ىلإ دعب نع لوصولا نيوكت ASA IKEv2 ليمعو EAP-PEAP مادختساب يلصألا

المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة معلومات أساسية AnyConnect Secure Mobility Client اعتبارات التكوين <u>الرسم التخطيطي</u> للشبكة الشهادات محرك خدمات كشف الهوية (ISE) الخطوة 1. إضافة ASA إلى أجهزة الشبكة على ISE. الخطوة 2. قم بإنشاء اسم مستخدم في المخزن المحلي. ASA نظام التشغيل. Windows 7 الخطوة 1. تثبيت شهادة المرجع المصدق. الخطوة 2. تكوين اتصال VPN. التحقق من الصحة عميل Windows السجلات تص<u>حيح الأخطاء على ASA</u> مستوى الحزمة <u>استكشاف الأخطاء واصلاحها</u> معلومات ذات صلة

المقدمة

يقدم هذا المستند مثالا للتكوين الخاص بإصدار 9.3.2 من جهاز الأمان القابل للتكيف (ASA) من Cisco والإصدارات الأحدث، والذي يسمح بوصول الشبكة الخاصة الظاهرية (VPN) عن بعد لاستخدام بروتوكول تبادل مفتاح الإنترنت (IKEv2) المزود بمصادقة بروتوكول المصادقة المتوسع (EAP) القياسي. وهذا يسمح لعميل IKevs و ASA 7 الأصلي (وأي IKEv2 آخر مستند إلى المعايير) بالاتصال بالموجه ASA باستخدام مصادقة IKEv2 و EAP.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشبكة الخاصة الظاهرية (VPN) الأساسية والإصدار الثاني من بروتوكول IKEv
 - المصادقة والتفويض والمحاسبة (AAA) الأساسية ومعرفة RADIUS
 - التجربة مع تكوين ASA VPN
 - تجربة تكوين محرك خدمات الهوية (ISE)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- نظام التشغيل Microsoft Windows 7
- برنامج Cisco ASA، الإصدار 9.3.2 والإصدارات الأحدث
 - Cisco ISE، الإصدار 1.2 والإصدارات الأحدث

معلومات أساسية

اعتبارات AnyConnect Secure Mobility Client

لا يدعم عميل Windows IKEv2 الأصلي النفق المقسم (لا توجد سمات CONF REPLY التي يمكن قبولها من قبل عميل Windows 7)، لذلك فإن النهج الوحيد الممكن مع عميل Microsoft هو نفق حركة مرور البيانات (محددات حركة مرور 0/0). إذا كانت هناك حاجة إلى سياسة نفق تقسيم معين، فيجب إستخدام AnyConnect.

لا يدعم AnyConnect أساليب EAP القياسية التي يتم إنهاؤها على خادم PEAP) AAA، أمان طبقة النقل). إذا كانت هناك حاجة لإنهاء جلسات EAP على خادم AAA، فيمكن إستخدام عميل Microsoft.

التكوين

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



تم تكوين ASA للمصادقة باستخدام شهادة (يحتاج العميل إلى الثقة في تلك الشهادة). يتم تكوين عميل Windows 7 للمصادقة باستخدام EAP (EAP-PEAP).

يعمل ASA كبوابة VPN يقوم بإنهاء جلسة عمل IKEv2 من العميل. يعمل ISE كخادم AAA ينهي جلسة EAP من العميل. يتم تضمين حزم EAP في حزم IKE_AUTH لحركة مرور البيانات بين العميل و ASA(IKEv2) ثم في حزم RADIUS لحركة مرور المصادقة بين ASA و ISE.

الشهادات

تم إستخدام Microsoft Certificate Authority (CA) لإنشاء الشهادة ل ASA. متطلبات الشهادة لكي يتم قبولها بواسطة العميل الأصلي لنظام التشغيل Windows 7 هي:

- يجب أن يتضمن ملحق إستخدام المفتاح الموسع (EKU) مصادقة الخادم (تم إستخدام قالب "خادم ويب" في هذا المثال).
 - يجب أن يتضمن اسم الموضوع اسم المجال المؤهل بالكامل (FQDN) الذي سيتم إستخدامه من قبل العميل للاتصال (في هذا المثال ASAv.example.com).

