WLC 및 Microsoft Windows 2003 IAS Server용 RADIUS IPSec 보안 구성

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>IPSec RADIUS 컨피그레이션</u> <u>WLC 구성</u> <u>IAS 구성</u> <u>Microsoft Windows 2003 도메인 보안 설정</u> <u>Windows 2003 시스템 로그 이벤트</u> <u>무선 LAN 컨트롤러 RADIUS IPSec 성공 디버그 예</u> <u>Ethreal 캡처</u> <u>관련 정보</u>

<u>소개</u>

이 가이드에서는 WCS 및 다음 WLAN 컨트롤러에서 지원되는 RADIUS IPSec 기능을 구성하는 방 법을 설명합니다.

- 4400 시리즈
- WiSM
- 3750G

컨트롤러 RADIUS IPSec 기능은 컨트롤러 GUI의 **Security(보안) > AAA > RADIUS Authentication Servers(RADIUS 인증 서버) 섹션에** 있습니다. 이 기능은 IPSec을 사용하여 컨트롤러와 IAS(RADIUS 서버) 간의 모든 RADIUS 통신을 암호화하는 방법을 제공합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LWAPP에 대한 지식
- RADIUS 인증 및 IPSec에 대한 지식
- Windows 2003 Server 운영 체제에서 서비스를 구성하는 방법에 대한 지식

<u>사용되는 구성 요소</u>

컨트롤러 RADIUS IPSec 기능을 구축하려면 다음 네트워크 및 소프트웨어 구성 요소를 설치하고 구성해야 합니다.

- WLC 4400, WiSM 또는 3750G 컨트롤러. 이 예에서는 소프트웨어 버전 5.2.178.0을 실행하는 WLC 4400을 사용합니다
- LAP(Lightweight Access Point). 이 예에서는 1231 Series LAP를 사용합니다.
- DHCP로 전환
- Microsoft 2003 Server가 Microsoft Certificate Authority 및 Microsoft IAS(Internet Authentication Service)와 함께 설치된 도메인 컨트롤러로 구성되었습니다.
- Microsoft 도메인 보안
- ADU 버전 3.6이 WPA2/PEAP로 구성된 Cisco 802.11 a/b/g 무선 클라이언트 어댑터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙을 참고하십시오.</u>

<u>IPSec RADIUS 컨피그레이션</u>

이 컨피그레이션 가이드에서는 Microsoft WinServer, Certificate Authority, Active Directory 또는 WLAN 802.1x 클라이언트의 설치 또는 컨피그레이션을 다루지 않습니다. 이러한 구성 요소는 컨트 롤러 IPSec RADIUS 기능을 구축하기 전에 설치 및 구성해야 합니다. 이 가이드의 나머지 부분에서 는 이러한 구성 요소에서 IPSec RADIUS를 구성하는 방법을 설명합니다.

- 1. Cisco WLAN 컨트롤러
- 2. Windows 2003 IAS
- 3. Microsoft Windows 도메인 보안 설정

<u>WLC 구성</u>

이 섹션에서는 GUI를 통해 WLC에서 IPSec을 구성하는 방법에 대해 설명합니다.

컨트롤러 GUI에서 다음 단계를 완료합니다.

1. 컨트롤러 GUI에서 Security(보안) > AAA > RADIUS Authentication(RADIUS 인증) 탭으로 이 동하여 새 RADIUS 서버를 추가합니다

CISCO SYSTEMS							S
Lalin.adus	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	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	1000
CA Certificate			3	192.168.30.105	1812	Enabled	

2. 새 RADIUS 서버의 IP 주소, 포트 1812 및 공유 암호를 구성합니다. IPSec **Enable-** 확인란을 선택하고 이러한 IPSec 매개변수를 구성한 다음 Apply를 **클릭합니다.참고:** 공유 암호는 RADIUS 서버를 인증하는 데 사용되며 IPSec 인증을 위한 사전 공유 키(PSK)로 사용됩니다

