Configurazione della protezione IPSec RADIUS per WLC e Microsoft Windows 2003 IAS Server

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione IPSec RADIUS Configurare il WLC Configurare IAS Impostazioni protezione dominio di Microsoft Windows 2003 Eventi registro eventi di sistema di Windows 2003 Esempio di debug riuscito del controller LAN wireless RADIUS IPSec Cattura etreale Informazioni correlate

Introduzione

In questa guida viene illustrato come configurare la funzionalità IPSec RADIUS supportata da WCS e dai seguenti controller WLAN:

- Serie 4400
- WiSM
- 3.750 G

La funzione IPSec RADIUS del controller si trova nella GUI del controller nella sezione **Sicurezza** > **AAA** > **Server di autenticazione RADIUS**. Questa funzionalità consente di crittografare tutte le comunicazioni RADIUS tra i controller e i server RADIUS (IAS) con IPSec.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze su LWAPP
- Informazioni sull'autenticazione RADIUS e su IPSec
- Informazioni sulla configurazione dei servizi nel sistema operativo Windows 2003 Server

Componenti usati

Per distribuire la funzionalità IPSec RADIUS del controller, è necessario installare e configurare i seguenti componenti di rete e software:

- Controller WLC 4400, WiSM o 3750G. In questo esempio viene usato WLC 4400 con software versione 5.2.178.0
- Lightweight Access Point (LAP). In questo esempio viene utilizzato il LAP serie 1231.
- Switch con DHCP
- Server Microsoft 2003 configurato come controller di dominio installato con Microsoft Certificate Authority e con Microsoft Internet Authentication Service (IAS).
- Microsoft Domain Security
- Cisco 802.11 a/b/g Wireless Client Adapter con ADU versione 3.6 configurato con WPA2/PEAP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Configurazione IPSec RADIUS

Questa guida alla configurazione non riguarda l'installazione o la configurazione di Microsoft WinServer, Certificate Authority, Active Directory o client WLAN 802.1x. Questi componenti devono essere installati e configurati prima della distribuzione della funzionalità RADIUS IPSec del controller. Nella parte restante di questa guida viene illustrato come configurare IPSec RADIUS su questi componenti:

- 1. Cisco WLAN Controller
- 2. Windows 2003 IAS
- 3. Impostazioni protezione dominio di Microsoft Windows

Configurare il WLC

In questa sezione viene spiegato come configurare IPSec sul WLC tramite la GUI.

Dalla GUI del controller, attenersi alla seguente procedura.

 Selezionare la scheda Security > AAA > RADIUS Authentication (Sicurezza > AAA > Autenticazione RADIUS) nella GUI del controller, quindi aggiungere un nuovo server RADIUS.

Cisco Systems	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	s cc
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 User	Management	Server Index	Server Address	; Port	IPSec	
Access Control Lists			1	192.168.30.10	1812	Disabled	
CA Certificate			3	192.168.30.105	1812	Enabled	

 Configurare l'indirizzo IP, la porta 1812 e un segreto condiviso del nuovo server RADIUS. Selezionare la casella di controllo Attiva IPSec, configurare i parametri IPSec e quindi fare clic su Applica.Nota: il segreto condiviso viene utilizzato sia per autenticare il server RADIUS che come chiave precondivisa (PSK) per l'autenticazione IPSec.

CISCO SYSTEMS		
. Alta Alta	MONITOR WLANS CONTI	ROLLER WIRELESS SECURITY MANAGEME
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	Support for RFC 3576	Disabled 💌
ID Certificate	Retransmit Timeout	2 seconds
Web Auth Certificate		
Wireless Protection Policies	Network User	🗹 Enable
Trusted AP Policies Rogue Policies 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 used	as the Preshared Key)
	IKE Phase 1	Main 🖌
	Lifetime (seconds)	28800
	IKE Diffie Hellman Group	Group 2 (1024 bits) 🗸

Configurare IAS

Completare i seguenti passaggi sullo IAS:

1. Passare al gestore IAS in Win2003 e aggiungere un nuovo client RADIUS.



2. Configurare le proprietà del client RADIUS con l'indirizzo IP e il segreto condiviso configurati

ettings			
Eriendly name:			
4404			
Address (IP or DNS	S):		
192.168.30.2			
Verifu			
If you are using ren attribute, specify th	mote access policies based ne vendor of the RADIUS (d on the client vendor client.	's
Client-Vendor:	HADIUS Standard		
Cli <u>e</u> nt-Vendor:	contain the Message Auth	enticator attribute	
Cli <u>e</u> nt-Vendor:	contain the Message Auth	enticator attribute	
Cli <u>e</u> nt-Vendor: <u>R</u> equest must o <u>S</u> hared secret: C <u>o</u> nfirm shared sec	contain the Message Auth	enticator attribute	
Cli <u>e</u> nt-Vendor: <u>B</u> equest must of <u>S</u> hared secret: C <u>o</u> nfirm shared sec	contain the Message Auth	enticator attribute	
Cli <u>e</u> nt-Vendor: <u>R</u> equest must of <u>S</u> hared secret: C <u>o</u> nfirm shared sec	contain the Message Auth	enticator attribute	

sul controller: 3. Configurare un nuovo criterio di accesso remoto per il

controller:

🍫 Internet Authentication Service		
Elle Action View Help		
← → 🗈 🖬 🕑 💀 😫		
Internet Authentication Service (Local)	Name	Order
RADIUS Clients Remote Access Logging	S 4404	1
Remote Access Policies Connection Request Processing		

4. Modificare le proprietà del criterio di accesso remoto del controller. Assicurarsi di aggiungere il tipo di porta NAS - Wireless - IEEE

•	
802.11	:

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 OR Wireles	Agailable types: Selected types: ADSL-CAP - Asymmetri ▲ Add >> ADSL-DMT - Asymmetri ▲ Add >> Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110
Add Edt Bemove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection Edt Profile	ISDN Async V.120 ISDN Sync
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 © Grant remote access permission	Recycle Bn
OK Cancel Apply	

5. Fare clic su **Modifica profilo**, fare clic sulla scheda **Autenticazione** e selezionare MS-CHAP v2 per

Autenticazione:

Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
	thods you want to allow	v for this connection.
EAP Methods	uthantiastion version 2	(MC CUAD2)
User can <u>chang</u>	uthentication version <u>≥</u> je password after it has uthentication (MS-CHAI	(MS-CHAP V2) expired P)
🔲 User can chang	je password after it has	expired
Encrypted authenticat	ion (CHAP) cation (PAP, SPAP)	
Unauthenticated access-		
Allow clients to connect method.	ct without negotiating a	n authentication
	EAP Methods Microsoft Encrypted A User can chang Microsoft Encrypted A User can chang Encrypted authenticat Unauthenticated access Allow clients to connered authenticat	 EAP Methods Microsoft Encrypted Authentication version 2 User can change password after it has Microsoft Encrypted Authentication (MS-CHAN) User can change password after it has Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Unauthenticated access Allow clients to connect without negotiating a method.

6. Fare clic su **Metodi EAP**, selezionare Provider EAP e aggiungere PEAP come tipo EAP:

dit Dial-in Profile		?	×	
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced		
Select the authentication	methods you want to allo	ow for this connection.		
EAP Methods				
Microsoft Encrypt	elect EAP Providers			? ×
🗖 User can <u>c</u>	EAP types are negotiate	ed in the order in which the	y are listed.	
Microsoft Encrypt	EAP types:			
🗖 Uger can c	Protected EAP (PEAP)			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	ОК	Cancel
	OK	Cancel Apply	J	

7. Fare clic su Modifica in Seleziona provider EAP e scegliere dal menu a discesa il server associato agli account utente e alla CA di Active Directory (ad esempio, tme.tme.com). Aggiungere il tipo EAP MSCHAP v2[.]

Select EAP Providers			? X		
EAP types are negotiated in the	Protected EAP Prope	itles		<u> ? ×</u>	
EAP types:	This server identifies it Select the certificate t	self to callers befor hat you want it to u	e the connection is completed. se as proof of identity.		
	Certificate issued	tme.tme.com			
	Friendly name:				
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:	32:22 PM		
	Enable Fast Recon	inect			
<u>A</u> dd <u>E</u> dit	Secured password (E/	AP-MSCHAP v2)	EAP MSCHAPy2 Properties		×
OK Cancel			Number of authentication retri	es: 2	
	Add	Edit Rem	Allow client to change pass	word after it has expired	
			[ОК	Cancel	