لمزيد من التفاصيل حول عميل Microsoft، راجع <u>أستكشاف أخطاء إتصالات IKEv2 VPN وإصلاحها</u>.

ملاحظة: يعد نظام التشغيل Android 4.x أكثر تقييدا ويتطلب الاسم البديل للموضوع الصحيح وفقا لمعيار RFC 6125. لمزيد من المعلومات ل Android، راجع <u>IKEv2 من Android StrongSwan إلى Cisco IOS مع</u> <u>مصادقة EAP و RSA</u>.

لإنشاء طلب توقيع شهادة على ASA، تم إستخدام هذا التكوين:

hostname ASAv domain-name example.com

crypto ca trustpoint TP enrollment terminal

crypto ca authenticate TP crypto ca enroll TP

محرك خدمات كشف الهوية (ISE)

الخطوة 1. إضافة ASA إلى أجهزة الشبكة على ISE.

أختر **إدارة > أجهزة الشبكة**. ثبتت a سابق كلمة أن يكون استعملت ب ال ASA.

الخطوة 2. قم بإنشاء اسم مستخدم في المخزن المحلي.

أختر **الإدارة > الهويات > المستخدمين**. قم بإنشاء اسم المستخدم كما هو مطلوب.

ويتم تمكين كافة الإعدادات الأخرى بشكل افتراضي لكي يقوم ISE بمصادقة نقاط النهاية مع EAP-PEAP (بروتوكول المصادقة المتوسع المحمي).

ASA

ويكون تكوين الوصول عن بعد مماثلا ل IKEv1 و IKEv2.

aaa-server ISE2 protocol radius aaa-server ISE2 (inside) host 10.62.97.21 key cisco group-policy AllProtocols internal group-policy AllProtocols attributes vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0 crypto ipsec ikev2 ipsec-proposal ipsec-proposal protocol esp encryption aes-256 aes-192 aes protocol esp integrity sha-256 sha-1 md5 crypto dynamic-map DYNMAP 10 set ikev2 ipsec-proposal ipsec-proposal crypto map MAP 10 ipsec-isakmp dynamic DYNMAP crypto map MAP interface outside crypto ikev2 policy 10 encryption 3des

encryption 3des integrity sha group 2 prf sha lifetime seconds 86400 ونظرا لأن نظام التشغيل Windows 7 يرسل عنوان نوع IKE-ID في حزمة IKE_AUTH، فيجب إستخدام DefaultRAGgroup للتأكد من وصول الاتصال إلى مجموعة النفق الصحيحة. يصادق ASA بشهادة (مصادقة محلية) ويتوقع من العميل أن يستخدم EAP (مصادقة عن بعد). كما يحتاج ASA إلى إرسال طلب هوية EAP على وجه التحديد للعميل للاستجابة باستخدام إستجابة هوية EAP (query-identity).

```
tunnel-group DefaultRAGroup general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
ikev2 remote-authentication eap query-identity
ikev2 local-authentication certificate TP
وأخيرا، يلزم تمكين IKEv2 واستخدام الشهادة الصحيحة.
```

crypto ikev2 enable outside client-services port 443 crypto ikev2 remote-access trustpoint TP

نظام التشغيل Windows 7

الخطوة 1. تثبيت شهادة المرجع المصدق.

من أجل الثقة في الشهادة المقدمة من قبل ASA، يحتاج عميل Windows إلى الثقة في CA الخاص به. يجب إضافة شهادة المرجع المصدق هذه إلى مخزن شهادات الكمبيوتر (وليس مخزن المستخدم). يستخدم عميل Windows مخزن الكمبيوتر للتحقق من شهادة IKEv2.

أخترت in order to أضفت ال CA، **MMC > إضافة أو إزالة إضافات > شهادات**.

1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1			1	Canada Dant	E da E anada
ip-in	Vendor	â		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	Remove
Authorization Manager	Microsoft Cor				
Certificates	Microsoft Cor	н			(
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				Move Down
Device Manager	Microsoft Cor		Add >		
Disk Management	Microsoft and				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor	-			Advanced
1-1-1-1			-		
hption:					

انقر فوق زر انتقاء **حساب الكمبيوتر**.