CISCO SYSTEMS		
	MONITOR WLANS CON	ROLLER WIRELESS SECURITY MANAGEMI
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
Wineless Protection	Notwork Usor	C Frankla
Policies	Network User	🖭 Enable
Trusted AP Policies Rogue Policies Standard Suppatures	Management	🗹 Enable
Custom Signatures Client Exclusion Policies	IPSec	Enable
AP Authentication	IPsec Parameters	
	IPSec	HMAC SHA1 ¥
	IPSEC Encryption	3DES 💌
	(Shared Seceret will be use	d as the Preshared Key)
	IKE Phase 1	Main 🔽
	Lifetime (seconds)	28800
	IKE Diffie Hellman Group	Group 2 (1024 bits) 🔽



IAS에서 다음 단계를 완료합니다.

1. Win2003에서 IAS 관리자로 이동하여 새 RADIUS 클라이언트를 추가합니다



3. 컨트롤러에 대한 새 원격 액세스 정책을 구성합니다

bild for the second service with the service s		
Elle Action Yiew Help		
⇔ → 🗈 🖬 🚱 🔂 😫		
Internet Authentication Service (Local)	Name	Order
E Clents	\$ 4404	1
E Remote Access Logging		
Remote Access Policies		
Connection Request Processing		

4. 컨트롤러 원격 액세스 정책의 속성을 편집합니다. NAS 포트 유형 - 무선 - IEEE 802.11을 추가 해야 합니다

.

.

4404 Properties	NAS-Port-Type	?×
Settings Specify the conditions that connection requests must match. Policy gonditions: NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 DR Wireless Add	Available types: ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110 ISDN Async V.120 ISDN Sync CK	BO211 F
Edt 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 @K Cancel Apply	Recycle Bn	

5. Edit **Profile(프로필 수정**)을 클릭하고 **Authentication(인증)** 탭을 클릭한 다음 MS-CHAP v2에 서 인증을 선택합니다

Specify the condit	dit Dial-in Profile		1
Policy <u>c</u> onditions: NAS-Port-Type n	Dial-in Constraints Authentication	IP Encryption thods you want to allo	Multilink Advanced
▲	EAP Methods	thentication version '	
f connection requassociated profile	User can chang	e password after it ha uthentication (MS-CH/	s expired AP)
Edit Profile	📕 Uger can chang	e password after it ha	s expired
Jnless individual policy controls acc f a connection re Denv remote 2	Encrypted authenticati Unencrypted authenticati Unauthenticated access	on (CHAP) :ation (PAP, SPAP)	
<u>G</u> rant remote .	Allo <u>w</u> clients to connect method.	st without negotiating	an authentication

6. EAP **Methods(EAP 방법)**를 클릭하고 EAP Providers(EAP 제공자)를 선택한 다음 PEAP를 EAP 유형으로 추가합니다

.

dit Dial-ın Profile			? >	KI 🛛		
Dial-in Constraints Authentication	IP		Multilink			
Select the authentication	methods you want	to allow for this	connection.			
EAP Methods						
Microsoft Encrypt	Select EAP Provid	lers				<u>?</u> ×
🔲 User can <u>c</u>	EAP types are neg	gotiated in the o	rder in which they	are listed		
🔲 Microsoft Encrypt	EAP types:					
🗖 Üger can c	Protected EAP (F	PEAPI				Move <u>U</u> p
Encrypted auther						Move Down
Unencrypted auti						
Unauthenticated acc						
Allow clients to cimethod.						
	Add	<u>E</u> dit	<u>R</u> emove	[ОК	Cancel
	OK.	Cancel	Apply	1		

7. Select **EAP** Providers(EAP 제공자 선택)에서 Edit(편집)를 클릭하고 풀다운 메뉴에서 Active Directory 사용자 계정 및 CA와 연결된 서버(예: tme.tme.com)를 선택합니다. EAP 유형 MSCHAP v2를 추가합니다

.

