TANet DDoS 攻擊防護方式

麟瑞科技股份有限公司

技術服務處　資深工程師

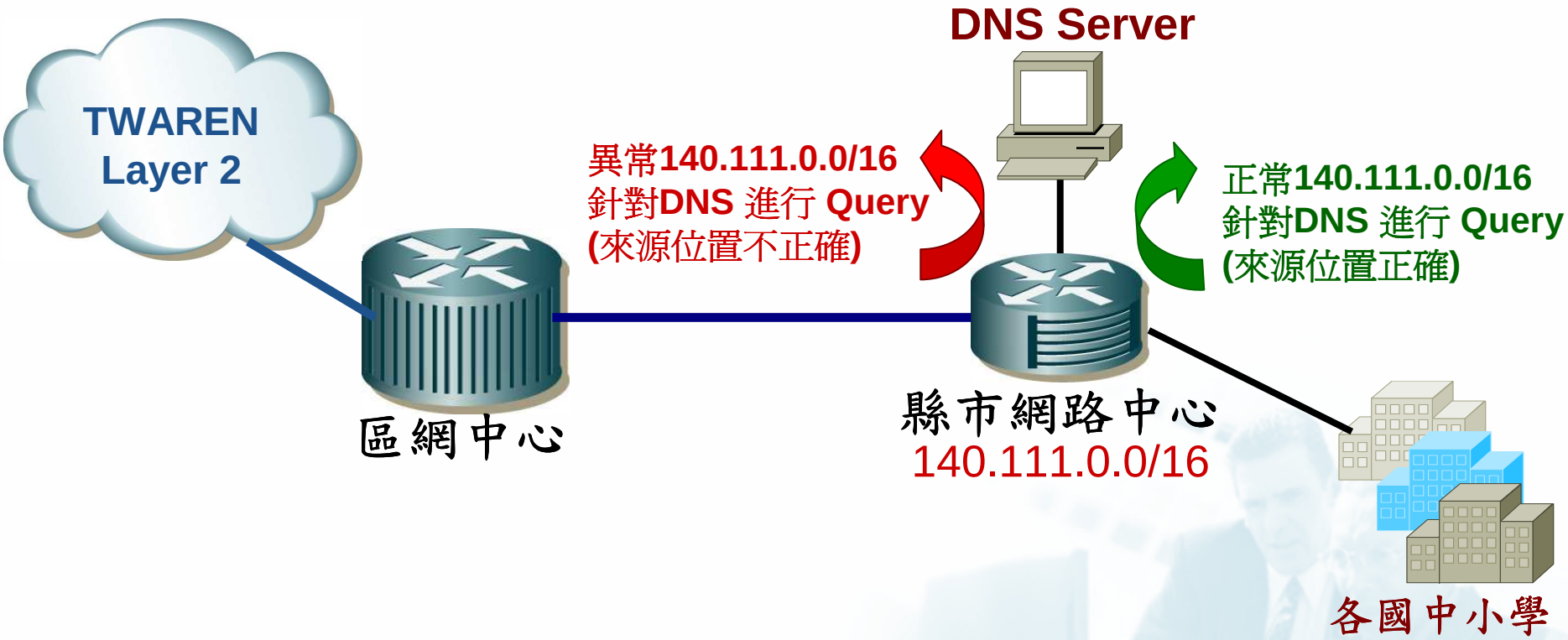
王光宜

麟瑞科技 RING LINE CORPORATION

縣市網路中心防護方式

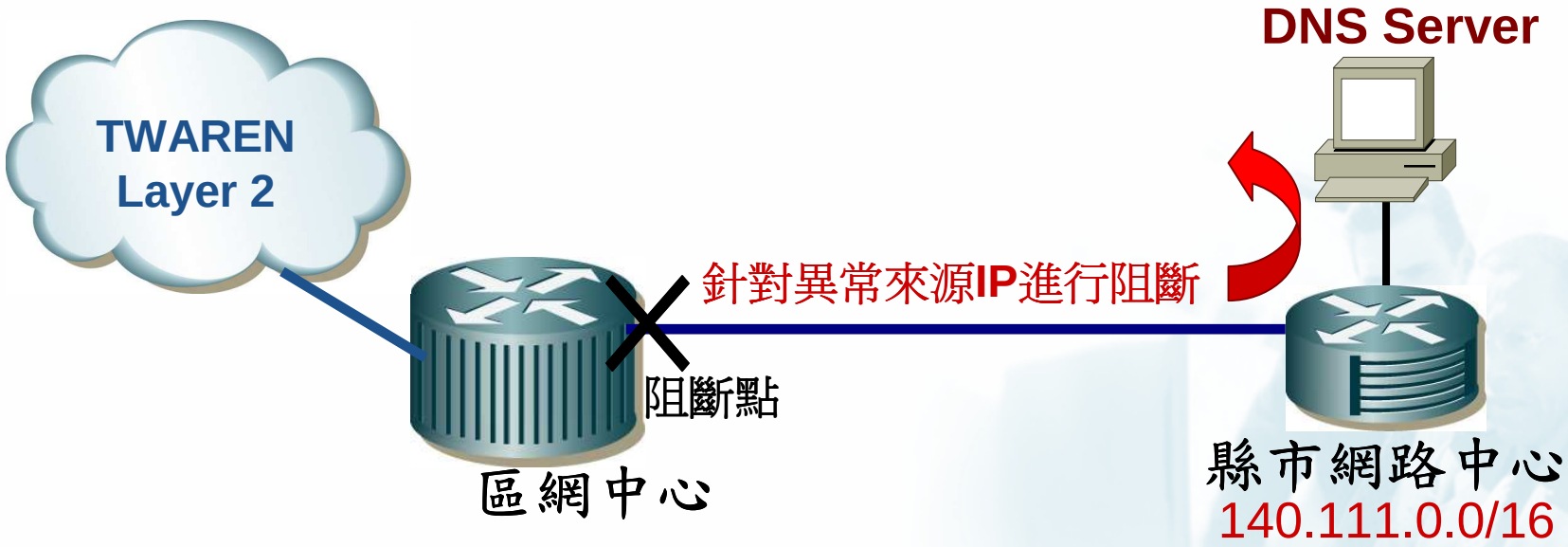
TANet DDoS 攻擊防護

假冒 IP 攻擊



- 縣市網路中心網段為：140.111.0.0/16。
- 在縣網端發現大量來自區網，而來源IP為縣市網網段，針對縣市網DNS進行Query動作。

在區網端設定阻斷點


DNS Server
TWAREN
Layer 2
針對異常來源IP進行阻斷
阻斷點