Certificates snap-in	Send Feedback
This snap-in will always manage certificates for:	
My user account	
Service account	
Omputer account	
< Back	Next > Cancel

قم باستيراد المرجع المصدق إلى مراجع الشهادات الجذر الموثوق بها.



إذا لم يتمكن عميل Windows من التحقق من صحة الشهادة المقدمة من قبل ASA، فإنه يقوم بالإبلاغ عن:

IKE authentication credentials are unacceptable :13801

الخطوة 2. تكوين اتصال VPN.

أخترت in order to شكلت ال VPN توصيل من الشبكة ومشاركة مركز، **يربط إلى مكان عمل** in order to خلقت VPN توصيل.



أختر إستخدام اتصال الإنترنت (VPN).

How do you want to connect?





قم بتكوين العنوان باستخدام ASA FQDN. تأكد من حلها بشكل صحيح بواسطة خادم اسم المجال (DNS).

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:	ASAv.example.com
Destination name:	IKEv2 connection to ASA
Use a smart card	
🛞 📃 Allow other peop This option allow	le to use this connection s anyone with access to this computer to use this connection.
Don't connect no	ow; just set it up so I can connect later

قم بضبط الخصائص (مثل التحقق من صحة الشهادة) في إطار خصائص EAP المحمية، إذا كان ذلك مطلوبا.

Protected EAP Properties	×
When connecting:	
Validate server certificate	
Connect to these servers:	
Trusted Root Certification Authorities:	
AddTrust External CA Root	*
asa.mga.com	
ASAv ASAv	
Baltimore CyberTrust Root	
CA	
CA	
Certum Trusted Network CA	-
()	- F-
	+
Do not prompt user to authorize new servers or trusted certification authorities.	•
Do not prompt user to authorize new servers or trusted certification authorities.	•
Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method:	4
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co	⊧ nfigure
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Enable Fast Reconnect	⊧ nfigure
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Co Co Enable Fast Reconnect Enforce Network Access Protection	⊧
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV	⊧ nfigure
 III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy 	⊧ nfigure
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	▶
III Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Co Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK	nfigure
Image: Construction of the server of the	▶ nfigure

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

عميل Windows

عند الاتصال، أدخل بيانات الاعتماد الخاصة بك.





IKEv2 connection to ASA Disconnected WAN Miniport (IKEv2)

User name: cisco Password: [To change the saved password, click here]
Domain:

بعد المصادقة الناجحة، يتم تطبيق تكوين IKEv2.

Connect	ing to ASA-IKEv2
s,	Registering your computer on the network
	Cancel

تم إنهاء جلسة العمل.



تم تحديث جدول التوجيه باستخدام المسار الافتراضي باستخدام واجهة جديدة ذات المقياس المنخفض.

C:\Users\admin>route print _____ Interface List IKEv2 connection to ASA.....41 d2 cb 54Karta Intel(R) PRO/1000 MT Desktop Adapter 27 00 08...11 Software Loopback Interface 1.....1 e0 Karta Microsoft ISATAP 00 00 00 00 00 00 00...15 e0 Teredo Tunneling Pseudo-Interface 00 00 00 00 00 00 00...12 e0 Karta Microsoft ISATAP #4 00 00 00 00 00 00 00...22 IPv4 Route Table :Active Routes Network Destination Gateway Interface Metric Netmask 192.168.10.68 4491 192.168.10.1 0.0.0.0 0.0.0.0 On-link 192.168.1.10 11 0.0.0.0 0.0.0.0 4236 192.168.10.68 192.168.10.1 255.255.255.255 10.62.71.177 On-link 127.0.0.1 4531 255.0.0.0 127.0.0.0 4531 255.255.255.255 127.0.0.1 On-link 127.0.0.1 On-link 127.0.0.1 4531 255.255.255.255 127.255.255.255 On-link 192.168.1.10 266 255.255.255.255 192.168.1.10 On-link 192.168.10.68 4491 255.255.255.0 192.168.10.0 On-link 192.168.10.68 4491 255.255.255.255 192.168.10.68 On-link 192.168.10.68 4491 255.255.255.255 192.168.10.255 127.0.0.1 4531 On-link 240.0.0.0 224.0.0.0 4493 On-link 192.168.10.68 240.0.0.0 224.0.0.0 On-link 192.168.1.10 11 240.0.0.0 224.0.0.0 On-link 127.0.0.1 4531 255.255.255.255 255.255.255 On-link 192.168.10.68 4491 255.255.255.255 255.255.255

