

排除FTD中的OSPF配置故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[OSPF背景](#)

[基本配置](#)

[重分發](#)

[篩選](#)

[介面引數](#)

[Hello和Dead計時器](#)

[MTU Ignore-OSPF](#)

[驗證](#)

[一般CLI驗證](#)

[示例拓撲](#)

[內部FTD](#)

[外部FTD](#)

[疑難排解指令](#)

[show running-config router](#)

[show route](#)

[show ospf neighbor](#)

[show ospf interface](#)

[show ospf database](#)

[相關資訊](#)

簡介

本檔案介紹如何使用FMC作為管理員驗證FTD裝置上的OSPF組態並疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

- [開放最短路徑優先\(OSPF\)概念和功能](#)
- [思科安全防火牆管理中心\(FMC\)](#)
- [思科安全防火牆威脅防禦\(FTD\)](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 虛擬FTD 7.2.5
- 虛擬FMC 7.2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

OSPF背景

可以在FMC上設定OSPF，以便在FTD裝置與其他OSPF功能裝置之間使用動態路由。

FMC允許針對不同的介面集同時運行兩個OSPF進程。

每台裝置都有一個路由器ID，這類似於OSPF過程中的裝置名稱。預設情況下，這是設定為較低介面IP，但可以自定義為不同的IP。

需要注意的重要一點是，這些引數必須在鄰居上匹配才能形成OSPF鄰接關係：

- 介面屬於同一個IP網路
- 子網路遮罩
- 區域
- Hello間隔和Dead間隔
- MTU
- 區域型別（正常/NSSA/末節）
- 驗證

基本配置

本部分顯示為OSPF配置的基本引數，這些引數用於開始搜尋與其鄰居的鄰接關係。

1. 導航到裝置>裝置管理>編輯裝置
2. 按一下Routing頁籤。
3. 按一下左側選單欄上的OSPF。
4. 選擇Process 1以啟用OSPF配置。FTD可以在不同的介面組上同時執行兩個處理。

區域邊界路由器(ABR)位於兩個不同區域之間，而自治系統邊界路由器(ASBR)位於使用其他路由協定的裝置之間。

5. 選擇OSPF role作為Internal、ABR、ASBR以及ABR and ASBR。

Device **Routing** Interfaces Inline Sets DHCP VTEP

Process 1 ID: 1

OSPF Role:
ASBR Enter Description here [Advanced](#)

Process 2 ID:

OSPF Role:
Internal Router Enter Description here [Advanced](#)

角色選擇

6. (可選) 更改自動路由器ID。選擇OSPF role旁邊的Advanced，然後選擇Router ID作為IP address進行自定義。

Advanced

General Non Stop Forwarding

Router ID
IP Address 3.3.3.3

路由器ID選擇

7. 選取區域>新增。

8. 輸入「區域」資訊：

- OSPF進程
- 區域ID
- 區域型別
- 可用的網路

9. 按一下確定儲存配置。

Edit Area



Area Range Virtual Link

OSPF Process:

1

Area ID:*

0

Area Type:

Normal

Summary Stub Redistribute Summary NSSA Default Information originate

Metric Value:

Metric Type:

2

Available Network + C

Q Search

0.0.0.0
10.10.10.0_24
10.24.107.100

< < Viewing 1-100 of 142 > >

Authentication:

Add

Selected Network

3.11.0.0_24
10.3.11.0_27

Cancel

OK

區域選取

重分發

FTD可以將路由從一個OSPF程式重分配到另一個OSPF程式。重分配還可以從RIP、BGP、EIGRP (7.2+版本)、靜態路由和連線路由到OSPF路由進程。

1. 要配置OSPF重分配，請導航到裝置>裝置管理>編輯裝置。
2. 按一下路由
3. 按一下OSPF。

4. 選擇重分配>增加。

5. 輸入重分配欄位：

- OSPF進程
- 路由型別 (從重分發的位置)
 - 靜態
 - 已連線
 - OSPF進程
 - BGP
 - RIP
 - EIGRP

對於BGP和EIGRP，請增加AS編號。

6. (可選) 選擇是否使用子網。

7. 選取測量結果型態。

- 第1類使用外部度量並增加通向ASBR的每一跳的內部開銷。
- 型別2僅使用外部測量結果。

8. 按一下確定儲存更改。

Edit Redistribution



OSPF Process*:

