概念與範例
ScreenOS 參考指南

第 2 卷：
基本原理

版本 5.3.0，修訂本 B

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

產品編號：093-1660-000-TC，修訂本 B

Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Network's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: Anita Davey, Carrie Nowocin, Jozef Wroblewski

Editor: Lisa Eldridge

目錄

關於本卷 ix

文件慣例 x
CLI 慣例 x
插圖慣例 xi
命名慣例和字元類型 xii
WebUI 慣例 xiii
Juniper Networks 文件 xiv

第 1 章 ScreenOS 架構 1

安全區 2
安全區介面 3
實體介面 3
子介面 4
虛擬路由器 5
政策 6
虛擬私人網路 8
虛擬系統 10
封包流動順序 11
範例 : (第 1 部份) 具有六個區域的企業 14
範例 : (第 2 部份) 六個區域的介面 16
範例 : (第 3 部份) 兩個路由設定網域 19
範例 : (第 4 部份) 政策 20

第 2 章 區域 25

檢視預先組態的區域 26
安全區 28
Global 區域 28
SCREEN 選項 28
將通道介面連結至通道區 28
設定安全區和通道區 30
建立區域 30
修改區域 31
刪除區域 31
功能區 32
Null 區域 32
MGT 區域 32
HA 區域 32
自我區域 32
VLAN 區域 32

連接埠模式 32
Trust-Untrust 模式 33
Home-Work 模式 34
Dual Untrust 模式 35
Combined 模式 36
Trust/Untrust/DMZ (擴展) 模式 37
DMZ/Dual Untrust 模式 37
Dual DMZ 模式 38
設定連接埠模式 39
範例 : Home-Work 連接埠模式 39
Home-Work 與 Combined 連接埠模式的區域 40
範例 : Home-Work 區域 41

第 3 章 介面 43

介面類型 43
安全區介面 43
實體介面 43
子介面 44
聚集介面 44
冗餘介面 44
虛擬安全性介面 44
功能區介面 45
管理介面 45
高可用性介面 45
通道介面 46
刪除通道介面 48
檢視介面 49
設定安全區介面 50
將介面連結到安全區 51
從安全區解除介面連結 51
爲 L3 安全區介面定址 51
公開 IP 位址 52
私人 IP 位址 52
編址介面 53
修改介面設定 53
在根系統中建立子介面 54
刪除子介面 54
建立次要 IP 位址 55
回傳介面 56
建立回傳介面 56
設定用於管理的回傳介面 57
設定回傳介面上的 BGP 57
設定回傳介面上的 VSI 57
設定回傳介面作爲來源介面 58

介面狀態變更 58
實體連接監看 60
追蹤 IP 位址 60
介面監看 65
監看兩個介面 66
監看介面迴路 67
安全區監看 70
不工作中介面和通訊流量傳遞 70
出口介面上的失敗 71
入口介面上的失敗 73

第 4 章 介面模式 77

透明模式 78
區域設定 79
VLAN 區域 79
預先定義的第 2 層區域 79
通訊流量轉寄 79
未知的 Unicast 選項 80
氾濫方法 81
ARP/Trace-Route 方法 82
組態用於管理的 VLAN1 介面 84
組態透明模式 86
NAT 模式 90
向內與向外 NAT 通訊流量 91
介面設定 92
組態 NAT 模式 92
路由模式 95
介面設定 96
組態路由模式 96

第 5 章 爲政策建構區塊 99

位址 100
位址項目 100
修改位址 101
刪除位址 101
位址群組 102
編輯位址群組項目 103
移除成員與群組 104

服務 104
預先定義的服務 104
網際網路控制訊息通訊協定 105
Microsoft 遠端程序呼叫服務 109
動態路由設定通訊協定 111
資料流視訊 112
Sun 遠端程序呼叫服務 113
安全性與通道服務 113
IP 相關服務 114
管理服務 114
郵件服務 115
雜項服務 116
自訂服務 117
新增自訂服務 117
修改自訂服務 118
移除自訂服務 118
設定服務逾時 118
服務逾時組態與查詢 118
範例 120
定義自訂網際網路控制訊息通訊協定服務 121
遠端 Shell 應用程式層閘道 122
Sun 遠端程序呼叫應用程式層閘道 122
一般 RPC 呼叫情況 122
自訂 Sun RPC 服務 122
自訂 Microsoft 遠端程序呼叫應用程式層閘道 123
即時資料流傳遞通訊協定應用程式層閘道 124
RTSP 要求方式 126
RTSP 狀態代碼 127
在公開網域中組態媒體伺服器 130
服務群組 132
修改服務群組 133
移除服務群組 134
動態 IP 集區 134
連接埠位址轉譯 135
建立有 PAT 的 DIP 集區 136
修改 DIP 集區 137
相黏 DIP 位址 137
在不同子網路中使用 DIP 137
在回傳介面上使用 DIP 143
建立 DIP 群組 147
設定遞迴排程 150

第 6 章 政策 153

基本元素 154
三種類型的政策 155
區域間政策 155
區域部政策 156
全域政策 156
政策組清單 157
政策定義 158
政策和規則 158
政策的結構 158
ID 159
區域 159
位址 160
服務 160
名稱 161
VPN 通道 161
L2TP 通道 162
深入檢查 162
政策清單上方配置 162
來源位址轉譯 162
目的地位址轉譯 162
使用者 Auth 163
HA 會話備份 164
Web 篩選 164
記錄 164
計數 165
通訊流量警示臨界值 165
排程 165
防毒掃描 165
通訊流量整理 165
套用的政策 166
檢視政策 166
建立政策 166
建立區域間政策郵件服務 167
建立區域間政策組 170
建立區域內部政策 174
建立全域政策 176
輸入政策內容 177
各政策元件的多重項目 177
設定位址否定 178
修改和停用政策 181
政策驗證 181
重新排序政策 182
移除政策 182

第 7 章 通訊流量整理 183

在政策層級管理頻寬 183
設定通訊流量整理 184
設定服務優先順序 188
設定優先順序佇列 189
入口政策制訂 192
整理虛擬介面上的通訊流量 193
介面層級通訊流量整理 193
政策層級通訊流量整理 194
封包流動 195
範例：具入口政策制訂的以路由爲基礎的 VPN 195
範例：具入口政策制訂的以政策爲基礎的 VPN 199
使用回傳介面的通訊流量整理 203
DSCP 標記與整理 203

第 8 章 系統參數 205

網域名稱系統支援 206
DNS 查詢 206
DNS 狀態表 207
設定 DNS 伺服器並重新整理排程 208
設定 DNS 重新整理間隔 208
動態網域名稱系統 209
設定 DynDNS 伺服器的 DDNS 209
設定 DDO 伺服器的 DDNS 210
代理 DNS 位址分割 211
動態主機組態通訊協定 213
組態 DHCP 伺服器 214
自訂 DHCP 伺服器選項 218
在 NSRP 叢集中放置 DHCP 伺服器 219
DHCP 伺服器偵測 219
啓用 DHCP 伺服器偵測 220
停用 DHCP 伺服器偵測 220
將安全性裝置指派爲 DHCP 轉接代理程式 220
將安全性裝置作爲 DHCP 用戶端使用 225
傳播 TCP/IP 設定 226
乙太網路上的點對點通訊協定 228
設定 PPPoE 229
組態主要與備份 Untrust 介面上的 PPPoE 232
設定多個 PPPoE 會話使用單一介面 232
PPPoE 與高可用性 235
許可金鑰 235
訂閱服務的註冊與啓動訂閱 237
試用服務 237
更新訂閱金鑰 237
將防毒、Web 篩選、反垃圾郵件及深入檢查新增至現有或新裝置 238

系統時鐘 239
日期與時間 239
時區 239
網路時間通訊協定 239
組態多重 NTP 伺服器 239
組態備份網路時間通訊協定伺服器 240
最大時間調整 241
NTP 和 NSRP 241
將最大時間調整值設定至 NTP 伺服器 241
保護 NTP 伺服器 242

索引 ..... IX-I

關於本卷

*第 2 卷 : 基本原理*介紹 ScreenOS 的架構及其組成元素，包括組態不同元素的範例。本卷包含下列各章 :

- 第 1 章，「ScreenOS 架構」介紹 ScreenOS 中架構的基本元素，並以一個分爲四部份的範例作爲總結來說明以企業爲基礎的組態，這個組態結合了多種的架構元素。在本章及後續所有各章中，每個概念都附有說明性的範例。
- 第 2 章，「區域」解釋安全區、通道區域和功能區。
- 第 3 章，「介面」描述安全性裝置上的各種實體、邏輯和虛擬介面。
- 第 4 章，「介面模式」解釋「可見的」、「網路位址轉譯」(NAT) 和「路由器」介面操作模式的概念。
- 第 5 章，「爲政策建構區塊」討論有關建立政策和虛擬私人網路 (VPN) 方面的原理 : 位址 (包括 VIP 位址)、服務和 DIP 集區。也介紹數個支援 H.323 通訊協定的範例組態。
- 第 6 章，「政策」探索政策的組成及功能，而且提供建立和套用政策的導引。
- 第 7 章，「通訊流量整理」說明如何管理介面和政策層級的頻寬及優化服務。
- 第 8 章，「系統參數」介紹「網域名稱系統 (DNS)」定址的概念；使用「動態主機組態通訊協定 (DHCP)」去組態或中繼 TCP/IP 設定；下載及上載系統組態和軟體；設定系統時鐘。

文件慣例

本文件使用幾種類型的慣例，以下部分將加以介紹 :

- 本頁上的「CLI 慣例」
- 第 xiii 頁上的「插圖慣例」
- 第 xiv 頁上的「命名慣例和字元類型」
- 第 xv 頁上的「WebUI 慣例」

CLI 慣例

下列慣例用於在範例及文字中呈現 CLI 指令的語法。

在範例中 :

- 在中括弧 [ ] 中的任何內容都是可選的。
- 在大括弧 **{ }** 中的任何內容都是必需的。
- 如果選項不止一個，則使用導線 (|) 分隔每個選項。例如 :

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  意味著「設定 ethernet1、ethernet2 *或* ethernet3 介面的管理選項」。

- 變數以*斜體*方式顯示 :

  ```
  set admin user name1 password xyz
  ```

在文字中 :

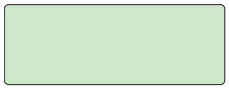
- 指令以**粗體**方式顯示。
- 變數以*斜體*方式顯示。

注意 : 當鍵入關鍵字時，只需輸入足夠的字母就可以專屬地識別單詞。例如，若要鍵入指令 **set admin user kathleen j12fmt54**，只要鍵入 **set adm u kath j12fmt54** 即可。儘管輸入指令時可以使用此捷徑，本文所述的所有指令都以完整的方式提供。

插圖慣例

下圖顯示貫穿本手冊的插圖所用的基本影像集 :

圖 1: 手冊插圖中的影像



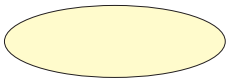
自治系統



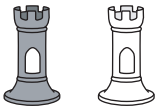
通用安全性裝置



虛擬路由設定網域



安全區



安全區介面

白色 = 受保護區段介面
(例如 = Trust 區段)

黑色 = 區域外介面
(例如 = Untrust 區段)



通道介面

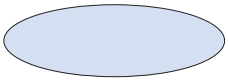
VPN 通道



路由器



交換機



包含單一子網路的區域網路 (LAN) (例如 : 10.1.1.0/24)



網際網路



動態 IP (DIP) 池



桌上型電腦



攜帶型電腦



通用網路裝置 (例如 : NAT 伺服器，存取集中器)



伺服器



集線器



IP 電話

命名慣例和字元類型

關於 ScreenOS 組態中定義的物件 (如位址、admin 使用者、auth 伺服器、IKE 閘道、虛擬系統、VPN 通道和區段) 的名稱，ScreenOS 採用下列慣例 :

- 若名稱字串包含一個或多個空格，則必須以雙引號 (") 包住整個字串，如 :

  set address trust "local LAN" 10.1.1.0/24

- 系統會刪除一組雙引號內文字的任何前導或結尾空格，例如，**" local LAN "** 將變爲 **"local LAN"**。

- 多個連續空格會被視爲單一空格。

- 儘管許多 CLI 關鍵字並不區分大小寫，但名稱字串是區分大小寫的。例如，**"local LAN"** 不同於 **"local lan"**。

ScreenOS 支援以下字元類型 :

- 單位元組字元集 (SBCS) 和多位元組字元集 (MBCS)。SBCS 的範例是 ASCII、歐洲語和希伯萊語。MBCS (也稱爲雙位元組字元集，DBCS) 的範例是中文、韓文和日文。

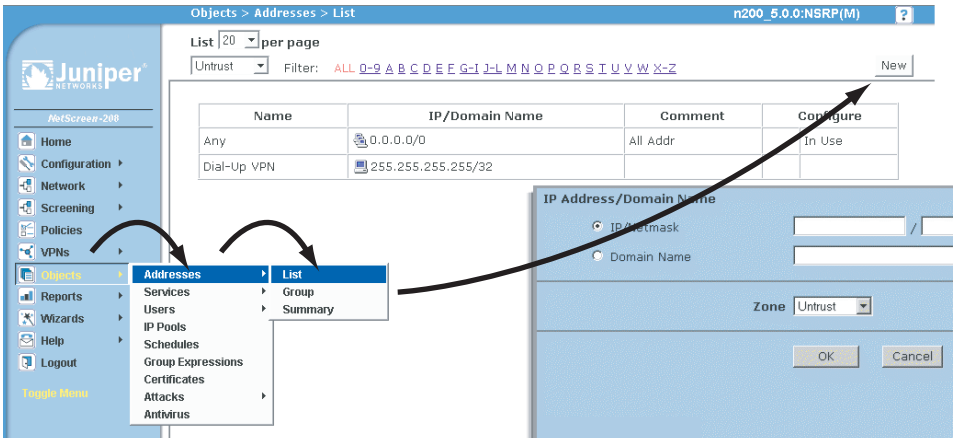
- ASCII 字元從 32 (十六進位 0x20) 到 255 (0xff)，雙引號 (") 除外，這些字元有特殊的意義，可作爲包含空格的名稱字串的開始或結尾指示符。

注意 : 主控台連接只支援 SBCS。WebUI 對 SBCS 和 MBCS 都支援，取決於 Web 瀏覽器所支援的字元集。

WebUI 慣例

尖角符號 (>) 表示 WebUI 中的瀏覽順序，您可按一下功能表選項及連結來依循該順序。下圖顯示了前往位址組態對話方塊的依循路徑 - Objects > Addresses > List > New:

圖 2: WebUI 導覽



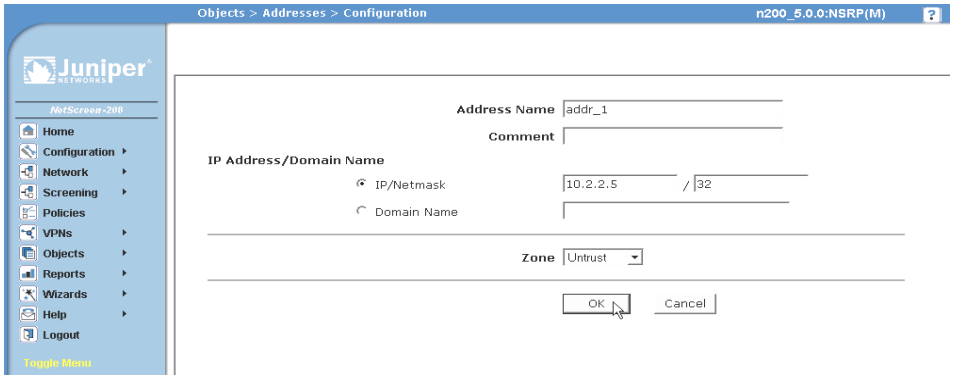
如要用 WebUI 執行任務，必須先瀏覽到相應的對話方塊，然後在該對話方塊中定義物件和設定參數。每個任務的說明集分爲瀏覽路徑及組態設定兩個部分 :

下圖列出了前往具有以下組態設定之位址組態對話方塊的路徑 :

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (選擇), 10.2.2.5/32
Zone: Untrust

圖 3: 瀏覽路徑與組態設定



Juniper Networks 文件

要獲得任何 Juniper Networks 產品的技術文件，請造訪 www.juniper.net/techpubs/。

如需技術支援，請使用 http://www.juniper.net/support/ 的 Case Manager 連結來開啓一個支援案例，或電洽 1-888-314-JTAC (美國境內) 或 1-408-745-9500 (美國境外)。

如果在本文件中發現任何錯誤或遺漏，請用下面的電子郵件位址與我們連絡 :

techpubs-comments@juniper.net

第 1 章

ScreenOS 架構

Juniper Networks ScreenOS 架構爲網路安全性配置的設計提供了極大的彈性。在有多個介面的 Juniper Networks 安全性裝置上，您可以建立兩個以上的安全區，並組態政策以調節區域內部及區域之間的通訊流量。可以爲每個區域連結一個或多個介面，並在每個區域上啓用一組唯一的管理和防火牆攻擊篩選選項。實際上，ScreenOS 讓您可以建立網路環境需要的區域數量、指派每個區域所需的介面數量，以及將每個介面按照自己的規格設計。

本章簡要介紹 ScreenOS，包括下列主要內容 :

- 第 2 頁上的「安全區」
- 第 3 頁上的「安全區介面」
- 第 5 頁上的「虛擬路由器」
- 第 6 頁上的「政策」
- 第 8 頁上的「虛擬私人網路」
- 第 10 頁上的「虛擬系統」

此外，爲了進一步瞭解 ScreenOS 處理通訊流量的機制，請參閱第 11 頁上的「封包流動順序」中的向內封包流動順序。

本章以一個包含四部份的範例作爲結束，說明使用 ScreenOS 的安全性裝置的基本組態 :

- 第 14 頁上的「範例 : (第 1 部份) 具有六個區域的企業」
- 第 16 頁上的「範例 : (第 2 部份) 六個區域的介面」
- 第 19 頁上的「範例 : (第 3 部份) 兩個路由設定網域」
- 第 20 頁上的「範例 : (第 4 部份) 政策」

安全區

一個安全區是一個或多個網路片段的集合，這些網路片段需要透過政策規定向內和向外通訊流量 (請參閱 第 6 頁上的「政策」)。安全區爲一邏輯實體，連結一個或多個介面。使用多種類型的 Juniper Networks 安全性裝置，您即可定義多個安全區，根據您的網路需要決定確切的數目。除使用者定義的區域外，您也可以使用預先定義的區域 : Trust、Untrust 和 DMZ (用於 Layer 3 (第 3 層) 操作)，或者 V1-Trust、V1-Untrust 和 V1-DMZ (用於 Layer 2 (第 2 層) 操作)。如果想要的話，可以繼續使用預先定義的區域。也可以忽略預先定義區域，並只使用使用者定義的區域。或者，您可以同時使用這兩種區域 - 預先定義和使用者定義。您可利用此區域設定彈性，建立最符合您特殊需求的網路設計。請參閱圖 4。

注意 : 不需要網路片段的安全區爲全域區域。(如需詳細資訊，請參閱第 28 頁上的「Global 區域」。) 另外，任何區域如果沒有連結的介面也沒有通訊錄項目，也可以說區域不包含任何網路片段。

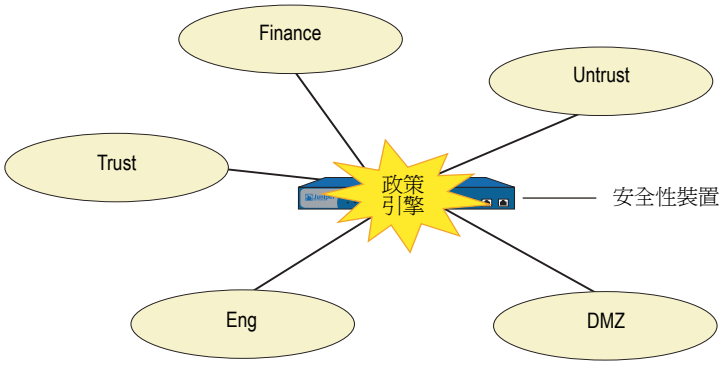
如果從 ScreenOS 的早期版本進行升級，這些區域的所有組態都會保持不變。

不可以刪除預先定義的安全區。但是，可以刪除使用者定義的安全區。刪除安全區時，也會同時自動刪除爲該區域組態的所有位址。

圖 4: 預先定義的安全區

組態了 5 個安全區的網路 - 3 個預設區域 (Trust、Untrust、DMZ)，及 2 個使用者定義的區域 (Finance、Eng)。

通訊流量只有在政策允許的時候才能夠由一個安全區傳遞到另一區。



安全區介面

安全區的介面可以視爲一個入口，TCP/IP 通訊流量可通過此入口在該區域和其他任何區域之間進行傳遞。

透過定義的政策，可以使兩個區域間的通訊流量向一個或兩個方向流動。利用定義的路由，可指定通訊流量從一個區域到另一個區域必須使用的介面。由於可將多個介面連結到一個區域上，所以您制定的路由對於將通訊流量引向選擇的介面是十分重要的。

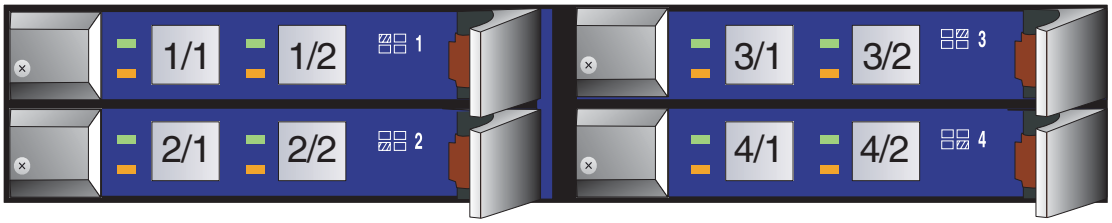
注意 : 對於在連結到相同區域的兩個介面之間流動的通訊流量，因爲兩個介面具有同等的安全性，所以不需要政策。ScreenOS 對於兩個區域間的通訊流量需要政策，如果是在一個區域內，就不需要。

若要允許在區域間流通的通訊流量，將介面連結到區域，而且要針對設定爲「路由」或 NAT 模式的介面 (請參閱第 77 頁上的「介面模式」) 將 IP 位址指派至介面。兩種常見的介面類型爲實體介面和 (對於那些具有虛擬系統支援的裝置) 子介面 (也就是，實體介面在第 2 層的具體證明)。如需詳細資訊，請參閱第 43 頁上的「介面」。

實體介面

實體介面與安全性裝置上實際存在的元件有關。各裝置的介面命名慣例各有不同之處。以 NetScreen-500 爲例，實體介面由介面模組的位置及該模組上的乙太網路連接埠識別。例如，介面 *ethernet1/2* 表示介面模組在**第一個停駐區** (*ethernet**1**/2*) 和**第二個連接埠** (*ethernet1/**2***)。請參閱圖 5。

圖 5: 介面實體指派



注意 : 若要檢視特定安全性裝置的命名慣例，請參閱該裝置的使用者指南。

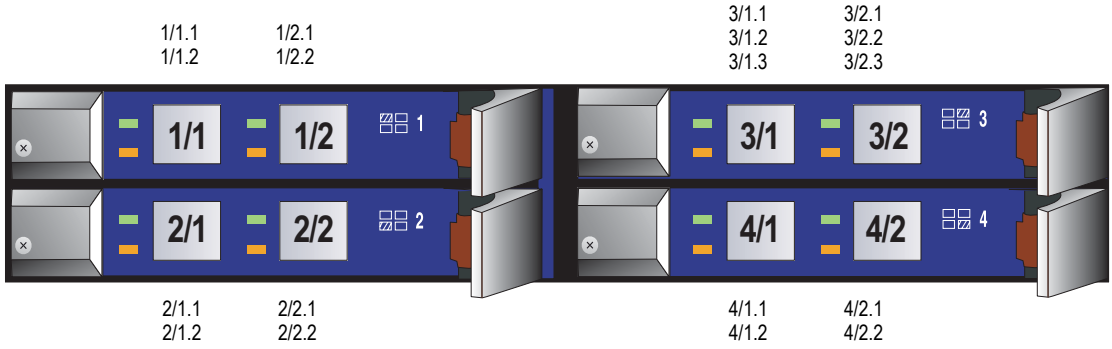
子介面

在支援虛擬 LAN (VLAN) 的裝置上，可以用邏輯方式將實體介面分成數個虛擬的子介面，每個子介面都從其源自的實體介面借用需要的頻寬。子介面是與實體介面功能相同的抽象，並且透過 802.1Q VLAN 標籤方法進行辨別。安全性裝置用子介面透過其 IP 位址和 VLAN 標籤來導引通訊流量流入和流出區域。爲了方便的目的，管理員通常使用相同的 VLAN 標籤號碼來作爲子介面號碼。例如，使用 VLAN 標籤 3 的介面 ethernet1/2 即命名爲 *ethernet1/2.3*。這表示介面模組在第一個停駐區，即該模組上的第二個連接埠，子介面編號爲 **3** *(ethernet1/2.**3**)*。

注意： 802.1Q 爲 IEEE 標準，定義執行虛擬橋接 LAN 的機制以及用來透過 VLAN 標籤指示 VLAN 成員資格的乙太網路框架格式。

請注意，雖然子介面與實體介面共用部分識別，但是其連結的區域並不依賴於實體介面連結到的區域。您可以將子介面 *ethernet1/2.3* 連結到與實體介面 *ethernet1/2* 或 *ethernet1/2.2* 所連結的不同區域上。同樣的，IP 位址的指派也沒有限制。術語 *子介面*並不暗示其位址在實體介面位址空間的子網路中。請參閱圖 6。

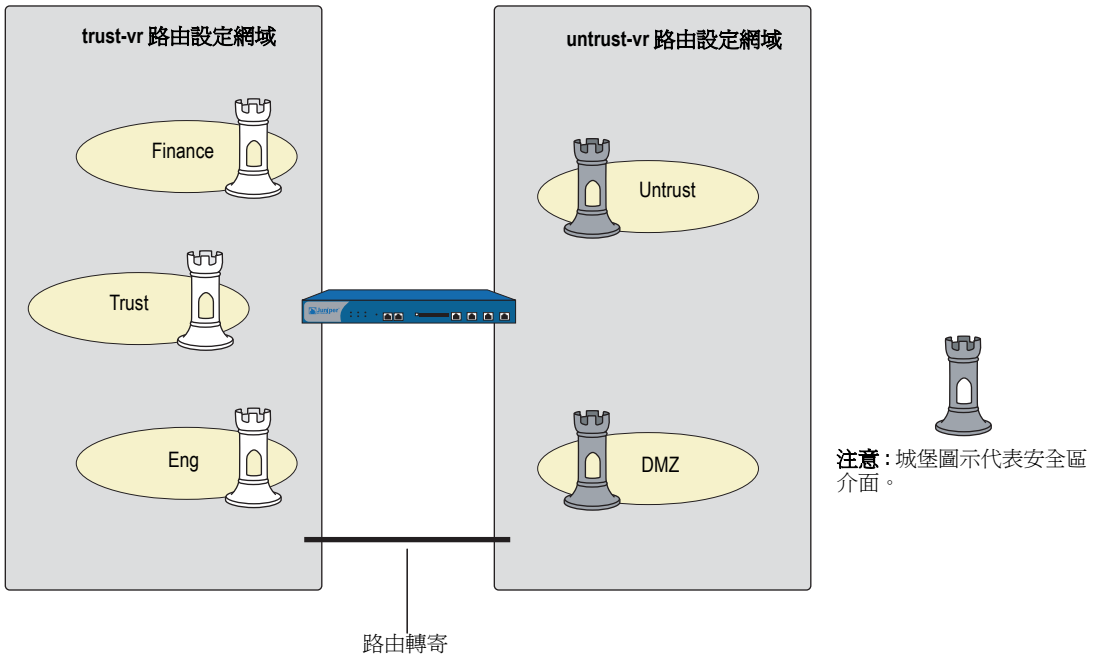
圖 6: 子介面指派



虛擬路由器

虛擬路由器 (VR) 與路由器的功能相同。它有自己的介面和單點傳送與多點傳送路由設定表。在 ScreenOS 中，安全性裝置支援兩個預先定義的虛擬路由器。這讓安全性裝置可以維護兩個分開的單點傳送和多點傳送路由設定表，並讓虛擬路由器彼此隱藏路由設定資訊。例如，untrust-vr 通常用於與不信任的方進行通訊，且不含保護區域的任何路由資訊。保護區域的路由資訊由 trust-vr 維護。因此，透過從 untrust-vr 中秘密抽取路由的方式，無法搜集到內部網路資訊。請參閱第 5 頁上的圖 7。

圖 7: 虛擬路由器安全區



若一個安全性裝置上具有兩個虛擬路由器，那麼即使有允許通訊流量的政策，通訊流量也*不會*自動在位於不同 VR 中的區域間轉寄。若您希望通訊流量能在虛擬路由器之間傳遞，您即需匯出 VR 之間的路由，或在一個 VR 上組態靜態路由，將其他 VR 定義爲下一躍點。如需有關使用兩個虛擬路由器的詳細資訊，請參閱*第 7 卷: 路由*。

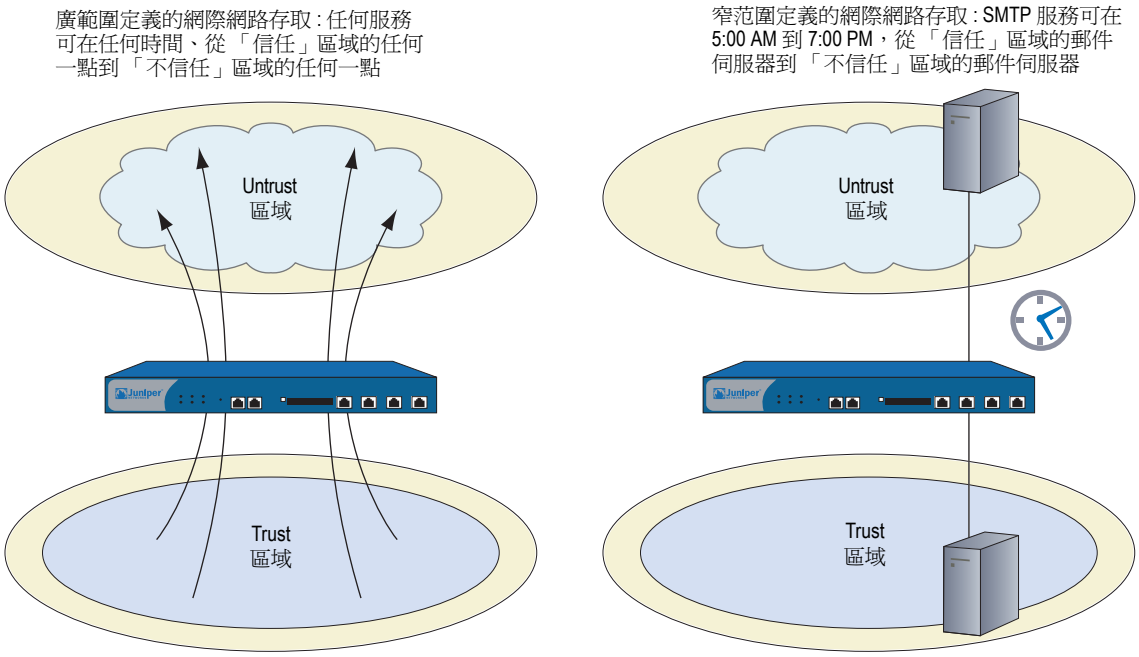
政策

Juniper Networks 安全性裝置保護網路的安全，做法是先檢查要求從一個安全區傳遞到另一個安全區的所有連接嘗試，然後予以允許或拒絕。

依預設，安全性裝置會拒絕所有方向中的所有通訊流量。透過建立政策，定義允許在排程時間透過指定來源地點到達指定目的地的通訊流量種類，您可以控制區域之間的通訊流量。在最廣泛的層級上，您可以讓所有類型的通訊流量從一個區域中的任何來源地點到達其他所有區域中的任何目的地，而且沒有任何排程限制。在最狹窄的層級上，可以建立一個政策，只允許一種通訊流量在預定的期間內、在一個區域中的指定主機與另一個區域中的指定主機之間流動。請參閱第 6 頁上的圖 8。

注意： 某些安全性裝置出售時隨附預設政策，允許從 Trust 至 Untrust 區域的向外通訊流量，但拒絕從 Untrust 區域至 Trust 區域的向內通訊流量。

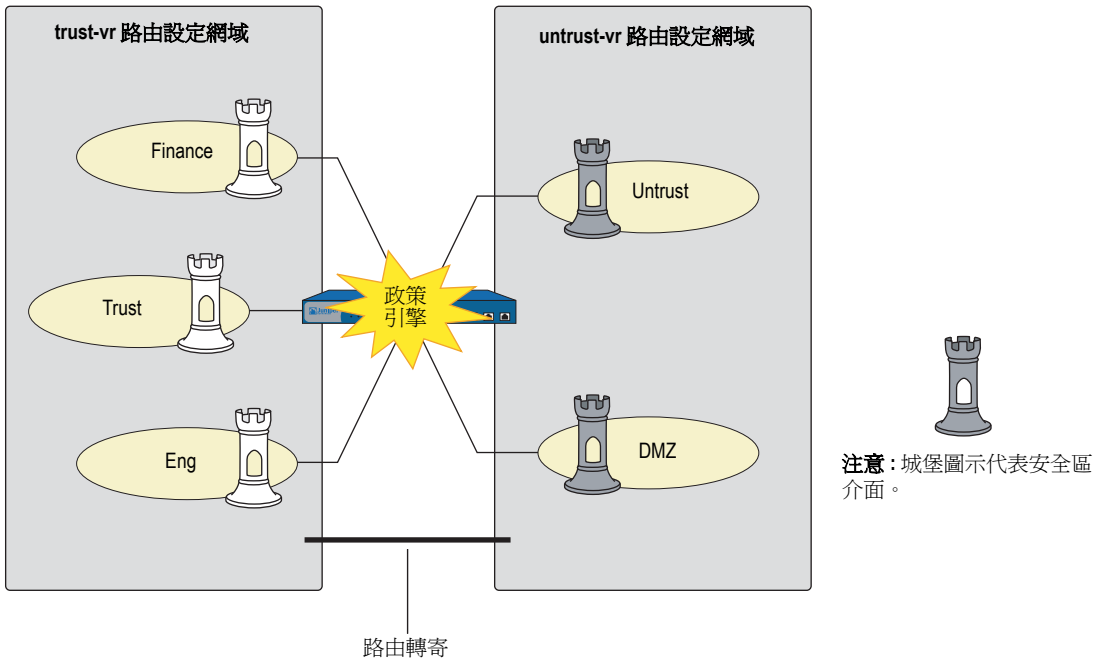
圖 8: 預設政策



每次封包嘗試從一個區域向另一個區域或在連結到同一區域的兩個介面之間通過時，安全性裝置會檢查其政策組清單中是否有允許這種通訊流量的政策（請參閱第 157 頁上的「政策組清單」）。若要讓通訊流量可以從一個安全區傳遞到另一個區域 - 例如，從區域 A 到區域 B - 必須組態一個允許區域 A 傳送通訊流量到區域 B

的政策。若要讓通訊流量向另一個方向流動，則必須組態另一個政策，允許通訊流量從區域 B 流向區域 A。對於從一個區域向另一區域傳遞的任何通訊流量，都必須有允許的政策。此外，如果啓用了區域內部阻斷，必須要有政策允許通訊流量在該區域中從一個介面向另一個介面傳遞。請參閱第 7 頁上的圖 9。

圖 9: 政策架構



注意： 如需關於政策的資訊，請參閱第 153 頁上的「政策」。

如果組態安全性裝置上的多點傳送路由設定，您可能必須組態多點傳送政策。依照預設，安全性裝置不允許區域之間的多點傳送控制通訊流量。多點傳送控制通訊流量是多點傳送通訊協定 (例如通訊協定無關多點傳送 (PIM)) 所傳輸的訊息。多點傳送政策只能控制多點傳送控制通訊流量的傳遞。若要讓資料通訊流量 (單點傳送和多點傳送) 可在區域之間傳遞，您必須組態防火牆政策。(如需關於多點傳送政策的資訊，請參閱第 **7**-120 頁上的「多點傳送政策」。)

虛擬私人網路

ScreenOS 支援多個虛擬私人網路 (VPN) 組態選項。主要的兩種類型如下：

- **以路由爲基礎的 VPN** - 路由查詢決定安全性裝置所封裝的通訊流量。政策將允許或拒絕傳至於路由中所指定之目的地的通訊流量。若政策允許通訊流量，且路由將通道介面連結參照至 VPN 通道，則安全性裝置亦會將之封裝。此組態會將政策的應用程式從 VPN 通道的應用程式分離。完成組態後，這些通道就成爲可用的資源，用於保護在安全區與另一個區域之間傳遞的通訊流量。

- **以政策爲基礎的 VPN** - 政策查詢會在政策參照某特定 VPN 通道，且將「通道」指定爲動作時，決定安全性裝置所要封裝的通訊流量。

若爲站台與站台間的 VPN 組態，可選擇使用以路由爲基礎的 VPN，因爲您可將多個政策套用至在單一 VPN 通間間傳遞的通訊流量。若爲撥接 VPN，則可選擇使用以政策爲基礎的 VPN，因爲撥接用戶端可能沒有可設定路由的內部 IP 位址。請參閱圖 10。

下列步驟爲以路由爲基礎的 VPN 組態之主要基本觀念：

1. 組態 VPN 通道時 (例如，*vpn-to-SF*，其中 *SF* 爲目的地或端項目)，在本機裝置上指定實體介面或子介面，以作爲向外介面。(遠端對等方組態遠端閘道時，必須使用此介面的 IP 位址。)

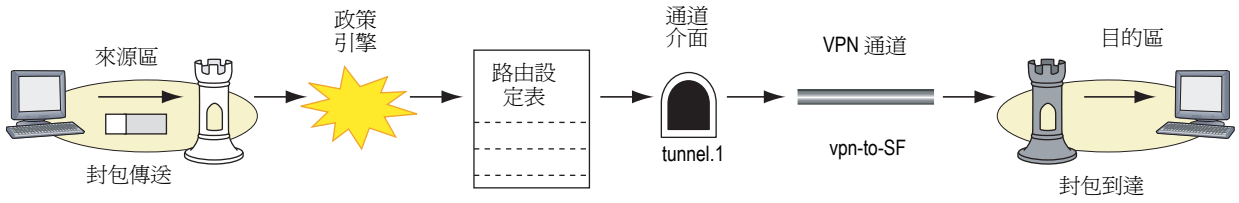
2. 建立通道介面 (例如，*tunnel.1*)，並將其連結到安全區。

注意： 不需要將通道介面連結到 VPN 通訊流量流向的相同區域。如果路由指向通道介面，則流向任何區域的通訊流量都可以存取該介面。

3. 將通道介面 *tunnel.1* 連結到 VPN 通道 *vpn-to-SF*。

4. 若要引導通訊流量通過此通道，請設定路由，指明到 *SF* 的通訊流量必須使用 *tunnel.1*。

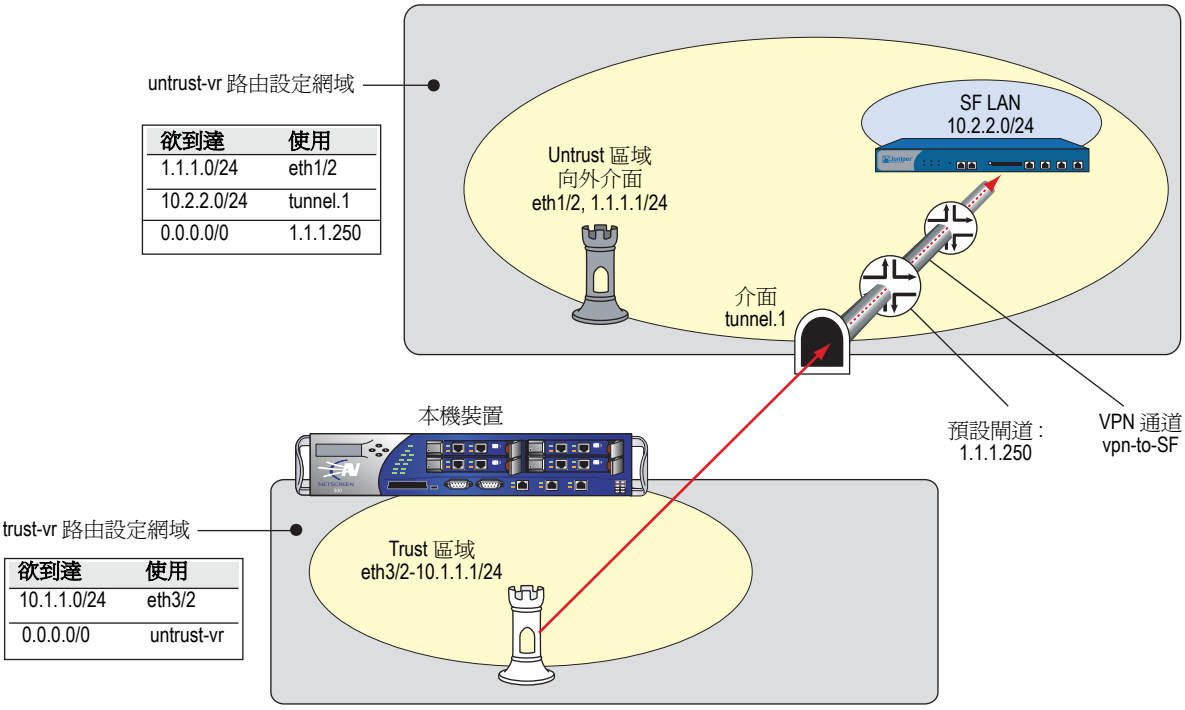
圖 10: VPN 通訊流量



此時，該通道已就緒，可讓爲 *SF* 連結的通訊流量通過。您現在可以建立通訊錄項目，如 "Trust LAN" (10.1.1.0/24) 與 "SF LAN" (10.2.2.0/24)，然後設定政策以允許或阻斷來自特定來源 (如 "Trust LAN") 或流向特定目的地 (如 "SF LAN") 的不同類型通訊流量。請參閱第 9 頁上的圖 11。

圖 11: 來自 Untrust 安全區的 VPN 通訊流量

本機安全性裝置會透過 tunnel.1 介面將通訊流量從 Trust 區域路由至 Untrust 區域中的 "SF LAN"。由於 tunnel.1 連結到 VPN 通道 "vpn-to-SF"，因此安全性裝置會將通訊流量加密，然後經由通道傳送至遠端對等方。

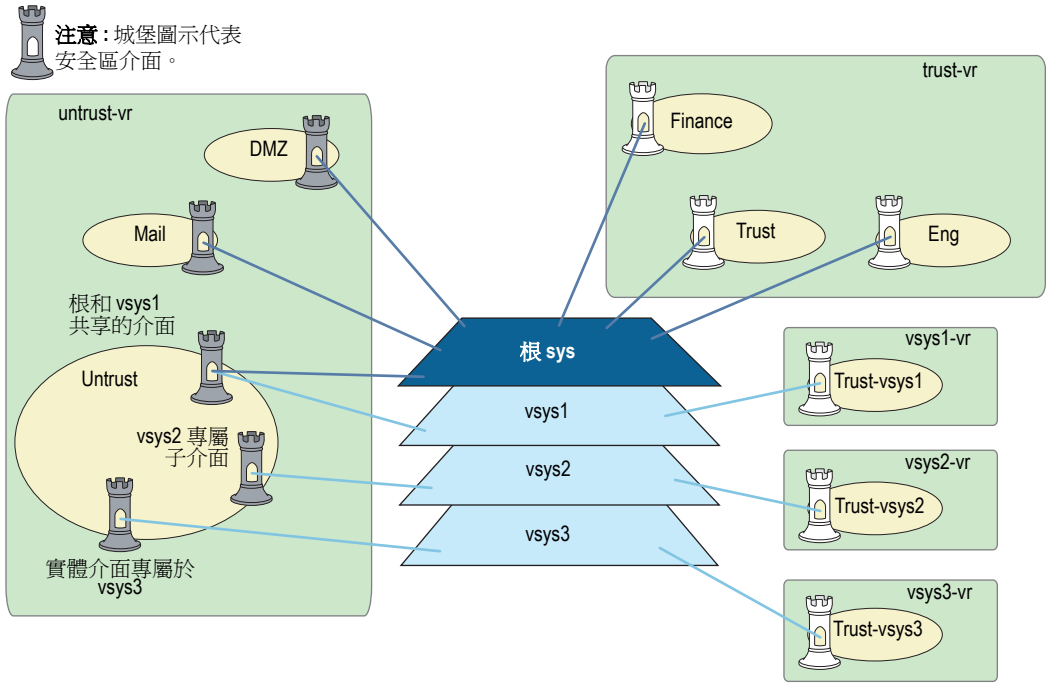


注意： 如需關於 VPN 的詳細資訊，請參閱*第 5 卷：虛擬私人網路*。

虛擬系統

某些 Juniper Networks 安全性裝置支援虛擬系統 (vsys)。虛擬系統是主系統的一部分，當作獨立的項目顯示在使用者面前。虛擬系統和相同安全性裝置中的任何其他虛擬系統及根系統常駐於不同的位置。將 ScreenOS 套用於虛擬系統時需要協調三個主要元件：區域、介面和虛擬路由器。第 10 頁上的圖 12 介紹了概念性的總覽，簡要說明了 ScreenOS 如何同時在根層級和 vsys 層級上整合這些元件。

圖 12: Vsys 架構

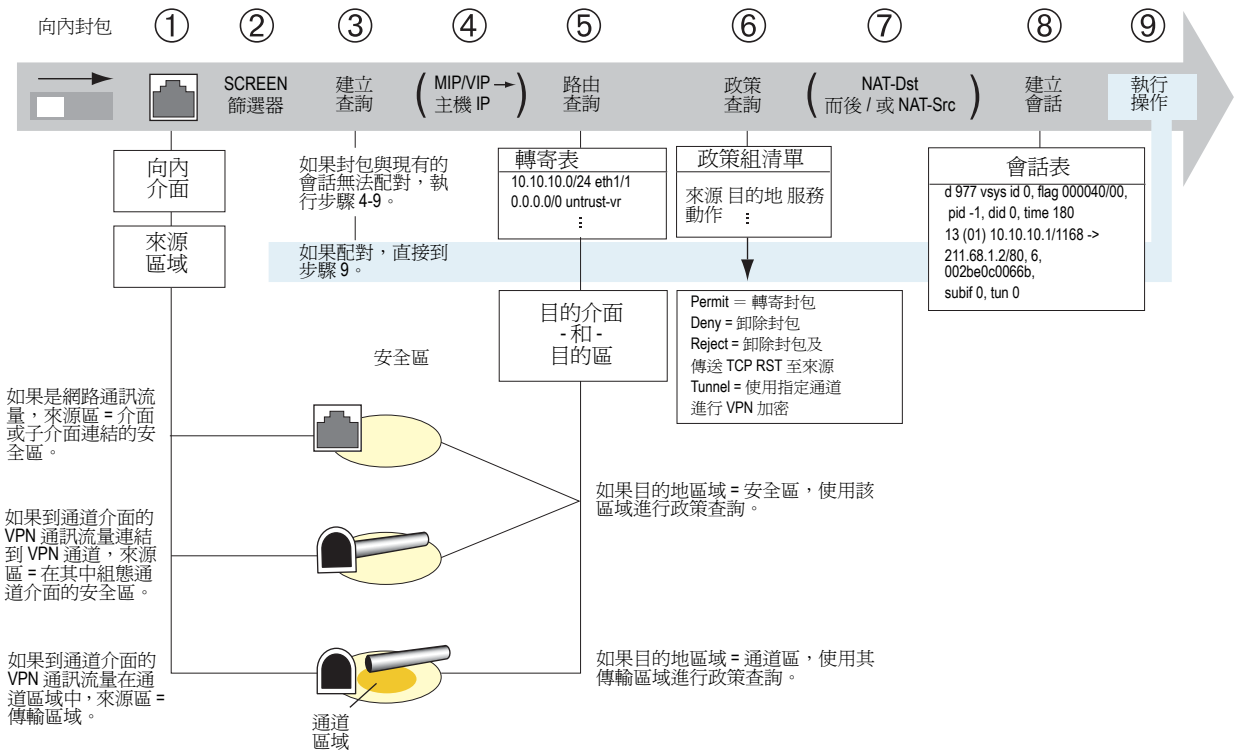


注意： 如需虛擬系統及在虛擬系統環境中套用區域、介面和虛擬路由器的詳細資訊，請參閱*第 10 卷：虛擬系統*。

封包流動順序

在 ScreenOS 中，向內封包的流動順序用圖 13 所示的方式進行。

圖 13: 通過安全區的的封包流量



1. 介面模組會識別向內介面，並進而識別連結到該介面的來源區。

   來源區判斷根據下列的準則 :

   - 如果封包沒有封裝，來源區爲向內介面或子介面連結的安全區。
   - 如果封包進行了封裝而且通道介面連結到 VPN 通道，來源區爲在其中組態通道介面的安全區。
   - 如果封包進行了封裝而且通道介面位於通道區域，來源區爲該通道區域相應的傳輸區域 (*攜帶*通道區域的安全區)。

2. 若您已啓用來源區域的 SCREEN 選項，安全性裝置此時即會啓動 SCREEN 模組。SCREEN 檢查會產生下列三個結果中的一種 :

   - 若 SCREEN 機制偵測到異常行爲 (組態爲阻斷封包)，則安全性裝置會將幫包卸除，並在事件記錄中產生一個項目。
   - 若 SCREEN 機制偵測到異常行爲 (組態爲記錄事件，但不阻斷封包)，則安全性裝置會將事件記錄在入口介面的 SCREEN 計數器清單中，然後繼續進行下一步。
   - 若 SCREEN 機制未偵測到任何異常行爲，安全性裝置即會繼續進行下一步。

3. 會話模組會執行會話查詢，嘗試將封包和現有的會話配對。

   如果封包與現有會話無法配對，安全性裝置會執行「第一個封包處理」，這個程序包括下面的步驟 4 到 9。

   如果封包和現有會話配對，安全性裝置會執行「快速處理」，使用現有會話項目中的可用資訊來處理封包。「快速處理」會繞過步驟 4 到 8，因爲這些步驟產生的資訊已經在會話的第一個處理期間取得。

4. 如果使用對應的 IP (MIP) 或虛擬 IP (VIP) 位址，位址對應模組會解析 MIP 或 VIP，以便讓路由設定表能查詢到實際的主機位址。

5. 路由設定表查詢會尋找指向目的地位址的介面。同時，介面模組會識別該介面連結的目的地區域。

   目的地區域根據下列準則判斷 :

   - 如果目的地區域是安全區，該區域會用於政策查詢。
   - 如果目的地區域是通道區，使用相應的傳輸區域進行政策查詢。
   - 如果目的地區域與來源區域相同，且該區域的區域內阻斷已停用，安全性裝置會略過步驟 6 和 7，並建立一個會話 (步驟 8)。如果啓用區域內阻斷功能，安全性裝置會卸除封包。

6. 政策引擎會搜尋政策組清單，在識別出來的來源和目的地區域中的位址之間查詢政策。

   在政策中組態的動作決定了安全性防火牆將會對封包執行的動作 :

   - 如果動作爲 **permit**，安全性裝置會決定將封包轉寄到其目的地。
   - 如果動作爲 **deny**，安全性裝置會決定將封包卸除。
   - 如果動作爲 **reject**，安全性裝置會決定卸除封包，且如果通訊協定爲 TCP，裝置會傳送重設 (RST) 至來源 IP 位址。
   - 如果動作爲 **tunnel**，安全性裝置會決定將封包轉寄給 VPN 模組，該模組會封裝封包，並使用指定的 VPN 通道設定傳送。

7. 若在政策中指定目的地位址轉譯 (NAT-dst)，則 NAT 模組會將 IP 封包標頭中的原始目的地位址轉譯爲不同的位址。

   如果指定來源位址轉譯 (以介面爲基礎的 NAT 或以政策爲基礎的 NAT-src)，NAT 模組會在將 IP 封包標題中的來源位址轉寄到目的地或 VPN 模組前將其轉譯。

   (若在相同的政策中同時指定 NAT-dst 與 NAT-src，則安全性裝置會先執行 NAT-dst，再執行 NAT-src。)

8. 會話模組在會話表中建立一個新項目，其中包含步驟 1 到 7 的結果。

   然後，安全性裝置使用會話項目中維護的資訊來處理同一會話的後續封包。

9. 安全性裝置執行在會話中指定的操作。

   典型的操作有來源位址轉譯、VPN 通道選擇、加密、解密和封包轉寄。

範例：(第 1 部份) 具有六個區域的企業

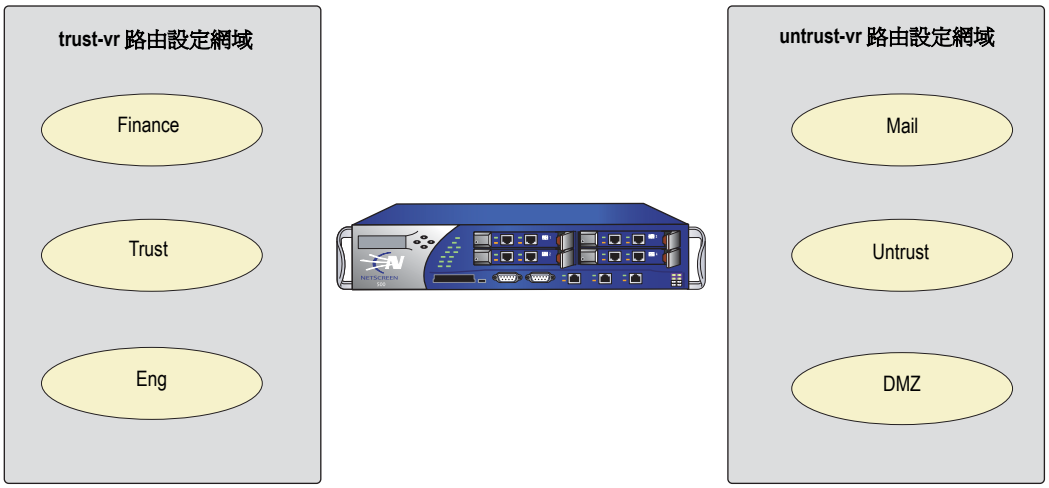
這是四部份範例中的第一部份，其目的是說明前面幾節所提到的概念。在第二個部份中，將設定每個區域的介面，請參閱第 16 頁上的「範例：(第 2 部份) 六個區域的介面」。在這裡爲企業組態下列六個區域：

- Finance
- Trust
- Eng
- Mail
- Untrust
- DMZ

Trust、Untrust 和 DMZ 區域已預先組態。您必須定義 Finance、Eng 和 Mail 區域。依預設，使用者定義的區域位於 trust-vr 路由設定網域。因此，不必爲 Finance 和 Eng 區域指定虛擬路由器。然而，除了組態 Mail 區域外，您也需要指定它位於 untrust-vr 路由設定網域。也必須將 Untrust 和 DMZ 區域的虛擬路由器連結設定從 trust-vr 轉移到 untrust-vr。請參閱第 14 頁上的圖 14。

注意： 如需虛擬路由器及其路由設定網域的詳細資訊，請參閱*第 7 卷：路由*。

圖 14: 區域到虛擬路由器連結



WebUI

Network > Zones > New: 輸入下面的內容，然後按一下 **OK**:

Zone Name: Finance
Virtual Router Name: trust-vr
Zone Type: Layer 3: (選擇)

Network > Zones > New: 輸入下面的內容，然後按一下 **OK**:

Zone Name: Eng
Virtual Router Name: trust-vr
Zone Type: Layer 3: (選擇)

Network > Zones > New: 輸入下面的內容，然後按一下 **OK**:

Zone Name: Mail
Virtual Router Name: untrust-vr
Zone Type: Layer 3: (選擇)

Network > Interfaces > Edit (對於 Untrust): 從 Virtual Router Name 下拉式清單中選擇 **untrust-vr**，然後按一下 **OK**。

Network > Zones > Edit (對於 DMZ): 從 Virtual Router Name 下拉式清單中選擇 **untrust-vr**，然後按一下 **OK**。

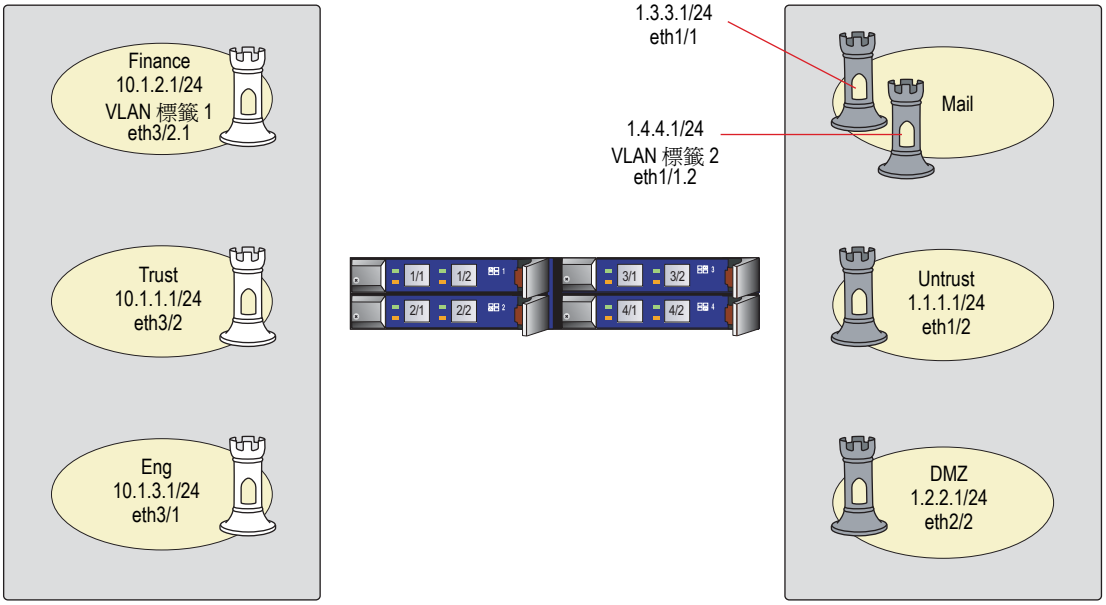
CLI

```
set zone name finance
set zone name eng
set zone name mail
set zone mail vrouter untrust-vr
set zone untrust vrouter untrust-vr
set zone dmz vrouter untrust-vr
save
```

範例：(第 2 部份) 六個區域的介面

這是漸進式範例的第二部份。在第一部份中，對區域進行了組態，請參閱第 14 頁上的「範例：(第 1 部份) 具有六個區域的企業」。在下一個部份中，將對虛擬路由器進行組態，請參閱第 19 頁上的「範例：(第 3 部份) 兩個路由設定網域」。此部份的範例說明如何將介面連結到區域，及利用 IP 位址及多個管理選項來組態區域。請參閱圖 15。

圖 15: 介面對區域連結



WebUI

1. **介面 ethernet3/2**
   Network > Interfaces > Edit (對於 ethernet3/2): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Manageable: (選擇)
   Management Services: WebUI, Telnet, SNMP, SSH (選擇)
   Other Services: Ping (選擇)

2. **介面 ethernet3/2.1**
   Network > Interfaces > Sub-IF New: 輸入下面的內容，然後按一下 **OK**:

   Interface Name: ethernet3/2.1
   Zone Name: Finance
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.2.1/24
   VLAN Tag: 1
   Other Services: Ping (選擇)

3. 介面 **ethernet3/1**
   Network > Interfaces > Edit (對於 ethernet3/1): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Eng
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.3.1/24
   Other Services: Ping (選擇)

4. 介面 **ethernet1/1**
   Network > Interfaces > Edit (對於 ethernet1/1): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Mail
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.3.3.1/24

5. 介面 **ethernet1/1.2**
   Network > Interfaces > Sub-IF New: 輸入下面的內容，然後按一下 **OK**:

   Interface Name: ethernet1/1.2
   Zone Name: Mail
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.4.4.1/24
   VLAN Tag: 2

6. 介面 **ethernet1/2**
   Network > Interfaces > Edit (對於 ethernet1/2): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.1.1.1/24
   Manageable: (選擇)
   Management Services: SNMP (選擇)

7. 介面 **ethernet2/2**
   Network > Interfaces > Edit (對於 ethernet2/2): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: DMZ
   Static IP: (選擇)
   IP Address/Netmask: 1.2.2.1/24

CLI

1. 介面 **ethernet3/2**
   set interface ethernet3/2 zone trust
   set interface ethernet3/2 ip 10.1.1.1/24
   set interface ethernet3/2 manage ping
   set interface ethernet3/2 manage webui
   set interface ethernet3/2 manage telnet
   set interface ethernet3/2 manage snmp
   set interface ethernet3/2 manage ssh

2. 介面 **ethernet3/2.1**
   set interface ethernet3/2.1 tag 1 zone finance
   set interface ethernet3/2.1 ip 10.1.2.1/24
   set interface ethernet3/2.1 manage ping

3. 介面 **ethernet3/1**
   set interface ethernet3/1 zone eng
   set interface ethernet3/1 ip 10.1.3.1/24
   set interface ethernet3/1 manage ping

4. 介面 **ethernet1/1**
   set interface ethernet1/1 zone mail
   set interface ethernet1/1 ip 1.3.3.1/24

5. 介面 **ethernet1/1.2**
   set interface ethernet1/1.2 tag 2 zone mail
   set interface ethernet1/1.2 ip 1.4.4.1/24

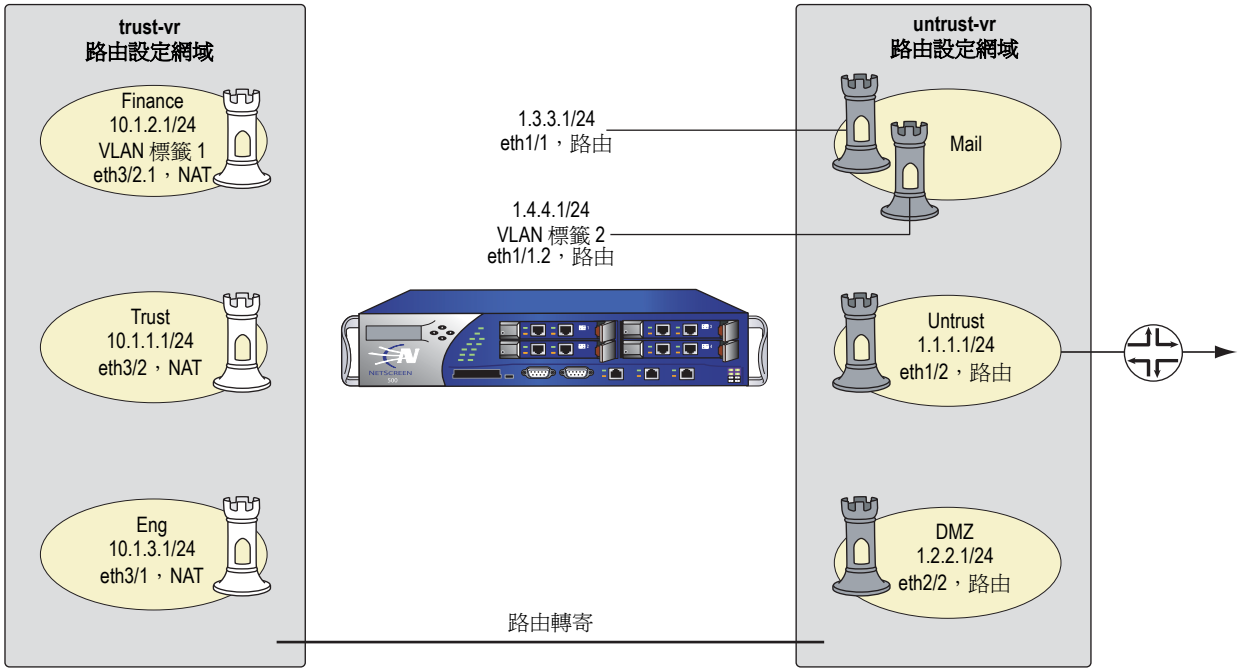
6. 介面 **ethernet1/2**
   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ip 1.1.1.1/24
   set interface ethernet1/2 manage snmp

7. 介面 **ethernet2/2**
   set interface ethernet2/2 zone dmz
   set interface ethernet2/2 ip 1.2.2.1/24
   save

範例 : (第 3 部份) 兩個路由設定網域

這是漸進式範例的第三部分。在前一個部份中，定義了多個安全區的介面，請參閱第 16 頁上的「範例 : (第 2 部份) 六個區域的介面」。在下一個部份中，將對政策進行設定，請參閱第 20 頁上的「範例 : (第 4 部份) 政策」。在本範例中，您只需爲連接到網際網路的預設閘道組態路由。其他路由在您建立介面 IP 位址時會由安全性裝置自動建立。請參閱第 19 頁上的圖 16。

圖 16: 路由設定網域



WebUI

Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 0.0.0.0/0
Next Hop Virtual Router Name: (選擇); untrust-vr

Network > Routing > Routing Entries > untrust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (選擇)
Interface: ethernet1/2
Gateway IP Address: 1.1.1.254

CLI

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface eth1/2 gateway 1.1.1.254
save
```

安全性裝置會自動建立表 1 和第 20 頁上的表 2 中所示的路由 (另有指明者除外)。

表 1: trust-vr 路由表

到達 :	使用介面 :	使用閘道 / 虛擬路由器 :	建立者 :
0.0.0.0/0	n/a	untrust-vr	由使用者組態
10.1.3.0/24	eth3/1	0.0.0.0	安全性裝置
10.1.1.0/24	eth3/2	0.0.0.0	安全性裝置
10.1.2.0/24	eth3/2.1	0.0.0.0	安全性裝置

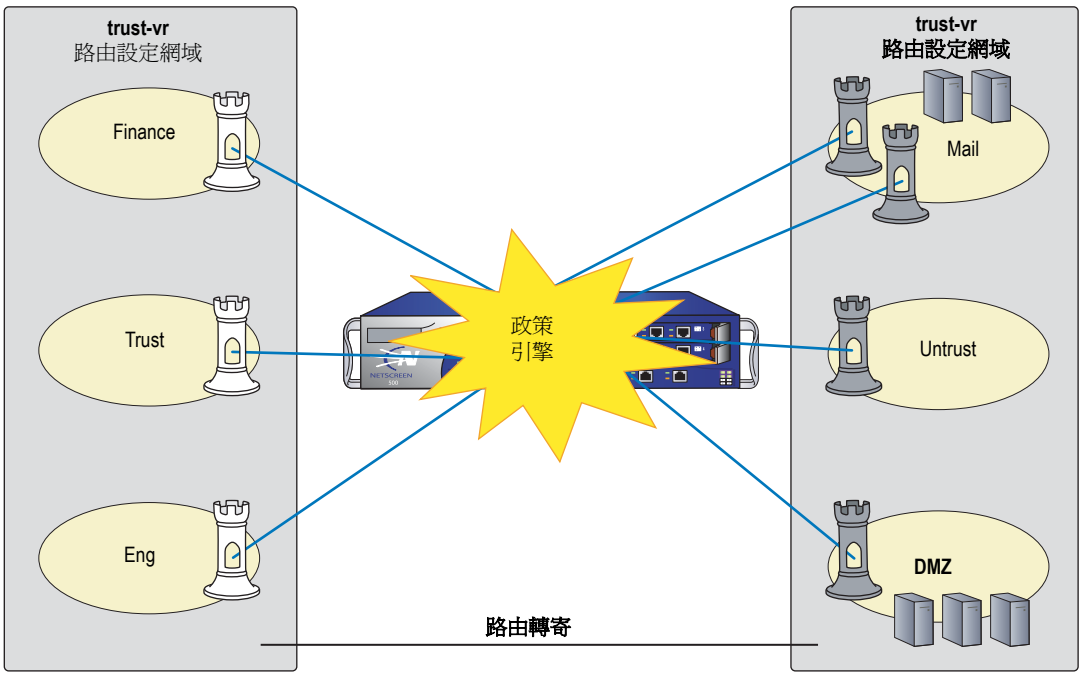
表 2: untrust-vr 路由表

到達 :	使用介面 :	使用閘道 / 虛擬路由器 :	建立者 :
1.2.2.0/24	eth2/2	0.0.0.0	安全性裝置
1.1.1.0/24	eth1/2	0.0.0.0	安全性裝置
1.4.4.0/24	eth1/1.2	0.0.0.0	安全性裝置
1.3.3.0/24	eth1/1	0.0.0.0	安全性裝置
0.0.0.0/0	eth1/2	1.1.1.254	由使用者組態

範例 : (第 4 部份) 政策

這是漸進式範例的最後一個部份。前一個部份爲第 19 頁上的「範例 : (第 3 部份) 兩個路由設定網域」。範例的這一部份示範如何組態新的政策。請參閱圖 17。

圖 17: 政策



爲了本範例的目的，在開始組態新政策前，您需要建立新的服務群組。

注意 : 建立區域時，安全性裝置會自動爲該區域內的所有主機建立位址 **Any**。本範例對於所有的主機會使用位址 **Any**。

WebUI

1. **服務群組**
   Objects > Services > Groups > New: 輸入下面的內容，然後按一下 **OK**:

   Group Name: Mail-Pop3

   選擇 **Mail**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

   選擇 **Pop3**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

   Objects > Services > Groups > New: 輸入下面的內容，然後按一下 **OK**:

   Group Name: HTTP-FTPGet

   選擇 **HTTP**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

   選擇 **FTP-Get**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

2. **政策**
   Policies > (From: Finance, To: Mail) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), Any
   Service: Mail-Pop3
   Action: Permit

   Policies > (From: Trust, To: Mail) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), Any
   Service: Mail-Pop3
   Action: Permit

Policies > (From: Eng, To: Mail) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: Mail-Pop3
Action: Permit

Policies > (From: Untrust, To: Mail) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: Mail
Action: Permit

Policies > (From: Finance, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

Policies > (From: Finance, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

Policies > (From: Trust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

Policies > (From: Eng, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

Policies > (From: Eng, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: FTP-Put
Action: Permit

Policies > (From: Untrust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: HTTP-FTPGet
Action: Permit

CLI

1. 服務群組

```
set group service mail-pop3 add mail
set group service mail-pop3 add pop3
set group service http-ftpget add http
set group service http-ftpget add ftp-get
```

2. 政策

