WLC 用および Microsoft Windows 2003 IAS サ ーバ用に RADIUS IPSec セキュリティを設定す る

内容

概要
前提条件
要件
使用するコンポーネント
表記法
IPSec RADIUSの設定
WLC の設定
IASの設定
Microsoft Windows 2003ドメインのセキュリティ設定
Windows 2003システムログイベント
ワイヤレスLANコントローラのRADIUS IPSec成功のデバッグ例
民族的捕獲
関連情報

<u>概要</u>

このガイドでは、WCSおよび次のWLANコントローラでサポートされるRADIUS IPSec機能を設 定する方法について説明します。

- •4400 シリーズ
- WISM
- 3750 G

コントローラのRADIUS IPSec機能は、コントローラのGUIの[Security] > [AAA] > [RADIUS Authentication Servers] セクションにあります。この機能を使用すると、コントローラと RADIUSサーバ(IAS)間のすべてのRADIUS通信をIPSecで暗号化できます。

<u>前提条件</u>

<u>要件</u>

次の項目に関する知識があることが推奨されます。

- LWAPPに関する知識
- RADIUS認証とIPSecに関する知識
- Windows 2003 Serverオペレーティングシステムでのサービスの設定方法に関する知識

<u>使用するコンポーネント</u>

コントローラのRADIUS IPSec機能を導入するには、次のネットワークコンポーネントとソフト ウェアコンポーネントをインストールして設定する必要があります。

- WLC 4400、WiSM、または3750Gコントローラこの例では、ソフトウェアバージョン 5.2.178.0が稼働するWLC 4400を使用しています
- Lightweightアクセスポイント(LAP)。この例では、1231シリーズのLAPを使用しています。
- DHCPを使用したスイッチ
- Microsoft Certificate Authority (CA;認証局)およびMicrosoft Internet Authentication Service (IAS; インターネット認証サービス)とともにインストールされるドメインコント ローラとして設定されたMicrosoft 2003サーバ。
- Microsoftドメインセキュリティ
- ADUバージョン3.6がWPA2/PEAPで設定されたCisco 802.11 a/b/gワイヤレスクライアントア ダプタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

<u>IPSec RADIUSの設定</u>

この設定ガイドでは、Microsoft WinServer、認証局、Active Directory、またはWLAN 802.1xクラ イアントのインストールや設定については説明していません。これらのコンポーネントは、コン トローラIPSec RADIUS機能を導入する前にインストールして設定する必要があります。このガ イドの残りの部分では、次のコンポーネントでIPSec RADIUSを設定する方法について説明しま す。

- 1. Cisco WLAN コントローラ
- 2. Windows 2003 IAS
- 3. Microsoft Windowsドメインのセキュリティ設定

<u>WLC の設定</u>

このセクションでは、GUIを使用してWLCでIPSecを設定する方法について説明します。

コントローラのGUIから、次の手順を実行します。

1. コントローラGUIで[Security] > [AAA] > [RADIUS Authentication] タブに移動し、新しい RADIUSサーバを追加します。

CISCO SYSTEMS							s
all the call the	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C
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 User Login Policies	Use AES	Key Wrap					
AP Policies	Network	Management	Server	Server Address	5 Port	IPSec	
Access Control Lists	USEF		muex				
IPSec Certificates		(1993) 🖾 (1993)	1	192.168.30.10	1812	Disabled	1000
CA Certificate		V	3	192.168.30.105	1812	Enabled	

2. 新しいRADIUSサーバのIPアドレス、ポート1812、および共有秘密を設定します。[IPSec Enable] チェックボックスをオンにして、これらのIPSecパラメータを設定し、[Apply] をク リックします。注:共有秘密は、RADIUSサーバの認証と、IPSec認証用の事前共有キー (PSK)の両方に使用されます。

CISCO SYSTEMS	MONITOR WLANS CO	ONTROLLER WIRELESS SECUR	ITY MANAGEMEN		
Security	Shared Secret	••			
AAA General RADIUS Authentication	Confirm Shared Secret				
Local Net Users MAC Filtering Disabled Clients	Key Wrap Port Number	1812			
User Login Policies AP Policies Access Control Lists	Server Status	Enabled 💌			
IPSec Certificates CA Certificate	Support for RFC 3576	Disabled 💌			
Web Auth Certificate	Retransmit Timeout	2 seconds			
Wireless Protection Policies	Network User	🗹 Enable	🗹 Enable		
Trusted AP Policies Rogue Policies Standard Signatures	Management	🗹 Enable			
Custom Signatures Client Exclusion Policies	IPSec	Enable			
AP Autoentication	IPsec Parameters				
	IPSec	HMAC SHA1 ¥			
	IPSEC Encryption	3DES 💙			
	(Shared Seceret will be	used as the Preshared Key)			
	IKE Phase 1	Main 🔽			
	Lifetime (seconds)	28800			
	IKE Diffie Hellman Group	Group 2 (1024 bits) ⊻			