區網中心
縣市網路中心
140.111.0.0/16

TANet DDoS 攻擊防護

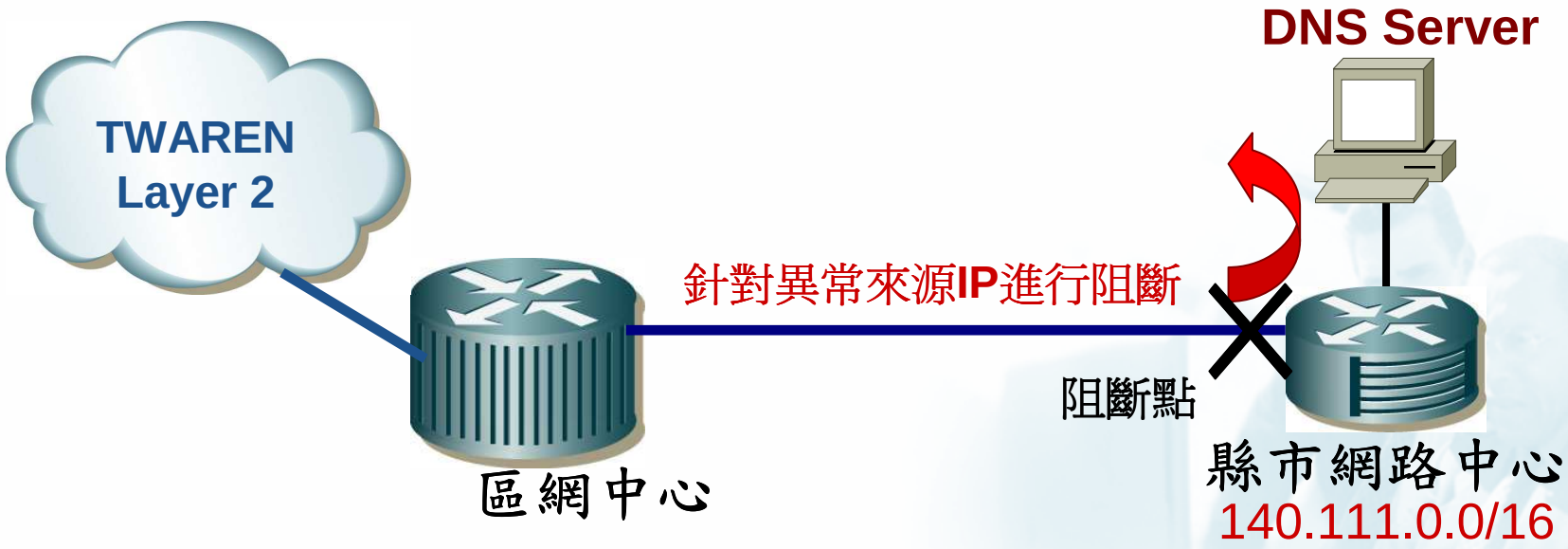
在區網端設定阻斷點


```
ip access-list extended DEMO
  deny ip 140.111.0.0 0.0.255.255 any
  permit ip any any

Interface vlan 11
  ip access-group DEMO out

Interface vlan 21
  ip access-group DEMO out

Interface vlan 31
  ip access-group DEMO out
```