```
set policy from finance to mail any any mail-pop3 permit
set policy from trust to mail any any mail-pop3 permit
set policy from eng to mail any any mail-pop3 permit
set policy from untrust to mail any any mail permit
set policy from finance to untrust any any http-ftpget permit
set policy from finance to dmz any any http-ftpget permit
set policy from trust to untrust any any http-ftpget permit
set policy from trust to dmz any any http-ftpget permit
set policy from eng to untrust any any http-ftpget permit
set policy from eng to dmz any any http-ftpget permit
set policy from eng to dmz any any ftp-put permit
set policy from untrust to dmz any any http-ftpget permit
save
```

第 2 章

區域

區域可以是已套用安全措施的網路空間片段 (安全區)、連結了 VPN 通道介面的邏輯片段 (通道區)，或者是一個執行特定功能的實體或邏輯項目 (功能區)。

本章研究各種類型的區域，特別將重點放在安全區上，並說明連接埠模式。本章包括下列各節 :

- 第 26 頁上的「檢視預先組態的區域」
- 第 28 頁上的「安全區」
  - 第 28 頁上的「Global 區域」
  - 第 28 頁上的「SCREEN 選項」
- 第 28 頁上的「將通道介面連結至通道區」
- 第 30 頁上的「設定安全區和通道區」
  - 第 30 頁上的「建立區域」
  - 第 31 頁上的「修改區域」
  - 第 31 頁上的「刪除區域」
- 第 32 頁上的「功能區」
  - 第 32 頁上的「Null 區域」
  - 第 32 頁上的「MGT 區域」
  - 第 32 頁上的「HA 區域」
  - 第 32 頁上的「自我區域」
  - 第 32 頁上的「VLAN 區域」

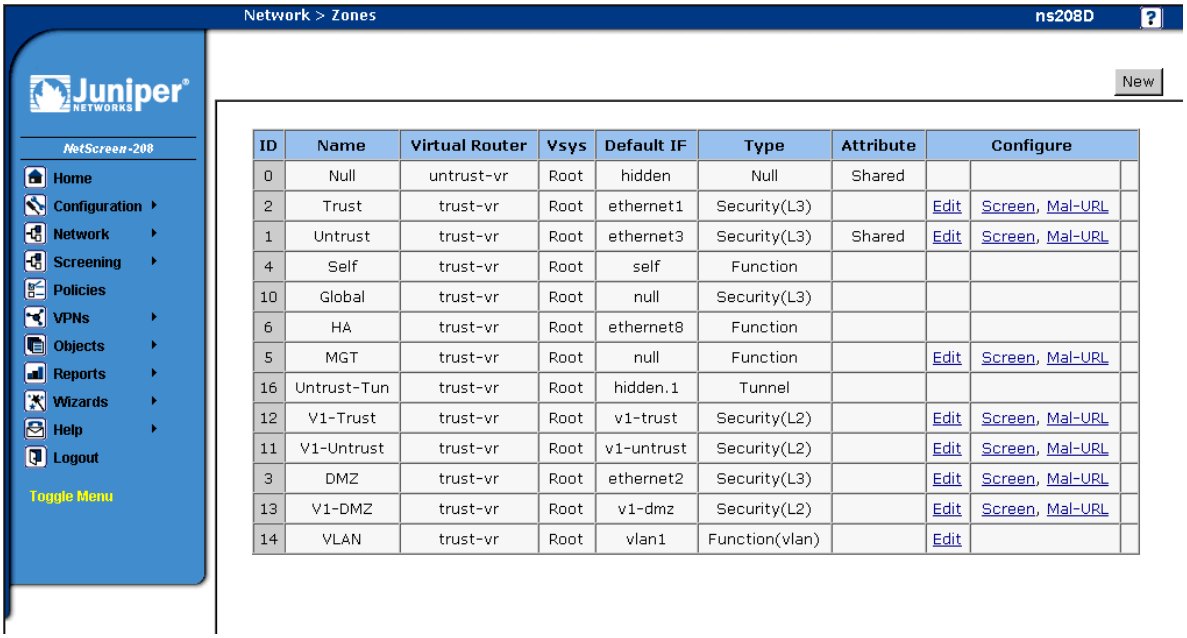
- 第 32 頁上的「連接埠模式」
  - 第 33 頁上的「Trust-Untrust 模式」
  - 第 34 頁上的「Home-Work 模式」
  - 第 35 頁上的「Dual Untrust 模式」
  - 第 36 頁上的「Combined 模式」
  - 第 37 頁上的「Trust/Untrust/DMZ (擴展) 模式」
  - 第 37 頁上的「DMZ/Dual Untrust 模式」
  - 第 38 頁上的「Dual DMZ 模式」
- 第 39 頁上的「設定連接埠模式」
- 第 40 頁上的「Home-Work 與 Combined 連接埠模式的區域」

檢視預先組態的區域

首次啓動安全性裝置時，可以看到數個預先組態的區域。若要使用 WebUI 檢視這些區域，請按一下左側功能表欄中的 **Network > Zones**。請參閱圖 18。

若要使用 CLI 檢視這些區域，請使用 **get zone** 指令。請參閱第 27 頁上的圖 19。

圖 18: WebUI 中的 Network > Zones 頁面



ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure	
0	Null	untrust-vr	Root	hidden	Null	Shared		
2	Trust	trust-vr	Root	ethernet1	Security(L3)		Edit	Screen, Mal-URL
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	Edit	Screen, Mal-URL
4	Self	trust-vr	Root	self	Function			
10	Global	trust-vr	Root	null	Security(L3)			
6	HA	trust-vr	Root	ethernet8	Function			
5	MGT	trust-vr	Root	null	Function		Edit	Screen, Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel			
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)		Edit	Screen, Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)		Edit	Screen, Mal-URL
3	DMZ	trust-vr	Root	ethernet2	Security(L3)		Edit	Screen, Mal-URL
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)		Edit	Screen, Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)		Edit	

圖 19 顯示 **get zone** 指令的輸出。

圖 19: Get zone 指令輸出

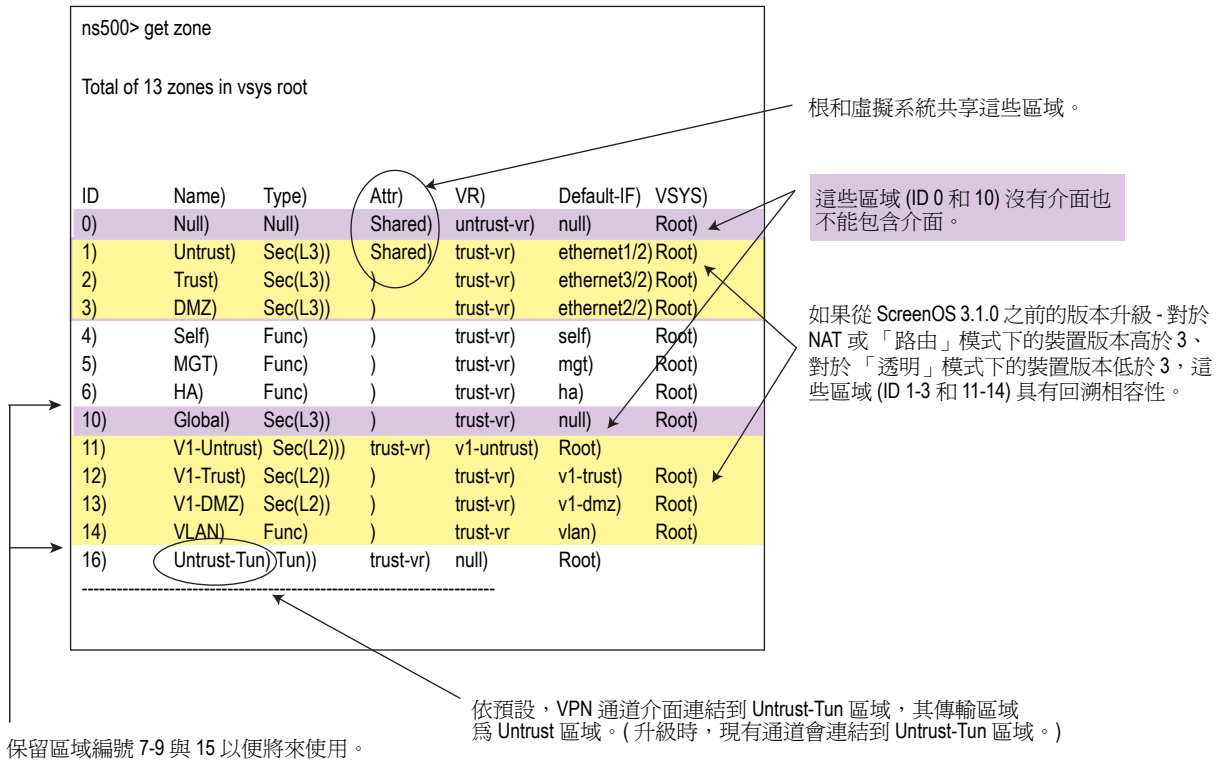


圖 18 和圖 19 中所示的預先組態區域可分成三種不同的類型 :

- 安全區 : Untrust、Trust、DMZ、Global、V1-Untrust、V1-Trust、V1-DMZ
- 通道區 : 不信任的通道
- 功能區 : Null、Self、MGT、HA、VLAN

安全區

在單一安全性裝置上，可以組態多個安全區，將網路分成區域，可對這些區域套用各種安全選項以滿足其需求。您必須至少定義兩個安全區，基本上是爲了保護網路的不同區域。在某些安全性平台上，您可以定義多個安全區，讓網路安全設計具有更高的精確度 - 而且這麼做並不需要組態多個安全設備。

Global 區域

您可以識別安全區，因爲它有通訊錄而且可以在政策中參考。Global 區域滿足這些條件。但是，它沒有其他安全區都有的一種元素 - 介面。Global 區域可作爲對應的 IP (MIP) 和虛擬 IP (VIP) 位址的儲存區域。預先定義的 Global 區位址 "Any" 套用至所有 MIP、VIP 與其他在 Global 區域中設定的使用者定義位址。因爲通往這些位址的通訊流量對應到其他的位址，所以 Global 區域不需要讓通訊流量從中流過的介面。

Global 區域也包含全域政策中使用的位址。如需關於全域政策的詳細資訊，請參閱第 156 頁上的「全域政策」。

注意： 以 Global 區域作爲其目的地的政策都不支援 NAT 或通訊流量整理。

SCREEN 選項

Juniper Networks 防火牆保護網路的安全，做法是先檢查要求從一個安全區傳遞到另一個安全區的所有連接嘗試，然後予以允許或拒絕。您可以針對每一個安全區及 MGT 區域啓用一組預先定義的 SCREEN 選項，以偵測及阻斷多種安全性裝置判定爲有害的通訊流量。

如需有關可用 SCREEN 選項的詳細資訊，請參閱*第 4 卷：攻擊偵測與防禦機制*。

將通道介面連結至通道區

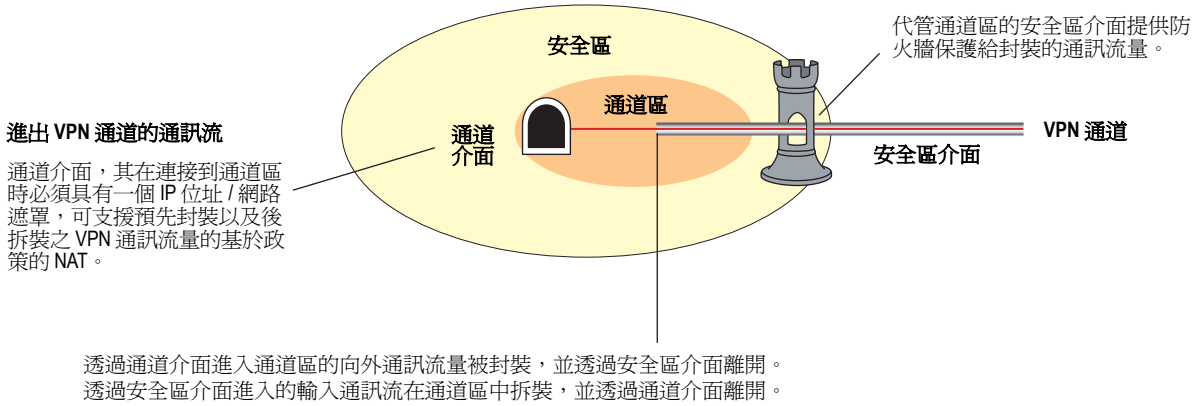
通道區是代管一個或多個通道介面的邏輯片段。通道區就概念而言以「子父」關係附屬到安全區。安全區充當「父項」，可以將其視爲承載區域，爲封裝的通訊流提供防火牆保護。通道區提供封包封裝 / 拆裝作業，並且透過支援具可代管對應的 IP (MIP) 與動態 IP (DIP) 集區的 IP 位址和遮罩的通道介面，也可提供以政策爲基礎的 NAT 服務。

安全性裝置使用路由設定資訊讓傳輸區域將通訊流量引導到通道終點。預設的通道區爲 Untrust-Tun，與 Untrust 區域相關聯。您可以建立其他通道區並將其連結到其他安全區，每個虛擬系統上的每個傳輸區域最多只能有一個通道區。

注意： 根系統與所有虛擬系統可以共享 Untrust 區域。但是，每個系統都有自己獨自的 Untrust-Tun 區域。

依預設，通道區在 trust-vr 路由設定網域中，但是也可以將通道區移動到其他路由設定網域中。請參閱第 29 頁上的圖 20。

圖 20: 通道區路由設定網域



從 3.1.0 以前版本的 ScreenOS 升級時，依預設，現有的通道介面連接到預先組態的 Untrust-Tun 通道區，這是預先組態的 Untrust 安全區的「子」區域。可以將多個通道區連結到相同的安全區；但是不可以將通道區連接到另一個通道區。

在本範例中，建立一個通道介面，並將之命名爲 tunnel.3。將之連結至 Untrust-Tun 區，並爲其指派 IP 位址 3.3.3.3/24；然後在 tunnel.3 上定義對應的 IP (MIP) 位址，將 3.3.3.5 轉譯爲 10.1.1.5，即 Trust 區中的伺服器位址。Untrust 區域 (Untrust-Tun 區域的傳輸區) 與 Trust 區域均位在 trust-vr 路由設定網域內。

WebUI

1. **通道介面**
   Network > Interfaces > New Tunnel IF: 輸入下面的內容，然後按一下 **OK**:

   Tunnel Interface Name: tunnel.3
   Zone (VR): Untrust-Tun (trust-vr)
   Fixed IP: (選擇)
   IP Address/Netmask: 3.3.3.3/24

2. **MIP**
   Network > Interfaces > Edit (對於 tunnel.3) > MIP > New: 輸入下面的內容，然後按一下 **OK**:

   Mapped IP: 3.3.3.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

CLI

1. **通道介面**
   set interface tunnel.3 zone Untrust-Tun
   set interface tunnel.3 ip 3.3.3.3/24

2. **MIP**
   set interface tunnel.3 mip 3.3.3.5 host 10.1.1.5
   save

設定安全區和通道區

建立、修改及刪除 Layer 3 (第 3 層) 或 Layer 2 (第 2 層) 安全區和通道區的程序相當類似。

注意： 您不能刪除預先定義的安全區或預先定義的通道區，但是可以加以編輯。

建立區域

若要建立 Layer 3 (第 3 層) 或 Layer 2 (第 2 層) 安全區或建立 Tunnel 區，請使用 WebUI 或 CLI:

WebUI

Network > Zones > New: 輸入下面的內容，然後按一下 **OK**:

Zone Name: 鍵入區域名稱。

Virtual Router Name: 選擇要在其路由設定網域中放置區域的虛擬路由器。

Zone Type:

選擇 **Layer 3** 以建立區域，可以將處於 NAT 或「路由」模式的介面連結到該區域。

選擇 **Layer 2** 以建立區域，可以將在「透明」模式中的介面連結到該區域。

建立通道區並將其連結到傳輸區域時，請選擇 **Tunnel Out Zone**，然後從下拉式清單中選擇特定的傳輸區域。

Block Intra-Zone Traffic: 選擇此選項以阻斷相同安全區中主機之間的通訊流量。依預設，會停用區域內部阻斷。

注意： Layer 2 (第 2 層) 安全區的名稱必須以 "L2-" 開頭；例如，"L2-Corp" 或 "L2-Xnet"。

CLI

```
set zone name zone [ l2 vlan_id_num | tunnel sec_zone ]
set zone zone block
set zone zone vrouter name_str
```

注意： 建立 Layer 2 (第 2 層) 安全區時，VLAN ID number 必須爲 1 (對於 VLAN1)。

修改區域

若要修改安全區或通道區的名稱，或變更通道區的傳輸區域，必須先刪除區域，然後再用變更的值重新建立區域。您可以變更現有區域上的區域內部阻斷選項和虛擬路由器。

注意 : 移除區域前，必須先解除所有連結到它的介面。

您必須先移除任何與某區域相連結的介面才能變更該區域的虛擬路由器。

WebUI

1. **修改區域名稱**
   Network > Zones: 按一下 **Remove** (對於要變更其名稱的安全區或通道區，或對於要變更其傳輸區域的通道區)。

   出現提示要求對刪除操作進行確認時，按一下 **Yes**。

   Network > Zones > New: 輸入變更後的區域設定，然後按一下 **OK**。

2. **變更區域內部阻斷選項或虛擬路由器**
   Network > Zones > Edit (對於要修改的區域): 輸入下面的內容，然後按一下 **OK**:

   Virtual Router Name: 從下拉式清單中，選擇要將區域移動到其路由設定網域中的虛擬路由器。

   Block Intra-Zone Traffic: 若要啓用，請選取該核取方塊。若要停用，請將其清除。

CLI

1. **修改區域名稱**
   unset zone *zone*
   set zone name *zone* [l2 *vlan_id_num* | tunnel *sec_zone*]

2. **變更區域內部阻斷選項或虛擬路由器**
   { set | unset } zone *zone* block
   set zone *zone* vrouter *name_str*

刪除區域

若要刪除安全區或通道區，請執行下面的操作之一 :

WebUI

Network > Zones: 按一下 **Remove** (對於要刪除的區域)。

出現提示要求對刪除操作進行確認時，按一下 **Yes**。

CLI

unset zone *zone*

注意 : 移除區域前，必須先解除所有連結到它的介面。若要解除介面與區域之間的連結，請參閱第 51 頁上的「將介面連結到安全區」。

功能區

共有五個功能區，分別是 Null、MGT、HA、Self 與 VLAN。每個區域的存在都有其專門的目的，如下列各小節所述。

Null 區域

此區域用於暫時儲存沒有連結到任何其他區域的介面。

MGT 區域

此區域管理超出頻寬的管理介面 MGT。您可以在此區域上設定防火牆選項，以避免管理通訊流量受到不同類型的攻擊。如需有關防火牆選項的詳細資訊，請參閱 *第 4 卷 : 攻擊偵測與防禦機制*。

HA 區域

此區域管理高可用性介面 HA1 和 HA2。雖然您可以針對 HA 區域設定介面，但區域本身是無法組態的。

自我區域

此區域管理遠端管理連接的介面。透過 HTTP、SCS 或 Telnet 連接到安全性裝置時，就會連接到 自我區域。

VLAN 區域

此區域代管 VLAN1 介面，您可以在裝置處於「透明」模式時，使用此介面來管理裝置，及終止 VPN 通訊流量。您亦可在此區域上設定防火牆選項，以避免 VLAN1 介面受到不同類型的攻擊。

連接埠模式

您可針對某些 Juniper Networks 安全性裝置選擇一種*連接埠模式*。連接埠模式自動爲裝置設定不同的連接埠、介面和區域連結。

在連接埠模式內容中，*連接埠*指的是裝置背面的實體介面。連接埠上的標籤可識別連接埠的用途 :

- Untrusted (不受信任的)
- 1-4
- 主控台
- Modem (數據機)

*介面*一詞指的是可透過 WebUI 或 CLI 組態的邏輯介面。每一個連接埠僅能連結到一個介面，但每一個介面可以有多個連接埠連結。

警告 : 變更連接埠模式會移除安全性裝置上任何現有的組態，並需進行系統重設。

表 3 顯示安全性裝置上可用的連接埠模式。若要檢視無線介面到區域的連結，請參閱第 12-33 頁上的「無線區域網路」。

表 3: 連接埠模式可用性

連接埠模式	裝置上可用
Trust-Untrust (預設)	NetScreen-5GT、NetScreen-5GT ADSL、NetScreen-5GT Wireless、NetScreen-5GT Wireless ADSL 及 NetScreen-5XT
Home-Work	NetScreen-5GT、NetScreen-5GT ADSL、NetScreen-5GT Wireless、NetScreen-5GT Wireless ADSL 及 NetScreen-5XT
Dual Untrust	NetScreen-5GT、NetScreen-5GT Wireless 及 NetScreen-5XT
Combined	NetScreen-5GT、NetScreen-5GT Wireless 及 NetScreen-5XT
Trust/Untrust/ DMZ (擴展) (必須具有擴展許可金鑰)	NetScreen-5GT、NetScreen-5GT ADSL、NetScreen-5GT Wireless 及 NetScreen-5GT Wireless ADSL
DMZ/Dual Untrust (必須具有擴展許可金鑰)	NetScreen-5GT 及 NetScreen-5GT Wireless
Dual DMZ (必須具有擴展許可金鑰)	NetScreen-5GT 及 NetScreen-5GT Wireless

Trust-Untrust 模式

Trust-Untrust 模式爲預設的連接埠模式。請參閱圖 21。

圖 21: Trust-Untrust 連接埠模式介面到區域連結

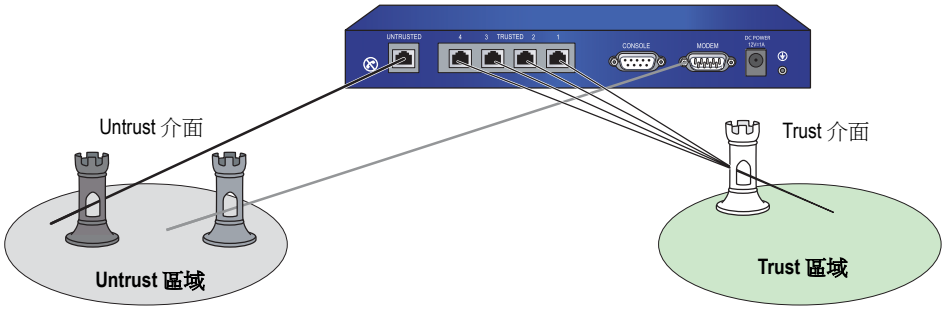


表 4 提供 Trust-Untrust 模式介面到區域連結。

表 4: Trust-Untrust 連結

連接埠	介面	區域
Untrusted (不受信任的)	Untrust	Untrust
1	Trust	Trust
2	Trust	Trust
3	Trust	Trust
4	Trust	Trust
Modem (數據機)	序列	Null

Home-Work 模式

Home-Work 模式會將介面連結至 Untrust 安全區及 Home 和 Work 安全區。Work 與 Home 區域允許您將各區域中的使用者與資源分離。在此模式下，預設政策允許自 Work 區域至 Home 區域的通訊流量，但不允許自 Home 區域至 Work 區域的通訊流量。您可自訂套用至從 Home 區域傳輸到 Work 區域的通訊流量的政策。請參閱圖 22。依預設，對自 Home 區域至 Untrust 區域的通訊流量沒有任何限制。Home 區域會對 Ping 做出回應。

圖 22: Home-Work 連接埠模式介面到區域連結

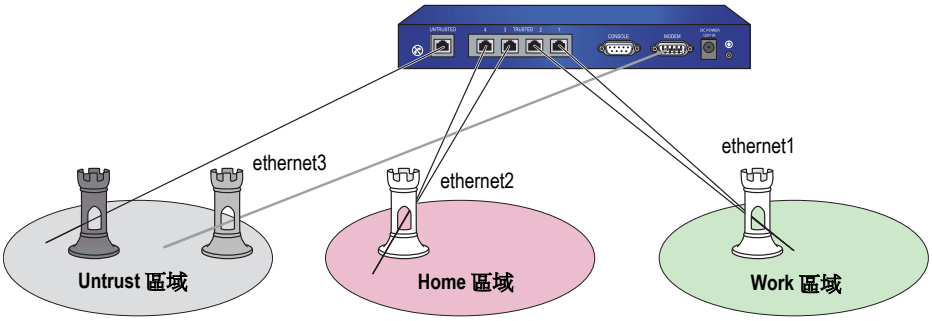


表 5 提供 Home-Work 模式介面到區域連結。

表 5: Home-Work 連結

連接埠	介面	區域
Untrusted (不受信任的)	Untrust	Untrust
1	ethernet1	Work
2	ethernet1	Work
3	ethernet2	Home
4	ethernet2	Home
Modem (數據機)	ethernet3	Untrust

請參閱第 40 頁上的「Home-Work 與 Combined 連接埠模式的區域」以取得有關組態及使用 Home-Work 模式的詳細資訊。

Dual Untrust 模式

Dual Untrust 模式將兩個介面連結至 Untrust 安全區，允許通訊流量同時通過內部網路。請參閱圖 23。

圖 23: Dual Untrust 連接埠模式介面到區域連結

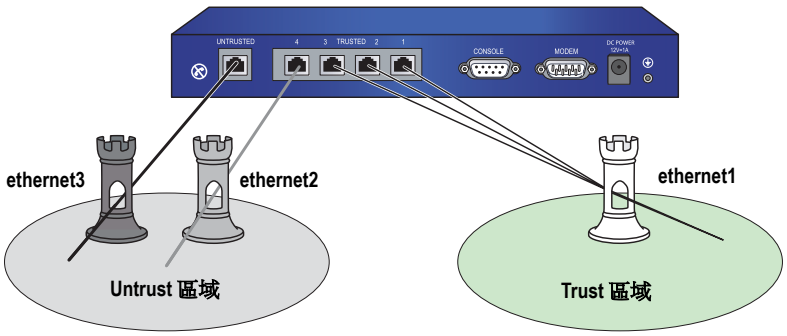


表 6 提供 Dual Untrust 模式介面到區域連結。

表 6: Dual Untrust 連結

連接埠	介面	區域
Untrusted (不受信任的)	ethernet3	Untrust
1	ethernet1	Trust
2	ethernet1	Trust
3	ethernet1	Trust
4	ethernet2	Untrust
Modem (數據機)	N/A	N/A

注意： 在「雙重不受信任」連接埠模式下無法使用序列介面。

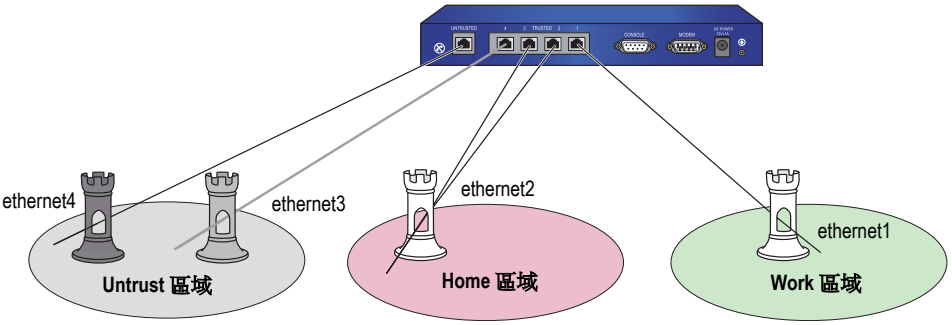
若要啓用故障後移轉功能，而不同時傳送通訊流量，請使用 **set failover enable** 指令。

請參閱*第 11 卷：高可用性*以取得有關組態及使用「雙重不受信任」模式的詳細資訊。

Combined 模式

Combined 模式將主要介面及備份介面連結至網際網路，並可分離 Work 與 Home 區域中的使用者與資源。請參閱圖 24。

圖 24: Combined 連接埠模式介面到區域連結



注意： 若爲 NetScreen-5XT，僅在 NetScreen-5XT Elite (不受限制使用者) 平台上才支援 Combined 模式。您無法使用 Initial Configuration Wizard (初始組態精靈) 來組態 Combined 模式。此模式只能使用 WebUI 或 CLI 來組態。

表 7 提供 Combined 模式介面到區域連結。

表 7: Combined 連結

連接埠	介面	區域
Untrusted (不受信任的)	ethernet4	Untrust
1	ethernet1	Work
2	ethernet2	Home
3	ethernet2	Home
4	ethernet3	Untrust
Modem (數據機)	N/A	N/A

注意： 在 Combined 連接埠模式下無法使用序列介面。

請參閱*第 11 卷：高可用性*與第 40 頁上的「Home-Work 與 Combined 連接埠模式的區域」以取得有關組態及使用 Combined 模式的詳細資訊。

Trust/Untrust/DMZ (擴展) 模式

Trust/Untrust/DMZ (擴展) 模式會將介面連結至 Untrust、Trust 與 DMZ 安全區，允許您分離來自內部網路的 web、電子郵件或其他應用程式伺服器。請參閱圖 25。

圖 25: 擴展連接埠模式介面到區域連結

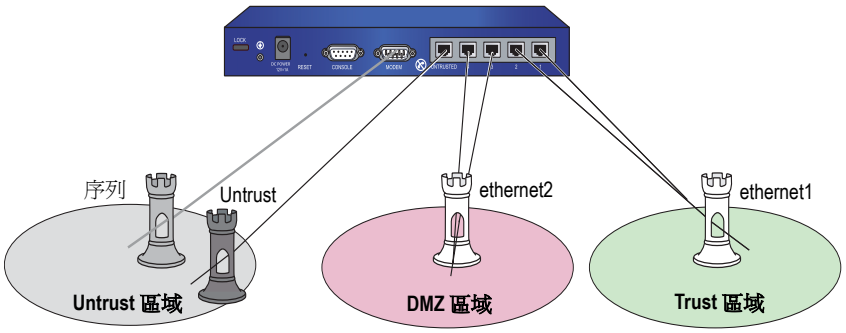


表 8 提供 Extended 模式介面到區域連結。

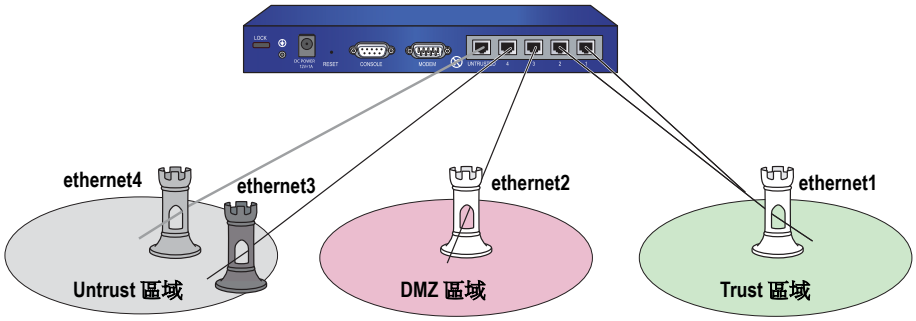
表 8: Extended 連結

連接埠	介面	區域
Untrusted (不受信任的)	Untrust	Untrust
1	ethernet1	Trust
2	ethernet1	Trust
3	ethernet2	DMZ
4	ethernet2	DMZ
Modem (數據機)	序列	Untrust

DMZ/Dual Untrust 模式

DMZ/Dual Untrust 模式將 Untrust、Trust 和 DMZ 安全區的介面結合在一起，可讓您同時從內部網路傳送通訊流量。請參閱第 37 頁上的圖 26。

圖 26: DMZ/Dual Untrust 連接埠模式介面到區域連結



注意： DMZ/Dual Untrust 模式僅在 NetScreen-5GT 及 NetScreen-5GT Wireless 平台上受支援，且需具有擴展許可金鑰。

表 9 提供 DMZ/Dual Untrust 模式介面到區域連結。

表 9: DMZ/Dual Untrust 連結

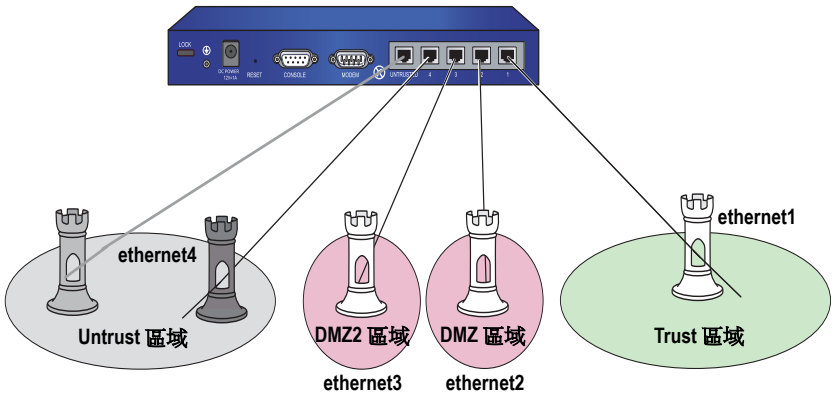
連接埠	介面	區域
Untrusted（不受信任的）	ethernet4	Untrust
1	ethernet1	Trust
2	ethernet1	Trust
3	ethernet2	DMZ
4	ethernet3	Untrust
Modem（數據機）	N/A	N/A

注意： 在「DMZ/Dual Untrust 連接埠」模式下無法使用序列介面。若要啓用故障後移轉功能，而不同時傳送通訊流量，請使用 **set failover enable** 指令。

Dual DMZ 模式

Dual DMZ 模式將 Untrust、Trust、DMZ 和 DMZ2 安全區的介面結合在一起，可讓您從內部網路同時傳送通訊流量。請參閱第 38 頁上的圖 27。

圖 27: Dual DMZ 連接埠模式介面到區域連結



注意： Dual DMZ 模式僅在 NetScreen-5GT 及 NetScreen-5GT Wireless 平台上受支援，且需具有擴展許可金鑰。

表 10 提供 Dual DMZ 模式介面到區域連結。

表 10: Dual DMZ 連結

連接埠	介面	區域
Untrusted (不受信任的)	ethernet5	Untrust
1	ethernet1	Trust
2	ethernet2	DMZ
3	ethernet3	DMZ2
4	ethernet4	Untrust
Modem (數據機)	N/A	N/A

設定連接埠模式

您可以透過 WebUI 或 CLI 變更安全性裝置上的連接埠模式設定。設定連接埠模式之前，請注意下列各點 :

- 變更連接埠模式會*移除*裝置上任何現有的組態，並需進行系統重設。
- 發出 **unset all** CLI 指令並不會影響裝置上的連接埠模式設定。例如，若您想要將連接埠模式設定從 Combined 模式變回預設的 Trust-Untrust 模式，發 **unset all** 指令會移除現有的組態，但*不會*將裝置設爲 Trust-Untrust 模式。

範例 : Home-Work 連接埠模式

在本範例中，將 NetScreen-5XT 上的連接埠模式設爲 Home-Work 模式。

WebUI

Configuration > Port Mode > Port Mode: 從下拉式清單中選擇 Home-Work，然後按一下 **Apply**。

在下列提示中按一下 **OK**:

Operational mode change will erase current configuration and reset the device, continue?

CLI

```
exec port-mode home-work
```

在下列提示中輸入 **y** (表示是):

```
Change port mode from <trust-untrust> to <home-work> will erase system
configuration and reboot box

Are you sure y/[n] ?
```

若要檢視裝置上目前的連接埠設定，請執行下列操作之一：

WebUI

Configuration > Port Mode

CLI

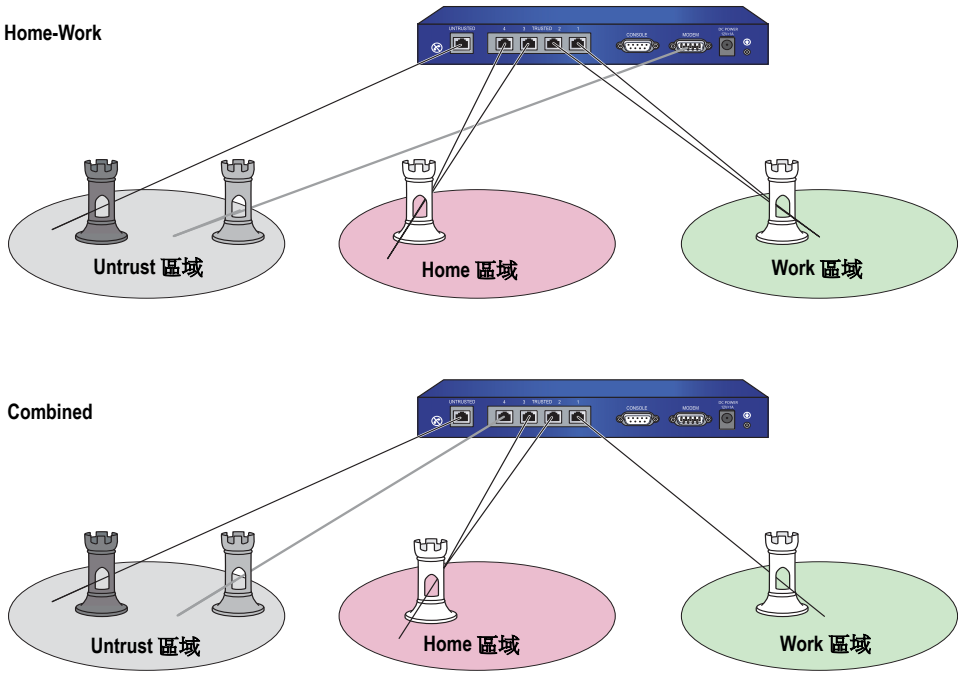
get system

Home-Work 與 Combined 連接埠模式的區域

遠距通勤員工及家庭網路益發普及均會導致安全性衝突發生。由遠距通勤者及其家庭成員所使用的家庭網路對於公司網路來說可能會造成一個危險的後門，其攜帶如病毒及破壞程式的威脅，及允許非員工存取如伺服器及網路等公司資源。

Home-Work 與 Combined 連接埠模式會將 ScreenOS 介面連結到特殊的 Work 與 Home 區域。如此即可分離商務及住家使用者與資源，而又讓 Home 與 Work 區域的使用者可以存取 Untrust 區域。請參閱第 40 頁上的圖 28。

圖 28: Home-Work 及 Combined 連接埠模式區域連結



Home-Work 連接埠模式亦會將「數據機」連接埠連結到序列介面，您可將該之作爲備份介面連結至 Untrust 安全區。如需有關使用作爲備份介面連結至 Untrust 安全區的序列介面詳細資訊，請參閱*第 11 卷：高可用性*。

Combined 連接埠模式也會使乙太網路連接埠 4 連結至 Untrust 區域，以備份 Untrust 安全連接埠。備份介面僅在 Untrust 區域的主要介面故障時才予以使用。如需有關使用作爲備份介面連結至 Untrust 安全區的 ethernet3 介面詳細資訊，請參閱*第 11 卷：高可用性*。

依預設，NetScreen-5XT 作爲「動態主機組態通訊協定」(DHCP) 伺服器，將 IP 位址配置至 Work 區域的 DHCP 用戶端。(如需詳細資訊，請參閱第 220 頁上的「將安全性裝置指派爲 DHCP 轉接代理程式」。)

您可以使用 Telnet 連線或 Work 區域的 WebUI 組態裝置。您無法從 Home 區域組態裝置。您無法在 Home 區域介面上使用任何管理服務，包括 Ping。Work 區域介面 (ethernet1) 的預設 IP 位址爲 192.168.1.1/24。

Home-Work 與 Combined 連接埠模式中的預設政策提供下列的區域間通訊流量控制權 :

- 允許所有自 Work 區域至 Untrust 區域的通訊流量
- 允許所有自 Home 區域至 Untrust 區域的通訊流量
- 允許所有自 Work 區域至 Home 區域的通訊流量
- 阻斷所有自 Home 區域至 Work 區域的通訊流量 (您無法移除此政策)

您可以針對自 Work 區域至 Untrust 區域、自 Home 區域至 Untrust 區域及自 Work 區域至 Home 區域的通訊流量建立新政策。您亦可移除允許所有自 Work 區域至 Untrust 區域、自 Home 區域至 Untrust 區域及自 Work 區域至 Home 區域的通訊流量的預設政策。

範例 : Home-Work 區域

在本範例中，您執行下列動作 :

1. 設定 home-work 連接埠模式。
2. 設定政策，以僅允許從 Home 區域通往 Untrust 區域的 FTP。
3. 刪除允許所有從 Home 區域通往 Untrust 區域的通訊流量的預設政策。
4. 取消設定政策 ID 2，其允許所有從任何來源位址通往任何目的地位址進行任何服務的通訊流量。



警告 : 變更連接埠模式會移除裝置上任何現有的組態，並需進行系統重設。

WebUI

Configuration > Port Mode > Port Mode: 從下拉式清單中選擇 Home-Work，然後按一下 **Apply**。

在下列提示中按一下 **OK**:

Operational mode change will erase current configuration and reset the device, continue?

此時，系統會重新開機。登入系統，然後執行下列操作 :

Policies > (From: Home, To: Untrust) > New: 輸入下面的內容，然後按一下 **OK**。

Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Any
Service: FTP
Action: Permit

政策 : 在 "From Home to Untrust" 政策清單中，按一下政策 (**ID 2**) 組態欄中的 **Remove**。

CLI

```
exec port-mode home-work
```

在下列提示中輸入 **y** (表示是):

Change port mode from *trust-untrust* to *home-work* will erase system configuration and reboot box

Are you sure y/[n] ?

```
set policy from home to untrust any any ftp permit
unset policy 2
save
```

第 3 章
介面

實體介面和子介面讓通訊流量可以進出安全區。若要讓網路通訊流量能流入和流出安全區，您必須將介面連結到該區域，如果是第 3 層區域，指派此區域的 IP 位址。然後，您必須組態允許通訊流量在區域之間從介面傳遞至介面的政策。可將多個介面指派給一個區域，但是不可將單一介面指派給多個區域。

本章包括下列各節 :

- 本頁上的「介面類型」
- 第 49 頁上的「檢視介面」
- 第 50 頁上的「設定安全區介面」
- 第 55 頁上的「建立次要 IP 位址」
- 第 56 頁上的「回傳介面」
- 第 58 頁上的「介面狀態變更」

介面類型

本節說明安全區、功能區及通道介面。如需檢視所有這些介面表格的資訊，請參閱第 49 頁上的「檢視介面」。

安全區介面

實體介面和子介面的目的是提供開口，讓網路通訊流量通過以便在區域之間流動。

實體介面

安全性裝置上的每個連接埠都代表一個實體介面，介面名稱爲預先定義的。實體介面的名稱由媒體類型、插槽編號 (對於某些裝置) 及連接埠號碼組成，例如，*ethernet3/2* 或 *ethernet2*（請同時參閱第 3 頁上的「安全區介面」）。您可以將實體介面連結到作爲入口的任何安全區，通訊流量通過入口以進出區域。沒有介面的話，通訊流量就無法進入或離開區域。

在支援對「介面至區域連結」進行變更的安全性裝置上，三個實體乙太網路介面預先連結到特定的第 2 層安全區 - V1-Trust、V1-Untrust 和 V1-DMZ。介面連結到的區域根據每個平台而有不同。(如需安全區的詳細資訊，請參閱第 2 頁上的「安全區」。)

子介面

子介面與實體介面相似，作爲通訊流量進出安全區的開口。邏輯上，可將實體介面分成數個虛擬子介面。每個虛擬子介面都從其主幹實體介面借用需要的頻寬，因此它的名稱是實體介面名稱的擴充，例如，*ethernet3/2.1* 或 *ethernet2.1* (請參閱第 3 頁上的「安全區介面」)。

可以將子介面連結到任何區域。也可以將子介面連結到和其實體介面相同的區域，或將其連結到不同的區域。(如需詳細資訊，請參閱第 51 頁上的「將介面連結到安全區」。)

聚集介面

NetScreen-5000 系列支援聚集介面。聚集介面是兩個或更多實體介面的聚集，它們平均分擔流向聚集介面 IP 位址的通訊流量負載。透過使用聚集介面，可以增加單一 IP 位址可用的頻寬量。此外，若聚集介面中的一個成員發生故障，其他成員仍可繼續處理通訊流量，雖然可用的頻寬量較先前少。

注意： 如需聚集介面的詳細資訊，請參閱第 **11**-39 頁上的「介面冗餘」。

冗餘介面

可以將兩個實體介面連結在一起以建立一個冗餘介面，然後再連結到安全區。兩個實體介面的其中一個作爲主要介面，並處理流向冗餘介面的所有通訊流量。另一個實體介面則作爲次要介面以及活動介面故障時的備用介面。如果發生故障，流向冗餘介面的通訊流量會切換至次要介面，該介面也就成爲新的主要介面。使用冗餘介面提供了升級到裝置級故障後移轉前的第一線冗餘。

注意： 如需冗餘介面的詳細資訊，請參閱第 **11**-39 頁上的「介面冗餘」。

虛擬安全性介面

虛擬安全性介面 (VSI) 是在 HA 模式中執行時，兩個安全性裝置形成的虛擬安全性裝置 (VSD) 共享的虛擬介面。網路和 VPN 通訊流量使用 VSI 的 IP 位址和虛擬 MAC 位址。然後，VSD 將通訊流量對應到之前已將該 VSI 連結到其上的實體介面、子介面或冗餘介面。兩個安全性裝置在 HA 模式中操作時，您必須將要在裝置發生故障後移轉時提供不間斷服務的安全區介面連結到一個或多個虛擬安全性裝置 (VSD)。將介面連結到 VSD 後，就有虛擬安全性介面 (VSI)。

注意： 如需 VSI 及其如何與 HA 叢集中 VSD 一起使用的詳細資訊，請參閱*第 11 卷：高可用性*。

功能區介面

功能區介面，如「管理」和 HA，皆有特殊的目的。

管理介面

在一些安全性裝置上，可以透過專用的實體介面 (管理 (MGT) 介面) 來移動一般網路使用者介面外部的管理通訊流量。從網路使用者通訊流量分離管理式通訊流量會大大增加安全性，並確保穩定的管理頻寬。

注意 : 如需組態管理裝置的資訊，請參閱第 **3**-1 頁上的「管理」。

高可用性介面

高可用性 (HA) 介面是專用於 HA 功能的實體連接埠。使用具有專用 HA 介面的安全性裝置，您可以將兩個裝置連結在一起，形成冗餘群組 (或稱爲叢集)。在冗餘群組中，一個裝置充當主裝置，執行網路防火牆、VPN 和通訊流量整理功能，而另一個裝置充當備份裝置，在主裝置發生故障時接手防火牆功能。這是一個主動 / 被動組態。也可以將叢集的兩個成員都設定爲彼此的主裝置和備份裝置。這是一個雙重主動組態。這兩種組態在*第 11 卷 : 高可用性*中都有完整的解釋。

虛擬 HA 介面

在沒有專用 HA 介面的安全性裝置上，虛擬 HA 介面提供相同的功能。由於沒有 HA 通訊流量專屬的獨立實體連接埠，因此必須將虛擬 HA 介面連結到一個實體乙太網路連接埠。使用與將網路介面連結到安全區相同的程序，將網路介面連結到 HA 區域 (請參閱第 51 頁上的「將介面連結到安全區」)。

注意 : 如需 HA 介面的詳細資訊，請參閱第 **11**-26 頁上的「雙重高可用性介面」。

通道介面

通道介面作爲 VPN 通道的入口。通訊流量透過通道介面進出 VPN 通道。

當您將通道介面連結到 VPN 通道時，您即可在通往特定目的地的路由中參考該通道介面，然後在一個或多個政策中參考該目的地。您可以利用這個方法精確控制通過通道的通訊流量。其亦支援 VPN 通訊流量的動態路由。如果沒有通道介面連結到 VPN 通道，必須在政策中指定通道並選擇 **tunnel** 作爲動作。因爲操作 **tunnel** 暗示允許，所以不能明確拒絕來自 VPN 通道的通訊流量。

您可以使用在通道介面的相同子網路中的動態 IP (DIP) 位址集區對向外或內向通訊流量執行以政策爲基礎的 NAT。對通道介面使用以政策爲基礎的 NAT 的主要原因是爲了避免 IP 位址在 VPN 通道終點的兩個站台之間發生衝突。

您必須將路由式的 VPN 通道連結到通道介面，如此安全性裝置才能路由往返裝置的通訊流量。您可將路由式的 VPN 通道連結到已編號 (含 IP 位址 / 網路遮罩) 或未編號 (無 IP 位址 / 網路遮罩) 的通道介面。若通道介面當未編號，您必須指定通道介面 IP 位址供用來源的介面。當安全性裝置自行初始化通道中的通訊流量 (如 OSPF 訊息) 時，安全性裝置僅會使用借用的 IP 位址作爲來源位址。只要兩個區域位在相同的路由網路內，通道介面即可借用相同 / 不同安全區域的介面位址。

將所有未編號的通道介面連結到一個區域內 (於其自身的虛擬路由網域內)，並從連結到相同區域的回傳介面借用 IP 位址，您即可達到相當安全的 VPN 通訊流量控制。例如，您可以將所有未編號的通道介面連結到名爲 "VPN" 的使用者定義區域，然後將之組態爲從 loopback.1 介面 (亦連結到 VPN 區域) 借用 IP 位址。VPN 區域位在名爲 "vpn-vr" 的使用者定義路由網域內。將所有通道通往方向的目的地位址放置在 VPN 區域中。通往這些位址的路由指向通道介面，政策則控制其他區與 VPN 區域之間的 VPN 通訊流量。請參閱第 46 頁上的圖 29。

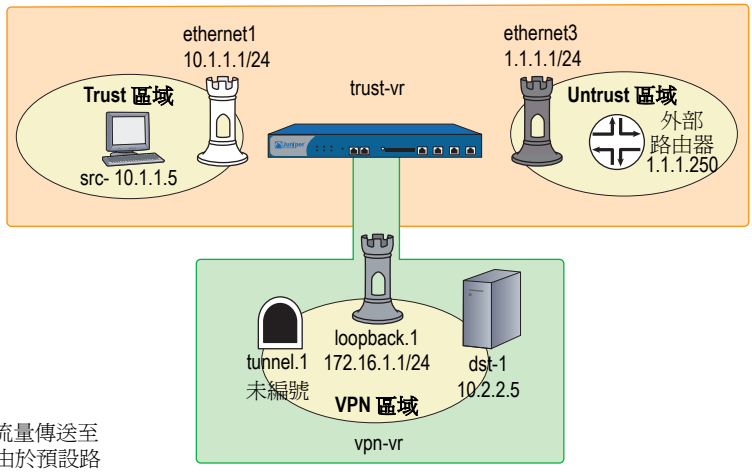
圖 29: 未編號的通道介面連結

```
set vrouter name vpn-vr
set zone name vpn vrouter vpn-vr
set interface loopback.1 zone vpn
set interface loopback.1 ip 172.16.1.1/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip unnumbered loopback.1

組態 src-1 與 dst-1 的位址。
組態 VPN 通道，並將之連結至 tunnel.1。

set vrouter trust-vr route 10.2.2.5/32 vrouter vpn-vr
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
      gateway 1.1.1.250
set vrouter vpn-vr route 10.2.2.5 interface tunnel.1

set policy from trust to vpn scr-1 dst-1 any permit
```



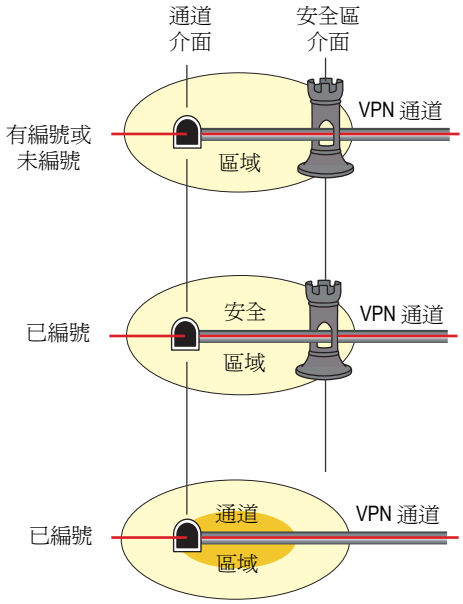
安全性裝置從 trust-vr 將指定給 10.2.2.5/32 的通訊流量傳送至 vpn-vr。若 tunnel.1 已停用，裝置即會卸除封包。由於預設路由 (至 0.0.0.0/0) 僅存在於 trust-vr 中，因此裝置不會嘗試將純文字格式的封包傳出 ethernet3。

把所有的通道介面放置在這樣的區域內是很安全的，因爲 VPN 不會因爲發生故障 (會導致通往相關通道介面的路由變成非活動狀態) 而重新定向原本要讓通道得以使用未開啓通道路由 (如預設路由) 的通訊流量。(若需有關避免發生這類問題的幾個建議，請參閱第 5-64 頁上的「以路由爲基礎的虛擬私人網路安全性考量」。)

您亦可將一個通道介面連結到通道區。執行上述動作後，該通道介面必定具有一個 IP 位址。將通道介面連結到通道區的用意是讓以政策爲基礎的 VPN 通道能使用 NAT 服務。請參閱第 47 頁上的圖 30。

注意 : 網路位址轉譯 (NAT) 服務包括動態 IP (DIP) 集區，以及在相同子網路中定義爲介面的對應 IP (MIP) 位址。

圖 30: 通道介面與區域連結



當通道介面在某安全區內時，必須將一個 VPN 通道連結到該通道介面。這樣您就可以建立以路由爲基礎的 VPN 組態。通道介面有無編號均可。如果通道介面沒有編號，它會從您在其中建立該介面的安全區預設介面借用 IP 位址。

注意 : 只有具 IP 位址和網路遮罩的通道介面才支援以政策爲基礎的的 NAT。

當有編號的通道介面在安全區內而且是該區域內唯一的介面時，就不需要建立安全區介面。在這種情況下，安全區支援透過通道介面的 VPN 通訊流量，但不支援其他類型的通訊流量。

當通道介面連結到通道區時，則通道介面必定具有 IP 位址和網路遮罩。這樣您就可以在該介面上定義 DIP 集區與 MIP 位址。如果您將 VPN 通道連結到通道區，您不能也將 VPN 通道連結到通道介面。在這種情況下，必須建立以政策爲基礎的 VPN 組態。

就概念而言，可將 VPN 通道視爲鋪設好的導線。它們從本機裝置延伸到遠端閘道，而通道介面就是這些導線的開口。導線一直存在，只要路由設定引擎將通訊流量引導到其中一個介面，就可隨時使用它們。

一般來說，若您希望介面支援一個或多個動態 IP (DIP) 以進行來源位址轉譯 (NAT-src)，及用於目的地位址轉譯 (NAT-src) 的對應 IP (MIP)，請將 IP 位址指派至通道介面。如需 VPN 和位址轉譯的詳細資訊，請參閱第 5-129 頁上的「具有重疊位址的 VPN 站台」。您可以於安全區或通道區內建立具 IP 位址及網路遮罩的通道介面。

如果通道介面不需要支援位址轉譯，並且組態不要求通道介面連結到通道區，可以將介面指定爲沒有編號。必須將沒有編號的通道介面連結到安全區；不能將其連結到通道區。您亦需指定一個介面，此介面 IP 位址與所連結的未編號介面位在與安全區相同的虛擬路由網域中。無編號的通道介面從該介面借用 IP 位址。

注意 : 如需顯示如何將通道介面連結到通道的範例，請參閱 第 5-71 頁上的「站台對站台的虛擬私人網路」 與 第 5-147 頁上的「撥接虛擬私人網路」 中以路由爲基礎的 VPN 範例。

如果您要透過 VPN 通道傳輸多點傳送封包，可啓用通道介面上的通用路由封裝 (Generic Routing Encapsulation，GRE) 將多點傳送封包封裝在單點傳送封包中。Juniper Networks 安全性裝置支援可將 IP 封包封裝在 IPv4 單點傳送封包中的 GREv1。如需有關 GRE 的附加資訊，請參閱第 **7**-118 頁上的「在通道介面上組態通用路由設定封裝」。

刪除通道介面

不能立即刪除代管對應 IP 位址 (MIP) 或動態 IP (DIP) 位址集區的通道介面。刪除代管任一這些功能的通道介面前，必須先刪除參考這些功能的所有政策。然後必須刪除通道介面上的 MIP 和 DIP 集區。同樣，如果以路由爲基礎的 VPN 組態參考通道介面，必須先刪除 VPN 組態，然後才能刪除通道介面。

在本範例中，通道介面 tunnel.2 連結到 DIP 集區 8。DIP 集區 8 則被一政策 (ID 10) (用於經由名爲 vpn1 的 VPN 通道，從 Trust 區域流向 Untrust 區域的 VPN 通訊流量) 參考。若要移除通道介面，必須先刪除政策 (或從政策中移除到 DIP 集區 8 參考)，然後依序移除 DIP 集區。然後您必須將 tunnel.2 從 vpn1 解除連結。移除所有依據通道介面的組態後，即可刪除該通道介面。

WebUI

1. **刪除參考 DIP 集區 8 的政策 10**
   Policies (From: Trust, To: Untrust): 爲政策 ID 10 按一下 **Remove**。

2. **刪除連結到 tunnel.2 的 DIP 集區 8**
   Network > Interfaces > Edit (對於 tunnel.2) > DIP: 爲 DIP ID 8 按一下 **Remove**。

3. **從 vpn1 解除連結 tunnel.2**
   VPNs > AutoKey IKE > Edit (對於 vpn1) > Advanced: 選擇 Bind to: Tunnel Interface 下拉式清單中的 **None**，按一下 **Return**，然後再按一下 **OK**。

4. **刪除 tunnel.2**
   Network > Interfaces: 爲 tunnel.2 按一下 **Remove**。

CLI

1. **刪除參考 DIP 集區 8 的政策 10**
   unset policy 10

2. **刪除連結到 tunnel.2 的 DIP 集區 8**
   unset interface tunnel.2 dip 8

3. **從 vpn1 解除連結 tunnel.2**
   unset vpn vpn1 bind interface

4. **刪除 tunnel.2**
   unset interface tunnel.2
   save

檢視介面

您可以檢視列出安全性裝置上所有介面的表格。因爲實體介面是預先定義的，所以不管有沒有組態都會列出來。對於子介面和通道介面，只有在建立和組態後才會列出。

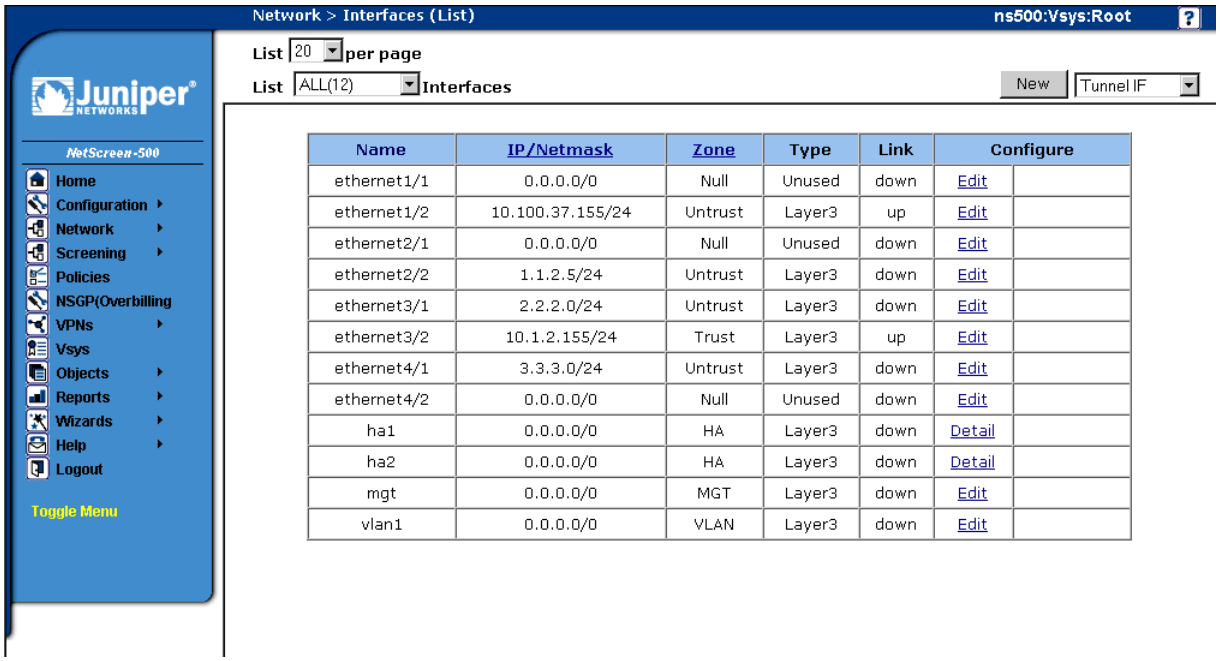
若要在 WebUI 中檢視介面表，請按一下 **Network > Interfaces**。可指定要在 List Interfaces 下拉式功能表中顯示的介面類型。

若要在 CLI 中檢視介面表，請使用 **get interface** 指令。

介面表顯示每個介面的下列資訊 :

- **Name:** 此欄位識別介面的名稱。
- **IP/Netmask:** 此欄位識別介面的 IP 位址和網路遮罩位址。
- **Zone:** 此欄位識別介面連結到的區域。
- **Type:** 此欄位指出介面類型: Layer 2 (第 2 層)、Layer 3 (第 3 層)、tunnel (通道)、redundant (冗餘)、aggregate (聚集)、VSI。
- **Link:** 此欄位識別介面是否爲活動 (啓動) 或非活動 (中斷)。
- **Configure:** 此欄位讓您可以修改或移除介面。

圖 31: WebUI 介面表



Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet1/2	10.100.37.155/24	Untrust	Layer3	up	Edit	
ethernet2/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet2/2	1.1.2.5/24	Untrust	Layer3	down	Edit	
ethernet3/1	2.2.2.0/24	Untrust	Layer3	down	Edit	
ethernet3/2	10.1.2.155/24	Trust	Layer3	up	Edit	
ethernet4/1	3.3.3.0/24	Untrust	Layer3	down	Edit	
ethernet4/2	0.0.0.0/0	Null	Unused	down	Edit	
ha1	0.0.0.0/0	HA	Layer3	down	Detail	
ha2	0.0.0.0/0	HA	Layer3	down	Detail	
mgt	0.0.0.0/0	MGT	Layer3	down	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	down	Edit	

圖 32: CLI 介面表

```
ns500-> get interface

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name           IP Address          Zone         MAC              VLAN State VSD Vsys
eth1/1         0.0.0.0/0           Null         0010.db0d.4ddc     -   D   -   Root
eth1/2         10.100.37.155/24    Untrust      0010.db0d.4dde     -   U   -   Root
eth2/1         0.0.0.0/0           Null         0010.db0d.4ddb     -   D   -   Root
eth2/2         1.1.2.5/24          Untrust      0010.db0d.4ddd     -   D   -   Root
eth3/1         2.2.2.0/24          Untrust      0010.db0d.4dd8     -   D   -   Root
eth3/2         10.1.2.155/24       Trust        0010.db0d.4dda     -   U   -   Root
eth4/1         3.3.3.0/24          Untrust      0010.db0d.4dd7     -   D   -   Root
eth4/2         0.0.0.0/0           Null         0010.db0d.4dd9     -   D   -   Root
mgt            0.0.0.0/0           MGT          0010.db0d.4dd0     -   D   -   Root
ha1            0.0.0.0/0           HA           0010.db0d.4dd5     -   D   -   Root
ha2            0.0.0.0/0           HA           0010.db0d.4dd6     -   D   -   Root
vlan1          0.0.0.0/0           VLAN         0010.db0d.4ddf     1   D   -   Root
null           0.0.0.0/0           Null         0010.dbff.0100     -   U   0   Root
ns500->
```

設定安全區介面

本節說明如何設定安全區介面的下列方面 :

- 將介面連結到安全區及解除連結
- 將位址指派給 Layer 3 (第 3 層) 安全區介面
- 修改實體介面和子介面
- 建立子介面
- 刪除子介面

注意 : 如需爲介面設定通訊流量頻寬的資訊，請參閱第 183 頁上的「通訊流量整理」。如需每種介面可用的管理及其他可用服務選項的詳細資訊，請參閱第 3-22 頁上的「控制管理式通訊流量」。

將介面連結到安全區

您可以將任何實體介面連結到 L2 (第 2 層) 或 L3 (第 3 層) 安全區。由於子介面需要 IP 位址，因此僅可將子介面連結到 L3 (第 3 層) 安全區。將介面繫結到 L3 安全區後，才能將 IP 位址指派給介面。

在本範例中，將 ethernet5 連結到 Trust 區域。

WebUI

Network > Interfaces > Edit (對於 ethernet5): 從 Zone Name 下拉式清單中選擇 **Trust**，然後按一下 **OK**。

CLI

```
set interface ethernet5 zone trust
save
```

從安全區解除介面連結

如果介面沒有編號，您可以解除其到一個安全區的連結，然後連結到另一個安全區。如果介面已編號，必須先將其 IP 位址和網路遮罩設定爲 0.0.0.0。然後，可以解除其到一個安全區的連結，然後連結到另一個安全區，並 (選擇性地) 爲它重新指派 IP 位址 / 網路遮罩。

在本範例中，ethernet3 的 IP 位址爲 210.1.1.1/24，並連結到 Untrust 區域。將其 IP 位址和網路遮罩設定爲 0.0.0.0/0 並連結到 Null 區域。

WebUI

Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

Zone Name: Null
IP Address/Netmask: 0.0.0.0/0

CLI

```
set interface ethernet3 ip 0.0.0.0/0
set interface ethernet3 zone null
save
```

爲 L3 安全區介面定址

定義第 3 層 (L3) 安全區介面或子介面時，必須爲其指派 IP 位址和網路遮罩。如果將介面連結到 trust-vr 中的區域，您也可以指定介面模式爲 NAT 或「路由」。(如果將介面連結到的區域在 untrust-vr 中，介面模式一定爲「路由」。)

注意 : 如需 NAT 和「路由」模式組態的範例，請參閱第 77 頁上的「介面模式」。

進行介面位址指派時，要考量下列兩種基本類型的 IP 位址 :

- 公開位址，由網際網路服務提供商 (ISP) 提供的位址，用於公用網絡 (如網際網路) 並且必須是唯一的
- 私人位址，由本機網路管理員指派，用於私人網路並且其他管理員也可指派用於其私人網路

注意 : 當您將 IP 位址新增至介面時，安全性裝置會透過 ARP 要求進行檢查，以確保該 IP 位址不存在於本機網路中。(此時實體連結必須爲工作中的狀態。) 若 IP 位址已存在，則會顯示警告。

公開 IP 位址

連接到公開網路的介面必須有公開 IP 位址。同樣，如果 untrust-vr 中的第 3 層安全區連接到公開網路，並且 trust-vr 中區域的介面模式爲「路由」，那麼 trust-vr 的區域中所有位址 (包括介面和主機的位址) 也必須爲公開位址。公開 IP 位址分成三類，A、B 和 C，如表 11 中所示 :

表 11: 公開位址範圍

位址類別	位址範圍	排除的位址範圍
A	0.0.0.0 - 127.255.255.255	10.0.0.0 - 10.255.255.255, 127.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255	172.16.0.0 - 172.31.255.255
C	192.0.0.0 - 223.255.255.255	192.168.0.0 - 192.168.255.255

注意 : 也有 D 和 E 類位址，保留給特殊目的。

IP 位址由四個八位元組組成，每個八位元組長爲 8 位元。在 A 類位址中，前 8 個位元表示網路 ID，後 24 個位元表示主機 ID (nnn.hhh.hhh.hhh)。在 B 類位址中，前 16 個位元表示網路 ID，後 16 個位元表示主機 ID (nnn.nnn.hhh.hhh)。在 C 類位址中，前 24 個位元表示網路 ID，後 8 個位元表示主機 ID (nnn.nnn.nnn.hhh)。

透過套用子網路遮罩 (或網路遮罩)，可進一步劃分網路。實際上，網路遮罩掩蔽了主機 ID 的一部分，以便使遮罩的部分成爲網路 ID 的子網路。例如，位址 10.2.3.4/24 中的 24 位元遮罩指出，前 8 個位元 (即第一個 8 位元組 - 010) 識別此私人類別 A 位址的網路部份，下一個 16 位元 (即第二與第三個 8 位元組 - 002.003) 則識別位址的子網路部份，而最後的 8 位元 (最後的 8 位元組 - 004) 則識別位址的主機部份。使用子網路可將大的網路位址空間縮小爲較小的子部門，大幅增強了 IP 資料電報的傳輸效率。

注意 : 24 位元遮罩的十進位小數點格式等值爲 255.255.255.0。

私人 IP 位址

如果將介面連接到私人網路，那麼本機網路管理員可爲其指派任何位址，雖然通常是使用私人位址保留範圍中的位址 - 10.0.0.0/8, 172.16.0.0 - 172.31.255.255, 192.168.0.0/16 - 如 RFC 1918，*Address Allocation for Private Internets* 中所定義。

如果 untrust-vr 中的第 3 層安全區連接到公開網路，並且 trust-vr 中區域連結的介面模式爲 NAT，那麼 trust-vr 的區域中所有位址 (包括介面和主機的位址) 也可以是私人位址。

編址介面

在本範例中，您爲 ethernet5 指派 IP 位址 210.1.1.1/24、「管理 IP」位址 210.1.1.5。(請注意，「管理 IP」位址必須和安全區介面 IP 位址在相同的子網路中。) 最後，在 NAT 模式中設定介面，將所有內部 IP 位址轉譯至連結到其他安全區的預設介面。

注意 : 安全區的預設介面是連結到區域的第一個介面。若要知道哪一個介面是區域的預設介面，請檢視 WebUI 上 Network > Zones 頁中的 Default IF 欄，或在 CLI 中檢視 **get zone** 指令輸出內容中的 Default-If 欄。

WebUI

Network > Interfaces > Edit (對於 ethernet5): 輸入下面的內容，然後按一下 **OK**:

```
IP Address/Netmask: 210.1.1.1/24
Manage IP: 210.1.1.5
```

CLI

```
set interface ethernet5 ip 210.1.1.1/24
set interface ethernet5 manage-ip 210.1.1.5
save
```

修改介面設定

設定實體介面、子介面、冗餘介面、聚集介面或「虛擬安全性介面」(VSI) 後，如有需要可以變更下列任何設定 :

- IP 位址和網路遮罩
- 管理 IP 位址
- (L3 區域介面) 管理和網路服務。
- (子介面) 子介面 ID 編號和 VLAN 標籤編號。
- (trust-vr 中連結到 Layer (第 3 層) 安全區的介面) 介面模式 - NAT 或「路由」。
- (實體介面) 通訊流量頻寬設定 (請參閱第 183 頁上的「通訊流量整理」)。
- (實體、冗餘與聚集介面) 最大傳輸單位 (MTU) 大小。
- (L3 介面) 阻斷進出相同介面的通訊流量，包括主、次要子網路之間或次要子網路之間的通訊流量 (您可利用含 **route-deny** 選項的 CLI **set interface** 指令執行這項作業)。

您可強迫某些安全性裝置上實體介面的實體連結狀態處於不在工作中或工作中狀態。若將實體連結狀態強制成爲不在工作中狀態，您即可從介面連接埠促使纜線中斷。(您可利用含 **phy link-down** 選項的 CLI **set interface** 指令執行上述作業。)

在本範例中，對 ethernet1 進行一些修改，這個介面連結到 Trust 區域。將「管理 IP」位址從 10.1.1.2 變更爲 10.1.1.12。爲了強制更高的管理通訊流量安全性，還變更管理服務選項，啓用 SCS 和 SSL 並停用 Telnet 和 WebUI。

WebUI

Network > Interfaces > Edit (對於 ethernet1): 進行下面的修改，然後按一下 **OK**:

Manage IP: 10.1.1.12
Management Services: (選擇) SSH, SSL; (清除) Telnet, WebUI

CLI

```
set interface ethernet1 manage-ip 10.1.1.12
set interface ethernet1 manage ssh
set interface ethernet1 manage ssl
unset interface ethernet1 manage telnet
unset interface ethernet1 manage web
save
```

在根系統中建立子介面

您可以在根系統或虛擬系統中的任何實體介面上建立子介面。子介面利用 VLAN 標籤區別連結到自己的通訊流量與連結到其他介面的通訊流量。請注意，雖然子介面從實體介面中分支，並借用其需要的頻寬，但是您可以將子介面連結到任何區域，不必連結到其「父代」介面連結到的區域。此外，子介面的 IP 位址所在的子網路必須和所有其他實體介面和子介面的 IP 位址不同。

注意 : 您也可以組態冗餘子介面和 VSI 上的子介面。如需在冗餘介面上組態子介面的範例，請參閱第 **11**-86 頁上的「虛擬系統故障後移轉」。

在本範例中，您會在根系統中建立 Trust 區域的子介面。在連結到 Trust 區域的 ethernet1 上組態子介面。將子介面連結到使用者定義的區域，名爲 "accounting" (在 trust-vr 中)。爲其指派子介面 ID 3、IP 位址 10.2.1.1/24 和 VLAN 標籤 ID 3。介面模式爲 NAT。

WebUI

Network > Interfaces > New Sub-IF: 輸入下面的內容，然後按一下 **OK**:

Interface Name: ethernet1.3
Zone Name: accounting
IP Address/Netmask: 10.2.1.1/24
VLAN Tag: 3

CLI

