# 在安全防火牆上使用環回介面配置eBGP

目錄
<u>必要條件</u>
採用元件
<u>背景資訊</u>
使用環回介面的eBGP配置
<u>案例</u>
<u>網路圖表</u>
<u>環回配置</u>
<u>靜態路由配置</u>
BGP配置
<u>驗證</u> (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
<u>疑難排解</u>

# 簡介

本文檔介紹如何使用Cisco安全防火牆上的環回介面配置eBGP。

必要條件

### 需求

思科建議您瞭解以下主題:

• BGP通訊協定

7.4.0版引入了對BGP的環回介面支援,這是安全防火牆管理中心和Cisco Secure Firepower威脅防 禦所需的最低版本。

採用元件

- 適用於VMware的安全防火牆管理中心版本7.4.1
- 2適用於VMware的Cisco安全Firepower威脅防禦7.4.1版

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。

# 背景資訊

邊界閘道通訊協定(BGP)是一種外部閘道通訊協定(EGP)標準化路徑向量路由通訊協定,可提供擴充 性、彈性及網路穩定性。具有相同自治系統(AS)的兩個對等體之間的BGP會話稱為內部BGP (iBGP)。具有不同自治系統(AS)的兩個對等體之間的BGP會話稱為外部BGP (eBGP)。

通常,對等體關係是使用最接近對等體的介面的IP地址建立的,但是,使用環回介面建立BGP會話 很有用,因為當BGP對等體之間存在多個路徑時,它不會導致BGP會話關閉。

✤ 注意:此進程描述對eBGP對等體使用Loopkack的過程,但對iBGP對等體使用相同的進程,因此可以將其用作參考。

# 使用環回介面的eBGP配置

案例

在此配置中,防火牆SFTD-1具有IP地址為10.1.1.1/32的環回介面,而防火牆SFTD-2具有IP地址為 10.2.2.2/32且AS64000為64001的環回介面。兩個防火牆均使用其外部介面到達另一個防火牆的環 回介面(在本場景中,兩個防火牆上均預配置了外部介面)。

### 網路圖表

此文件使用以下網路設定:



圖1.埃斯庫納里奧圖表

### 環回配置

步驟 1.按一下Devices > Device Management, 然後選擇您要配置環回的裝置。

步驟 2.按一下Interfaces > All Interfaces。

# 步驟 3.按一下Add Interface > Loopback Interface。

E ,	rewall Management Center wices / Secure Firewall Interfaces	r <sub>Overview</sub>	Analysis Po	olicies Devices	Objects	Integration		Deplo	iy Q +	¢ Ø   •	dmin ~ dbab SECURE
FTD- Cisco Fin Device	power Threat Defense for VMware Routing Interfaces Inlin	Ne Sets DHCP \	/TEP								Save Cancel
All Inte	faces Virtual Tunnels							Q. Search by name		Sync Device	Add Interfaces V Sub Interface Redundant Interface
Inter	anagement0/0	Logical Name management	Type Physical	Security Zones	MAC Ad	dress (Active/Standby)	IP Address		Path Monitoring Disabled	Global	Pridge Group Interfere Virtual Tunnel Interface
• G	gabitEthernet0/0	outside	Physical				10.10.10.1/24(Sta	atic)	Disabled	Global	VNI Interface
() () ()	gabitEthernet0/1		Physical						Disabled		/
ies G	gabitEthemet0/3		Physical						Disabled		,

圖2.增加介面環回

步驟 4. 在常規部分中,配置環回的名稱,選中已啟用框,然後配置環回ID。

# Add Loopback Interface General Image: Interface Name: Interface Looback1 Image: Interface </t



步驟 5.在IPv4部分中,在IP Type部分選擇Use Static IP選項,配置環回IP,然後按一下OK儲存更 改。

Edit Loop	back Int	erface					3
General	IPv4	IPv6					
IP Type:							
Use Stat	tic IP		$\sim$				
IP Addres	ss:						
10.1.1.1	/32						
e.g. 192.168	.1.1/255.255.255	5.0 or 192.168.	1.1/24				
回IP地址配置				Cancel		к	
<sup>[</sup> 回IP地址配置 6.點選儲存。 irewall Management Cent exces / Secure Firewall Interfaces	Qr Overview Analysis	Policies Devices Objects	Integration	Cancel	Deploy Q 🕻	K admin ~ [	adada (
回IP地址配置 6.點選儲存。 firewall Management Cent eveces / Secure Firewall Interfaces 1 epower Threat Defense for VMware a Routing Interfaces In	Ef Overview Analysis	Policies Devices Objects	Integration	Cancel	Deploy Q 🔹	K admin ~	altadia CISCO
回IP地址配置 6.點選儲存。 firewall Management Cent evices / Secure Firewall Interfaces 1 exouring Interfaces In a Routing Interfaces In	Ef Overview Analysis	Policies Devices Objects	Integration	Cancel	Deploy Q 🛟 You have ur	e la dmin v i	
e回IP地址配置 6.點選儲存。 firewall Management Cent evices / Secure Firewall Interfaces 1 epower Threat Defense for VMware e Routing Interfaces In unfaces Virtual Tunnets rface	CPT Overview Analysis	Policies Devices Objects	Integration Address (Active/Standby)	Cancel Q. Search IP Address	Deploy Q 🗘 Vou have ur by name	admin >      saved changes Save  Sync Device Add  Virtual Router	ethadu cisco di linterf
《回IP地址配置 6.點選儲存。 firewall Management Cent levices / Secure Frewall Interfaces 1 e Routing Interfaces In infaces Virtual Tunnels rface Aanagement0/0	er Overview Analysis filme Sets DHCP VTEP Logical Name Type management Physical	Policies Devices Objects	Integration Address (Active/Standby)	Cancel Q. Search	Deploy Q 🗘 Vou have ur by name Path Monitoring Disabled	E  admin  v	diade di Interf
图回IP地址配置 6.點選儲存。 Firewall Management Cent Vercies / Secure Firewall Interfaces 1 repower Threat Defense for VMware e Routing Interfaces In Interfaces Virtual Tunnels reface Anagement0/0 HigabitEthernet0/0	er     Overview     Analysis       line Sets     DHCP     VTEP       Logical Name     Type       management     Physical       outside     Physical	Policies Devices Objects	Integration Address (Active/Standby)	Cancel Cascel R Search IP Address	Deploy Q 🗘 Vou have ur by name I Path Monitoring Disabled Disabled	E  admin  source Sync Device Add Virtual Router Global Global	alada a
e Routing Interfaces In e Routing Interfaces In erfaces Virtual Tunnels urface GligabitEthermet0/1 GligabitEthermet0/1	CF     Overview     Analysis       line Sets     DHCP     VTEP       Logical Name     Type       management     Physical       outside     Physical       Ubscalard	Policies Devices Objects Security Zones MAC	Integration Address (Active/Standby)	Cancel Cancel R Search IP Address	Deploy Q 🗘 Vou have ur by name I Path Monitoring Disabled Disabled Disabled Disabled	k admin v sync Device Add Virtual Router Global Global	diade 0 1 1 1 1 1 1 1 1 1
受回IP地址配置 その.點選儲存。 Firewall Management Cent Devices / Secure Firewall Interfaces 1 repower Threat Defense for VMware we Routing Interfaces In outputs Virtual Tunnels wiface Management0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/2 GigabitEthernet0/3	Proverview Analysis Noverview Analysis Noverview Analysis DHCP VTEP Logical Name 1 management Physical outside Physical Physical Physical Physical Physical Physical	Policies Devices Objects Security Zones MAC	Integration Address (Active/Standby)	Cancel Cancel Other Cancel Othe	Deploy Q 🗘 Vou have ur by name I Disabled Disabled Disabled Disabled Disabled	E  admin  ( source) Add Virtual Router Global Global Global	altadı:

步驟 7.對第二個防火牆重複此過程。

Firewall Management Cente Devices / Secure Firewall Interfaces	r Overview	Analysis Po	licies Devices	Objects Integration	Dep	loy Q 🔅	admin v shada	SECURE			
FTD-2 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP											
All Interfaces Virtual Tunnels Add Interfaces *											
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router				
Management0/0	management	Physical				Disabled	Global	୦. ଏ			
GigabitEthernet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global	/			
GigabitEthernet0/1		Physical				Disabled		/			
GigabitEthernet0/2		Physical				Disabled		/			
GigabitEthernet0/3		Physical				Disabled		/			
Loopback1	Looback2	Loopback			10.2.2.2/32(Static)	Disabled	Global	11			

圖6.對等體上的環回介面配置

# 靜態路由配置

必須配置靜態路由,以確保用於對等操作的遠端對等體地址(環回)可透過所需介面訪問。

步驟 1.按一下Devices > Device Management,然後選擇您要配置靜態路由的裝置。

步驟 2.按一下Routing > Manage Virtual Routers > Static Route,然後按一下Add Route。

Firewall Management Devices / Secure Firewall Rout	Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🗘 🕜 ədmir	eisco SECURE
FTD-1 Cisco Firepower Threat Defense for V	/Mware							Save
Device Routing Interface:	s Inline Sets DHCP	VTEP						
Manage Virtual Routers								+ Add Route
Global 👻	Network *	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▶ IPv4 Routes							
ECMP	▼ IPv6 Routes							
BFD								
OSPFv3								
EIGRP								
RIP								
Policy Based Routing								
✓ BGP								
IPv4								
IPv6								
Static Route								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
BGP						é no 🔽		المتحدة

圖7.增加新的靜態路由

步驟 3.選中Type的IPv4選項。在Interface選項中選擇用於到達遠端對等體的環回的物理介面,然後 指定用於到達Gateway部分的Loopback的下一跳。 Edit Static Route Configuration

Type:      IPv4	IPv6
Interface*	
outside	٣
(Interface starting with this icon	🔊 signifie
Available Network C	+
Q, Search	
any-ipv4	
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private=172.16.0.0=12	

# Ensure that egress virtualrouter has route to that destination

Gateway	
10.10.10.2 -	+
Metric:	
1	
(1 - 254)	
Tunneled: Used only for default Rou	xute)
Route Tracking:	
	+

圖8.靜態路由配置

# 步驟 4. 點選可用網路部分旁邊的圖示(+)。

Edit Static Route Configuration

Type:	IPv4	○ IPv6
Interface*		
outside		*
(Interface startin	g with this	icon 🚳 signifi
Available Networ	кC	+
Q Search		
any-ipv4		
IPv4-Benchma	rk-Tests	
IPv4-Link-Loca	1	
IPv4-Multicast		
IPv4-Private-1	8-0.0.0	
IPv4-Private-1	72.16.0.0-	12

Ensure that egress virtualrouter has route to that destination

1000	-		
C.D.M.	8.85	646.AM	10.01
1000	10.00	1000	B101 -
1000	The line		чж.

10.10.10.2	*	+
Metric:		
1		

(1 - 254)

Tunneled:	Used	only for	default	Route)
-----------	------	----------	---------	--------

Route Tracking:

• + +

	(	Cancel	ОК

圖9.新增網路物件

步驟 5.配置供參考的名稱以及遠端對等體的Looback的IP,然後按一下Save。

0

# New Network Object

Name	
Loopback-FTD2	
Description	
Network	
Host O Range O Network	O FQDN
10.2.2.2	
Allow Overrides	
	Cancel Save

(2)

圖10.在靜態路由中配置網路目標

步驟 6.搜尋在搜尋欄中建立的新對象,選擇該對象,然後按一下Add,再按一下OK。

# Edit Static Route Configuration

Type:  IPv4 O IPv6 Interface* Outside (Interface starting with this icon Sig	) nifies it is available for route leak)
Available Network C + Q. Loopback-FTD2 X Loopback-FTD2	Add Loopback-FTD2

Ensure that egress virtualrouter has route to that destination

# Gateway

10.10.10.2	٠	+
Metric:		
1		

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

 $\mathbf{w}$ 



圖11.配置靜態路由中的下一跳

### 步驟 7.點選儲存。

ø

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies	Devices Objects I	ntegration		Deploy Q	admin 🗸 👘 states SE	ECURE
FTD-1 Cisco Firepower Threat Defense for VM Device Routing Interfaces	Aware Inline Sets DHCP	VTEP				You have	unsaved changes Save C	Cancel
Manage Virtual Routers							+ Add R	Route
Global 🔻	Network .	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
ECMP	Loopback-FTD2	outside	Global	10.10.10.2	false	1		11
OSPE	▼ IPv6 Routes							
OSPFv3								
EIGRP								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
Static Route								

圖12.儲存靜態路由介面配置

# 步驟 8.對第二個防火牆重複此過程。

Firewall Management ( Devices / Secure Firewall Routin	9 Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🔅 🙆 admin ~ 🔤 admin secure
FTD-2 Cisco Firepower Threat Defense for VM Device Routing Interfaces	fware Inline Sets DHCP	VTEP					Save Cancel
Manage Virtual Routers							+ Add Route
Global 🔻	Network .	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties	▼ IPv4 Routes						
ECMP	Loopback-FTD1	outside	Global	10.10.10.1	false	1	/1
OSPF	▼ IPv6 Routes						
OSPFv3							
EIGRP							
RIP							
Policy Based Routing							
IPv4							
IPv6							
Static Route							

圖13.配置對等體上的靜態路由

# BGP配置

- 步驟 1.按一下Devices > Device Management,然後選擇您要啟用BGP的裝置。
- 步驟 2. 按一下Routing > Manage Virtual Routers > General Settings,然後按一下BGP。
- 步驟 3.選中Enable BGP框,然後在AS Number部分配置防火牆的本地AS。



圖14.全局啟用BGP

# 步驟 4.按一下Save按鈕儲存更改。

Firewall Management	nt Center Overview Analysis Policies Devices Objects	Integration	Deploy	Q. 슈 @ admin ~ "finally SECURE
FTD-1 Cisco Firepower Threat Defense for Device Routing Interfac	r VMware res Inline Sets DHCP VTEP			You have unsaved changes Save Cancel
Manage Virtual Routers Global  Virtual Router Properties ECMP BFD OSPF OSPFv3 Ercap	Enable BGP: AS Number* 64000 Override BGP general settings router-id address: Router id Automatic IP Address*			
RIP	General	1	Neighbor Timers	1
Policy Based Routing	Scanning Interval	60	Keepalive Interval	60
∼ BGP	Number of AS numbers in AS_PATH attribute of received routes	None	Hold time	180
IPv4	Log Neighbor Changes	Yes	Min hold time	0
IPv6 Static Route	Use TCP path MTU discovery	Yes		

圖15.儲存BGP啟用更改

# 步驟 5.在管理虛擬路由器部分中,轉到BGP 選項,然後按一下IPv4。

步驟 6.選中Enable IPv4框,然後按一下Neighbor,然後按一下+ Add。

Firewall Management Center Devices / Secure Firewall Routing	nalysis Policies Devices Objec	ts Integration	Deploy	Q ♀ ♀ ● admin > thether SECURE
FTD-1 Cisco Firepower Threat Defense for VMware				You have unsaved changes Save Cancel
Device Routing Interfaces Inline Sets DHCP V	EP			
Manage Virtual Routers Global General Neighbor Add	Aggregate Address Filtering Network	Redistribution Route Injection		
ECMP				+ Add
BFD				
OSPF Address	Remote AS Number	Address Family	Remote Private AS Number	Description
OSPFv3		No records to display		
EIGRP				
RIP				
Policy Based Routing				
∽ BGP				
IPv4				
IPv6				
Static Route				
✓ Multicast Routing				

圖16.增加新的BGP對等體

步驟 7.在IP Address 部分中配置遠端對等體的IP地址,然後在Remote AS 部分中配置遠端對等體的AS,並選中Enable address 框。

0

步驟 8.在Update Source部分中選擇本地介面Loopback。

Edit Neighbor

IP ADDress*		Enabled address
10.2.2.2		Shutdown administratively
Remote AS*		Configure graceful restart
64001		Graceful restart(failover/spanned mode)
(1-4294967295 or 1.0-65535.65535)		
BFD Fallover	De	recription
none •		
Update Source:	1	
Loopbeck1 ·		
Filtering Routes Tin	ners	Advanced Migration
Incoming		Outgoing
Access List		Access List
Ψ	+	• +
* Route Map	+	v + Route Map
* Route Map	)+ )+	
Route Map  Prefx List	) + ) +	r + Route Map     r + Prefx List
Route Map   Prefix List	)+ )+ )+	v + Route Map     v + Prefx List     v +
Route Map  Prefix List  AS path filter	)+ )+ )+	
Route Map	+  +  +  +	

圖17.基本BGP對等體引數

注意:Update Source 選項用於啟用neighbor update-source 命令,該命令用於允許任何工作

# 步驟 9.按一下Advanced,然後在TTL Hops 選項中配置數字2,然後按一下OK。

6	dit Neighbor	0
	none v	
	Update Source:	
	Loopbeck1 v	
	Filtering Routes Routes Timers Advanced Migration	
	Enable Authentication	_
	Enable Encryption	
	0 v	
	Password	
	Confirm Password	
	Send Community attribute to this neighbor	
	Use itself as next hop for this neighbor	
	Disable Connection Verification	
	Allow connections with neighbor that is not directly connected	
	<ul> <li>Limited number of TTL hops to neighbor</li> </ul>	
	TTL Hops	
	2	
	Ose TCP path MTD discovery	
	TCP Transport Mode	
	Weight	
	Cancel	<b>x</b>
뢻1	8.配置TTL跳數	

✤ 注意:TTL Hops 選項用於啟用ebgp-multihop 命令,該命令用於更改TTL值,以允許資料包到 達非直連的外部BGP對等體或具有直連介面以外的介面。

步驟 10.點選儲存並部署更改。

Firewall Managemen Devices / Secure Firewall Ro	nt Center Oven	view Analysis	Policies	Devices	Objects	Integration			Deploy	۹	¢ 0	admin $\vee$	cisco SECURE
FTD-1 Cisco Firepower Threat Defense for	VMware									You h	ave unsaved	l changes S	ave
Device Routing Interfac	es Inline Sets DH	ICP VTEP											
Manage Virtual Routers Global v Virtual Router Properties	Enable IPv4: 🗹 AS Number 64000 General Neighbo	or Add Aggreg	ate Address	Filtering	Networks	Redistribution	Route Injection						
ECMP													+ Add
BFD	Address		Domoto AC M	humber		Address FreeDr		Domoto Debuto AC Number		Deser	lation		
OSPF	Address		Remote AS N	lumber		Address Family		Remote Private AS Number		Descr	ption		
OSPFv3	10.2.2.2		64001			Enabled							/1
EIGRP													
RIP													
Policy Based Routing													
∨ BGP													
IPv4													

圖19.儲存BGP配置

# 步驟 11.對第二個防火牆重複此過程。

Firewall Manageme Devices / Secure Firewall Ro	nt Center Overview Ana	lysis Policies Dev	ices Objects	Integration	Deploy	۹ 🔅 🕻	admin ~ strate SECURE
FTD-2 Cisco Firepower Threat Defense fo Device Routing Interfac	r VMware ces Inline Sets DHCP VTEP						Save Cancel
Manage Virtual Routers Global v Virtual Router Properties ECMP	Enable IPv4: AS Number 64001 General Neighbor Add Aq	gregate Address Filterin	ng Networks	Redistribution Route Injection			+ 444
BFD OSPF	Address	Remote AS Number		Address Family	Remote Private AS Number	Description	
OSPFv3 EIGRP	10.1.1.1	64000		Enabled			/1
RIP Policy Based Routing Y BGP							
IPv4 IPv6							

圖20.配置對等體上的BGP

# 驗證

步驟 1.驗證環回和靜態路由配置,然後使用ping測試檢查BGP對等體之間的連線。

show running-config interface interface\_name

show running-config route

show destination\_ip

SFTD-1	SFTD-2
show running-config interface Loopback1	show running-config interface Loopback1
interface Loopback1	interface Loopback1
nameif Loopback1	名稱Looback2

IP 網址 10.1.1.1 255.255.255.255	IP 網址 10.2.2.2 255.255.255.255
show running-config route	show running-config route
10.2.2.2 255.255.255.255 10.10.10.2外部的路由 1	10.1.1.1 255.255.255.255 10.10.10.1外部的路由 1
ping 10.2.2.2	ping 10.1.1.1
向10.2.2.2傳送5,100位元組ICMP響應,超時為 2秒:	向10.1.1.1傳送5,100位元組ICMP響應,超時為 2秒:
!!!!!	!!!!!
成功率為100% (5/5),往返最小/平均/最大= 1/1/1毫秒	成功率為100% (5/5),往返最小/平均/最大= 1/1/1毫秒

步驟 2.驗證BGP配置,然後確保BGP對等已建立。

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2
show running-config router bgp	show running-config router bgp
路由器bgp 64000	路由器bgp 64001
bgp log-neighbor-changes	bgp log-neighbor-changes
bgp router-id vrf auto-assign	bgp router-id vrf auto-assign
address-family ipv4 unicast	address-family ipv4 unicast
neighbor 10.2.2.2 remote-as 64001	neighbor 10.1.1.1 remote-as 64000
neighbor 10.2.2.2 ebgp-multihop 2	neighbor 10.1.1.1 ebgp-multihop 2
neighbor 10.2.2.2 transport path-mtu-discovery disable	neighbor 10.1.1.1 transport path-mtu-discovery disable
neighbor 10.2.2.2 update-source Loopback1	neighbor 10.1.1.1 update-source Looback2
鄰居10.2.2.2啟用	鄰居10.1.1.1啟用
no auto-summary	no auto-summary

無同步	無同步
exit-address-family	exit-address-family
!	!
show bgp neighbors   i BGP	show bgp neighbors   i BGP
BGP鄰居是10.2.2.2,vrf single_vf,遠端AS 64001,外部鏈路	BGP鄰居是10.1.1.1,vrf single_vf,遠端AS 64000,外部鏈路
BGP版本4,遠端路由器ID 10.2.2.2	BGP版本4,遠端路由器ID 10.1.1.1
BGP狀態= Established,持續1d15h	BGP狀態= Established,持續1d16h
BGP表版本7,鄰居版本7/0	BGP表版本1,鄰居版本1/0
外部BGP鄰居可能距離最多2跳。	外部BGP鄰居可能距離最多2跳。
show bgp summary	show bgp summary
BGP路由器識別符號10.1.1.1,本地AS編號 64000	BGP路由器識別符號10.2.2.2,本地AS編號 64001
BGP表版本為7,主路由表版本為7	BGP表版本為1,主路由表版本為1
鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd	鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0	10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0

# 疑難排解

如果在此過程中遇到任何問題,請檢視以下文章:

·<u>邊界閘道通訊協定(BGP)</u>

### 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)。