1. 紅字部份可依實際狀況調整。
2. 若區網連接多個縣市網，可將所屬縣市網的網段一併納入防護 **ACL** 中。

TANet DDoS 攻擊防護

在縣市網端設定阻斷點



TANet DDoS 攻擊防護

在縣市網端設定阻斷點

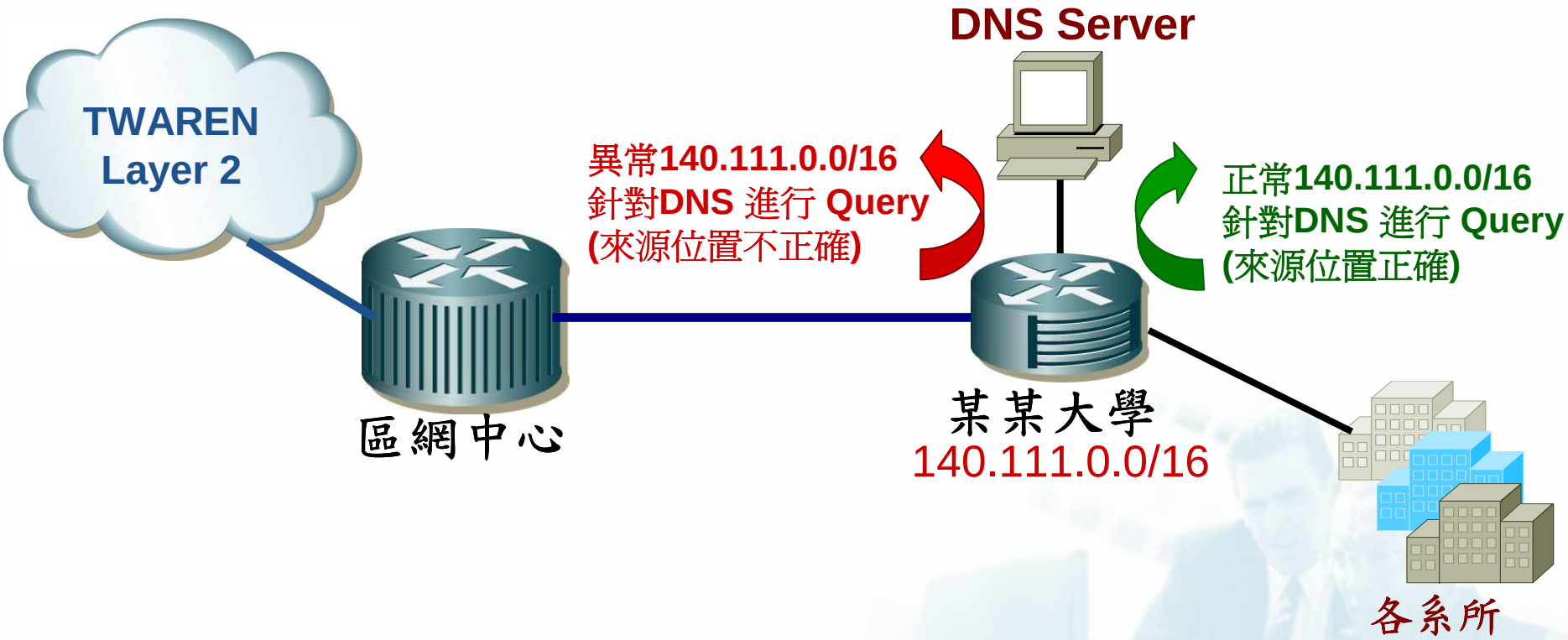
1. 紅字部份可依實際狀況調整。

```
ip access-list extended DEMO
  deny ip 140.111.0.0 0.0.255.255 any
  permit ip any any

Interface vlan 11
  ip access-group DEMO in

Interface vlan 21
  ip access-group DEMO in

Interface vlan 31
  ip access-group DEMO in
```