8. Fare clic sulla scheda Crittografia e verificare che tutti i tipi di crittografia siano accessibili in

Edit Dial-in Profile		<u>?×</u>
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
The following encryption k Routing and Remote Accor make sure the encryption	evels are supported by ser ess. If you use a different r levels you select are supp	vers running Microsoft emote access server, orted by that software.
If No encryption is the only using data encryption.	v option selected, then use	ars cannot connect by
☑ Basic encryption (MF	PE 40-bit)	
Strong encryption (M	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
☑ No encryption		
	ОК Са	ancel <u>Apply</u>

remoto:

9. Fare clic sulla scheda **Advanced** (Avanzate), quindi aggiungere RADIUS Standard/Framed come Service-Type (Tipo di

lit Dial-in Profile		<u>? ×</u>
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connectio Access server. Attributes:	n attributes to be retur	ned to the Remote
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
4		Þ
Add <u>E</u> dit	<u>H</u> emove	
	ОК	Cancel <u>Apply</u>

servizio):

10. Fare clic sulla scheda **IP** e selezionare **Client may request an IP address** (Il client potrebbe richiedere un indirizzo IP). Ciò presuppone che il protocollo DHCP sia abilitato su uno switch o su

Authentication	Encryption	Advance
Dial-in Constraints	IP	Multilin
IP address assignment (Fran	ned-IP-Address)	
© Server must supply an IF	^o address	
Client may request an IP	address	
O Server settings determin	e IP address assignmer	nt
O Assign a static IP addres	ss 255 . 255	5 . 255 . 255
If an IP address assignment overrides these settings.	method is specified in t	he user profile, it
IP filters		
If your remote access server you can define the filters to a	r is Microsoft Routing ar apply during this conner	nd Remote Acces ction.
To control the packets this i click Input Filters.	nterface receives,	Input Filters
To control the packets this i Output Filters.	nterface sends, click	Output Filters

WinServer."

Impostazioni protezione dominio di Microsoft Windows 2003

Completare questa procedura per configurare le impostazioni di protezione del dominio di Windows 2003:

1. Avviare lo strumento di gestione delle impostazioni predefinite di protezione del dominio e creare un nuovo criterio di protezione per i criteri di rete wireless (IEEE

<u>Eile A</u> ction <u>V</u> iew <u>H</u> elp	
← → 🗈 🖪 🗗 🗔 😭 🎽	
Security Settings	Name
🗄 📰 Account Policies	WI AN Network Policy
🗄 🛃 Local Policies	
🗄 🛃 Event Log	
🗄 🧕 Restricted Groups	
🕀 词 System Services	
File System	
Wireless Network (IEEE 802.11) Policies	

2. Aprire Proprietà criteri di rete WLAN e fare clic su **Reti preferite**. Aggiungere una nuova WLAN preferita e digitare il nome dell'SSID della WLAN, ad esempio Wireless. Fare doppio clic sulla nuova rete preferita e fare clic sulla scheda **IEEE 802.1x**. Scegliere PEAP come tipo EAP:

LAN Network Policy Propertie	• <u>? ×</u>	
General Preferred Networks	Edit 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 in the device de	
	Held period: 60 Authentication period: 30 EAP type: Protected EAP (PEAP) Settings.	
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 information is available</u> Computer authentication: With user re-authentication 	e
	ОК	Cancel

3. Fare clic su **PEAP Settings**, selezionare **Validate server certificate** (Convalida certificato server), quindi selezionare il certificato radice attendibile installato in Certificate Authority (Autorità di certificazione). A scopo di prova, deselezionare la casella MS CHAP v2 per Usa automaticamente il mio account di accesso e la mia password di

Windows.

Protected EAP Properties	<u>?×</u>	
When connecting:		
Validate server certificate		
Connect to these servers:		
Trusted <u>R</u> oot Certification Authorities:		
VeriSign Trust Network		
C Xcert EZ by DST		
1		
	EAP MSCHAPv2 Properties	
Select Authentication Method:		
Secured password (EAP-MSCHAP v2)	When connecting:	
Enable Fast Reconnect	Automatically use my Windows logon i password (and domain if any).	name and
	OK Cancel	

 Nella finestra Gestione impostazioni di protezione del dominio predefinito di Windows 2003 creare un altro nuovo criterio di protezione IP per i criteri di Active Directory, ad esempio 4404.



