使用EAP-PEAP和本地Windows客戶端配置ASA IKEv2遠端訪問

目錄

簡介 必要條件 需求 採用元件 背景資訊 AnyConnect安全移動客戶端注意事項 設定 網路圖表 慿證 ISE 步驟1.將ASA新增到ISE上的網路裝置。 步驟2.在本地儲存中建立使用者名稱。 **ASA** Windows 7 步驟1.安裝CA證書。 步驟2.配置VPN連線。 驗證 Windows客戶端 記錄檔 ASA上的調試 封包層級 疑難排解 相關資訊

簡介

本文檔提供了思科自適應安全裝置(ASA)版本9.3.2及更高版本的配置示例,允許遠端VPN訪問使用 網際網路金鑰交換協定(IKEv2)和標準可擴展身份驗證協定(EAP)身份驗證。這允許本地Microsoft Windows 7客戶端(以及任何其他基於標準的IKEv2)通過IKEv2和EAP身份驗證連線到ASA。

必要條件

思科建議您瞭解以下主題:

- •基本VPN和IKEv2知識
- •基本驗證、授權及記帳(AAA)和RADIUS知識
- ASA VPN配置經驗
- •身分識別服務引擎(ISE)配置體驗

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft Windows 7
- Cisco ASA軟體9.3.2版及更高版本
- Cisco ISE版本1.2及更高版本

背景資訊

AnyConnect安全移動客戶端注意事項

本機Windows IKEv2客戶端不支援拆分隧道(Windows 7客戶端無法接受任何CONF REPLY屬性),因此Microsoft客戶端唯一可能的策略是隧道所有流量(0/0流量選擇器)。 如果需要特定拆分 隧道策略,應使用AnyConnect。

AnyConnect不支援在AAA伺服器上終止的標準化EAP方法(PEAP、傳輸層安全)。如果需要終止 AAA伺服器上的EAP會話,則可以使用Microsoft客戶端。

設定

附註:使用<u>命令查詢工具(</u>僅供<u>已註冊</u>客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



ASA配置為使用證書進行身份驗證(客戶端需要信任該證書)。 Windows 7客戶端配置為使用 EAP(EAP-PEAP)進行身份驗證。

ASA充當從客戶端終止IKEv2會話的VPN網關。ISE充當從客戶端終止EAP會話的AAA伺服器。 EAP資料包封裝在客戶端和ASA(IKEv2)之間流量的IKE_AUTH資料包中,然後封裝在ASA和ISE之 間身份驗證流量的RADIUS資料包中。

慿證

已使用Microsoft證書頒發機構(CA)為ASA生成證書。要被Windows 7本機客戶端接受的證書要求是

- 擴展金鑰使用(EKU)擴展應該包括伺服器身份驗證(在該示例中使用了模板「Web伺服器」)。
- Subject-Name應包含客戶端用於連線的完全限定域名(FQDN)(在本示例中為 ASAv.example.com)。

有關Microsoft客戶端的詳細資訊,請參閱<u>排除IKEv2 VPN連線故障</u>。

附註:Android 4.x更具限制性,需要根據RFC 6125使用正確的主題替代名稱。有關Android的 詳細資訊,請<u>參閱從Android strongSwan到Cisco IOS with EAP和RSA Authentication的</u> IKEv2。

為了在ASA上生成證書簽名請求,已使用以下配置:

hostname ASAv domain-name example.com

crypto ca trustpoint TP enrollment terminal

crypto ca authenticate TP crypto ca enroll TP

ISE

步驟1.將ASA新增到ISE上的網路裝置。

選擇Administration > Network Devices。設定將由ASA使用的預共用密碼。

步驟2.在本地儲存中建立使用者名稱。

選擇Administration > Identities > Users。根據需要建立使用者名稱。

預設情況下,ISE啟用所有其他設定以使用EAP-PEAP(受保護的可擴展身份驗證協定)對終端進 行身份驗證。

ASA

IKEv1和IKEv2的遠端訪問配置類似。

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 integrity sha group 2 prf sha lifetime seconds 86400

由於Windows 7在IKE_AUTH資料包中傳送IKE-ID型別地址,因此應使用**DefaultRAGroup**以確保連 線位於正確的隧道組。ASA使用證書(本地身份驗證)進行身份驗證,並期望客戶端使用EAP(遠 端身份驗證)。此外,ASA需要專門為客戶端傳送EAP身份請求以使用EAP身份響應(queryidentity)進行響應。

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

最後,需要啟用IKEv2並使用正確的證書。

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

Windows 7

步驟1.安裝CA證書。

為了信任ASA提供的證書,Windows客戶端需要信任其CA。應將該CA證書新增到電腦證書儲存區 (而不是使用者儲存區)。 Windows客戶端使用電腦儲存區驗證IKEv2證書。