Select EAP Providers			? X		
EAP types are negotiated in the	Protected EAP Propert	les		<u> 1 × </u>	
EAP types:	This server identifies itse Select the certificate the	elf to callers befor at you want it to u	e the connection is completed. se as proof of identity.		
Protected EAP (PEAP)	Certificate (ssued	tme.tme.com	1		
	Friendly name:				
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:3	32:22 PM		
	Enable Fast Reconn	ect			
<u>A</u> dd <u>E</u> dit	Eap Types Secured password (EAF	P-MSCHAP ∨2)	FAP MSCHAPy2 Properties	in the second	X
OK Cancel	-				
			Number of authentication retri	ies: 2	
	Add E	dit Remi	Allow client to change pass	sword after it has expired	ł
			[minimum	Capcel	

8. Encryption(**암호화)** 탭을 클릭하고 원격 액세스에 대한 모든 암호화 유형을 선택합니다

Edit Dial-in Profile		<u>? ×</u>
Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
The following encryption le Routing and Remote Acce make sure the encryption le	vels are supported by ser ss. If you use a different r evels you select are supp	vers running Microsoft remote access server, orted by that software.
If No encryption is the only using data encryption.	option selected, then use	ers cannot connect by
Basic encryption (MPF)	РЕ 40-bit)	
✓ Strong encryption (MF	PE 56 bit)	
Strongest encryption (MPPE 128 bit)	
☑ No encryption		
<u> </u>		
	OK C	ancel <u>Apply</u>

9. **Advanced(고급)** 탭을 클릭하고 Service-Type(서비스 유형)으로 RADIUS Standard/Framed(RADIUS 표준/프레임)를 추가합니다

t Dial-in Profile		?
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connectio Access server. Attributes:	n attributes to be returi	ned to the Remote
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Add Edit	Bemove	

10. IP 탭을 클릭하고 Client may request an IP address(클라이언트가 IP 주소를 요청할 수 있음)를 선택합니다. 여기서는 스위치 또는 WinServer에서 DHCP를 활성화했다고 가정합니다

t Dial-in Profile		?
Authentication Dial-in Constraints	Encryption IP	Advanced Multilink
IP address assignment (Fra	amed-IP-Address)	
 Server must supply an Client may request an I 	P address	
C Server settings determi	ne IP address assignm	ent
C Assign a static IP addre	ess 255 . 2	55 . 255 . 255
If an IP address assignmen overrides these settings.	nt method is specified in	n the user profile, it
IP filters If your remote access serve you can define the filters to	er is Microsoft Routing apply during this conr	and Remote Access, nection.
To control the packets this click Input Filters.	interface receives,	Input Filters
To control the packets this Output Filters.	interface sends, click	<u>O</u> utput Filters
	ОК	Cancel Apply

<u>Microsoft Windows 2003 도메인 보안 설정</u>

Windows 2003 도메인 보안 설정을 구성하려면 다음 단계를 완료하십시오.

1. Default Domain Security Settings(기본 도메인 보안 설정) 관리자를 시작하고 무선 네트워크 (IEEE 802.11) 정책에 대한 새 보안 정책을 생성합니다

🚡 Default Domain Security Settings	
Eile Action Yiew Help	
← → 🗈 🖬 😰 🗟 😫 🎽	
Security 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(WLAN 네트워크 정책 속성)를 열고 Preferred Networks(기 본 설정 **네트워크)**를 클릭합니다. 새 기본 설정 WLAN을 추가하고 Wireless와 같은 WLAN SSID의 이름을 . 새로 선호하는 네트워크를 두 번 클릭하고 IEEE 802.1x 탭을 클릭합니다. EAP 유형으로 PEAP를 선택합니다