On-link

192.168.1.10

266

السجلات

بعد المصادقة الناجحة يبلغ ASA:

255.255.255.255 255.255.255.255

ASAv(config)# show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Index Username : cisco : 13 Assigned IP : 192.168.1.10 Public IP : 10.147.24.166 Protocol : IKEv2 IPsecOverNatT License : AnyConnect Premium Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)AES256 Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 Bytes Tx : 0 : 7775 : 94 Bytes Rx Pkts Tx : 0 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : AllProtocols Tunnel Group : DefaultRAGroup Login Time : 17:31:34 UTC Tue Nov 18 2014 Duration : 0h:00m:50s Inactivity : 0h:00m:00s VLAN VLAN Mapping : N/A : none Audt Sess ID : c0a801010000d000546b8276 Security Grp : none IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 :TKEv2 Tunnel ID : 13.1 UDP Src Port : 4500 UDP Dst Port : 4500 Rem Auth Mode: EAP Loc Auth Mode: rsaCertificate Encryption : 3DES Rekey Int (T): 86400 Seconds Hashing : SHA1 Rekey Left(T): 86351 Seconds : SHA1 D/H Group : 2 PRF : Filter Name :IPsecOverNatT Tunnel ID : 13.2 Local Addr : 0.0.0.0/0.0.0.0/0/0 Remote Addr : 192.168.1.10/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA1 Encapsulation: Tunnel Rekey Int (T): 28800 Seconds Rekey Left(T): 28750 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 0 Bytes Rx : 7834 Pkts Tx : 0 Pkts Rx : 95

تشير سجلات ISE إلى المصادقة الناجحة باستخدام قواعد المصادقة والتفويض الافتراضية.

ahaha		1								Locense Warning 🔥
cisco Identity Serv	rices Engin	e		4	Home 0	perations •	Policy 🔻	Guest Access 💌 Admi	nistration 🛛 🕶	
Authentications	E Report	s.	Endpoint	t Protection Ser	vice 💊	Troubleshoot	8			
Misconfigured	Supplicant	s ®		Misconfi	gured Networ	k Devices	Ð	RADIUS Drops	Ð	Client Stopped
0					0			6		0
ቨ Show Live Sessions	🙀 Add or	Remov	ve Columns -	🛞 Refresh	😗 Reset Rep	eat Counts			R	efresh Every 1 min
Time •	Status All 🔻 De	at	Repeat C	Identity (7)	Endpoint	t ID (i)	Authorization I	Policy (i)	Authorization Profiles	Network Device
2014-11-18 18:31:34	0	à	3	cisco	10.147.2	4.166				
2014-11-18 17:52:07		ò		cisco	10.147.2	4.166	Default >> Ba	sic_Authenticated_Access	PermitAccess	ASAV

تشير التفاصيل إلى أسلوب PEAP.

Authentication Details

Source Timestamp	2014-11-19 08:10:02.819
Received Timestamp	2014-11-19 08:10:02.821
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	cisco
User Type	User
Endpoint Id	10.147.24.166
Endpoint Profile	
IP Address	
Authentication Identity Store	Internal Users
Identity Group	
Audit Session Id	c0a8010100010000546c424a
Authentication Method	MSCHAPV2
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Login
Network Device	ASAv
Device Type	All Device Types
Location	All Locations
NAS IP Address	10.62.71.177
NAS Port Id	
NAS Port Type	Virtual
Authorization Profile	PermitAccess

تصحيح الأخطاء على ASA

تتضمن أهم تصحيح الأخطاء ما يلي:

ASAv# debug crypto ikev2 protocol 32most debugs omitted for clarity>

حزمة IKE_SA_INIT التي يتم استقبالها بواسطة ASA (تتضمن مقترحات IKEv2 وتبادل المفاتيح ل Diffie-Hellman (((DH))):