<u>IASの設定</u>

IASで次の手順を実行します。

1. Win2003のIASマネージャに移動し、新しいRADIUSクライアントを追加します。

Internet Authentication Servic	en e			
Elle Action ⊻lew Help	r 9			
Internet Authentication Service (Low ADJUS Clients Remote Access Logging Remote Access Policies Connection Request Processing	cal) Friendly Name	Address 192,168.30.2	Protocol RADIUS	Client-Vendor RADIUS Standard
2. RADIUSクライアントのフ 4404 Prope Settings Eriendly i 4404 Address 192.168 <u>V</u> erif If you are attribute,	*ロパティに、コ erties name: (IP or DNS): 1:30.2 y e using remote acc specify the vendo	コントローラで設定 cess policies based (pr of the RADIUS cli	EされたIPアド on the client ven ent.	レスと共有秘密を ・ ・ dor's
Cli <u>e</u> nt-Ve <u>B</u> eque <u>S</u> hared s C <u>o</u> nfirm s	ndor: R/ uest must contain ecret: shared secret:	ADIUS Standard the Message Auther	nticator attribute	
設定します。		ОК	Cancel	Apply

3. コントローラの新しいリモートアクセスポリシーを設定します。

🌮 Internet Authentication Service		
Eile Action View Help		
← → 🖻 🖬 🕑 💀 😫		
Internet Authentication Service (Local)	Name	Order
E Call RADIUS Clients	S 4404	1
Remote Access Policies Connection Request Processing		

4. コントローラのリモートアクセスポリシーのプロパティを編集します。必ずNASポートタイ <u>プ</u> – Wireless - IEEE 802.11を追加します。

04 Properties	NAS-Port-Type	212
Settings	Available types:	Selected types:
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.110 ISDN Async V.120 ISDN Sync	Add >> Ethemet Wireless - IEEE 802.11 Wireless - Other Wireless - Other OK Cencel
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:	2	
C Deny remote access permission	Recycle Bn	
Grant remote access permission		
OK Cancel Apply		

5. [Edit Profile] をクリックし、[Authentication] タブをクリックして、[MS-CHAP v2 for Authentication]にチェックマークを付けます。

Ed	it Dial-in Profile		<u>8</u>	
Policy <u>c</u> onditions: NAS-Port-Type m	Dial-in Constraints Authentication	IP Encryption hods you want to allow	Multilink Advanced w for this connection.	
∢	EAP Methods			
A <u>d</u> d	Microsoft Encrypted Au	thentication version <u>2</u>	(MS-CHAP v2)	
f connection requ associated profile	User can <u>c</u> hange	e password after it has thentication (MS-CHA	expired P)	
Edit <u>P</u> rofile	User can change password after it has expired			
Unless individual - policy controls act	Encrypted authentication Unencrypted authentication	on (CHAP) ation (PAP, SPAP)		
f a connection re	Unauthenticated access			
Grant remote .	Method.	t without negotiating a	in authentication	

6. [EAP Methods] をクリックし、[EAP Providers]を選択して、EAPタイプとしてPEAPを追加 します。

Edit Dial-in Profile		?]:	×	
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced		
Select the authentication	methods you want to allow	o for this connection.		
EAP Methods				
Microsoft Encrypt	Select EAP Providers			<u>?</u> ×
🗖 User can <u>c</u>	EAP types are negotiated	in the order in which they	y are listed.	
Microsoft Encrypt	EAP types:			
🗖 Uger can c	Protected EAP (PEAP)			Move Up.
Encrypted auther				Move Down
🔲 Unencrypted auti				
Unauthenticated acc				
Allow clients to commethod.				
	Add Ed	it <u>R</u> emove	OK	Cancel
	ОКСС	ancel Apply	J	

