
ADJUS Clients Amore Access Logging Amore Access Policies	<u>]</u> 4404	192.168.30.2	RADIUS	RADIUS Standard
Connection Request Processing				

2. Configureer de RADIUS-clienteigenschappen met het IP-adres en het gedeelde geheim dat op de controller is

ettings			
Friendly name:			
4404			
Address (IP or DNS):			
192.168.30.2			
Verifu			
If you are using remo attribute, specify the Cli <u>e</u> nt-Vendor:	vendor of the RADI	ased on the client v US client. ard	vendor's
<u>R</u> equest must co	, ontain the Message /	Authenticator attribu	ute
<u>S</u> hared secret:		×	
C <u>o</u> nfirm shared secre	et:	×	

geconfigureerd:

3. Configureer een nieuw beleid voor externe toegang voor de controller:

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

4. Bewerk de eigenschappen van het Controller Remote Access Policy. Zorg ervoor dat u het NAS-poorttype - Draadloos - IEEE 802.11

104 Properties	NAS-Port-Type	1)
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 Edt Ennove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.	Agailable 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	Add >> Ethernet 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:	Tecycle Bn	

5. Klik op **Profiel bewerken**, klik op het tabblad **Verificatie** en controleer MS-CHAP v2 op Verificatie:

Ed	it Dial-in Profile		<u>i</u>
opecity the condi Policy <u>c</u> onditions: NAS-Port-Type m	Dial-in Constraints Authentication	IP Encryption whods you want to allow	Multilink Advanced) for this connection.
< <u>↓</u>	EAP Methods		
<u>Add</u>	Microsoft Encrypted A	uthentication version 21	(MS-CHAP v2)
f connection requ associated profile	User can <u>c</u> hang	ge password after it has uthentication (MS-CHAF	expired ^o)
Edit Profile	📕 Uger can chang	je password after it has	expired
Unless individual (policy controls ac)	Encrypted authenticat Unencrypted authentic	ion (CHAP) cation (PAP, SPAP)	
f a connection re			
<u>G</u> rant remote -	Allo <u>w</u> clients to conne method.	ct without negotiating ar	n authentication

6. Klik op **EAP Methods**, selecteer EAP Providers en voeg PEAP toe als een EAPtype:

dit Dial-ın Profile			2	хI		
Dial-in Constraints Authentication	IP Encryption		Multilink Advanced			
Select the authentication	methods you want to	allow for this	connection.			
EAP Methods						
Microsoft Encrypt	Select EAP Provider	'S				? ×
🗖 User can <u>c</u>	EAP types are negoti	ated in the o	der in which they	are listed.		
Microsoft Encrypt	EAP types:					
🗖 Uger can c	Protected EAP (PEA	P)				Move <u>U</u> p
Encrypted auther						Move Down
Unencrypted auti						
Unauthenticated acc						
Allow clients to ci method.						
	<u>A</u> dd	<u>E</u> dit	<u>R</u> emove		OK	Cancel
<u> </u>	OK	Cancel	Apply:	J		

7. Klik op Bewerken op Selecteer EAP Providers en kies in het keuzemenu de server die is gekoppeld aan uw Active Directory-gebruikersaccounts en CA (bijvoorbeeld tme.tme.com). Voeg het EAP-type MSCHAP v2

toe:					
Select EAP Providers			? ×		
FAD have an exception of the	Protected EAP Prope	rties		<u>?×</u>	
EAP types: EAP types: Protected EAP (PEAP)	This server identifies it Select the certificate t	self to callers befor hat you want it to u	e the connection is completed. Ise as proof of identity.		
	Certificate issued	tme.tme.com	1		
	Friendly name:				
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:	32:22 PM		
	Enable Fast Recon	nect			
Add Edit	Eap Types				
	Secured password (E	AP-MSCHAP v2)	EAP MSCHAPv2 Properties		×
OK Cancel			Number of authentication retri	esi 2	
	Add	Edit Rem	Allow client to change pass	word after it has expired	
			ОК	Cancel	

8. Klik op het tabblad Encryptie en controleer alle coderingstypen voor externe

Edit Dial-in Profile		<u>?</u> ×
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
The following encryption la Routing and Remote Acce make sure the encryption I If No encryption is the only using data encryption.	evels are supported by ser ess. If you use a different r levels you select are supp v option selected, then use	rvers running Microsoft remote access server, ported by that software. ers cannot connect by
Basic encryption (MP)	PE 40-bit)	
Strong encryption (M	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
✓ <u>N</u> o encryption		
		ancel Apply

toegang:

9. Klik op het tabblad Geavanceerd en voeg RADIUS-standaard/framed toe als het

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

servicetype:

10. Klik op het tabblad **IP** en controleer of **de client een IP-adres kan aanvragen**. Dit veronderstelt dat DHCP is ingeschakeld op een switch of

Authentication	Encryption Ad	lvance
Dial-in Constraints	IP I	Multilin
IP address assignment (Fra	med-IP-Address)	
Server must supply an I	P address	
Client may request an IF	^D address	
C Server settings determin	ne IP address assignment	
C Assign a static IP addre	ess 255 . 255 . 255 .	255
If an IP address assignmen overrides these settings.	t method is specified in the user pr	ofile, it
IP filters		
If your remote access serve you can define the filters to	er is Microsoft Routing and Remote apply during this connection.	Acce
To control the packets this click Input Filters.	interface receives, <u>I</u> nput Fil	ters
To control the packets this	interface sends, click	ilters
Output Filters.		

WinServer."

Microsoft Windows 2003 domeinbeveiligingsinstellingen

Voltooi de volgende stappen om de beveiligingsinstellingen voor het domein van Windows 2003 te configureren:

1. Start Default Domain Security Settings Manager en maak een nieuw beveiligingsbeleid voor het beleid voor draadloze netwerken (IEEE

<u>Eile A</u> ction ⊻iew <u>H</u> elp	
← → 🗈 🖪 🗗 🗔 🖆	
Security Settings	Name
🗄 📰 Account Policies	WLAN Network Policy
🗄 🛃 Local Policies	—
🗄 🛃 Event Log	
🕀 🧖 Restricted Groups	
🕀 📴 System Services	
File System	
Wireless Network (IEEE 802.11) Policies	

2. Open WLAN-netwerkbeleidseigenschappen en klik op **Voorkeursnetwerken**. Voeg een nieuw geprefereerd WLAN toe en typ de naam van uw WLAN-SSID, zoals *Wireless*. Dubbelklik op dat nieuwe voorkeursnetwerk en klik op het tabblad **IEEE 802.1x**. PEAP als EAP-type kiezen:

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

3. Klik op **PEAP-instellingen**, controleer het **servercertificaat valideren** en selecteer de Trusted Root Cert die is geïnstalleerd in de certificeringsinstantie. Voor testdoeleinden vinkt u het vakje MS CHAP v2 uit om automatisch mijn Windows-login en -wachtwoord te gebruiken.

Protected EAP Properties	?×	
When connecting:		
Validate server certificate		
Connect to these servers:		
Trusted Root Certification Authorities:		
VeriSign Trust Network		
VeriSign Trust Network		
VeriSign Trust Network		
wnbu		
Xcert EZ by DST	· · · · · · · · · · · · · · · · · · ·	
	EAP MSCHAPv2 Properties	
Select Authentication Method:	At them compositions:	
Secured password (EAP-MSCHAP.v2)	when connecting.	
Enable Fast Reconnect	Automatically use my Wind password (and domain if ar	ows logon name and ny).
	ОК	Cancel

4. Maak in het venster van Windows 2003 Default Domain Security Settings een nieuw IPbeveiligingsbeleid voor het Active Directory-beleid, zoals

The Default Domain Security Settings			e de la companya de l
Eile Action View Help			
🗢 🔿 🖻 📧 🗙 🖀 🗔 😰 🏦 🕯	9 <u>.</u>		
Security Settings	Name A	Description	Policy Assigned
Account Policies	4404	O D S S D D S D D S D D S S D D S	Yes
E - 🛃 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
E System Services			
E Calstry			
Wireless Network (IEEE 802.11) Policies			
Public Key Policies			
Software Restriction Policies			
IP Security Policies on Active Directory (tme.com)			

5. Bewerk de nieuwe 4404 beleidseigenschappen en klik op het tabblad **Regels**. Voeg een nieuwe filterregel toe - IP Filet List (Dynamisch); Filter Actie (Default Response); Verificatie (PSK); Tunnel (Geen). Dubbelklik op de nieuwe filterregel en selecteer Beveiligingsmethoden:

4404 Prop	perties				?× IP traffic
Rules	General				
	g Security	rules for commun	icating with ot	her computers	
IP Sec	urity rules:				
IP Filt	er List	Filter Actio	n	Authentication.	Tu sisisis
)ynamic>	Default Re	esponse	Preshared Key	<n electronic<="" td=""></n>
Ed Ed	lit Rule Pro	perties			<u>?</u> ×
	Security Met	hads Authentia	ation Mathada	1	
	occounty mot	Addrenac	adon Methous	1	1
	Offer these	security methods	when negotia	ating with anothe	r computer.
	Security me	thod preference	order		
	Tupe	AH Integritu	ESP Confir	dential ES	Add 1
•	Custom	(None)	3DES	SH	
	Custom	<none></none>	3DES	ME ME	Edit
	Custom	<none></none>	DES	SH	
	Custom	<none></none>	DES	ME	<u>R</u> emove
	Custom	SHA1	<none></none>		
	Lustom	MD5	<none></none>	<n.< td=""><td>Move up</td></n.<>	Move up
	•			•	Move d <u>o</u> wn
	Use se:	ssion <u>k</u> ey perfect	forward secre	cy (PFS)	

6. Klik op Security Method bewerken en klik op de knop Aangepaste instellingen. Kies deze instellingen.Opmerking: deze instellingen moeten overeenkomen met de beveiligingsinstellingen van de controllerRADIUS IPSec.

Edit Security Method	? × Ptrattic, alwa	iys 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 	Data and address integrity without encryption (AH) Integrity algorithm: MD5 Data integrity and engryption (ESP): Integrity algorithm: SHA1 Integrity algorithm: SHA1 Integrity algorithm: SHA1 Integrity algorithm: Integrity algorithm: Integrity algorithm: SHA1 Integrity algorithm: Integrity algorithm:	<u>? ×</u>
	Session key settings: Generate a new key every: 100000 Kbytes OK Cance	ry:

7. Klik op het tabblad **Verificatiemethode** onder de Eigenschappen regel bewerken. Voer hetzelfde gedeelde geheim in dat u eerder hebt ingevoerd in de controller-RADIUS-configuratie.

Rule Properties		?×
ecurity Methods Auther Auther betwee offered compu	uthentication Methods ntication methods specify how trust is establis en computers. These authentication methods I and accepted when negotiating security wit ter.	hed are h another
Authentication <u>m</u> eth Method Preshared Key	od preference order: Details cisco	Add
Edit	Authentication Method Properties]
A	uthentication Method The authentication method spe between the computers.	cifies how trust is established
	C Active Directory <u>d</u> efault (Kerberos V5 pro	tocol)
	O Use a <u>certificate from this certification aut</u>	hority (CA): Browse
	Exclude the CA name from the certif	icate request ng
	Use this string (preshared key);	
	cisco	

Op dit punt zijn alle configuraties voor de Controller, IAS en Domain Security Settings voltooid. Sla alle configuraties op zowel de controller als WinServer op en herstart alle machines. Installeer op de WLAN-client die voor de test wordt gebruikt de basiskern en configureer deze voor WPA2/PEAP. Nadat de root cert is geïnstalleerd op de client, herstart de client machine. Nadat alle machines opnieuw zijn opgestart, sluit u de client aan op het WLAN en neemt u deze loggebeurtenissen op.

Opmerking: een clientverbinding is vereist om de IPSec-verbinding tussen de controller en WinServer RADIUS in te stellen.

Windows 2003-systeemloggebeurtenissen

Een succesvolle WLAN-clientverbinding die voor WPA2/PEAP met IPSec RADIUS is geconfigureerd, genereert deze systeemgebeurtenis op de WinServer:

192.168.30.105 = WinServer 192.168.30.2 = WLAN Controller

😽 Event Viewer							
Eile Action View	Help						
← → 🗈 🖪 🖆	• 🔁 🗟 😫						
Event Viewer (Local)	System 22 eve	nt(s)					
B Application	Туре	Date	Time	Source	Category	Event	User
Security System	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)
```

Een succesvolle controller <> RADIUS IPSec-verbinding genereert deze security gebeurtenis op de WinServer-logbestanden:

😫 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

Draadloze LAN-controller voor RADIUS en IPSec-succes bij debugvoorbeeld

U kunt de debug opdracht gebruiken **debug debug pm ikemsg inschakelen** op de controller om deze configuratie te verifiëren. Hierna volgt een voorbeeld.

```
(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] = 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 c0a81e69HASH: 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

Ethreal Capture

Hier is een voorbeeld van Ethreal Capture.

```
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 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
```

Gerelateerde informatie

- <u>Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 5.2</u>
- Technische ondersteuning en documentatie Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.