```
set interface ethernet1.3 zone accounting
set interface ethernet1.3 ip 10.2.1.1/24 tag 3
save
```

刪除子介面

您不能立即刪除代管對應的 IP 位址 (MIP)、虛擬 IP 位址 (VIP) 或「動態 IP」(DIP) 位址集區的子介面。刪除代管這些功能的子介面前，必須先刪除參考功能的所有政策或 IKE 閘道。然後必須刪除子介面上的 MIP、VIP 和 DIP 集區。

在本範例中，您刪除子介面 ethernet1:1。

WebUI

Network > Interfaces: 按一下 **Remove** (對於 ethernet1:1)。

系統訊息會提示您確認移除操作。

按一下 **Yes** 刪除子介面。

CLI

```
unset interface ethernet1:1
save
```

建立次要 IP 位址

每個 ScreenOS 介面都有一個唯一的*主要* IP 位址。但是，在某些情況下，介面需要有多個 IP 位址。例如，組織可能指派額外的 IP 位址，但不希望新增路由器來適應其需要。此外，組織擁有的網路裝置可能超過其子網路所能處理的範圍，如有多於 254 台的主機連接到 LAN。若要解決這樣的問題，您可以將*次要* IP 位址新增到 Trust、DMZ 或使用者定義區域中的介面。

注意 : 您不能爲 Untrust 區域中的介面設定多個次要 IP 位址。

次要位址具有某些屬性，會影響您執行此類位址的方法。這些屬性如下 :

- 任何兩個次要 IP 位址之間不能有子網路位址重疊。此外，安全性裝置上的次要 IP 和任何現有子網路之間不能有子網路位址重疊。
- 透過次要 IP 位址管理安全性裝置時，位址一定和主 IP 位址有相同的管理屬性。因此，您不能爲次要 IP 位址指定獨立的管理組態。
- 您不能爲次要 IP 位址組態閘道。
- 建立新的次要 IP 位址時，安全性裝置會自動建立相應的路由設定表項目。刪除次要 IP 位址時，裝置會自動刪除其路由設定表項目。

啓用或停用兩個次要 IP 位址之間的路由設定不會在路由設定表中導致變更。例如，如果停用兩個此類位址之間的路由設定，安全性裝置會卸除從一個介面導向到另一個介面的任何封包，但是路由設定表則沒有變更。

在本範例中，您爲 ethernet1 設定次要 IP 位址 - 192.168.2.1/24，介面 ethernet1 的 IP 位址爲 10.1.1.1/24 並連結到 Trust 區域。

WebUI

Network > Interfaces > Edit (對於 ethernet1) > Secondary IP: 輸入下面的內容，然後按一下 **Add**:

IP Address/Netmask: 192.168.2.1/24

CLI

```
set interface ethernet1 ip 192.168.2.1/24 secondary
save
```

回傳介面

回傳介面是一個邏輯介面，其模擬安全性裝置上的實體介面。然而與實體介面不同的是，只要其所在的裝置開啓，則該介面永遠處於工作中的狀態。回傳介面的名稱爲 loopback.*id_num*，其中 *id_num* 是大於或等於 1 的數字，表示裝置上獨特的回傳介面。如同實體介面，您必須將 IP 位址指派至回傳介面，並將之連結到安全區。

注意： 您可指定的最大 *id_num* 值視平台而定。

定義回傳介面後，您即可定義其他介面，以作爲其群組的成員。若通訊流量經由群組中的一個介面抵達，即可到達回傳介面。任何介面類型都可以作爲回傳介面群組的成員 - 實體介面、子介面、通道介面、冗餘介面或 VSI。

建立回傳介面後，您可以利用許多相同的實體介面使用方式來使用它：

- 第 57 頁上的「設定用於管理的回傳介面」
- 第 57 頁上的「設定回傳介面上的 BGP」
- 第 57 頁上的「設定回傳介面上的 VSI」
- 第 58 頁上的「設定回傳介面作爲來源介面」

注意： 您無法將回傳介面連結到 HA 區域，亦不能組態第 2 層操作的回傳介面，或是將回傳介面組態爲冗餘 / 聚集介面。您無法組態下列回傳介面功能：NTP、DNS、VIP、次要 IP、追蹤 IP 或 WebAuth。

您可以定義回傳介面上的 MIP。如此介面群組即可存取 MIP，此爲回傳介面的特殊功能。如需使用具 MIP 之回傳介面的資訊，請參閱 第 8-69 頁上的「MIP 與回傳介面」。

您可以使用回傳介面的 IP 位址或您指派給回傳介面的管理 IP 位址來管理安全性裝置。

建立回傳介面

在下列的範例中，建立回傳介面 loopback.1，將之連結到 Untrust 區域，然後指派 IP 位址 1.1.1.27/24。

WebUI

Network > Interfaces > New Loopback IF: 輸入下面的內容，然後按一下 **OK**:

Interface Name: loopback.1
Zone: Untrust (選擇)
IP Address/Netmask: 1.1.1.27/24

CLI

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.1.27
save
```

注意： 無法從網路或其他區域中的主機直接存取回傳介面。您必須定義政策以允許進出介面的通訊流量。

設定用於管理的回傳介面

在下列範例中，將先前定義的 loopback.1 介面組態爲裝置的管理介面。

WebUI

Network > Interfaces > loopback.1 > Edit: 選擇所有管理選項，然後按一下 **OK**。

CLI

```
set interface loopback.1 manage
save
```

設定回傳介面上的 BGP

回傳介面支援安全性裝置上的 BGP 動態路由通訊協定。在下列範例中，啓用 loopback.1 介面上的 BGP。

注意 : 若要啓用回傳介面上的 BGP，您必須先針對想要連結介面的虛擬路由器建立 BGP 實例。如需有關在 Juniper Networks 安全性裝置上設定 BGP 的資訊，請參閱*第 7 卷 : 路由*。

WebUI

Network > Interfaces > loopback.1 > Edit: 選取 **Protocol BGP**，然後按一下 **OK**。

CLI

```
set interface loopback.1 protocol bgp
save
```

設定回傳介面上的 VSI

您可以在回傳介面上針對 NSRP 組態虛擬安全性介面 (VSI)。回傳介面上的 VSI 實際狀態永遠爲工作中。介面可以是活動中或非活動中狀態，視介面所屬的 VSD 群組狀態而定。

WebUI

Network > Interfaces > New VSI IF: 輸入下面的內容，然後按一下 **OK**:

Interface Name: VSI Base: loopback.1
VSD Group: 1
IP Address/Netmask: 1.1.1.1/24

CLI

```
set interface loopback.1:1 ip 1.1.1.1/24
save
```

設定回傳介面作爲來源介面

您可以使用回傳介面作爲源自安全性裝置某特定通訊流量的來源介面。(當您爲應用程式定義來源介面時，即會使用指定的來源介面位址與外部裝置進行通訊，而不是使用向外介面位址。) 在下列範例中，指定安全性裝置使用先前定義的 loopback.1 介面來傳送系統日誌封包。

WebUI

Configuration > Report Settings > Syslog: 輸入下面的內容，然後按一下 **Apply**:

Enable Syslog Messages: (選擇)
Source Interface: loopback.1 (選擇)
Syslog Servers:
No.: 1 (選擇)
IP/Hostname: 10.1.1.1
Traffic Log: (選擇)
Event Log: (選擇)

CLI

```
set syslog config 10.1.1.1 log all
set syslog src-interface loopback.1
set syslog enable
save
```

介面狀態變更

介面可以爲下列任一狀態 :

- **Physically Up** - 當實體乙太網路介面在開放式系統互相連接 (Open Systems Interconnection，OSI) 模型中的第 2 層 (「透明」模式) 或第 3 層 (「路由」模式) 執行時。當某個介面以纜線連接到另一個網路裝置時，該介面即處於實體工作中狀態，可以建立與該裝置的連結。

- **Logically Up** - 用於實體介面與邏輯介面 (子介面、冗餘介面和聚集介面)。當通訊流量通過某個介面而能夠到達網路上的指定裝置 (位於被追蹤的 IP 位址) 時，就稱該介面處於邏輯工作中狀態。

- **Physically Down** - 如果某個介面沒有以纜線與另一個網路裝置連接，或是雖然以纜線連接，但沒有建立連結，就稱該介面處於實體不工作中狀態。您也可以使用下列 CLI 指令來強制介面成爲實體不工作中狀態 : **set interface interface phy link-down**。

- **Logically Down** - 當通訊流量通過某個介面卻無法到達網路上的指定裝置 (位於被追蹤的 IP 位址) 時，就稱該介面處於邏輯不工作中狀態。

考量介面狀態時，實體狀態的優先順序高於邏輯狀態。介面可在處於實體工作中狀態的同時處在邏輯工作中或邏輯不工作中狀態。如果介面處於實體不工作中狀態，則其邏輯狀態如何就不重要了。

當介面的狀態爲工作中時，則使用該介面的所有路由都會處於活動狀態且可以使用。當介面的狀態爲不工作中時，安全性裝置會停用所有使用該介面的路由，不過，視介面是處於實體不工作中還是邏輯不工作中狀態而定，通訊流量可能仍會通過狀態爲不工作中的介面 (請參閱第 70 頁上的「不工作中介面和通訊流量傳遞」)。爲了彌補因介面停用而無法使用的路由，您可使用備用介面來組態備用路由。

根據您對發現介面狀態有變化時設定要採取的動作而定，被監看的介面上的狀態如果從工作中變成不工作中，可能導致負責監看之介面的狀態從不工作中變成工作中。若要組態此行爲，可以使用下面的 CLI 指令 :

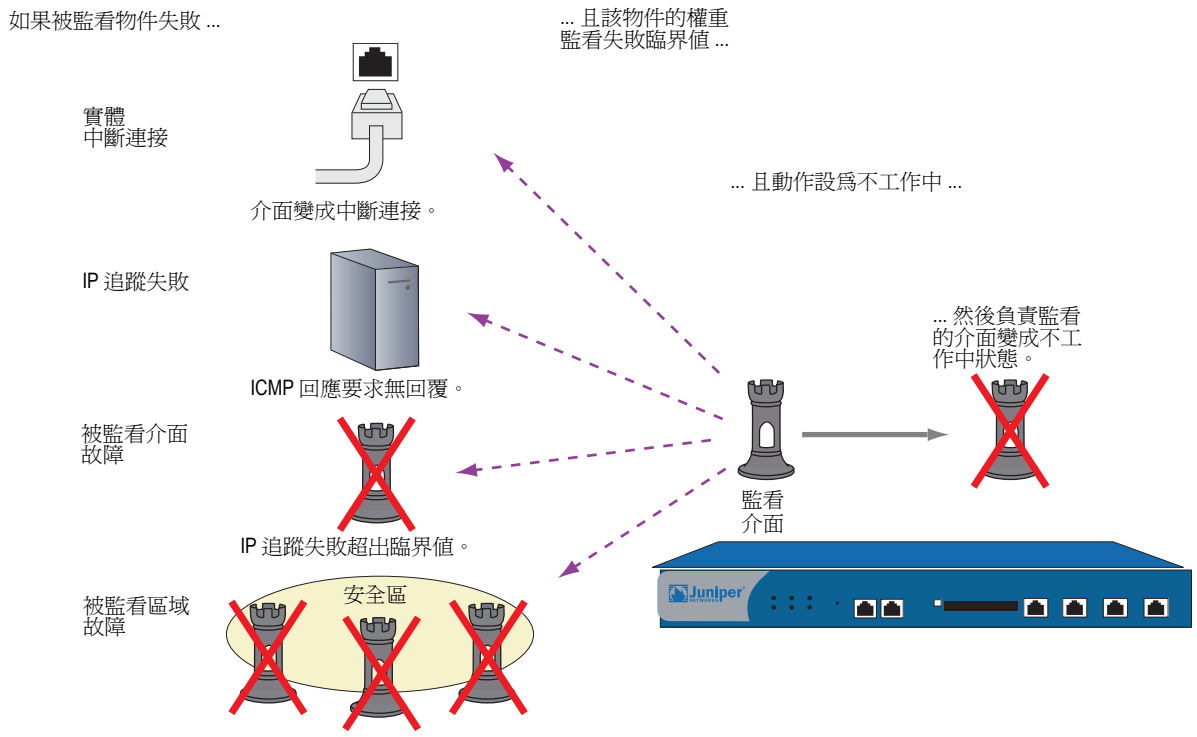
set interface *interface* monitor threshold *number* action up { logically | physically }

當您輸入以上指令時，安全性裝置會自動將負責監看之介面的狀態強制設爲不工作。如果被監看的物件 (被追蹤的 IP 位址、介面、區域) 發生故障，負責監看之介面的狀態會變成工作中，不論您設定的組態爲邏輯工作中還是實體工作中。

介面可監看物件是否發生下列一或多個事件。請參閱第 60 頁上的圖 33。這些事件的任何一種不論是獨自發生還是與其他事件一起發生，都會使負責監看的介面從工作中變成不工作中狀態，以及從不工作中變成工作中狀態 :

- 實體中斷連接 / 重新連接
- IP 追蹤失敗 / 成功
- 被監看介面失敗 / 成功
- 被監看安全區失敗 / 成功

圖 33: 介面狀態監看



如果在失敗後被監看物件成功 (介面重新連接或 IP 追蹤再度成功)，則負責監看的介面又會重新變成工作中狀態。從被監看的物件成功到監看介面重新啓動之間約有一秒的延遲。

下列小節分述以上各個事件。

實體連接監看

安全性裝置上的所有實體介面均監看它們與其他網路裝置之間的實體連接狀態。當介面與其他網路裝置連接並建立連結之後，其狀態將是實體工作中，而使用該介面的所有路由均處於活動狀態。

您可在 **get interface** 指令輸出結果的 State 欄內以及 WebUI 的 Network > Interfaces 頁面中的 Link 欄內檢視介面的狀態。狀態可能是工作中或不工作中。

您可在 **get route id** *number* 指令的 status 欄位內，以及 WebUI 的 Network > Routing > Routing Entries 頁面上檢視路由的狀態。路由如顯示星號，表示其爲活動狀態。如果沒有星號，則路由處於不活動狀態。

追蹤 IP 位址

安全性裝置可透過一個介面追蹤指定的 IP 位址，這樣當其中一或多個位址無法連接時，安全性裝置就可以停用與該介面聯結的所有路由，即使實體連結仍在作用中。當安全性裝置再次與這些 IP 位址連上線後，已停用的路由就會再次啓用。

注意 : 對於某些 ScreenOS 設備而言，此動作也會使故障後移轉至備份介面，此備份介面與組態 IP 追蹤時使用的介面連結在一起 (請參閱第 **11**-48 頁上的「決定介面故障後移轉」)。

類似於 NSRP 中使用的功能，ScreenOS 使用第 3 層路徑監看或進行 *IP 追蹤*，以監看透過介面與指定 IP 位址連接的情況。例如，如果介面直接連接到路由器，則可追蹤介面的下一躍點位址，以確定該路由器是否仍舊可達。當您在介面上組態 IP 追蹤時，安全性裝置會在該介面上以使用者定義的間隔傳送 ping 要求到最多四個目標 IP 位址。安全性裝置會監看是否收到來自這些目標的回應。如果未獲目標回應達到指定的次數，則將該 IP 位址視爲無法連接的位址。如無法取得來自一或多個目標的回應，會導致安全性裝置停用與該介面聯結的路由。如果有另一個通往同樣目的地的路由可用，安全性裝置會重新定向通訊流量，使其使用新的路由。

您可在下列已爲其設定了管理 IP 位址的介面上定義 IP 追蹤 :

- 與安全區 (非 HA 或 MGT 功能區) 連結的實體介面

注意 : 此介面可在第 2 層 (「透明」模式) 或第 3 層 (「路由」模式) 上執行。

- 子介面
- 冗餘介面
- 聚集介面

注意 : 雖然此介面可以是冗餘介面或聚集介面，但不得爲冗餘介面或聚集介面的成員。

在支援虛擬系統的裝置上，您用來設定 IP 追蹤的介面可以屬於根系統，也可以屬於虛擬系統 (virtual system，vsys)。不過，如果要在共享介面上設定 IP 追蹤，則只能在根層級設定。

注意 : 從 vsys 可設定介面監看，從屬於 vsys 的介面來監看共享介面。不過，您無法在 vsys 內設定從共享介面監看介面的功能。如需詳細資訊，請參閱第 65 頁上的「介面監看」。

在任何一種介面上，可以組態最多四個 IP 位址由安全性裝置追蹤。在單一裝置上，最多可組態 64 個追蹤 IP 位址。這個總數包括所有的追蹤 IP 位址，不論是以介面爲基礎的 IP 追蹤，還是以 NSRP 爲基礎的 IP 追蹤，也不論是在根層級還是在 vsys 層級都算在內。

追蹤的 IP 位址不見得要在與介面相同的子網路上。對於每個被追蹤 IP 位址，可指定以下資訊 :

- 將 ping 要求傳送到指定 IP 位址的時間間隔 (以秒爲單位)。
- 經過多少次連續失敗的 ping 嘗試後，認爲到指定 IP 位址的連接失敗。
- 失敗 IP 連接的權重 (所有失敗 IP 連接的權重之和一旦超過指定臨界值，就會停用與該介面聯結的路由)。

您也可以組態安全性裝置，使其追蹤作爲 PPPoE 或 DHCP 用戶端之介面的預設閘道。若要進行此組態，請使用 "Dynamic" 選項：(CLI) **set interface** *interface* **monitor dynamic** 或 (WebUI) Network > Interfaces > Edit（對於 DHCP 或 PPPoE 用戶端介面）> Monitor > Track IP > Add: 選擇 **Dynamic**。

注意： 當您組態要讓安全性裝置追蹤的 IP 位址時，安全性裝置不會將該 IP 位址的主機路由加入至路由設定表中。

組態追蹤 IP 位址時，可使用兩種類型的臨界值：

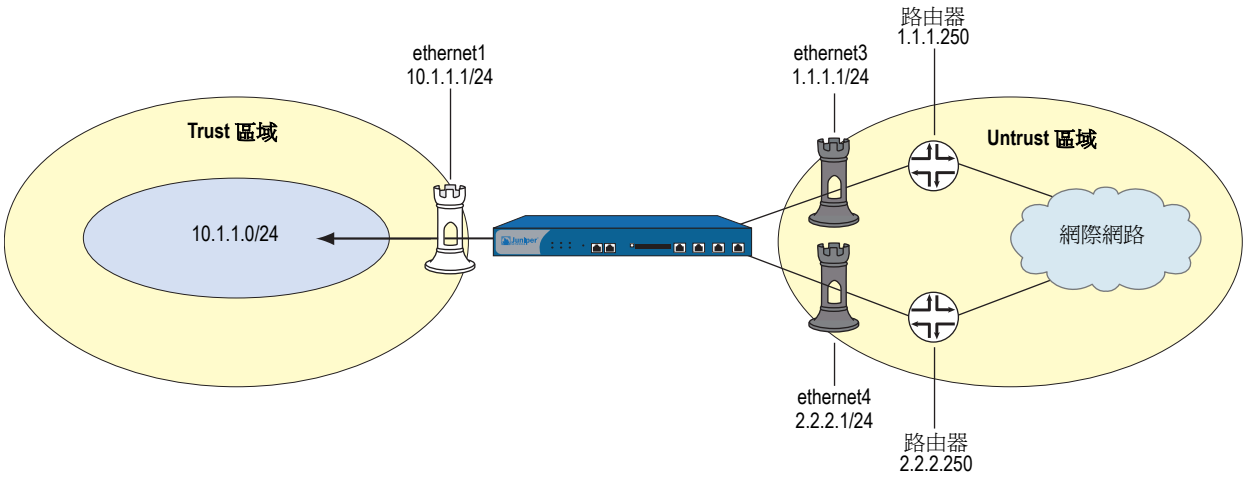
- 特定追蹤 IP 位址的失敗臨界值 - 引發特定 IP 位址發出 ping 回應的連續追蹤失敗次數，這些失敗次數表明與該 IP 位址的連接失敗。不超過臨界值表示可以接受該位址的連接性；超過臨界值則表示一個不可以接受層級。可以將每個 IP 位址的此臨界值設定爲 1 到 200 之間的任意值，預設值爲 3。

- 介面上 IP 追蹤的失敗臨界值 - 嘗試連接介面 IP 位址累計失敗嘗試的總權重，超過該臨界值會導致與該介面聯結的路由停用。可以將此臨界值設定爲 1 到 255 之間的任意值。預設值爲 1，意味著任何嘗試與組態的追蹤 IP 位址連接的失敗都會導致與該介面聯結的路由停用。

透過在被追蹤 IP 位址上套用*權重*或權值，可以調整該位址連接性的重要程度（與其他被追蹤 IP 位址相比）。可以將較大的權重分配給相對重要的位址，將較小的權重分配給相對次要的位址。注意，只有在達到特定追蹤 IP 位址的失敗臨界值時，分配的權重才會起作用。例如，如果某個介面上 IP 追蹤的失敗臨界值爲 3，權重爲 3 的單一追蹤 IP 位址失敗即符合該介面上的 IP 追蹤失敗臨界值，這會導致與該介面聯結的路由停用。權重爲 1 的單一追蹤 IP 位址失敗不符合該介面上的 IP 追蹤失敗臨界值，所以與該介面聯結的路由仍維持作用中狀態。

在下例中，介面 ethernet1 與 Trust 區域連結，並爲其指派了網路位址 10.1.1.1/24。介面 ethernet3 和 ethernet4 與 Untrust 區域連結。將網路位址 1.1.1.1/24 指派給 ethernet3 介面，將 ethernet3 介面與位於 1.1.1.250 的路由器連接。將網路位址 2.2.2.1/24 指派給 ethernet4 介面，將 ethernet4 介面與位於 2.2.2.250 的路由器連接。請參閱圖 34。

圖 34: 介面 IP 追蹤



已組態了兩個預設路由 : 其中一個使用 ethernet3 作爲向外介面，以路由器位址 1.1.1.250 作爲閘道；另一個使用 ethernet4 作爲向外介面，以路由器位址 2.2.2.250 作爲閘道且組態了計量值 10。使用 ethernet3 的預設路由是偏好路由，因爲它的計量值較低 (靜態路由的預設計量值爲 1)。下列 **get route** 指令的輸出結果顯示 trust-vr 的四個作用中路由 (作用中路由以星號標示)。通過 ethernet3 的預設路由處於活動狀態，通過 ethernet4 的預設路由處於非活動狀態，因爲它不是偏好路由。

圖 35: get route 指令輸出

```
ns-> get route
untrust-vr (0 entries)
-------------------------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
-------------------------------------------------------------------------------------------
  ID       IP-Prefix      Interface      Gateway   P Pref   Mtr    Vsys
-------------------------------------------------------------------------------------------
*  4       0.0.0.0/0          eth3     1.1.1.250   S   20     1    Root
*  2       1.1.1.0/24         eth3       0.0.0.0   C    0     0    Root
   3       0.0.0.0/0          eth4     2.2.2.250   S   20    10    Root
*  6       2.2.2.0/24         eth4       0.0.0.0   C    0     1    Root
*  5      10.1.1.0/24         eth1       0.0.0.0   C   20     1    Root
```

如果通過 ethernet3 的路由變得無法使用，則通過 ethernet4 的預設路由就會變成活動狀態。啓用並組態 ethernet3 介面上的 IP 追蹤，使其監看路由器位址 1.1.1.250。如果 IP 追蹤無法到達 1.1.1.250，則安全性裝置上與 ethernet3 介面聯結的所有路由都會變成不活動狀態。因此，通過 ethernet4 的預設路由會變成活動狀態。當 IP 追蹤又重新可以到達 1.1.1.250 時，通過 ethernet3 的預設路由會變成活動狀態，同時通過 ethernet4 的預設路由會變成不活動狀態，因爲通過 ethernet3 的預設路由才是優先使用的預設路由。

下列內容可啓用介面失敗臨界值爲 5 的 IP 追蹤，並組態 ethernet3 介面上的 IP 追蹤，使其監看路由器 IP 位址 1.1.1.250，爲其指派的權重爲 10。

WebUI

Network > Interfaces > Edit (對於 ethernet3) > Monitor: 輸入下面的內容，然後按一下 **Apply**:

Enable Track IP: (選擇)
Threshold: 5
> Monitor Track IP ADD: 輸入下面的內容，然後按一下 **Add**:
Static: (選擇)
Track IP: 1.1.1.250
Weight: 10

CLI

```
set interface ethernet3 monitor track-ip ip 1.1.1.250 weight 10
set interface ethernet3 monitor track-ip threshold 5
set interface ethernet3 monitor track-ip
save
```

在此範例中，目標位址的失敗臨界值設爲預設值 3。也就是說，如果該目標位址連續 3 次不回應 ping，就會對介面上 IP 追蹤的失敗臨界值套用權重 10。因爲介面上 IP 追蹤的失敗臨界值爲 5，所以權重 10 會導致安全性裝置上與該介面聯結的路由停用。

確認介面上 IP 追蹤狀態的方式是發出 CLI 指令 **get interface ethernet3 track-ip**，如圖 36 所示 :

圖 36: get interface 指令輸出

```
ns-> get interface ethernet3 track-ip

ip addressintervalthreshold wei gatewayfail-countsuccess-rate

1.1.1.250 11100.0.0.034346 %

threshold: 5, failed: 1 ip(s) failed, weighted sum = 10
```

get route 指令顯示通過 ethernet4 的預設路由目前處於活動狀態，通過 ethernet3 的所有路由則不再處於活動狀態。

圖 37: get route 指令輸出

```
ns-> get route
untrust-vr (0 entries)
------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
------------------------------------------------------------------------
   ID    IP-Prefix   Interface   Gateway   P  Pref    Mtr   Vsys
------------------------------------------------------------------------
    4    0.0.0.0/0     eth3    1.1.1.250   S    20      1   Root
    2   1.1.1.0/24     eth3      0.0.0.0   C     0      0   Root
*   3    0.0.0.0/0     eth4    2.2.2.250   S    20     10   Root
*   6   2.2.2.0/24     eth4      0.0.0.0   C     0      1   Root
*   5  10.1.1.0/24     eth1      0.0.0.0   C    20      1   Root
```

請注意，即使通過 ethernet3 的路由已不再處於活動狀態，IP 追蹤仍會繼續使用與 ethernet3 聯結的路由來傳送 ping 要求至目標 IP 位址。當 IP 追蹤又能夠到達 1.1.1.250 時，安全性裝置上通過 ethernet3 的預設路由又會再次處於活動狀態。同時，通過 ethernet4 的預設路由會變成不活動狀態，因爲通過 ethernet3 的預設路由才是優先使用的預設路由。

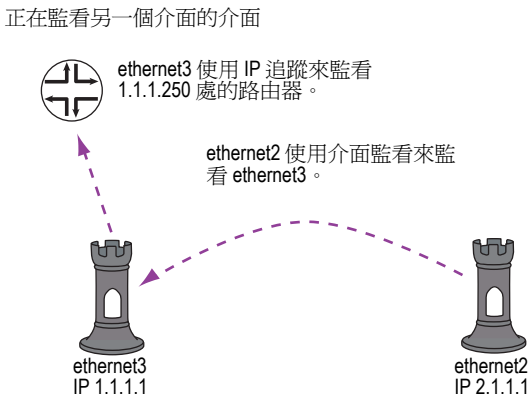
介面監看

安全性裝置可監看介面的實體和邏輯狀態，然後根據它所發現的變更採取行動。請參閱圖 38。例如，如果被監看介面的狀態從工作中變成不工作中，可能會發生下列情況，如表 12 所示 :

表 12: 被監看介面

若 :	之後 :
介面的實體狀態從工作中變成不工作中	狀態變更會使監看剛變成不工作中狀態之介面的另一個介面也變成不工作中狀態。您可指定要讓第二個介面變成實體不工作中還是邏輯不工作中狀態。 不論是哪一個介面的狀態變成實體不工作中狀態，或是兩個介面的結合權重一起變成實體不工作中狀態，都可能會觸發 NSRP 故障後移轉。只有在介面的實體狀態改變時，才會發生 NSRP 裝置或 VSD 群組故障後移轉。
如果 IP 追蹤失敗，會使介面的邏輯狀態從工作中變成不工作中	狀態變更會使監看剛變成不工作中狀態之介面的另一個介面也變成不工作中狀態。雖然第一個介面處於邏輯不工作中狀態，您仍可指定要讓第二個介面的不工作中狀態成爲實體還是邏輯不工作中。

圖 38: Ethernet1 與 Ethernet2 介面監看



若要設定介面監看，請執行以下操作之一 :

WebUI

Network > Interfaces > Edit (對於要負責監看的介面) > Monitor > Edit Interface: 輸入下面的內容，然後按一下 **Apply**:

Interface Name: 選擇要接受監看的介面。
Weight: 輸入介於 1 和 255 之間的權重值。

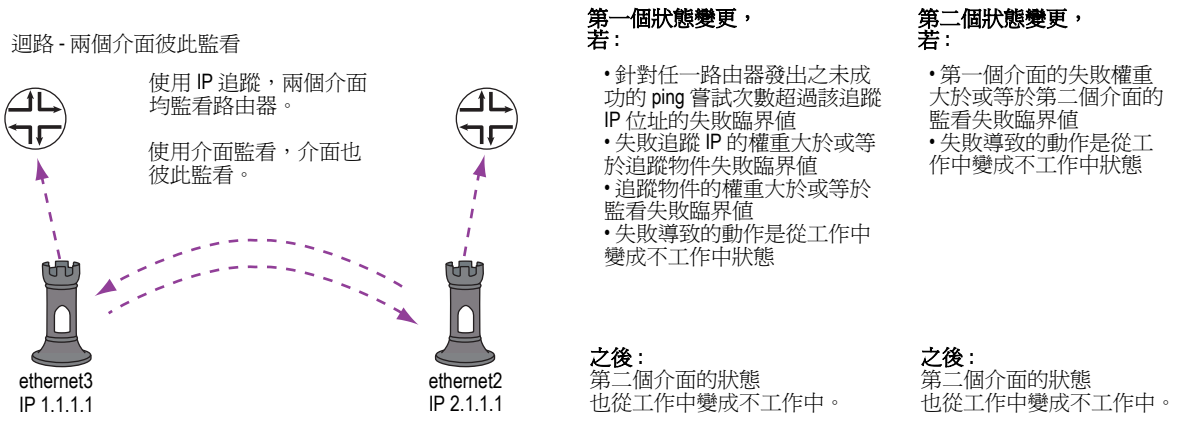
CLI

set interface *interface1* monitor interface *interface2* [weight *number*]
如果不設定權重，安全性裝置會套用預設的權重值 255。

如果兩個介面彼此監看，就會形成一個迴路。在這種情況下，如果其中一個介面的狀態改變，迴路中的另一個介面的狀態也會改變。請參閱圖 39。

注意： 一個介面一次只能在一個迴路中。我們不支援同一介面屬於多個迴路的組態。

圖 39: 迴路監看



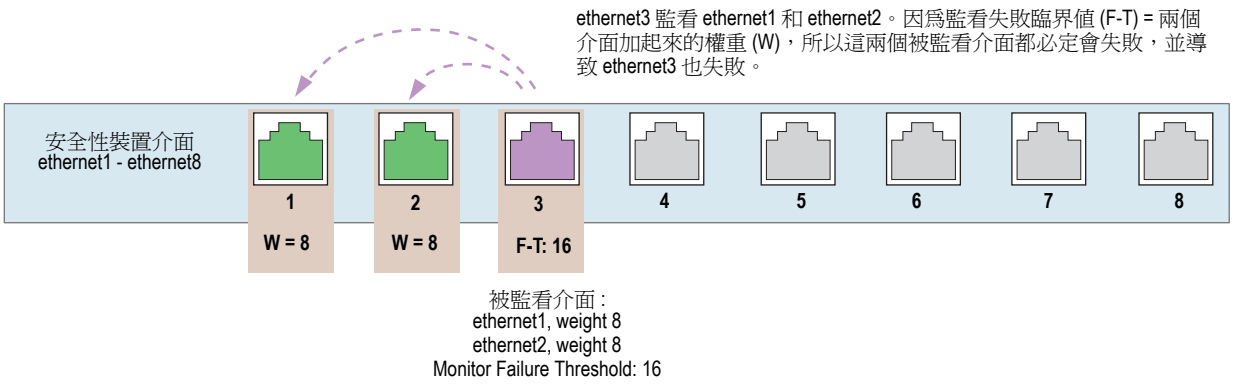
監看兩個介面

在下例中，組態 ethernet3，使其監看兩個介面 - ethernet1 和 ethernet2。因爲每個被監看介面的權重加起來 (8 + 8) 等於監看失敗臨界值 (16)，所以 ethernet1 和 ethernet2 必定會同時失敗 (且其狀態從工作中變成不工作中)，然後導致 ethernet3 也失敗 (且其狀態從工作中變成不工作中)。請參閱圖 40。

注意： 此範例省略了 ethernet1 和 ethernet2 介面上的 IP 追蹤組態 (請參閱第 60 頁上的「追蹤 IP 位址」)。在沒有 IP 追蹤的情況下，只有一個原因可能使 ethernet1 和 ethernet2 失敗，就是當它們實體上與其他網路裝置中斷連接，或是它們無法維持與這些網路裝置的連結時。

如果將監看失敗臨界值設爲 8，或使其保持 16 不變，並將每個被監看介面的權重設爲 16，則不論 ethernet1 還是 ethernet2 失敗，都會導致 ethernet3 失敗。

圖 40: 兩個迴路介面監看



WebUI

Network > Interfaces > Edit (對於 ethernet3) > Monitor > Edit Interface: 輸入下面的內容，然後按一下 **Apply**:

ethernet1: (選擇); Weight: 8
ethernet2: (選擇); Weight: 8

Network > Interfaces > Edit (對於 ethernet3) > Monitor: 在 Monitor Threshold 欄位中輸入 **16**，然後按一下 **Apply**。

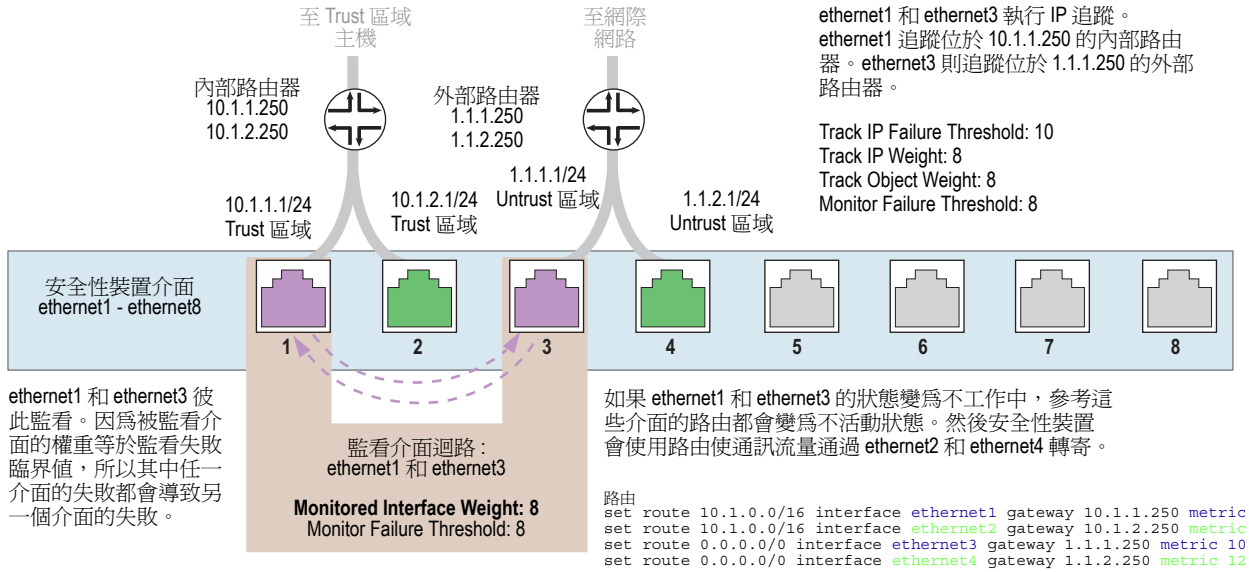
CLI

```
set interface ethernet3 monitor interface ethernet1 weight 8
set interface ethernet3 monitor interface ethernet2 weight 8
set interface ethernet3 monitor threshold 16
save
```

監看介面迴路

在下例中，先組態兩個介面 (ethernet1 和 ethernet3) 的 IP 追蹤。然後組態這些介面，使其彼此監看，這樣當其中一個介面的狀態改變時，另一個介面的狀態也會改變。最後，定義兩組路由。第一組路由轉寄通訊流量，使其通過 ethernet1 和 ethernet3。第二組路由的目的地位址與第一組相同，但這些路由的計量值等級較低，且使用的出口介面 (ethernet2 和 ethernet4) 和閘道與第一組不同。如果第一組介面在套用此組態之後失敗，安全性裝置會將所有通訊流量重新路由通過第二組路由。所有區域都在 trust-vr 路由設定網域中。

圖 41: 四個介面迴路監看



WebUI

1. **IP 追蹤**
   Network > Interfaces > Edit (對於 ethernet1) > Monitor: 輸入下面的內容，然後按一下 **Apply**。

   Enable Track IP: (選擇)
   Monitor Threshold: 8
   Track IP Option: Threshold: 8
   Weight: 8

注意： 若要控制介面狀態是變爲邏輯還是實體不工作中 (或是工作中) 狀態，必須使用 CLI 指令 **set interface** *interface* **monitor threshold** *number* **action { down | up } { logically | physically }**。只有與非 Null 區域的任何其他安全區連結的實體介面的狀態才可爲實體工作中或不工作中。

   > Monitor Track IP ADD: 輸入下面的內容，然後按一下 **Add**:

   Static: (選擇)
   Track IP: 10.1.1.250
   Weight: 8
   Interval: 3 Seconds
   Threshold: 10

   Network > Interfaces > Edit (對於 ethernet3) > Monitor: 輸入下面的內容，然後按一下 **Apply**。

   Enable Track IP: (選擇)
   Monitor Threshold: 8
   Track IP Option: Threshold: 8
   Weight: 8

   > Monitor Track IP ADD: 輸入下面的內容，然後按一下 **Add**:

   Static: (選擇)
   Track IP: 1.1.1.250
   Weight: 8
   Interval: 3 Seconds
   Threshold: 10

2. **介面監看**
   Network > Interfaces > Edit (對於 ethernet1) > Monitor > Edit Interface: 輸入下面的內容，然後按一下 **Apply**:

   ethernet3: (選擇); Weight: 8

   Network > Interfaces > Edit (對於 ethernet3) > Monitor > Edit Interface: 輸入下面的內容，然後按一下 **Apply**:

   ethernet1: (選擇); Weight: 8

3. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 10.1.0.0/16
   Gateway: (選擇)
   Interface: ethernet1
   Gateway IP Address: 10.1.1.250
   Metric: 10

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 10.1.0.0/16
   Gateway: (選擇)
   Interface: ethernet2
   Gateway IP Address: 10.1.2.250
   Metric: 12

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250
   Metric: 10

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet4
   Gateway IP Address: 1.1.2.250
   Metric: 12

CLI

1. **IP 追蹤**
   set interface ethernet1 track-ip ip 10.1.1.250 weight 8
   set interface ethernet1 track-ip threshold 8
   set interface ethernet1 track-ip weight 8
   set interface ethernet1 track-ip
   set interface ethernet3 track-ip ip 1.1.1.250 weight 8
   set interface ethernet3 track-ip threshold 8
   set interface ethernet3 track-ip weight 8
   set interface ethernet3 track-ip

2. **介面監看**
   set interface ethernet1 monitor interface ethernet3 weight 8
   set interface ethernet1 monitor threshold 8 action down physically
   set interface ethernet3 monitor interface ethernet1 weight 8
   set interface ethernet3 monitor threshold 8 action down physically

3. **路由**

```
set vrouter trust-vr route 10.1.0.0/16 interface ethernet1 gateway 10.1.1.250
    metric 10
set vrouter trust-vr route 10.1.0.0/16 interface ethernet2 gateway 10.1.2.250
    metric 12
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250 metric
    10
set vrouter trust-vr route 0.0.0.0/0 interface ethernet4 gateway 1.1.2.250 metric
    12
save
```

安全區監看

除了監看個別介面外，介面還可以監看安全區內的所有介面，它可以監看任何安全區，但它本身所屬的安全區除外。要使整個安全區失敗，與該安全區連結的每個介面都必須失敗。只要與被監看區域連結的介面是工作中狀態，安全性裝置就會將整個區域視爲處於工作中狀態。

若要組態介面，使其監看某個安全區，請執行下面的操作之一：

WebUI

Network > Interfaces > Edit（對於要負責監看的介面）> Monitor > Edit Zone: 輸入下面的內容，然後按一下 **Apply**:

Zone Name: 選擇要接受監看的區域。
Weight: 輸入介於 1 和 255 之間的權重值。

CLI

```
set interface interface monitor zone zone [ weight number ]
```

如果不設定權重，安全性裝置會套用預設的權重值 255。

不工作中介面和通訊流量傳遞

組態介面上的 IP 追蹤可讓安全性裝置在透過第一個介面無法連接某些 IP 位址時，透過不同介面將向外通訊流量重新路由。不過，雖然安全性裝置會因爲 IP 追蹤失敗而將與某個介面聯結的路由停用，但該介面仍可保持實體活動狀態，也仍然可以傳送和接收通訊流量。例如，安全性裝置會繼續處理現有會話的向內通訊流量，這些通訊流量可能會到達 IP 追蹤失敗的原始介面。安全性裝置也會繼續使用該介面來傳送 ping 要求至目標 IP 位址，以確定這些目標位址是否又再度變得可以連接。在這些情況下，通訊流量仍會通過 IP 追蹤失敗、安全性裝置已停用其路由的介面。

安全性裝置在這類介面上處理會話通訊流量的方式視下列情況而定：

- 如果您用來組態 IP 追蹤的介面是某個會話的出口介面，會話的回覆會繼續到達該介面，且安全性裝置仍會處裡它們。
- 如果您用來組態 IP 追蹤的介面是某個會話的入口介面，則套用 **set arp always-on-dest** 指令會導致安全性裝置將會話回覆重新路由至另一個介面。如果您不設定此指令，安全性裝置會將會話回覆透過 IP 追蹤失敗的介面來轉寄，即使安全性裝置已經停用使用該介面的路由。（預設未設定此指令。）

依照預設，安全性裝置會在它收到新會話的初始封包時，快取會話初始程式的 MAC 位址。如果您輸入 CLI 指令 **set arp always-on-dest**，安全性裝置不會快取會話初始程式的 MAC 位址。安全性裝置會在處理對該初始封包的回覆時，執行 ARP 查詢。如果初始程式的 MAC 位址在 ARP 表中，安全性裝置會使用該位址。如果 MAC 位址沒有在 ARP 表中，安全性裝置會傳送 ARP 要求以獲得目的地 MAC 位址，然後將它收到的 MAC 位址加入到它的 ARP 表中。每當路由發生變更時，安全性裝置就會執行另一個 ARP 查詢。

「出口介面上的失敗」分別說明 IP 追蹤在出口介面和入口介面上失敗的不同情況；以及後者發生時，如果使用指令 **set arp always-on-dest** 會有何影響。

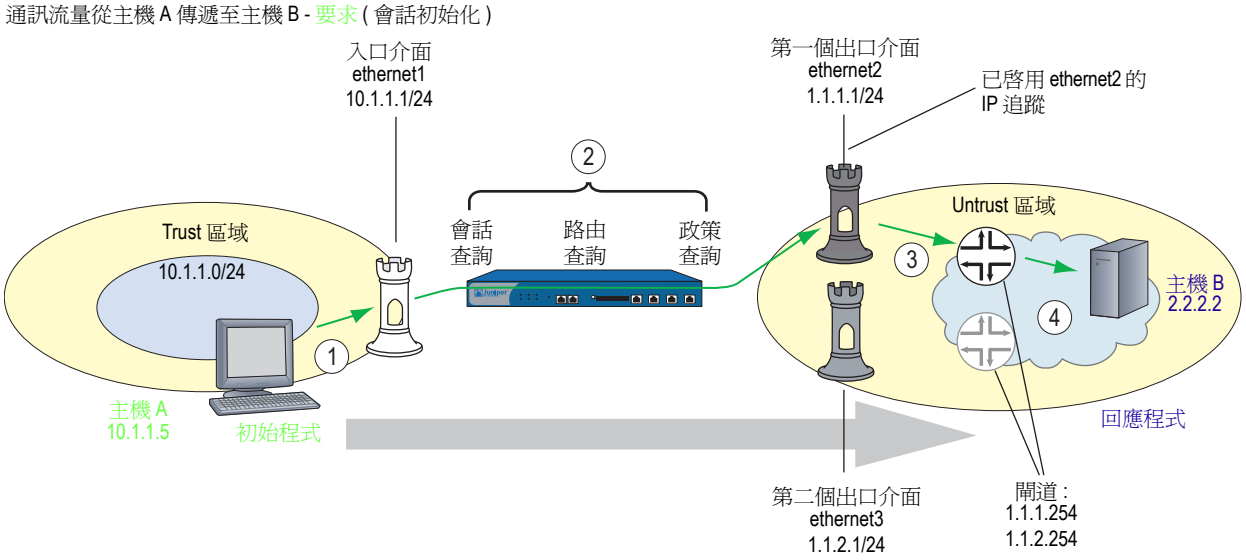
注意： 「出口介面上的失敗」說明 IP 追蹤會觸發什麼樣的路由變更，以及這些變更對通過所有 Juniper Networks 安全性裝置 (NetScreen-5XT 與 NetScreen-5GT 除外) 的封包有何影響。在這兩個例外的裝置上，IP 追蹤失敗會觸發介面故障後移轉。如需詳細資訊，請參閱第 **11**-46 頁上的「雙 Untrust 介面」。

出口介面上的失敗

在下列情況下，組態 ethernet2 上的 IP 追蹤，該介面是從主機 A 傳遞至主機 B 的會話的出口介面。主機 A 初始化此會話的方式是將封包傳送至主機 B，如圖 42 中所示。

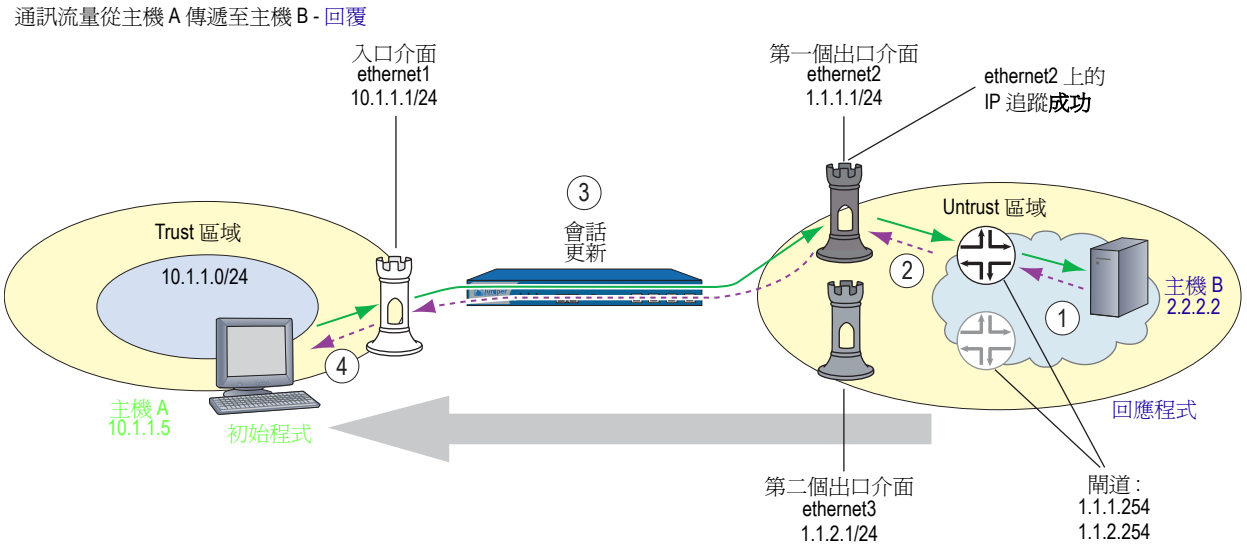
注意： 您必須先建立兩個至主機 B 的路由，兩個出口介面必須位於相同區域中，這樣重新路由通訊流量之前和之後才能套用相同的政策。

圖 42: 主機 A 與主機 B IP 追蹤



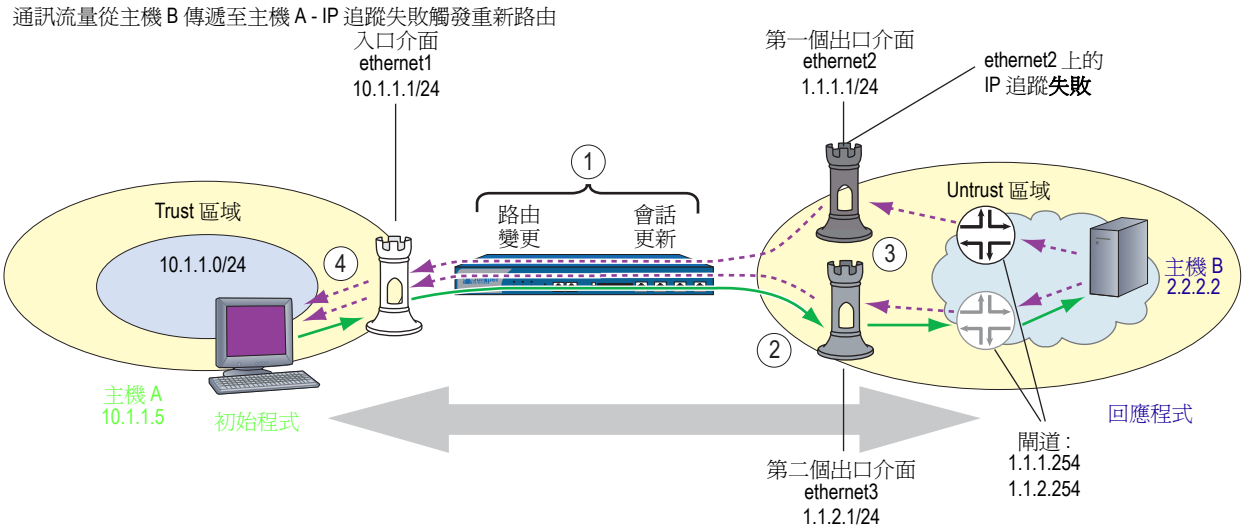
當主機 B 向主機 A 回覆時，回傳的通訊流量會依循類似的路徑傳回安全性裝置，如圖 43 中所示。

圖 43: 主機 B 至主機 A 出口通訊流量



如果 ethernet2 上的 IP 追蹤失敗，安全性裝置會停止使用 ethernet2 的路由，而使用 ethernet3 將向外通訊流量傳至主機 B。不過，主機 B 對主機 A 作出的回覆可能會通過 ethernet2 或 ethernet3 之一到達，然後安全性裝置再透過 ethernet1 將它們轉寄至主機 A。請參閱圖 44。

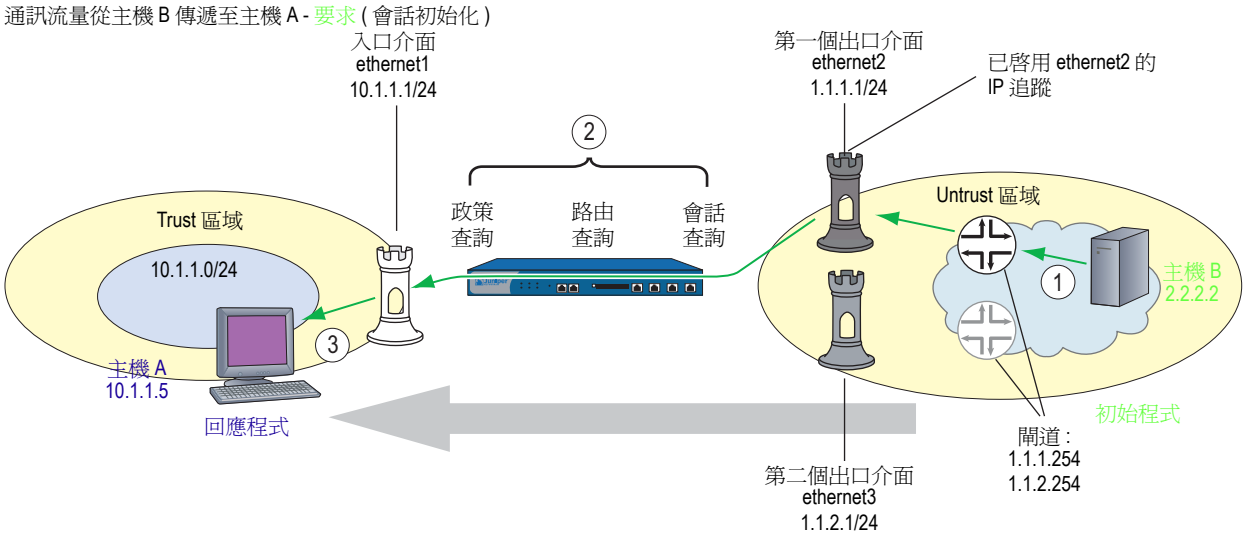
圖 44: 出口 IP 追蹤失敗



入口介面上的失敗

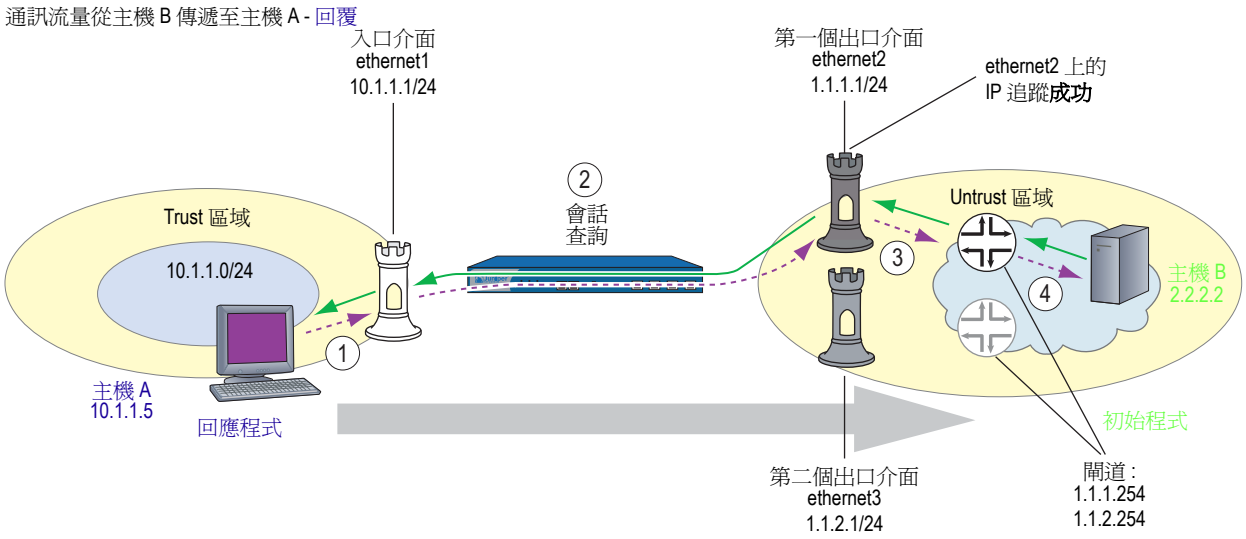
在下列情況下，再次組態 ethernet2 上的 IP 追蹤，但這次 ethernet2 是安全性裝置上從主機 B 傳遞至主機 A 的會話的入口介面。主機 B 初始化此會話的方式是將封包傳送至主機 A，如圖 45 中所示。

圖 45: 主機 B 至主機 A 入口通訊流量



當主機 A 向主機 B 回覆時，回傳的通訊流量會依循類似的路徑傳回安全性裝置，如圖 46 中所示。

圖 46: 主機 A 至主機 B 入口通訊流量



1. 位於 10.1.1.5 的主機 A 將回覆封包經由位於 10.1.1.1 的 ethernet1 送達主機 B (2.2.2.2)。
2. 安全性裝置會執行會話查詢。因爲這是一個回覆，裝置會將其與現有的會話加以配對，並隨之重新整理 會話表項目。
3. 裝置透過使用閘道 1.1.1.254 快取的 MAC 位址或是進行 ARP 查詢以搜尋其 MAC 位址的方式，使裝置 透過 ethernet2 將封包轉寄至閘道。
4. 當位於 1.1.1.254 的閘道收到回覆時，會將回覆轉寄至它的下一個躍點。路由會不斷進行，直到主機 B 收到封包爲止。

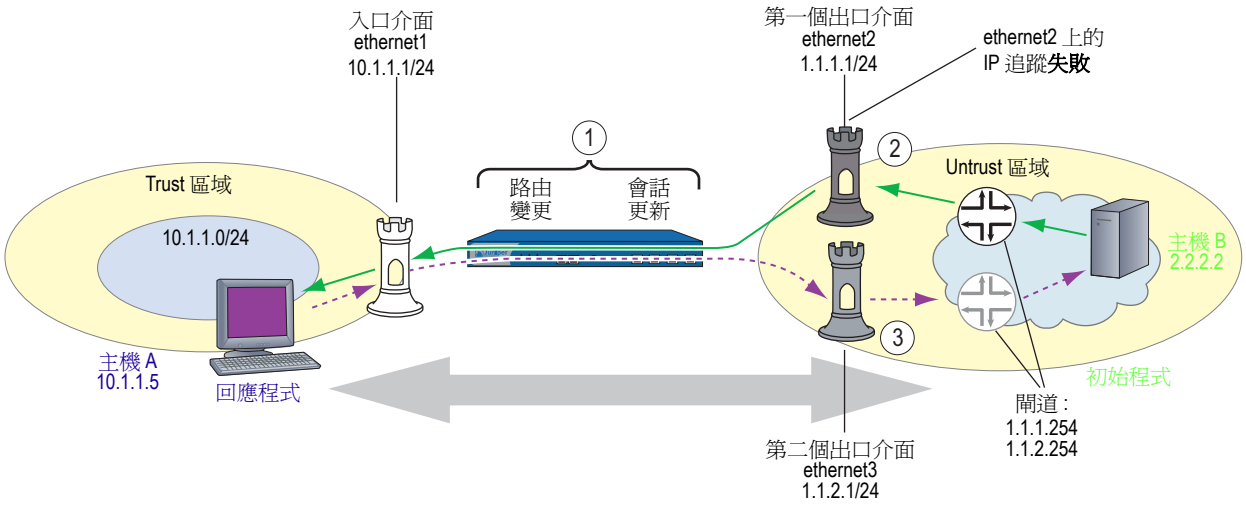
如果 ethernet2 上的 IP 追蹤失敗，安全性裝置會停止使用 ethernet2 的路由，而使用 ethernet3 將向外通訊流量傳至主機 B。不過，主機 B 對主機 A 作出的要求仍可通過 ethernet2 到達，然後安全性裝置仍透過 ethernet1 將它們轉寄至主機 A。IP 追蹤失敗後，從主機 B 至主機 A 的資料傳遞要求與 IP 追蹤失敗前並無不同。不過，根據 **set arp always-on-dest** 指令的不同應用，來自主機 A 的回覆可能會採用兩個不同路徑的其中一個。

如果設定指令 **set arp always-on-dest**，安全性裝置會在處理對會話中第一個封包的回覆或路由發生變更時，傳送 ARP 要求來獲得目的地 MAC 位址。(如果未設定此指令，安全性裝置會快取會話初始程式的 MAC 位址，並在處理回覆時使用該位址。預設未設定此指令)。

如果 ethernet2 上的 IP 追蹤失敗，安全性裝置會先停止使用 ethernet2 的所有路由，然後進行路由查詢。它會找出可透過 ethernet3 和閘道 1.1.2.254 到達主機 B 的另一個路由。然後它會掃描它的會話表並將所有會話重新定向至新的路由。如果您啓用 **set arp always-on-dest** 指令，安全性裝置會在收到從主機 A 傳來的下一個封包時進行 ARP 查詢，因爲它處於受到路由變更影響的會話中。不管來自主機 B 的封包送達哪一個入口介面，安全性裝置都會將所有後續的回覆從主機 A 透過 ethernet3 傳送至閘道 1.1.2.254。請參閱圖 47。

圖 47: 具通訊流量重新路由的入口 IP 追蹤失敗

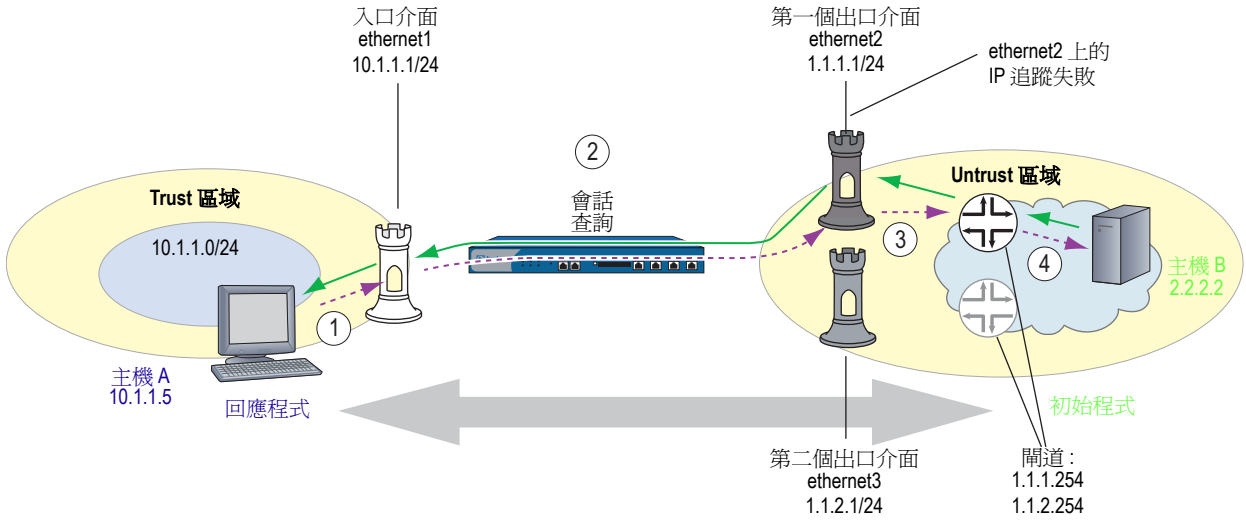
通訊流量從主機 B 傳遞至主機 A - IP 追蹤失敗觸發重新路由



如果您設定的指令是 **unset arp always-on-dest**（此爲預設組態），安全性裝置會使用閘道 1.1.1.1 的 MAC 位址，該 MAC 位址是主機 B 傳送初始會話封包時裝置快取的位址。安全性裝置會繼續透過 ethernet2 傳送會話回覆。在這種情況下，IP 追蹤失敗不會使透過安全性裝置傳遞的資料發生任何變化。

圖 48: 無通訊流量重新路由的入口 IP 追蹤失敗

通訊流量從主機 B 傳遞至主機 A - IP 追蹤失敗未觸發重新路由



第 4 章
介面模式

介面可以在三種不同的模式中操作：網路位址轉譯 (NAT)、路由和透明。如果連結到 Layer 3 (第 3 層) 區域的介面有 IP 位址，您可以爲該介面定義 NAT 或「路由」操作模式。連結到 Layer 2 (第 2 層) 區域 (如預先定義的 v1-trust、v1-untrust 和 v1-dmz，或使用者定義的 Layer 2 (第 2 層) 區域的介面必須爲「透明」模式。您在組態介面時選擇操作模式。

注意： 雖然您可以將連結到任何 Layer 3 (第 3 層) 區域的介面操作模式定義爲 NAT，但是，安全性裝置只對透過該介面傳遞至 Untrust 區域的通訊流量執行 NAT。對於通往 Untrust 區域之外其他任何區域的通訊流量，ScreenOS 不會執行 NAT。同時也請注意，ScreenOS 讓您可以在 NAT 模式中設定 Untrust 區域介面，但是這麼做並不會啓動任何 NAT 操作。

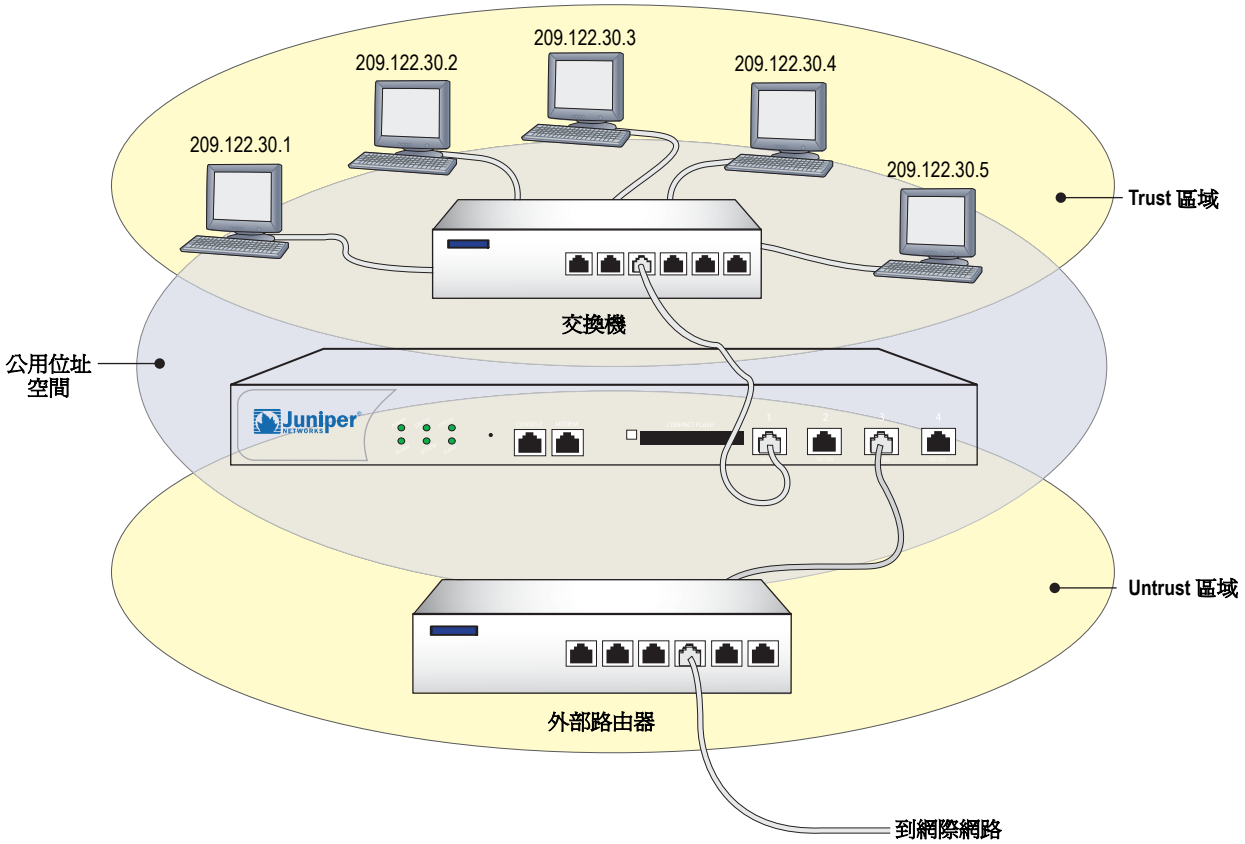
本章包括下列各節：

- 第 78 頁上的「透明模式」
  - 第 79 頁上的「區域設定」
  - 第 79 頁上的「通訊流量轉寄」
  - 第 80 頁上的「未知的 Unicast 選項」
- 第 90 頁上的「NAT 模式」
  - 第 91 頁上的「向內與向外 NAT 通訊流量」
  - 第 92 頁上的「介面設定」
- 第 95 頁上的「路由模式」
  - 第 96 頁上的「介面設定」

透明模式

介面爲「透明」模式時，安全性裝置會過濾通過防火牆的封包，而不會修改 IP 封包標頭中的任何來源或目的地資訊。所有的介面都像是相同網路中的一部分，而安全性裝置的作用更像是 Layer 2 (第 2 層) 交換機或橋接器。在「透明」模式中，介面的 IP 位址設定爲 0.0.0.0，讓使用者可以看見安全性裝置，也就是「透明」的。請參閱圖 49。

圖 49: 透明模式



「透明」模式是一種簡便的方法，保護 Web 伺服器或主要從不信任來源接收通訊流量的其他任何種類伺服器。使用「透明」模式有下列優點 :

- 不需要重新組態路由器或受保護伺服器的 IP 位址設定
- 不需要爲到達受保護伺服器的向內通訊流量建立對應或虛擬 IP 位址

區域設定

依預設，ScreenOS 會建立一個功能區，即 VLAN 區域，及三個 L2 安全區 : V1-Trust、V1-Untrust 與 V1-DMZ。

VLAN 區域

VLAN 區域代管 VLAN1 介面，具有與實體介面相同的組態和管理能力。安全性裝置在「透明」模式中時，您可使用 VLAN1 介面來管理裝置和終止 VPN 通訊流量。您可以將 VLAN1 介面組態爲允許 L2 安全區中的主機來管理裝置。因此，必須將 VLAN1 介面的 IP 位址設定爲和 L2 安全區中的主機在相同的子網路中。

對於管理通訊流量，VLAN1 管理 IP 比 VLAN1 介面 IP 優先。您可以爲管理通訊流量設定「VLAN1 管理 IP」，並將 VLAN1 介面 IP 專用於 VPN 通道終止。

預先定義的第 2 層區域

依預設，ScreenOS 提供三個 L2 安全區 : V1-Trust、V1-Untrust 與 V1-DMZ。這三個安全區共享同一個 L2 網域。在某個區域中組態介面時，介面會新增到由所有 L2 區域中的所有介面共用的第 2 層網域中。L2 區域中的所有主機必須位在相同的子網路中以進行通訊。

如上一節所述，當裝置處於透明模式時，您可以使用 VLAN1 介面來管理裝置。若是到達 VLAN1 介面的管理通訊流量，您則必須啓用 VLAN1 介面以及管理通訊流量流經區域上的管理選項。依預設，V1-Trust 區域中的所有管理選項均爲啓用狀態。若要啓用其他區域中的主機以管理裝置，您必須設定所屬區域上的管理選項。

注意 : 若要查看哪一個介面實體爲每個 Juniper Networks 安全性平台預先連結到 L2 區域，請參閱該平台的安裝程式指南。

通訊流量轉寄

在第 2 層 (L2) 上執行的安全性裝置不會允許任何區域間或區域內部的通訊流量通過，除非已在裝置上組態好政策。如需如何設定政策的詳細資訊，請參閱第 153 頁上的「政策」。在安全性裝置上組態政策後，裝置會執行下列作業 :

- 允許或拒絕政策中所指定的通訊流量。
- 允許 ARP 與 L2 非 IP 多點傳送與廣播通訊流量。而後安全性裝置會接收與傳送 L2 旋狀樹狀通訊協定的廣播通訊流量。
- 繼續阻斷所有非 IP 及 非 ARP 單點傳送通訊流量與 IPSec 通訊流量

您可依照下列所述變更裝置的轉寄行爲 :

- 若爲阻斷包含多點傳送與廣播通訊流量在內的所有 L2 非 IP 與 非 ARP 通訊流量，請輸入 **unset interface vlan1 bypass-non-ip-all** 指令。
- 若要允許所有 L2 非 IP 通訊流量通過裝置，請輸入 **set interface vlan1 bypass-non-ip** 指令。
- 若要回復裝置的預設行爲，即阻斷所有非 IP 與非 ARP 單點傳通訊流量，請輸入 **unset interface vlan1-bypass-non-ip** 指令。