WLAN Network Policy Propertie	•s ? ×	
General Preferred Networks	Edit sroller Properties	? ×
,	Network Properties IEEE 802.1x	
Automatically conne	Enable network access control using IEEE 802.1x	
	EAPOL-Start message:	
Networks:	Parameters (seconds)	
Network Name (SSID) IEE	Max start: 3 Start period: 60	
sroller E	Held period: 60 (1997) Authentication period: 30 (1997)	
	EAP type: Protected EAP (PEAP)	
	Authenticate as guest when user or computer information is unavailable	
	Authenticate as computer when computer information is availab	le
Add <u>E</u> dit	Computer authentication: With user re-authentication	
	ОК	Cancel

3. PEAP Settings(PEAP 설정)를 클릭하고 Validate server certificate(서버 인증서 검증)를 선택 한 다음 Certificate Authority(인증 기관)에 설치된 Trusted Root Cert(신뢰할 수 있는 루트 인증 서)를 선택합니다. 테스트용으로 Automatically use my Windows login and password(내 Windows 로그인 및 비밀번호 자동 사용)에 대한 MS CHAP v2 상자의 선택을 취소합니다

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

4. Windows 2003 Default Domain Security Settings(Windows 2003 기본 도메인 보안 설정) 관리 자 창에서 4404와 같은 Active Directory 정책에 대해 다른 새 IP 보안 정책을 **생성합니다**

.

Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp			
🗢 🔶 🗈 💌 🗙 😰 🗟 🏦	18 <u>1</u>		
Security Settings	Name A	Description	Policy Assigned
🗉 👽 Account Policies	4404		Yes
E Local Policies	Server (Request Secu	For all IP traffic, always reg	No
Event Log	Client (Respond Only)	Communicate normally (uns	No
Restricted Groups	Secure Server (Requir	For all IP traffic, always reg	No
E System Services			
Registry			
E 🛄 File System			
Wireless Network (IEEE 802.11) Policies			
🗄 🧰 Public Key Policies			
Software Restriction Policies			
IP Security Policies on Active Directory (tme.co	(mc		

5. 새 4404 정책 속성을 편집하고 Rules 탭을 클릭합니다. 새 필터 규칙 추가 - IP 필렛 목록(동적

), 필터 작업(기본 응답), 인증(PSK), 터널(없음). 새로 생성된 필터 규칙을 두 번 클릭하고 Security Methods(보안 방법)를 선택합니다

4404 Prop	erties				?×
Rules	General				
) Securitu	rules for commun	icating with oth	er computers	
85	j occanty	raics for commun	icaang maroa	or compaters	
IP Secu	urity rules:				
IP Filt	er List	Filter Actio	in (Authentication	. Tu
. .)ynamic>	Default Re	esponse	Preshared Key	<n distant<="" td=""></n>
EC EC	it Rule Pro	perties			<u> ? ×</u>
	Security Met	hods Authentic	ation Methods	1	
					in the second
	Uffer these	security methods	when negotia	ting with another	computer.
	Security me	ethod preference	order:		
1	Туре	AH Integrity	ESP Confid	ential ES	A <u>d</u> d
	Custom	<none></none>	3DES	SH	
	Custom	<none></none>	DES	SH	<u>Ear</u>
	Custom	<none></none>	DES	ME	Remove
	Custom	SHA1	<none></none>	<n< td=""><td></td></n<>	
	Custom	MD5	<none></none>	<n< td=""><td>Move up</td></n<>	Move up
	•			Þ	Move d <u>o</u> wn
				(050)	
	Use se:	ssion <u>key</u> perfect	forward secred	y(PFS)	

6. Edit Security Method(보안 방법 수정)를 클릭하고 Custom Settings(맞춤형 설정) 라디오 버튼 을 클릭합니다. 이 설정을 선택합니다.참고: 이러한 설정은 컨트롤러 RADIUS IPSec 보안 설 정과 일치해야 합니다