> [IKEv2-PROTO-2: Received Packet [From 10.147.24.166:500/To 10.62.71.177:500/VRF i0:f0 Initiator SPI : 7E5B69A028355701 - Responder SPI : 0000000000000 Message id: 0 ,IKEv2 IKE_SA_INIT Exchange REQUESTIKEv2-PROTO-3: Next payload: SA version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 528 :Payload contents SA Next payload: KE, reserved: 0x0, length: 256 last proposal: 0x2, reserved: 0x0, length: 40 ,Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 last transform: 0x3 reserved: 0x0: length: 8

إستجابة IKE_SA_INIT للبادئ (تتضمن مقترحات IKEv2، وتبادل المفاتيح ل DH، وطلب الشهادة):

IKEv2-PROTO-2: (30): Generating IKE_SA_INIT message ,(IKEv2-PROTO-2: (30): IKE Proposal: 1, SPI size: 0 (initial negotiation Num. transforms: 4 3DES(30): SHA1(30): SHA96(30): DH_GROUP_1024_MODP/Group :(30) :2IKEv2-PROTO-5 Construct Vendor Specific Payload: DELETE-REASONIKEv2-PROTO-5: Construct Vendor :Specific Payload: (CUSTOM)IKEv2-PROTO-5: Construct Notify Payload :NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Construct Notify Payload :NAT_DETECTION_DESTINATION_IPIKEv2-PROTO-5: Construct Vendor Specific Payload : (FRAGMENTATION (30 IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:500/From [VRF i0:f0/10.62.71.177:500 IKE_AUTH للعميل المزود ب IKE-ID، طلب الشهادة، مجموعات التحويل المقترحة، التكوين المطلوب، ومحددات

חות אשמיל העלפג ה לו-שור מעד השויד המשונס, מجموعات היבפיל המשילכה, הרצפיל המשילבה, הרצפילי המשופה, ومحددا حركة مرور البيانات:

إستجابة IKE_AUTH من ASA التي تتضمن طلب هوية EAP (الحزمة الأولى مع امتدادات EAP). تتضمن الحزمة أيضا الشهادة (إذا لم يكن هناك شهادة صحيحة على ASA هناك فشل):

IKEv2-PROTO-2: (30): Generating EAP request IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:4500/From 10.62.71.177:4500/VRF [i0:f0 إستجابة EAP التي تم تلقيها بواسطة ASA (الطول 5، الحمولة: cisco):

REAL Decrypted packet:(30): Data: 14 bytes :(30) EAP(30): Next payload: NONE, reserved: 0x0, length: 14 :(30) **Code: response**: id: 36, length: 10 :(30) **Type: identity** :(30) EAP data: 5 bytes :(30) ثم يتم تبادل حزم متعددة كجزء من EAP-PEAP. وأخيرا، يتلقى ASA نجاح EAP ويرسل إلى الملتمس:

```
Payload contents:
EAP(30): Next payload: NONE, reserved: 0x0, length: 8 :(30)
Code: success: id: 76, length: 4 :(30)
مصادقة النظير ناجحة:
```

IKEv2-PROTO-2: (30): Verification of peer's authenctication data PASSED وتم إنهاء جلسة عمل الشبكة الخاصة الظاهرية (VPN) بشكل صحيح.

مستوى الحزمة

يتم تضمين طلب هوية EAP في "المصادقة الموسعة" ل IKE_AUTH Send بواسطة ASA. مع طلب الهوية، يتم إرسال IKE_ID والشهادات.