若要新增CA,請選擇MMC > Add or Remove Snap-ins > Certificates。

			(19) a	and Brok	
sp-in	Vendor	Â		Continent Cont	Edit Extensions
ActiveX Control	Microsoft Cor		4	Certificates (Local Computer)	Remove
Authorization Manager	Microsoft Cor				
Certificates	Microsoft Cor	Ξ			
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor		10.00		Move Down
Device Manager	Microsoft Cor		Add >		- nore contri
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
1.0					
nption:					

按一下Computer account單選按鈕。

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

將CA匯入到受信任的根證書頒發機構。



如果Windows客戶端無法驗證ASA提供的證書,則會報告:

13801: IKE authentication credentials are unacceptable

步驟2.配置VPN連線。

要從網路和共用中心配置VPN連線,請選擇Connect to a workplace以建立VPN連線。



選擇Use my Internet connection(VPN)。

How do you want to connect?



使用ASA FQDN配置地址。確保域名伺服器(DNS)已正確解析。

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 people to use this connection This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

如果需要,請在「受保護的EAP屬性」視窗中調整屬性(如證書驗證)。

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root
asa.mga.com
ASAV
Baltimore CyberTrust Root
Certum Trusted Network CA
Select Authentication Method:
Enable Fast Reconnect
Configure: The configure of the conf

驗證

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸 出的分析。

Windows客戶端

連線時,請輸入憑據。

Cisco AnyConnect Secure Mobility Client Connection Disabled	IKEv2 connection to ASA Disconnected WAN Miniport (IKEv2)
Street IKEv	2 connection to ASA
User name:	isco
Domain:	
Save this use Me only Anyone v Connect	er name and password for the following users: who uses this computer Cancel Properties Help

身份驗證成功後,將應用IKEv2配置。

Connect	ing to ASA-IKEv2
S .	Registering your computer on the network
	Cancel

會話已啟動。



通過使用具有低度量的新介面,路由表已用預設路由更新。

C:\Users\admin>route print

Interface List
41.....IKEv2 connection to ASA
11...08 00 27 d2 cb 54Karta Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
15...00 00 00 00 00 00 00 e0 Karta Microsoft ISATAP
12...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
22...00 00 00 00 00 00 e0 Karta Microsoft ISATAP #4

IPv4 Route Table

======		======	 	=====	=====	=====	======	======	======	
Active	Routes	:								

Network	Destinatio	on Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.68	4491
	0.0.0.0	0.0.0.0	On-link	192.168.1.10	11
10.6	52.71.177	255.255.255.255	192.168.10.1	192.168.10.68	4236
1	L27.0.0.0	255.0.0.0	On-link	127.0.0.1	4531
1	L27.0.0.1	255.255.255.255	On-link	127.0.0.1	4531
127.255	5.255.255	255.255.255.255	On-link	127.0.0.1	4531
192.	168.1.10	255.255.255.255	On-link	192.168.1.10	266
192.	168.10.0	255.255.255.0	On-link	192.168.10.68	4491
192.1	L68.10.68	255.255.255.255	On-link	192.168.10.68	4491
192.16	58.10.255	255.255.255.255	On-link	192.168.10.68	4491
2	224.0.0.0	240.0.0.0	On-link	127.0.0.1	4531
2	224.0.0.0	240.0.0.0	On-link	192.168.10.68	4493
2	224.0.0.0	240.0.0.0	On-link	192.168.1.10	11
255.255	5.255.255	255.255.255.255	On-link	127.0.0.1	4531
255.255	5.255.255	255.255.255.255	On-link	192.168.10.68	4491
255.255	5.255.255	255.255.255.255	On-link	192.168.1.10	266

記錄檔

身份驗證成功後,ASA報告:

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

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Index : 13 Public IP : **10.147.24.166** : cisco Username Assigned IP : 192.168.1.10 Protocol : IKEv2 IPsecOverNatT License : AnyConnect Premium Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)AES256 Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 Bytes Tx : 0 Bytes Rx : 7775 Pkts Tx : 0 Pkts Rx : 94 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 Mapping : N/A VLAN : none Audt Sess ID : c0a801010000d000546b8276 Security Grp : none IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 IKEv2: Tunnel ID : 13.1 UDP Src Port : 4500 UDP Dst Port : 4500 Rem Auth Mode: EAP Loc Auth Mode: rsaCertificate Hashing : SHA1 Encryption : 3DES Rekey Int (T): 86400 Seconds Rekey Left(T): 86351 Seconds PRF : SHA1 D/H Group : 2 Filter Name : IPsecOverNatT: Tunnel ID : 13.2 Local Addr : 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