其他連線單位防護方式

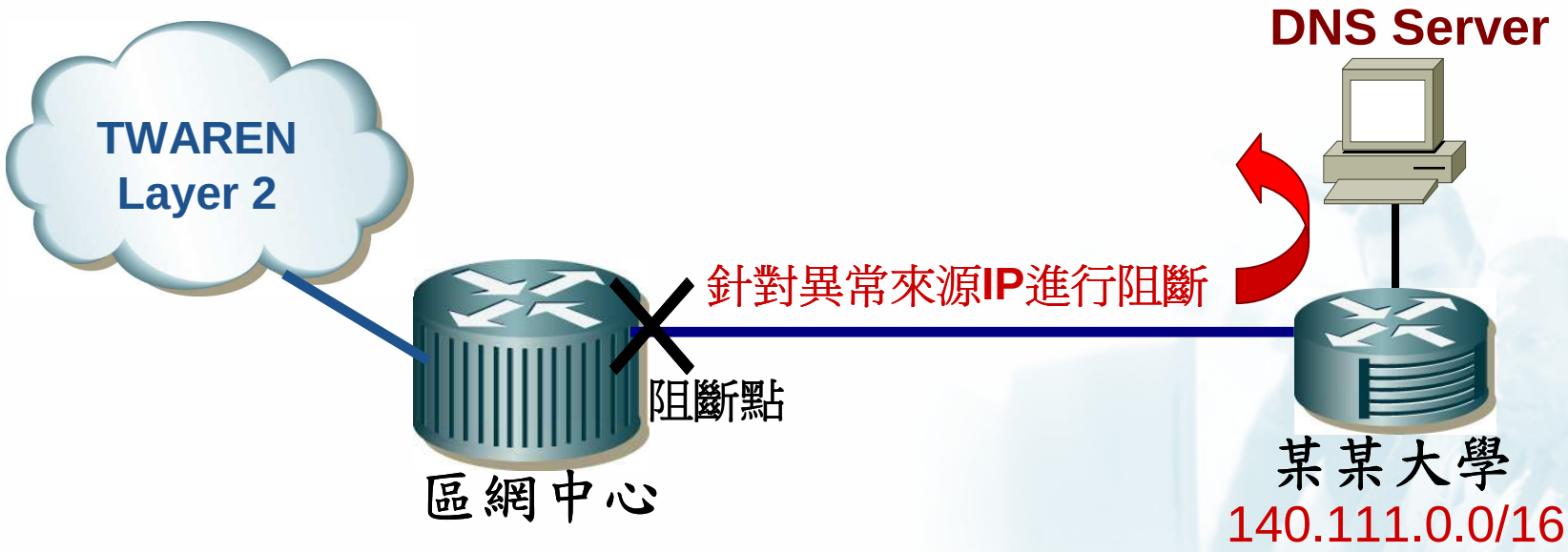
TANet DDoS 攻擊防護

假冒 IP 攻擊



- 某大學網段為：140.111.0.0/16。
- 發現大量來自區網，而來源IP為該大學網段，針對縣市網DNS進行大量Query動作。

在區網端設定阻斷點


DNS Server
TWAREN
Layer 2
針對異常來源IP進行阻斷
阻斷點
區網中心
某某大學