Edit Security Method		P trathic, always req.
Security Method		
 Integrity and encrya Data will be encry unmodified. Integrity only Data will be verific encrypted. Qustom Settings 	Dition	curity method. t encryption (<u>AH</u>) :
	Session key settings: <u>G</u> enerate a new key every: 100000 <u>K</u> bytes	Generate a new key every: 28800 Generate a new key every: 2800 Genera

7. Edit Rule Properties(규칙 **속성** 수정) 아래의 Authentication Method(인증 방법) 탭을 클릭합니 다. 컨트롤러 RADIUS 컨피그레이션에 이전에 입력한 것과 동일한 공유 암호를 입력합니다

.

Rule Properti ecurity Methods Aut bet offe cor	Authentication Methods hentication methods specify how trust is ween computers. These authentication r ared and accepted when negotiating sec inputer.	established methods are curity with another
Authentication <u>m</u>	ethod preference order:	
Method Preshared Keu	Details	Add
r reandred ricy	0.000	<u>E</u> dit
	C Active Directory default (Kerberos	s. s V5 protocol) ation authority (CA):
	 Exclude the CA name from t Enable certificate to account Use this string (preshared key); 	<u>B</u> rowse he certificate request at mapping
	cisco	

이 시점에서 컨트롤러, IAS 및 도메인 보안 설정에 대한 모든 컨피그레이션이 완료됩니다. 컨트롤러 와 WinServer 모두에 모든 컨피그레이션을 저장하고 모든 시스템을 재부팅합니다. 테스트에 사용 되는 WLAN 클라이언트에서 루트 인증서를 설치하고 WPA2/PEAP를 구성합니다. 클라이언트에 루 트 인증서를 설치한 후 클라이언트 시스템을 재부팅합니다. 모든 시스템이 재부팅되면 클라이언트 를 WLAN에 연결하고 이러한 로그 이벤트를 캡처합니다.

참고: 컨트롤러와 WinServer RADIUS 간에 IPSec 연결을 설정하려면 클라이언트 연결이 필요합니 다.

<u>Windows 2003 시스템 로그 이벤트</u>

IPSec RADIUS가 활성화된 WPA2/PEAP에 대해 구성된 성공적인 WLAN 클라이언트 연결은 WinServer에서 다음 시스템 이벤트를 생성합니다.

192.168.30.2 = WLAN Controller

😽 Event Viewer							
Eile Action View	Help						
⇔ → 🗈 💽 🖆	• 🗗 🗟 🔒						
Event Viewer (Local)	System 22 eve	nt(s)					
8 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)
```

컨트롤러 <> RADIUS IPSec 연결이 성공하면 WinServer 로그에서 이 보안 이벤트가 생성됩니다.

😫 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	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>무선 LAN 컨트롤러 RADIUS IPSec 성공 디버그 예</u>

이 컨피그레이션을 확인하기 위해 컨트롤러에서 debug pm ikemsg enable 명령을 사용할 수 있습니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다.

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

67 TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc ookie=0x064bdcaf50d5f555 ID: packet[8] = 0x01000000 c0a81e69 HASH: hash[20] = 0x04814190 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 = secsLifeDuration =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 c0a81e69TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc ookie=0x064bdcaf50d5f555 msgid=0x73915967 HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc ookie=0x064bdcaf50d5f555 msgid=0x73915967 HASH: hash[20] = 0xcb862635 2b30202f 83fc5d7a 2264619d b09faed2 NOTIFY: doi=1 proto=ESP type=CONNECTED, spi[4] = 0xbb243261 data[8] = 0x434f4e4e 45435431

<u>Ethreal 캡처</u>

다음은 Ethreal Capture 샘플입니다.

```
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=0xb243261)
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=0xb243261)
6 1.625168 192.168.30.2 192.168.30.105 ESP ESP (SPI=0xb243261)
```

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

<u>관련 정보</u>

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 5.2
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.