Route Type:

AS Number*:

Optional

- Internal
- External1
- External2
- NSSA External1
- NSSA External2
- Use Subnets

Metric Value:

Metric Type:

Tag Value:

RouteMap: +

Cancel

OK

篩選

您可以執行區域間過濾，從而限制從某個區域傳送到另一個區域的入站或出站路由。此操作僅在ABR上執行。

過濾使用字首清單進行配置，然後這些字首清單將連結到OSPF配置。這是可選功能，OSPF無需使用此功能。

1. 要配置OSPF區域間過濾，請導航到Devices > Device Management > Edit裝置。
2. 按一下路由
3. 按一下OSPF。
4. 選擇區域間>增加。
5. 配置過濾欄位：
 - OSPF進程
 - 區域ID
 - 字首清單
 - 流量方向-入站或出站

Edit InterArea



OSPF Process:*

Area ID:*

PrefixList:*



Traffic Direction:

Cancel

OK

6. 如果您已設定首碼清單，請移至步驟10。如果需要建立新字首，您可以從Objects > Object Management > Prefix Lists > IPv4 prefix list > Add選擇加號或建立該加號。

7. 按一下增加條目。

8. 使用以下欄位配置字首清單：

- 序號
- IP 位址
- 動作
- 最小/最大字首長度 (可選)







Edit Prefix List Object

Name

filter_4.4.4.0

▼ Entries (2)

Add

Sequence No ▲	IP Address	Permit	Min Prefix Length	Max Prefix Length	
5	4.4.4.0/24	 Block			 
10	0.0.0.0/0	 Allow		32	 

字首清單對象編輯

9. 按一下確定儲存字首清單。

10. 按一下確定儲存區域間配置。

介面引數

對於參與OSPF的每個介面，可以修改某些引數。

1. 要配置OSPF介面引數，請導航到Devices > Device Management > Edit device。

2. 按一下路由

3. 按一下OSPF。

4. 選擇介面>增加。

5. 選取要修改的引數

Hello和Dead計時器

傳送OSPF Hello資料包是為了維護裝置之間的鄰接關係。這些資料包按可配置的時間隔傳送。如果裝置在dead間隔內未收到來自鄰居的hello資料包（也可以配置），則該鄰居會變為關閉狀態。

預設情況下，Hello間隔為10秒，Dead間隔是Hello間隔的四倍，即40秒。這些間隔在鄰居之間必須匹配。

Hello Interval:

10

Transmit Delay:

1

Retransmit Interval:

5

Dead Interval:

40

計時器配置

MTU Ignore-OSPF

MTU ignore覈取方塊是一個選項，用於避免由於鄰居介面之間的MTU不匹配而導致OSPF鄰接停滯在EXSTART狀態。驗證MTU匹配，因為在該狀態下，DBD在鄰居之間傳送，大小差異會導致問題。但是，最佳做法是取消選中此選項。

Interface*

inside

Default Cost:

10

Priority:

1

MTU Ignore:

MTU忽略檢查配置

驗證

您可以選擇三種不同型別的介面OSPF身份驗證。預設情況下，不啟用身份驗證。

- 無
- 密碼- 明文密碼
- MD5 -使用MD5雜湊


建議使用MD5作為身份驗證，因為它是提供安全性的雜湊演算法。

配置MD5 ID和MD5金鑰，然後按一下確定進行儲存。

Authentication:

MD5

+ Add

MD5 Id	MD5 Key	
1	

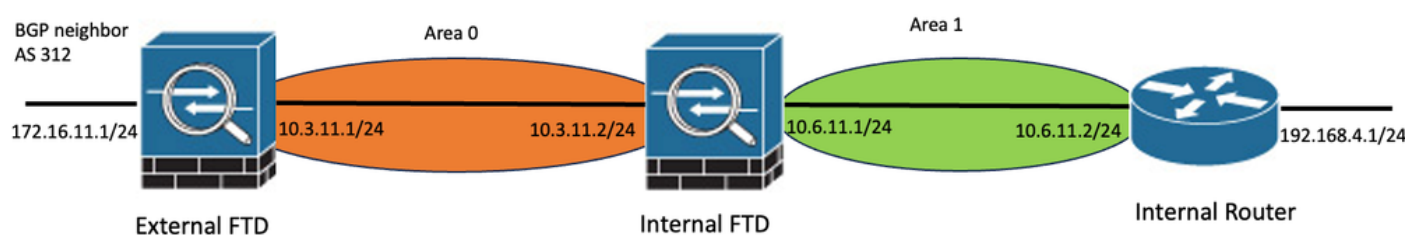
MD5金鑰配置

MD5金鑰或口令在經過身份驗證的鄰居的介面引數上必須匹配。

一般CLI驗證

示例拓撲

考慮將此網路拓撲作為示例：



網路拓撲範例

考慮以下因素：

- OSPF在外部FTD、內部FTD和內部路由器上設定。
- 外部FTD被選為ASBR角色，內部FTD被選為ABR，內部路由器被選為內部角色。
- 區域0建立於外部和內部FTD之間，而區域1建立於內部FTD和內部路由器之間。
- 外部FTD也在與另一個裝置執行BGP鄰居關係。
- 由自治系統312獲取的BGP路由被重分配到OSPF中。
- MTU和間隔均使用預設值進行配置。
- 內部FTD正在過濾從內部路由器獲知到區域0的傳入區域間路由。
- 在參與OSPF的所有裝置上，介面身份驗證配置為MD5。

內部FTD

內部FTD的組態如下所示：

使用MD5身份驗證的介面配置

```

interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.6.11.1 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.3.11.2 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!

```

OSPF配置表明，網路10.3.11.0/24會通告給區域0，網路10.6.11.0/24會通告給區域1上的鄰居。

區域間過濾將字首清單應用到進入區域0的入站路由。在此字首清單中，來自內部路由器的網路192.168.4.0被拒絕，並且允許所有其他內容。

Process 1 ID: 1

OSPF Role: ABR [Advanced](#)

Process 2 ID:

OSPF Role: Internal Router [Advanced](#)

Area	Redistribution	InterArea	Filter Rule	Summary Address	Interface
OSPF Process	Area ID	Area Type	Networks	Options	Authentication
1	0	normal	10.3.11.0_24	false	none
1	1	normal	10.6.11.0_24	false	none

內部FTD區域組態

Area	Redistribution	InterArea	Filter Rule	Summary Address	Interface
OSPF Process	Area ID	Prefix List Name	Traffic Direction		
1	0	filter_192.168.4.0	Inbound		

內部FTD篩選組態

Edit Prefix List Object



Name

filter_192.168.4.0

▼ Entries (2)

Add

Sequence No ▲	IP Address	Permit	Min Prefix Length	Max Prefix Length	
5	192.168.4.0/24	🚫 Block			
10	0.0.0.0/0	🟢 Allow		32	

內部FTD首碼清單

```
router ospf 1
network 10.3.11.0 255.255.255.0 area 0
network 10.6.11.0 255.255.255.0 area 1
area 0 filter-list prefix filter_192.168.4.0 in
log-adj-changes
```

```
prefix-list filter_192.168.4.0 seq 5 deny 192.168.4.0/24
prefix-list filter_192.168.4.0 seq 10 permit 0.0.0.0/0 le 32
```

外部FTD

外部FTD的組態在CLI中顯示如下：

使用MD5身份驗證的介面配置。

```
interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.3.11.1 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 172.16.11.1 255.255.255.0
!
```

OSPF配置顯示，路由10.3.11.0/24已通告給區域0中的內部FTD。

還可以觀察到BGP重分配到OSPF的情況。

Process 1 ID: 1

OSPF Role:
ASBR

Process 2 ID:

OSPF Role:
Internal Router

Area Redistribution InterArea Filter Rule Summary Address Interface

OSPF Process	Area ID	Area Type	Networks	Options	Authentication	Cost
1	0	normal	10.3.11.0_27	false	none	

外部FTD區域組態

Area **Redistribution** InterArea Filter Rule Summary Address Interface

OSPF Process	Route Type	Match	Subnets	Metric Value	Metric Type
1	bgp	false	true		2

外部FTD重新發佈組態

```
router ospf 1
network 10.3.11.0 255.255.255.0 area 0
log-adj-changes
redistribute bgp 312 subnets
```

疑難排解指令

有幾個命令可用於確定OSPF是否按預期工作。

注意：當FTD故障排除檔案是除OSPF配置之外生成的，並且需要從FTD CLI手動輸入時，show tech files上不會顯示這些命令。

show running-config router

此命令不僅顯示OSPF，還顯示動態路由協定的配置。

在CLI中檢查OSPF相關配置很有用。

show route

show route輸出顯示有關當前可用路由的重要資訊。

- 透過OSPF獲知的路由以字母O顯示。
- 區域間路由以字母O IA顯示。
- 透過重分配從其他路由協定獲知的路由會顯示O E1或O E2字母，具體取決於所選的度量型別。

內部FTD的show route輸出顯示，存在三個已知來自ASBR鄰居10.3.11.1的外部路由。

它還顯示網路192.168.4.0/24從同一區域的鄰居10.6.11.2獲知。

```
<#root>
```

```
Internal-FTD#
```

```
show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
```

```
Gateway of last resort is not set
```

```
C      10.3.11.0 255.255.255.0 is directly connected, outside
L      10.3.11.2 255.255.255.255 is directly connected, outside
O E2   10.5.11.0 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
O E2   10.5.11.32 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
O E2   10.5.11.64 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
C      10.6.11.0 255.255.255.0 is directly connected, inside
L      10.6.11.1 255.255.255.255 is directly connected, inside
O      192.168.4.0 255.255.255.0 [110/20] via 10.6.11.2, 02:19:24, inside
```

從外部FTD中，可以觀察到，路由10.6.11.0/24從鄰居10.3.11.2得知並屬於不同區域。

在此輸出中並未觀察到路由192.168.4.0/24，因為它是透過內部FTD篩選的。

此外，從其他裝置得知的三個BGP路由會重新分配到OSPF中，作為外部2型路由（如內部FTD所示）。

```
<#root>
```

```
External-FTD#
```

```
show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is not set
```

```
C      10.3.11.0 255.255.255.0 is directly connected, inside
```

```
L      10.3.11.1 255.255.255.255 is directly connected, inside
B      10.5.11.0 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
B      10.5.11.32 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
B      10.5.11.64 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
O IA   10.6.11.0 255.255.255.0 [110/20] via 10.3.11.2, 02:03:27, inside
C      172.16.11.0 255.255.255.0 is directly connected, outside
L      172.16.11.1 255.255.255.255 is directly connected, outside
```

show ospf neighbor

此命令有助於驗證OSPF鄰接的狀態是什麼，以及該鄰居是指定路由器(DR)、備用指定路由器(BDR)還是其他(DROTHER)。

DR是在網路發生變化時更新同一子網中其餘裝置的裝置。如果不再提供，BDR將擔任DR角色。

此命令也很有用，因為它顯示了鄰居的路由器ID，以及獲知鄰居的IP地址和介面。

也會觀察停頓時間倒計時。如果您有預設計時器，在傳送新的hello資料包並重新啟動計時器之前，您可以看到時間從00:40縮短到00:30。

如果此時間一直為零，則鄰接將丟失。

在本範例中，內部FTD輸出顯示，此裝置是一個BDR處於FULL狀態，且有兩個可從每個介面連線的DR，作為回報。它們的路由器ID分別為10.3.11.1和192.168.4.1。

<#root>

Internal-FTD#

show ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.11.1	1	FULL/DR	0:00:38	10.3.11.1	outside
192.168.4.1	1	FULL/DR	0:00:33	10.6.11.2	inside

show ospf interface

show ospf interface輸出顯示詳細資訊，並更廣泛地展示了每個已配置介面上的OSPF進程。

以下是此輸出顯示的部分引數：

- OSPF進程ID
- 路由器ID
- 度量 (成本)
- 狀態- DR、BDR或DROTHER
- 誰是DR和BDR。
- Hello和Dead計時器間隔

- 鄰居摘要
- 身份驗證詳細資訊

在內部FTD的下一個輸出中，可以觀察到，此裝置確實是兩個介面上的BDR，且鄰居與來自show ospf neighbors的資訊相符。

```
<#root>
```

```
Internal-FTD#
```

```
show ospf interface
```

```
outside is up, line protocol is up
Internet Address 10.3.11.2 mask 255.255.255.0, Area 0
Process ID 1, Router ID 10.6.11.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 10.3.11.1, Interface address 10.3.11.1
Backup Designated router (ID) 10.6.11.1, Interface address 10.3.11.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 0:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.3.11.1 (Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
Youngest key id is 1
```

```
inside is up, line protocol is up
Internet Address 10.6.11.1 mask 255.255.255.0, Area 1
Process ID 1, Router ID 10.6.11.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.4.1, Interface address 10.6.11.2
Backup Designated router (ID) 10.6.11.1, Interface address 10.6.11.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 0:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.4.1 (Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
Youngest key id is 1
```

show ospf database

此命令具有有關OSPF的鏈路狀態通告(LSA)型別的詳細資訊。輸出非常複雜，僅對更深層故障排除有用。

LSA是OSPF在裝置之間交換資訊和更新，而不是傳送完整路由表的方式。

最常見的LSA型別有：

第1類-路由器鏈路狀態- 通告路由器的路由器ID

第2類-網路鏈路狀態- 與指定路由器在同一鏈路中連線的介面。

第3類-總結網路鏈路狀態- 區域邊界路由器(ABR)注入此區域的區域間路由。

第4類-彙總ASB鏈路狀態- 自治系統邊界路由器(ASBR)的路由器ID。

第5類- AS外部鏈路狀態 -從ASBR獲知的外部路由。

因此，此指令的輸出可從內部FTD範例中解釋。

- 資料庫按區域顯示。
- 連結ID欄包含要注意的重要資訊。
- 如前所述，第1類顯示區域中每個裝置的路由器ID，第2類顯示每個子網鏈路的DR。在本例中，10.3.11.1用於區域0,10.6.11.2用於區域1。
- 第3類顯示區域0的ABR 10.6.11.0和區域1的10.3.11.0注入各自區域的區域間路由。
- 第4類顯示ASBR的路由器ID。區域1認為10.3.11.1裝置是進程的ASBR。
- 第5類顯示ASBR重分配的路由。在本例中，有三條外部路由：10.5.11.0、10.5.11.32和10.5.11.64。

<#root>

Internal-FTD#

show ospf database

OSPF Router with ID (10.6.11.1) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.3.11.1	10.3.11.1	234	0x8000002b	0x4c4d	1
10.6.11.1	10.6.11.1	187	0x8000002e	0x157b	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.3.11.1	10.3.11.1	234	0x80000029	0x7f2b

Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.6.11.0	10.6.11.1	187	0x8000002a	0x7959

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.6.11.1	10.6.11.1	187	0x8000002c	0x513b	1
192.168.4.1	192.168.4.1	1758	0x8000002a	0x70f1	2

Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
10.6.11.2	192.168.4.1	1759	0x80000028	0xd725

Summary Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
10.3.11.0	10.6.11.1	189	0x80000029	0x9f37

Summary ASB Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
10.3.11.1	10.6.11.1	189	0x80000029	0x874d

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
10.5.11.0	10.3.11.1	1726	0x80000028	0x152b	311
10.5.11.32	10.3.11.1	1726	0x80000028	0xd34c	311
10.5.11.64	10.3.11.1	1726	0x80000028	0x926d	311

相關資訊

- [思科技術支援與下載](#)
- [瞭解「優先開啟最短路徑」\(OSPF\) 設計指南](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。