140.111.0.0/16

TANet DDoS 攻擊防護

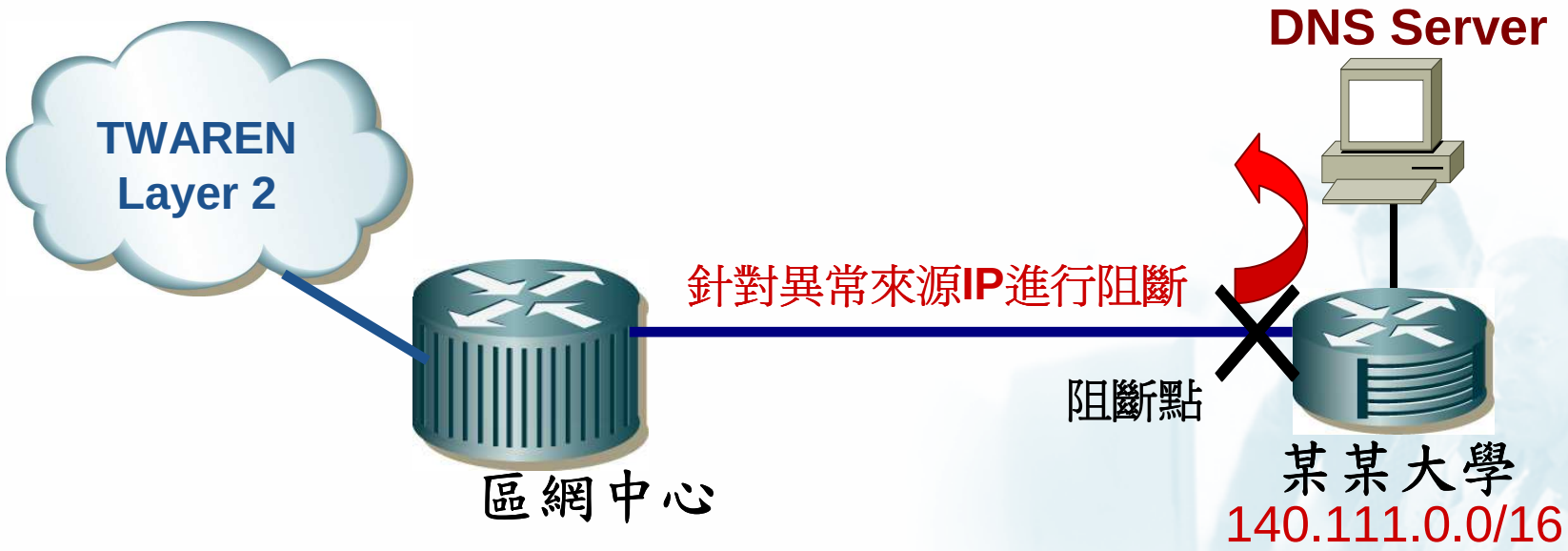
在區網端設定阻斷點


```
ip access-list extended DEMO
  deny ip 140.111.0.0 0.0.255.255 any
  permit ip any any

Interface Gigaethernet
  ip access-group DEMO in
```