ISE日誌表示使用預設身份驗證和授權規則成功進行身份驗證。

cisco Identity Serv	vices Engine		6	Home Operations	Policy	Guest Access	Administration •	Loosas Warning 👖
Authentications	E Reports	🔯 Endpoint	Protection Sen	rice 🍾 Troublesh	tot			
Misconfigured O	l Supplicants 🤅		Misconfiç	gured Network Devices 0	¢	RADIUS D	Drops T	Client Stopped O
🔝 Show Live Sessions	🏭 Add or Rem	ove Columns 🔻	😵 Refresh	😗 Reset Repeat Count	8			Refresh Every 1 minu
Time •	Status All T	Repeat C	Identity (7)	Endpoint ID	Authorization	Policy ⁽⁷⁾	Authorization	Profiles Network Device
2014-11-18 18:31:34	0 0	3	cisco	10.147.24.166				
2014-11-18 17:52:07	0		cisco	10.147.24.166	Default >> Ba	sic_Authenticated_A	ccess PermitAccess	ASAV

詳細資訊顯示PEAP方法。

Aut	hen	tica	tion	Detai	Is
Aut	nen	ucu	cion	Detui	19

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

ASA上的調試

最重要的調試包括:

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

ASA接收的IKE_SA_INIT資料包(包括Diffie-Hellman(DH)的IKEv2建議和金鑰交換):

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 : 00000000000000 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
.....

對發起方的IKE_SA_INIT響應(包括IKEv2提議、DH金鑰交換和證書請求):

IKEv2-PROTO-2: (30): Generating IKE_SA_INIT message IKEv2-PROTO-2: (30): IKE Proposal: 1, SPI size: 0 (initial negotiation), Num. transforms: 4 (30): 3DES(30): SHA1(30): SHA96(30): DH_GROUP_1024_MODP/Group 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 10.62.71.177:500/VRF i0:f0]

﹐適用於具有IKE-ID、證書請求、建議的轉換集、請求的配置和流量選擇器的客戶端的IKE_AUTH:

IKEv2-PROTO-2: (30): Received Packet [From 10.147.24.166:4500/To 10.62.71.177:500/VRF i0:f0] (30): Initiator SPI : 7E5B69A028355701 - Responder SPI : 1B1A94C7A7739855 Message id: 1 (30): IKEv2 IKE_AUTH Exchange REQUESTIKEv2-PROTO-3: (30): Next payload: ENCR, version: 2.0 (30): Exchange type: IKE_AUTH, flags: INITIATOR (30): Message id: 1, length: 948(30):

來自ASA的IKE_AUTH響應,包括EAP身份請求(第一個具有EAP擴展的資料包)。 該資料包還包 括證書(如果ASA上沒有正確的證書,則表明存在故障):

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]

ASA接收的EAP響應(長度5,負載:思科):

(30): 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

然後作為EAP-PEAP的一部分交換多個資料包。最後,ASA收到EAP成功並將其轉發給請求方:

(30): EAP(30): Next payload: NONE, reserved: 0x0, length: 8
(30): Code: success: id: 76, length: 4
對等身份驗證成功:

IKEv2-PROTO-2: (30): Verification of peer's authenctication data PASSED **VPN會話正確完成。**

封包層級

EAP身份請求封裝在ASA傳送的IKE_AUTH的「可擴展身份驗證」中。與身份請求一起傳送 IKE_ID和證書。

No.	Source	Destination	Protocol	Length	Info
1	10.147.24.166	10.62.71.177	ISAKMP	570	IKE_SA_INIT
2	10.62.71.177	10.147.24.166	ISAKMP	501	IKE_SA_INIT
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	

Length: 1440

```
> Type Payload: Vendor ID (43) : Unknown Vendor ID
```

```
Type Payload: Identification - Responder (36)
```

```
Type Payload: Certificate (37)
```

Next payload: Authentication (39)

0... = Critical Bit: Not Critical

Payload length: 1203

Certificate Encoding: X.509 Certificate - Signature (4)

Certificate Data (iso.2.840.113549.1.9.2=ASAv.example.com)

- > Type Payload: Authentication (39)
- ▼ Type Payload: Extensible Authentication (48)
 - Next payload: NONE / No Next Payload (0)

```
0... .... = Critical Bit: Not Critical
```

```
Payload length: 10
```

▼ Extensible Authentication Protocol Code: Request (1) Id: 36 Length: 6 Type: Identity (1) Identity:

所有後續的EAP資料包都封裝在IKE_AUTH中。請求方確認方法(EAP-PEAP)後,開始建立安全套接 字層(SSL)隧道,該隧道保護用於身份驗證的MSCHAPv2會話。

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

交換多個資料包後,ISE確認成功。

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

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

IKEv2會話由ASA完成,最終配置(配置回覆包含值,如分配的IP地址)、轉換集和流量選擇器將 推送到VPN客戶端。

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

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco ASA系列VPN CLI配置指南9.3
- <u>思科身份服務引擎使用手冊,版本1.2</u>
- 技術支援與文件 Cisco Systems