7. [Select EAP Providers]で[Edit] をクリックし、プルダウンメニューからActive Directoryユー ザアカウントとCAに関連付けられたサーバ(tme.tme.comなど)を選択します。EAPタイプ MSCHAP v2を追加します。

elect EAP Providers			? ×		
EAP types are negotiated in the (Protected EAP Properties This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.			<u>?</u> ×	
Protected EAP (PEAP)	Certificate (ssued	tme.tme.com			
	Issuer: Expiration date:	wnbu 3/30/2007 3::	32:22 PM		
<u>A</u> dd <u>E</u> dit	Enable Fast Recon Eap Types Secured password (E/	nect AP-MSCHAP ∨2)	EAP MSCHAPv2 Properties		×
OK Cancel			Number of authentication retr	ies: 2	
	Add	Edit Kern	Allow client to change pas	sword after it has expired	

8. [Encryption] タブをクリックし、リモートアクセス用のすべての暗号化タイプを確認します

Edit Dial-in Profile		?×				
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced				
The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.						
If No encryption is the only o using data encryption.	ption selected, then us	ers cannot connect by				
☑ Basic encryption (MPP)	E 40-bit)					
Strong encryption (MPF	PE 56 bit)					
Strongest encryption (M	(PPE 128 bit)					
☑ No encryption						
	ОК С	ancel Apply				

。 9. [Advanced] タブをクリックし、[Service-Type]として[RADIUS Standard/Framed]を追加しま

Dial-in Constraints	IP	Multilink
Authentication	Encryption	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	
Image: A second seco		
▲ Add <u>E</u> dit	<u>R</u> emove	<u>.</u>
▲ <u>E</u> dit	<u>R</u> emove	<u>•</u>
▲ Add Edit	<u>R</u> emove	<u>•</u>

す。

10. [IP] タブをクリックし、[Client may request an IP address] にチェックマークを付けます。 ここでは、スイッチまたはWinServerでDHCPが有効になっていることを前提としています

dit Dial-in Profile	x
Authentication Encryption Advanced Dial-in Constraints IP Multilink	
 IP 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 If an IP address assignment method is specified in the user profile, it overrides these settings. 	
IP filters If your remote access server is Microsoft Routing and Remote Access, you can define the filters to apply during this connection. To control the packets this interface receives, click Input Filters. To control the packets this interface sends, click Output Filters.	
OK Cancel Apply	

<u>Microsoft Windows 2003ドメインのセキュリティ設定</u>

o

Windows 2003ドメインのセキュリティ設定を行うには、次の手順を実行します。

1. 既定のドメインセキュリティ設定マネージャーを起動し、ワイヤレスネットワーク(IEEE 802.11)ポリシーの新しいセキュリティポリシーを作成します。

🚡 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	

2. [WLAN Network Policy Properties]を開き、[Preferred Networks] をクリックします。新しい 優先WLANを追加し、WLAN SSIDの名前(wirelessなど)を入力します。新しい優先ネットワ ークをダブルクリックし、[IEEE 802.1x]タブをクリックします。EAPタイプとしてPEAPを 選択します。

WLAN Network Policy Propertie	s ? ×	
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 and a descent descent and the	
Networks:	Parameters (seconds)	
Network Name (SSID) IEE	Max start: 3 1 2 2 2 2 Start period: 60 2 2 2 2 2	
A sroller E	Held period: 60 (10) Authentication period: 30 (10) (10)	
	EAP type: Protected EAP (PEAP)	•
	Authenticate as guest when user or computer information is unavailable	
	Authenticate as computer when computer information is available	
<u>Add</u>	Computer authentication: With user re-authentication	
	ОК Са	incel

3. [PEAP Settings] をクリックし、[Validate server certificate] にチェックマークを入れて、 [Trusted Root Cert installed on Certificate Authority]を選択します。テスト目的で、 [Automatically use my Windows login and password]の[MS CHAP v2]ボックスをオフにしま す。

Protected EAP Properties	<u>?×</u>
When connecting:	
Validate server certificate	
Connect to these servers:	
Trusted <u>R</u> oot Certification Authorities:	
VeriSign Trust Network	
VeriSign Trust Network	
VeriSign Trust Network	
🗖 wnbu	
wnbu	
Xcert EZ by DST	
	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. Windows 2003の[Default Domain Security Settings]マネージャウィンドウで、**4404**などの別の新しいIPセキュリティポリシーをActive Directoryポリシーに作成します。