1. 紅字部份可依實際狀況調整。
2. 對點IP設在實體介面上方可使用該設定方法。
3. 若對點IP設在Vlan介面上，請參照縣市網設定方法。

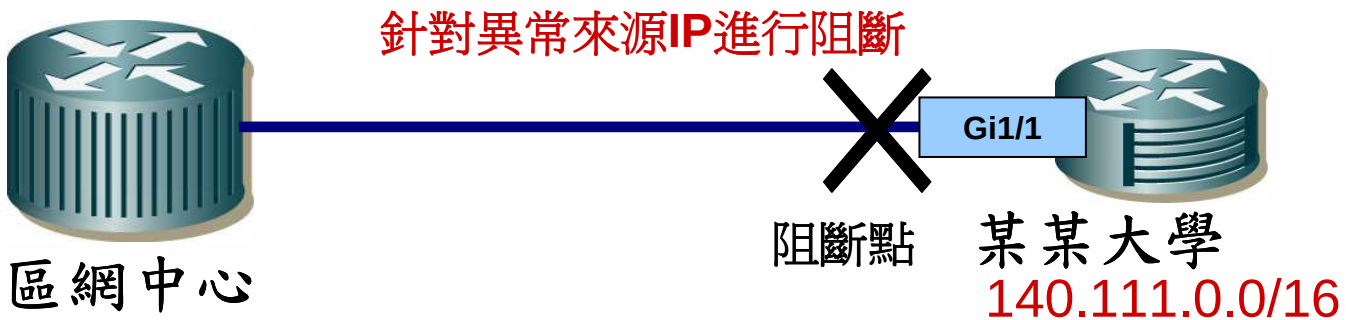
TANet DDoS 攻擊防護

在連線單位端設定阻斷點



TANet DDoS 攻擊防護

在連線單位端設定阻斷點




```
ip access-list extended DEMO
  deny ip 140.111.0.0 0.0.255.255 any
  permit ip any any

Interface Gigaethernet
  ip access-group DEMO out
```

1. 紅字部份可依實際狀況調整。
2. 對點IP設在實體介面上方可使用該設定方法。
3. 若對點IP設在Vlan介面上，請參照縣市網設定方法。

注意事項

- 目前該方案只能針對假冒內部IP做防護
- 大量的ACL設定會增加骨幹路由器Loading
- 實體介面以及Vlan介面ACL設定上需注意
- 該方案除DNS外，其他服務也有防護作用

補充資料

Cisco設備CPU使用狀況查詢指令

show processes cpu

```
CPU utilization for five seconds: 8%/3%; one minute: 6%; five minutes: 6%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1          48       239        200  0.00%  0.00%  0.00%   0 Chunk Manager
   2       38004   3969763          9  0.00%  0.00%  0.00%   0 Load Meter
   3       24652    203019        121  0.00%  0.00%  0.00%   0 Collection proce
   4           0        48          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0         6          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6           0         1          0  0.00%  0.00%  0.00%   0 PF Redun ICC Req
   7           0         1          0  0.00%  0.00%  0.00%   0 PF Redun ICC Req
   8    82239952   4278902      19219  2.87%  0.54%  0.40%   0 Check heaps
   9        4796      4241       1130  0.00%  0.00%  0.00%   0 Pool Manager
  10           0         2          0  0.00%  0.00%  0.00%   0 Timers
```

若有相關網管偵測主機，可針對CPU進行效能統計

Cisco CPU OID：.1.3.6.1.4.1.9.2.1.58.0