5. Modificare le proprietà del nuovo criterio 4404 e fare clic sulla scheda **Regole**. Aggiungere una nuova regola di filtro - Elenco filtri IP (dinamico); Operazione filtro (risposta predefinita);

Autenticazione (PSK); Tunnel (nessuno). Fare doppio clic sulla nuova regola di filtro creata e selezionare Metodi di

protezione:

Rules	erties General Security	rules for commun	icating with oth	ner computers	?× ^{IP tratti}
IP Secu IP Filtr ☑ <d< th=""><th>inty rules: er List lynamic></th><th>Filter Actio</th><th>on</th><th>Authentication. Preshared Key</th><th><u>Tu</u> <n< th=""></n<></th></d<>	inty rules: er List lynamic>	Filter Actio	on	Authentication. Preshared Key	<u>Tu</u> <n< th=""></n<>
	Security Met	hods Authentic	ation Methods : when negotia	 ting with anothe	r computer.
•	Type Custom	AH Integrity <none></none>	ESP Confid 3DES	lential ES SH ME	Add
	Custom Custom Custom Custom Custom	<none> <none> SHA1 MD5</none></none>	DES DES <none> <none></none></none>	ML SH ME <n <n< td=""><td><u>R</u>emove</td></n<></n 	<u>R</u> emove
				Þ	Move down
	Use se:	ssion <u>k</u> ey perfect	forward secret	sy (PFS)	

6. Fare clic su **Modifica metodo di protezione**, quindi sul pulsante di opzione Impostazioni **personalizzate**. Scegliere queste impostazioni.**Nota:** queste impostazioni devono corrispondere alle impostazioni di protezione IPSec RADIUS del controller.

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 	Detion Custom Security Method Settings Specify the settings for this custom security method.	? ×
	Session key settings: Generate a new key every: 100000 Kbytes OK Cance	ry:

7. Fare clic sulla scheda **Metodo di autenticazione** in Modifica proprietà regola. Immettere lo stesso segreto condiviso immesso in precedenza nella configurazione RADIUS del controller.

ntication Methods tion methods specify omputers. These au l accepted when ne reference order: Details cisco Contraction Method	y how trust is athentication r egotiating sec	established methods are curity with anoth <u>Add</u> <u>E</u> dit		
I accepted when ne reference order: Details cisco thentication Met ntication Method	egotiating sec	curity with anoth <u>Add</u> <u>E</u> dit		
reference order: Details cisco thentication Met ntication Method	Lind Proper	A <u>d</u> d <u>E</u> dit		
thentication Met	thod Proper	rties		
The authe between the	entication met he computers	thod specifies h s.	ow trust is establis	hed
Active Directory defa Use a certificate from	ault (Kerberos m this certifica A name from t	s V5 protocol) ation authority ((the certificate re	CA): Brows	e
Enable certifica	ate to accour hared key)	nt mapping		
	Enable certific Jse this <u>s</u> tring (pres	Exclude the UA name from Enable certificate to accour Use this <u>string (preshared key)</u>	Exclude the LA name from the certificate re Enable certificate to account mapping Use this string (preshared key):	Esclude the LA name from the certificate request Enable certificate to account mapping Use this string (preshared key):

A questo punto, vengono completate tutte le configurazioni per il controller, le impostazioni IAS e le impostazioni di sicurezza del dominio. Salvare tutte le configurazioni sia sul controller che su WinServer e riavviare tutti i computer. Sul client WLAN utilizzato per il test, installare il certificato radice e configurare per WPA2/PEAP. Dopo aver installato il certificato radice nel client, riavviare il computer client. Dopo il riavvio di tutti i computer, connettere il client alla WLAN e acquisire questi eventi di registro.

Nota: è necessaria una connessione client per impostare la connessione IPSec tra il controller e WinServer RADIUS.

Eventi registro eventi di sistema di Windows 2003

Se la connessione client WLAN configurata per WPA2/PEAP con IPSec RADIUS abilitato genera questo evento di sistema sul server 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)
```

Se la connessione IPSec RADIUS del controller <> riesce, nei registri di WinServer verrà generato questo evento di protezione:

😫 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

Esempio di debug riuscito del controller LAN wireless RADIUS IPSec

Per verificare questa configurazione, è possibile usare il comando debug **pm ikemsg enable** sul controller. Ecco un esempio.

```
(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

Cattura etreale

Di seguito è riportato un esempio di Cattura Etica.

```
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
```

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.2
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).