🚡 Default Domain Security Settings									
Eile Action View Help									
Security Settings	Name /	Description	Policy Assigned						
🗈 🛃 Account Policies	111		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 reg	No						
System Services									
Registry									
🗄 🛄 File System									
Wireless Network (IEEE 802.11) Policies									
🕀 🧱 Public Key Policies									
Software Restriction Policies									
IP Security Policies on Active Directory (tme.com)									

5. 新しい4404ポリシーのプロパティを編集し、[Rules] タブをクリックします。新しいフィル タルールを追加します(IPフィレットリスト(ダイナミック)、フィルタアクション(デフ ォルト応答)、認証(PSK)、トンネル(なし))。新しく作成したフィルタルールをダブルク リックし、[Security Methods]を選択します。

4404 Proj	perties				?× IP traffic
Rules	General				
	g Security	rules for commun	icating with othe	er computers	
IP Sec	urity rules:				
IP Filt	er List	Filter Actio	on /	Authentication.	Tu
)ynamic>	Default Re	esponse l	Preshared Key	<n detected<="" td=""></n>
	lit Dule Pro	nerties			2 1 1
	ine ikulie Pro	percies			كن
	Security Met	hods Authentic	ation Methods		
	Offer these	security methods	when negotiati	na with anothe	er computer
	Offici diese	secondy methods	s when negotiat	ng man anoand	a compater.
	C				
	Security me	anoa prererence			
•	Type	AH Integrity	ESP Confide	ntial ES	A <u>d</u> d
	Custom	<none></none>	3DES	эп МГ	Edit
	Custom	<none></none>	DES	SH	
	Custom	<none></none>	DES	ME ME	Remove
	Custom	SHA1	<none></none>	leisisis KN	
	Lustom	MD5	<none></none>	×N	Move <u>up</u>
					Move down
				1	
	Use se:	ssion key perfect	forward secrecy	(PFS)	

6. [Edit Security Method] をクリックし、[Custom Settings] オプションボタンをクリックします 。次の設定を選択します。**注:これらの設**定は、コントローラのRADIUS IPSecセキュリテ ィ設定と一致している必要があります。

Edit Security Method	?×	ays 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 	Detion Custom Security Method Settings Specify the settings for this custom security method.	<u>?</u> ×
	Session key settings: Generate a new key every: Generate a new key every: 28800 Seconds OK Canc	el

7. [Edit Rule Properties]の下の[Authentication Method] タブをクリックします。コントローラの RADIUS設定で以前に入力したのと同じ共有秘密を入力します。



この時点で、コントローラ、IAS、およびドメインセキュリティ設定のすべての設定が完了しま す。コントローラとWinServerの両方ですべての設定を保存し、すべてのマシンをリブートしま す。テストに使用するWLANクライアントで、ルート証明書をインストールし、WPA2/PEAPを 設定します。ルート証明書がクライアントにインストールされたら、クライアントマシンをリブ ートします。すべてのマシンが再起動したら、クライアントをWLANに接続し、これらのログイ ベントをキャプチャします。

注:コントローラとWinServer RADIUS間のIPSec接続をセットアップするには、クライアント接 続が必要です。

Windows 2003システムログイベント

IPSec RADIUSが有効になっているWPA2/PEAP用に設定されたWLANクライアント接続が成功すると、WinServerで次のシステムイベントが生成されます。

192.168.30.105 = WinServer 192.168.30.2 = WLAN Controller

😽 Event Viewer							
Eile Action View	Help						
← → 1 € 1	• 🗟 🗟 😫						
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 = 192.168.30.2NAS-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 = 1Proxy-Policy-Name = Use Windows authentication for all users Authentication-Provider = Windows Authentication-Server = <undetermined> Policy-Name = 4404Authentication-Type = PEAP EAP-Type = Secured password (EAP-MSCHAP v2)コントローラ<> RADIUS IPSec接続が成功すると、WinServerログに次のセキュリティイベント が生成されます。

😫 Event Viewer							
Ele Action View H	<u>t</u> elp						
← → 🗈 🖬 🖆	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

<u> ワイヤレスLANコントローラのRADIUS IPSec成功のデバッグ例</u>

この設定を確認するには、コントローラでdebugコマンド**debug pm ikemsg enable**を使用します 。次に例を示します。

(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 = SHAAuthMethod = 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

<u>民族的捕獲</u>

以下に民族的捕獲の例を示す。

```
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
```

<u>関連情報</u>

- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.2
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。