請注意，若組態檔案中同時具有上述兩個指定，則 **unset interface vlan1 bypass-non-ip-all** 指令一律會覆寫 **unset interface vlan1 bypass-non-ip** 指令。因此，如果您先前已經輸入了 **unset interface vlan1 bypass-non-ip-all** 指令，而現在您想要讓裝置回復只阻斷非 IP 及非 ARP 單點傳送通訊流量的預設行爲，您就應先輸入 **set interface vlan1 bypass-non-ip** 指令，以允許所有非 IP 及非 ARP 通訊流量 (包括多點傳送、單點傳送及廣播通訊流量) 通過裝置。然後您必須輸入 **unset interface vlan1-bypass-non-ip** 指令以只阻斷非 IP、非 ARP 單點傳送通訊流量。

- 若要讓安全性裝置允許 IPSec 通訊流量通過，而不試圖將之終止，請使用 **set interface vlan1 bypass-others-ipsec** 指令。而後安全性裝置即會允許 IPSec 通訊流量通過，前往其他 VPN 終止點。

注意： 具有透明模式介面的安全性裝置需要使用路由，兩個用途如下：定向如 SNMP 回報的自生通訊流量，以及在封裝或解除封裝通訊流後，轉寄 VPN 通訊流量。

未知的 Unicast 選項

當主機或任何種類的網路裝置不知道與其他裝置的 IP 位址相關的 MAC 位址時，會使用「位址解析通訊協定 (ARP)」來取得位址。要求者將 ARP 查詢 (arp-q) 廣播到相同子網路上的所有其他裝置。arp-q 要求指定目的地 IP 位址處的裝置傳送回 ARP 回覆 (arp-r)，爲要求者提供回覆者的 MAC 位址。子網路中的所有其他裝置收到 arp-q 時，會檢查目的地 IP 位址，而且，由於這不是它們的 IP 位址，會卸除封包。只有有指定 IP 位址的裝置才會傳回 arp-r。裝置將 IP 位址與 MAC 位址配對後，將資訊儲存在其 ARP 快取記憶體中。

當 ARP 通訊流量通過處於「透明」模式的安全性裝置時，裝置會將來源 MAC 位址記錄在每一個封包中，並記住通往該 MAC 位址的介面。實際上，安全性裝置會記錄收到的所有封包中的來源 MAC 位址，以得知哪個介面通往哪個 MAC 位址。然後將這項資訊儲存在轉寄表中。

注意： 處於「透明」模式的安全性裝置不會允許區域間的任何通訊流量通過，除非已在裝置上組態好政策。若需如何在裝置處於透明模式時轉寄通訊流量的詳細資訊，請參閱 第 79 頁上的「通訊流量轉寄」。

當裝置傳送帶有目的地 MAC 位址的 unicast 封包 (位址在其 ARP 快取記憶體中)，但安全性裝置的轉寄表中沒有該位址時，會出現這種情況。例如，安全性裝置每次重新啓動時，都會清除其轉寄表。(也可用 CLI 指令 **clear arp** 來清除轉寄表。) 「透明」模式中的安全性裝置收到在轉寄表中沒有其項目的 unicast 封包時，可執行兩個過程之一：

- 執行政策查詢以確定允許接收來自來源位址通訊流量的區域後，從連結到這些區域的介面大量傳送初始封包出去，然後使用收到回覆的任何介面繼續。這就是預設啓用的氾濫選項。

- 卸除初始封包，將 ARP 查詢 (也可選擇 trace-route 封包，是活動時間值設定爲 1 的 ICMP 回應要求) 從所有介面 (封包已到達的介面除外) 大量傳送出去，然後透過從路由器或主機 (其 MAC 位址與初始封包中的目的地 MAC 位址配對) 收到 ARP (或 trace-route) 回覆的任何介面傳送後續封包。當目的地 IP 位址位於不相鄰的子網路時，Trace-route 選項可讓安全性裝置找出目的地 MAC 位址。

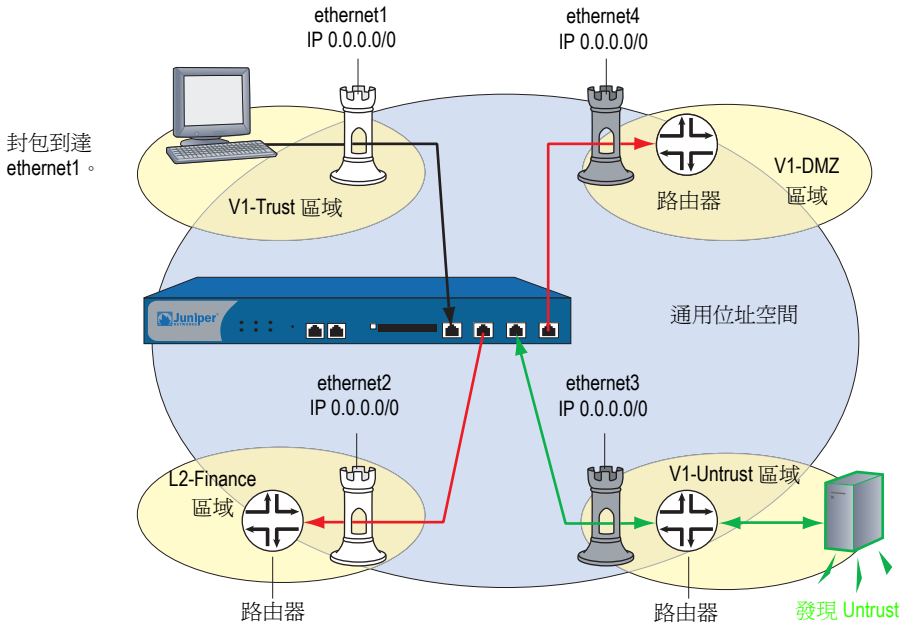
注意： 就氾濫和 ARP/trace-route 這兩種方法來說，ARP/trace-route 比較安全，因爲安全性裝置將 ARP 查詢和 trace-route 封包（而非初始封包）從所有的介面大量傳送出去。

氾濫方法

氾濫方法用與大多數 Layer 2（第 2 層）交換機相同的方式傳送封包。交換機維護轉寄表，其中包含 MAC 位址和每個 Layer 2（第 2 層）網域的相關連接埠。表格也包含相應的介面，交換機可以透過介面將通訊流量轉寄到每個裝置。每次在框架標頭中帶有新來源 MAC 位址的封包到達時，交換機都會將 MAC 位址新增到其轉寄表中。也會追蹤封包到達的介面。如果交換機不知道目的地 MAC 位址，交換機會複製封包並將其大量傳送出所有介面（封包到達的介面除外）。當帶有該 MAC 位址的回覆到達一個介面時，就會得知之前未知的 MAC 位址及其相應介面。

啓用氾濫方法後，當安全性裝置收到目的地 MAC 位址未在安全性裝置 MAC 表中列出的乙太網路框架時，會將封包大量傳送出所有的介面。

圖 50: 氾濫方法



安全性裝置將封包大量傳送出 ethernet2，但是沒有收到回覆。

若要啓用氾濫方法來處理未知的 unicast 封包，請執行下列的操作之一：

WebUI

Network > Interface > Edit（對於 VLAN1）：對於廣播選項，選擇 **Flood**，然後按一下 **OK**。

CLI

```
set interface vlan1 broadcast flood
save
```

ARP/Trace-Route 方法

啓用帶有 trace-route 選項的 ARP 方法後，如果安全性裝置收到目的地 MAC 位址未在其 MAC 表中列出的乙太網路框架時，安全性裝置執行下面的一系列動作 :

注意： 啓用 ARP 方法時，依預設會啓用 trace-route 選項。也可以啓用沒有 trace-route 選項的 ARP 方法。但是，如果目的地 IP 位址與入口 IP 位址在相同的子網路中，此方法只允許安全性裝置發現 unicast 封包的目的地 MAC 位址。(如需入口 IP 位址的詳細資訊，請參閱下一個注意事項。)

---

1. 安全性裝置記錄初始封包中的目的地 MAC 位址 (而且，如果轉寄表中沒有此位址，則將來源 MAC 位址及其相應的介面新增到其轉寄表中)。

2. 安全性裝置會卸除初始封包。

3. 安全性裝置產生兩個封包 - ARP 查詢 (arp-q) 和活動時間 (TTL) 欄位爲 1 的 trace-route (ICMP 回應請求或 PING)，並將這些封包大量傳送出所有的介面，除了初始封包到達的介面以外。安全性裝置會針對 arp-q 封包與 ICMP 回應請求，使用來自初始封包的來源與目的地 IP 位址。若是 arp-q 封包，安全性裝置則會以 VLAN1 的 MAC 位址取代來自初始封包的來源 MAC 位址，並以 ffff.ffff.ffff 取代來自初始封包的目的地 MAC 位址；若是 trace-route 選項，安全性裝置則會使用所廣播之 ICMP 回應請求中初始封包的來源及目的地 MAC 位址。

   如果目的地 IP 位址屬於與入口 IP 位址在相同子網路中的裝置，主機會傳回附有其 MAC 位址的 ARP 回覆 (arp-r)，進而指出安全性裝置必須透過其來轉寄以該位址爲目的地的通訊流量的介面。(請參閱第 83 頁上的圖 51「ARP 方法」。)

注意： 入口 IP 位址指的是將封包傳送到安全性裝置的最後一個裝置的 IP 位址。此裝置可能是傳送封包的來源或轉寄封包的路由器。

   如果目的地 IP 位址屬於入口 IP 位址所在子網路外其他子網路中的裝置，trace-route 會傳回通往目的地的路由器的 IP 和 MAC 位址，特別明顯的是指出了安全性裝置必須透過其來轉寄流向該 MAC 位址的通訊流量的介面。(請參閱第 84 頁上的圖 52 "Trace-Route"。)

注意： 事實上，trace-route 會傳回子網路中所有路由器的 IP 和 MAC 位址。然後安全性裝置將初始封包的目的地 MAC 位址與 arp-r 封包中的來源 MAC 位址配對，以確定要指向哪個路由器，並確定要使用哪個介面到達該目標。

---

4. 安全性裝置將從初始封包中收集的目的地 MAC 位址與通向該 MAC 位址的介面結合，將新項目新增到其轉寄表中。

5. 安全性裝置將其收到的所有後續封包轉寄出正確的介面以到達目的地。

若要啓用 ARP/trace-route 方法來處理未知的 unicast 封包，請執行下列的操作之一 :

WebUI

Network > Interface > Edit (對於 VLAN1): 對於廣播選項，選擇 **ARP**，然後按一下 **OK**。

CLI

```
set interface vlan1 broadcast arp
save
```

注意 : 依預設會啓用 trace-route 選項。如果要使用沒有 trace-route 選項的 ARP，請輸入下面的指令 : **unset interface vlan1 broadcast arp trace-route**。此指令會取消設定 trace-route 選項，但是不會取消將 ARP 設定爲處理未知 unicast 封包的方法。

圖 51 顯示當目的地 IP 位址位在相鄰子網路中時，ARP 找到目的地 MAC 的方式。

圖 51: ARP 方法

注意 : 下面只顯示封包標頭的相關元素和 MAC 位址中的最後四個數字。

如果下面的封包 :

乙太網路框架			IP 資料電報	
目的地	來源	類型	來源	目的地
11bb	11aa	0800	210.1.1.5	210.1.1.75

到達 ethernet1，而且轉寄表中沒有 MAC 位址 00dd.11dd.11dd 的項目，安全性裝置會大量傳送下面的 arp-q 封包 :

乙太網路框架			ARM 訊息	
目的地	來源	類型	來源	目的地
ffff	39ce	0806	210.1.1.5	210.1.1.75

當裝置在 ethernet2 收到下面的 arp-r 時 :

乙太網路框架			ARM 訊息	
目的地	來源	類型	來源	目的地
39ce	11bb	0806	210.1.1.75	210.1.1.5

它現在可以將 MAC 位址與通往該位址的介面相關聯。

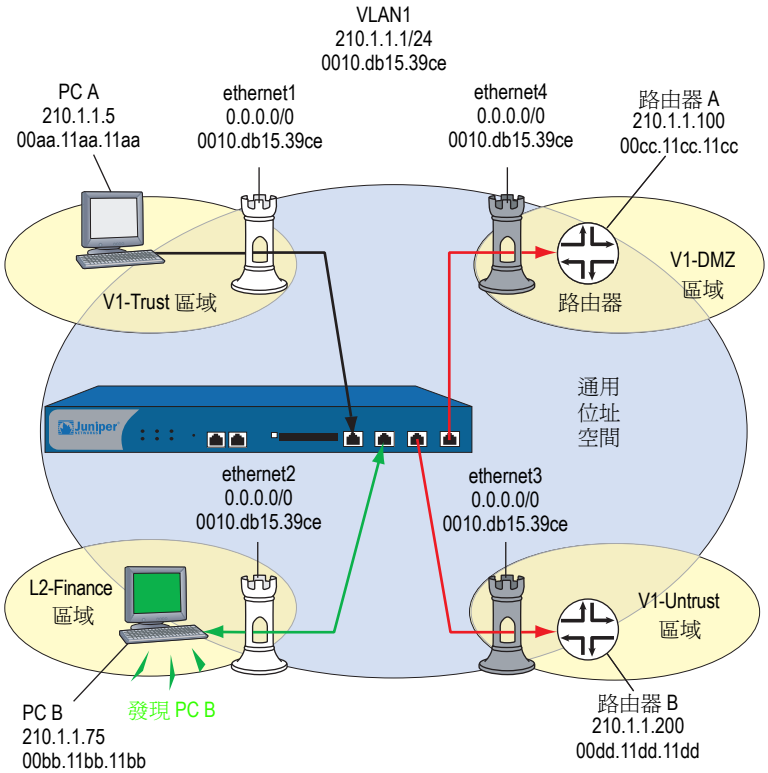


圖 52顯示當目的地 IP 位址位在不相鄰的子網路中時，trace-route 選項找到目的地 MAC 的方式。

圖 52: Trace-Route

注意：下面只顯示封包標頭的相關元素和 MAC 位址中的最後四個數字。

如果下面的封包：

乙太網路框架			IP 資料電報	
目的地	來源	類型	來源	目的地
11dd	11aa	0800	210.1.1.5	195.1.1.5

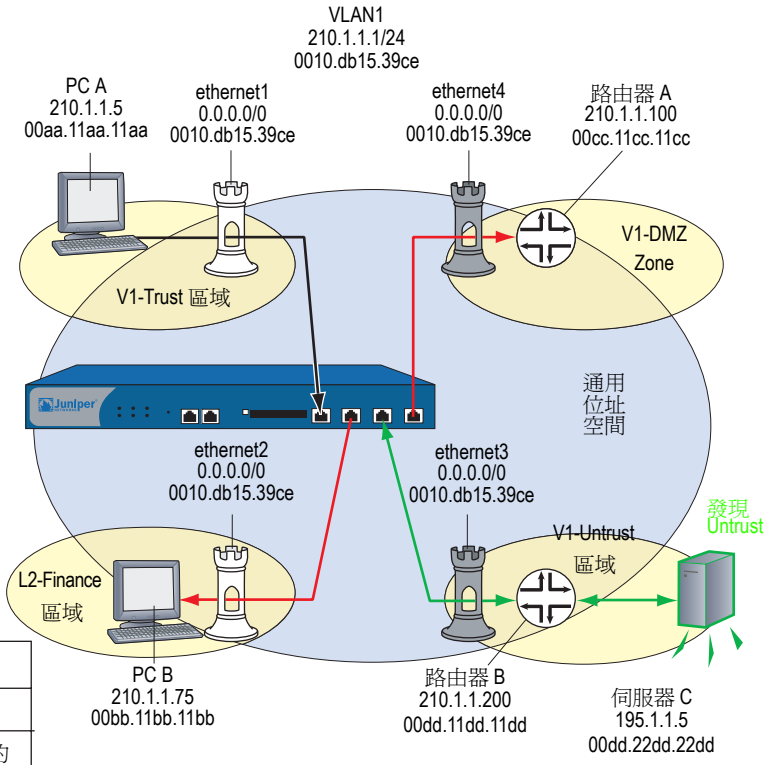
到達 ethernet1，而且轉寄表中沒有 MAC 位址 00dd.11dd.11dd 的項目，安全性裝置會將下面的 trace-route 封包大量傳送出 ethernet2、ethernet3 和 ethernet4:

乙太網路框架			ICMP 訊息		
目的地	來源	類型	來源	目的地	TTL
11dd	11aa	0800	210.1.1.5	195.1.1.5	1

當裝置在 ethernet3 收到下面的回應時：

乙太網路框架			ICMP 訊息		
目的地	來源	類型	來源	目的地	訊息
11aa	11dd	0800	210.1.1.200	210.1.1.5	超過的時間

它現在可以將 MAC 位址與通往該位址的介面相關聯。



組態用於管理的 VLAN1 介面

在本範例中，如下所示組態安全性裝置來管理其 VLAN1 介面：

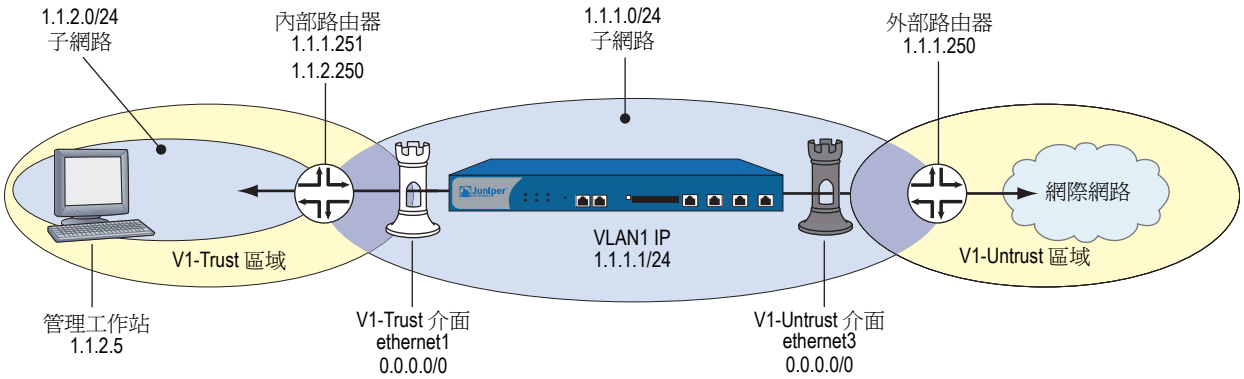
- 爲 VLAN1 介面指派 IP 位址 1.1.1.1/24。
- 在 VLAN1 介面和 V1-Trust 安全區上啓用 Web、Telnet、SSH 和 Ping。

注意： 依預設，安全性會啓用 VLAN1 介面和 V1-Trust 安全區的管理選項。本範例中所包括啓用的這些選項只是爲了說明目的。除非之前已經停用了選項，其實不需要手動啓動。

若要從第 2 層安全區管理裝置，必須在 VLAN1 介面和第 2 層安全區上設定相同的管理選項。

- 在信任虛擬路由器中 (所有的第 2 層安全區都在 trust-vr 路由設定網域中) 新增路由，讓管理通訊流量能在安全性裝置和管理工作站 (該工作站在安全性裝置的緊鄰子網路外) 之間流動。所有安全區都在 trust-vr 路由設定網域中。

圖 53: 透明 VLAN



WebUI

1. **VLAN1 介面**
   Network > Interfaces > Edit (對於 VLAN1): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet, SSH (選擇)
   Other Services: Ping (選擇)

2. **V1-Trust 區域**
   Network > Zones > Edit (對於 V1-Trust): 選擇下面的內容，然後按一下 **OK**:

   Management Services: WebUI, Telnet, SSH
   Other Services: Ping

3. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 1.1.2.0/24
   Gateway: (選擇)
   Interface: vlan1(trust-vr)
   Gateway IP Address: 1.1.1.251
   Metric: 1

CLI

1. **VLAN1 介面**

```
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ssh
set interface vlan1 manage ping
```

2. **V1-Trust 區域**
   set zone v1-trust manage web
   set zone v1-trust manage telnet
   set zone v1-trust manage ssh
   set zone v1-trust manage ping

3. **路由**
   set vrouter trust-vr route 1.1.2.0/24 interface vlan1 gateway 1.1.1.251 metric 1
   save

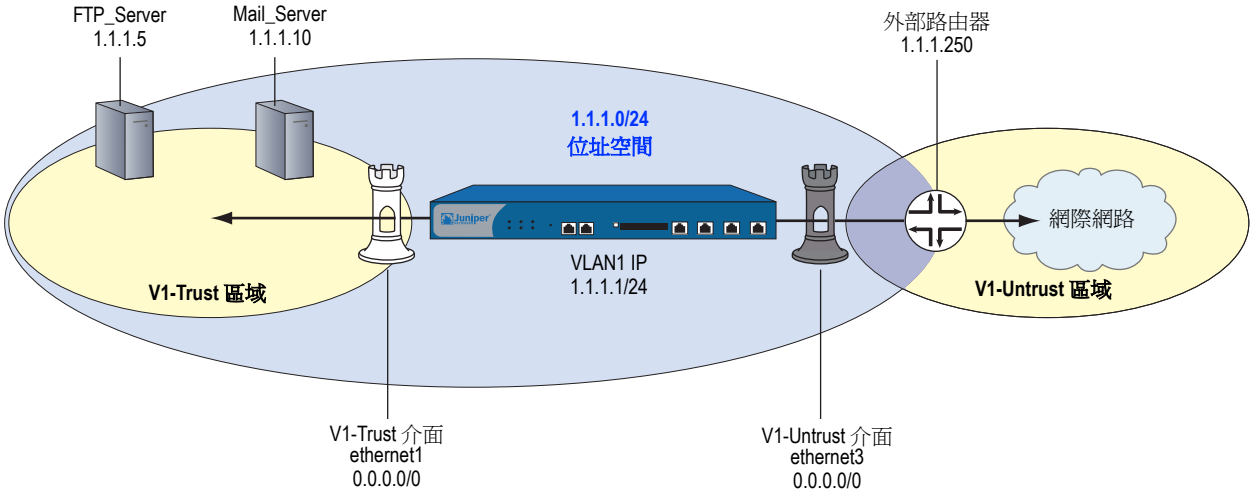
組態透明模式

下面的範例說明由在「透明」模式中的安全性裝置保護的單一 LAN 基本組態。政策允許 V1-Trust 區域中所有主機的向外通訊流量、郵件伺服器的向內 SMTP 服務，以及 FTP 伺服器的向內 FTP-GET 服務。

爲了提高管理通訊流量的安全性，將 WebUI 管理的 HTTP 連接埠號碼從 80 變更爲 5555，將 CLI 管理的 Telnet 連接埠號碼從 23 改爲 4646。使用 VLAN1 IP 位址 1.1.1.1/24 來管理 V1-Trust 安全區的安全性裝置。您定義 FTP 與郵件服務的位址。也組態至位於 1.1.1.250 的外部路由器預設路由，以便安全性裝置可以向其傳送向外 VPN 通訊流量。(V1-Trust 區域中所有主機的預設閘道也是 1.1.1.250。)

注意： 如需檢視在具透明模式介面的安全性裝置組態 VPN 通道的範例，請參閱第 5-139 頁上的「透明模式 VPN」。

圖 54: 基本透明模式



WebUI

1. **VLAN1 介面**
   Network > Interfaces > Edit (對於 VLAN1 介面): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet (選擇)
   Other Services: Ping (選擇)

2. **HTTP 連接埠**
   Configuration > Admin > Management: 在 HTTP Port 欄位中，鍵入 5555，然後按一下 **Apply**。

注意 : 預設連接埠號碼爲 80。建議將此號碼變更爲 1024 和 32,767 之間的數字，以防止對組態的未授權存取。稍後登入以管理裝置時，請在瀏覽器的 URL 欄位輸入下面的內容 : http://1.1.1.1:5555。

---

3. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: V1-Trust
   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: V1-Untrust
   IP Address/Netmask: 0.0.0.0/0

4. **V1-Trust 區域**
   Network > Zones > Edit (對於 v1-trust): 選擇下面的內容，然後按一下 **OK**:

   Management Services: WebUI, Telnet
   Other Services: Ping

5. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: FTP_Server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 1.1.1.5/32
   Zone: V1-Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: Mail_Server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 1.1.1.10/32
   Zone: V1-Trust

6. **路由**

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: vlan1(trust-vr)
   Gateway IP Address: 1.1.1.250
   Metric: 1

7. **政策**

   Policies > (From: V1-Trust, To: V1-Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: Any
   Action: Permit

   Policies > (From: V1-Untrust, To: V1-Trust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Mail_Server
   Service: Mail
   Action: Permit

   Policies > (From: V1-Untrust, To: V1-Trust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), FTP_Server
   Service: FTP-GET
   Action: Permit

CLI

1. **VLAN1**
   set interface vlan1 ip 1.1.1.1/24
   set interface vlan1 manage web
   set interface vlan1 manage telnet
   set interface vlan1 manage ping

2. **Telnet**
   set admin telnet port 4646

注意 : Telnet 的預設連接埠號碼爲 23。建議將此號碼變更爲 1024 和 32,767 之間的數字，以防止對組態的未授權存取。稍後登入 Telnet 以管理裝置時，輸入下面的位址 : 1.1.1.1 4646。

---

3. **介面**
   set interface ethernet1 ip 0.0.0.0/0
   set interface ethernet1 zone v1-trust
   set interface ethernet3 ip 0.0.0.0/0
   set interface ethernet3 zone v1-untrust

4. **V1-Trust 區域**
   set zone v1-trust manage web
   set zone v1-trust manage telnet
   set zone v1-trust manage ping

5. **位址**
   set address v1-trust FTP_Server 1.1.1.5/32
   set address v1-trust Mail_Server 1.1.1.10/32

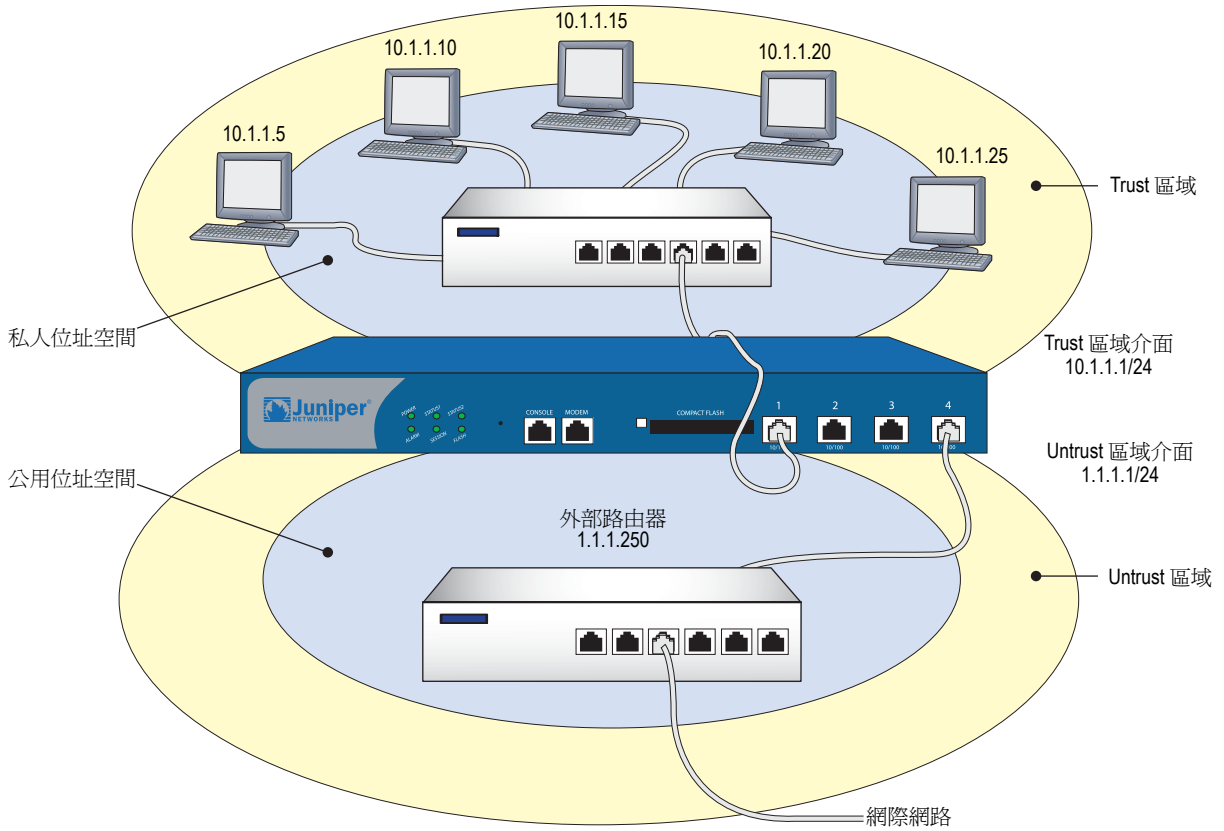
6. **路由**
   set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250 metric 1

7. **政策**
   set policy from v1-trust to v1-untrust any any any permit
   set policy from v1-untrust to v1-trust any Mail_Server mail permit
   set policy from v1-untrust to v1-trust any FTP_Server ftp-get permit
   save

NAT 模式

入口介面處於「網路位址轉譯 (NAT)」模式中時，安全性裝置的作用與 Layer 3 (第 3 層) 交換機 (或路由器) 相似，轉譯目的地爲 Untrust 區域向外 IP 封包標頭中的兩個元件 : 其來源 IP 位址和來源連接埠號碼。安全性裝置會以 Untrust 區域介面的 IP 位址取代通訊流量來源主機的來源 IP 位址。此外，用另一個由安全性裝置產生的隨機連接埠號碼取代來源連接埠號碼。

圖 55: NAT 拓樸



當回覆封包到達安全性裝置時，該裝置轉譯向內封包 IP 標頭中的兩個元件 : 目的地位址和連接埠號碼，它們被轉譯回原始號碼。然後安全性裝置將該封包轉寄到其目的。

NAT 新增「透明」模式中未提供的一個安全性層級 : 經由入口介面 (NAT 模式) 傳送通訊流量的主機位址絕對不會暴露於出口區域 (如 Untrust 區域) 的主機，除非兩個區域位在相同的虛擬路由設定網路中，且安全性裝置經由動態路由設定通訊協定 (DRP) 將路由傳佈至對等。即使如此，除非您具有允許向內通訊流量通往 Trust 區域位址的政策，否則通訊流量將無法到達該位址。(若您想要在使用 DRP 時隱藏 Trust 區域位址，請將 Untrust 區域置於 untrust-vr，將 Trust 區域置於 trust-vr，然後將 trust-vr 中的內部位址路由匯出至 untrust-vr。)

若安全性裝置使用靜態路由設定與單一虛擬伺服器，則當通訊流量向內時，因爲使用以介面爲基礎的 NAT 之故，內部位址將保持隱藏。您所組態的政策控制向內通訊流量。若您僅使用對應的 IP (MIP) 與虛擬 IP (VIP) 位址作爲向內政策中的目的地，則內部位址仍將維持隱藏。

此外，NAT 也保留對公開 IP 位址的使用。在許多環境中，沒有資源可提供給網路上所有裝置的公開 IP 位址。NAT 服務允許多個私人 IP 位址經由一個或少數公開 IP 位址存取網際網路資源。下面的 IP 位址範圍保留給私人 IP 網路，而且不必在網際網路上設定路由 :

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

向內與向外 NAT 通訊流量

經由 NAT 模式介面傳送通訊流量的主機可初始通往 Untrust 區域的通訊流量 (若政策允許)。ScreenOS 5.0.0 前一版中，位於 NAT 模式介面後的主機是無法接收來自 Untrust 區域的通訊流量的，除非已針對這一點設定好對應的 IP (MIP)、虛擬 IP (VIP) 或 VPN 通道。但在 ScreenOS 5.0.0 中，從任何區域 (包括 Untrust 區域) 向有已啓用 NAT 的介面區域傳送通訊流量時，不需要使用 MIP、VIP 或 VPN。若您想要保持位址的隱密性，或是使用未出現在如網際網路這類公開網路上的私人位址，那麼您還是可以定義 MIP、VIP 或 VPN，以讓通訊流量到達這些位址。但若不需考慮隱密性及私人 IP 位址的問題，那麼來自 Untrust 區域的通訊流量可以到達位於 NAT 模式介面後的主機，而不需使用 MIP、VIP 或 VPN。

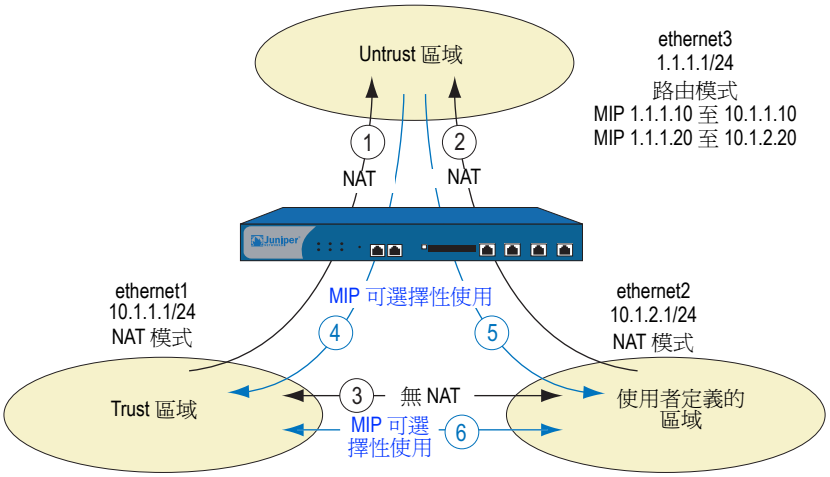
注意 : 您可以僅在連結到 Untrust 區域的介面上定義虛擬 IP (VIP)。

圖 56: NAT 通訊流量

1. 從 Trust 區域到 Untrust 區域的通訊流量上以介面爲基礎的 NAT。
2. 從使用者定義區域到 Untrust 區域的通訊流量上以介面爲基礎的 NAT。

   (注意 : 只有當使用者定義區域與 Untrust 區域位在不同的虛擬路由設計網域時，才能進行上述作業。)
3. Trust 區域和使用者定義區域之間的通訊流量上沒有以介面爲基礎的 NAT。

4 與 5. 您可以使用 MIP、VIP 或 VPN 讓來自 Untrust 區域的通訊流量通往 Trust 區或使用者定義的區域，但並無必要性。



注意 : 如需 MIP 的詳細資訊，請參閱第 **8**-59 頁上的「對應的 IP 位址」。如需 VIP 的詳細資訊，請參閱第 **8**-76 頁上的「虛擬 IP 位址」。

介面設定

對於 NAT 模式，定義下列介面設定，其中 *ip_addr1* 和 *ip_addr2* 代表 IP 位址中的數字，*mask* 代表網路遮罩中的數字，*vlan_id_num* 代表 VLAN 標籤的編號，*zone* 代表區域名稱，*number* 代表以 kbps 爲單位的頻寬大小：

區域介面	設定	區域子介面
使用 NAT 的 Trust、DMZ 和使用者定義的區域	IP: *ip_addr1* Netmask: *mask* Manage IP[1]: *ip_addr2* Traffic Bandwidth[2]: *number* NAT[3]: (選擇)	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone* NAT[3]: (選擇)
Untrust[4]	IP: *ip_addr1* Netmask: *mask* Manage IP[1]: *ip_addr2* Traffic Bandwidth[2]: *number*	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone*

1.您可以以每個介面爲基礎來設定管理 IP 位址。主要目的是爲從網路通訊流量中分離出來的管理通訊流量提供 IP 位址。當特定裝置爲高可用性組態時，也可使用管理 IP 位址來存取。
2.用於通訊流量整理的選擇性設定。
3.選擇 NAT 會將介面模式定義爲 NAT。選擇「路由」會將介面模式定義爲「路由」。
4.雖然可以選擇 NAT 作爲連結到 Untrust 區域的介面模式，但是，安全性裝置不會在該介面上執行任何 NAT 操作。

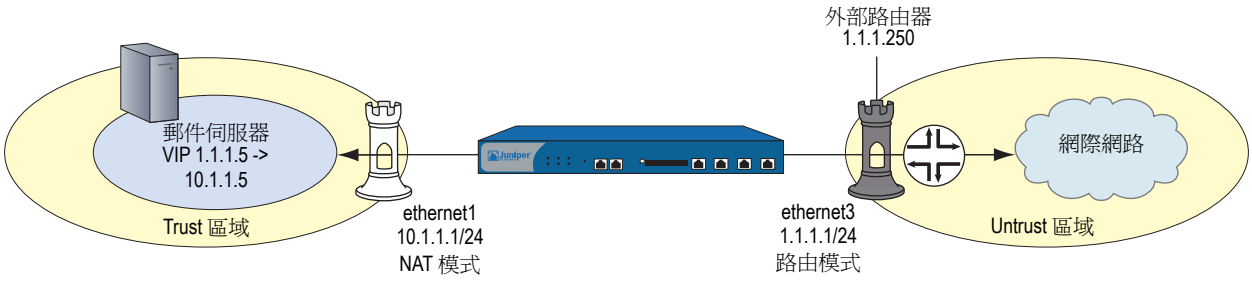
注意： 在 NAT 模式中，您可以使用系統 IP 位址、介面 IP 位址、管理 IP 位址或 MGT IP 位址從任何介面及從多個介面管理安全性裝置。

組態 NAT 模式

下面的範例說明 Trust 區域中有單一子網路的 LAN 的簡單組態。LAN 受 NAT 模式中的安全性裝置保護。政策允許 Trust 區域中所有主機的向外通訊流量和郵件伺服器的向內郵件。向內郵件透過虛擬 IP 位址傳送到郵件伺服器。Trust 區域和 Untrust 區域都在 trust-vr 路由設定網域中。

注意： 將圖 57 與第 96 頁上的圖 59「路由模式中的裝置」中的「路由」模式進行比較。

圖 57: NAT 模式中的裝置



WebUI

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   輸入下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

注意 : 依預設，連結到 Trust 區域的任何介面都在 NAT 模式中。因此，對於連結到 Trust 區域的介面，已啓用此選項。

Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

Zone Name: Untrust
Static IP: (出現時選擇此選項)
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

注意 : 如果安全性裝置上 Untrust 區域中的 IP 位址由 ISP 動態指派，請勿填入 IP 位址和網路遮罩欄位，並選擇 **Obtain IP using DHCP**。如果 ISP 使用經由乙太網路的點對點通訊協定，請選擇 **Obtain IP using PPPoE**，按一下 **Create new PPPoE settings** 連結，然後輸入名稱與密碼。

---

2. **VIP**
   Network > Interfaces > Edit (對於 ethernet3) > VIP: 輸入下面的內容，然後按一下 **Add**:

   Virtual IP Address: 1.1.1.5

   Network > Interfaces > Edit (對於 ethernet3) > VIP > New VIP Service: 輸入下面的內容，然後按一下 **OK**:

   Virtual Port: 25
   Map to Service: Mail
   Map to IP: 10.1.1.5

注意 : 如需有關虛擬 IP (VIP) 位址的資訊，請參閱 第 **8**-76 頁上的「虛擬 IP 位址」。

---

3. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

4. **政策**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

   Policies > (From: Untrust, To: Global) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), VIP(1.1.1.5)
   Service: MAIL
   Action: Permit

CLI

1. **介面**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet3 route

注意： **set interface ethernet***n* **nat** 指令確定安全性裝置以 NAT 模式運作。

如果安全性裝置上 Untrust 區域中的 IP 位址由 ISP 動態指派，使用下面的指令：**set interface untrust dhcp**。如果 ISP 使用「乙太網路上的點對點通訊協定」，使用 **set pppoe** 和 **exec pppoe** 指令。如需詳細資訊，請參閱 *ScreenOS CLI Reference Guide IPv4 Command Descriptions*。

---

2. **VIP**
   set interface ethernet3 vip 1.1.1.5 25 mail 10.1.1.5

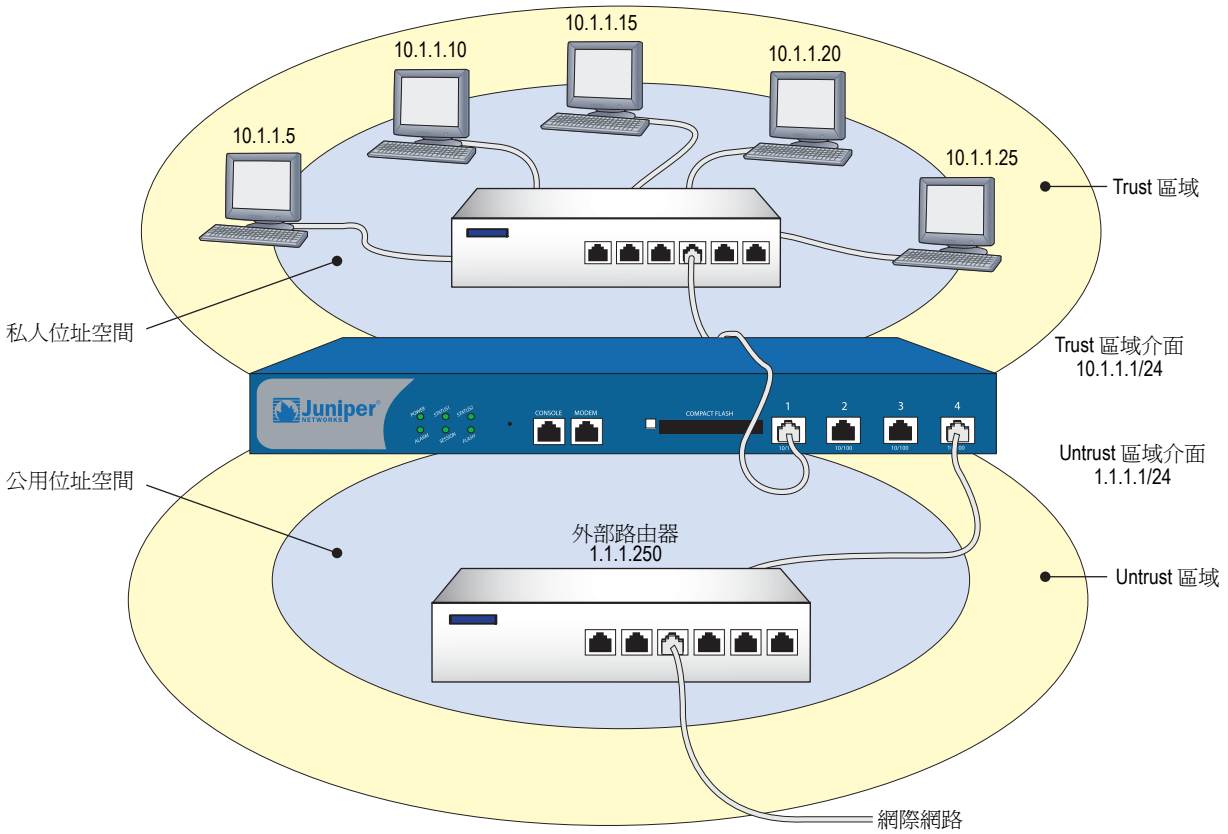
3. **路由**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

4. **政策**
   set policy from trust to untrust any any any permit
   set policy from untrust to global any vip(1.1.1.5) mail permit
   save

路由模式

介面爲「路由」模式時，安全性裝置在不同區域之間路由通訊流量時不會執行來源 NAT (NAT-src)；也就是說，當通訊流量通過安全性裝置時，IP 封包標頭中的來源位址和連接埠號碼保持不變。與 NAT-src 不同的是，若目的地區域介面爲「路由」模式時，您將無需建立對應的 IP (MIP) 與虛擬 IP (VIP) 位址以允許向內通訊流量到達主機。與「透明」模式不同，每個區域中的介面均位於不同的子網路中。

圖 58: NAT 拓樸



您不必爲了讓所有初始向外通訊流量的來源位址轉譯爲目的地區域介面 IP 位址，而在介面層級套用「來源網路位址轉譯」(NAT-src)。您反而可以在政策層級選擇性執行 NAT-src。透過爲向內或向外通訊流量上的指定來源位址建立啓用 NAT-src 的政策，可確定要路由的通訊流量，以及在哪些通訊流量上執行 NAT-src。對於網路通訊流量，可使用 IP 位址或動態 IP (DIP) 集區的目的地區域介面位址，動態 IP 集區與目的地區域介面位在相同的子網路中。對於 VPN 通訊流量，NAT 可使用通道介面 IP 位址，或其相關 DIP 集區的位址。

注意： 如需組態以政策爲基礎的 NAT-src 的詳細資訊，請參閱第 **8**-13 頁上的「來源網路位址轉譯」。

介面設定

對於「路由」模式，定義下列介面設定，其中 *ip_addr1* 和 *ip_addr2* 代表 IP 位址中的數字，*mask* 代表網路遮罩中的數字，*vlan_id_num* 代表 VLAN 標籤的編號，*zone* 代表區域名稱，*number* 代表以 kbps 爲單位的頻寬大小：

表 13: 介面設定

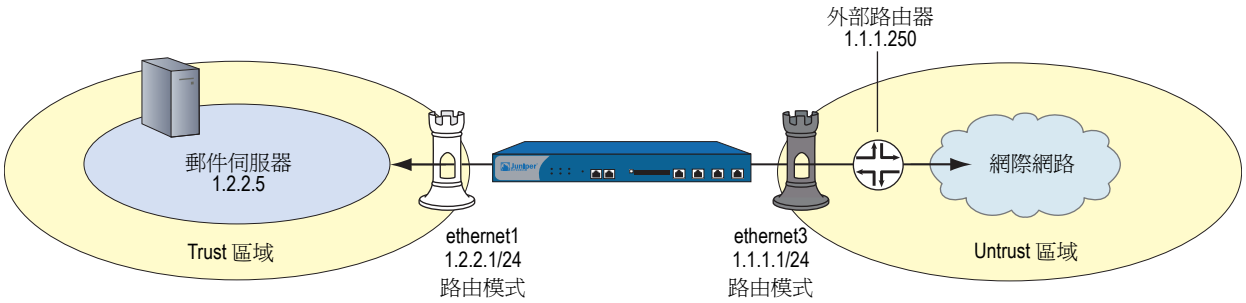
區域介面	設定	區域子介面
Trust、Untrust、DMZ 和使用者定義的區域	IP: *ip_addr1* Netmask: *mask* Manage IP[1]: *ip_addr2* Traffic Bandwidth[2]: *number* Route[3]: (選擇)	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone* Route[3]: (選擇)

1.您可以以每個介面爲基礎來設定管理 IP 位址。主要目的是爲從網路通訊流量中分離出來的管理通訊流量提供 IP 位址。當特定裝置爲高可用性組態時，也可使用管理 IP 位址來存取。
2.用於通訊流量整理的選擇性設定。
3.選擇「路由」會將介面模式定義爲「路由」。選擇 NAT 會將介面模式定義爲 NAT。

組態路由模式

在第 92 頁上的「組態 NAT 模式」中，Trust 區域 LAN 中的主機有私人 IP 位址和郵件伺服器的對應 IP。在下面相同的網路 (由在「路由」模式中操作的安全性裝置保護) 範例中，請注意，主機有公用 IP 位址，而且郵件伺服器不需要 MIP。所有安全區都在 trust-vr 路由設定網域中。

圖 59: 路由模式中的裝置



WebUI

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.2.2.1/24
   輸入下面的內容，然後按一下 **OK**:
   Interface Mode: Route

Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

Zone Name: Untrust
Static IP: (出現時選擇此選項)
IP Address/Netmask: 1.1.1.1/24

注意 : 選擇 **Route**，確定安全性裝置在「路由」模式中執行，不對進出 Trust 區域的通訊流量執行 NAT。

如果安全性裝置上 Untrust 區域中的 IP 位址由 ISP 動態指派，請勿填入 IP 位址和網路遮罩欄位，並選擇 **Obtain IP using DHCP**。如果 ISP 使用經由乙太網路的點對點通訊協定，請選擇 **Obtain IP using PPPoE**，按一下 **Create new PPPoE settings** 連結，然後輸入名稱與密碼。

---

2. 位址

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

Address Name: Mail Server
IP Address/Domain Name:
    IP/Netmask: (選擇), 1.2.2.5/32
Zone: Trust

3. 路由

Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (選擇)
    Interface: ethernet3
    Gateway IP Address: 1.1.1.250

4. 政策

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Any
Service: ANY
Action: Permit

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), Mail Server
Service: MAIL
Action: Permit

CLI

1. 介面
   set interface ethernet1 zone trust
   set interface ethernet1 ip 1.2.2.1/24
   set interface ethernet1 route
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet3 route

注意： **set interface ethernet***number* **route** 指定確定安全性裝置以「路由」模式運作。

---

2. 位址
   set address trust mail_server 1.2.2.5/24

3. 路由
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

4. 政策
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any mail_server mail permit
   save

第 5 章

爲政策建構區塊

本章討論您可在政策中參考的元件或建構區塊。本章包含下列各節：

- 第 100 頁上的「位址」
  - 第 100 頁上的「位址項目」
  - 第 102 頁上的「位址群組」
- 第 104 頁上的「服務」
  - 第 104 頁上的「預先定義的服務」
  - 第 117 頁上的「自訂服務」
  - 第 118 頁上的「設定服務逾時」
  - 第 121 頁上的「定義自訂網際網路控制訊息通訊協定服務」
  - 第 122 頁上的「遠端 Shell 應用程式層閘道」
  - 第 122 頁上的「Sun 遠端程序呼叫應用程式層閘道」
  - 第 123 頁上的「自訂 Microsoft 遠端程序呼叫應用程式層閘道」
  - 第 124 頁上的「即時資料流傳遞通訊協定應用程式層閘道」
  - 第 132 頁上的「服務群組」
- 第 134 頁上的「動態 IP 集區」
  - 第 137 頁上的「相黏 DIP 位址」
  - 第 137 頁上的「在不同子網路中使用 DIP」
  - 第 143 頁上的「在回傳介面上使用 DIP」
  - 第 147 頁上的「建立 DIP 群組」
- 第 150 頁上的「設定遞迴排程」

注意： 如需關於使用者驗證的資訊，請參閱*第 9 卷：使用者驗證*。

位址

ScreenOS 根據位置和網路遮罩分類所有其他裝置的位址。每個區域都有自己的位址和位址群組清單。

個別主機僅具有單一的已定義 IP 位址，因此網路遮罩設定必須設爲 255.255.255.255 (遮罩除本主機以外的所有其他裝置)。

子網路有 IP 位址和網路遮罩 (例如，255.255.255.0 或 255.255.0.0)。

必須先在按區域組織的 ScreenOS 位址清單中爲區域製作項目，然後才能組態政策以允許、拒絕或導向出入個別主機和子網路的通訊流量。

注意： 不需要爲 "Any" 製作位址項目。此術語會自動套用到所有實際位於各自區域中的裝置。

位址項目

您需要先在一個或多個位址清單中定義位址，才能設定許多 Juniper Networks 防火牆、VPN 和通訊流量整理功能。安全區的位址清單包含主機或子網路的 IP 位址或功能變數名稱，其通訊流量將被允許、阻斷、加密或進行使用者驗證。

注意： 必須爲「網域名稱系統 (DNS)」服務組態安全性裝置，才能使用位址項目的網域名稱。如需 DNS 組態的資訊，請參閱第 205 頁上的「網域名稱系統支援」。

若需有關 ScreenOS 命名慣例的資訊 (適用於您爲位址所建立的名稱) 請參閱第 xiv 頁上的「命名慣例和字元類型」。

新增位址

在本範例中，將 IP 位址爲 10.1.10.0/24 的子網路 "Sunnyvale_Eng" 新增爲 Trust 區域中的位址，並將位址 www.juniper.net 新增爲 Untrust 區域中的位址。

WebUI

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

```
Address Name: Sunnyvale_Eng
IP Address/Domain Name:
    IP/Netmask: ( 選擇 ), 10.1.10.0/24
Zone: Trust
```

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

```
Address Name: Juniper
IP Address/Domain Name:
    Domain Name: ( 選擇 ), www.juniper.net
Zone: Untrust
```

CLI

```
set address trust Sunnyvale_Eng 10.1.10.0/24
set address untrust Juniper www.juniper.net
save
```

修改位址

在本範例中，變更位址 "Sunnyvale_Eng" 的位址項目，以反映此部門專責軟體工程設計，且具有不同的 IP 位址 - 10.1.40.0/24。

WebUI

Objects > Addresses > List > Edit (對於 Sunnyvale_Eng): 將名稱和 IP 位址變更爲下面的內容，然後按一下 **OK**:

```
Address Name: Sunnyvale_SW_Eng
IP Address/Domain Name:
        IP/Netmask: ( 選擇 ), 10.1.40.0/24
Zone: Trust
```

CLI

```
unset address trust Sunnyvale_Eng
set address trust Sunnyvale_SW_Eng 10.1.40.0/24
save
```

注意： 在定義位址或位址群組，並將其與政策相關聯後，不能將位址位置變更成其他區域 (例如，從 Trust 區域變更爲 Untrust 區域)。若要變更其位置，必須先將其從底層政策中分離。

刪除位址

在本範例中，移除位址 "Sunnyvale_SW_Eng" 的位址項目。

WebUI

Objects > Addresses > List: 在 Sunnyvale_SW_Eng 的 Configure 欄中按一下 **Remove**。

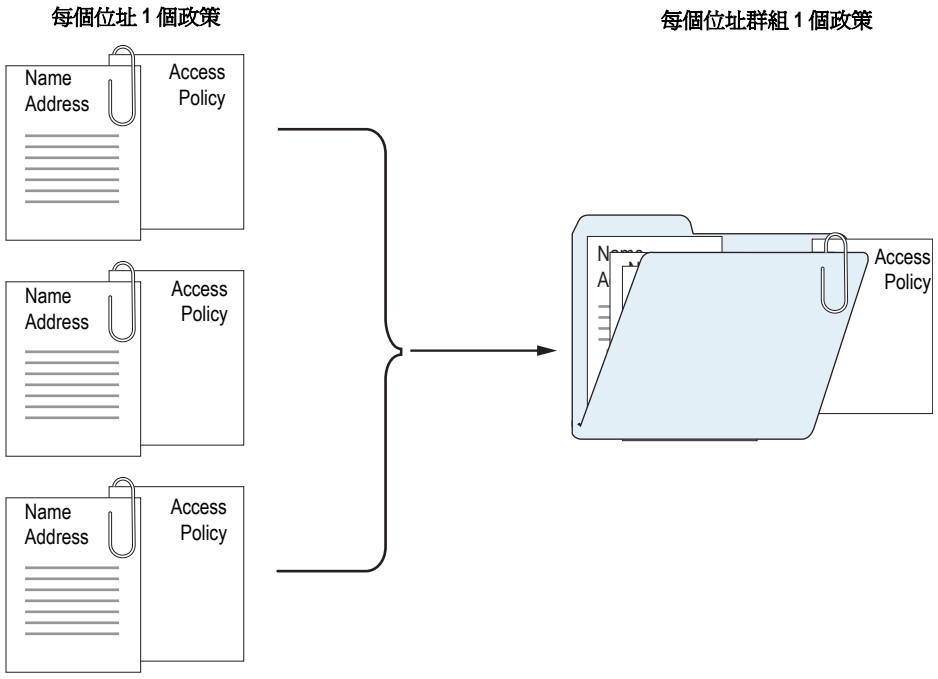
CLI

```
unset address trust "Sunnyvale_SW_Eng"
save
```

位址群組

第 100 頁上的「位址項目」解釋如何建立、修改和刪除個別主機和子網路的通訊錄項目。將位址新增到位址清單中後，就很難控制政策會如何影響每個位址項目。ScreenOS 讓您可以建立位址群組。您可以管理少數的群組，而不用管理大量的位址項目。對群組的變更會套用到群組中的每個位址項目。

圖 60: 位址群組



位址群組選項有下列功能：

- 您可以在任何區域中建立位址群組。
- 您可以建立包含現有使用者的位址群組，或者可以建立空的位址群組，並稍後填入使用者。
- 位址群組可以是其他位址群組的成員。

注意： 爲確保群組不會誤將自身作爲成員包含在群組內，安全性裝置會在您將群組新增至另一群組時執行完整的檢查。例如，若您將群組 A 作爲成員新增至群組 B，安全性裝置即會自動檢查群組 B 並未作爲成員包含在群組 A 中。

- 您可以政策中的參考位址群組項目，如個別通訊錄項目。
- ScreenOS 透過在內部爲每個群組成員建立個別政策，將政策套用到群組的每個成員。您只需要爲群組建立一個政策，但 ScreenOS 實際上爲群組中的每個成員（以及爲每個使用者組態的每項服務）都建立了內部政策。

注意： 由於安全性裝置會自動將政策套用到每個位址群組成員，因此不需要逐一爲每個位址建立政策。此外，ScreenOS 也將這些政策寫入 ASIC，增快查詢執行的速度。

- 當您刪除通訊錄中的個別通訊錄項目時，安全性裝置即會自動將之從所屬的所有群組中移除。

下列限制會套用到位址群組 :

- 位址群組只能包含屬於相同區域的位址。
- 位址名稱不能與群組名稱相同。如果名稱 "Paris" 用於個別的位址項目，就不能當作群組名稱使用。
- 如果在政策中參考位址群組，就不能移除群組。但是可以進行編輯。
- 將單一政策指派給位址群組時，政策會個別套用到每個群組成員，而且安全性裝置將爲存取控制清單 (ACL) 中的每個成員都製作一個項目。如果不夠謹慎，可能會超過可用政策資源的數目，尤其是在來源位址和目的地位址都是位址群組，而且指定服務是服務群組時。
- 不能將預先定義的位址 : "Any"、"All Virtual Ips" 和 "Dial-Up VPN" 新增到群組中。

建立位址群組

在下面的範例中，建立名稱爲 "HQ 2nd Floor" 的群組，其中包括 "Santa Clara Eng" 和 "Tech Pubs" 兩個位址，都已輸入 Trust 區域的通訊錄。

WebUI

Objects > Addresses > Groups > (對於區域 : Trust) New: 輸入下面的群組名稱，移動下列位址，然後按一下 **OK**:

Group Name: HQ 2nd Floor

選擇 **Santa Clara Eng**，然後使用按鈕 < < 將位址從 Available Members 欄中移動到 Group Members 欄中。

選擇 **Tech Pubs**，然後使用按鈕 < < 將位址從 Available Members 欄中移動到 Group Members 欄中。

CLI

```
set group address trust "HQ 2nd Floor" add "Santa Clara Eng"
set group address trust "HQ 2nd Floor" add "Tech Pubs"
save
```

編輯位址群組項目

在本範例中，將 "Support" (已輸入通訊錄的位址) 新增到 "HQ 2nd Floor" 位址群組中。

WebUI

Objects > Addresses > Groups > (對於區域 : Trust) Edit (對於 HQ 2nd Floor): 移動下面的位址，然後按一下 **OK**:

選擇 **Support**，然後使用按鈕 < < 將位址從 Available Members 欄中移動到 Group Members 欄中。

CLI

```
set group address trust "HQ 2nd Floor" add Support
save
```

移除成員與群組

在本範例中，從 HQ 2nd Floor 位址群組中移除成員 "Support"，並刪除之前已建立的 "Sales" 位址群組。

WebUI

Objects > Addresses > Groups > (對於區域 : Trust) Edit (對於 HQ 2nd Floor): 移動下面的位址，然後按一下 **OK**:

選擇 **Support**，然後使用按鈕 > > 將位址從 Group Members 欄中移動到 Available Members 欄中。

Objects > Addresses > Groups > (對於區域 : Trust): 在 Sales 的 Configure 欄中按一下 **Remove**。

CLI

```
unset group address trust "HQ 2nd Floor" remove Support
unset group address trust Sales
save
```

注意： 安全性裝置不會自動刪除已經移除其中所有名稱的群組。

服務

服務是通訊流量的類型，有適用的通訊協定標準。每項服務都有一個與其聯結的傳輸通訊協定和目的地連接埠號碼，例如 FTP 爲 TCP/ 連接埠號 21，Telnet 爲 TCP/ 連接埠號 23。建立政策時，必須爲它指定服務。可以從服務簿中選擇一個預先定義的服務或您建立的自訂服務或服務群組。透過檢視 Policy Configuration 頁中的 Service 下拉式清單 (WebUI)，或使用 **get service** 指令 (CLI)，您可以查看能夠在政策中使用的服務。

預先定義的服務

可使用 WebUI 或 CLI 檢視安全性裝置上的預先定義清單、自訂服務或服務群組。

- 使用 WebUI:
  - Objects > Services > Predefined
  - Objects > Services > Custom
  - Objects > Services > Groups
- 使用 CLI:

  ```
  get service [ group | predefined | user ]
  ```

注意 : 每一個預先定義的服務皆具有範圍 1-65535 的來源連接埠，包含所有有效連接埠號碼組。如此可避免潛在的攻擊者利用此範圍之外的來源連接埠取得存取權。若您需針對任何預先定義的服務使用不同的來源連接埠範圍，請建立自訂服務。如需詳細資訊，請參閱第 117 頁上的「自訂服務」。

本節包含與下列預先定義服務有關的資訊 :

- 第 105 頁上的「網際網路控制訊息通訊協定」
- 第 108 頁上的「網際網路相關的預先定義服務」
- 第 109 頁上的「Microsoft 遠端程序呼叫服務」
- 第 111 頁上的「動態路由設定通訊協定」
- 第 112 頁上的「資料流視訊」
- 第 113 頁上的「Sun 遠端程序呼叫服務」
- 第 113 頁上的「安全性與通道服務」
- 第 114 頁上的「IP 相關服務」
- 第 114 頁上的「即時通訊服務」
- 第 114 頁上的「管理服務」
- 第 115 頁上的「郵件服務」
- 第 116 頁上的「UNIX 服務」
- 第 116 頁上的「雜項服務」

您可以在下列頁面中找到部份所列項目的詳細資訊 :

- 第 121 頁上的「定義自訂網際網路控制訊息通訊協定服務」
- 第 122 頁上的「遠端 Shell 應用程式層閘道」
- 第 122 頁上的「Sun 遠端程序呼叫應用程式層閘道」
- 第 123 頁上的「自訂 Microsoft 遠端程序呼叫應用程式層閘道」
- 第 124 頁上的「即時資料流傳遞通訊協定應用程式層閘道」

網際網路控制訊息通訊協定

「網際網路控制訊息通訊協定」(ICMP) 是 IP 的一部份，可查詢網路 (ICMP 查詢訊息) 和接收網路傳回之反饋以獲得錯誤模式 (ICMP 錯誤訊息)。不過，ICMP 並不保證能傳輸錯誤訊息或報告所有遺失的資料電報，其並非可靠的通訊協定。ICMP 代碼及類型代碼可說明「ICMP 查詢訊息」及「ICMP 錯誤訊息」。

您可以選擇允許或拒絕任何或特定類型的 ICMP 訊息，以提升網路安全性。有些 ICMP 訊息類型可用來取得可能犧牲安全性的網路相關資訊。例如，可建構 ICMP、TCP 或 UDP 封包來傳回包含網路相關資訊 (如其拓樸) 的 ICMP 錯誤訊息，並存取清單過濾特性。下表列出 ICMP 訊息名稱、相應代碼、類型及說明。

ICMP 訊息名稱	代碼	類型	說明
ICMP-ANY	所有	所有	ICMP-ANY 影響任何使用 ICMP 的通訊協定。 拒絕 ICMP-ANY 會損及使用 ICMP 進行 ping 嘗試及監看網路的作業。 允許 ICMP-ANY 會允許所有 ICMP 訊息。
ICMP-ADDRESS-MASK ■ Request ■ Reply	 17 18	 0 0	「ICMP 位址遮罩查詢」適用於需使用來自開機伺服器之本地子網路遮罩的系統。 「拒絕 ICMP 位址遮罩」要求訊息會對無磁碟系統造成不利的影響。 「允許 ICMP 位址遮罩」要求訊息可能會允許其他人識別您網路中主機之作業系統。
ICMP-DEST-UNREACH	3	0	「ICMP 目的地無法到達錯誤」訊息指出該目的地主機已被設定爲拒絕封包。 代碼 0、1、4 或 5 可來自於某閘道。代碼 2 或 3 來自某主機 (RFC 792)。 「拒絕 ICMP 目的地無法到達錯誤」訊息可移除安全性裝置後有一主機開啓且運行中這一假定。 「允許 ICMP 目的地無法到達錯誤」訊息可允許設定關於網路的某些假定，如安全性過濾。
ICMP Fragment Needed	3	4	「ICMP 分段錯誤」訊息指出需要進行分段作業，但已設定不進行分段作業旗標。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。
ICMP 片段重組	11	1	「ICMP 片段重組超時錯誤」指出正在重組片段訊息的主機耗盡了時間，已卸除封包。有時候會傳送此訊息。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。
ICMP-HOST-UNREACH	3	1	「ICMP 主機無法到達錯誤」訊息指出路由設定表項目將或未將某特定主機列爲無限大。有時候，當接收到要求分段作業的封包但無法分段時，閘道便會傳送此錯誤訊息。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。 允許這些訊息會讓其他人可以藉由淘汰程序或進行閘道與分段相關假定來判定您的內部主機 IP 位址。
ICMP-INFO ■ Request ■ Reply	 15 16	 0 0	「ICMP-INFO 查訊」訊息允許無磁碟的主機系統查詢網路及進行自我組態。 「拒絕 ICMP 位址遮罩」要求訊息會對無磁碟系統造成不利的影響。 「允許 ICMP 位址遮罩」要求訊息可能會讓其他人將資訊查詢廣播至網路片段，來判定電腦類型。

ICMP 訊息名稱	代碼	類型	說明
ICMP-PARAMETER-PROBLEM	12	0	「ICMP 參數問題錯誤」訊息會在提供不正確的標頭參數且造成封包遭到丟棄時通知您 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。 「允許 ICMP 參數問題」錯誤訊息允許其他人針對您的網路進行相關假定。
ICMP-PORT-UNREACH	3	3	「ICMP 連接埠無法到達錯誤」訊息指出要求特定連接埠的閘道處理資料電報不可用或在網路中不受支援。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。 「允許 ICMP 連接埠無法到達錯誤」訊息允許其他人判定您針對特定通訊協定使用哪些連接埠。
ICMP-PROTOCOL-UNREACH	3	2	「ICMP 通訊協定無法到達錯誤」訊息指出要求特定通訊協定的閘道處理資料電報不可用或在網路中不受支援。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。 「允許 ICMP 通訊協定無法到達錯誤」訊息允許其他人判定您的網路執行哪些通訊協定。
ICMP-REDIRECT	5	0	「ICMP 重新定向網路錯誤」訊息由路由器傳送。 建議拒絕這些從網際網路 (untrust) 通往受信任網路的訊息。
ICMP-REDIRECT-HOST	5	1	ICMP 重新定向訊息指出通往特定主機的資料電報將沿著另一條路徑傳送。
ICMP-REDIRECT-TOS-HOST	5	3	「ICMP 重新定向服務類型 (TOS) 及主機錯誤」是一種訊息類型。
ICMP-REDIRECT-TOS-NET	5	2	「ICMP 重新定向 TOS 及網路錯誤」是一種訊息類型。
ICMP-SOURCE-QUENCH	4	0	「ICMP 來源抑制錯誤」訊息指出路由器沒有可以用來接受、佇列及傳送封包至下一躍點的緩衝區空間。 拒絕這些訊息不會促進或損及內部網路效能。 允許這些訊息可允許其他人得知路由器擁塞，使其成爲可行的攻擊目標。
ICMP-SOURCE-ROUTE-FAIL	3	5	ICMP 來源路由失敗錯誤訊息 建議拒絕這些來自網際網路 (untrust) 的訊息。
ICMP-TIME-EXCEEDED	11	0	「ICMP 活動時間 (TTL) 超時錯誤」訊息指出在封包到達其目的地之前，此封包的 TTL 設定已達到零。如此可確保先丟棄較舊的封包後再處理重新傳送的封包。 建議拒絕這些來自受信任網路通往網際網路的訊息。
ICMP-TIMESTAMP			「ICMP-TIMESTAMP 查詢」訊息提供在大型、不同的網路中同步化時間及協調時間分配的機制。
■ Request	13	0	
■ Reply	14	0	

ICMP 訊息名稱	代碼	類型	說明
Ping (ICMP ECHO)	8	0	Packet Internet Groper 是一種用來判定某特定主機是否可由其 IP 位址 .0/0 回應回覆存取的公用程式。 拒絕 ping 功能您將無法查看某主機是否在活動中。 允許 ping 可允許其他人執行服務中斷 (DoS) 或 Smurf 攻擊。
ICMP-ECHO-FRAGMENT-ASSEMBLY-EXPIRE	11	1	「ICMP 片段回應重組時間過時」錯誤訊息指出已超過重組時間。 建議拒絕這些訊息。
Traceroute ■ Forward ■ Discard	 30 30	 0 1	Traceroute 是用來指出存取特定主機路徑的公用程式。 建議拒絕這一從網際網路 (untrust) 通往您內部網路 (trust) 的公用程式。

網際網路相關的預先定義服務

下表列出了網際網路相關的預先定義服務。視您的網路需求而定，您可以選擇允許或拒絕任何或所有此類服務。每一個項目將列出服務名稱、預設接收連接埠及服務說明。

服務名稱	連接埠	服務說明
AOL	5190-5193	America Online Internet Service Provider (ISP) 提供網際網路、聊天及即時通訊服務。
DHCP-Relay	67 (預設)	動態主機組態。
DHCP	68 用戶端 67 伺服器	「動態主機組態通訊協定」會配置網路位址，並將組態參數由伺服器傳送至主機。
DNS	53	「網域名稱系統」將網域名稱轉譯爲 IP 位址。
FTP ■ FTP-Get ■ FTP-Put	 20 資料 21 控制	「檔案傳輸通訊協定」(FTP) 允許在機器間傳送及接收檔案。您可以選擇拒絕或允許 ANY (GET 或 PUT) 或選擇性允許或拒絕 GET 或 PUT。GET 接收來自另一台機器的檔案，PUT 則將檔案傳送至另一台機器。 建議拒絕來自不受信任來源 (網際網路) 的 FTP 服務。
Gopher	70	Gopher 可整理網際網路伺服器的內容，並使其以階層式結構的檔案清單顯示。 建議拒絕 Gopher 存取，以避免暴露您的網路結構。
HTTP	8080	「超文字傳輸通訊協定」是「全球資訊網」(WWW) 使用的基本通訊協定。 拒絕 HTTP 服務將使您的使用者無法檢視網際網路。 允許 HTTP 服務會允許受信任的主機檢視網際網路。
HTTP-EXT	-	具擴充非標準連接埠的「超文字傳輸通訊協定」

服務名稱	連接埠	服務說明
HTTPS	443	具「安全通訊端階層」(SSL) 的「超文字傳輸通訊協定」是用於透過網際網路傳輸私人文件的通訊協定。 拒絕 HTTPS 會使您的使用者無法在網際網路上購物且無法存取某些要求安全密碼交換的線上資源。 允許 HTTPS 可讓受信任的主機參與密碼交換、線上購物及造訪各種要求使用者登入的受保護線上資源。
網際網路定址器服務	-	「網際網路定址器服務」包括 LDAP、「使用者定址器服務」及「經由 TSL/SSL 的 LDAP」。
IRC	6665-6669	「網際網路聊天室」(IRC) 允許連線至網際網路的人加入即時交談。
LDAP	389	「輕量目錄存取通訊協定」是一組用來存取資訊目錄的通訊協定。
PC-Anywhere	-	PC-Anywhere 是一種遠端控制及檔案傳輸軟體。
TFTP	69	TFTP 是用於簡單檔案傳輸的通訊協定。
WAIS	-	Wide Area Information Server 是一種可在網際網路上尋找文件的程式。

Microsoft 遠端程序呼叫服務

下表列出預先定義的 Microsoft 服務、服務相關參數及服務簡短說明。參數包括通用唯一識別碼 (UUID) 及 TCP/UDP 來源與目的地連接埠。UUID 是從一個硬體位址、時戳及種子值產生而來的 128 位元唯一碼。

服務	參數 /UUID	說明
MS-RPC-EPM	135 e1af8308-5d1f-11c9-91a4-08002b14a0fa	Microsoft 遠端程序呼叫 (RPC) 端點對應表 (EPM) 通訊協定
MS-RPC-ANY	-	任何 Microsoft 遠端程序呼叫 (Remote Procedure Call，RPC) 服務
MS-AD	4 個成員	Microsoft Active Directory 服務群組包括 : ■ MS-AD-BR ■ MS-AD-DRSUAPI ■ MS-AD-DSROLE ■ MS-AD-DSSETUP
MS-EXCHANGE	6 個成員	Microsoft Exchange 服務群組包括 : ■ MS-EXCHANGE-DATABASE ■ MS-EXCHANGE-DIRECTORY ■ MS-EXCHANGE-INFO-STORE ■ MS-EXCHANGE-MTA ■ MS-EXCHANGE-STORE ■ MS-EXCHANGE-SYSATD

服務	參數 /UUID	說明
MS-IIS	6 個成員	Microsoft IIS Server 服務群組包括 : ■ MS-IIS-COM ■ MS-IIS-IMAP4 ■ MS-IIS-INETINFO ■ MS-IIS-NNTP ■ MS-IIS-POP3 ■ MS-IIS-SMTP
MS-AD-BR	ecec0d70-a603-11d0-96b1-00a0c91ece30 16e0cf3a-a604-11d0-96b1-00a0c91ece30	Microsoft Active Directory 備份與還原服務
MS-AD-DRSUAPI	e3514235-4b06-11d1-ab04-00c04fc2dcd2	Microsoft Active Directory 複寫服務
MS-AD-DSROLE	1cbcad78-df0b-4934-b558-87839ea501c9	Microsoft Active Directory DSROLE 服務
MS-AD-DSSETUP	3919286a-b10c-11d0-9ba8-00c04fd92ef5	Microsoft Active Directory 設定服務
MS-DTC	906b0ce0-c70b-1067-b317-00dd010662da	Microsoft 分散式異動協調器服務
MS-EXCHANGE-DATABASE	1a190310-bb9c-11cd-90f8-00aa00466520	Microsoft Exchange 資料庫服務
MS-EXCHANGE-DIRECTORY	f5cc5a18-4264-101a-8c59-08002b2f8426 f5cc5a7c-4264-101a-8c59-08002b2f8426 f5cc59b4-4264-101a-8c59-08002b2f8426	Microsoft Exchange 目錄服務
MS-EXCHANGE-INFO-STORE	0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde 1453c42c-0fa6-11d2-a910-00c04f990f3b 10f24e8e-0fa6-11d2-a910-00c04f990f3b 1544f5e0-613c-11d1-93df-00c04fd7bd09	Microsoft Exchange 資訊儲存服務
MS-EXCHANGE-MTA	9e8ee830-4459-11ce-979b-00aa005ffebe 38a94e72-a9bc-11d2-8faf-00c04fa378ff	Microsoft Exchange MTA 服務
MS-EXCHANGE-STORE	99e66040-b032-11d0-97a4-00c04fd6551d 89742ace-a9ed-11cf-9c0c-08002be7ae86 a4f1db00-ca47-1067-b31e-00dd010662da a4f1db00-ca47-1067-b31f-00dd010662da	Microsoft Exchange 儲存服務
MS-EXCHANGE-SYSATD	67df7c70-0f04-11ce-b13f-00aa003bac6c f930c514-1215-11d3-99a5-00a0c9b61b04 83d72bf0-0d89-11ce-b13f-00aa003bac6c 469d6ec0-0d87-11ce-b13f-00aa003bac6c 06ed1d30-d3d3-11cd-b80e-00aa004b9c30	Microsoft Exchange System Attendant 服務
MS-FRS	f5cc59b4-4264-101a-8c59-08002b2f8426 d049b186-814f-11d1-9a3c-00c04fc9b232 a00c021c-2be2-11d2-b678-0000f87a8f8e	Microsoft 檔案複寫服務
MS-IIS-COM	70b51430-b6ca-11d0-b9b9-00a0c922e750 a9e69612-b80d-11d0-b9b9-00a0c922e70	Microsoft 網際網路資訊伺服器 COM GUID/UUID 服務
MS-IIS-IMAP4	2465e9e0-a873-11d0-930b-00a0c90ab17c	Microsoft 網際網路資訊伺服器 IMAP4 服務
MS-IIS-INETINFO	82ad4280-036b-11cf-972c-00aa006887b0	Microsoft 網際網路資訊伺服器管理服務
MS-IIS-NNTP	4f82f460-0e21-11cf-909e-00805f48a135	Microsoft 網際網路資訊伺服器 NNTP 服務
MS-IIS-POP3	1be617c0-31a5-11cf-a7d8-00805f48a135	Microsoft 網際網路資訊伺服器 POP3 服務

服務	參數 /UUID	說明
MS-IIS-SMTP	8cfb5d70-31a4-11cf-a7d8-00805f48a135	Microsoft 網際網路資訊伺服器 SMTP 服務
MS-ISMSERV	68dcd486-669e-11d1-ab0c-00c04fc2dcd2 130ceefb-e466-11d1-b78b-00c04fa32883	Microsoft 站台間傳訊服務
MS-MESSENGER	17fdd703-1827-4e34-79d4-24a55c53bb37 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc	Microsoft Messenger 服務
MS-MQQM	fdb3a030-065f-11d1-bb9b-00a024ea5525 76d12b80-3467-11d3-91ff-0090272f9ea3 1088a980-eae5-11d0-8d9b-00a02453c33 5b5b3580-b0e0-11d1-b92d-0060081e87f0 41208ee0-e970-11d1-9b9e-00e02c064c39	Microsoft Windows 訊息佇列管理服務
MS-NETLOGON	12345678-1234-abcd-ef00-01234567cffb	Microsoft Netlogon 服務
MS-SCHEDULER	1ff70682-0a51-30e8-076d-740be8cee98b 378e52b0-c0a9-11cf-822d-00aa0051e40f 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53	Microsoft Scheduler 服務
MS-WIN-DNS	50abc2a4-574d-40b3-9d66-ee4fd5fba076	Microsoft Windows DNS 伺服器
MS-WINS	45f52c28-7f9f-101a-b52b-08002b2efabe 811109bf-a4e1-11d1-ab54-00a0c91e9b45	Microsoft WINS 服務

動態路由設定通訊協定

視您的網路需求而定，您可選擇允許或拒絕從這些動態路由設定通訊協定的封包產生而來的訊息。下表依據名稱、連接埠及說明列出各個受支援的動態路由設定通訊協定。

動態路由設定通訊協定	連接埠	說明
RIP	520	RIP 是一種常見的距離向量路由設定通訊協定。
OSPF	89	OSPF 是一種常見的連結狀態路由設定通訊協定。
BGP	179	BGP 是一種外部 / 內部網域路由設定通訊協定。

資料流視訊

下表列依據名稱列出各個受支援的資料流視訊服務，並包含預設連接埠與說明。視您的網路需求而定，您可以選擇允許或拒絕任何或所有此類服務。

服務	連接埠	說明
H.323	TCP 來源 1-65535；TCP 目的地 1720、1503、389、522、1731 UDP 來源 1-65535；UDP 來源 1719	H.323 是由「國際電信聯盟」(ITU) 核准的標準，其定義音訊及視訊會議資訊如何透過網路傳輸。
NetMeeting	TCP 來源 1-65535；TCP 目的地 1720、1503、389、522 UDP 來源 1719	Microsoft NetMeeting 使用 TCP 透過網際網路提供電信會議 (視訊及音訊) 服務。
Real media	TCP 來源 1-65535；TCP 目的地 7070	Real Media 是一種資料流視訊與音訊技術。
RTSP	554	用於資料流媒體應用程式的「即時資料流通訊協定」(RTSP)
SIP	5056	「會話初始化通訊協定」(SIP) 是一種應用程式層的控制通訊協定，用於建立、修改及終止會話。
VDO Live	TCP 來源 1-65535；TCP 目的地 7000-7010	VDOLive 是一種可調適的視訊資料流技術。

Sun 遠端程序呼叫服務

下表列出各個 Sun「遠端程序呼叫應用程式層閘道」(RPC ALG) 的服務名稱、參數及全名。

服務	程式編號	全名
SUN-RPC-PORTMAPPER	111 100000	Sun RPC 連接埠對應表通訊協定
SUN-RPC-ANY	ANY	任何 Sun RPC 服務
SUN-RPC-PROGRAM-MOUNTD	100005	Sun RPC 裝載端口監控程式
SUN-RPC-PROGRAM-NFS	100003 100227	Sun RPC 網路檔案系統
SUN-RPC-PROGRAM-NLOCKMGR	100021	Sun RPC 網路鎖定管理員
SUN-RPC-PROGRAM-RQUOTAD	100011	Sun RPC 遠端配額監控程式
SUN-RPC-PROGRAM-RSTATD	100001	Sun RPC 遠端狀態監控程式
SUN-RPC-PROGRAM-RUSERD	100002	Sun RPC 遠端使用者監控程式
SUN-RPC-PROGRAM-SADMIND	100232	Sun RPC 系統管理監控程式
SUN-RPC-PROGRAM-SPRAYD	100012	Sun RPC SPRAY 監控程式
SUN-RPC-PROGRAM-STATUS	100024	Sun RPC STATUS
SUN-RPC-PROGRAM-WALLD	100008	Sun RPC WALL 監控程式
SUN-RPC-PROGRAM-YPBIND	100007	SUN RPC 黃頁連結服務

安全性與通道服務

下表列出各個受支援的服務，並提供連接埠與各項目說明。

服務	連接埠	說明
IKE	UDP 來源 1-65535；UDP 目的地 500 4500 (用於 NAT-Traversal)	IKE 是一種用來取得已驗證金鑰製作材料以與 ISAKMP 搭配使用的通訊協定。 組態自動 IKE 時，您可以從三個預先定義的「階段 1」或「階段 2」提案中選擇 : ■ 標準 : AES 與 3DES ■ 基本 : DES 與兩個不同類型的驗證演算法 ■ 相容 : 四個常用的驗證及加密演算法
L2TP	1723	L2TP 結合了「點對點通道通訊協定」(PPTP) 及「第二層轉寄」(L2F) 來進行遠端存取。
PPTP	-	「點對點通道通訊協定」允許企業經由公開網際網路上的私人*通道*擴充其自身的私人網路。

IP 相關服務

下表列出了預先定義的 IP 相關服務。每一個項目都包括預設連接埠及服務說明。

服務	連接埠	說明
Any	-	任何服務
TCP-ANY	1-65535	使用「傳輸控制通訊協定」的任何通訊協定
		TCPMUX 連接埠 1
UDP-ANY	137	使用「使用者資料電報通訊協定」的任何通訊協定

即時通訊服務

下表列出了預先定義的網際網路即時通訊服務。每一個項目都包括服務名稱、預設或指定的連接埠及服務說明。

服務	連接埠	說明
Gnutella	6346 (預設)	「Gnutella 檔案共享通訊協定」是一種在分配網路上執行的公開網域檔案共享通訊協定。您可指定任意連接埠，但預設連接埠爲 6346。
MSN	1863	Microsoft Network Messenger 是一種允許您傳送即時訊息及線上交談的公用程式。
NNTP	119	「網路新聞傳輸通訊協定」是一種用來張貼、散佈及擷取 USENET 訊息的通訊協定。
SMB	445	「IP 上的伺服器訊息區 (SMB) 通訊協定」允許您讀取網路上的檔案，並可將檔案寫入網路上的伺服器。
YMSG	5010	Yahoo! Messenger 是一種允許您檢視其他人是否上線、傳送即時訊息及線上交談的公用程式。

管理服務

下表列出了預先定義的管理服務。每一個項目都包括服務名稱、預設或指定的連接埠及服務說明。

服務	連接埠	說明
NBNAME	137	「NetBIOS 名稱服務」顯示所有在 UDP 連接埠 137 上傳送的 NetBIOS 名稱封包。
NDBDS	138	由 IBM 公佈的「NetBIOS 資料電報服務」爲與廣播媒體連接的 PC 提供無連線 (資料電報) 服務，以尋找資源、啓動會話和終止會話。其並不可靠，且封包也未定序。
NFS	-	「網路檔案系統」使用 UDP 讓網路使用者存取儲存在不同類型電腦上的共享檔案。SUN RPC 是 NFS 的建構區塊。
NS Global	-	NS-Global 是 Juniper Networks 防火牆 /VPN 裝置的中央管理通訊協定。
NS-Global PRO	-	NS Global-PRO 是 Juniper Networks 防火牆 /VPN 裝置系列的可調適監看系統。
NSM	-	NetScreen-Security Manager

服務	連接埠	說明
NTP	123	「網路時間通訊協定」爲電腦提供一種同步化時間指示物的方法。
RLOGIN	513	RLOGIN 可在遠端主機上開始一終端會話。
RSH	514	RSH 可在遠端主機上執行 Shell 指令。
SNMP	161	「簡易網路管理通訊協定」是一組用於管理複雜網路的通訊協定。
SQL*Net V1	66	SQL*Net Version 1 是一種資料庫語言，可用於建立、存取、修改及保護資料。
SQL*Net V2	66	SQL*Net Version 2 是一種資料庫語言，可用於建立、存取、修改及保護資料。
MSSQL	1433 (預設實例)	Microsoft SQL 是一種專有資料庫伺服器工具，可用於建立、存取、修改及保護資料。
SSH	22	「安全 Shell」是一種在不安全通道上利用強力驗證及安全通訊登入至網路上另一台電腦的程式。
SYSLOG	514	Syslog 是一種 UNIX 程式，可將訊息傳送系統記錄程式。
Talk	517-518	Talk 是一種視訊通訊程式，可將您終端機的指令行複製至另一使用者的終端機上。
Telnet	23	Telnet 是一種 UNIX 程式，其提供以介面連接終端裝置及終端間終端導向程序的標準方法。
WinFrame	-	WinFrame 是一種可讓非 Windows 機器的使用者執行 Windows 應用程式的技術。
X-Windows	-	X-Windows 是一種視窗化及圖形化的系統，Motif 及 OpenLook 均以此系統爲基礎。

郵件服務

下表列出了預先定義的郵件服務。每一個都包括服務名稱、預設或指定的連接埠號碼及服務說明。

服務	連接埠	說明
IMAP	143	「網際網路訊息存取通訊協定」是一種用於擷取訊息的通訊協定。
Mail (SMTP)	25	「簡單郵件傳輸通訊協定」是一種用於在伺服器間傳送訊息的通訊協定。
POP3	110	「郵局通訊協定」是一種用於擷取電子郵件的通訊協定。

UNIX 服務

下表列出了預先定義的 UNIX 服務。每一個項目都包括服務名稱、預設或指定的連接埠及服務說明。

服務	連接埠	說明
FINGER	79	Finger 是一種 UNIX 程式，可提供使用者的相關資訊。
UUCP	117	「Unix 至 Unix 複製通訊協定」(UUCP) 是一種 UNIX 公用程式，允許兩台電腦間透過直接序列或數據機連線進行檔案傳輸。

雜項服務

下表列出了預先定義的雜項服務。每一個項目都包括服務名稱、預設或指定的連接埠及服務說明。

服務	連接埠	說明
CHARGEN	19	「字元產生器通訊協定」是一種以 UDP 或 TCP 爲基礎的除錯與測量工具。
DISCARD	9	「丟棄通訊協定」是一種應用程式層通訊協定，其說明將傳送至連接埠 9 的 TCP 或 UDP 資料丟棄的程序。
IDENT	113	「識別通訊協定」是一種用於 TCP 用戶端驗證的 TCP/IP 應用程式層通訊協定。
LPR	515 聆聽； 721-731 來源範圍 (含)	「線路印表機監控程式通訊協定」是一種用於列印服務的以 TCP 爲基礎的通訊協定。
RADIUS	1812	「遠端驗證撥接使用者服務」是一種用於驗證及帳戶處理的伺服器程式。
SQLMON	1434 (SQL 監看連接埠)	SQL 監看 (Microsoft)
VNC	5800	「虛擬網路運算」可促進檢視其他電腦及與其他電腦或連線至網際網路的行動裝置的互動。
WHOIS	43	「網路目錄服務通訊協定」是一種查詢網域名稱的方式。
IPSEC-NAT	-	IPSEC-NAT 允許針對 ISAKMP 和 ESP 封包進行「網路位址轉譯」。
SCCP	2000	「Cisco 工作站呼叫控制通訊協定」使用訊號發出連接控制連接埠 (SCCP) 來提供高可用性及流量控制。
VOIP	-	「IP 語音通訊服務群組」提供網際網路上的語音服務，包括 H.323 及「會話初始化通訊協定」(SIP)。

自訂服務

不需使用預先定義的服務，您也可以輕鬆建立自訂服務。您可爲每項自訂服務指派下列屬性 :

- 名稱
- 傳輸通訊協定
- 使用 TCP 或 UDP 服務的來源與目的地連接埠號碼
- 使用 ICMP 服務的類型和代碼值
- 逾時值

如果您在虛擬系統 (virtual system，vsys) 中建立一項自訂服務，其名稱與根系統中某個先前定義的自訂服務相同，vsys 中的服務會採用指定傳輸通訊協定 (TCP、UDP 或 ICMP) 的預設逾時值。若要定義 vsys 中某項服務的自訂逾時值，該值與預設值不同，而根系統中具有相同名稱的某個自訂服務有它自己的逾時值，則請以下列順序在 vsys 和根系統中建立自訂服務 :

1. 首先，在 vsys 中以自訂逾時值建立自訂服務。
2. 然後在根系統中以相同名稱但不同逾時值建立另一個自訂服務。

下列範例說明如何新增、修改與移除自訂服務。

注意 : 若需有關 ScreenOS 命名慣例的資訊 (適用於您針對自訂服務所建立的名稱)，請參閱第 xiv 頁上的「命名慣例和字元類型」。

新增自訂服務

若要將自訂服務新增到服務簿中，需要下面的資訊 :

- 服務名稱 : 在本範例中爲 "cust-telnet"。
- 來源連接埠號碼範圍 : 1 - 65535。
- 接收服務要求的目的地連接埠號碼範圍 : 例如 : 23000 - 23000。
- 服務是使用 TCP 通訊協定還是使用 UDP 通訊協定，或者使用網際網路規定定義的一些其他通訊協定。在本範例中，爲 TCP 通訊協定。

WebUI

Objects > Services > Custom > New: 輸入下面的內容，然後按一下 **OK**:

```
Service Name: cust-telnet
Service Timeout: Custom ( 選擇 ), 30 ( 類型 )
Transport Protocol: TCP ( 選擇 )
Source Port Low: 1
Source Port High: 65535
Destination Port Low: 23000
Destination Port High: 23000
```

CLI

```
set service cust-telnet protocol tcp src-port 1-65535 dst-port 23000-23000
set service cust-telnet timeout 30
save
```

注意： 逾時值的單位爲分鐘。如果沒有設定，自訂服務的逾時值爲 180 分鐘。如果不要服務逾時，請輸入 **never**。

修改自訂服務

在本範例中，將目的地連接埠號碼範圍變更爲 23230-23230 以修改自訂服務 "cust-telnet"。

使用 **set service** *service_name* **clear** 指令，在不從服務簿中移除服務的情況下，移除自訂服務的定義：

WebUI

Objects > Services > Custom > Edit (對於 cust-telnet): 輸入下面的內容，然後按一下 **OK**:

Destination Port Low: 23230
Destination Port High: 23230

CLI

```
set service cust-telnet clear
set service cust-telnet + tcp src-port 1-65535 dst-port 23230-23230
save
```

移除自訂服務

在本範例中，移除自訂服務 "cust-telnet"。

WebUI

Objects > Services > Custom: 在 "cust-telnet" 的 Configure 欄中，按一下 **Remove**。

CLI

```
unset service cust-telnet
save
```

設定服務逾時

您針對某項服務所設定的服務逾時值將決定會話逾時。您可針對預先定義的或自訂服務設定逾時臨界值；您可以使用服務預設逾時、指定自訂逾時或完全不使用逾時。虛擬系統 (vsys) 安全性網域中的服務逾時行爲與根層級上的是相同的。

服務逾時組態與查詢

服務逾時值儲存在服務項目資料庫及對應的以 vsys TCP 與 UDP 連接埠爲基礎的逾時表中。設定服務逾時值時，安全性裝置會以新值更新這些表。服務項目資料庫中亦有預設逾時值，此值取自預先定義的服務。您可設定逾時值，但不可改變預設值。

具多重規則項目的服務共用同一個逾時值。若多重服務共用同一個通訊協定及目的地連接埠範圍，則所有服務將共用最新設定的逾時值。

至於單一服務項目，服務逾時查詢處理順序如下 :

1. 服務項目資料庫中的指定逾時 (若已設定)。

2. 服務項目資料庫中的預設逾時 (若已於預先定義的服務中指定)。

3. 以通訊協定爲基礎的預設逾時表。

圖 61: 以通訊協定爲基礎的預設逾時表

通訊協定	預設逾時 (分)
TCP	30
UDP	1
ICMP	1
OSPF	1
其他	30

至於服務群組 (包括在多槽政策組態中建立的隱藏群組) 及預先定義的服務 "ANY" (若未設定逾時)，服務逾時查詢處理順序如下 :

1. 以 vsys TCP 及 UDP 連接埠爲基礎的逾時表 (若已設定逾時)。

2. 以通訊協定爲基礎的預設逾時表。

意外情況

設定逾時時，請注意下列事項 :

- 若某項服務包含多個服務規則項目，則所有規則項目會共用同一個逾時。逾時表會依據符合通訊協定 (UDP 及 TCP - 其他通訊協定使用預設值) 的每一項規則項目進行更新。您僅需定義服務逾時一次。例如，若您建立具有兩個規則的服務，則下列指令將會爲兩個規則設定 20 分鐘的逾時 :

  ```
  set service test protocol tcp dst-port 1035-1035 timeout 20
  set service test + udp src-port 1-65535 dst-port 1111-1111
  ```

- 若多個服務以同一個通訊協定及重疊的目的地連接埠進行組態，則最新組態的服務逾時將會覆寫以連接埠爲基礎的表中的其他逾時。例如 :

  ```
  set service ftp-1 protocol tcp src 0-65535 dst 2121-2121 timeout 10
  set service telnet-1 protocol tcp src 0-65535 dst 2100-2148 timeout 20
  ```

  設定此組態後，安全性裝置會爲服務群組中的目的地連接埠 2121 套用 20 分鐘的逾時，因爲 telnet-1 (2100-2148) 的目的地連接埠號碼與 ftp-1 (2121) 的連接埠號碼重疊，且您在定義 ftp-1 後才定義 telnet-1。

  當多重服務使用同一個通訊協定和重疊的目的地連接埠範圍時，若要修改服務逾時，您必須取消設定服務，並以新的逾時值重新設定服務。這是因爲重新開機時，系統會依據建立時間而非修改時間載入服務。

  若要避免某服務發生不想要的應用程式錯誤逾時，請勿以重疊的目的地連接埠號碼建立服務。

- 若您取消設定某服務逾時，系統會使用服務項目資料庫中以通訊協定爲基礎的預設逾時，且會以預設值更新服務項目及以連接埠爲基礎的逾時表中的逾時值。

  若已修改的服務具有與其他服務重疊的目的地連接埠，則以通訊協定爲基礎的預設逾時可能不是所需的值。在這種情況下，請將安全性裝置重新開機，或是再次設定服務逾時，讓所需的逾時生效。

- 當您修改預先定義的服務並重新開機時，已修改的服務可能不是組態中最後出現的服務。這是因爲預先定義的服務比自訂服務先載入，且任何針對自訂服務所做的變更 (即使時間較早) 也都會在您重新開機時顯示爲較預先定義的服務晚。

  例如，若您建立了下列服務 :

  ```
  set service my_service protocol tcp dst-port 179-179 timeout 60
  ```

  並在之後將預先定義服務 BGP 的逾時做了如下修改 :

  ```
  set service bgp timeout 75
  ```

  BGP 服務會使用 75 分鐘的逾時值，因爲其現被寫入至服務項目資料庫。但是在以 TCP 連接埠爲基礎的逾時表中，連接埠 BGP 針對連接埠 179 所使用的逾時亦會變更爲 75。在您重新開機後，BGP 服務 (單一服務) 將繼續使用其從服務項目資料庫所取得的 75 分鐘逾時。但是連接埠 179 的以 TCP 連接埠爲基礎的表中的逾時現在將爲 60。您可輸入 **get service bgp** 指令來予以確認。

  這對於單一服務不會造成任何影響。但若您將 BGP 或 my_service 新增至服務群組，則目的地連接埠 179 將會使用 60 分鐘的逾時值。這是因爲服務群組逾時是取自以連接埠爲基礎的逾時表 (若已設定)。

  因此，爲了在您修改預先定義服務逾時時確保可預測性，您可以建立一個類似的服務，如 :

  ```
  set service my-bgp protocol tcp dst-port 179-179 timeout 75
  ```

範例

在以下範例中，將 FTP 預先定義服務的逾時臨界時變更爲 75 分鐘。

WebUI

Objects > Services > Predefined > Edit (FTP): 輸入下面的內容，然後按一下 **OK**:

Service Timeout: Custom (選擇), 75 (類型)

CLI

```
set service FTP timeout 75
save
```

定義自訂網際網路控制訊息通訊協定服務

ScreenOS 支援作爲預先定義或自訂服務的「網際網路控制訊息通訊協定」(ICMP) 及多種 ICMP 訊息。組態自訂 ICMP 服務時，您必須定義類型與代碼。ICMP 內具有不同的訊息類型。例如 :

類型 0 = 回應要求訊息

類型 3 = 目的地無法到達訊息

注意 : 如需 ICMP 類型和代碼的詳細資訊，請參閱 RFC 792，*Internet Control Message Protocol*。

ICMP 訊息類亦可具有訊息代碼。此代碼提供更特定的訊息資訊，如表 14 中所示。

表 14: 訊息說明

訊息類型	訊息代碼
5 = 重新定向	0 = 重新定向網路 (或子網路) 的資料電報
	1 = 重新定向主機的資料電報
	2 = 重新定向服務與網路類型的資料電報
	3 = 重新定向服務與主機類型的資料電報
11 = 超過的時間代碼	0 = 傳輸中超過的活動時間
	1 = 超過的碎片重新組合時間

ScreenOS 支援 0-255 範圍內的所有類型與代碼。

在本範例中，使用 ICMP 作爲傳輸通訊協定，以定義名爲 "host-unreachable" 的自訂服務。類型爲 3 (「目的地無法到達」)，代碼爲 1 (「主機無法到達」)。將逾時值設定爲 2 分鐘。

WebUI

Objects > Services > Custom: 輸入下面的內容，然後按一下 **OK**:

Service Name: host-unreachable
Service Timeout: Custom (選擇), 2 (類型)
Transport Protocol: ICMP (選擇)
ICMP Type: 3
ICMP Code: 1

CLI

```
set service host-unreachable protocol icmp type 5 code 0
set service host-unreachable timeout 2
save
```

遠端 Shell 應用程式層閘道

「遠端 Shell 應用程式層閘道」(RSH ALG) 允許已通過驗證的使用者於遠端主機執行 Shell 指令。Juniper Networks 安全性裝置支援「透明」(L2) 模式、「路由」(L3) 模式及 NAT 模式的 RSH 服務，但裝置並不支援 RSH 通訊流量的連接埠轉譯。

Sun 遠端程序呼叫應用程式層閘道

Sun 遠端程序呼叫，又稱爲「開放網路運算遠端程序呼叫」(ONC RPC)，它提供了一種方式，可以讓執行於某台主機上的程式呼叫執行於另一台主機上的程式的程序。由於存在大量的 RPC 服務和廣播需求，會根據服務的程式編號和版本編號動態交涉 RPC 服務的傳輸位址。有好幾種連結通訊協定是專爲將 RPC 程式編號和版本編號與傳輸位址加以對應而定義的。

Juniper Networks 安全性裝置支援將 Sun RPC 用作預先定義的服務，並可根據您組態的政策來允許和拒絕通訊流量。「應用程式層閘道」(ALG) 可以爲安全性裝置提供處理 Sun RPC 之動態傳輸位址交涉機制並確保執行以程式編號爲基礎的防火牆政策的功能。您可以定義一個防火牆政策以允許或拒絕所有 RPC 要求，或是允許或拒絕特定程式編號的 RPC 要求。ALG 也支援傳入與傳出要求的「路由」和 NAT 模式。

一般 RPC 呼叫情況

當用戶端呼叫遠端服務時，它需要尋找服務的傳輸位址，在使用 TCP/UDP 的情況下，該位址是一個連接埠號碼。此情況的一般程序如下：

1. 用戶端傳送 GETPORT 訊息至遠端電腦上的 RPCBIND 服務。GETPORT 訊息包含程式編號，以及它要呼叫之遠端服務的版本和程序編號。
2. RPCBIND 服務以一個連接埠號碼回應。
3. 用戶端使用傳回的連接埠號碼來呼叫遠端服務。
4. 遠端服務回應用戶端。

用戶端也可以使用 CALLIT 訊息直接呼叫遠端服務，而不需知道服務的連接埠號碼。在這種情況下，執行的程序如下：

1. 用戶端傳送 CALLIT 訊息至遠端電腦上的 RPCBIND 服務。CALLIT 訊息包含程式編號，以及它要呼叫之遠端服務的版本和程序編號。
2. RPCBIND 呼叫用戶端的服務。
3. 如果呼叫成功，RCPBIND 會回應用戶端。回應內容包含呼叫結果和服務的連接埠號碼。

自訂 Sun RPC 服務

因爲 Sun RPC 服務使用動態交涉的連接埠，所以您無法使用以固定 TCP/UDP 連接埠爲基礎的一般服務物件在安全政策中允許它們，而是必須使用程式編號來建立 Sun RPC 服務物件。例如，NFS 使用以下兩個程式編號：100003 和 100227。對應的 TCP/UDP 連接埠是動態的。要允許程式編號，您可以建立包含這兩個編號的 sun-rpc-nfs 服務物件。ALG 會將程式編號與動態交涉的 TCP/UDP 連接埠加以對應，並根據您組態的政策來允許或拒絕服務。

在下例中，建立稱爲 my-sunrpc-nfs 的服務物件以使用 Sun RPC 網路檔案系統，它以兩個程式 ID 表示：100003 和 100227。

WebUI

Objects > Services > Sun RPC Services > New: 輸入下面的內容，然後按一下 **Apply**:

Service Name: my-sunrpc-nfs
Service Timeout: (選擇)
Program ID Low: 100003
Program ID High: 100003
Program ID Low: 100227
Program ID High: 100227

CLI

```
set service my-sunrpc-nfs protocol sun-rpc program 100003-100003
set service my-sunrpc-nfs + sun-rpc program 100227-100227
save
```

自訂 Microsoft 遠端程序呼叫應用程式層閘道

Microsoft 遠端程序呼叫 (MS RPC) 是以 Microsoft 方式執行的「分散式運算環境」(DCE) RPC。就像 Sun RPC (請參閱第 122 頁上的「Sun 遠端程序呼叫應用程式層閘道」) 一樣，MS RPC 提供了一種方式，可以讓執行於某台主機上的程式呼叫執行於另一台主機上的程式的程序。由於存在大量的 RPC 服務和廣播需求，會根據服務程式的統一專屬識別元 (Universal Unique IDentifier，UUID) 動態交涉 RPC 服務的傳輸位址。ScreenOS 中已定義了端點對應表連結通訊協定，可將特定 UUID 與某個傳輸位址加以對應。

Juniper Networks 安全性裝置支援將 MS RPC 用作預先定義的服務，並可根據您組態的政策來允許和拒絕通訊流量。ALG 可以爲安全性裝置提供處理 MS RPC 之動態傳輸位址交涉機制並確保執行以 UUID 爲基礎的防火牆政策的功能。您可以定義一個防火牆政策以允許或拒絕所有 RPC 要求，或是允許或拒絕特定 UUID 編號的 RPC 要求。ALG 也支援傳入與傳出要求的「路由」和 NAT 模式。

因爲 MS RPC 服務使用動態交涉的連接埠，所以您無法使用以固定 TCP/UDP 連接埠爲基礎的一般服務物件在安全政策中允許它們，而必須使用 UUID 來建立 MS RPC 服務物件。例如，MS Exchange 資訊儲存服務使用下列四個 UUID:

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
- 1453c42c-0fa6-11d2-a910-00c04f990f3b
- 10f24e8e-0fa6-11d2-a910-00c04f990f3b
- 1544f5e0-613c-11d1-93df-00c04fd7bd09

對應的 TCP/UDP 連接埠是動態的。若要允許它們，必須建立包含這四個 UUID 的 ms-exchange-info-store 服務物件。ALG 會根據這四個 UUID 將程式編號與動態交涉的 TCP/UDP 連接埠加以對應，並根據您組態的政策來允許或拒絕服務。

在下例中，建立稱爲 my-ex-info-store 的服務物件，它包含 MS Exchange 資訊儲存服務的 UUID。

WebUI

Objects > Services > MS RPC: 輸入下面的內容，然後按一下 **Apply**:

Service Name: my-ex-info-store
UUID: 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
UUID: 1453c42c-0fa6-11d2-a910-00c04f990f3b
UUID: 10f24e8e-0fa6-11d2-a910-00c04f990f3b
UUID: 1544f5e0-613c-11d1-93df-00c04fd7bd09

CLI

```
set service my-ex-info-store protocol ms-rpc uuid
    0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
set service my-ex-info-store + ms-rpc uuid
    1453c42c-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid
    10f24e8e-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid
    1544f5e0-613c-11d1-93df-00c04fd7bd09
save
```

即時資料流傳遞通訊協定應用程式層閘道

「即時資料流通訊協定」(RTSP) 是一種「應用程式層」通訊協定，可用來控制一或多個同步化多媒體資料流 (例如音訊與視訊) 的傳送。雖然 RTSP 本身能夠傳送資料流 (使用控制資料流來插補連續性的媒體資料流)，它通常是用來作爲多媒體伺服器的一種「網路遠端控制」。通訊協定是專爲選取傳送通道 (例如 UDP、多點傳送 UDP 和 TCP) 以及根據即時通訊協定 (RTP) 選取傳送機制而設計的一種方法。RTSP 也可以使用會話說明通訊協定 (SDP) 作爲向用戶端提供資訊的一種方法，讓用戶端得以將來自一或多個伺服器之資料流組合而成的呈報加以整合控制，並將來自單一伺服器之多個資料流組合而成的呈報加以分散控制。資料來源可爲即時訊息或儲存的剪輯。

Juniper Networks 安全性裝置支援將 RTSP 用作一種服務，並可根據您組態的政策來允許或拒絕 RTSP 通訊流量。因爲 RTSP 使用動態指派的連接埠號碼，該號碼是在建立控制連線時透過封包負載傳遞的，所以需要 ALG。ALG 會追蹤動態指派的連接埠號碼並隨之開啓針孔。在 NAT 模式中，如有需要，ALG 會轉譯 IP 位址和連接埠。安全性裝置在「路由」模式、「透明」模式及以介面爲基礎和以政策爲基礎的 NAT 模式中支援 RTSP。

第 125 頁上的圖 62 圖示了典型的 RTSP 會話。用戶端會初始化會話 (例如，當使用者按一下 RealPlayer 上的 Play 按鈕時) 並透過連接埠 554 建立與 RTSP 伺服器的 TCP 連線，然後傳送 OPTIONS 訊息 (訊息亦稱爲方法)，以確定伺服器支援哪些音訊和視訊功能。伺服器以指定伺服器名稱和版本以及會話識別字的方式向 OPTIONS 訊息作出回應，例如 24256-1。(如需有關方法的詳細資訊，請參閱第 14 頁上的「SIP 要求方式」 和 RFC 2326 中的第 11 節)。

然後用戶端傳送 DESCRIBE 訊息，內含它所需之實際媒體檔案的 URL。伺服器使用 SDP 格式的媒體描述向 DESCRIBE 訊息作出回應。然後用戶端傳送 SETUP 訊息，它指定用戶端可接受之資料流處理媒體的傳輸機制 (例如，RTP/RTCP 或 RDT)，並指定接收媒體所使用的連接埠。使用 NAT 時，RTSP ALG 會追蹤這些連接埠並視需要轉譯它們。伺服器向 SETUP 方法作出回應，並選取其中一個傳輸通訊協定，這樣一來用戶端和伺服器端就媒體傳輸機制達成一致。然後用戶端傳送 PLAY 方法，而伺服器開始將媒體的資料流傳遞至用戶端。

圖 62: 典型的 RTSP 會話



RTSP 要求方式

下表列出了可對資源 (媒體物件) 執行的方法，資訊傳遞的一或多個方向，以及方法的類別 : 必要、建議或選用。呈報是指向用戶端呈現的完整媒體資訊，諸如有關一個資料流或多個資料流集的網路位址、編碼和內容。「資料流」是單一媒體實例，例如音訊或視訊，以及由會話內某個來源建立的全部封包。

表 15: RTSP 要求方式

方法	方向	物件	要求
OPTIONS	用戶端至伺服器	呈報、資料流	必須爲用戶端至伺服器
	伺服器至用戶端	呈報、資料流	可爲伺服器至用戶端
DESCRIBE	用戶端至伺服器	呈報、資料流	建議
ANNOUNCE	用戶端至伺服器	呈報、資料流	可選
	伺服器至用戶端	呈報、資料流	
SETUP	用戶端至伺服器	資料流	必要
GET_PARAMETER	用戶端至伺服器	呈報、資料流	可選
	伺服器至用戶端		
SET_PARAMETER	用戶端至伺服器	呈報、資料流	可選
	伺服器至用戶端		
PLAY	用戶端至伺服器	呈報、資料流	必要
PAUSE	用戶端至伺服器	呈報、資料流	建議
RECORD	用戶端至伺服器	呈報、資料流	可選
REDIRECT	伺服器至用戶端	呈報、資料流	可選
TEARDOWN	用戶端至伺服器	呈報、資料流	必要

按如下方式定義方法 :

- OPTIONS - 用戶端向伺服器查詢它可支援的音訊或視訊，以及伺服器的名稱和版本和會話 ID 等。
- DESCRIBE - 用於交換媒體初始化資訊，如時鐘頻率、色彩表和用戶端播放媒體資料流所需的任何與傳輸無關的資訊。通常用戶端會傳送它所要求的檔案的 URL，而伺服器會以 SDP 格式的媒體描述作出回應。
- ANNOUNCE - 用戶端使用此方法來發送呈報的描述或是要求 URL 所代表的媒體物件。伺服器使用此方法來即時更新會話描述。
- SETUP - 用戶端指定要使用的可接受傳輸機制，如它接收媒體資料流所使用的連接埠及傳輸通訊協定。
- GET_PARAMETER - 擷取呈報的值或 URL 中指定的資料流參數。此方法可用於無實體的主體，以測試用戶端或伺服器是否在執行中。也可以用 Ping 來測試用戶端或伺服器是否在執行中。
- SET_PARAMETER - 用戶端使用此方法來設定某個呈報的參數值或 URL 指定的資料流。基於防火牆的考量，無法使用此方法來設定傳輸參數。

- PLAY - 指示伺服器使用 SETUP 中指定的機制開始傳送資料。所有 SETUP 要求都成功時，用戶端才會發出 PLAY 要求。伺服器會依序將 PLAY 要求排在佇列中，並延遲執行任何新的 PLAY 要求，直到目前處理中的 PLAY 要求完成爲止。PLAY 要求可能包含或不包含指定的範圍。範圍可能包含一個用於開始播放的時間參數 (以協調通用時間 (UTC) 格式指定)，該參數也可以用來同步化不同來源的資料流。

- PAUSE - 暫停傳送中呈報的傳送。如果要求 URL 指定了特定的資料流 (例如，音訊)，就相當於靜音。儘管當 PAUSE 針對的是 SETUP 中的逾時參數所指定的期間時伺服器可能會關閉會話，但恢復播放或錄音時，音軌仍可維持同步。PAUSE 要求會丟棄所有佇列中的 PLAY 要求。

- RECORD - 啓動錄製呈報描述中定義的一系列媒體。UTC 時戳指示開始和結束時間，否則伺服器會使用呈報描述中的開始和結束時間。

- REDIRECT - 通知用戶端它必須與其他伺服器連線，並包含位置資訊，還可能包含該新 URL 的範圍參數。若要繼續接收此 URL 的媒體，用戶端必須爲目前的會話發出 TEARDOWN 要求，並爲新的會話發出 SETUP 要求。

- TEARDOWN - 停止指定 URL 的資料流傳送並釋放與其聯結的資源。除非會話描述定義了所有傳輸參數，否則必須發出 SETUP 要求，才能再次執行該會話。

RTSP 狀態代碼

RTSP 使用狀態代碼提供有關用戶端和伺服器要求的資訊。狀態代碼包含機器可讀取的三位數結果代碼，以及人們可讀取的原因分析短句。用戶端必須自行斟酌是否要顯示原因分析短句。狀態代碼的分類如下 :

- 資訊性 (100 至 199) - 已接收並正在處理要求

- 成功 (200 至 299) - 已成功接收、瞭解並接受動作

- 重新定向 (300 至 399) - 需要進一步的動作才能完成要求

- 用戶端錯誤 (400 至 499) - 要求包含錯誤的語法，無法執行

- 伺服器錯誤 (500 至 599) - 伺服器無法執行顯然有效的要求

下表列出針對 RTSP 1.0 定義的所有狀態代碼及建議的原因分析短句。可在不影響通訊協定執行的情況下修訂或重新定義原因分析短句。

表 16: RTSP 1.0 狀態代碼

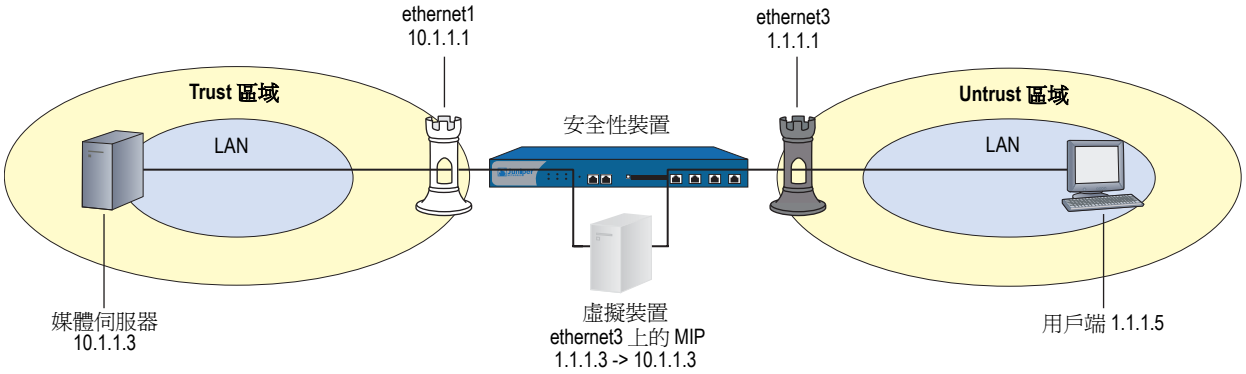
狀態代碼	原因分析短句	狀態代碼	原因分析短句
100	繼續	414	Request-URI 太大
200	確定	415	不支援的媒體類型
201	已建立	451	不支援的媒體類型
250	儲存空間不足	452	找不到會議
300	多重選擇	453	頻寬不足
301	永久移動	454	找不到會話
303	參閱其他	455	方法在此狀態下無效
304	未修改	456	資源的標頭欄位無效
305	使用代理	457	範圍無效
400	錯誤要求	458	參數爲唯讀性質
401	未經授權	459	不允許聚集操作
402	需付費	460	只允許聚集操作
403	禁止	461	不支援的傳輸
404	找不到	462	目的地無法到達
405	不允許的方法	500	伺服器內部錯誤
406	無法接受	501	未執行
407	需代理驗證	502	錯誤閘道
408	要求逾時	503	服務不可用
410	遺失	504	閘道逾時
411	需要長度	505	不支援的 RTSP 版本
412	事前處理失敗	551	不支援的選項
413	要求實體太大		

注意： 如需狀態代碼的完整定義，請參閱 RFC 2326，*Real Time Streaming Protocol (RTSP)*。

在私人網域中組態媒體伺服器

在下例中，媒體伺服器位於 Trust 區域中，用戶端位於 Untrust 區域中。將 ethernet3 介面上的 MIP 置於 Trust 區域的媒體伺服器中，然後建立一個政策，使 RTSP 通訊流量得以從 Untrust 區域內的用戶端傳遞至 Trust 區域中的媒體伺服器。

圖 63: RTSP 私人網域



WebUI

1. **介面**

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.2

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.1.1.1/24
   Manage IP: 1.1.1.2

2. **位址**

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: media_server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.1.3/24
   Zone: Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: client
   IP Address/Domain Name:
   IP/Netmask: (選擇), 1.1.1.5/24
   Zone: Untrust

3. **MIP**

   Network > Interfaces > Edit (對於 ethernet3) > MIP > New: 輸入下面的內容，然後按一下 **OK**:

   Mapped IP: 1.1.1.3
   Host IP Address: 10.1.1.5

4. **政策**

   Policies > (From: Untrust, To: Trust) > New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), client
   Destination Address:
   Address Book Entry: (選擇), MIP(1.1.1.3)
   Service: RTSP
   Action: Permit

CLI

1. **介面**

   set interface ethernet1 trust
   set interface ethernet1 ip 10.1.1.1
   set interface ethernet3 untrust
   set interface ethernet3 ip 1.1.1.1

2. **位址**

   set address trust media_server 10.1.1.3/24
   set address untrust client 1.1.1.5

3. **MIP**

   set interface ethernet3 mip (1.1.1.3) host 10.1.1.3

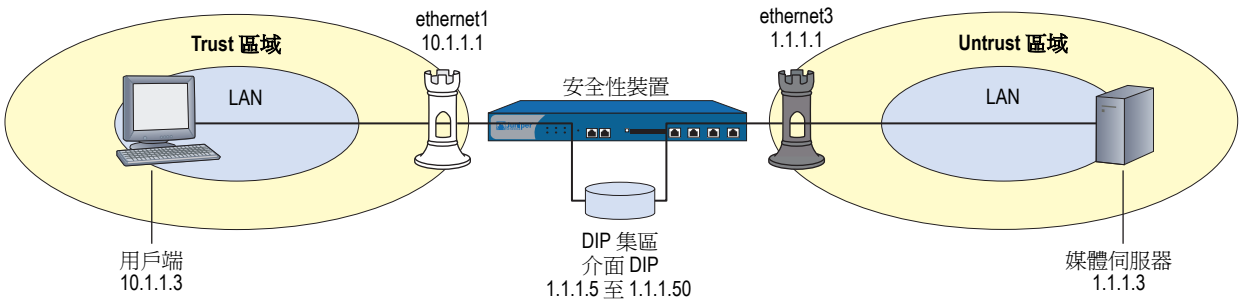
4. **政策**

   set policy from untrust to trust client mip(1.1.1.3) rtsp permit
   save

在公開網域中組態媒體伺服器

在下例中，媒體伺服器位於 Untrust 區域中，用戶端位於 Trust 區域中。當媒體伺服器從 Untrust 區域向用戶端作出回應時，將 DIP 集區置於 ethernet3 介面上進行 NAT，然後建立一個政策，使得 RTSP 通訊流量可以從 Trust 區域傳遞至 Untrust 區域。

圖 64: RTSP 公開網域



WebUI

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.2

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.1.1.1/24
   Manage IP: 1.1.1.2

2. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: client
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.1.3/24
   Zone: Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: media_server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 1.1.1.3/24
   Zone: Untrust

3. **DIP 集區**
   Network > Interfaces > Edit (對於 ethernet3) > DIP > New: 輸入下面的內容，然後按一下 **OK**:

   ID: 5
   IP Address Range: (選擇) 1.1.1.5 ~ 1.1.1.50
   Port Translation: (選擇)

4. **政策**
   Policies > (From: Trust, To: Untrust) > New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry (選擇): client
   Destination Address:
   Address Book Entry (選擇): media_server
   Service: RTSP
   Action: Permit

   > Advanced: 輸入下面的內容，然後按一下 **OK**:

   NAT:
   Source Translation: (選擇)
   (DIP on): 5 (1.1.1.5-1.1.1.50)/port-xlate

CLI

1. **介面**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **位址**
   set address trust client ip 10.1.1.3/24
   set address untrust media_server ip 1.1.1.3/24

3. **DIP 集區**
   set interface ethernet3 dip 5 1.1.5 1.1.1.50

4. **政策**
   set policy from trust to untrust client media_server rtsp nat dip 5 permit
   save

服務群組

服務群組是一組集合在一個名稱下的服務。建立包含數個服務的群組後，就可以在群組層級將服務套用到政策，進而簡化管理。

ScreenOS 服務群組選項有下列功能 :

- 每個服務簿項目都可以被一個或多個服務群組參考。
- 每個服務群組都可以包含預先定義的和使用者定義的服務簿項目。

服務群組受到下列限制 :

- 服務群組不能和服務有相同的名稱；因此，如果有名爲 "FTP" 的服務，就不能將服務群組命名爲 "FTP"。
- 如果在政策中參考服務群組，可以編輯但不能移除群組，除非先在政策中移除對它的參考。
- 從服務簿中刪除自訂服務簿項目時，項目也會從所有參考它的群組中移除。
- 一個服務群組不能將其他服務群組當作成員包含在內。
- 包含式服務術語 "ANY" 不能新增到群組中。
- 一個服務每次僅能作爲一個群組中的一部份。

建立服務群組

在本範例中，您建立命名爲 grp1 的服務群組，其中包括 IKE、FTP 和 LDAP 服務。

WebUI

Objects > Services > Groups > New: 輸入下面的群組名稱，移動下列服務，然後按一下 **OK**:

Group Name: grp1

選擇 **IKE**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

選擇 **FTP**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

選擇 **LDAP**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

CLI

```
set group service grp1
set group service grp1 add ike
set group service grp1 add ftp
set group service grp1 add ldap
save
```

注意 : 如果嘗試將服務新增到不存在的服務群組，安全性裝置會建立群組。此外，請確認參考其他群組的群組不能將自身包括在參考清單中。

修改服務群組

在本範例中，變更您在第 133 頁上的「建立服務群組」所建立，名爲 grp1 的服務群組成員。移除 IKE、FTP 與 LDAP 服務，然後新增 HTTP、FINGER 與 IMAP。

WebUI

Objects > Services > Groups > Edit (對於 grp1): 移動下面的服務，然後按一下 **OK**:

選擇 **IKE**，然後使用按鈕 > > 將服務從 Group Members 欄中移動到 Available Members 欄中。

選擇 **FTP**，然後使用按鈕 > > 將服務從 Group Members 欄中移動到 Available Members 欄中。

選擇 **LDAP**，然後使用按鈕 > > 將服務從 Group Members 欄中移動到 Available Members 欄中。

選擇 **HTTP**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

選擇 **Finger**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

選擇 **IMAP**，然後使用按鈕 < < 將服務從 Available Members 欄中移動到 Group Members 欄中。

CLI

```
unset group service grp1 clear
set group service grp1 add http
set group service grp1 add finger
set group service grp1 add imap
save
```

移除服務群組

在本範例中，您刪除名爲 "grp1" 的服務群組。

WebUI

Objects > Services > Groups: 按一下 **Remove** (對於 grp1)。

CLI

```
unset group service grp1
save
```

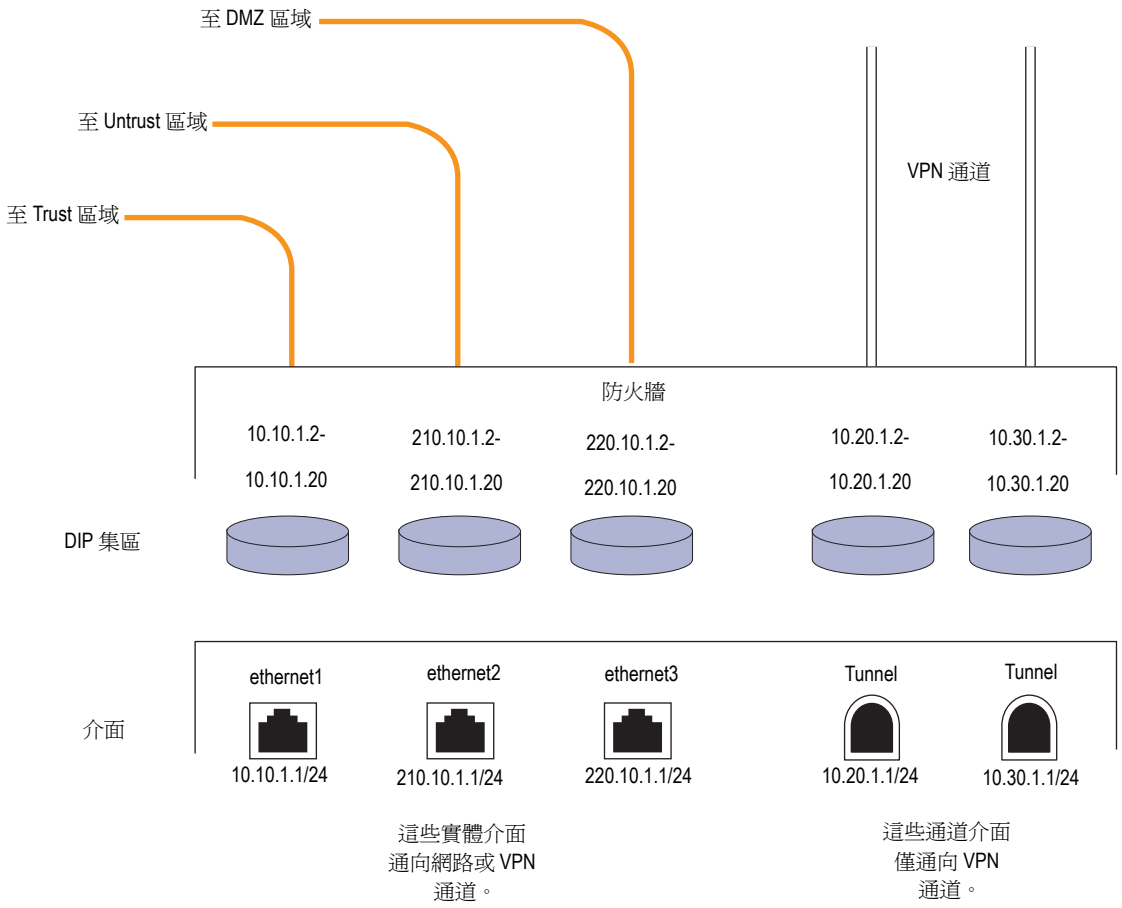
注意： 安全性裝置不會自動刪除已經移除其中所有成員的群組。

動態 IP 集區

動態 IP (DIP) 集區包含一個範圍內的 IP 位址，安全性裝置在對 IP 封包標頭中的來源 IP 位址執行網路位址轉譯 (NAT-src) 時，可從中進行動態或定態提取位址。(如需定態來源位址轉譯的資訊，請參閱第 **8**-18 頁上的「來自 DIP 集區 (具位址轉移) 的 NAT-Src」。) 如果 DIP 集區的位址範圍與介面 IP 位址在相同的子網路中，那麼集區不可以包括也可能存在於該子網路中的介面 IP 位址、路由器 IP 位址及任何對應 IP (MIP) 或虛擬 IP (VIP) 位址。如果位址範圍在擴展介面的子網路中，那麼集區必須排除擴展介面的 IP 位址。

可將三種介面連結到「動態 IP」(DIP) 集區：網路和 VPN 通訊流量的實體介面和子介面，以及僅用於 VPN 通道的通道介面。

圖 65: DIP 介面



連接埠位址轉譯

使用「連接埠位址轉譯」(PAT)，多台主機可共享相同的 IP 位址，安全性裝置維護一份已指派連接埠號碼的清單，以識別哪個會話屬於哪個主機。啓用 PAT 後，最多 64,500 台主機即可共享單一 IP 位址。

如「NetBIOS 擴展使用者介面」(NetBEUI) 和「Windows 網際網路命名服務」(WINS) 等應用程式需要具體的連接埠號碼，如果套用 PAT，它們將無法正常運作。對於此類應用程式，套用 DIP 時，可指定不執行 PAT (也就是使用固定連接埠)。對於固定連接埠 DIP，安全性裝置雜湊原始的主機 IP 位址，並將之儲存在其主機雜湊表中，進而允許安全性裝置將正確的會話與每個主機相關聯。

建立有 PAT 的 DIP 集區

在本範例中，您要爲本機網站的使用者建立 VPN 通道，以到達遠端網站的 FTP 伺服器。然而，這兩個網站的內部網路使用相同的私人位址空間 (10.1.1.0/24)。爲了解決重疊位址的問題，在本機安全性裝置的 Untrust 區域中建立通道介面，爲其指派 IP 位址 10.10.1.1/24，然後將它與 DIP 集區聯結，並啓用位址範圍 10.10.1.2-10.10.1.2 和連接埠位址轉譯。

遠端網站的管理也必須建立一通道介面，此介面具有存在於中性位址空間的 IP 位址，如 10.20.2.1/24，然後設定到其 FTP 伺服器的「對應的 IP」(MIP) 位址，如到主機 10.1.1.5 的 10.20.2.5。

注意： 本範例僅包括通道介面組態及其伴隨的 DIP 集區。如需此方案所有必要組態步驟的完整範例，請參閱第 **5**-129 頁上的「具有重疊位址的 VPN 站台」。

WebUI

Network > Interfaces > New Tunnel IF: 輸入下面的內容，然後按一下 **OK**:

```
Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: ( 選擇 )
        IP Address/Netmask: 10.10.1.1/24
```

Network > Interfaces > Edit (對於 tunnel.1) > DIP > New: 輸入下面的內容，然後按一下 **OK**:

```
ID: 5
IP Address Range: 10.10.1.2 ~ 10.10.1.2
Port Translation: ( 選擇 )
In the same subnet as the interface IP or its secondary IPs: ( 選擇 )
```

注意： 您可以使用顯示的 ID 編號，爲按照順序的下一個可用號碼，或鍵入不同的編號。

CLI

```
set interface tunnel.1 zone untrust-tun
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2
save
```

注意： 依預設會啓用 PAT，因此沒有啓用它的引數。若要建立與上述相同的 DIP 集區，但無 PAT (也就是使用固定連接埠號碼)，請執行下面的操作 :

(WebUI) Network > Interfaces > Edit (對於 tunnel.1) > DIP > New: 清除 Port Translation 核取方塊，然後按一下 **OK**。

(CLI) set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2 fix-port

---

修改 DIP 集區

在本範例中，您變更現有 DIP 集區 (ID 5) 中的位址範圍，從 10.20.1.2 - 10.20.1.2 至 10.20.1.2 - 10.20.1.10。此 DIP 集區與 tunnel.1 相關聯。請注意，若要透過 CLI 變更 DIP 集區範圍，必須先移除 (或取消設定) 現有 DIP 集區，然後建立新集區。

注意 : 沒有使用此特定 DIP 集區的政策。若政策使用 DIP 集區，則您必須先刪除政策或將之修改爲不使用 DIP 集區，然後您才能修改 DIP 集區。

WebUI

Network > Interfaces > Edit (對於 tunnel.1) > DIP > Edit (對於 ID 5): 輸入下面的內容，然後按一下 **OK**:

IP Address Range: 10.20.1.2 ~ 10.20.1.10

CLI

```
unset interface tunnel.1 dip 5
set interface tunnel.1 dip 5 10.20.1.2 10.20.1.10
save
```

相黏 DIP 位址

當主機初始化多個符合要求進行網路位址轉譯 (NAT) 的會話，並且取得來自 IP 集區 (已啓用連接埠轉譯) 的指派位址時，安全性裝置會爲每個會話指派不同的來源 IP 位址。對於建立多個會話 (每個會話都需要相同來源 IP 位址) 的服務，這種隨機位址指派可能會產生問題。

注意 : 若 DIP 集區未執行連接埠轉譯，安全性裝置將會從相同的主機爲所有同時會話指派一個 IP 位址。

例如，使用 AOL Instant Messaging (AIM) 用戶端時，多個會話一定要有相同的 IP 位址。您登入時會建立一個會話，並建立另一個用於每個聊天的會話。對於驗證新聊天屬於驗證使用者的 AIM 伺服器，必須讓登入會話的來源 IP 位址與聊天會話的來源 IP 位址相配對。如果有差異 (可能是由於它們在 NAT 程序期間是從 DIP 隨機指定的)，AIM 伺服器會拒絕聊天會話。

若要確保安全性裝置從 DIP 集區將相同的 IP 位址指派給主機的多個同時會話，可輸入 CLI 指令 **set dip sticky** 來啓用「相黏」DIP 位址功能。

在不同子網路中使用 DIP

根據情況，如果需要將向外防火牆通訊流量中的來源 IP 位址從出口介面的位址轉譯成不同子網路中的位址，您可以使用擴展介面選項。此選項讓您可以將第二個 IP 位址和一個伴隨的 DIP 集區連接到一個在不同子網路中的介面。然後，您可以以每個政策爲基礎啓用 NAT，並且指定建立在用於轉譯的晾托介面上的 DIP 集區。

在本範例中，兩個分公司租借連到總公司的線路。總公司要求他們僅使用總公司指派給他們的授權 IP 位址。然而，這兩個分公司從其 ISP 處獲得其他用於網際網路通訊流量的 IP 位址。爲了與總公司進行通訊，使用擴展介面選項組態每個分公司的安全性裝置，將其傳送至總公司的封包的來源 IP 位址轉譯爲授權位址。分公司 A 和 B 的授權和指派的 IP 位址如下：

表 17: 授權的公司 IP 位址

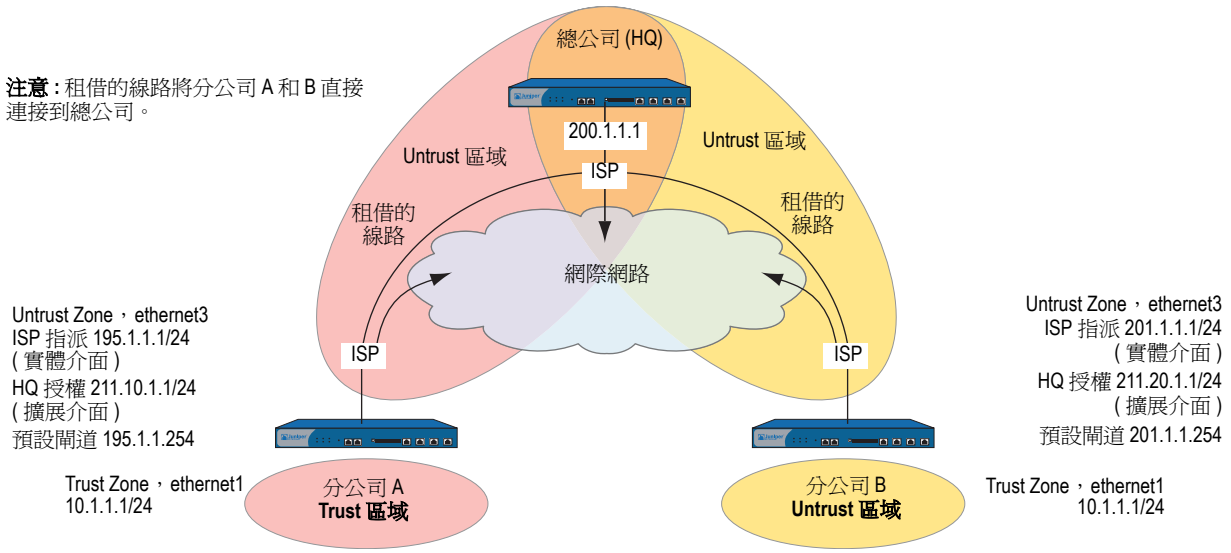
	指派的 IP 位址 (自 ISP) 用於 Untrust 區域實體介面	授權的 IP 位址 (自總公司) 用於 Untrust 區域擴展介面 DIP
分公司 A	195.1.1.1/24	211.10.1.1/24
分公司 B	201.1.1.1/24	211.20.1.1/24

兩個站台的安全性裝置都有 Trust 區域和 Untrust 區域。所有安全區都在 trust-vr 路由設定網域中。將 ethernet1 連結到 Trust 區域並指派其 IP 位址 10.1.1.1/24。將 ethernet3 連結到 Untrust 區域並指定由 ISP 指派的 IP 位址：「分公司 A」爲 195.1.1.1/24，「分公司 B」爲 201.1.1.1/24。然後在 ethernet3 上建立有 DIP 集區的擴展介面，其中包含授權 IP 位址：

- 分公司 A: 擴展介面 IP 211.10.1.10/24；DIP 集區 211.10.1.1 - 211.10.1.1；PAT 已啓用
- 分公司 B: 擴展介面 IP 211.20.1.10/24；DIP 集區 211.20.1.1 - 211.20.1.1；PAT 已啓用

設定 NAT 模式中的 Trust 區域介面。它使用 Untrust 區域介面 IP 位址作爲其所有向外通訊流量的來源位址 (傳送至總公司的通訊流量除外)。組態到達總公司的政策，將來源位址轉譯爲擴展介面 DIP 集區中的位址。(DIP 集區的 ID 編號爲 5。包含一個 IP 位址，使用連接埠位址轉譯後，可爲多達 64,500 台主機處理會話。) 總公司用於向內通訊流量的 MIP 位址是 200.1.1.1，它是您在每個安全性裝置的 Untrust 區域通訊錄中輸入的 "HQ"。

圖 66: 在另一個子網路下的 DIP



注意 : 爲了使用該租借線路，每個 ISP 都必須爲流向租借線路端點網站的通訊流量設定路由。ISP 將他們從本機安全性裝置接收到的任何其他通訊流量傳送到網際網路。

WebUI (分公司 A)

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 195.1.1.1/24
   Interface Mode: Route

   Network > Interfaces > Edit (對於 ethernet3) > DIP > New: 輸入下面的內容，然後按一下 **OK**:

   ID: 5
   IP Address Range: 211.10.1.1 ~ 211.10.1.1
   Port Translation: (選擇)
   Extended IP/Netmask: 211.10.1.10/255.255.255.0

2. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: HQ
   IP Address/Domain Name:
   IP/Netmask: (選擇), 200.1.1.1/32
   Zone: Untrust

3. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP address: 195.1.1.254

4. **政策**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Source Address:
    Address Book Entry: (選擇), Any
Destination Address:
    Address Book Entry: (選擇), HQ
Service: ANY
Action: Permit
Position at Top: (選擇)

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

NAT:
Source Translation: (選擇)
  (DIP on): 5 (211.10.1.1-211.10.1.1)/X-late

WebUI (分公司 B)

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 201.1.1.1/24
   Interface Mode: Route

   Network > Interfaces > Edit (對於 ethernet3) > DIP > New: 輸入下面的內容，然後按一下 **OK**:

   ID: 5
   IP Address Range: 211.20.1.1 ~ 211.20.1.1
       Port Translation: (選擇)
   Extended IP/Netmask: 211.20.1.10/255.255.255.0

2. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: HQ
   IP Address/Domain Name:
       IP/Netmask: (選擇), 200.1.1.1/32
   Zone: Untrust

3. **路由**

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP address: 201.1.1.254

4. **政策**

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), HQ
   Service: ANY
   Action: Permit
   Position at Top: (選擇)

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   NAT:
   Source Translation: (選擇)
   DIP On: (選擇), 5 (211.20.1.1-211.20.1.1)/X-late

CLI (分公司 A)

1. 介面
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 195.1.1.1/24
   set interface ethernet3 route
   set interface ethernet3 ext ip 211.10.1.10 255.255.255.0 dip 5 211.10.1.1

2. 位址
   set address untrust hq 200.1.1.1/32

3. 路由
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 195.1.1.254

4. 政策
   set policy from trust to untrust any any any permit
   set policy top from trust to untrust any hq any nat src dip 5 permit
   save

CLI (分公司 B)

1. 介面
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 201.1.1.1/24
   set interface ethernet3 route
   set interface ethernet3 ext ip 211.20.1.10 255.255.255.0 dip 5 211.20.1.1

2. 位址
   set address untrust hq 200.1.1.1/32

3. 路由
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.1.1.254

4. 政策
   set policy from trust to untrust any any any permit
   set policy top from trust to untrust any hq any nat src dip 5 permit
   save

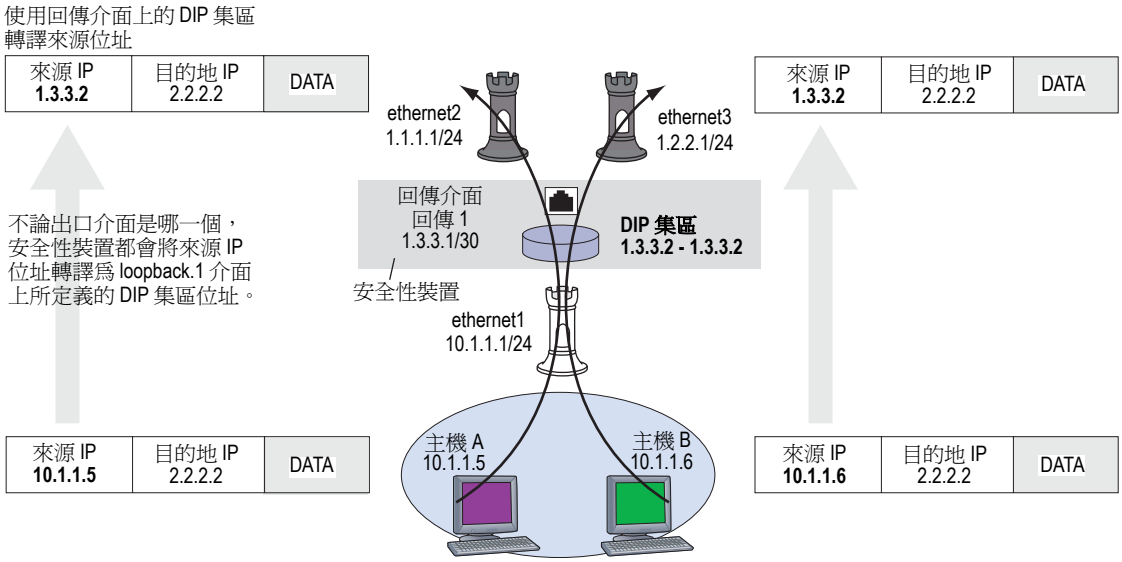
在回傳介面上使用 DIP

回傳介面是一個邏輯介面，只要其所在的裝置開啓，則該介面永遠處於工作中的狀態。您可以在回傳介面上建立一個動態 IP (DIP) 位址集區，如此在執行來源位址轉譯時，屬於其相關回傳介面群組的介面群組即可存取該集區。安全性裝置從這類 DIP 集區所取得的位址與回傳介面 IP 位址處於相同的子網路中，而不是在任何成員介面的子網路中。(請注意，DIP 集區中的位址不得與介面 IP 或任何已於回傳介面定義的 MIP 位址重疊。)

注意 : 如需回傳介面的詳細資訊，請參閱第 56 頁上的「回傳介面」。

將 DIP 集區放置在回傳介面上的主要應用方式是 : 將來源位址轉譯爲相同位址或位址範圍，但不同的封包可能會使用不同的出口介面。

圖 67: 回傳 DIP



在本範例中，安全性裝置從不同的網際網路服務供應商 (ISP) 接收到兩個 Untrust 區域介面的 IP 位址 : ISP-1 與 ISP-2:

- ethernet2、1.1.1.1/24、ISP-1
- ethernet3、1.2.2.1/24、ISP-2

將這些介面連結到 Untrust 區域，然後將之指派至上列 IP 位址。並將 ethernet1 連結到 Trust 區域，然後爲其指派 IP 位址 10.1.1.1/24。

您希望安全性裝置能將 Trust 區域中的向外通訊流量中的來源位址轉譯爲 Untrust 區域中的遠端辦公室。轉譯出來的位址必須是相同的 IP 位址 (1.3.3.2)，因此遠端辦公室的政策僅允許來自該 IP 位址的向內通訊流量。您先前已取得公開 IP 位址 1.3.3.1 與 1.3.3.2，且已通知兩個 ISP 您除了使用其指派給裝置的位址外，亦使用這些位址。

您以 IP 位址 1.3.3.1/30 組態回傳介面 loopback.1，並以 1.3.3.2 - 1.3.3.2 組態介面上的 DIP 集區。DIP 集區的 ID 號碼是 10。而後，您將 ethernet1 與 ethernet2 加入 loopback.1 回傳群組，成爲該群組成員。

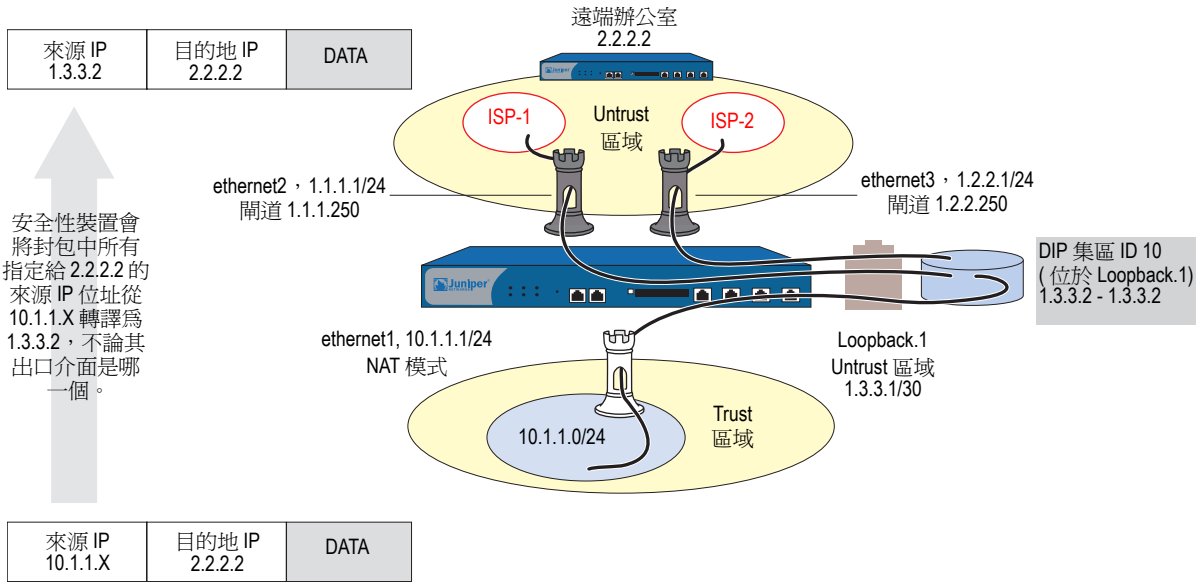
定義名爲 "r-office" 的遠端辦公室位址 (IP 位址爲 2.2.2.2/32)，並定義分別指向 ISP-1 與 ISP-2 路由器的 ethernet1 與 ethernet2 介面預設路由。

定義向外通訊流量所使用的兩個閘道路由。由於您對兩個路由並沒有偏好，因此不將計量加入路由中。向外通訊流量可能會流向任一個路由。

注意： 若要指出路由偏好 (即將計量加入兩個路由)，請將較高的計量加入您偏好的路由，也就是較相近 1 的值。

最後您建立一個政策，此政策所套用的來源位址轉譯 (NAT-src) 方式是：向外通訊流量轉譯至遠端辦公室。政策參考 DIP 集區 ID 10。

圖 68: 回傳 DIP 政策



WebUI

1. 介面

   Network > Interfaces > New Loopback IF: 輸入下面的內容，然後按一下 **OK**:

   Interface Name: loopback.1
   Zone: Untrust (trust-vr)
   IP Address/Netmask: 1.3.3.1/30

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   As member of loopback group: loopback.1
   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

Network > Interfaces > Edit (對於 ethernet2): 輸入下面的內容，然後按一下 **OK**:

As member of loopback group: loopback.1
Zone Name: Untrust
Static IP: (出現時選擇此選項)
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

Zone Name: Untrust
Static IP: (出現時選擇此選項)
IP Address/Netmask: 1.2.2.1/24
Interface Mode: Route

2. **DIP 集區**

Network > Interfaces > Edit (對於 loopback.1) > DIP > New: 輸入下面的內容，然後按一下 **OK**:

ID: 5
IP Address Range: 1.3.3.2 ~ 1.3.3.2
Port Translation: (選擇)

3. **位址**

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

Address Name: r-office
IP Address/Domain Name:
IP/Netmask: (選擇), 2.2.2.2/32
Zone: Untrust

4. **路由**

Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (選擇)
Interface: ethernet2
Gateway IP address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (選擇)
Interface: ethernet3
Gateway IP address: 1.2.2.250

5. **政策**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), r-office
   Service: ANY
   Action: Permit

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   NAT:
   Source Translation: (選擇)
   DIP On: (選擇), 10 (1.3.3.2-1.3.3.2)/port-xlate

CLI

1. **介面**
   set interface loopback.1 zone untrust
   set interface loopback.1 ip 1.3.3.1/30
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 zone untrust
   set interface ethernet2 ip 1.1.1.1/24
   set interface ethernet2 loopback-group loopback.1
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.2.2.1/24
   set interface ethernet3 loopback-group loopback.1

2. **DIP 集區**
   set interface loopback.1 dip 10 1.3.3.2 1.3.3.2

3. **位址**
   set address untrust r-office 2.2.2.2/32

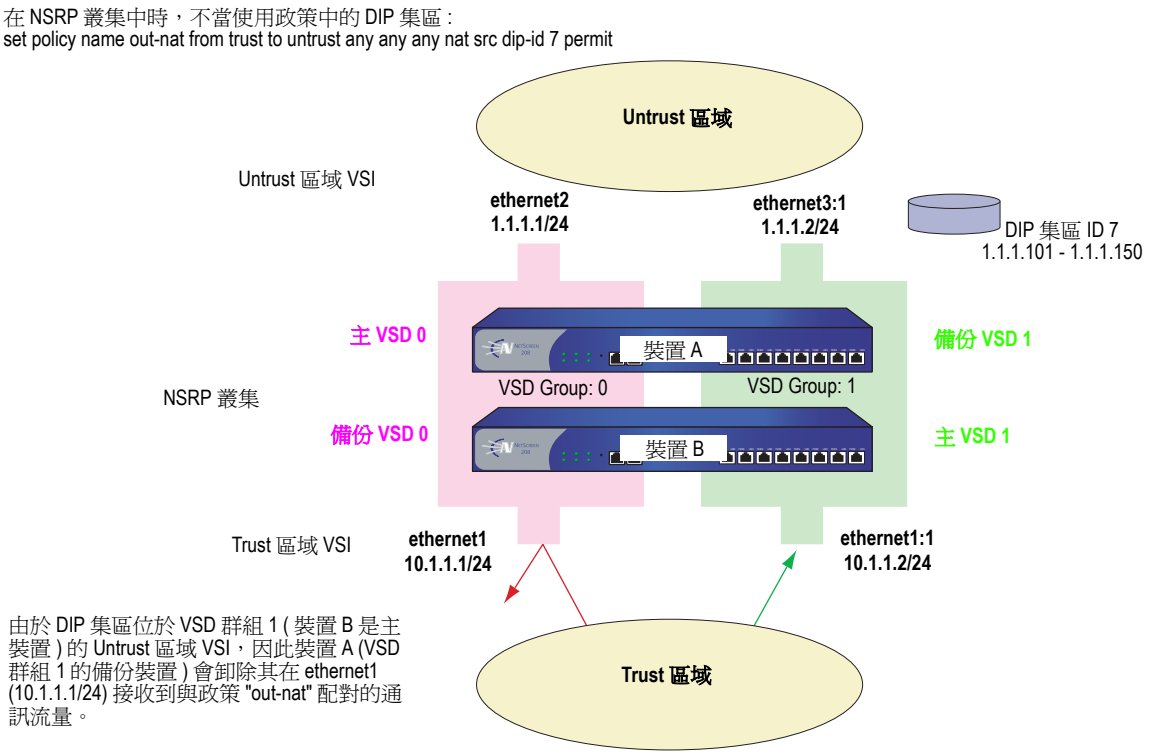
4. **路由**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet2 gateway 1.1.1.250
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.2.2.250

5. **政策**
   set policy from trust to untrust any r-office any nat src dip-id 10 permit
   save

建立 DIP 群組

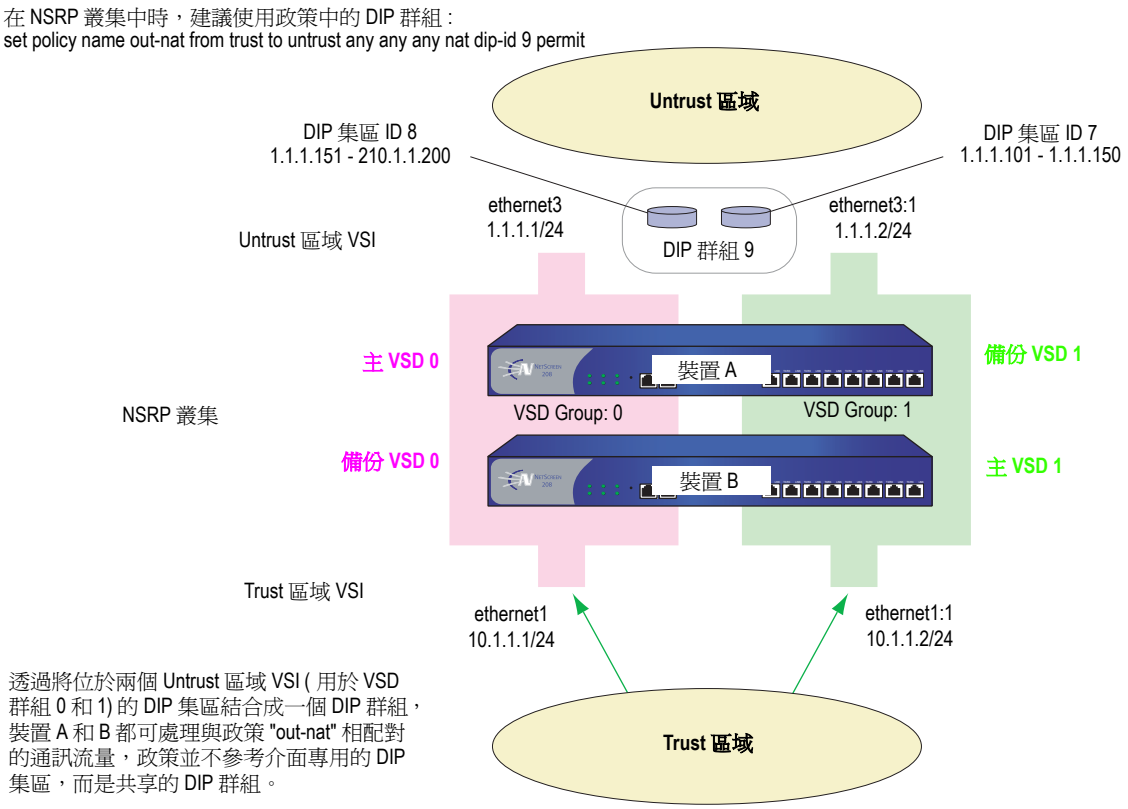
當您將兩個安全性裝置群組成冗餘叢集，以提供雙重主動組態的高可用性 (HA) 時，兩個裝置會共享相同的組態並同時處理通訊流量。定義使用動態 IP (DIP) 集區 (位於一個 VSI 上) 執行網路位址轉譯 (NAT) 的政策時，可能會出現問題。因爲僅在安全性裝置作爲連結 VSI 的 VSD 群組的主裝置時，該 VSI 才是活動的，因此任何傳送到其他安全性裝置 (作爲該 VSD 群組的備份裝置) 的通訊流量無法使用該 DIP 集區並被卸除。

圖 69: 具一個 VSI 的 NAT 的 DIP 問題



爲了解決此問題，您可以建立兩個 DIP 集區 (一個在每個 VSD 群組的 Untrust 區域 VSI 上)，並將兩個 DIP 集區結合成一個在政策中參考的 DIP 群組。即使政策指定 DIP 群組，每個 VSI 仍會使用自己的 VSD 集區。

圖 70: 在一個 DIP 群組中建立兩個 DIP 集區



注意： 如需爲 HA 設定安全性裝置的詳細資訊，請參閱*第 11 卷：高可用性*。

在本範例中，您在雙重主動 HA 對中的兩個安全性裝置 (裝置 A 和 B) 上提供 NAT 服務。

建立兩個 DIP 集區 - ethernet3 上的 DIP 5 (1.1.1.20 - 1.1.1.29) 和 ethernet3:1 上的 DIP 6 (1.1.1.30 - 1.1.1.39)。然後將它們結合成一個 DIP 群組並識別爲 DIP 7，在政策中參考。

VSD 群組 0 和 1 的 VSI 如下：

- Untrust 區域 VSI ethernet3 1.1.1.1/24 (VSD 群組 0)
- Untrust 區域 VSI ethernet3:1 1.1.1.2/24 (VSD 群組 1)
- Trust 區域 VSI ethernet1 10.1.1.1/24 (VSD 群組 0)
- Trust 區域 VSI ethernet1:1 10.1.1.1/24 (VSD 群組 1)

假設您已經設定 NSRP 叢集中的裝置 A 和 B，建立 VSD 群組 1（將裝置放入 NSRP 叢集時，ScreenOS 自動建立 VSD 群組 0），並組態上述的介面。（如需爲 NSRP 組態安全性裝置的資訊，請參閱*第 11 卷：高可用性*。）

WebUI

1. **DIP 集區**
   Network > Interfaces > Edit（對於 ethernet3）> DIP > New: 輸入下面的內容，然後按一下 **OK**:

   ID: 5
   IP Address Range: 1.1.1.20 - 1.1.1.29
   Port Translation: (選擇)

   Network > Interfaces > Edit（對於 ethernet3:1）> DIP > New: 輸入下面的內容，然後按一下 **OK**:

   ID: 6
   IP Address Range: 1.1.1.30 - 1.1.1.39
   Port Translation: (選擇)

注意： 在本版發行時，您只能透過 CLI 定義 DIP 群組。

2. **政策**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面：

   NAT:
   Source Translation: (選擇)
   DIP On: (選擇), 7

CLI

1. **DIP 集區**
   set interface ethernet3 dip 5 1.1.1.20 1.1.1.29
   set interface ethernet3:1 dip 6 1.1.1.30 1.1.1.39

2. **DIP 群組**
   set dip group 7 member 5
   set dip group 7 member 6

3. **政策**
   set policy from trust to untrust any any any nat src dip-id 7 permit
   save

設定遞迴排程

排程是一個可組態的物件，您可以將其與一個或多個政策相關聯以定義政策生效的時間。透過套用排程，可以控制網路通訊流量並強制網路安全性。

定義排程時，請輸入下列參數的值：

- **Schedule Name:** 出現在 Policy Configuration 對話方塊的 Schedule 下拉式清單中的名稱。請選擇說明性的名稱以協助識別排程。名稱必須是唯一的，而且限制在 19 個字元以內。
- **Comment:** 要新增的任何其他資訊。
- **Recurring:** 在希望排程每周重複時啓用本選項。

  Start and End Times: 必須組態開始和結束時間。同一天內最多可指定兩個時間週期。
- **Once:** 希望排程只開始和結束一次時啓用本選項。

  mm/dd/yyyy hh:mm: 必須輸入開始和停止的日期和時間。

在本範例中，有一個叫做 Tom 的雇員，他在下班後使用公司的網際網路進行私人事務。您建立非上班時間的排程，可以和政策相關聯，以在正常上班時間以外拒絕發自該職員電腦 (10.1.1.5/32) 的向外 TCP/IP 通訊流量。

WebUI

1. **排程**
   Objects > Schedules > New: 輸入下面的內容，然後按一下 **OK**:

   Schedule Name: After Hours
   Comment: For non-business hours
   Recurring: (選擇)

週期 1:

Weekday	Start Time	End Time
Sunday	00:00	23:59
Monday	00:00	06:00
Tuesday	00:00	06:00
Wednesday	00:00	06:00
Thursday	00:00	06:00
Friday	00:00	06:00
Saturday	00:00	23:59

週期 2:

Weekday	Start Time	End Time
Sunday	17:00	23:59
Monday	17:00	23:59
Tuesday	17:00	23:59
Wednesday	17:00	23:59
Thursday	17:00	23:59
Friday	17:00	23:59
Saturday	17:00	23:59

2. 位址
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: Tom
   Comment: Temp
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.1.5/32
   Zone: Trust

3. 政策
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Name: No Net
   Source Address:
   Address Book Entry: (選擇), Tom
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: HTTP
   Action: Deny
   Schedule: After Hours

CLI

1. 排程
   set schedule "after hours" recurrent sunday start 00:00 stop 23:59
   set schedule "after hours" recurrent monday start 00:00 stop 06:00 start 17:00 stop 23:59
   set schedule "after hours" recurrent tuesday start 00:00 stop 06:00 start 17:00 stop 23:59
   set schedule "after hours" recurrent wednesday start 00:00 stop 06:00 start 17:00 stop 23:59
   set schedule "after hours" recurrent thursday start 00:00 stop 06:00 start 17:00 stop 23:59
   set schedule "after hours" recurrent friday start 00:00 stop 06:00 start 17:00 stop 23:59
   set schedule "after hours" recurrent saturday start 00:00 stop 23:59 comment "for non-business hours"

2. 位址
   set address trust tom 10.1.1.5/32 "temp"

3. 政策
   set policy from trust to untrust tom any http deny schedule "after hours"
   save

第 6 章
政策

安全性裝置的預設行爲是拒絕安全區之間所有的通訊流量 (區域間通訊流量)，而且 (除了 Untrust 區域內的通訊流以外) 允許連結到相同區域的介面之間所有的通訊流量 (區域內部通訊流量)。爲了允許選取的區域間通訊流量通過安全性裝置，您必須建立覆寫預設行爲的區域間政策。同樣，爲了防止選取的區域內部通訊流量通過安全性裝置，必須建立區域內部政策。

注意： 依預設，NetScreen-5XP 及 NetScreen-5XT 均允許自 Trust 區域至 Untrust 區域的通訊流量。

本章介紹政策的功能以及組成政策的不同元素之間的關係。本章包含下列各節 :

- 第 154 頁上的「基本元素」
- 第 155 頁上的「三種類型的政策」
- 第 157 頁上的「政策組清單」
- 第 158 頁上的「政策定義」
- 第 166 頁上的「套用的政策」

注意： 如果組態安全性裝置上的多點傳送路由設定，您可能必須組態多點傳送政策。如需關於多點傳送政策的資訊，請參閱第 **7**-120 頁上的「多點傳送政策」。

基本元素

允許、拒絕或設定兩點之間指定類型單向通訊流量通道的政策。通訊流量 (或「服務」) 的類型、兩個端點的位置以及調用的動作構成政策的基本元素。雖然也可以有其他元件，但是共同構成政策核心部份的必要元素如下 :

注意 : "tunnel" 動作 (VPN 或 L2TP 通道)，隱含「允許」的概念。

- **Direction** - 兩個安全區 (從來源區域到目的地區域) 之間通訊流量的方向
- **Source Address** - 發起通訊流量的位址
- **Destination Address** - 通訊流量傳送到的位址
- **Service**- 傳輸的通訊流量類型
- **Action** - 安全性裝置接收到滿足前四個標準的通訊流量時執行的動作，這些標準爲 : deny (拒絕)、permit (允許)、reject (駁回) 或 tunnel (開通)

例如，在下列 CLI 指令中陳述的政策允許 FTP 通訊流量從 Trust 區域中的任何位址流向 DMZ 區域中名爲 "server1" 的 FTP 伺服器 :

set policy from trust to untrust any server1 ftp permit

- **Direction**: **from trust to untrust** (即從 Trust 區域到 Untrust 區域)
- **Source Address**: **any** (即 Trust 區域中的任何位址。術語 "any" 代表套用到區域中任何位址的預先定義位址)
- **Destination Address**: **server1** (Untrust 區域通訊錄中使用者定義的位址)
- **Service**: **ftp** (檔案傳輸通訊協定)
- **Action**: **permit** (安全性裝置允許此通訊流量通過其防火牆)

三種類型的政策

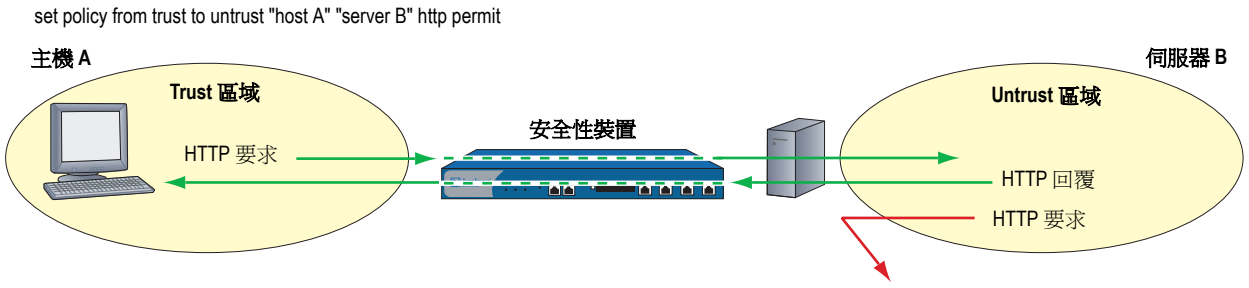
您可以透過下列三種政策控制通訊流量的流動 :

- 透過建立區域間政策，可以管理允許從一個安全區到另一個安全區的通訊流量種類。
- 透過建立區域內部政策，也可以控制允許透過連結到相同區域的介面之間的通訊流量類型。
- 透過建立全域政策，可以管理位址之間的通訊流量，不考慮它們的安全區。

區域間政策

區域間政策可控制安全區之間的通訊流量。可以設定區域間政策來拒絕、允許、駁回或開通從一個區域到另一個區域的通訊流量通道。使用狀態檢查技術，安全性裝置會維護活動 TCP 會話表和活動 UDP "pseudo" 會話表，以便能夠允許回應服務要求。例如，如果有一個政策允許從 Trust 區域中的主機 A 到 Untrust 區域中的伺服器 B 的 HTTP 要求，當安全性裝置接收到從伺服器 B 到主機 A 的 HTTP 回應時，安全性裝置將接收到的封包與表對照檢查。找到回應已認可 HTTP 要求的封包時，安全性裝置允許來自 Untrust 區域中伺服器 B 的封包跨越防火牆到達 Trust 區域中的主機 A。若要允許由伺服器 B 發起、流向主機 A 的通訊流量 (不只是回應由主機 A 發起的通訊流量)，必須建立從 Untrust 區域中伺服器 B 到 Trust 區域中主機 A 的第二個政策。

圖 71: 區域間政策

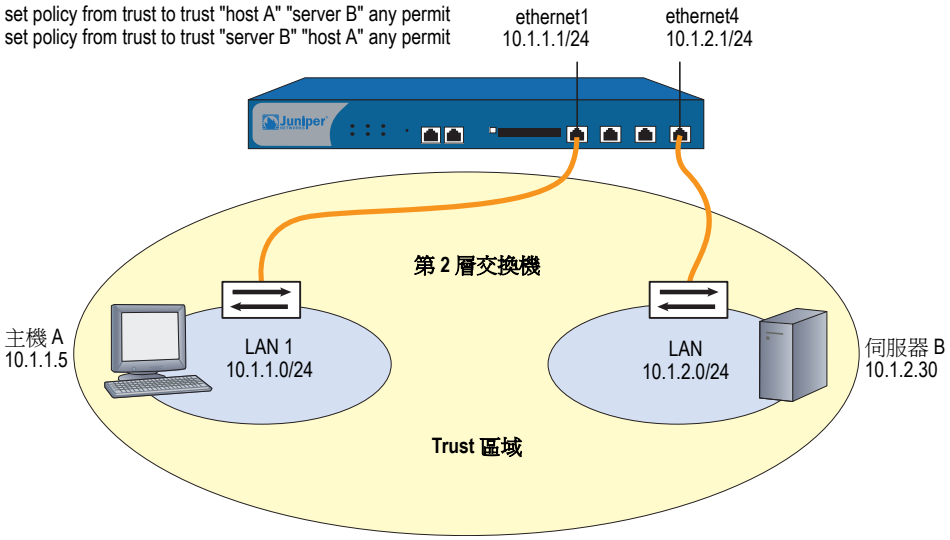


注意 : 安全性裝置會拒絕來自伺服器 B 的 HTTP 請求，因爲並無任何允許此作業的政策。

區域部政策

區域間政策提供可控制連結到相同安全區的介面間通訊流量。來源位址和目的地位址都在相同的安全區中，但是透過安全性裝置上的不同介面到達。與區域間政策一樣，區域內部政策也控制通訊流量單向流動。若要允許從資料路徑任一端發起的通訊流量，必須建立兩個政策，每個方向一個政策。

圖 72: 區域內部政策



區域間政策不支援 VPN 通道，或於介面層級設定的來源網路位址轉譯 (**set interface** *interface* **nat**)。但是區域間政策支援以政策爲基礎的 NAT-src 與 NAT-dst。若政策參考對應的 IP (MIP) 作爲目的地位址時，其亦支援目的地位址轉譯。(如需有關 NAT-src、NAT-dst 與 MIP 的資訊，請參閱 *第 8 卷: 位址轉譯*。)

全域政策

與區域間和區域內部政策不同，全域政策不參考特定的來源和目的地區域。全域政策會參考使用者定義的 Global 區域位址或預先定義的 Global 區域位址 "any"。這些位址可以跨越多個安全區。例如，如果要提供對多個區域的存取或從多個區域進行存取，您可以建立具有 Global 區域位址 "any" 的全域政策，其中包含所有 區域中的所有位址。

注意： 在本版本發行時，全域政策不支援來源網路位址轉譯 (NAT-src)、VPN 通道或「透明」模式。但您可以在全域政策中指定 MIP 或 VIP 作爲目的地位址。

政策組清單

安全性裝置維護三種不同的政策組清單，每種政策組清單對應到下列三種政策之一 :

- 區域間政策
- 區域內部政策
- 全域政策

安全性裝置接收到發起新會話的封包時，會記錄入口介面，因而得知介面連結的來源區域。然後安全性裝置執行路由查詢以確定出口介面，進而確定該介面連結的目的地區域。使用來源區域和目的地區域，安全性裝置可以執行政策查詢，按下面的順序查閱政策組清單 :

1. 如果來源區域和目的地區域不同，安全性裝置會在區域間政策組清單中執行政策查詢。

   (或)

   如果來源區域和目的地區域不同，安全性裝置會在區域內部政策組清單中執行政策查詢。

2. 如果安全性裝置執行區域間或區域內部政策查詢，但是找不到配對的政策，安全性裝置會檢查全域政策組清單以查詢配對的政策。

3. 如果安全性裝置執行區域間和全域政策查詢，但是沒有找到配對政策，安全性裝置會將預設的允許 / 拒絕政策套用到封包。**unset/set policy default-permit-all**。

   (或)

   如果安全性裝置執行區域間和全域政策查詢，但是沒有找到配對政策，安全性裝置會將該區域的區域間阻斷設定套用到封包 : **unset/set zone** *zone* **block**。

安全性裝置會從上而下搜尋每個政策組清單。因此，您必須在清單中將較爲具體的政策放在比較不具體的政策上面。(如需政策順序的資訊，請參閱第 182 頁上的「重新排序政策」。)

政策定義

防火牆提供具有單一出入點的網路邊界。由於所有通訊流量都必須通過此點，您可以篩選並引導透過執行政策組清單 (區域間政策、內部區域政策和全域政策) 產生的通訊流量。

政策可讓您拒絕、允許、駁回 (拒絕並傳送無法到達 TCP RST 或 ICMP 連接埠的訊息給來源主機)、加密與解密、驗證、排定優先次序、排程、篩選及監看嘗試跨過一個安全區到另一個安全區的通訊流量。您決定哪些使用者和資料能進入和離開，以及它們可以離開的時間和地點。

注意： 對於支援虛擬系統的安全性裝置來說，根系統中的政策組不會影響虛擬系統中的政策組。

政策和規則

單一使用者定義的政策會在內部產生一個或多個邏輯規則，而每個邏輯規則都由一組元件 (來源位址、目的地位址和服務) 組成。元件會消耗記憶體資源。參考元件的邏輯規則不會消耗記憶體資源。

根據來源位址群組、目的地位址群組以及政策中服務元件的使用情況而定，邏輯規則的數量可以遠遠超過建立單一政策時明顯可見的數量。例如，下面的政策會產生 125 個邏輯規則 :

1 個政策 : 5 個來源位址 x 5 個目的地位址 x 5 個服務 = 125 個邏輯規則

但是，安全性裝置不會爲每個邏輯規則複製元件。規則以不同的組合使用同一組元件。例如，產生 125 個邏輯規則的上述政策只生成 15 個元件 :

5 個來源位址 + 5 個目的地位址 + 5 個服務 = 15 個元件

這 15 個元件以不同方式組合，產生由單個政策產生的 125 個邏輯規則。允許多個邏輯規則以不同組合使用同一組元件，與每個邏輯規則與其元件具有一對一關係相比，安全性裝置消耗的資源更少。

由於新政策的安裝時間與安全性裝置新增、刪除或修改的元件數量成比例，因此元件較少時政策的安裝就更快。同樣，與每個規則都需要專用元件相比，透過允許大量的邏輯規則共用一小組元件，安全性讓使用者能建立更多的政策，安全性裝置也能建立更多的規則。

政策的結構

政策必須包含下列元素 :

- ID (自動產生，但可爲 CLI 中的使用者定義項目)
- 區域 (來源和目的地)
- 位址 (來源和目的地)
- 服務
- 動作 (deny, permit, reject, tunnel)

政策也可以包含下列元素 :

- 應用程式
- 名稱
- VPN 通道
- L2TP 通道
- 深入檢查
- 政策清單上方配置
- 來源位址轉譯
- 目的地位址轉譯
- 使用者 Auth
- HA 會話備份
- Web 篩選
- 記錄
- 計數
- 通訊流量警示臨界值
- 排程
- 防毒掃描
- 通訊流量整理

本節的其餘部分將依序分析上述的每一個元素。

ID

每一項政策均具有 ID number，不論是由您所定義的號碼，或是安全性裝置自動指派的號碼。您僅能定義透過 CLI 中已設定的政策指定來定義 ID number: **set policy id** *number …* 得知 ID number 後，您即可輸入政策內容以發出進一步的指令來修改政策。(如需關於政策內容的詳細資訊，請參閱第 177 頁上的「輸入政策內容」。)

區域

區域可以是已套用安全措施的網路空間片段 (安全區)、連結了 VPN 通道介面的邏輯片段 (通道區域)，或者是一個執行特定功能的實體或邏輯項目 (功能區)。政策允許通訊流量在兩個安全區之間流動 (區域間政策)，或在兩個連結到相同區域的介面之間流動 (區域內政策)。(如需詳細資訊，請參閱第 25 頁上的「區域」、第 155 頁上的「區域間政策」和第 156 頁上的「區域部政策」。)

位址

位址是透過相對於防火牆 (在一個安全區中) 的位置，用來識別網路裝置 (如主機和網路) 的物件。個別的主機使用遮罩 255.255.255.255 指定，表示位址所有的 32 位元都有意義。網路使用其子網路遮罩指定，指示有意義的位元。若要爲特定位址建立政策，您必須先在通訊錄中建立相關主機和網路的項目。

您也可以建立位址群組，並將政策套用到位址群組，就像套用到其他通訊錄項目一樣。將位址群組當作政策的元素使用時，請注意由於安全性裝置將政策套用到群組中的每個位址，可用的內部邏輯規則數目和組成這些規則的元件數目將會比預期的更快耗盡。來源和目的地位址都使用位址群組時就特別有這個危險。(如需詳細資訊，請參閱第 158 頁上的「政策和規則」。)

服務

服務是使用第 4 層資訊 (如應用程式服務 Telnet、FTP、SMTP 和 HTTP 的標準和公認的 TCP 和 UDP 連接埠號碼) 識別應用程式通訊協定的物件。ScreenOS 包括預先定義的核心網際網路服務。此外，也可以定義自訂服務。

您可以定義政策，指定允許、拒絕、加密、驗證、記錄或統計哪些服務。

動作

動作是說明防火牆如何處理所接收通訊流量的物件。

- **Deny** 阻斷封包，使之不能通過防火牆。
- **Permit** 允許封包通過防火牆。
- **Reject** 阻斷封包，使之不能通過防火牆。安全性裝置會卸除封包並將 TCP 通訊流量的 TCP 重設 (RST) 片段傳送至來源主機，同時傳送一則 UDP 通訊流量的 ICMP "destination unreachable, port unreachable" 訊息 (類型 3，代碼 3)。如果通訊流量類型不是 TCP 和 UDP，安全性裝置會在不通知來源主機的情況下卸除封包，這與執行 "deny" 動作時的情況相同。

注意： 安全性裝置會在接收 (與卸除) TCP 片段 (具有與另一個 RST 不同的任一代碼位元組) 之後傳送 TCP RST。

當入口介面執行於 Layer 2 或 3 且通訊協定爲 TCP 時，TCP RST 中的來源 IP 位址是原始封包 (已卸除) 中的目的地 IP 位址。當入口介面執行於 Layer 2 且通訊協定爲 UDP 時，ICMP 訊息中的來源 IP 位址同時也是原始封包中的目的地 IP 位址。不過，如果入口介面執行於 Layer 3 且通訊協定爲 UDP，則 ICMP 訊息中的來源 IP 位址爲入口介面的 IP 位址。

- **Tunnel** 封裝向外 IP 封包和解除內向 IP 封包的封裝。對於 IPSec VPN 通道，指定要使用的 VPN 通道。對於 L2TP 通道，指定要使用的 L2TP 通道。對於 IPSec 上的 L2TP，指定 IPSec VPN 通道和 L2TP 通道。

注意： 對於 IPSec 上的 L2TP，IPSec VPN 通道的來源位址和目的地位址必須與 L2TP 通道的來源位址和目的地位址相同。

安全性裝置將指定動作套用到與預先提供的標準配對的通訊流量，這些標準爲：區域 (來源區域和目的地區域)、位址 (來源位址和目的地位址) 以及服務。

應用程式

應用程式選項指定對應至第 4 層服務 (您於政策中所參考的服務) 的第 7 層應用程式。預先定義的服務已具有至第 7 層應用程式的對應。然而就自訂服務而言，您必須明確地將服務連結至應用程式，特別是當您想要讓政策將「應用程式層閘道」(ALG) 或「深入檢查」套用至自訂服務時。

注意 : ScreenOS 支援用於多種服務的 ALG，包括 DNS、FTP、H.323、HTTP、RSH、SIP、Telnet 與 TFTP。

若要 ALG 套用至自訂服務，須執行下列兩個步驟 :

- 以名稱、逾時值、傳輸通訊協定及來源與目的地連接埠定義自訂服務。
- 組態政策時，參考該服務及想要套用的 ALG 應用程式類型。

如需有關將 Deep Inspection (深入檢查) 套用至自訂服務的資訊，請參閱 第 **4**-123 頁上的「對應自訂服務至應用程式」。

名稱

您可以爲政策取一個說明性的名稱，作爲識別其用途的便利方法。

注意 : 若需有關 ScreenOS 命名慣例的資訊，即套用至您爲政策所建立的名稱，請參閱第 xiv 頁上的「命名慣例和字元類型」。

VPN 通道

可以將單一或多個政策套用到已組態的任何 VPN 通道。在 WebUI 中，VPN Tunnel 選項提供所有這類通道的下拉式清單。在 CLI 中，可以用 **get vpn** 指令查看所有可用的通道。(如需詳細資訊，請參閱第 **5**-71 頁上的「站台對站台的虛擬私人網路」和第 **5**-147 頁上的「撥接虛擬私人網路」。)

當 VPN 通道兩端的 VPN 組態都使用以 NAT 爲基礎的政策時，兩個閘道裝置的管理員都需要建立向內和向外政策 (總共有四個政策)。當 VPN 政策構成配對組 (也就是，除來源位址和目的地位址反向外，向內和向外政策組態中的任何內容都相同) 時，可以組態一個政策，然後選擇 **Modify matching bidirectional VPN policy** 核取方塊，自動爲相反的方向建立第二個政策。對於新政策的組態，matching VPN policy 核取方塊依預設爲不選取。對於配對組成員的現有政策修改，依預設，該核取方塊被選取，並且對一個政策所作的變更會傳播到其他的政策。

注意 : 此選項只能透過 WebUI 使用。若下列政策元件中的任一元件具有多個項目，即不支援此選項 : 來源位址、目的地位址或服務。

L2TP 通道

可以將單一或多個政策套用到已組態的任何「第 2 層通道通訊協定 (L2TP)」通道。在 WebUI 中，L2TP 選項提供所有這些通道的下拉式清單。您可利用 CLI 的 **get l2tp *tunn_str* active** 指令來顯示活動中 L2TP 通道的狀態，並使用 **get l2tp all** 指令查看所有可用的通道。也可以將 VPN 通道和 L2TP 通道組合在一起 (如果兩者有相同的端點)，以建立結合每個通道特徵的通道。這稱爲 IPSec 上的 L2TP。

注意： 處於「透明」模式的安全性裝置不支援 L2TP。

深入檢查

深入檢查 (DI) 是一種篩選「網路」與「傳輸層」上所允許之通訊流量的機制，藉由檢驗這些層以及「應用程式層」上的內容與通訊協定特性來達到篩選的目的。DI 的目標是偵測與預防任何可能出現在 Juniper Networks 防火牆所允許通訊流量中的任何攻擊與異常行爲。

注意： 在 Open Systems Interconnection (OSI) 模型中，「網路層」爲「第 3 層」、「傳輸層」爲「第 4 層」、「應用程式層」爲「第 7 層」。OSI 模式網路通訊協定架構的網路產業標準模型。OSI 模型共有七層。

若要組態用來預防攻擊的政策，您必須做出兩個選擇：要使用哪一個攻擊群組 (或多個攻擊群組)，以及若偵測到攻擊，要採取什麼攻擊動作。(如需詳細資訊，請參閱第 **4**-91 頁上的「深入檢查」。)

政策清單上方配置

依預設，ScreenOS 將最近建立的政策放在政策組清單的底部。如果需要重新定位政策，可以使用在第 182 頁上的「重新排序政策」中說明的政策重新排序方法。將最近建立的政策重新定位到政策清單的最上面時，爲避免額外的步驟，可以在 WebUI 中選擇 **Position at Top** 選項，或在 CLI 中的 **set policy** 指令中使用關鍵字 **top** (**set policy top …**)。

來源位址轉譯

您可在政策層級套用來源位址轉譯 (NAT-src)。您可以使用 NAT 轉譯向內或向外網路和 VPN 通訊流量中的來源位址。新的來源位址可以是來自動態 IP (DIP) 集區或出口介面的位址。NAT-src 亦支援來源連接埠位址轉譯 (PAT)。如需所有可用 NAT-src 選項的資訊，請參閱 第 **8**-13 頁上的「來源網路位址轉譯」。

注意： 您亦可於介面層級執行來源位址轉譯，即所知的網路位址轉譯 (NAT)。如需有關介面層級 NAT-src 或 NAT 的資訊，請參閱 第 90 頁上的「NAT 模式」。

目的地位址轉譯

您可在政策層級套用目的地位址轉譯 (NAT-dst)。您可以使用 NAT-dst 轉譯向內或向外網路和 VPN 通訊流量中的目的地位址。NAT-dst 亦可支援目的地連接埠對應。如需所有可用 NAT-dst 選項的資訊，請參閱 第 **8**-25 頁上的「目的地網路位址轉譯」。

使用者 Auth

選擇此選項要求來源位址上的 auth 使用者，在允許通訊流量跨越防火牆或進入 VPN 通道前，提供使用者名稱和密碼以 Auth 身份。安全性裝置可以使用本機資料庫或外部 RADIUS、SecurID 或 LDAP Auth 伺服器以執行驗證檢查。

注意 : 如果將需要驗證的政策套用到 IP 位址的子網路，則子網路中的每個 IP 位址都需要驗證。

如果主機支援多個 Auth 使用者帳號 (就像執行 Telnet 的 Unix 主機)，則在安全性裝置驗證第一個使用者後，該主機的所有其他使用者都可以繼承第一個使用者的權限，讓通訊流量通過安全性裝置而不必經過驗證。

ScreenOS 提供兩種驗證方案 :

- 執行階段 Auth，在收到與啓用驗證的政策配對的 HTTP、FTP 或 Telnet 通訊流量時，安全性裝置會提示 Auth 使用者登入
- WebAuth，透過安全性裝置傳送通訊流量前，使用者必須驗證自己

執行階段 Auth

執行階段 Auth 的過程如下 :

1. auth 使用者傳送 HTTP、FTP 或 Telnet 連接要求到目的地位址時，安全性裝置會截取封包並對其進行緩衝。
2. 安全性裝置向 auth 使用者傳送登入提示。
3. auth 使用者用自己的使用者名稱和密碼回應此提示。
4. 安全性裝置驗證 auth 使用者的登入資訊。

   如果驗證成功，就會在 auth 使用者和目的地位址之間建立連接。

對於初始的連接要求，政策必須包括下列三個服務中的一項或所有服務 : Telnet、HTTP 或 FTP。只有具有這些服務中的一個或所有服務的政策才能啓動驗證過程。可以在涉及使用者驗證的政策中使用下列的任何服務 :

- Any (因爲 "any" 包括所有三項必要的服務)。
- Telnet 或 FTP 或 HTTP。
- 包括所希望的服務或多個服務的服務群組，加上啓動驗證過程必要的三個服務中的一個或多個 (Telnet、FTP 或 HTTP)。例如，可以建立名爲 "Login" 的自訂服務群組，支援 FTP、NetMeeting 和 H.323 服務。然後，在建立政策時，指定服務爲 "Login"。

對於成功驗證後進行的任何連接，在政策中指定的所有服務都有效。

注意 : 已啓用驗證的政策不支援將 DNS (連接埠爲 53) 作爲服務。

政策前檢查 Auth (WebAuth)
WebAuth Auth 的過程如下：

1. Auth 使用者建立連至 WebAuth 伺服器 IP 位址的 HTTP 連線。
2. 安全性裝置向 auth 使用者傳送登入提示。
3. auth 使用者用自己的使用者名稱和密碼回應此提示。
4. 安全性裝置或外部驗證伺服器驗證 auth 使用者的登入資訊。

   如果驗證嘗試成功，則安全性裝置允許 auth 使用者啓動通訊流量，使之流向在強制透過 WebAuth 方法執行驗證的政策中指定的目的地位置。

注意： 如需這兩種使用者 Auth 方法的詳細資訊，請參閱第 **9**-32 頁上的「在政策中參考 Auth 使用者」。

透過選擇特定的使用者群組、本機或外部使用者、或群組運算式，可以限制或擴展套用政策的 Auth 使用者範圍。(如需群組運算式的詳細資訊，請參閱第 **9**-5 頁上的「群組運算式」。) 如果在政策中沒有參考 Auth 使用者或使用者群組 (在 WebUI 中，選擇 **Allow Any** 選項)，政策會套用到指定 Auth 伺服器中的所有 Auth 使用者。

注意： ScreenOS 用 auth 使用者登入的主機 IP 位址連結 Auth 權限。如果安全性裝置 Auth 來自 NAT 裝置後面的主機的使用者，而且該 NAT 裝置對所有 NAT 指派都使用單一的 IP 位址，則該 NAT 裝置後面其他主機的使用者自動具有相同的權限。

HA 會話備份

當兩台安全性裝置都在高可用性 (HA) 的 NSRP 叢集中時，可以指定哪些會話要備份，而哪些會話不要備份。對於不要備份的通訊流量會話，請套用停用 HA 會話備份選項的政策。在 WebUI 中，清除 **HA Session Backup** 核取方塊。在 CLI 中，在 **set policy** 指令中使用 **no-session-backup** 引數。依預設，NSRP 叢集中的安全性裝置會備份會話。

Web 篩選

Web 篩選 (又稱爲 URL 篩選) 可讓您管理網際網路的存取，並避免存取不良的網站內容。如需詳細資訊，請參閱第 **4**-75 頁上的「Web 篩選」。

記錄

在政策中啓用記錄時，安全性裝置會記錄套用特定政策的所有連接。您可以透過 WebUI 或 CLI 檢視日誌。在 WebUI 中，按一下 **Reports > Policies > Logging** (對於要檢視其日誌的政策)。在 CLI 中，使用 **get log traffic policy** *id_num* 指令。

注意： 如需檢視日誌和圖表的詳細資訊，請參閱第 **3**-45 頁上的「監看安全性裝置」。

計數

在政策中啓用計數時，安全性裝置會計算套用此政策的通訊流量的總位元組數，並將資訊記錄在記錄圖表中。若要在 WebUI 中檢視政策的記錄圖表，請按一下 **Reports > Policies > Counting** (對於要檢視其通訊流量計數的政策)。

通訊流量警示臨界值

您可以設定當政策允許的通訊流量超過指定的每秒位元組數、每分鐘位元組數 (或兩者) 時，觸發警示的臨界值。由於通訊流量警示要求安全性裝置監看位元組總數，因此也必須啓用計數功能。

注意 : 如需通訊流量警示的詳細資訊，請參閱第 **3**-55 頁上的「通訊流量示警」。

排程

透過將排程與政策相關聯，可以決定政策何時生效。可以將排程組態爲循環生效，也可組態爲單次事件。排程爲控制網路通訊流量的流動以及確定網路安全提供了強有力的工具。對於後者的範例，如果您擔心職員向公司外傳輸重要資料，可以設定一個政策，阻斷正常上班時間以外的向外 FTP-Put 和 MAIL 通訊流量。

在 WebUI 中，在 **Objects > Schedules** 區域中定義排程。在 CLI 中，使用 **set schedule** 指令。

注意 : 在 WebUI 中，已排定進度的政策如果有灰色背景，表示目前的時間不在已定義的排程內。已排定進度的政策成爲活動時，背景是白色的。

防毒掃描

有些 Juniper Networks 安全性裝置支援內部 AV 掃瞄程式，您可進行組態以篩選 FTP、HTTP、IMAP、POP3 和 SMTP 通訊流量。若內嵌的 AV 掃瞄程式偵測到病毒，程式便會卸除封包，並將呈報病毒的訊息傳送至初始通訊流量的用戶端。

注意 : (如需防毒掃瞄的詳細資訊，請參閱第 165 頁上的「防毒掃描」。)

通訊流量整理

可以爲每個政策設定控制和整理通訊流量的參數。通訊流量整理參數包括 :

- **Guaranteed Bandwidth:** 以每秒 KB 數 (kbps) 表示的保證輸送量。低於此臨界值的通訊流量以最高優先順序通過，不受任何通訊流量管理或整理機制的限制。

- **Maximum Bandwidth:** 以每秒 KB 數 (kbps) 表示的連接類型可用的安全頻寬。超過此臨界值的通訊流量會被抑制並卸除。

注意 : 建議不要使用低於 10 Kbps 的速率。低於此臨界值的速率會導致封包被卸除以及過多的重試，進而讓通訊流量無法進行管理。

- **Traffic Priority:** 當通訊流量頻寬在保障的頻寬和最大頻寬設定之間時，安全性裝置會先讓較高優先順序的通訊流量通過，並且只有在沒有其他更高優先順序的通訊流量時，才會讓較低優先順序的通訊流量通過。有八個優先順序等級。

- **DiffServ Codepoint Marking:** 差異服務 (DiffServ) 系統會標記通訊流量在優先順序階層中的位置。可以將八個 ScreenOS 優先順序對應到 DiffServ 系統中。依預設，ScreenOS 系統中的最高優先順序 (優先順序 0) 對應到 DiffServ 欄位 (請參閱 RFC 2474) 中的頭三位 (111)，或對應到 IP 封包標頭的 TOS 位元組 (請參閱 RFC 1349) 的 IP 優先欄位中。ScreenOS 中的最低優先順序 (優先順序 7) 對應至 TOS DiffServ 系統中的 (000)。當您啓用 DSCP 時，ScreenOS 會以 IP 優先的優先順序覆寫 ToS 位元組中的前三個位元。當您啓用 DSCP 並設定 *dscp-byte* **值**時，ScreenOS 會以 DSCP 值覆寫 ToS 位元組的前六個位元。

注意： 如需通訊流量管理和整理更加詳細的討論，請參閱第 183 頁上的「通訊流量整理」。

若要變更 ScreenOS 優先順序和 DiffServ 系統間的對應，請使用下面的 CLI 指令：

set traffic-shaping ip_precedence *number0 number1 number2 number3 number4 number5 number6 number7*

其中 *number0* 是優先順序 0 (TOS DiffServ 系統中的最高優先順序) 的對應，*number1* 是優先順序 1 的對應，依此類推。

若要將 IP 的優先順序納入類別選擇器程式碼點中，也就是使 DiffServ 欄位中的第二個三位均爲零，進而確保維持您以 **ip_precedence** 設定的優先等級，以及下游路由器能正確地處理此優先等級，請使用下列 CLI 指令：

set traffic-shaping dscp-class-selector

套用的政策

本節說明政策的管理：檢視、建立、修改、排序和重新排序以及移除政策。

檢視政策

若要透過 WebUI 檢視政策，請按一下 **Policies**。透過從 **From** 和 **To** 下拉式清單中選擇區域名稱，然後按一下 **Go**，可以按來源區域和目的地區域分類顯示政策。使用 CLI 中的 **get policy** [**all** | **from** *zone* **to** *zone* | **global** | **id** *number*] 指令。

建立政策

若要允許通訊流量在兩個區域之間流動，可在這些區域間建立拒絕、允許、駁回或開通通訊流量通道的政策。如果安全性裝置是唯一能夠設定 (在政策中參考的) 來源和目的地位址之間區域內部通訊流量的路由的網路裝置，您也可以建立政策以控制相同區域內的通訊流量。也可以建立全域政策，利用 Global 區域通訊錄中的來源和目的地位址。

若要允許兩個區域之間 (例如，Trust 區域和 Untrust 區域) 的雙向通訊流量，即需要建立從 Trust 到 Untrust 區域的政策，然後再建立從 Untrust 到 Trust 的第二個政策。視您的需求而定，政策可使用相同或不同的 IP 位址，只會保留來源與目的地位址。

可以在相同系統 (根或虛擬系統) 中的任何區域之間定義政策。若要在根系統和虛擬系統之間定義政策，其中一個區域必須爲共享區域。(如需和虛擬系統有關的共享區域資訊，請參閱*第 10 卷 : 虛擬系統*。)

建立區域間政策郵件服務

在本範例中，建立三個用來控制電子郵件通訊流量的政策。

第一個政策允許 Trust 區域中的內部使用者傳送或擷取來自 DMZ 區域本機郵件伺服器的電子郵件。此政策允許服務 MAIL (即 SMTP) 與發自內部使用者的 POP3 通過 Juniper Networks 防火牆，到達本機郵件伺服器。

第二與第三個政策允許服務 MAIL 通過 DMZ 區域本機郵件伺服器與 Untrust 區域遠端郵件伺服器之間的防火牆。

但在建立控制不同安全區間通訊流量的政策之前，您必須先設計要套用這些政策的環境。首先，您先將介面連結至區域，然後爲介面指派 IP 位址 :

- 將 ethernet1 連結到 Trust 區域，然後爲其指派 IP 位址 10.1.1.1/24。
- 將 ethernet2 連結到 DMZ 區域，然後爲其指派 IP 位址 1.2.2.1/24。
- 將 ethernet3 連結到 Untrust 區域，然後爲其指派 IP 位址 1.1.1.1/24。

  所有安全區都在 trust-vr 路由設定網域中。

其次，建立要在政策中做用的位址 :

- 在名爲 "corp_net" 的 Trust 區域中定義位址，並爲其指派位址 10.1.1.0/24。
- 在名爲 "mail_svr" 的 DMZ 區域中定義位址，並爲其指派位址 1.2.2.5/32。
- 在名爲 "r-mail_svr" 的 Untrust 區域中定義位址，並爲其指派位址 2.2.2.5/32。

第三，建立一個名爲 "MAIL-POP3" 的服務群組，其中包括兩個預先定義的服務 MAIL 與 POP3。

第四，在經由 ethernet3 指向外部路由器 (1.1.1.250) 的 trust-vr 路由設定網域中定義預設路由。

完成步驟 1 到步驟 4 之後，即可建立允許在受保護的網路內向內 / 外傳輸、擷取與傳送電子郵件所需的政策。

WebUI

1. 介面
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   輸入下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (對於 ethernet2): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: DMZ
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone Name: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.1.1.1/24

2. 位址
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: corp_net
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.1.0/24
   Zone: Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: mail_svr
   IP Address/Domain Name:
   IP/Netmask: (選擇), 1.2.2.5/32
   Zone: DMZ

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: r-mail_svr
   IP Address/Domain Name:
   IP/Netmask: (選擇), 2.2.2.5/32
   Zone: Untrust

3. **服務群組**
   Objects > Services > Groups: 輸入下面的群組名稱，移動下列服務，然後按一下 **OK**:

   Group Name: MAIL-POP3

   選擇 **MAIL** 並使用 < < 按鈕將服務從 Available Members 欄移至 Group Members 欄。

   選擇 **POP3** 並使用 < < 按鈕將服務從 Available Members 欄移至 Group Members 欄。

4. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

5. **政策**
   Policies > (From: Trust, To: Untrust) > New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), corp_net
   Destination Address:
   Address Book Entry: (選擇), mail_svr
   Service: Mail-POP3
   Action: Permit

   Policies > (From: DMZ, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), mail_svr
   Destination Address:
   Address Book Entry: (選擇), r-mail_svr
   Service: MAIL
   Action: Permit

   Policies > (From: Untrust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), r-mail_svr
   Destination Address:
   Address Book Entry: (選擇), mail_svr
   Service: MAIL
   Action: Permit

CLI

1. 介面
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 1.2.2.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. 位址
   set address trust corp_net 10.1.1.0/24
   set address dmz mail_svr 1.2.2.5/32
   set address untrust r-mail_svr 2.2.2.5/32

3. 服務群組
   set group service MAIL-POP3
   set group service MAIL-POP3 add mail
   set group service MAIL-POP3 add pop3

4. 路由
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. 政策
   set policy from trust to dmz corp_net mail_svr MAIL-POP3 permit
   set policy from dmz to untrust mail_svr r-mail_svr MAIL permit
   set policy from untrust to dmz r-mail_svr mail_svr MAIL permit
   save

建立區域間政策組

一家小型軟體公司 (ABC Design) 已將其內部網路分成兩個子網路，這兩個子網路都在 Trust 區域中。這兩個子網路爲 :

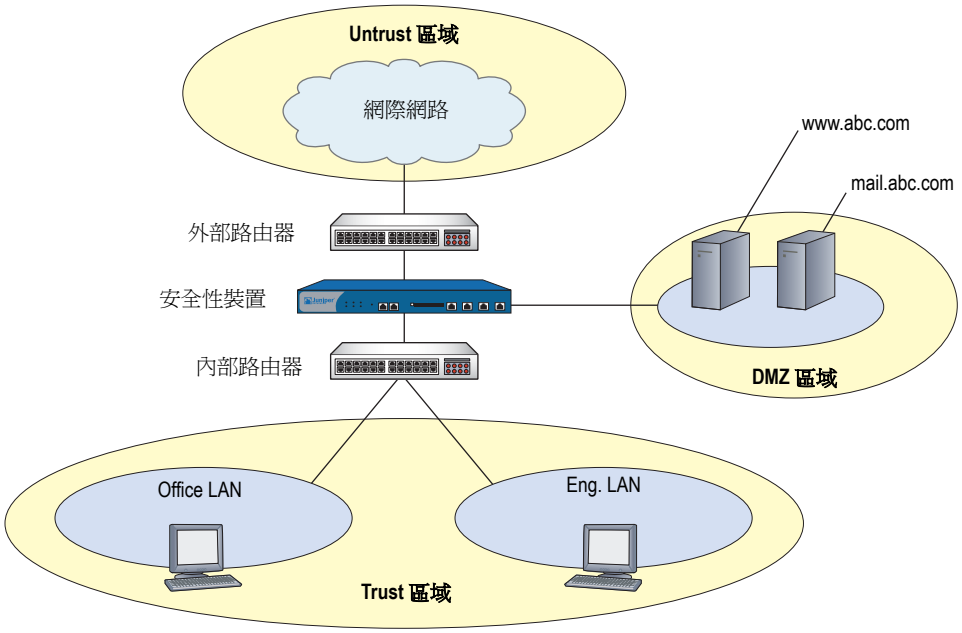
- 工程 (具已定義的位址 "Eng")
- 公司的其他部分 (已定義的位址爲 "Office")。

其 Web 和郵件伺服器也有一個 DMZ 區域。

下面的範例是下列使用者的典型政策組 :

- "Eng" 可以使用用於向外通訊流量的所有服務，除了 FTP-Put、IMAP、MAIL 和 POP3 外。
- "Office" 可以使用電子郵件和存取「網際網路」，只要它們透過 WebAuth 驗證自己。(如需 WebAuth 使用者驗證的資訊，請參閱第 **9**-31 頁上的「驗證使用者」。)
- Trust 區域中的每一個人均可以存取 DMZ 區域中的 Web 與郵件伺服器。
- Untrust 區域中的遠端郵件伺服器可存取 DMZ 區域中的本機郵件伺服器。
- 也有一組系統管理員 (具使用者定義的位址 "sys-admins")，對 DMZ 區域中的伺服器具有全部使用者和管理存取權限。

圖 73: 區域間政策組



假設您已組態好介面、位址、服務群組及必須適用的路由。如需有關組態上述各項目的詳細資訊，請參閱第 43 頁上的「介面」，第 100 頁上的「位址」、第 132 頁上的「服務群組」 和 *第 7 卷：路由*。

表 18: 已組態政策

從區域 (來源位址)	到區域 (目的地位址)	服務	動作
Trust - Any	Untrust - Any	Com (服務群組 : FTP-Put、IMAP、MAIL、POP3)	Reject
Trust - Eng	Untrust - Any	Any	Permit
Trust - Office	Untrust - Any	Internet(服務群組 : FTP-Get、HTTP、HTTPS)	Permit (+ WebAuth)
Untrust - Any	DMZ - mail.abc.com	MAIL	Permit
Untrust - Any	DMZ - www.abc.com	Web (服務群組 : HTTP、HTTPS)	Permit
Trust - Any	DMZ - mail.abc.com	電子郵件 (服務群組 : IMAP、MAIL、POP3)	Permit
Trust - Any	DMZ - www.abc.com	Internet(服務群組 : FTP-Get、HTTP、HTTPS)	Permit
Trust - sys-admins	DMZ - Any	Any	Permit
DMZ - mail.abc.com	Untrust - Any	MAIL	Permit

注意： 預設政策爲全部拒絕。

WebUI

1. 從 **Trust** 到 **Untrust**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Eng
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Office
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: Internet
   Action: Permit

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   Authentication: (選擇)
   WebAuth: (選擇)

注意： "Internet" 是具有下列成員的服務群組 : FTP-Get、HTTP 和 HTTPS。

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: Com
   Action: Reject
   Position at Top: (選擇)

注意： "Com" 是具有下列成員的服務群組 : FTP-Put、MAIL、IMAP 和 POP3。

對於從 Untrust 區域到 Trust 區域的通訊流量，預設的拒絕政策會拒絕所有的通訊流量。

2. **從 Untrust 到 DMZ**
   Policies > (From: Untrust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), mail.abc.com
   Service: MAIL
   Action: Permit

   Policies > (From: Untrust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), www.abc.com
   Service: Web
   Action: Permit

注意 : "Web" 是具有下列成員的服務群組 : HTTP 和 HTTPS。

---

3. **從 Trust 到 DMZ**
   Policies > (From: Trust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), mail.abc.com
   Service: e-mail
   Action: Permit

注意 : "e-mail" 是具有下列成員的服務群組 : MAIL、IMAP 和 POP3。

   Policies > (From: Trust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), Any
   Destination Address:
   　　Address Book Entry: (選擇), www.abc.com
   Service: Internet
   Action: Permit

   Policies > (From: Trust, To: DMZ) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   　　Address Book Entry: (選擇), sys-admins
   Destination Address:
   　　Address Book Entry: (選擇), Any
   Service: ANY
   Action: Permit

4. **從 DMZ 到 Untrust**
   Policies > (From: DMZ, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), mail.abc.com
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: MAIL
   Action: Permit

CLI

1. **從 Trust 到 Untrust**
   set policy from trust to untrust eng any any permit
   set policy from trust to untrust office any Internet permit webauth
   set policy top from trust to untrust any any Com reject

注意： "Internet" 是具有下列成員的服務群組：FTP-Get、HTTP 和 HTTPS。

"Com" 是具有下列成員的服務群組：FTP-Put、MAIL、IMAP 和 POP3。

2. **從 Untrust 到 DMZ**
   set policy from untrust to dmz any mail.abc.com mail permit
   set policy from untrust to dmz any www.abc.com Web permit

注意： "Web" 是具有下列成員的服務群組：HTTP 和 HTTPS。

3. **從 Trust 到 DMZ**
   set policy from trust to dmz any mail.abc.com e-mail permit
   set policy from trust to dmz any www.abc.com Internet permit
   set policy from trust to dmz sys-admins any any permit

注意： "e-mail" 是具有下列成員的服務群組：MAIL、IMAP 和 POP3。

"Internet" 是具有下列成員的服務群組：FTP-Get、HTTP 和 HTTPS。

4. **從 DMZ 到 Untrust**
   set policy from dmz to untrust mail.abc.com any mail permit
   save

建立區域內部政策

在本範例中，您會建立內部區域政策，允許一組帳號存取 Trust 區域中企業 LAN 上的機密伺服器。先將 ethernet1 連結到 Trust 區域，並指定 IP 位址爲 10.1.1.1/24。然後將 ethernet2 連結到 Trust 區域，並指派 IP 位址爲 10.1.5.1/24。啓用 Trust 區域中的區域內部阻斷。接著，定義兩個位址，一個作爲公司儲存財務記錄的伺服器位址 (10.1.1.100/32)，另一個作爲會計部門主機所在位置的子網路位址 (10.1.5.0/24)。然後建立區域內部政策，允許從這些主機存取伺服器。

WebUI

1. **Trust Zone - 介面和阻斷**

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   選擇下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.5.1/24
   選擇下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

   Network > Zones > Edit (對於 Trust): 輸入下面的內容，然後按一下 **OK**:

   Block Intra-Zone Traffic: (選擇)

2. **位址**

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: Hamilton
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.1.100/32
   Zone: Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: accounting
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.5.0/24
   Zone: Trust

3. **政策**

   Policies > (From: Trust, To: Trust) > New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), accounting
   Destination Address:
   Address Book Entry: (選擇), Hamilton
   Service: ANY
   Action: Permit

CLI

1. **Trust Zone -** 介面和阻斷
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.1.5.1/24
   set interface ethernet2 nat
   set zone trust block

2. 位址
   set address trust Hamilton 10.1.1.100/32
   set address trust accounting 10.1.5.0/24

3. 政策
   set policy from trust to trust accounting Hamilton any permit
   save

建立全域政策

在此範例中，將建立一全域政策，讓每個區域中的主機都能存取公司網站 www.juniper.net。有很多安全區時，使用全域政策是很便利的捷徑。在本範例中，一個全域政策即可實現 *n* 個區域間政策所實現的任務 (其中 *n* = 區域數)。

注意： 若要用網域名稱而非 IP 位址，請確定在安全性裝置上組態了 DNS 服務。

WebUI

1. 全域位址
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: server1
   IP Address/Domain Name:
   Domain Name: (選擇), www.juniper.net
   Zone: Global

2. 政策
   Policies > (From: Global, To: Global) > New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), server1
   Service: HTTP
   Action: Permit

CLI

1. 全域位址
   set address global server1 www.juniper.net

2. 政策
   set policy global any server1 http permit
   save

輸入政策內容

經由 CLI 組態政策時，在您建立政策後，即可輸入政策內容，以進行增補或修改。例如，您可能先建立了下列政策 :

```
set policy id 1 from trust to untrust host1 server1 HTTP permit attack
    HIGH:HTTP:SIGS action close
```

如果您想要變更政策，如新增另一個來源或目的地位址、另一個服務或另一個攻擊群組，您即可輸入政策 1 的內容，然後再輸入適當指令 :

```
set policy id 1
ns(policy:1)-> set src-address host2
ns(policy:1)-> set dst-address server2
ns(policy:1)-> set service FTP
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS
```

您亦可移除單一政策元件的多個項目，只要不移除所有項目即可。例如，您可以將移除上列組態的 server2，而不是 server2 與 server1，因爲如此政策中即不會留下任何目的地位址。

各政策元件的多重項目

ScreenOS 允許您將多個項目新增至下列政策元件中 :

- 來源位址
- 目的地位址
- 服務
- 攻擊群組

在 5.0.0 之前的 ScreenOS 版本中，具有多個來源與目的地位址或服務的唯一方法是先建立具有多個成員的位址或服務群組，然後在政策中參考該群組。在 ScreenOS 5.0.0 中，您仍可使用政策中的位址與服務群組。除此之外，您還可以直接將額外的項目新增至政策元件。

注意 : 若政策中所參考的第一個位址或服務是 "Any"，則您將無法以邏輯性的方式將任何項目新增到政策中。若發生上述情形，ScreenOS 會避免發生此類不當組態，並顯示錯誤訊息。

若要將多個項目新增至政策元件，請執行下列操作之一 :

WebUI

若要新增更多位址與服務，請按一下欲將更多項目新增至其中之元件旁的 **Multiple** 按鈕。若要新增更多攻擊群組，請按一下 **Attack Protection** 按鈕。在 "Available Members" 欄中選擇一個項目，然後使用 **< <** 鍵將之移至 "Active Members" 欄。您可以針對其他項目重複執行此動作。完成後，請按一下 **OK** 以返回政策組態頁面。

CLI

以下列指令輸入政策內容 :

```
set policy id number
```

然後視情況使用下列指令 :

```
ns(policy:number)-> set src-address string
ns(policy:number)-> set dst-address string
ns(policy:number)-> set service string
ns(policy:number)-> set attack string
```

設定位址否定

您可以組態政策，使其套用至所有位址，指定爲來源或目的地的位址除外。例如，您可能想要建立允許所有人存取網際網路，但 "P-T_contractors" 位址群組除外的政策。爲了達成上述目標，您可以使用位址否定選項。

在 WebUI 中，當您在按一下政策組態頁面上「來源位址」或「目的地位址」旁的 **Multiple** 按鈕，即會出現一個蹦現式視窗，位址否定選項便位於其中。

您立即在 CLI 中的來源或目的地位址前輸入驚嘆號 (!)。

注意 : 位址否定會發生在政策元件層級，套用至所有否定元件中的項目。

在本範例中，建立允許 Trust 區域所有位址存取所有 FTP 伺服器 (名爲 "vulcan" 的 FTP 伺服器除外) 的政策，工程部門會使用 "vulcan" 伺服器將功能規格發送給其他方。

但在建立政策前，您必須先設定要套用政策的環境。首先，啓用 Trust 區域的區域間阻斷功能。安全性裝置在兩個連結到相同區域的介面之間傳送通訊流量之前，阻斷功能必須先進行政策查詢。

其次，將兩個介面連結到 Trust 區域，並爲其指派 IP 位址 :

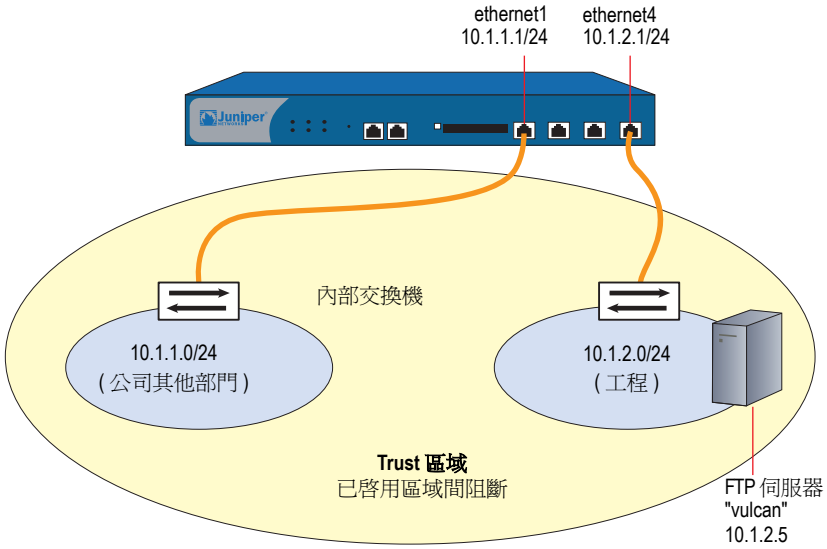
- 將 ethernet1 連結到 Trust 區域，然後爲其指派 IP 位址 10.1.1.1/24。
- 將 ethernet4 連結到 Trust 區域，然後爲其指派 IP 位址 10.1.2.1/24。

第三，爲 Trust 區域內名爲 "vulcan" 的 FTP 伺服器建立位址 (10.1.2.5/32)。

完成這兩個步驟後，即可建立區域間政策。

注意： 您不必針對工程部門建立政策以到達其 FTP 伺服器，因爲工程師亦位在 10.1.2.0/24 子網路內，您亦不需越過 Juniper Networks 防火牆才能到達其所屬伺服器。

圖 74: 區域內部政策否定



WebUI

1. **區域間阻斷**
   Network > Zones > Edit (對於 Trust): 輸入下面的內容，然後按一下 **OK**:

   Virtual Router Name: trust-vr
   Block Intra-Zone Traffic: (選擇)

2. **Trust 區域介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.1.1/24
   選擇下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (對於 ethernet4): 輸入下面的內容，然後按一下 **Apply**:

   Zone Name: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 10.1.2.1/24
   選擇下面的內容，然後按一下 **OK**:
   Interface Mode: NAT

3. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: vulcan
   IP Address/Domain Name:
   IP/Netmask: (選擇), 10.1.2.5/32
   Zone: Trust

4. **政策**
   Policies > (From: Trust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), vulcan

   > 按一下 **Multiple**，選擇 **Negate Following** 核取方塊，然後再按一下 **OK** 以返回基本 policy 組態頁面。

   Service: FTP
   Action: Permit

CLI

1. **區域間阻斷**
   set zone trust block

2. **Trust 區域介面**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet4 zone trust
   set interface ethernet4 ip 10.1.2.1/24
   set interface ethernet1 nat

3. **位址**
   set address trust vulcan 10.1.2.5/32

4. **政策**
   set policy from trust to trust any !vulcan ftp permit
   save

修改和停用政策

建立政策後，始終都可以返回該政策進行修改。在 WebUI 中，按一下要變更的政策的 Configure 欄中的 **Edit** 連結。在該政策出現的 Policy 組態頁面中進行變更，然後按一下 **OK**。在 CLI 中，使用 **set policy** 指令。

ScreenOS 也提供啓用和停用政策的方法。依預設，會啓用政策。若要停用政策，請執行下面的操作 :

WebUI

Policies: 在要停用的政策的 Configure 欄中，清除 **Enable** 核取方塊。

停用政策的文字列以灰色顯示。

CLI

```
set policy id id_num disable
save
```

注意 : 若要再次啓用政策，請在要啓用的政策的 Configure 欄中選擇 **Enable** (WebUI)，或鍵入 **unset policy id** id_num **disable** (CLI)。

政策驗證

ScreenOS 提供一個工具，可用來驗證政策清單中的政策順序是否有效。某個政策可能會覆蓋 (或「遮蔽」) 另一個政策。請參考下列範例 :

```
set policy id 1 from trust to untrust any any HTTP permit
set policy id 2 from trust to untrust any dst-A HTTP deny
```

由於安全性裝置會從清單上方開始執行政策查詢，因此若裝置找到與所接收通訊流量符合的項目時，即不會再往下查詢。在上列範例中，安全性裝置從未到達政策 2，因爲政策 1 中的目的地位址 "any" 包含政策 2 中更特定的 "dst-A" 位址。當 HTTP 封包到達安全性 (來自與 Untrust 區域 dst-A 連結的 Trust 區域位址) 時，安全性裝置一律會先尋找符合政策 1 的項目。

只要保留政策順序，並將更爲特定的政策置前，即可修正上列範例 :

```
set policy id 2 from trust to untrust any dst-A HTTP deny
set policy id 1 from trust to untrust any any HTTP permit
```

當然，我們是爲了說明基本概念才特地使上述範例較爲簡單。若是有數十條或數百條政策的情況，可能就無法如此輕易的找出發生政策遮蔽的所在。若要檢查政策清單中是否有任何政策遮蔽的情況，您可以使用下列 CLI 指令 :

```
exec policy verify
```

此指令呈報遮蔽情況及被遮蔽的政策。之後就是管理員負起修正此情況的責任。

注意 : 政策「遮蔽」的概念所指的是處於政策清單中較上方的政策永遠比後續的政策先產生效用。由於政策查詢永遠會使用找到的第一個政策 (符合來源與目的地區域、來源與目的地位址及服務類型的五部份組合)，因此若有適用於相同組合 (或組合子網路) 的另一個政策，政策查詢仍會使用清單中的第一個政策，而永遠不會再往下找到第二個。

若某政策組態遮蔽另一政策，政策驗證工具將無法偵測到這種情況。在下列範例中，沒有任何政策遮蔽到政策 3，但政策 1 與政策 2 結合卻會遮蔽政策 3:

```
set group address trust grp1 add host1
set group address trust grp1 add host2
set policy id 1 from trust to untrust host1 server1 HTTP permit
set policy id 2 from trust to untrust host2 server1 HTTP permit
set policy id 3 from trust to untrust grp1 server1 HTTP deny
```

重新排序政策

安全性裝置將所有跨越防火牆的嘗試與政策進行對照檢查，從列在相應清單 (請參閱第 157 頁上的「政策組清單」) 的政策組中的第一個開始，並檢查整個清單。由於安全性裝置將政策中指定的動作套用到清單中第一個配對的政策，因此，必須按從最特殊到最廣泛的順序來安排政策。(特殊政策不排除位於清單下部比較一般性政策的套用，但位於特殊政策前的一般性政策會產生此排除效應。)

依預設，最近建立的政策放在政策組清單的底部。有一個選項允許將政策放在清單的最上面。在 WebUI 的 Policy 組態頁面中，選擇 **Position at Top** 核取方塊。在 CLI 中，將關鍵字 **top** 新增到 **set policy** 指令中 : **set policy top** …

若要將政策移動到清單中的不同位置，請執行下面的操作之一 :

WebUI

在 WebUI 中有兩種重新排序政策的方法 : 在要移動的政策的 Configure 欄中，按一下圓形箭頭或按一下單向箭頭。

如果按一下圓形箭頭 :

會出現 User Prompt 對話方塊。

若要將政策移到清單的最後面，請輸入 < -1 > 。若要將政策向上移動，輸入要移動到其前面的政策的 ID number。

按一下 **OK** 以執行移動。

如果按一下單箭頭 :

出現 Policy Move 頁面，顯示要移動的政策以及顯示其他政策的表格。

在顯示其他政策的表格中，第一欄 (Move Location) 包含指向不同位置的箭頭，可將政策移到這些位置。按一下指向政策要移動到的清單中位置的箭頭。

出現 Policy List 頁面，移動的政策出現在新位置上。

CLI

```
set policy move id_num { before | after } number
save
```

移除政策

除了修改和重新排序政策外，也可以刪除政策。在 WebUI 中，在要移除的政策的 Configure 欄中按一下 **Remove**。當系統訊息提示確認是否繼續刪除時，按一下 **Yes**。在 CLI 中，請使用 **unset policy** *id_num* 指令。

第 7 章

通訊流量整理

本章討論在不犧牲所有使用者的網路連接品質及可用性的情況下，使用 Juniper Networks 安全性裝置來管理有限頻寬的各種方法。本章包含下列各節 :

- 本頁上的「在政策層級管理頻寬」
- 第 184 頁上的「設定通訊流量整理」
- 第 188 頁上的「設定服務優先順序」
- 第 189 頁上的「設定優先順序佇列」
- 第 192 頁上的「入口政策制訂」
- 第 193 頁上的「整理虛擬介面上的通訊流量」
- 第 203 頁上的「DSCP 標記與整理」

通訊流量整理是指爲介面上的每一個使用者和應用程式分配適當的網路頻寬數量。適當的頻寬數量旨在保障服務品質 (QoS) 的前提下合乎成本效益的傳輸容量。透過建立政策並將適當的速率控制套用到流經裝置的每個通訊流量類別，您可以使用安全性裝置整理通訊流量。

在政策層級管理頻寬

若要分類通訊流量，請建立政策並指定每類通訊流量的保障頻寬數量、最大頻寬及優先順序等內容。保障頻寬及最大頻寬並非嚴格地以政策爲基礎，而是以政策及可用的出口實體介面總頻寬爲基礎 (在出口區域中有多個實體介面的情況下)。每一個介面的實體頻寬都配置給所有政策的保障的頻寬參數。如果有剩餘的頻寬，可讓其他通訊流量共享。換句話說，每個政策可得到其保障的頻寬並按照優先順序與其他所有政策共享剩餘的頻寬 (直至達到其最大頻寬規格的限制)。

通訊流量整理功能套用到來自所有政策的通訊流量。若您關閉某特定政策的通訊流量整理，而另一政策的通訊流量整理仍然開啓，則系統會將具下列參數的預設通訊流量整理政策套用至該特定政策：

- 保障頻寬 0
- 無限最大頻寬
- 第 7 優先順序（最低優先順序設定）

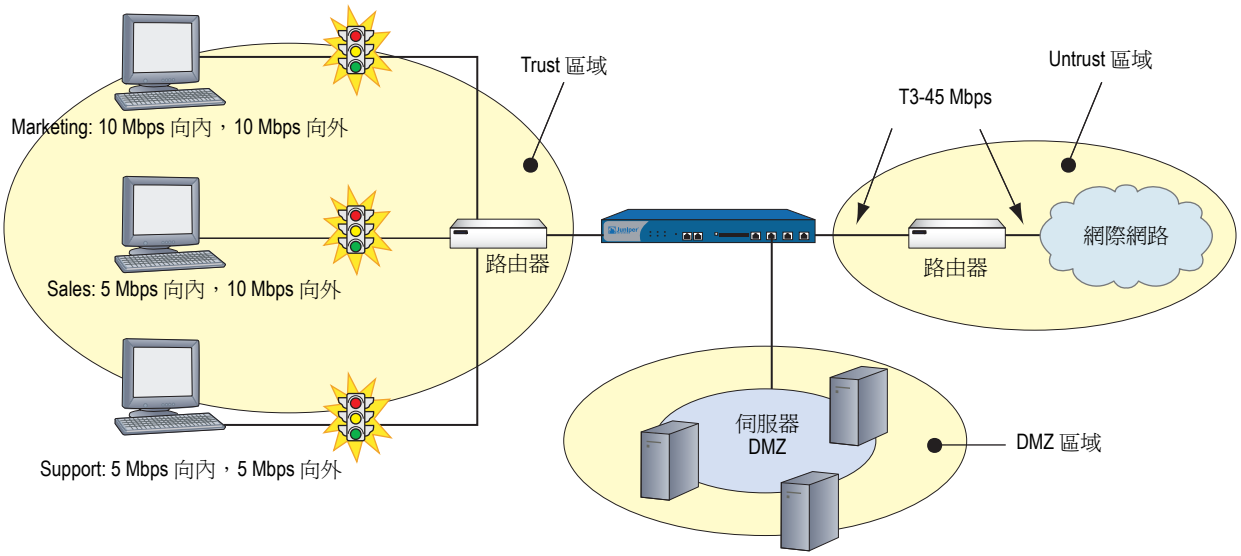
注意： 您可以啓用優先順序層級至 DiffServ Codepoint 標記系統的對應。如需「DS Codepoint 標記」的詳細資訊，請參閱第 165 頁上的「通訊流量整理」。

如果您不希望系統將此預設通訊流量整理政策指派給已停用其通訊流量整理的政策，可以透過 CLI 指令停用整個系統的通訊流量整理：**set traffic-shaping mode off**. 使用 CLI 指令：**set traffic-shaping mode on** 在介面上啓用整理。或是在 WebUI 中將通訊流量整理設定爲自動：**Configuration > Advanced > Traffic Shaping**。這允許系統在政策需要時開啓通訊流量整理，在政策不需要時將其停用。

設定通訊流量整理

在本範例中，您需要在 T3 介面上分割 45Mbps 的頻寬，此介面在相同子網路的三個部門之間。ethernet1 介面被連結到 Trust 區域，而 ethernet3 被連結到 Untrust 區域。

圖 75: 通訊流量整理



WebUI

1. **介面上的頻寬**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Traffic Bandwidth: 45000

注意 : 如果您沒有在介面上指定頻寬設定，則安全性裝置會使用可用的實體頻寬。

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Traffic Bandwidth: 45000

2. **政策中的頻寬**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Name: Marketing Traffic Shaping
   Source Address:
   Address Book Entry: (選擇), Marketing
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: Any
   Action: Permit
   VPN Tunnel: None

注意 : 您也可以在參考 VPN 通道的政策中啓用通訊流量整理。

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   Traffic Shaping: (選擇)
   Guaranteed Bandwidth: 10000
   Maximum Bandwidth: 15000

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Name: Sales Traffic Shaping Policy
   Source Address:
   Address Book Entry: (選擇), Sales
   Destination Address:
   Address Book Entry: (選擇), Any
   Service: Any
   Action: Permit

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   Traffic Shaping: (選擇)
   Guaranteed Bandwidth: 10000
   Maximum Bandwidth: 10000

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Support Traffic Shaping Policy
Source Address:
Address Book Entry: (選擇), Support
Destination Address:
Address Book Entry: (選擇), Any
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Allow Incoming Access to Marketing
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Marketing
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 10000
Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Allow Incoming Access to Sales
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Sales
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Allow Incoming Access to Support
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Support
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 5000

CLI

若要用政策啓用通訊流量整理，請執行下面的操作 :

1. 介面上的頻寬

```
set interface ethernet1 bandwidth 45000
set interface ethernet3 bandwidth 45000
```

注意 : 如果您沒有在介面上指定頻寬設定，則安全性裝置會使用可用的實體頻寬。

2. 政策中的頻寬

```
set policy name "Marketing Traffic Shaping" from trust to untrust marketing any
    any permit traffic gbw 10000 priority 0 mbw 15000
set policy name "Sales Traffic Shaping Policy" from trust to untrust sales any any
    permit traffic gbw 10000 priority 0 mbw 10000
set policy name "Support Traffic Shaping Policy" from trust to untrust support any
    any permit traffic gbw 5000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Marketing" from untrust to trust any
    marketing any permit traffic gbw 10000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Sales" from untrust to trust any sales
    any permit traffic gbw 5000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Support" from untrust to trust any
    support any permit traffic gbw 5000 priority 0 mbw 5000
save
```

設定服務優先順序

透過 Juniper Networks 安全性裝置的通訊流量整理功能，您可對未配置保障頻寬或有保障但未使用的頻寬執行優先順序佇列。優先順序佇列功能讓您所有的使用者和應用程式在需要時都能夠存取可用頻寬，同時也確定重要的通訊流量可以通過，必要時可以犧牲次要的通訊流量頻寬。透過佇列功能，安全性裝置能夠以八種不同的優先順序佇列緩衝通訊流量。這八種佇列爲：

- High priority
- 2nd priority
- 3rd priority
- 4th priority
- 5th priority
- 6th priority
- 7th priority
- Low priority (預設)

政策的優先設定表示未分配給其他政策的頻寬會根據高優先順序在前低優先順序在後的原則進行佇列。具有相同優先設定的政策會以輪詢 (round robin) 方式競爭頻寬。安全性裝置會先處理具有較高優先順序政策的所有通訊流量，然後再處理具有次優先設定政策的通訊流量，依此類推，直至處理完所有的通訊流量要求。如果通訊流量要求超過可用頻寬，會卸除優先順序最低的通訊流量。



小心：小心不要將超過其支援能力的頻寬配置給介面。政策組態程式本身不能防止您建立不支援的政策組態。如果競爭政策的保障的頻寬超過介面上設定的通訊流量頻寬，會有可能遺失資料。

如果您沒有配置任何保障的頻寬，那麼您可以使用優先順序佇列來管理網路的所有通訊流量。也就是說，必須在傳送完所有的高優先順序通訊流量之後，才能傳送第 2 優先順序的通訊流量，依此類推。只有在處理完其他所有通訊流量之後，安全性裝置才會處理低優先順序通訊流量。

設定優先順序佇列

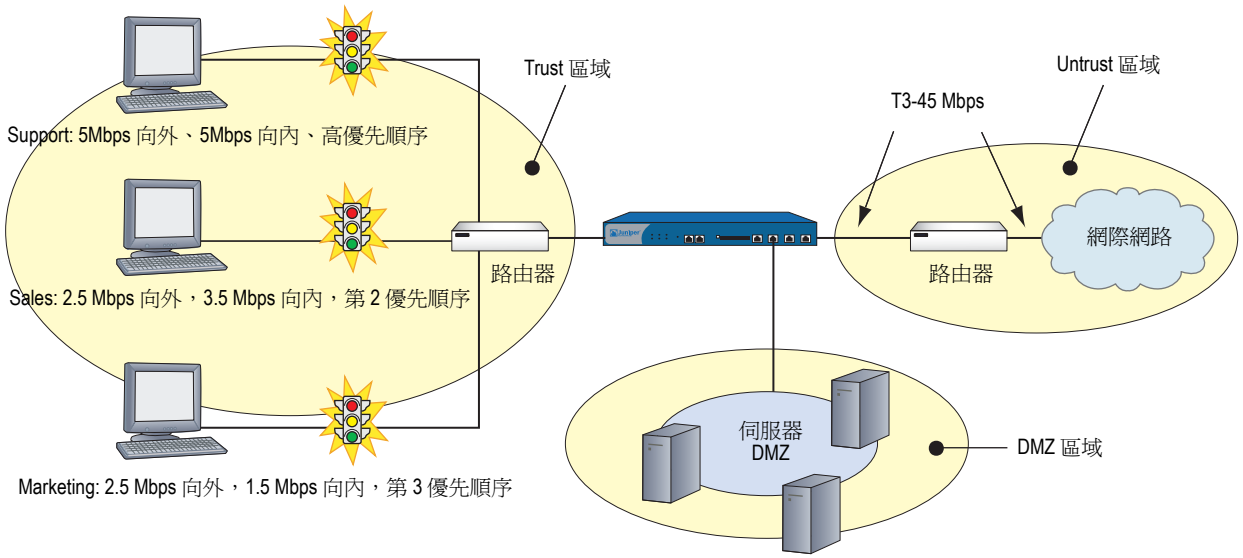
在此範例中，爲三個部門 (Support、Sales 和 Marketing) 組態保障的最大頻寬 (以 Mbps 爲單位)，如表 19 中所示 :

表 19: 最大頻寬組態

	向外保障	向內保障	結合保障	優先順序
Support	5	5	10	High
Sales	2.5	3.5	6	2
Marketing	2.5	1.5	4	3
總計	10	10	20	

如果三個部門同時透過防火牆傳送和接收通訊流量，那麼安全性裝置必須配置 20 Mbps 的頻寬以滿足保障的政策需求。ethernet1 介面被連結到 Trust 區域，而 ethernet3 被連結到 Untrust 區域。

圖 76: 優先順序佇列



WebUI

1. **介面上的頻寬**
   Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Traffic Bandwidth: 40000

   Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Traffic Bandwidth: 40000

2. 政策中的頻寬

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Sup-out
Source Address:
Address Book Entry: (選擇), Support
Destination Address:
Address Book Entry: (選擇), Any
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 40000
Traffic Priority: High priority
DiffServ Codepoint Marking: (選擇)

注意： 差異服務 (DS) 系統會標記通訊流量在優先順序階層中的位置。DS Codepoint 標記將 ScreenOS 的政策優先順序對應到 IP 封包標頭 DS 欄位中程式碼點的前三位。如需「DS Codepoint 標記」的詳細資訊，請參閱第 165 頁上的「通訊流量整理」。

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Sal-out
Source Address:
Address Book Entry: (選擇), Sales
Destination Address:
Address Book Entry: (選擇), Any
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 2500
Maximum Bandwidth: 40000
Traffic Priority: 2nd priority
DiffServ Codepoint Marking: Enable

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Mar-out
Source Address:
Address Book Entry: (選擇), Marketing
Destination Address:
Address Book Entry: (選擇), Any
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 2500
Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (選擇)

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Sup-in
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Support
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 40000
Traffic Priority: High priority
DiffServ Codepoint Marking: (選擇)

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Sal-in
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Sales
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 3500
Maximum Bandwidth: 40000
Traffic Priority: 2nd priority
DiffServ Codepoint Marking: (選擇)

Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

Name: Mar-in
Source Address:
Address Book Entry: (選擇), Any
Destination Address:
Address Book Entry: (選擇), Marketing
Service: Any
Action: Permit

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

Traffic Shaping: (選擇)
Guaranteed Bandwidth: 1500
Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (選擇)

CLI

1. **介面上的頻寬**
   set interface ethernet1 bandwidth 40000
   set interface ethernet3 bandwidth 40000

2. **政策中的頻寬**
   set policy name sup-out from trust to untrust support any any permit traffic gbw 5000 priority 0 mbw 40000 dscp enable
   set policy name sal-out from trust to untrust sales any any permit traffic gbw 2500 priority 2 mbw 40000 dscp enable
   set policy name mar-out from trust to untrust marketing any any permit traffic gbw 2500 priority 3 mbw 40000 dscp enable
   set policy name sup-in from untrust to trust any support any permit traffic gbw 5000 priority 0 mbw 40000 dscp enable
   set policy name sal-in from untrust to trust any sales any permit traffic gbw 3500 priority 2 mbw 40000 dscp enable
   set policy name mar-in from untrust to trust any marketing any permit traffic gbw 1500 priority 3 mbw 40000 dscp enable
   save

入口政策制訂

入口政策制訂是在安全性裝置的入口側進行通訊流量控制。藉由在入口點限制通訊流量，超出您頻寬設定的通訊流量便會在進行最小幅度的處理後遭到卸除，以保護系統資源。您可在介面層級及安全性政策中組態入口政策制訂。

您藉由設定最大頻寬 (**mbw** 關鍵字) 在介面上組態入口政策制訂。例如，下列指令可將入口介面 Ethernet1 上的頻寬限制爲 22 Mbps:

```
set interface ethernet1 bandwidth ingress mbw 22000
```

Ethernet1 上超出此頻寬的向內通訊流量會遭到卸除。若您在介面上設定通訊流量整理，則您也必須將通訊流量整理模式設定爲開啓 (**set traffic-shaping mode on**)。

不過，若要將入口政策制訂套用至特定應用程式還是需要使用政策。下列指令會建立一個名爲 *my_ftp* 的政策，會將安全性裝置入口側上的 FTP 頻寬限制爲 10 Mbps:

```
set policy my_ftp from untrust to trust any any ftp permit traffic pbw 10000
```

超出已組態政策制訂頻寬 (**pbw** 關鍵字) 的向內 FTP 通訊流量會遭到卸除。您亦可在政策中設定 **mbw**，但是政策層級 **mbw** 僅會套用至通訊流量的出口側，超出您所組態速率的通訊流量仍然會得到處理，但僅會在出口側被卸除 (請參閱第 195 頁上的圖 78「通訊流量整理封包流動」)。您可在政策中組態 **mbw** 或 **pbw**，但不能同時組態兩者。

在虛擬介面上組態及執行入口政策制訂與在實體介面上相同，唯一一點不同在於，您亦可在虛擬介面上組態保障的頻寬 (**gbw** 關鍵字) (請參閱第 194 頁上的「政策層級通訊流量整理」)。在實體介面上，保障的頻寬與最大頻寬相同。

注意 : VPN 引擎解密加密的封包後，便會執行通道介面上的入口政策制訂。

整理虛擬介面上的通訊流量

在通訊流量整理環境下，*虛擬介面*一詞僅指子介面和通道介面，而非其他虛擬介面類型，如虛擬安全性介面 (VSI)，聚集介面或冗餘介面。您無法在於 vsys 中所建立的政策中組態整理參數。同樣地，亦無法在由使用者建立的 vsys 所擁有 (繼承) 的介面上整理頻寬。有關詳細資訊，請參閱*第 10 卷 : 虛擬系統*。

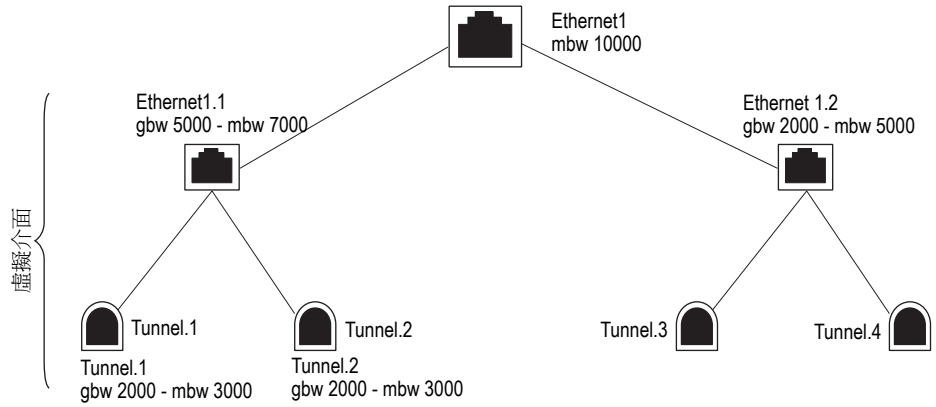
通訊流量整理 (與入口政策制訂的不同處) 涉及安全性裝置出口側的通訊流量管理。在具有實體介面的情況下，您可藉由在介面層級及政策中設定頻寬值，在虛擬介面上整理通訊流量。

介面層級通訊流量整理

介面層級的通訊流量整理是控制特定介面上通訊流量的最小及最大速率。您藉由指定保障的頻寬 (**gbw**) 來控制最小頻寬。這表示不論裝置上發生什麼運作情況，適當的通訊流量保證能具有此最小速率。您所設定的最大頻寬 (**mbw**) 會建立通訊流量永遠無法超過的速率。依預設，實體介面上的最大頻寬即是介面的傳輸流量；因此，您不能在實體介面上設定保障頻寬。

在通訊流量整理環境下，虛擬介面所指的是連結至實體介面的子介面，且進一步包括連結至該子介面的通訊介面 (建立介面階層)。連結至實體介面的子介面被稱爲該實體介面 (該子介面的*父*介面) 的*子*介面。同樣，連結至子介面的通道介面是該子介面的子介面，而實體介面便是其*祖父*介面。圖 77 說明這些相依關係。

圖 77: 介面階層



使用虛擬介面時，請記住下列介面階層規則：

- 配置給子介面的保障頻寬不能大於其所連結之實體介面的傳輸容量。例如，在圖 77 中，ethernet1.1 與 ethernet 1.2 相加的 **gbw** 爲 9000 Kbps，比 ethernet1 的 **mbw** 低 1000 Kbps。不過，請注意，這兩個子介面相加的最大頻寬超出其所連結之實體介面傳輸容量 2000 Kbps。這是可接受的，因爲 **mbw** 關鍵字僅用於將通訊流量限制於最大速率。若通訊流量低於子介面上的最大設定，則該頻寬即可用於其他任何連結至相同實體介面的子介面。
- 配置給通道介面的頻寬不能大於其所連結之子介面的保障頻寬。
- 若未針對最近的父項組態保障頻寬，則會從祖父介面取得頻寬。
- 子項的總保障頻寬不能超過父項的保障頻寬。
- 子項最大頻寬不能超出父項最大頻寬。

如前所述，您不能在實體介面上組態保障頻寬，因爲保障頻寬與最大頻寬 (介面的連結速度) 相同。不過，在虛擬介面上，您可以組態出口 **gbw** 與 **mbw**。您亦可組態入口 **mbw**，即介面層級的入口政策制訂。下列指令保障在 Ethernet4.1 上有 2000 Kbps 的最小向外位元速率，以及 2000 Kbps 的最大向內及向外速率：

```
set interface ethernet4.1 bandwidth egress gbw 1000 mbw 2000 ingress mbw
    2000
```

您可在 WebUI 中的 **Network > Interfaces > Edit** 頁面上設定頻寬。

設定頻寬後，您可以使用 **get traffic-shaping interface** 指令來檢視流經安全性裝置的實際頻寬。例如，您可能有進入 ethernet1 及離開 ethernet3 的通訊流量。若您在 ethernet1 上設定入口頻寬，則指令 **get traffic-shaping interface ethernet3** 會顯示裝置上的實際輸送量。

若您在介面上設定通訊流量整理，則您也必須將通訊流量整理模式設定爲開啓 (**set traffic-shaping mode on**)。

政策層級通訊流量整理

您在政策層級整理通訊流量，以針對特定的通訊流量類型配置頻寬。下列指令保障 FTP 通訊流量最小 1Mbps 的頻寬，並卸除任何超出 2 Mbps 的通訊流量：

```
set policy from trust to untrust any any ftp permit traffic gbw 1000 pbw 2000
```

請注意，此指令使用政策制訂頻寬 (**pbw**) 關鍵字。您可在政策中使用 **pbw** 或 **mbw**，但不能同時使用兩者。使用 **pbw** 的優點在於通訊流量會在安全性裝置的入口側被卸除，減少系統資源處理及保留的輸送量。(請參閱第 192 頁上的「入口政策制訂」。)

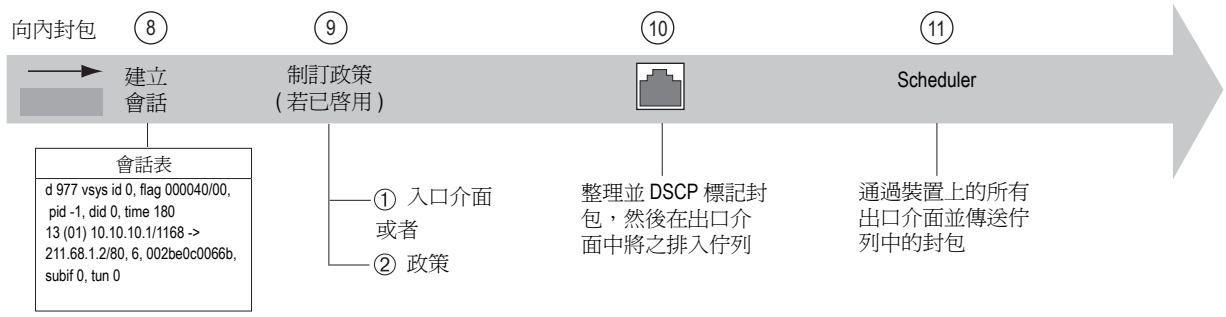
在 WebUI 中，建立政策後，按一下 **Advanced** 按鈕，以組態通訊流量整理參數。

雖然您必須將通訊流量整理模式設定爲 **on** 以整理介面上的通訊流量，但整理政策中的通訊流量時，不一定要開啓通訊流量整理。這是因爲通訊流量整理模式依預設設定爲 **auto**。會話變成活動中狀態且政策查詢發現通訊流量整理時，ScreenOS 便會針對該會話開啓通訊流量整理。您僅可在 WebUI 中將通訊流量整理模式設定或取消設定爲 **auto**: **Configuration > Advanced > Traffic Shaping**。

封包流動

圖 78 說明流經安全性裝置（受通訊流量整理及政策制訂影響）的封包流動部份。（請參閱第 11 頁上的「封包流動順序」以獲得封包流量的完整資訊。）超出 **pbw**（或於介面上組態的 **mbw**）的封包會在步驟 9 遭到卸除，整理及 DSCP 標記則在步驟 10 發生，而超出 **mbw**（於政策中組態）的封包則會在步驟 11 遭到卸除。

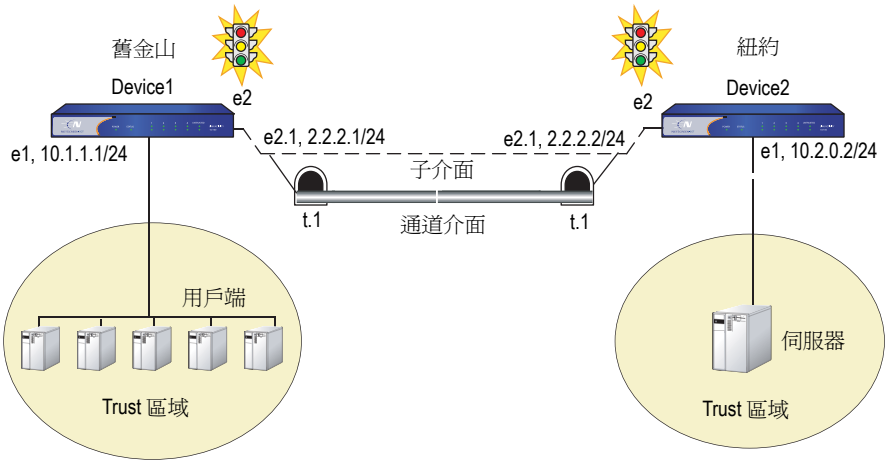
圖 78: 通訊流量整理封包流動



範例：具入口政策制訂的以路由爲基礎的 VPN

此範例說明如何針對加密通訊流量在介面層級執行入口政策制訂。入口政策制訂同時在子介面 (e2.1，最大頻寬：1200 Kbps) 及通道介面 (t.1，最大頻寬：1000 Kbps) 上進行組態。您將子介面上的政策制訂速率設定得較其所連結之通道介面爲高，以允許加密虛耗（在此範例中，假設在子介面上接收到的所有通訊流量均欲通往通道介面）。子介面上的政策制訂套用至已加密的封包，而通道介面上的政策制訂則套用至已解密的內封包。e2.1 上所有超過 1200 kbps 的已加密通訊流量均會遭到卸除。然後 t.1 介面上所有超過 1000 Kbps 的已解密（純文字）通訊流量均會遭到卸除。

圖 79: 以路由爲基礎的 VPN



WebUI (Device1 的組態)

1. **介面**
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 10.1.1.1/24
   Zone: Trust

   Network > Interfaces > Sub-IF > New: 輸入下面的內容，然後按一下 **Apply**:

   Interface Name: (選擇) ethernet2 然後輸入 : 1
   Zone: Untrust
   IP Address/Netmask: 2.2.2.1/24
   VLAN Tag: 128

   Network > Interfaces > New Tunnel IF: 輸入下面的內容，然後按一下 **Apply**:

   Tunnel Interface Name: 1
   Zone: Untrust
   Unnumbered (選擇) ethernet2.1
   Interface: e2.1

2. **路由**
   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 10.2.0.0/24
   Interface (選擇): Tunnel.1

3. **IKE**
   VPNs > AutoKey Advanced > Gateway > New: 輸入下面的內容，然後按一下 **OK**:

   Gateway Name: device1_ike
   Security Level: Standard
   Remote Gateway Type:
   Static IP Address: (選擇), IP Address/Hostname: 2.2.2.2

預先共享的金鑰
Preshared Key: secret
Outgoing Interface: e2.1

VPNs > AutoKey IKE New: 輸入下面的內容，然後按一下 **OK**:

VPN Name: device1_vpn
Gateway Name: device1_ike

> Advanced: 輸入下面的進階設定，然後按一下 **Return** 返回基本 AutoKey IKE 組態頁面 :

Bind to: (選擇) Tunnel Interface, (選擇) tunnel.1

CLI (Device1 的組態)

1. 介面

```
set interface e1 zone trust
set interface e1 ip 10.1.1.1/24
set interface e2.1 tag 128 zone untrust
set interface t.1 zone trust
set interface e2.1 ip 2.2.2.1/24
set interface t.1 ip unnumbered interface e2.1
set route 10.2.0.0/24 int t.1
```

2. **IKE**

```
set ike gateway device1_ike address 2.2.2.2 outgoing-interface e2.1 preshare
    sec-level standard
set vpn device1_vpn gateway 208a_ike sec-level standard
set vpn device1_vpn bind interface t.1
```

WebUI (Device2 的組態)

1. 介面

Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

IP Address/Netmask: 10.2.0.2/24
Zone: Trust

Network > Interfaces > Sub-IF > New: 輸入下面的內容，然後按一下 **Apply**:

Interface Name: (選擇) ethernet2 然後輸入 : 1
Zone: Untrust
IP Address/Netmask: 2.2.2.2/24
VLAN Tag: 128

Network > Interfaces > Tunnel IF > New: 輸入下面的內容，然後按一下 **Apply**:

Tunnel Interface Name: 1
Unnumbered (選擇) ethernet2.1
Interface: e2.1

2. 介面上的頻寬

Network > Interfaces > Edit (對於 ethernet2.1): 輸入下面的內容，然後按一下 **OK**:

Traffic Bandwidth, Ingress: 1200

Network > Interfaces > Edit (對於 tunnel.1): 輸入下面的內容，然後按一下 **OK**:

Traffic Bandwidth, Ingress: 1000

3. 路由

Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

Network Address/Netmask: 10.1.1.0/24
Interface (選擇): Tunnel.1

4. **IKE**

   VPNs > AutoKey Advanced > Gateway > New: 輸入下面的內容，然後按一下 **OK**:

   Gateway Name: device2_ike
   Security Level: Standard
   Remote Gateway Type:
   Static IP Address: (選擇), IP Address/Hostname: 2.2.2.2

預先共享的金鑰

   Preshared Key: secret
   Outgoing Interface: e2.1

   VPNs > AutoKey IKE New: 輸入下面的內容，然後按一下 **OK**:

   VPN Name: device2_vpn
   Gateway Name: device2_ike

   > Advanced: 輸入下面的進階設定，然後按一下 **Return** 返回基本 AutoKey IKE 組態頁面 :

   Bind to: (選擇) Tunnel Interface, (選擇) tunnel.1

5. **政策**

   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Service: Any
   Action: Permit

   Policies > (From: Untrust, To: Trust) New: 輸入下面的內容，然後按一下 **OK**:

   Service: Any
   Action: Permit

CLI (Device2 的組態)

1. **介面**

```
set interface e1 zone trust
set interface e1 ip 10.2.0.2/24
set interface e2.1 tag 128 zone untrust
set interface e2.1 ip 2.2.2.2/24
set interface t.1 zone untrust
set interface t.1 ip unnumbered interface e2.1
set route 10.1.1.0/24
```

2. **介面上的頻寬**

```
set interface e2.1 bandwidth ingress mbw 1200
set interface t.1 bandwidth ingress mbw 1000
```

3. **IKE**

```
set ike gateway device2_ike address 2.2.2.1 preshare secret sec-level standard
set vpn device2_vpn gateway 208b_ike sec-level standard
set vpn device2_vpn bind interface t.1
```

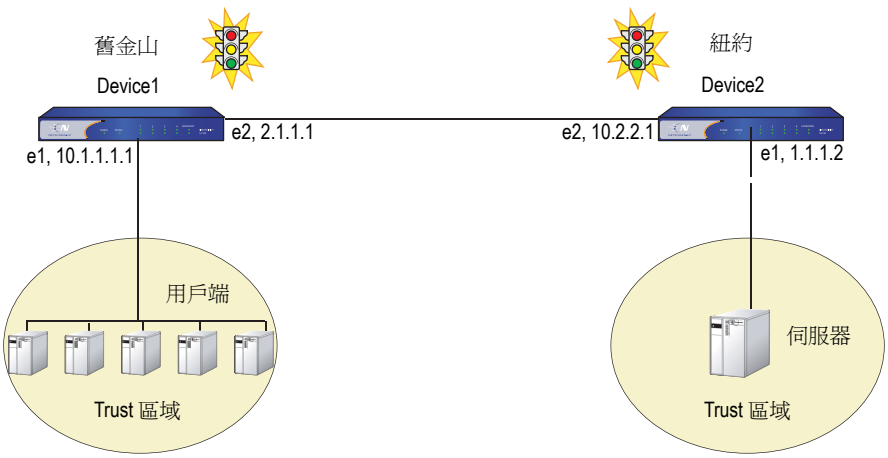
4. **政策**

```
set policy from trust to untrust any any any permit
set policy from untrust to trust any any any permit
```

範例：具入口政策制訂的以政策爲基礎的 VPN

此範例說明如何同時在介面層級及政策中執行入口政策制訂。在 *Device1* 的 ethernet1 介面上，您將入口最大頻寬設定爲 20000 Kbps。如此設定後，所有超過 20000 kbps 的通訊流量 (來自連接至 ethernet1 介面上的 *Device1* 的用戶端) 均會遭到卸除。介面的入口政策制訂會套用至所有抵達該介面的通訊流量。爲達到更高的精確度，您可於政策層級套用入口政策制訂。在此範例中，您建立限制 *Device1* 上所有入口 FTP 通訊協定通訊流量的政策，方法是在 trust 和 untrust 區之間建立政策，並將政策制訂頻寬設定爲 5000 Kbps。所有來自 trust 區通往 untrust 區並超過 5000 Kbps 的 FTP 通訊流量均會遭到卸除。

圖 80: 以政策爲基礎的 VPN



WebUI (Device1 的組態)

1. **介面**

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 10.1.1.1/24
   Zone: Trust
   Interface mode: (選擇) NAT

   Network > Interfaces > Edit (對於 ethernet2): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 2.1.1.1/24
   Zone: Untrust
   Interface mode: (選擇) Route

2. **IKE VPN**

   VPNs > AutoKey Advanced > Gateway > New: 輸入下面的內容，然後按一下 **OK**:

   Gateway Name: device2_ike
   Security Level: Standard
   Remote Gateway Type:
   Static IP Address: (選擇), IP Address/Hostname: 2.2.2.2

預先共享的金鑰

Preshared Key: secret
Outgoing Interface: ethernet2

> Advanced: 輸入下面的進階設定，然後按一下 OK 返回基本 Gateway 組態頁面 :
Phase 1 Proposal: pre-g2-3des-sha

VPNs > AutoKey IKE New: 輸入下面的內容，然後按一下 **OK**:

VPN Name: device2_vpn
Gateway Name: device2_ike

3. **以介面爲基礎的政策制訂**

Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

Traffic Bandwidth, Ingress: 20000

4. **路由**

Network > Routing > Destination > New: 輸入下面的內容，然後按一下 **OK**:

Network IP Address/Netmask: 10.2.1.0/24
Interface: (選擇) ethernet2
Gateway IP Address: 2.2.2.2

5. **政策**

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: 1
Service: FTP
Action: Tunnel
Tunnel VPN: (選擇), device2_vpn
Modify matching bidirectional VPN policy: (選擇)

> Advanced: 輸入下面的進階設定，然後按一下 **Return** 返回基本 Policies 組態頁面 :

Traffic Shaping (選擇) Policing Bandwidth: 5000

CLI (Device1 的組態)

1. 介面
   set interface ethernet1 zone trust
   set interface ethernet2 zone untrust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 ip 2.1.1.1/24
   set interface ethernet1 route

2. **IKE VPN**
   set ike gateway device2_ike address 2.2.2.2 main outgoing interface ethernet2 preshare secret proposal pre-g2-3des-sha
   set vpn device2_vpn gateway device2_ike no-replay tunnel idletime 0 sec-level standard

3. 路由
   set route 10.2.1.0/24 interface ethernet2 gateway 2.2.2.2

4. 政策
   set policy from trust to untrust any any ftp tunnel vpn device2_vpn pair-policy 2 traffic pbw 5000
   set policy from untrust to trust any any ftp tunnel vpn netscreeen2_vpn pair-policy 1 traffic pbw 5000

5. 以介面爲基礎的政策制訂
   set interface ethernet1 bandwidth ingress mbw 20000

WebUI (Device2 的組態)

1. 介面
   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 1.1.1.1/24
   Zone: Trust
   Interface mode: (選擇) Route

   Network > Interfaces > Edit (對於 ethernet2): 輸入下面的內容，然後按一下 **OK**:

   IP Address/Netmask: 10.2.2.1/24
   Zone: Untrust
   Interface mode: (選擇) NAT

2. **IKE VPN**
   VPNs > AutoKey Advanced > Gateway > New: 輸入下面的內容，然後按一下 **OK**:

   Gateway Name: device1_ike
   Security Level: Standard
   Remote Gateway Type:
   Static IP Address: (選擇), IP Address/Hostname: 2.1.1.1

預先共享的金鑰

Preshared Key: secret
Outgoing Interface: ethernet2

> Advanced: 輸入下面的進階設定，然後按一下 **OK** 返回基本 Gateway 組態頁面 :

Phase 1 Proposal: pre-g2-3des-sha

VPNs > AutoKey IKE New: 輸入下面的內容，然後按一下 **OK**:

VPN Name: device1_vpn
Gateway Name: device1_ike

3. 路由

Network > Routing > Destination > New: 輸入下面的內容，然後按一下 **OK**:

Network IP Address/Netmask: 10.1.1.0/24
Interface: (選擇), ethernet2
Gateway IP Address: 1.1.1.1

4. 政策

Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

Name: 1
Service: FTP
Action: Tunnel
Tunnel VPN: (選擇), device1_vpn
Modify matching bidirectional VPN policy: (選擇)

CLI (Device2 的組態)

1. 介面

```
set interface ethernet1 1.1.1.2/24
set interface ethernet1 route
set interface ethernet2 ip 10.2.2.1/24
set interface ethernet2 nat
```

2. IKE VPN

```
set ike gateway device1_ike address 2.1.1.1 main outgoing interface ethernet2
    preshare secret proposal pre-g2-3des-sha
set vpn device1_vpn gateway device1_ike no-replay tunnel idletime 0 sec-level
    standard
```

3. 路由

```
set route 10.1.1.0/24 interface ethernet1 gateway 1.1.1.1
```

4. 政策

```
set policy id 1 from trust to untrust any any ftp tunnel vpn device1_vpn pair-policy 2
set policy id 2 from untrust to trust any any ftp tunnel vpn device1_vpn pair-policy 1
```

使用回傳介面的通訊流量整理

通訊流量整理在回傳介面上不受支援，因爲實際上並沒有通訊流量在回傳介面上傳輸。不過，回傳介面通常用來作爲錨點 (例如在 VPN 的情況下，用來獲得來源 IP 位址)，而資料則是在實際的出口介面上傳輸。因此，使用 VPN 中的回傳介面時，您需在向外介面上組態通訊流量整理。然後 ScreenOS 便會將會話與實際的向外介面建立關聯，其從路由設定表推論出實際的向外介面，並在路由設定表發生變更時以動態方式更新關聯。

DSCP 標記與整理

您可以在使用 DSCP 標記的政策中整理通訊流量，或是使用與通訊流量整理無關的 DSCP 標記。通訊流量整理管制安全性裝置上處理通訊流量的方式，並可於介面層級或政策中組態。您在政策層級所設定的 DSCP 標記管制下游路由器處理通訊流量的方式。

若您啓用 DSCP 標記但未設定值，ScreenOS 會將政策優先順序對應至 DSCP 系統中同等的 IP 優先優先順序。進行對應時，ScreenOS 會以 IP 優先優先順序覆寫 ToS 位元組中的前三個位元。例如，若您建立一個給予所有通訊流量優先順序爲 2 的政策 (0 爲最高優先順序)，且您啓用 DSCP 標記，則 ScreenOS 會在出口介面上針對具層級 2 優先順序的政策佇列通訊流量，並將之以同等的 IP 優先優先順序進行標記。下列指令會建立一個給予所有通訊流量優先順序 2 的政策，並啓用 DSCP 標記 :

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable
```

但若您給予 DSCP 一個 46 (最高優先順序) 的 *dscp-byte* **值**，安全性裝置仍然會在出口介面佇列優先順序爲 2 的通訊流量，但會以 DSCP 值覆寫 ToS 位元組的前 6 個位元。

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable
    value 46
```

DSCP 標記在所有平台上均受支援，且可利用通訊流量整理進行組態或獨立組態。下表顯示 DSCP 標記在各種平台上的運作方式。

表 20: 用於純文字通訊流量的 DSCP 標記

說明	硬體安全性用戶端 NetScreen-5XT, NetScreen-5GT, NetScreen 25/50, NetScreen-204/208, NetScreen 500	NetScreen-5000 系列 , ISG 1000, ISG 2000
純封包，政策上無標記。	無標記。	無標記。
純封包，政策上有標記。	依據政策標記封包。	依據政策標記封包。
預先標記封包，政策上無標記。	維持封包中的標記。	維持封包中的標記。
預先標記封包，政策上有標記。	依據政策覆寫封包中的標記。	依據政策覆寫封包中的標記。

表 21: 用於以政策爲基礎的 VPN 的 DSCP 標記

說明	硬體安全性用戶端 NetScreen-5XT, NetScreen-5GT, NetScreen 25/50, NetScreen-204/208, NetScreen 500	NetScreen-5000 系列 , ISG 1000, ISG 2000
純封包進入以政策爲基礎的 VPN，政策上無標記。	無標記。	無標記。
純封包進入以政策爲基礎的 VPN，政策上有標記	僅標記 ESP 標頭，以政策爲依據。	僅標記 ESP 標頭，以政策爲依據。
預先標記封包進入以政策爲基礎的 VPN，政策上無標記。	未標記 ESP 標頭，維持內封包中的標記。	未標記 ESP 標頭，維持內封包中的標記。
預先標記封包進入以政策爲基礎的 VPN，政策上有標記。	已標記 ESP 標頭，以政策爲依據，維持內封包中的標記。	已標記 ESP 標頭，以政策爲依據，維持內封包中的標記。

表 22: 用於以路由爲基礎的 VPN 的 DSCP 標記

說明	硬體安全性用戶端 NetScreen-5XT, NetScreen-5GT, NetScreen-25/50, NetScreen-204/208, NetScreen-500	NetScreen-5000 系列 , ISG 1000, ISG 2000
純封包進入以路由爲基礎的 VPN，政策上無標記。	無標記。	無標記。
純封包進入以路由爲基礎的 VPN，政策上有標記。	內封包與 ESP 標頭均已標記，以政策爲依據。	依據政策標記內封包。未標記 ESP 標頭。
預先標記封包進入以路由爲基礎的 VPN，政策上無標記。	將內封包標記複製至 ESP 標頭，維持內封包中的標記。	未標記 ESP 標頭，維持內封包中的標記。
預先標記封包進入以路由爲基礎的 VPN，政策上有標記。	依據政策覆寫內封包中的標記，並將內封包標記複製至 ESP 標頭。	依據政策覆寫內封包中的標記。未標記 ESP 標頭。

第 8 章
系統參數

本章重點在於介紹與建立系統參數有關的概念，這些參數會影響安全性裝置的下列方面。本章包含下列各節 :

- 本頁上的「網域名稱系統支援」
- 第 213 頁上的「動態主機組態通訊協定」
- 第 228 頁上的「乙太網路上的點對點通訊協定」
- 第 235 頁上的「許可金鑰」
- 第 237 頁上的「訂閱服務的註冊與啓動訂閱」
- 第 239 頁上的「系統時鐘」

網域名稱系統支援

Juniper Networks 安全性裝置合併了「網域名稱系統」(DNS) 支援，讓您可以使用網域名稱和 IP 位址來識別位置。DNS 伺服器保存一份與網域名稱相關聯的 IP 位址表。除了使用可路由的 IP 位址 (網域名稱 www.juniper.net 對應的 IP 位址是 207.17.137.68) 來參考位置以外，也可以透過 DNS 用網域名稱 (如 www.juniper.net) 參考位置。下列所有程式均支援 DNS 轉譯 :

- 通訊錄
- 系統日誌
- 電子郵件
- WebTrends
- Websense
- LDAP
- SecurID
- RADIUS
- NetScreen-Security Manager

在將 DNS 用於網域名稱 / 位址解析之前，必須在安全性裝置中輸入第三 DNS 伺服器 (主要和次要 DNS 伺服器) 的位址。

注意： 啓用安全性裝置作爲「動態主機組態通訊協定」(DHCP) 伺服器 (請參閱第 213 頁上的「動態主機組態通訊協定」) 時，也必須在 WebUI 的 DHCP 頁面中輸入 DNS 伺服器的 IP 位址，也可以使用 CLI 中的 **set interface** *interface* **dhcp** 指令。

DNS 查詢

安全性裝置會重新整理其 DNS 表中的所有項目，而方法則是在下列時間以指定的 DNS 伺服器的檢查這些項目 :

- 在發生 HA 故障後移轉之後
- 在定期排定的日期時間以及在全天中定期排定的間隔
- 當您以手動方式要求裝置執行 DNS 查詢
  - WebUI: Network > DNS: 按一下 Refresh DNS cache (重新整理 DNS 快取)。
  - CLI: **exec dns refresh**

除了每日自動重新整理 DNS 表這種設定時間的現有方法以外，您也可以定義從 4 小時到 24 小時的時間間隔。

注意： 當您透過 WebUI 新增例如位址 IKE 閘道等完全合格的網域名稱 (FQDN) 時，安全性裝置會在您按一下 **Apply** 或 **OK** 時解析此名稱。當您鍵入參考 FQDN 的 CLI 指令時，安全性裝置會嘗試在您輸入時解析名稱。

安全性裝置連接到 DNS 伺服器以解析網域名稱 / 位址對應時，會將該項目儲存在其 DNS 狀態表中。下面的清單包含 DNS 查詢所涉及的一些詳細內容 :

- 當 DNS 查詢傳回多個項目時，通訊錄會接受所有的項目。在第 205 頁上面所列的其他程式只會接受第一個項目。
- 使用 WebUI 中的 **Refresh** 按鈕或輸入 **exec dns refresh** CLI 指令重新整理查詢時，如果安全性裝置發現網域名稱表中發生了任何變更，會重新安裝所有的政策。
- 如果 DNS 伺服器發生故障，安全性裝置會再度查詢所有內容。
- 如果查詢失敗，安全性裝置會從快取記憶體表中將其移除。
- 在向通訊錄新增位址時，如果網域名稱查詢失敗，安全性裝置會顯示錯誤訊息，陳述已成功新增位址，但是 DNS 名稱查詢失敗。

安全性裝置必須每天進行一次新的查詢，可以安排在指定時間進行。

WebUI

Network > DNS: 輸入下面的內容，然後按一下 **Apply**:

DNS refresh every day at: 選取核取方塊並輸入時間 <hh:mm>

CLI

set dns host schedule *time_str*

DNS 狀態表

DNS 狀態表會報告所有查詢過的網域名稱、其相應的 IP 位址、查詢是否成功以及每個網域名稱 /IP 位址最近一次解析的時間。

圖 81: DNS 狀態表

Name	IP Address	Status	Last Lookup
www.yahoo.com	204.71.200.74 204.71.200.75 204.71.200.67 204.71.200.68	Success	8/13/2000 16:45:33
www.hotbot.com	209.185.151.28 209.185.151.210 216.32.228.18	Success	8/13/2000 16:45:38

若要檢視 DNS 狀態表，請執行下列操作之一：

WebUI

Network > DNS > Show DNS Table

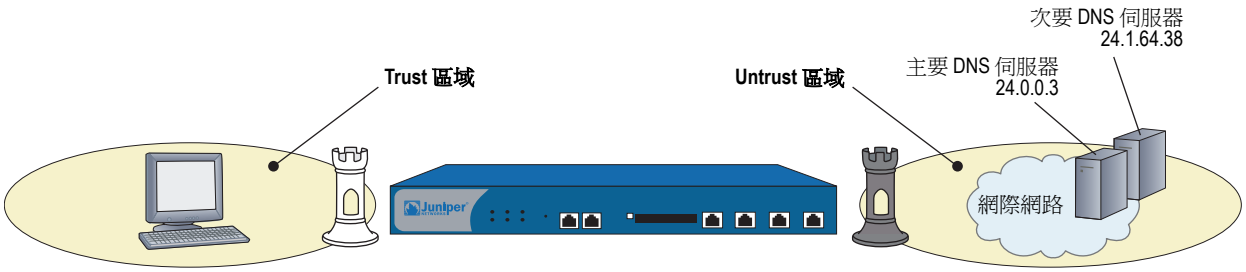
CLI

get dns host report

設定 DNS 伺服器並重新整理排程

若要執行 DNS 功能，在 NetScreen 裝置中爲 24.1.64.38 和 24.0.0.3 上的 DNS 伺服器輸入 IP 位址，這台安全性裝置保護總公司的一台主機。將安全性裝置安排爲在每天晚上 11:00 時重新整理儲存在 DNS 狀態表中的 DNS 設定。

圖 82: DNS 重新整理



WebUI

Network > DNS: 輸入下面的內容，然後按一下 **Apply**:

Primary DNS Server: 24.0.0.3
Secondary DNS Server: 24.1.64.38
DNS Refresh: (選擇)
Every Day at: 23:00

CLI

```
set dns host dns1 24.0.0.3
set dns host dns2 24.1.64.38
set dns host schedule 23:00
save
```

設定 DNS 重新整理間隔

在此範例中，您可以設定安全性裝置以便每 4 小時重新整理它的 DNS 表，開始時間爲每天的 00:01 AM。

WebUI

Network > DNS: 輸入下面的內容，然後按一下 **Apply**:

DNS Refresh: (選擇)
Every Day at: 00:01
Interval: 4

CLI

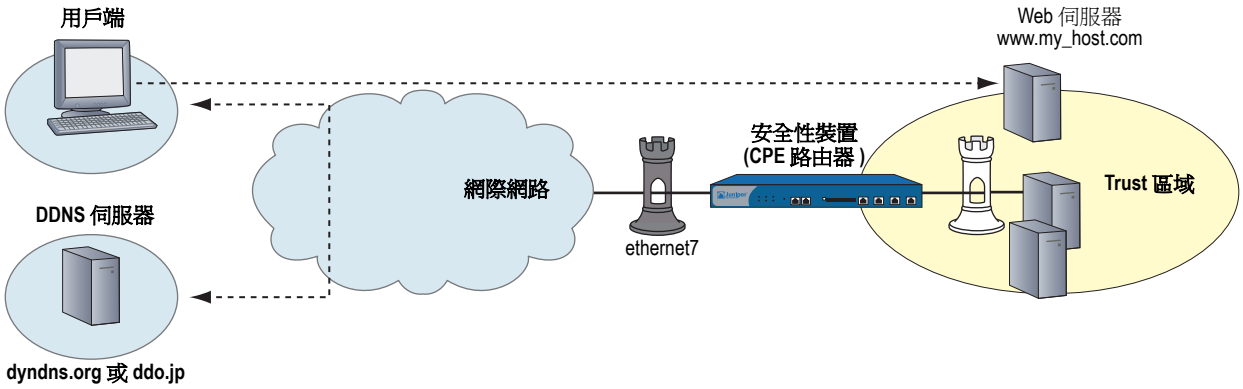
```
set dns host schedule 00:01 interval 4
save
```

動態網域名稱系統

「動態網域名稱系統」(DDNS) 是一種可讓用戶端動態更新已註冊之網域名稱的 IP 位址的機制。這種更新適用於當 ISP 使用 PPP、DHCP 或 XAuth 來動態變更可保護 web 伺服器之 CPE 路由器 (如安全性裝置) 的 IP 位址。網際網路中的用戶端可使用網域名稱來存取 web 伺服器，即使 CPE 路由器的 IP 位址先前已變更過。可利用 DDNS 伺服器 (如 dyndns.org 或 ddo.jp) 來進行此變更，該伺服器包含動態變更的位址及與其聯結的網域名稱。CPE 會定期或是因應 IP 位址的變更，以此資訊更新 DDNS 伺服器。

若要使用 DDNS，請在 DDNS 伺服器上建立一個帳戶 (使用者名稱與密碼)。該伺服器使用此帳戶資訊來組態用戶端裝置。

圖 83: 動態 DNS



在圖 83 中，介面 ethernet7 的 IP 位址可能變更。發生變更時，用戶端仍可透過 dyndns.org 伺服器或 ddo.jp 伺服器，使用主機名稱 (www.my_host.com) 來存取受保護的 Web 伺服器。不論是哪一個伺服器，都需要在安全性裝置上進行不同的組態。

設定 DynDNS 伺服器的 DDNS

在下例中，組態安全性裝置，使其進行 DDNS 操作。裝置使用 dyndns.org 伺服器來解析變更後的位址。針對此伺服器，您需指定使用 Host Name 設定 (明確連結至 DNS 介面 (ethernet7)) 的受保護主機。裝置傳送更新至 ddo.jp 伺服器時，會將 Host Name 與介面的 IP 位址建立關聯。

WebUI

Network > DNS > DDNS > New: 輸入下面的內容，然後按一下 **OK**:

ID: 12
Server Settings:
    Server Type: dyndns
    Server Name: dyndns.org
    Refresh Interval: 24
    Minimum Update Interval: 15
Account Settings:
    Username: swordfish
    Password: ad93lvb
Bind to Interface: ethernet7
Host Name: www.my_host.com

注意： Minimum Update Interval 指定兩次 DDNS 更新之間的最小時間間隔 (以分鐘計)。預設值爲 10 分鐘，允許範圍爲 1-1440。在某些情況下，裝置可能不會更新間隔，因爲 DNS 伺服器首先需要使在快取記憶體中的 DDNS 項目逾時。此外，若您將 Minimum Update Interval 設定爲低值，則安全性裝置可能會將您鎖定。因此，建議使用的值爲 10 分鐘或更多。

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 12 server dyndns.org server-type dyndns refresh-interval 24
    minimum-update-interval 15
set dns ddns id 12 src-interface ethernet7 host-name www.my_host.com
set dns ddns id 12 username swordfish password ad93lvb
save
```

設定 DDO 伺服器的 DDNS

在下例中，組態安全性裝置，使其進行 DDNS 操作。裝置使用 ddo.jp 伺服器來解析位址。如使用 ddo.jp 伺服器，請指定受保護的主機 FQDN 作爲 DDNS 項目的 Username，不要指定使用 Host Name 設定的受保護主機。此服務會根據 Username 值自動產生主機名稱。例如，ddo.jp 伺服器會將使用者名稱 my_host 轉譯成 my_host.ddo.jp。請確定在 ddo.jp 上註冊的網域名稱與產生的 DNS 相符合。

WebUI

Network > DNS > DDNS > New: 輸入下面的內容，然後按一下 **OK**:

```
ID: 25
Server Settings:
        Server Type: ddo
        Server Name: juniper.net
        Refresh Interval: 24
        Minimum Update Interval: 15
Account Settings:
        Username: my_host
        Password: ad93lvb
Bind to Interface: ethernet7
```

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 25 server ddo.jp server-type ddo refresh-interval 24
    minimum-update-interval 15
set dns ddns id 25 src-interface ethernet7
set dns ddns id 25 username my_host password ad93lvb
save
```

代理 DNS 位址分割

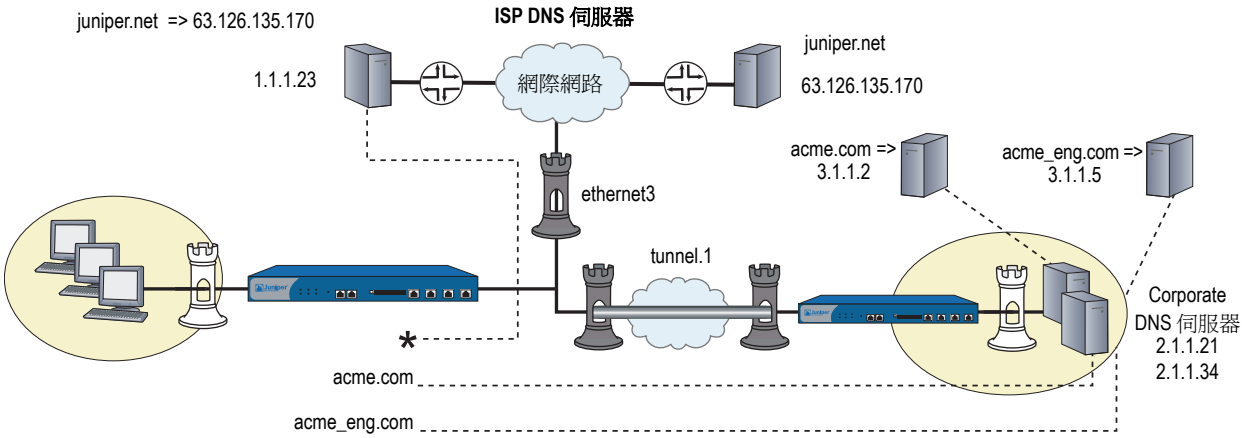
代理 DNS 功能提供一種透明機制，使用戶端可以分割 DNS 查詢。使用此技巧，代理即可根據部分或完整網域名稱，選擇性地將 DNS 查詢重新定向爲特定的 DNS 伺服器。當多個 VPN 通道或 PPPoE 虛擬連結提供了網路連接，必須將某些 DNS 查詢導向某個網路，並將其他查詢導向另一個網路時，這會很有用。

DNS proxy 的優點如下 :

- 通常網域查詢會更有效率。例如，公司網域 (如 acme.com) 用的 DNS 查詢只能在公司 DNS 伺服器中進行，所有其他的查詢在 ISP DNS 伺服器中進行，這可降低公司伺服器的負載。這樣也可以避免公司網域資訊外洩到網際網路上。
- DNS proxy 可讓您透過通道介面傳輸所選的 DNS 查詢，可避免惡意使用者取得內部網路組態。例如，公司伺服器連結的 DNS 查詢可通過通道介面來使用安全性功能，例如驗證、加密與反重播攻擊。

下列指令可建立兩個代理 -DNS 項目，這些項目會選擇性地將 DNS 查詢轉寄至不同的伺服器。

圖 84: 分割 DNS 要求



- 任何以 FQDN (包含網域名稱 acme.com) 進行的 DNS 查詢都會透過通道介面 tunnel.1 外傳至位於 IP 位址 2.1.1.21 的公司 DNS 伺服器。

  例如，如果主機傳送 www.acme.com 的 DNS 查詢，裝置會自動將查詢導向至此伺服器。(我們假設伺服器將查詢解析到 IP 位址 3.1.1.2。)

- 任何以 FQDN (包含網域名稱 acme_engineering.com) 進行的 DNS 查詢都會透過通道介面 tunnel.1 外傳至位於 IP 位址 2.1.1.34 的 DNS 伺服器。

  例如，如果主機傳送 intranet.acme_eng.com 的 DNS 查詢，裝置會將查詢導向至此伺服器。(我們假設伺服器將查詢解析到 IP 位址 3.1.1.5。)

- 所有其他 DNS 查詢 (以星號表示) 會略過公司伺服器，透過介面 ethernet3 外傳至位於 IP 位址 1.1.1.23 的 DNS 伺服器。

  例如，如果主機和網域名稱是 www.juniper.net，裝置會自動略過公司伺服器，並將查詢導向至此伺服器，這樣會將查詢解析爲 IP 位址 207.17.137.68。

WebUI

1. **Network > DNS > Proxy:** 輸入下面的內容，然後按一下 **Apply:**
   Initialize DNS Proxy: Enable
   Enable DNS Proxy: Enable

2. **Network > DNS > Proxy > New:** 輸入下面的內容，然後按一下 **OK:**
   Domain Name: acme.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.21

3. **Network > DNS > Proxy > New:** 輸入下面的內容，然後按一下 **OK:**
   Domain Name: acme_eng.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.34

4. **Network > DNS > Proxy > New:** 輸入下面的內容，然後按一下 **OK:**
   Domain Name: *
   Outgoing Interface: ethernet3
   Primary DNS Server: 1.1.1.23

CLI

```
set dns proxy
set dns proxy enable
set interface ethernet3 proxy dns
set dns server-select domain acme.com outgoing-interface tunnel.1 primary-server
    2.1.1.21
set dns server-select domain acme_eng.com outgoing-interface tunnel.1
    primary-server 2.1.1.34
set dns server-select domain * outgoing-interface ethernet3 primary-server
    1.1.1.23
save
```

動態主機組態通訊協定

「動態主機組態通訊協定」(DHCP) 的設計是透過自動爲網路上的主機指派 TCP/IP 設定，來減少對網路管理員的工作需求。DHCP 會代替管理員自動爲網路中的每台機器指派、組態、追蹤和變更 (有必要時) 所有的 TCP/IP 設定。此外，DHCP 確保不會使用重複位址、重新指派未使用的位址，並且可以自動爲主機連接的子網路指派適當的 IP 位址。

不同的安全性裝置支援不同的 DHCP 角色 :

- **DHCP 用戶端 :** 有些安全性裝置可以作爲 DHCP 用戶端，接收爲任何區域中的實體介面指派的 IP 位址。
- **DHCP 伺服器 :** 有些安全性裝置也可以作爲 DHCP 伺服器，爲任何區域內任何實體的主機 (作爲 DHCP 用戶端) 或 VLAN 介面配置動態 IP 位址。

注意 : 使用 DHCP 伺服器模組爲區域內的主機 (如工作站) 指派位址時，您仍然可以將固定 IP 位址用於其他機器 (如郵件伺服器和 WINS 伺服器)。

- **DHCP 轉接代理程式 :** 此外，有些安全性裝置也可以作爲 DHCP 轉接代理程式，接收來自 DHCP 伺服器的 DHCP 資訊，並將該資訊轉送給任何區域內的任何實體或 VLAN 介面上的主機。
- **DHCP 用戶端/伺服器/轉接代理程式:** 有些安全性裝置可以同時作爲 DHCP 用戶端、伺服器和轉接代理程式。您僅能夠在單一介面上設定一個 DHCP 角色。例如，您不能夠在相同的介面上設定 DHCP 用戶端和伺服器。您也可以選擇將 DHCP 用戶端模組設定爲轉寄它所收到的 TCP/IP 設定給 DHCP 伺服器模組，以便在將 TCP 設定提供給 Trust 區域中的主機作爲 DHCP 用戶端時使用。

DHCP 由兩個元件組成 : 用於傳送主機專用的 TCP/IP 組態設定的通訊協定和用於配置 IP 位址的機制。當安全性裝置作爲 DHCP 伺服器時，會在每台主機開機時爲其提供下面的 TCP/IP 設定 :

- 預設的閘道 IP 位址和網路遮罩。如果您將這些設定保留爲 0.0.0.0/0，DHCP 伺服器模組會自動使用預設 Trust 區域介面的 IP 位址和網路遮罩。

注意 : 在可以有多個介面繫結到 Trust 區域的裝置上，預設介面是第一個繫結到該區域並指派 IP 位址的介面。

- 下列伺服器的 IP 位址 :
  - WINS 伺服器 (2):「Windows 網際網路命名服務」(WINS) 伺服器將 Windows NT 網路環境中使用的 NetBIOS 名稱對應到以 IP 爲基礎的網路中使用的 IP 位址。括弧中的數字表示支援的伺服器數量。
  - NetInfo 伺服器 (2): NetInfo 是一種 Apple 網路服務，用於在 LAN 中分配管理資料。
  - NetInfo 標籤 (1): Apple NetInfo 資料庫使用的識別標籤。
  - DNS 伺服器 (3):「網域名稱系統」(DNS) 伺服器會將全域資源定址器 (URL) 對應到 IP 位址。
  - SMTP 伺服器 (1):「簡單郵件傳輸通訊協定」(SMTP) 伺服器將 SMTP 訊息傳送給儲存向內郵件的郵件伺服器 (如 POP3 伺服器)。
  - POP3 伺服器 (1):「郵局通訊協定版本 3」(POP3) 伺服器儲存向內郵件。POP3 伺服器必須與 SMTP 伺服器一起使用。
  - 新聞伺服器 (1): 新聞伺服器接收並儲存新聞群組寄來的文章。

注意 : 安全性裝置向 DHCP 用戶端傳遞上述參數時，如果該用戶端有指定的 IP 位址，該位址將覆寫從 DHCP 伺服器接收到的所有動態資訊。

組態 DHCP 伺服器

安全性裝置在任何區域中的任何實體或 VLAN 介面中最多可支援八台 DHCP 伺服器。作爲 DHCP 伺服器時，安全性裝置以兩種模式配置 IP 位址和子網路遮罩 :

- 在 Dynamic mode (動態模式) 中，當作 DHCP 伺服器的安全性裝置會爲從作爲主機 DHCP 用戶端的位址集區中指派 (或「租借」) IP 位址。IP 位址可租用固定的時間，或租用到用戶端放棄該 IP 位址爲止。(若要定義無限制的租用期，請輸入 0。)
- 在 Reserved mode (保留模式) 中，特定用戶端每次上線時，安全性裝置都會從位址集區中專門爲其指派指定的 IP 位址。

注意 : 位址集區是指相同子網路中的 IP 位址定義範圍，安全性裝置可以從中提取 DHCP 位址進行指派。最多可以群組 255 個 IP 位址。

DHCP 伺服器最多支援 64 個項目，可包括單一 IP 位址和動態及已保留 IP 位址的 IP 位址範圍。

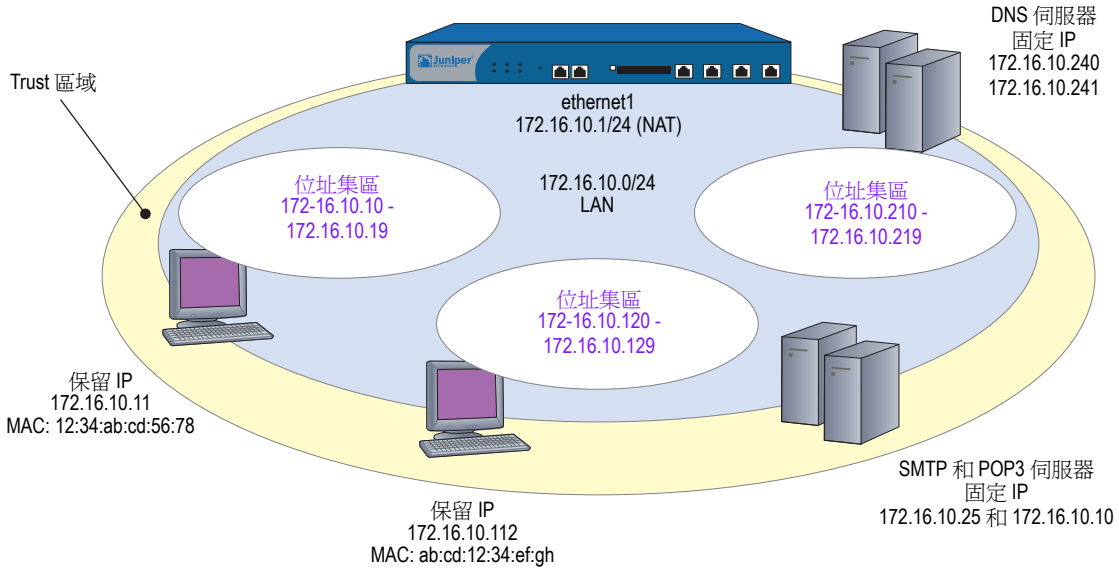
安全性裝置將透過 DHCP 指派的每個 IP 位址儲存在快閃記憶體中。因此，將安全性裝置重新開機並不會影響位址指派。

在本範例中，使用 DHCP 將 Trust 區域內的 172.16.10.0/24 網路分成三個 IP 位址集區。

- 172.16.10.10 到 172.16.10.19
- 172.16.10.120 到 172.16.10.129
- 172.16.10.210 到 172.16.10.219

除了使用保留 IP 位址的兩個工作站和具有靜態 IP 位址的四個伺服器以外，DHCP 伺服器會以動態方式指派所有的 IP 位址。介面 ethernet1 連結到 Trust 區域，其 IP 位址爲 172.16.10.1/24，在 NAT 模式中。網域名稱是 dynamic.com。

圖 85: 作爲 DHCP 伺服器的裝置



WebUI

1. 位址

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: DNS#1
   Comment: Primary DNS Server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 172.16.10.240/32
   Zone: Trust

   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: DNS#2
   Comment: Secondary DNS Server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 172.16.10.241/32
   Zone: Trust

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

Address Name: SMTP
Comment: SMTP Server
IP Address/Domain Name:
IP/Netmask: (選擇), 172.16.10.25/32
Zone: Trust

Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

Address Name: POP3
Comment: POP3 Server
IP Address/Domain Name:
IP/Netmask: (選擇), 172.16.10.110/32
Zone: Trust

2. **DHCP 伺服器**
Network > DHCP > Edit (對於 ethernet1) > DHCP Server: 輸入下面的內容，然後按一下 **Apply**:

Lease: Unlimited (選擇)
WINS#1: 0.0.0.0
DNS#1: 172.16.10.240

注意： 如果您將 Gateway 和 Netmask 欄位保留爲 0.0.0.0，DHCP 伺服器模組會將 ethernet1 的 IP 位址和子網路遮罩集傳送至它的用戶端 (在此範例中爲 172.16.10.1 和 255.255.255.0)。但是，如果您啓用 DHCP 用戶端模組以便將 TCP/IP 設定轉寄至 DHCP 伺服器模組 (請參閱 第 226 頁上的「傳播 TCP/IP 設定」)，則您必須以手動方式在 Gateway 和 Netmask 欄位中輸入 172.16.10.1 和 255.255.255.0。

> Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

WINS#2: 0.0.0.0
DNS#2: 172.16.10.241
DNS#3: 0.0.0.0
SMTP: 172.16.10.25
POP3: 172.16.10.110
NEWS: 0.0.0.0
NetInfo Server #1: 0.0.0.0
NetInfo Server #2: 0.0.0.0
NetInfo Tag: (不填入欄位)
Domain Name: dynamic.com

> Addresses > New: 輸入下面的內容，然後按一下 **OK**:

Dynamic: (選擇)
IP Address Start: 172.16.10.10
IP Address End: 172.16.10.19

> Addresses > New: 輸入下面的內容，然後按一下 **OK**:

Dynamic: (選擇)
IP Address Start: 172.16.10.120
IP Address End: 172.16.10.129

> Addresses > New: 輸入下面的內容，然後按一下 **OK**:

Dynamic: (選擇)
IP Address Start: 172.16.10.210
IP Address End: 172.16.10.219

> Addresses > New: 輸入下面的內容，然後按一下 **OK**:

Reserved: (選擇)
IP Address: 172.16.10.11
Ethernet Address: 1234 abcd 5678

> Addresses > New: 輸入下面的內容，然後按一下 **OK**:

Reserved: (選擇)
IP Address: 172.16.10.112
Ethernet Address: abcd 1234 efgh

CLI

1. 位址
   set address trust dns1 172.16.10.240/32 "primary dns server"
   set address trust dns2 172.16.10.241/32 "secondary dns server"
   set address trust snmp 172.16.10.25/32 "snmp server"
   set address trust pop3 172.16.10.110/32 "pop3 server"

2. **DHCP 伺服器**
   set interface ethernet1 dhcp server option domainname dynamic.com
   set interface ethernet1 dhcp server option lease 0
   set interface ethernet1 dhcp server option dns1 172.16.10.240
   set interface ethernet1 dhcp server option dns2 172.16.10.241
   set interface ethernet1 dhcp server option smtp 172.16.10.25
   set interface ethernet1 dhcp server option pop3 172.16.10.110
   set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19
   set interface ethernet1 dhcp server ip 172.16.10.120 to 172.16.10.129
   set interface ethernet1 dhcp server ip 172.16.10.210 to 172.16.10.219
   set interface ethernet1 dhcp server ip 172.16.10.11 mac 1234abcd5678
   set interface ethernet1 dhcp server ip 172.16.10.112 mac abcd1234efgh
   set interface ethernet1 dhcp server service
   save

注意 : 如果您沒有爲閘道或網路遮罩設定 IP 位址，DHCP 伺服器模組會將 ethernet1 (在本例爲 172.16.10.1 和 255.255.255.0) 的 IP 位址和網路遮罩傳送給它的用戶端。但是，如果您啓用 DHCP 用戶端模組以便將 TCP/IP 設定轉寄至 DHCP 伺服器模組 (請參閱 第 226 頁上的「傳播 TCP/IP 設定」)，則您必須手動地設定這些選項。**set interface ethernet1 dhcp server option gateway 172.16.10.1** 和 **set interface ethernet1 dhcp server option netmask 255.255.255.0**。

自訂 DHCP 伺服器選項

當您指定介面的 DHCP 伺服器時，可能必須指定選項來識別伺服器，或是提供伺服器所使用的資訊。例如，您可指定主要與次要 DNS 伺服器的 IP 位址，或是設定 IP 位址租用時間。

以下是預先定義的 DHCP 服務，如 RFC 2132 *中的 DHCP Options and BOOTP Vendor Extensions* 所述。

表 23: 預先定義的 DHCP 服務

術語	ScreenOS CLI 術語	選項代碼
子網路遮罩	netmask	1
路由器選項	gateway	3
「網域名稱系統」(DNS) 伺服器	dns1, dns2, dns3	6
網域名稱	domainname	15
NetBIOS 上的 TCP/IP 名稱伺服器選項	wins1, wins2	44
IP 位址租用時間	lease	51
SMTP 伺服器選項	smtp	69
POP3 伺服器選項	pop3	70
NNTP 伺服器選項	news	71
(N/A)	nis1, nis2	112
(N/A)	nistag	113

當預先定義的伺服器選項不足以應付時，您可定義自訂 DHCP 伺服器選項。例如，使用某些 Voice-over-IP (VoIP) 組態時，必須傳送預先定義的伺服器選項所不支援的附加組態資訊。在這種情況下，就必須定義適當的自訂選項。

在下例中，爲作爲 DHCP 用戶端的 IP 電話建立 DHCP 伺服器定義。該電話使用下列自訂選項 :

- 選項代碼 444，包含字串 "Server 4"
- 選項代碼 66，包含 IP 位址 1.1.1.1
- 選項代碼 160，包含整數 2004

CLI

1. 位址
   set address trust dns1 172.16.10.240/32 "primary dns server"
   set address trust dns2 172.16.10.241/32 "secondary dns server"

2. **DHCP 伺服器**
   set interface ethernet1 dhcp server option domainname dynamic.com
   set interface ethernet1 dhcp server option lease 0
   set interface ethernet1 dhcp server option dns1 172.16.10.240
   set interface ethernet1 dhcp server option dns2 172.16.10.241
   set interface ethernet1 dhcp server option custom 444 string "Server 4"
   set interface ethernet1 dhcp server option custom 66 ip 1.1.1.1
   set interface ethernet1 dhcp server option custom 160 integer 2004
   set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19

在 NSRP 叢集中放置 DHCP 伺服器

冗餘 NSRP 叢集中的主單元發揮 DHCP 伺服器的功能時，叢集中的所有成員都會保留全部的 DHCP 組態以及 IP 位址指派。一旦發生故障後移轉，新的主單元會維護所有的 DHCP 指派。然而 HA 通訊的終止將會中斷叢集成員間現有 DHCP 指派的同步化。在還原 HA 通訊之後，您可以在叢集中的兩個單位上使用下列的 CLI 指令，重新同步化 DHCP 指派 : **set nsrp rto-mirror sync**。

DHCP 伺服器偵測

當安全性裝置中的 DHCP 伺服器啓動時，系統可以先檢查介面上是否已經有 DHCP 伺服器。如果在網路上偵測到另外的 DHCP 伺服器，ScreenOS 會自動停止本機 DHCP 伺服器程序而不啓動。爲了偵測其它 DHCP 伺服器，裝置會以兩秒爲間隔傳送出 DHCP 啓動要求。如果裝置沒有收到對於其啓動要求的任何回應，它接著會啓動其本機 DHCP 伺服器程序。

如果安全性裝置收到來自其它 DHCP 伺服器的回應，系統會產生一個訊息指出安全性裝置上的 DHCP 服務已啓用，但是由於網路上出現其它 DHCP 伺服器，因此尚未啓動。記錄記錄包括現有 DHCP 伺服器的 IP 位址。

您可以設定以下三種操作模式的其中一種，以進行介面上的 DHCP 伺服器偵測 : 自動、啓用或停用。自動模式會使安全性裝置永遠在啓動時檢查現有的 DHCP 伺服器。在將安全性 DHCP 伺服器設定爲「啓用」或「停用」模式之後，您可以將裝置組態爲不嘗試偵測介面上其它的 DHCP 伺服器。在「啓用」模式中，DHCP 伺服器永遠爲開啓狀態，而且如果網路上已經有現存的 DHCP 伺服器，裝置也不會檢查。在「停用」模式中，DHCP 伺服器永遠爲關閉狀態。

注意 : Auto 模式爲 NetScreen-5XP 和 NetScreen-5XT 裝置的預設 DHCP 伺服器偵測模式。對於支援 DHCP 伺服器的其它 Juniper Networks 安全性裝置而言，Enable 模式爲預設的 DHCP 伺服器偵測模式。

啓用 DHCP 伺服器偵測

在本範例中，您可以在 ethernet1 介面上設定 DHCP 伺服器，在啓動前先檢查介面上現有的 DHCP 伺服器。

WebUI

Network > DHCP > Edit (對於 ethernet1) > DHCP Server: 輸入下面的內容，然後按一下 **OK**:

Server Mode: Auto (選擇)

CLI

```
set interface ethernet1 dhcp server auto
save
```

停用 DHCP 伺服器偵測

在本範例中，您可以在 ethernet1 介面上設定 DHCP 伺服器，直接啓動而不檢查網路上是否已經存在現有的 DHCP 伺服器。

WebUI

Network > DHCP > Edit (對於 ethernet1) > DHCP Server: 輸入下面的內容，然後按一下 **OK**:

Server Mode: Enable (選擇)

CLI

```
set interface ethernet1 dhcp server enable
save
```

注意： 發佈 CLI 指令 **set interface** 介面 **dhcp server service** 指令將會啓動 DHCP 伺服器。如果介面的 DHCP 伺服器偵測模式設定爲「自動」，只有在網路上沒有找到現有伺服器的情況下，安全性裝置上的 DHCP 伺服器才會啓動。發佈 **unset interface** interface **dhcp server service** 指令將會停用安全性裝置上的 DHCP 伺服器，並且同時刪除任何現有的 DHCP 組態。

將安全性裝置指派爲 DHCP 轉接代理程式

作爲 DHCP 轉接代理程式時，安全性裝置會在單一區域內的主機與另外區域內的 DHCP 伺服器之間轉寄 DHCP 要求和指派資訊。DHCP 訊息可以在安全性裝置與 DHCP 伺服器之間公開傳送，或透過 VPN 通道傳送。

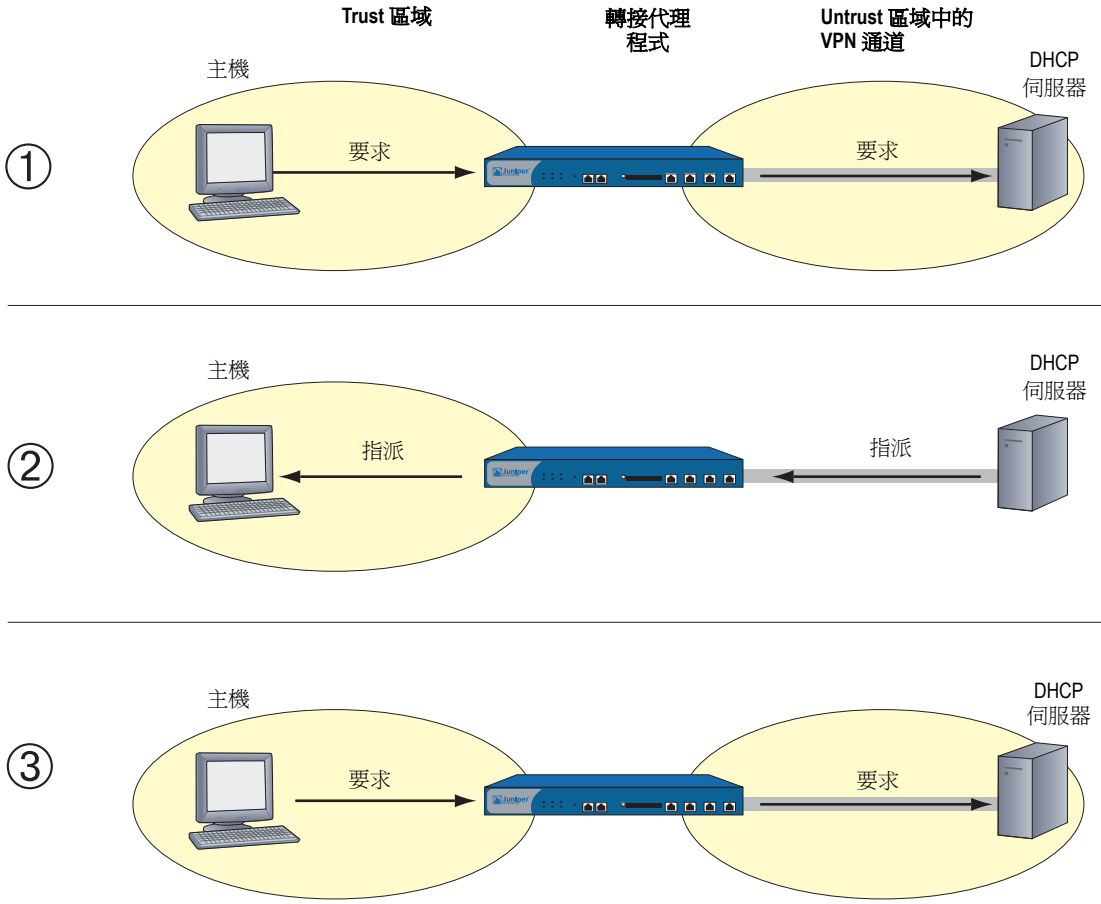
可在安全性裝置的一或多個實體或 VLAN 介面上組態 DHCP 轉接代理程式，但不能在同一介面上組態 DHCP 轉接代理程式和 DHCP 伺服器或用戶端功能。安全性裝置作爲 DHCP 轉接代理程式時，其介面必須在「路由」模式或「透明」模式中。對於「路由」模式中的介面，您必須爲預先定義的服務 DHCP- 轉接組態從一個區域到另一個區域的政策。對於「透明」模式中的介面，DHCP 用戶端必須位於 V1-Trust 區域中，DHCP 伺服器則可以位於 V1-Untrust 或 V1-DMZ 區域。在「透明」模式中的介面不需要政策。

您最多可以爲每個 DHCP 轉接代理程式組態三個 DHCP 伺服器。轉接代理程式會將位址要求從 DHCP 用戶端單點廣播 (unicast) 至所有組態的 DHCP 伺服器。轉接代理程式會將從伺服器收到的第一個回應轉寄至用戶端。

注意： 安全性裝置作爲 DHCP 轉接代理程式時，由於遠端 DHCP 伺服器控制所有的 IP 位址配置，所以該裝置不會產生 DHCP 分配狀態報告。

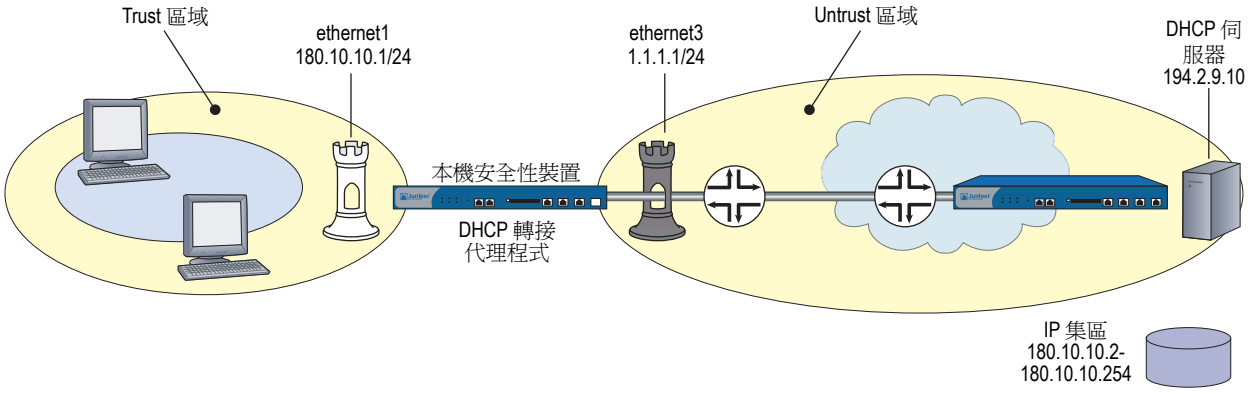
圖 86 說明將安全性裝置作爲 DHCP 轉接代理程式使用的有關程序。當 DHCP 訊息在不信任網路中傳送時，爲確保安全，這些訊息將透過 VPN 通道傳遞。

圖 86: DHCP 轉接代理程式通訊流量



在本範例中，安全性裝置從 IP 位址爲 194.2.9.10 的 DHCP 伺服器中接收 DHCP 資訊，並將其轉送給 Trust 區域中的主機。主機從 DHCP 伺服器上定義的 IP 集區中接收 IP 位址。位址範圍是 180.10.10.2-180.10.10.254。DHCP 訊息會通過在本機安全性裝置和 DHCP 伺服器之間的 VPN 通道，位置在遠端安全性裝置的後面，其 Untrust 區域介面 IP 位址爲 2.2.2.2/24。介面 ethernet1 連結 Trust 區域，IP 位址爲 180.10.10.1/24 而且爲「路由」模式。介面 ethernet3 連結到 Untrust 區域，其 IP 位址爲 1.1.1.1/24。所有的安全區都在 trust-vr 路由設定網域中。

圖 87: 作爲 DHCP 轉接代理程式的裝置



WebUI

1. **介面**
   Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **Apply**:

   Zone: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 180.10.10.1/24

   輸入下面的內容，然後按一下 **OK**:

   Interface Mode: Route

   Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone: Untrust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 1.1.1.1/24

2. **位址**
   Objects > Addresses > List > New: 輸入下面的內容，然後按一下 **OK**:

   Address Name: DHCP Server
   IP Address/Domain Name:
   IP/Netmask: (選擇), 194.2.9.10/32
   Zone: Untrust

3. **VPN**

   VPNs > AutoKey Advanced > Gateway > New: 輸入下面的內容，然後按一下 **OK**:

   Gateway Name: dhcp server
   Security Level: Custom
   Remote Gateway Type:
   Static IP: (選擇), Address/Hostname: 2.2.2.2
   Outgoing Interface: ethernet3

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   Security Level:
   User Defined: Custom (選擇)
   Phase1 Proposal: rsa-g2-3des-sha
   Mode (Initiator): Main (ID Protection)

   VPNs > AutoKey IKE > New: 輸入下面的內容，然後按一下 **OK**:

   VPN Name: to_dhcp
   Security Level: Compatible
   Remote Gateway:
   Predefined: (選擇), to_dhcp

   > Advanced: 輸入下面的內容，然後按一下 **Return** 以設定進階選項並返回基本組態頁面 :

   Bind to: None

4. **DHCP 轉接代理程式**

   Network > DHCP > Edit (對於 ethernet1) > DHCP Relay Agent: 輸入下面的內容，然後按一下 **Apply**:

   Relay Agent Server IP or Domain Name: 194.2.9.10
   Use Trust Zone Interface as Source IP for VPN: (選擇)

5. **路由**

   Network > Routing > Routing Entries > trust-vr New: 輸入下面的內容，然後按一下 **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選擇)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

注意 : 對於向外 VPN 和網路通訊流量，都必須設定通往指定爲預設閘道的外部路由器的路由。在本範例中，安全性裝置將封裝的 VPN 通訊流量傳送到此路由器，作爲它到遠端安全性裝置的路由上的第一個躍點。在本範例的圖解中，透過說明通過路由器的通道來介紹這個概念。

---

6. **政策**
   Policies > (From: Trust, To: Untrust) New: 輸入下面的內容，然後按一下 **OK**:

   Source Address:
   Address Book Entry: (選擇), Any
   Destination Address:
   Address Book Entry: (選擇), DHCP Server
   Service: DHCP-Relay
   Action: Tunnel
   Tunnel VPN: to_dhcp
   Modify matching outgoing VPN policy: (選擇)

CLI

1. **介面**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 180.10.10.1/24
   set interface ethernet1 route
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **位址**
   set address untrust dhcp_server 194.2.9.10/32

3. **VPN**
   set ike gateway "dhcp server" ip 2.2.2.2 main outgoing-interface ethernet3
   proposal rsa-g2-3des-sha
   set vpn to_dhcp gateway "dhcp server" proposal g2-esp-3des-sha

4. **DHCP 轉接代理程式**
   set interface ethernet1 dhcp relay server-name 194.2.9.10
   set interface ethernet1 dhcp relay vpn

5. **路由**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

6. **政策**
   set policy from trust to untrust any dhcp_server dhcp-relay tunnel vpn to_dhcp
   set policy from untrust to trust dhcp_server any dhcp-relay tunnel vpn to_dhcp
   save

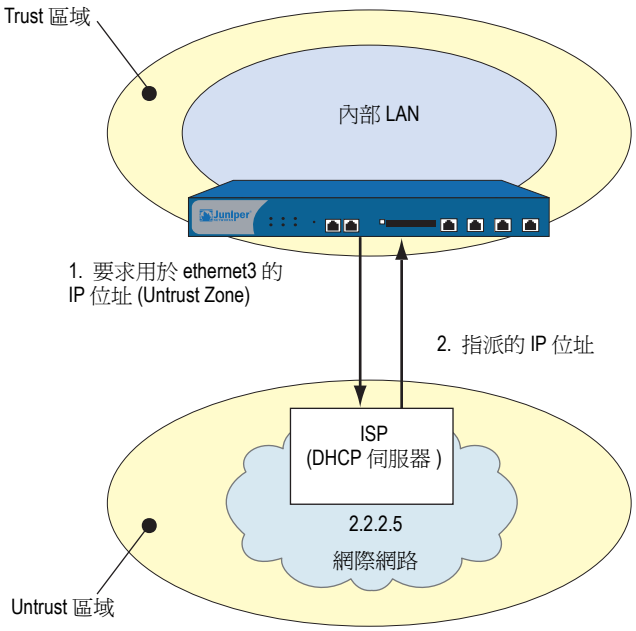
將安全性裝置作爲 DHCP 用戶端使用

作爲 DHCP 用戶端時，安全性裝置會從 DHCP 伺服器中動態接收任何安全性區域中任何實體介面的 IP 位址。如果有多個介面連結至單一安全性區域，只要每個介面並未連接至相同的網路片段，您可以爲每個介面組態一個 DHCP 用戶端。如果您爲連接至相同網路片段的兩個介面組態 DHCP 用戶端，則會使用 DHCP 伺服器所指定的第一個位址。(如果 DHCP 用戶端收到相同 IP 位址的位址更新，則 IKE 不會重新建立金鑰。)

注意： 雖然某些安全性裝置可以同時作爲 DHCP 伺服器、DHCP 轉接代理程式或 DHCP 用戶端，但是您不可以在單一的介面上組態一個以上的 DHCP 角色。

在本例中，連結到 Untrust 區域的介面有動態指派的 IP 位址。安全性裝置向其 ISP 要求 IP 位址時，會接收到其 IP 位址、子網路遮罩、閘道 IP 位址以及租用該位址的期限。DHCP 伺服器的 IP 位址是 2.2.2.5。

圖 88: 作爲 DHCP 用戶端的裝置



注意： 爲 DHCP 服務設定站台前，您必須具有一條「數位用戶線路」(DSL) 及「網際網路服務供應商 (ISP) 提供的帳戶。

WebUI

Network > Interfaces > Edit (對於 ethernet3): 選擇 **Obtain IP using DHCP**，然後按一下 **OK**。

注意： 不能透過 WebUI 指定 DHCP 伺服器的 IP 位址，但可以透過 CLI 這麼做。

CLI

```
set interface ethernet3 dhcp client
set interface ethernet3 dhcp settings server 2.2.2.5
save
```

傳播 TCP/IP 設定

有些安全性裝置可以作爲「動態主機組態通訊協定」(DHCP) 用戶端，從外部 DHCP 伺服器接收任何安全性區域中的任何實體介面的 TCP/IP 設定和 IP 位址。有些安全性裝置可以作爲 DHCP 伺服器，提供 TCP/IP 設定和 IP 位址給任何區域中的用戶端。當安全性裝置同時作爲 DHCP 用戶端和 DHCP 伺服器時，可以傳輸透過 DHCP 用戶端模組獲悉的 TCP/IP 設定給 DHCP 伺服器模組。

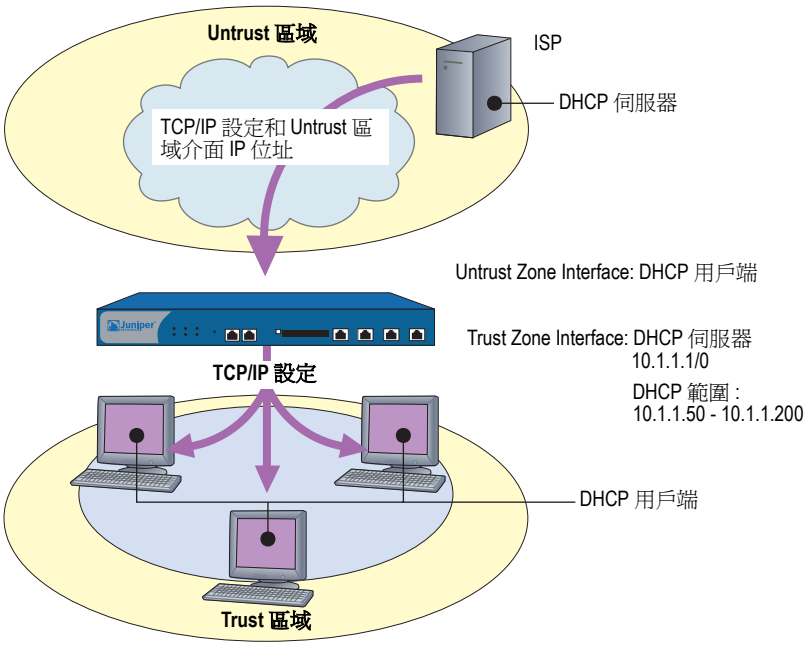
TCP/IP 設定包括預設閘道的 IP 位址和子網路遮罩，和用於任何或所有下列伺服器的 IP 位址 :

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)

注意 : 雖然您可以在任何實體或 VLAN 介面上組態多達八個 DHCP 伺服器，但是裝置上預設的 DHCP 伺服器則常駐於每個平台上的特定介面。在 NetScreen-5XP，預設的 DHCP 伺服器是常駐於 Trust 介面。在 NetScreen-5XT，預設 DHCP 伺服器在 Trust-Untrust 連接埠模式中是常駐於 Trust 介面，在 Dual-Untrust Trust 連接埠模式中是常駐於 ethernet1 介面，而在 Home-Work 和 Combined 連接埠模式中則是常駐於 ethernet2 介面。至於其它裝置，預設 DHCP 伺服器則是常駐於 ethernet1 介面。

在第 227 頁上的圖 89 中，安全性裝置同時是 Untrust 區域中 DHCP 伺服器的用戶端和 Trust 區域中用戶端的 DHCP 伺服器。該裝置採用自己作爲 DHCP 用戶端時接收的 TCP/IP 設定，然後作爲 DHCP 伺服器將設定轉寄給 Trust 區域中的用戶端。Untrust 區域介面是 DHCP 用戶端，且以動態方式從 ISP 接收 IP 位址。

圖 89: DHCP 傳播



您可以組態 DHCP 伺服器模組，使用 **set interface** *interface* **dhcp-client settings update-dhcpserver** 指令傳播從 DHCP 用戶端模組接收的所有 TCP/IP 設定。您也可以用不同設定覆寫任何設定。

在本範例中，您組態安全性裝置以同時作爲 ethernet3 介面上的 DHCP 用戶端和 ethernet1 介面上的 DHCP 伺服器。(預設 DHCP 伺服器是位於 ethernet1 介面。)

作爲 DHCP 用戶端，安全性裝置會從位址爲 211.3.1.6 的外部 DHCP 伺服器接收 ethernet3 介面及其 TCP/IP 設定的 IP 位址。您啓用安全性裝置中的 DHCP 用戶端模組將它所接收的 TCP/IP 設定傳送至 DHCP 伺服器模組。

您組態安全性裝置 DHCP 伺服器模組對其從 DHCP 用戶端模組接收到的 TCP/IP 設定進行下列工作 :

- 轉寄 DNS IP 位址到其在 Trust 區域中的 DHCP 用戶端。
- 以下列內容覆寫預設閘道、網路遮罩和 SMTP 伺服器及 POP3 伺服器 IP 位址 :
  - 10.1.1.1 (這是 ethernet1 介面的 IP 位址)
  - 255.255.255.0 (這是 ethernet1 介面的網路遮罩)
  - SMTP: 211.1.8.150
  - POP3: 211.1.8.172

注意 : 如果 DHCP 伺服器已在 Trust 介面上啓用並有已定義的 IP 位址集區 (這是有些平台上的預設行爲)，您必須先刪除 IP 位址集區，然後才能變更預設閘道和網路遮罩。

您也會組態 DHCP 伺服器模組以傳送下列未從 DHCP 用戶端模組接收到的 TCP/IP 設定 :

- Primary WINS server: 10.1.2.42
- Secondary WINS server: 10.1.5.90

最後，您組態 DHCP 伺服器模組以從下列 IP 集區指派 IP 位址給在 Trust 區域中作爲 DHCP 用戶端的主機 : 10.1.1.50 - 10.1.1.200.

WebUI

注意 : 只能透過 CLI 設定此功能。

CLI

1. **DHCP 用戶端**
   ```
   set interface ethernet3 dhcp-client settings server 211.3.1.6
   set interface ethernet3 dhcp-client settings update-dhcpserver
   set interface ethernet3 dhcp-client settings autoconfig
   set interface ethernet3 dhcp-client enable
   ```
2. **DHCP 伺服器**
   ```
   set interface ethernet1 dhcp server option gateway 10.1.1.1
   set interface ethernet1 dhcp server option netmask 255.255.255.0
   set interface ethernet1 dhcp server option wins1 10.1.2.42
   set interface ethernet1 dhcp server option wins2 10.1.5.90
   set interface ethernet1 dhcp server option pop3 211.1.8.172
   set interface ethernet1 dhcp server option smtp 211.1.8.150
   set interface ethernet1 dhcp server ip 10.1.1.50 to 10.1.1.200
   set interface ethernet1 dhcp server service
   save
   ```

乙太網路上的點對點通訊協定

「乙太網路上的點對點通訊協定」(PPP-over-Ethernet, PPPoE) 將通常用於撥接連線的點對點協定 (PPP)，與乙太網路協定合併。而乙太網路則可以將站台中的多位使用者連接至相同的客戶生產場所設備。許多使用者可以共用相同的實體連接，但是存取控制、請款以及服務類型則還是依單一使用者的方式進行處理。有些安全性裝置支援 PPPoE 用戶端，允許它們將 PPPoE 用於其用戶端的網際網路存取，以相容方式在 ISP 營運的 DSL、Ethernet Direct 和纜線網路上執行。

在支援 PPPoE 的裝置中，您可以在任何或所有介面上組態 PPPoE 用戶端實例。您可以用使用者名稱、密碼和其它參數來組態特定的 PPPoE 實例，然後將此實例連接至介面。如果兩個乙太網路介面 (主要介面與備份介面) 連結至 Untrust 區域，您可以爲 PPPoE 組態一個介面或兩個介面。例如，在 Dual Untrust 連接埠模式中，您可以爲 DHCP 組態主要介面 (ethernet3) 以及爲 PPPoE 組態備份介面 (ethernet2)，或是同時爲主要及備份介面組態 PPPoE。

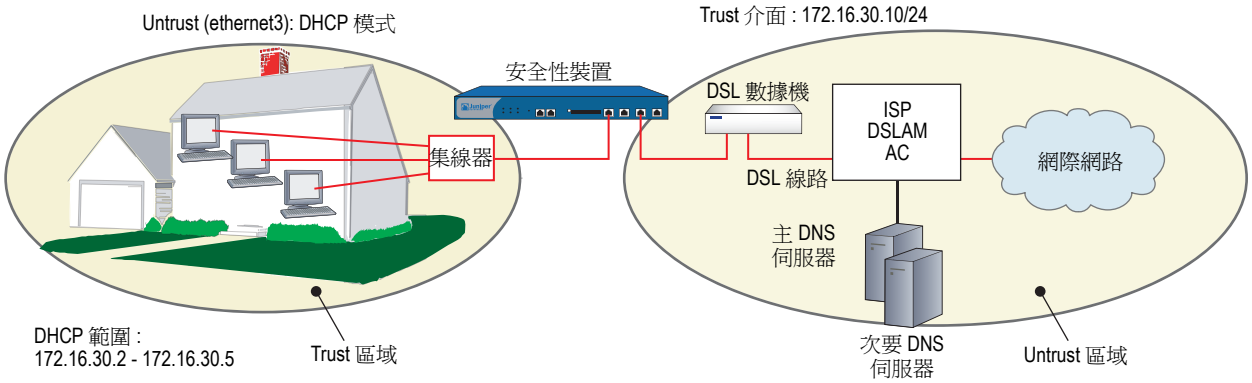
注意 : 在有些平台 (例如 NetScreen-5XT 裝置) 上支援連接埠模式。

設定 PPPoE

下面的範例說明如何爲 PPPoE 連接定義安全性裝置的不信任介面，以及如何初始化 PPPoE 服務。

在本範例中，安全性裝置從 ISP 處接收爲其 Untrust 區域介面 (ethernet3) 動態指派的 IP 位址，而且安全性裝置也會爲其 Trust 區域中的三台主機動態指派 IP 位址。在這種情況下，安全性裝置同時作爲 PPPoE 用戶端和 DHCP 伺服器。Trust 區域介面必須在 NAT 模式或「路由」模式中。在本範例中，爲 NAT 模式。

圖 90: PPPoE



在設定本範例中用於 PPPoE 服務的站台之前，必須具備下列條件 :

- 數位用戶線路 (DSL) 數據機和纜線
- ISP 帳戶
- 使用者名稱和密碼 (從 ISP 取得)

WebUI

1. **介面與 PPPoE**

   Network > Interfaces > Edit (對於 ethernet1): 輸入下面的內容，然後按一下 **OK**:

   Zone: Trust
   Static IP: (出現時選擇此選項)
   IP Address/Netmask: 172.16.30.10/24

   Network > Interfaces > Edit (對於 ethernet3): 輸入下面的內容，然後按一下 **OK**:

   Zone: Untrust
   Obtain IP using PPPoE: (選擇)
   User Name/Password: *<name>/<password>*

   Network > Interfaces > Edit (對於 ethernet3): 若要測試 PPPoE 連接，請按一下 **Connect**。

注意： 初始化 PPPoE 連接後，ISP 會自動爲 Untrust 區域介面和「網域名稱系統」(DNS) 伺服器提供 IP 位址。依預設，當安全性裝置經由 PPPoE 收到 DNS 位址，新的 DNS 設定將會覆寫本機設定。如果您不希望新的 DNS 設定取代本機設定，您可以使用 CLI 指令 **unset pppoe dhcp-updateserver** 以停用此行爲。
如果爲 Untrust 區域介面使用靜態 IP 位址，您必須先取得 DNS 伺服器的 IP 位址，然後在安全性裝置和 Trust 區域中的主機上手動輸入這些位址。

2. DHCP 伺服器

Network > Interfaces > Edit (對於 ethernet1) > DHCP: 選擇 **DHCP Server**，然後按一下 **Apply**。

Network > Interfaces > Edit (對於 ethernet1) > DHCP: 輸入下面的內容，然後按一下 **Apply**:

```
Lease: 1 hour
Gateway: 0.0.0.0
Netmask: 0.0.0.0
DNS#1: 0.0.0.0
```

> Advanced: 輸入下面的內容，然後按一下 **Return**:

```
DNS#2: 0.0.0.0
Domain Name: ( 留空 )
```

Network > Interfaces > DHCP (對於 ethernet1) > New Address: 輸入下面的內容，然後按一下 **OK**:

```
Dynamic: ( 選擇 )
      IP Address Start: 172.16.30.2
      IP Address End: 172.16.30.5
```

3. 在安全性裝置上啓動 PPPoE

1. 關閉 DSL 數據機、安全性裝置和三台工作站的電源。
2. 開啓 DSL 數據機。
3. 開啓安全性裝置。

安全性裝置與 ISP 建立 PPPoE 連接，並透過 ISP 取得 DNS 伺服器的 IP 位址。

4. 在內部網路上啓動 DHCP
開啓工作站。

工作站會自動接收 DNS 伺服器的 IP 位址。在它們嘗試進行 TCP/IP 連接時，會取得自己的 IP 位址。

注意 : 在使用 DHCP 爲 Trust 區域的主機指派 IP 位址時，安全性裝置會自動將從 ISP 接收的 DNS 伺服器的 IP 位址轉寄給主機。

如果不透過 DHCP 動態指派主機 IP 位址，必須在每台主機中手動輸入 DNS 伺服器的 IP 位址。

Trust 區域中的主機與 Untrust 區域建立的每個 TCP/IP 連接都要自動經過 PPPoE 封裝處理。

CLI

1. 介面與 PPPoE

```
set interface ethernet1 zone trust
set interface ethernet1 ip 172.16.30.10/24
set interface ethernet3 zone untrust
set pppoe interface ethernet3
set pppoe username name_str password pswd_str
```

若要測試 PPPoE 連接 :

```
exec pppoe connect
get pppoe
```

2. DHCP 伺服器

```
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 172.16.30.2 to 172.16.30.5
set interface ethernet1 dhcp server option lease 60
save
```

3. 在安全性裝置上啓動 PPPoE

1. 關閉 DSL 數據機、安全性裝置和三台工作站的電源。
2. 開啓 DSL 數據機。
3. 開啓安全性裝置。

4. 在內部網路上啓動 DHCP
開啓工作站。

工作站會自動接收 DNS 伺服器的 IP 位址。在它們嘗試進行 TCP/IP 連接時，會取得自己的 IP 位址。

Trust 區域中的主機與 Untrust 區域建立的每個 TCP/IP 連接都要自動經過 PPPoE 封裝處理。

組態主要與備份 Untrust 介面上的 PPPoE

在此範例中，NetScreen-5XT 裝置爲 Dual Untrust 模式。在下列範例中，您將主要 (ethernet3) 與備份 (ethernet2) 介面中的 PPPoE 組態爲 Untrust 區域。

WebUI

Ethernet3 介面的 PPPoE 組態

Network > PPPoE > New: 輸入下面的內容，然後按一下 **OK**:

PPPoE instance: eth3-pppoe
Bound to interface: ethernet3 (選擇)
Username: user1
Password: 123456
Authentication: Any (選擇)
Access Concentrator: ac-11

Ethernet2 介面的 PPPoE 組態

Network > PPPoE > New: 輸入下面的內容，然後按一下 **OK**:

PPPoE instance: eth2-pppoe
Bound to interface: ethernet2 (選擇)
Username: user2
Password: 654321
Authentication: Any (選擇)
Access Concentrator: ac-22

CLI

1. **Ethernet3 介面的 PPPoE 組態**
   set pppoe name eth3-pppoe username user1 password 123456
   set pppoe name eth3-pppoe ac ac-11
   set pppoe name eth3-pppoe authentication any
   set pppoe name eth3-pppoe interface ethernet3

2. **Ethernet2 介面的 PPPoE 組態**
   set pppoe name eth2-pppoe username user2 password 654321
   set pppoe name eth2-pppoe ac ac-22
   set pppoe name eth2-pppoe authentication any
   set pppoe name eth2-pppoe interface ethernet2
   save

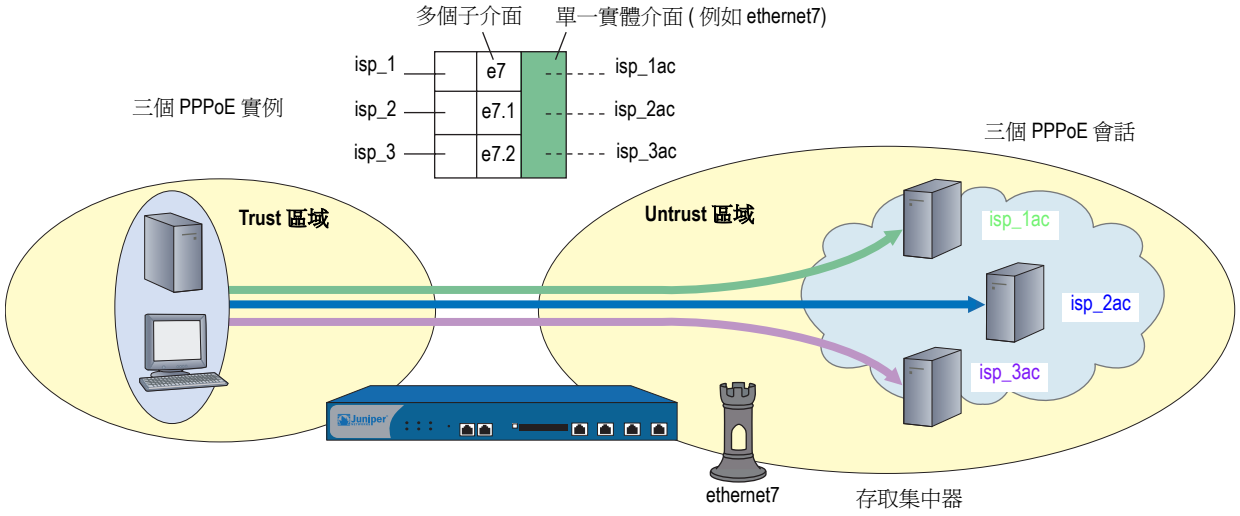
設定多個 PPPoE 會話使用單一介面

某些安全性裝置可支援在某個指定的實體介面上建立多個 PPPoE 子介面 (每個子介面具有相同的 MAC 位址)。此支援功能可讓您建立與某個 ISP 的私人網路連線，並使用相同的實體介面透過不同的 ISP 與網際網路連線。您可使用不同的使用者或網域名稱來建立這些連線，也可以同時與多個不同的 ISP 連線。

一個實體介面上所能允許的最大同時 PPPoE 會話數量僅受該裝置所允許的子介面數量的限制。可支援多會話的實體介面數量是沒有限制的。您可分別爲每個 PPPoE 實例或會話指定 username、static-ip、idle-timeout 和 auto-connect 以及其他參數。

爲了支援 PPPoE 會話，子介面不能有標籤。無標籤介面會使用 Encap (非 VLAN 標籤) 將 VLAN 識別爲子介面。Encap 會將子介面連結至 PPPoE 封裝。藉由裝載多個子介面的方式，單一實體介面即可裝載多個 PPPoE 實例。您可組態每個實例，使其通往指定的存取集中器 (AC)，讓各個實體 (例如 ISP) 透過單一介面管理 PPPoE 會話。如需有關 VLAN 和 VLAN 標籤的詳細資訊，請參閱*第 10 卷：虛擬系統*。

圖 91: 具多個會話的 PPPoE



在下例中，定義三個 PPPoE 實例，爲每個實例指定一個存取集中器 (Access Concentrator，AC)，然後初始化每個實例。

- 實例 isp_1，用戶名爲 "user1@domain1"，密碼爲 "swordfish"，與介面 ethernet7 連結。AC 名爲 "isp_1ac"。
- 實例 isp_2，用戶名爲 "user2@domain2"，密碼爲 "marlin"，與子介面 ethernet7.1 連結。AC 名爲 "isp_2ac"。
- 實例 isp_3，用戶名爲 "user3@domain3"，密碼爲 "trout"，與子介面 ethernet7.2 連結。AC 名爲 "isp_3ac"。

WebUI

介面與子介面

1. **Network > Interfaces > Edit (對於 ethernet7):**
   輸入下面的內容，然後按一下 **OK**:

   Zone Name: Untrust

2. **Network > Interfaces > New (Sub-IF):**
   輸入下面的內容，然後按一下 **OK**:

   Interface Name: ethernet7.1
   Zone Name: Untrust

3. **Network > Interfaces > New (Sub-IF):**
   輸入下面的內容，然後按一下 **OK**:

   Interface Name: ethernet7.2
   Zone Name: Untrust

PPPoE 實例與 AC

4. **Network > PPPoE > New:**
   輸入下面的內容，然後按一下 **OK**:

   PPPoE Instance: isp_1
   Enable: Enable
   Bound to Interface: ethernet7
   Username: user1@domain1
   Access Concentrator: isp_1ac

5. **Network > PPPoE > New:**
   輸入下面的內容，然後按一下 **OK**:

   PPPoE Instance: isp_2
   Enable: Enable
   Bound to Interface: ethernet7.1
   Username: user2@domain2
   Access Concentrator: isp_2ac

6. **Network > PPPoE > New:**
   輸入下面的內容，然後按一下 **OK**:

   PPPoE Instance: isp_3
   Enable: Enable
   Bound to Interface: ethernet7.2
   Username: user3@domain3
   Access Concentrator: isp_3ac

PPPoE 初始化

7. **Network > PPPoE > Connect (對於 isp_1)**
8. **Network > PPPoE > Connect (對於 isp_2)**
9. **Network > PPPoE > Connect (對於 isp_3)**

CLI

1. **介面與子介面**
   set interface ethernet7 zone untrust
   set interface ethernet7.1 encap pppoe zone untrust
   set interface ethernet7.2 encap pppoe zone untrust

2. **PPPoE 實例與 AC**
   set pppoe name isp_1 username user1@domain1 password swordfish
   set pppoe name isp_1 interface ethernet7
   set pppoe name isp_1 ac isp_1ac
   set pppoe name isp_2 username user2@domain2 password marlin
   set pppoe name isp_2 interface ethernet7.1
   set pppoe name isp_2 ac isp_2ac
   set pppoe name isp_3 username user3@domain3 password trout
   set pppoe name isp_3 interface ethernet7.2
   set pppoe name isp_3 ac isp_3ac
   save

3. **PPPoE 初始化**
   exec pppoe name isp_1 connect
   exec pppoe name isp_2 connect
   exec pppoe name isp_3 connect

PPPoE 與高可用性

在「主動 / 被動」模式下支援 PPPoE 的兩個安全性裝置可處理 PPPoE 連接的故障後移轉。初始化連接時，主裝置會使其 PPPoE 狀態與備份裝置同步化。因爲被動裝置使用相同的 IP 位址作爲主裝置，所以不需在其成爲主裝置後建立新的 PPPoE 連接。因此，它可以在主裝置故障後維持與「存取集中器」之間的通訊。這在 PPPoE 介面支援 VPN 連接，且這些連接必須在故障後移轉時使用同一介面 IP 繼續進行的情況下，是十分必要的。如需有關高可用性組態的詳細資訊，請參閱*第 11 卷 : 高可用性*。

許可金鑰

利用許可金鑰功能，無需將 Juniper Networks 安全性裝置升級爲不同的裝置或系統影像，即可擴充其能力。您可購買下列金鑰類型 :

- Advanced
- Capacity
- Extended
- Virtualization
- GTP
- Vsys
- IDP

每台安全性裝置出廠時都已啓用了標準功能集，而且可能會支援啓動選擇性功能或提高現有功能的能力。若要瞭解目前有哪些功能可以進行升級，請參閱 Juniper Networks 的最新行銷文獻。

取得並套用許可金鑰的程序如下：

1. 收集您的授權碼及裝置序號。

   授權碼：是一個密鑰，在爲您或您的公司所購買的 Juniper Networks 安全性裝置產生及啓動許可金鑰時需要此密鑰。注意：產生許可金鑰需要使用「授權碼」，其並非實際的許可金鑰。

   裝置序號：一個唯一的 16 字元代碼，產生許可金鑰時，Juniper Networks 用來識別您的特定安全性裝置。您可在裝置底部或背面找到裝置序號。您亦可在 GUI 的裝置資訊部份中找到序號，或是在 CLI 上執行 "get system" 指令以找到序號。

2. 登入至 Juniper Networks License Management System (LMS) (網址爲 http://www.juniper.net/generate_license)，選擇 **Firewall/IPSec VPN and Intrusion Prevention** 連結，然後遵照系統使用者介面中的指示。

3. Juniper License Management System 以下列兩種方式之一提供許可金鑰：

   - 將許可金鑰下載至您的電腦。
   - 接收含有您許可金鑰的電子郵件。

4. 以下列方式之一安裝許可金鑰：

WebUI

Configuration > Update > ScreenOS/Keys > 選擇 **License Key Update (Features)** > 按一下 **Browse** > 選擇具有許可金鑰的檔案，然後按一下 **Apply**。

CLI

exec license-key *key_num*

訂閱服務的註冊與啓動訂閱

您必須先執行下列作業，Juniper Networks 安全性裝置才能接收防毒 (AV) 模式檔案、「深入檢查」(DI) 簽名、反垃圾郵件或 Web 篩選等一般訂閱服務 :

- 購買訂閱
- 註冊訂閱
- 擷取訂閱金鑰

擷取訂閱許可金鑰可啓動您在裝置上的服務，以所購買的期間爲限。您特定的服務啓動程序取決於您所購買的服務及購買服務的方式。

試用服務

爲了讓您能夠使用 AV、DI、反垃圾郵件或 Web 篩選服務，安全性裝置提供一個試用期間。在此期間中，裝置可以暫時獲得服務。若要從權利伺服器擷取符合條件的試用許可金鑰，請使用 **exec license-key** 更新試用 CLI 指令。

- 出廠時 Juniper Networks 安全性裝置均未啓用 DI。若要獲得試用 DI 服務，您必須啓動 WebUI 會話，並按一下 Configuration > Update > ScreenOS/Keys 頁面中的 **Retrieve Subscriptions Now** 按鈕。此動作將會提供可使用一次，有限使用期爲一天的 DI 金鑰。
- 如果您的裝置在購買時已經有連結 AV 服務，則裝置將擁有預先安裝的試用服務。此試用服務最多可持續 60 天。
- 反垃圾郵件
- 出廠時 Juniper Networks 安全性裝置均未啓用 Web 篩選。此功能不提供試用服務。



警告 : 若要避免服務中斷的情況，您必須在購買訂閱之後儘快註冊 Juniper Networks 安全性裝置。註冊可以訂閱持續進行。

更新訂閱金鑰

若安全性裝置上安裝了具有到期日的任何軟體，則裝置會定期連線至權利伺服器以擷取訂閱金鑰。在下列情況下，裝置會連線至權利伺服器，即 License Management System:

- 金鑰將在兩個月內到期
- 金鑰將在一個月內到期
- 金鑰將在兩週內到期
- 金鑰已到期
- 金鑰到期後 30 天

注意： 若要刪除金鑰檔案中的單一許可金鑰，請使用 **exec license-key delete** *name_str* CLI 指令。

將防毒、Web 篩選、反垃圾郵件及深入檢查新增至現有或新裝置

在購買 AV、Web 篩選、反垃圾郵件或深入檢查 (DI) 訂閱並新增至現有的 Juniper Networks 安全性裝置後，請執行下列步驟以啓動服務。

1. 訂購訂閱後，您應該會收到 Juniper Networks 或您授權的 VAR 以電子郵件提供的一組授權碼。此代碼爲一份可讀文件，內容包含註冊訂閱所需要的資訊。
2. 確定已註冊裝置。如果目前尚未註冊，請至下列網站：

   http://tools.juniper.net/subreg

3. 將訂閱授權碼註冊至裝置。
4. 確認您的裝置有網際網路連接。
5. 擷取裝置的訂閱金鑰。擷取的方式有兩種：
   - 在 WebUI 中，按一下 Configuration > Update > ScreenOS/Keys 頁面中的 **Retrieve Subscriptions Now** 按鈕。
   - 使用 CLI，執行下列指令：

     ```
     exec license-key update
     ```

6. 您必須在載入金鑰後重設裝置。

您現在可以將裝置設定爲自動擷取或手動擷取簽名服務。如需有關爲您的安全性裝置組態這些服務的說明，請參閱下列章節：

- 第 **4-**50 頁上的「片段重組」
- 第 **4-**53 頁上的「防毒掃描」
- 第 **4-**72 頁上的「反垃圾郵件篩選」
- 第 **4-**75 頁上的「Web 篩選」

系統時鐘

永遠將 Juniper Networks 安全性裝置設定在正確的時間是很重要的。裝置上的時間會影響到 VPN 通道的設定以及排程的時機。首先，爲確保裝置能永遠保持正確時間，您必須將系統時間設定爲目前時間。下一步，您可以啓用日光節約時間選項，而且可以組態最多三台 NTP 伺服器 (一台主伺服器以及兩台備份伺服器)，讓裝置可以定期更新其系統時鐘。

日期與時間

若要將時鐘設定爲目前的時間和日期，您可以使用 WebUI 或 CLI。也可以透過 WebUI 使系統時鐘與電腦時鐘同步的方式來完成 :

1. Configuration > Date/Time: 按一下 **Sync Clock with Client** 按鈕。

   彈出的訊息會提示您指定是否已在電腦時鐘上啓用了夏令時間選項。

2. 按一下 **Yes** 以同步化系統時鐘並根據日光節約時間調整，或是按 **No** 以同步化系統時鐘而不根據日光節約時間調整。

透過 CLI，您可以使用指令 "**set clock mm/dd/yyyy hh:mm:ss**" 以手動方式輸入日期與時間，以便設定時鐘。

時區

設定時區時，請指定安全性裝置當地時間早於或晚於 GMT (格林威治標準時間) 的小時數。例如，如果裝置的當地時區是「太平洋標準時間」，就比 GMT 時間晚 8 小時。因此，您必須將時鐘設定爲 **-8**。

如果您使用 WebUI 設定時區 :

Configuration > Date/Time > Set Time Zone_hours_minutes from GMT

如果您使用 CLI 設定時區 :

ns -> set clock timezone *number* (從 -12 到 12 的數字)

或者

ns-> set ntp timezone *number* (從 -12 到 12 的數字)

網路時間通訊協定

若要確保安全性裝置永遠維持正確的時間，可以使用網路時間通訊協定 (NTP) 以同步化系統時鐘與網際網路中 NTP 伺服器的時鐘。您可以用手動的方式來執行這個動作，或是組態裝置依您指定的時間間隔自動執行此同步化。

組態多重 NTP 伺服器

您最多可以在 Juniper Networks 安全性裝置中組態三個 NTP 伺服器 : 一個主要伺服器以及兩個備份伺服器。當您將安全性裝置設定爲自動同步化其系統時鐘，它將會接著查詢每個組態的 NTP 伺服器。裝置永遠會先查詢主要 NTP 伺服器。如果查詢不成功，裝置接著會查詢第一個備份 NTP 伺服器，依此類推，直到獲得來自裝置中其中一個組態 NTP 伺服器的有效回應爲止。裝置在每個 NTP 伺服器上會嘗試四次後才會終止更新並記錄失敗。

當您以手動方式同步化系統時鐘，而您只能夠使用 CLI 執行此動作時，您可以指定一個特殊 NTP 伺服器或完全不指定。如果您指定 NTP 伺服器，安全性裝置將會只查詢該伺服器。如果您沒有指定 NTP 伺服器，裝置接著會查詢在裝置上組態的每個 NTP 伺服器。您可以使用其 IP 位址或其網域名稱指定 NTP 伺服器。

組態備份網路時間通訊協定伺服器

您可以依需要將個別介面指定爲來源位址，以將「網路時間通訊協定」(NTP) 要求透過 VPN 通道從裝置導向至主要 NTP 伺服器或備份伺服器。您可在其他介面類型中選擇一個回傳介面來執行此功能。

安全性裝置會從來源介面傳送 NTP 要求，並在將 NTP 要求傳送至 NTP 伺服器時選擇性使用加密的預先共享金鑰。該金鑰提供驗證。

在下列範例中，藉由指派 IP 位址至各個伺服器來組態主要 NTP 伺服器和兩個備份 NTP 伺服器。接著，將各個伺服器設定爲從 Trust 介面傳送 NTP 要求。之後，爲各個伺服器設定金鑰 ID 和預先共享金鑰。

WebUI

Configuration > Date/Time: 輸入下面的內容，然後按一下 **Apply**:

Primary Server IP/Name: 1.1.1.1
Primary server Key ID: 10
Source Interface: 從清單中選擇 Trust。
Preshared Key: !2005abc
Backup Server1 IP/Name: 1.1.1.2
Primary server Key ID: 10
Source Interface: 從清單中選擇 Trust。
Preshared Key: !2005abc
Backup Server2 IP/Name: 1.1.1.3
Primary server Key ID: 10
Source Interface: 從清單中選擇 Trust。
Preshared Key: !2005abc

CLI

```
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp server src-interface trust
set ntp server backup1 src-interface trust
set ntp server backup2 src-interface trust
set ntp server key-id 10 pre-share-key !2005abc
set ntp server backup1 key-id 10 pre-share-key !2005abc
set ntp server backup2 key-id 10 pre-share-key !2005abc
save
```

最大時間調整

在自動同步化中，您可以指定最大時間調整值 (單位爲秒)。最大時間調整值代表安全性裝置系統時鐘以及從 NTP 伺服器所收到時間之間可接受的時差。如果裝置的時鐘以及 NTP 伺服器時間之間的時差是在您設定的最大時間調整值以內，則裝置只會以 NTP 伺服器時間來調整其時鐘。例如，如果最大時間調整值爲 3 秒，而裝置系統時鐘上的時間爲 4:00:00 而 NTP 伺服器傳送 4:00:02 作爲時間，則兩者之間的時差是可接收的，而裝置也可以更新其時鐘。如果時間調整大於您所設定的值，裝置將不會同步化其時鐘並且會繼續嘗試在裝置中組態的第一個備份 NTP 伺服器。如果裝置在嘗試所有組態 NTP 伺服器之後並沒有收到有效的回覆，它會在事件記錄中產生一個錯誤訊息。此功能的預設值爲 3 秒，而其範圍則爲 0 (無限制) 到 3600 (一小時)。

當您以手動方式同步化系統時鐘，而您只能夠使用 CLI 執行此動作時，安全性裝置並不會確認最大時間調整值。如果裝置收到有效的回覆，它則會顯示一則訊息通知您它所到達的 NTP 伺服器，時間調整爲何，以及使用的驗證方式類型。這個訊息也會要求您確認或取消系統時鐘更新。

如果安全性裝置並沒有收到回覆，它將會顯示一個逾時訊息。只有當裝置未能成功嘗試到達在裝置上組態的所有 NTP 伺服器時，才會出現這個訊息。

注意 : 當您使用 CLI 發出請求時，可以藉由按下鍵盤上的 **Ctrl-C** 鍵來取消目前的請求。

NTP 和 NSRP

「NetScreen 冗餘通訊協定 (NSRP)」包含同步化 NSRP 叢集成員的系統時鐘的機制。雖然同步化的解析只是幾秒鐘的時間，但是 NTP 則擁有子秒的解析。由於每個叢集成員的時間可能因爲處理延遲而有數秒鐘的差異，因此 Juniper Networks 建議當兩個叢集成員皆啓用 NTP 時，應該停用 NSRP 時間同步化，這樣每個成員便都可從 NTP 伺服器更新其系統時鐘。若要停用 NSRP 時間同步化功能，請輸入下列指令 :

```
set ntp no-ha-sync
```

將最大時間調整值設定至 NTP 伺服器

在下列的範例中，您組態了安全性裝置以便從 IP 位址爲 1.1.1.1、1.1.1.2 和 1.1.1.3 的 NTP 伺服器更新其時鐘，以五分鐘爲更新間隔。您也可以設定 2 秒的最大時間調整值。

WebUI

Configuration > Date/Time: 輸入下面的內容，然後按一下 **Apply**:

```
Automatically synchronize with an Internet Time Server (NTP): ( 選擇 )
Update system clock every minutes: 5
Maximum time adjustment seconds: 2
Primary Server IP/Name: 1.1.1.1
Backup Server1 IP/Name: 1.1.1.2
Backup Server2 IP/Name: 1.1.1.3
```

CLI

```
set clock ntp
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp interval 5
set ntp max-adjustment 2
save
```

保護 NTP 伺服器

您可以使用以 MD5 爲基礎的總和檢查，提供 NTP 封包的驗證來確保 NTP 通訊流量的安全。您不需要建立 IPSec 通道。此種驗證類型可確保 NTP 通訊流量的完整性。它無法避免外人可能檢視資料的情況，但是可以避免資料遭到任何人的竄改。

若要啓用 NTP 通訊流量的驗證，您必須將一個唯一的金鑰 ID，以及預先共享的金鑰指派給您在安全性裝置中設定的每個 NTP 伺服器。金鑰 ID，以及預先共享的金鑰是用於建立總和檢查，安全性裝置和 NTP 伺服器可以利用總和檢查來驗證資料。

NTP 通訊流量的驗證類型有兩種 :

- Required
- Preferred

當您選取 **Required** 驗證時，安全性裝置必須將驗證資訊 (金鑰 ID 和總和) 檢查包括在每個它傳送至 NTP 伺服器的封包中，而且必須驗證它從 NTP 伺服器所收到的所有 NTP 封包。在驗證發生於安全性裝置和 NTP 伺服器之間以前，安全性裝置和 NTP 伺服器的管理員必須先交換金鑰 ID 以及預先共享金鑰。他們必須以手動方式進行交換，並且能夠以不同方式進行，例如透過電子郵件或電話。

當您選取 **Preferred** 驗證時，必須嘗試以驗證所有 NTP 通訊流量的方式，先將安全性裝置以 Required 模式操作。如果所有驗證的嘗試皆失敗，安全性裝置接著會以您沒有選取驗證的方式來操作。它會將外傳封包傳送至不包含金鑰 ID 和總和檢查的 NTP 伺服器。實際上，雖然會有偏好的驗證方式，但是如果驗證失敗，安全性裝置仍然會允許 NTP 通訊。

索引

A

ALG
- MS RPC 123
- RTSP 124
- Sun RPC 122
- 用於自訂服務 161

ARP 80
ARP，入口 IP 位址 82
auth 使用者
- WebAuth 164
- 政策前驗證 164
- 執行階段驗證 163
- 執行階段驗證過程 163

C

CLI，set arp always-on-dest 70, 74

D

DHCP 93, 97, 229
- HA 219
- 用戶端 213
- 伺服器 213
- 轉接代理程式 213

DiffServ 166, 190
- *請同時參閱* DS Codepoint 標記

DIP 95, 134-137
- PAT 135, 136
- 固定連接埠 136
- 集區 162
- 集區，修改 137
- 群組 147-149

DNS 205
- 位址，分割 211
- 伺服器 230
- 伺服器，通道 211
- 狀態表 207
- 查詢 206
- 查詢，網域 211

DS Codepoint 標記 184, 190
DSL 225, 229

H

HA
- DHCP 219
- *請參閱* NSRP
- 介面 45
- 介面，虛擬 HA 45

I

ICMP 服務 121
- 訊息代碼 121
- 訊息類型 121

IP 位址
- 介面，追蹤 60
- 公開 52
- 主機 ID 52
- 次要 55
- 次要，路由 55
- 私人 52
- 私人位址範圍 52
- 第 3 層安全區 51-53
- 連接埠，定義 100
- 管理 92
- 網路 ID 52

IP 追蹤
- dynamic 選項 62
- vsys 61
- 介面，支援 61
- 介面，共享 61
- 物件失敗臨界值 62
- 重新路由通訊流量 60-75
- 權重 62

IP 追蹤，失敗
- 入口介面，於 73-75
- 出口介面，於 71-72
- 追蹤的 IP 臨界值 62

IP 集區
- *請參閱* DIP 集區

ISP 211

L

L2TP 政策 162

M

MGT 介面 45
MIP 12
MIP，流向具以介面爲基礎的 NAT 的區域 91
MS RPC ALG，已定義 123

N

NAT 模式 90-94
介面設定 92
流向「不信任」區域的通訊流量 77, 91
NAT-src，路由模式 95
NetInfo 214
NSRP
DHCP 219
DIP 群組 147-149
HA 會話備份 164
NTP 同步化 241
VSI 44
冗餘介面 44
NTP 239-242
NSRP 同步化 241
多重伺服器 239
安全伺服器 242
伺服器 239
最大時間調整 241
驗證類型 242

P

PAT 135

Q

QoS 183

R

RFC
1349，*Type of Service in the Internet Protocol Suite* 166
1918，*Address Allocation for Private Internets* 52
2132，*DHCP Options and BOOTP Vendor Extensions* 218
2326，*Real Time Streaming Protocol (RTSP)* 124, 128
2474，*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* 166
792，*Internet Control Message Protocol* 121
RSH ALG 122
RTSP ALG
已定義 124
公開網域中的伺服器 130
私人網域中的伺服器 129
狀態代碼 127
要求方式 126

S

ScreenOS
功能區 32
全域區域 28
安全區 2, 28
安全區，全域 2
安全區，預先定義 2
封包流動 11-13
政策 3
區域 25-32
通道區 28
虛擬系統 10
綜述 1
ScreenOS 介面
子介面 4
安全區 3
實體 3
SCREEN，MGT 區域 28
Sun RPC ALG
已定義 122
呼叫情況 122

T

trace-route 82

U

URL 篩選
請參閱 Web 篩選

V

VIP 12
VIP，流向具以介面爲基礎的 NAT 的區域 91
VLAN 區域 79
VLAN1
介面 79, 84
區域 79
VLAN，標籤 4
VPN
政策 161
流向有以介面爲基礎的 NAT 的區域 91
通道區 28
VR
簡介 5
轉寄通訊流量區間 5

W

Web 篩選 164
WebAuth，政策前驗證過程 164

三畫

子介面 4
刪除 54
建立 (根系統) 54

四畫

介面
- DIP 134
- HA 45
- HA 功能區 45
- IP 追蹤
  - *請參閱*「IP 追蹤」
- MGT 45
- VLAN1 79
- VSI 44
- 工作中，實體 58
- 工作中，邏輯 58
- 不工作中，實體 58
- 不工作中，邏輯 58
- 介面表，檢視 49
- 冗餘 44
- 以政策爲基礎的 NAT 通道 46
- 功能區 45
- 回傳 56
- 安全區中的實體 43
- 次要 IP 位址 55
- 狀態變更 58
- 修改 53
- 第 3 層安全區 51
- 通道 46, 46-48
- 連接，監控 60
- 連結到區域 51
- 虛擬 HA 45
- 解除連結，區域 51
- 預設值 53
- 實體 3
- 聚集 44
- 編址 51
- 檢視介面表 49

介面，監看 65-70
- 安全區 70
- 迴路 65

公開位址 52

五畫

以政策爲基礎的 NAT，通道介面 46
功能區介面 45
- HA 45
- 管理 45

未知的 unicast 選項 80-84
- ARP 82-84
- trace-route 82
- 氾濫 81

六畫

回傳介面 56
存取政策
- *請參閱*政策

安全區 2
- global 2
- 判斷，目的地區域 12
- 判斷，來源區 11
- 預先定義的 2

安全區，介面 3, 43
- 子介面 44
- 實體 43

次要 IP 位址 55
自訂服務 117
自訂服務，在根系統與 vsys 中 117

七畫

位址
- IP，主機和網路 ID 52
- 已定義 160
- 公開 52
- 在政策中 160
- 私人 52
- 通訊錄項目 100-104

位址否定 178
位址群組 102, 160
- 建立 103
- 項目，移除 104
- 編輯 103
- 選項 102

否定，位址 178
私人位址 52
系統時鐘 239-242
- 日期與時間 239
- 時區 239
- 與用戶端同步 239

系統參數 242

八畫

服務 104
- ICMP 121
- 下拉式清單 104
- 已定義 160
- 在政策中 160
- 逾時臨界值 118

服務群組 132-134
- 刪除 134
- 建立 133
- 修改 133

服務群組 (WebUI) 132
服務簿
- 項目，修改 (CLI) 118
- 項目，移除 (CLI) 118

服務簿，服務
自訂 104
自訂 (CLI) 117
新增 117
預先組態 104
服務，自訂 117
ALG 161
vsys 中 117
金鑰，許可 235

九畫

封包流動 11-13
政策 3
deny 160
DIP 群組 148
global 156, 166, 176
HA 會話備份 164
ID 159
L2TP 162
L2TP 通道 162
NAT-dst 162
NAT-src 162
permit 160
reject 160
VPN 161
VPN 撥接使用者群組 160
內部規則 158
功能 153
必要元素 154
各元件的多重項目 177
名稱 161
安全區 159
位址 160
位址否定 178
位址於 160
位址群組 160
位於最上面 162, 182
服務 160
服務於 104, 160
服務群組 132
服務簿 104
政策內容 177
政策組清單 157
查詢順序 157
計數 165
重新排序 182
根系統 158
停用 181
動作 160
區域內部 156, 166, 174
區域間 155, 166, 167, 170
排程 165
啓用 181
深入檢查 (DI) 162
移除 182
通訊流量記錄 164
通訊流量整理 165
通道 160
最大限制 103
虛擬系統 158
順序 182
管理 166
管理頻寬 183
編輯 181
遮蔽 181
應用程式，明確將服務連結至 161
雙向式 VPN 161
類型 155-156
警示 165
變更 181
驗證 163, 181
訂閱
註冊與啓動 237-238
暫時服務 237

十畫

時區 239
時鐘 , *系統*
請參閱系統時鐘
記錄 164
記錄圖表 165
高可用性
請參閱 HA

十一畫

動態 IP (DIP) 池 137, 162
區域 25-32
global 28
Layer 2 79
VLAN 32, 79
功能，MGT 介面 45
功能，函數 32
全域安全性 2
安全性介面 43
定義 30
通道 28
編輯 31
區域，ScreenOS 25-32
安全性介面 3
預先定義的 2
區域，安全 2, 28
子介面 44
介面，實體 43
介面，監看 70
全域 2
判斷，目的地區域 12
判斷，來源區 11

執行階段驗證 163
排程 150, 165
規則，衍生自政策 158
許可金鑰 235
通訊流量
  計數 165
  記錄 164
  整理 183
  優先順序 166
通訊流量整理 183
  自動 184
  服務優先順序 188
通訊錄
  位址，修改 101
  位址，移除 104
  位址，新增 100
  項目 100
  群組 102
  群組項目，編輯 103
  *請同時參閱*位址
通道介面 46
  以政策爲基礎的 NAT 46
  定義 46
連接埠位址轉譯
  請參閱 PAT
連接埠模式 32
  Combined 36
  DMZ/Dual Untrust 37
  Dual DMZ 38
  Dual Untrust 35
  Home-Work 34
  Trust/Untrust/ DMZ (擴展) 37
  Trust-Untrust 33
  可用性 33
  設定 39
  預設值 33
透明模式 78-89
  ARP/trace-route 80
  unicast 選項 80
  氾濫 80
  阻斷非 ARP 通訊流量 79
  阻斷非 IP 通訊流量 79
  路由 80
  廣播通訊流量 79

十二畫

虛擬 HA 介面 45
虛擬系統 10
虛擬路由器
  請參閱 VR

十三畫

群組
  位址 102
  服務 132
路由模式 95-98
  NAT-src 95
  介面設定 96

十四畫

圖表 , 記錄 165
管理 IP 92
網域名稱系統
  請參閱 DNS
網路遮罩 52, 160
網路，頻寬 183
網際網路服務供應商 (ISP) 211
聚集介面 44

十五畫

標籤，VLAN 4
模式
  Combined 36
  Dual DMZ 38
  Dual Untrust 35
  Home-Work 34
  NAT，流向 Untrust 區域的通訊流量 77
  Trust-Untrust 33
  連接埠 32
  連接埠模式可用性 33
  透明 78

十六畫

頻寬 165
  保證的 165, 183, 189
  最大值，無限制 184
  最大，最高 165, 183, 189
  管理 183
頻寬優先順序
  佇列 188
  預設值 188
  層級 188

十七畫

優先順序佇列 188
應用程式選項，政策中 161

二十畫

警示，臨界值 165

二十三畫

驗證
  Allow Any 164
  使用者 163
  政策 163