No.	Source	Destination	Protocol	Length	Info	
1	10.147.24.166	10.62.71.177	ISAKMP	570	IKE_SA_I	NIT
2	10.62.71.177	10.147.24.166	ISAKMP	501	IKE_SA_I	NIT
3	10.147.24.166	10.62.71.177	ISAKMP	990	IKE_AUTH	
4	10.147.24.166	10.62.71.177	ISAKMP	959	IKE_AUTH	
5	10.62.71.177	10.147.24.166	EAP	1482	Request,	Identity
6	10.62.71.177	10.147.24.166	ISAKMP	1514		
Þ -	Length: 1440 Type Payload: Vende Type Payload: Iden	or ID (43) : Unknow tification - Respor	n Vendor der (36)	ID		
~	Type Payload: Cert	ificate (37)	.uci (50)			
	Next payload: Aut	thentication (39)				
	0 = Criti	ical Bit: Not Criti	cal			
	Payload length: 1	203				
	Certificate Encod	ling: X.509 Certifi	cate - S	ignatur	e (4)	
1	Certificate Data	(iso.2.840.113549.	1.9.2=AS	Av.exam	ple.com)	
٥. ٩	Type Payload: Auth	entication (39)				
Δ.	Type Payload: Exte	nsible Authenticati	ion (48)			
	Next payload: NON	IE / No Next Payloa	d (0)			
	0 = Criti	ical Bit: Not Criti	cal			
	Payload length: 1	LO				
	Extensible Auther	ntication Protocol				
	Code: Request (1)				
	Id: 36					
	Length: 6					
	Type: Identity	(1)				
	Identity:					
	مان مُأْي (EAD DEAD)	ا مُلا اللمال ملا بأبير		السلام م		

يتم تضمين جميع حزم EAP التالية في IKE_AUTH. بعد أن يؤكد الطالب الأسلوب (EAP-PEAP)، يبدأ في بناء نفق طبقة مآخذ التوصيل الآمنة (SSL) الذي يحمي جلسة MSCHAPv2 المستخدمة للمصادقة.

5 10.62.71.177	10.147.24.166	EAP	1482 Request, Identity
6 10.62.71.177	10.147.24.166	ISAKMP	1514
7 10.147.24.166	10.62.71.177	ISAKMP	110 IKE_AUTH
8 10.147.24.166	10.62.71.177	EAP	84 Response, Identity
9 10.62.71.177	10.147.24.166	EAP	80 Request, Protected EAP (EAP-PEAP)
10 10.62.71.177	10.147.24.166	ISAKMP	114
11 10.147.24.166	10.62.71.177	ISAKMP	246 IKE_AUTH
12 10.147.24.166	10.62.71.177	SSL	220 Client Hello
13 10.62.71.177	10.147.24.166	TLSv1	1086 Server Hello

بعد تبادل حزم متعددة، يؤكد ISE النجاح.

43 10.147.24.166	10.62.71.177	ISAKMP	150 IKE_AUTH
44 10.147.24.166	10.62.71.177	TLSv1	117 Application Data
45 10.62.71.177	10.147.24.166	EAP	78 Success

Type Payload: Extensible Authentication (48) Next payload: NONE / No Next Payload (0) 0... ... = Critical Bit: Not Critical Payload length: 8

Extensible Authentication Protocol Code: Success (3) Id: 101 Length: 4

يتم إكمال جلسة عمل IKEv2 بواسطة ASA، ويتم دفع رد التكوين النهائي (رد التكوين مع قيم مثل عنوان IP المعين) ومجموعات التحويل ومحددات حركة مرور البيانات إلى عميل VPN.

45 10.62.71.177	10.147.24.166	EAP	78 Success
46 10.62.71.177	10.147.24.166	ISAKMP	114
47 10.147.24.166	10.62.71.177	ISAKMP	126 IKE_AUTH
48 10.147.24.166	10.62.71.177	ISAKMP	98 IKE_AUTH
49 10.62.71.177	10.147.24.166	ISAKMP	222 IKE_AUTH

Type Payload: Configuration (47)

Type Payload: Security Association (33)

▼ Type Payload: Traffic Selector - Initiator (44) # 1 Next payload: Traffic Selector - Responder (45) 0... = Critical Bit: Not Critical Payload length: 24 Number of Traffic Selector: 1 Traffic Selector Type: TS IPV4 ADDR RANGE (7) Protocol ID: Unused Selector Length: 16 Start Port: 0 End Port: 65535 Starting Addr: 192.168.1.10 (192.168.1.10) Ending Addr: 192.168.1.10 (192.168.1.10) ▼ Type Payload: Traffic Selector - Responder (45) # 1 Next payload: Notify (41) 0... = Critical Bit: Not Critical Payload length: 24

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- <u>دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN، 9.3</u>
 - <u>دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2</u>
 - <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما