

使用ASDM為ASA上的特定流量配置連線超時

目錄

[簡介](#)

- [需求](#)
- [採用元件](#)
- [預設值](#)

[設定連線逾時](#)

- [ASDM](#)
- [ASA CLI](#)

[驗證](#)

[參考資料](#)

簡介

本文檔介紹為特定應用協定（如HTTP、HTTPS、FTP或任何其他協定）配置ASA和ASDM上的連線超時。Connection timeout是指在防火牆或網路裝置終止空閒連線以釋放資源並提高安全性之前處於非活動狀態的時間。首先，第一個問題是：此配置的要求是什麼？如果應用具有正確的TCP keepalive設定，則通常不需要在防火牆上配置連線超時。但是，如果應用缺乏適當的Keepalive設定或超時配置，在這種情況下，在防火牆上配置連線超時對於管理資源、增強安全性、提高網路效能、確保合規性和最佳化使用者體驗至關重要。

需求

思科建議您瞭解以下主題：

- [存取控制清單\(ACL\)](#)
- [服務策略](#)
- [連線超時](#)


採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 9.17(1)
- ASDM 7.17(1)

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

預設值

 注意：預設逾時

預設的embryonic超時為30秒。

預設的half-closed空閒超時為10分鐘。

預設dcd max_retries值為5。

預設dcd retry_interval值為15秒。

預設tcp空閒超時為1小時。

預設值為2分鐘的udp空閒超時。

預設icmp空閒超時為2秒。

預設sip空閒超時為30分鐘。

預設sip_media空閒超時為2分鐘。

預設的esp和ha空閒超時為30秒。

對於所有其他協定，預設空閒超時為2分鐘。

若要永不逾時，請輸入0:0 : 0。

設定連線逾時

ASDM

如果特定流量具有連線表，則該流量具有特定的空閒超時；例如，在本文中，我們將更改DNS流量的連線超時。

考慮到此流量的網路圖，下面有許多選項可用於為特定流量配置連線超時：

Client ----- [Interface : MNG] Firewall [Interface : OUT] ----- Server

也可以為介面分配ACL。

第1步：建立ACL

我們可以指定來源、目的地或服務

ASDM > Configuration > Firewall > Advanced > ACL Manager

Dialog box titled "Edit ACE" showing configuration options:

- Action: Permit Deny
- Source Criteria:
 - Source: any
 - User:
 - Security Group:
- Destination Criteria:
 - Destination: any
 - Security Group:
 - Service: udp/domain
- Description:
- Enable Logging
- Logging Level: Default
- More Options

Buttons: Help, Cancel, OK

第2步：建立服務策略規則

如果您已經擁有ACL，可以跳過最後一個步驟，也可以將其中一個引數（源、目標或服務）分配給服務策略到介面。

ASDM > Configuration > Firewall > Service Policy rules

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Global - applies to all interfaces

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

第3步：建立流量類

可以選擇源和目標IP地址（使用ACL）

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP or SCTP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.


< Back Next > Cancel Help

第4步：分配ACL


在此步驟中，您可以指定現有的ACL或選取相符條件（來源、目的地或服務）


Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address


Action: Match Do not match

Existing ACL: ExistingACL 


Source Criteria


Source: 


User: 

Security Group: 

Destination Criteria

Destination: 

Security Group: 

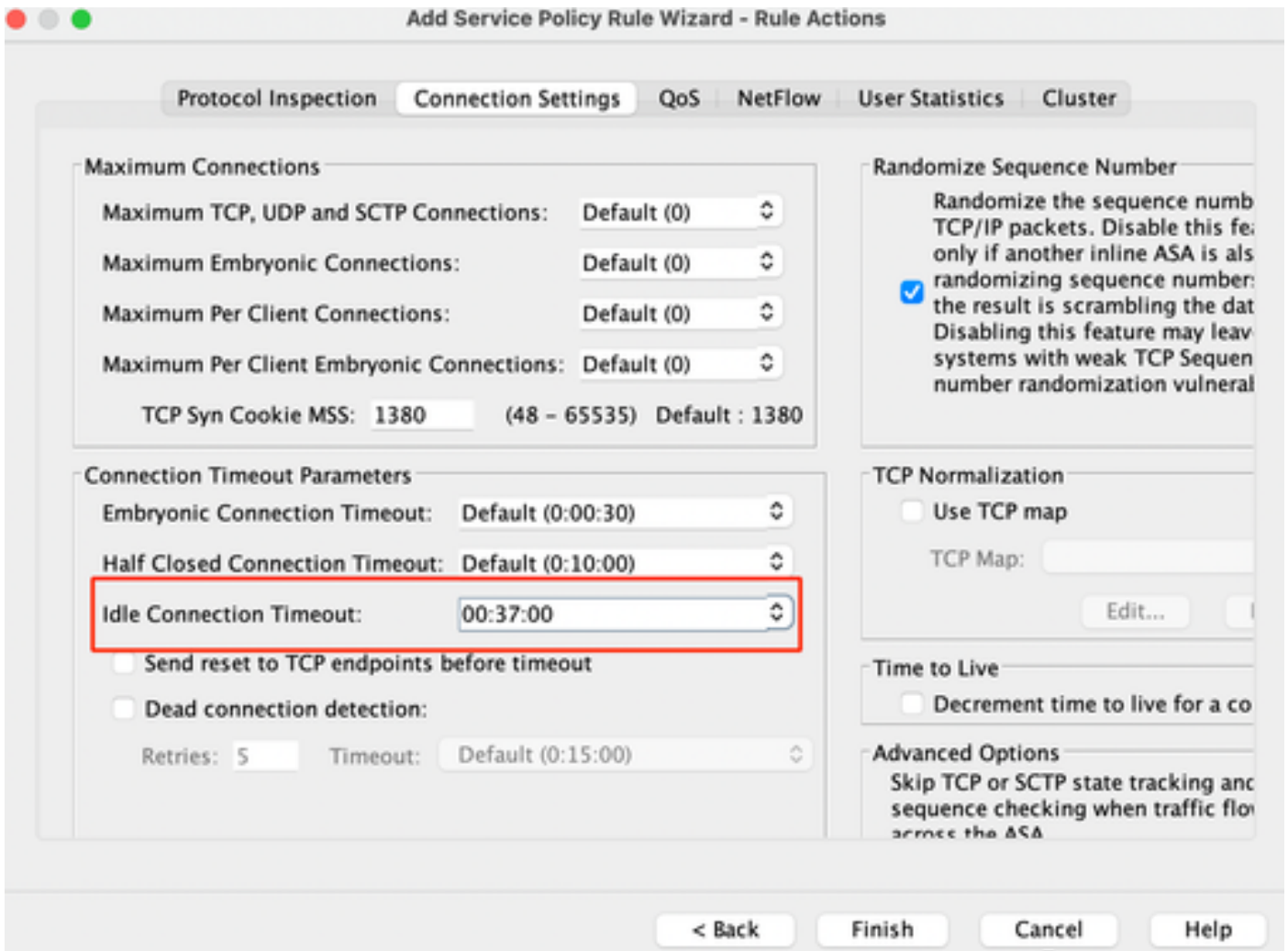
Service: 

Description:

More Options

步驟5：配置空閒超時引數

根據有效格式HH：MM：SS配置空閒超時。



清除該特定流量的連線：

```
#clear conn address 輸入IP地址或IP地址範圍
#clear conn protocol 輸入此關鍵字以僅清除SCP/TCP/UDP連線
```

ASA CLI

您可以透過CLI配置所有這些設定：

```
ACL :
access-list DNS_TIMEOUT extended permit udp any any eq domain

類對映：
class-map MNG-class
match access-list DNS_TIMEOUT


策略對映：
```

```
policy-map MNG-policy
類MNG-class
set connection timeout idle 0:37:00
```

在介面上應用策略對映：

```
service-policy MNG-policy interface MNG
```

驗證

 提示：如果運行此命令，可確認DNS流量的連線超時：

ASA CLI > enable mode > show conn long

示例：show conn long address 192.168.1.1

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53)輸出 : 10.10.10.30/63327 (10.10.10.30/63327) , 標  
誌- , 空閒17秒 , 正常運行時間17秒 , 超時2m0秒 , 位元組36
```

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53)輸出 : 10.10.10.30/62558 (10.10.10.30/62558) , 標  
誌- , 空閒40秒 , 正常運行時間40秒 , 超時2m0秒 , 位元組36
```

然後，在配置之後，我們可以確認空閒超時配置：

示例：show conn long address 192.168.1.1

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53)輸出 : 10.10.10.30/63044 (10.10.10.30/63044) , 標  
誌- , 空閒8秒 , 正常運行時間8秒 , 超時37m0秒 , 位元組37
```

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53)輸出 : 10.10.10.30/63589 (10.10.10.30/63589) , 標  
誌- , 空閒5秒 , 正常運行時間5秒 , 超時37m0秒 , 位元組41
```

參考資料

[什麼是連線設定](#)

關於此翻譯

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