

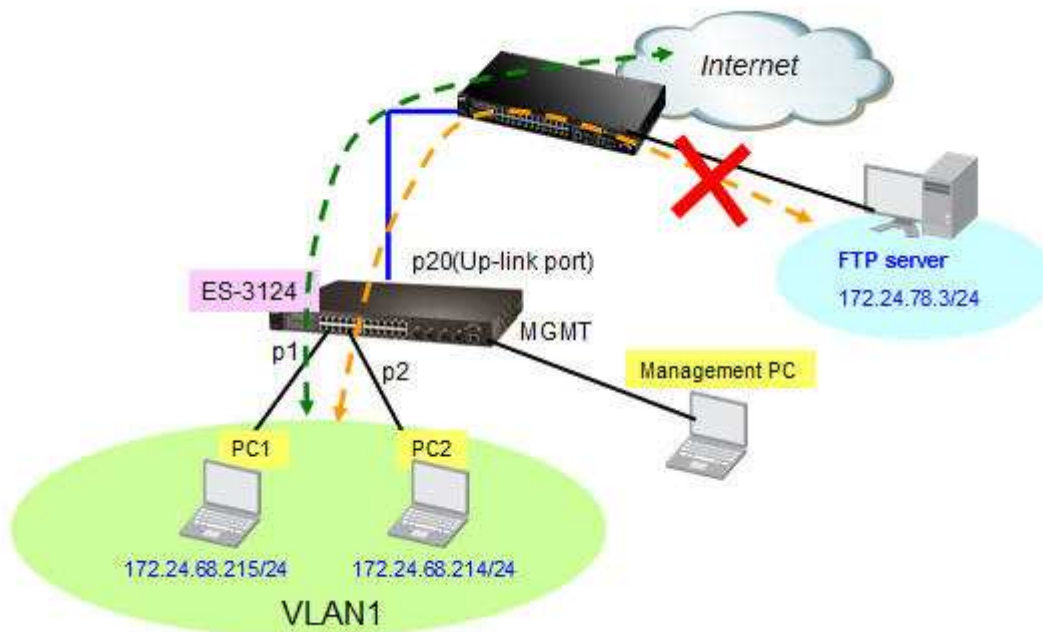
如何利用 ACL 功能(Classifier & Policy Rule)

管控內部電腦存取某 FTP Server 服務

需求說明：

一般員工電腦可連出至外部網路，但都無法使用內部某特定 FTP Server 服務。

範例架構拓撲圖：



交換器設定說明：

1. 首先，請將管理者電腦與 switch 介接，舉例設定 switch 管理用的 IP 位址 172.24.68.200。
2. 架設如上網路範例架構，並登入 switch 的 Web GUI 管理介面。

3. 切換至 Advance Application > Classifier 頁面, 新增一筆 ftp service 的 Classifier 服務, 並在 layer 3 Destination 欄位, 輸入您計劃不開放存取的 FTP Server IP 位址及 access port

Classifier

Active:

Name: ftp service

Packet Format: All

VLAN: Any

Priority: Any

Layer 2 Ethernet Type: IP

Source MAC Address: Any

Port: Any

Destination MAC Address: Any

DSCP: Any

Layer 3 IP Protocol: TCP

Source IP Address / Address Prefix: 0.0.0.0 /

Socket Number: Any

Destination IP Address / Address Prefix: 172.24.78.3 / 24

Socket Number: Any

21

Add Cancel Clear

4. 切換至 Advance Application > Policy Rule 頁面, 新增一筆 block ftp 的 Policy Rule。

Policy

Active	<input checked="" type="checkbox"/>																														
Name	block ftp																														
Classifier(s)	ftpservice																														
Parameters	<table border="0"> <tr> <td>VLAN ID</td> <td>1</td> <td>Bandwidth</td> <td>0</td> <td>Kbps</td> </tr> <tr> <td>Egress Port</td> <td>1</td> <td>Out-of-Profile DSCP</td> <td>0</td> <td></td> </tr> <tr> <td>Outgoing packet format for Egress port</td> <td colspan="4"><input checked="" type="radio"/> Tag <input type="radio"/> Untag</td> </tr> <tr> <td>Priority</td> <td>0</td> <td colspan="3"></td> </tr> <tr> <td>DSCP</td> <td>0</td> <td colspan="3"></td> </tr> <tr> <td>TOS</td> <td>0</td> <td colspan="3"></td> </tr> </table>	VLAN ID	1	Bandwidth	0	Kbps	Egress Port	1	Out-of-Profile DSCP	0		Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag				Priority	0				DSCP	0				TOS	0			
	VLAN ID	1	Bandwidth	0	Kbps																										
	Egress Port	1	Out-of-Profile DSCP	0																											
	Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag																													
	Priority	0																													
	DSCP	0																													
	TOS	0																													
Forwarding	<input type="radio"/> No change <input checked="" type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping																														

Action	Priority	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1 priority <input type="radio"/> Send the packet to priority queue <input type="radio"/> Replace the 802.1 priority field with the IP TOS value
	Diffserv	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Replace the IP TOS field with the 802.1 priority value <input type="radio"/> Set the Diffserv Codepoint field in the frame
	Outgoing	<input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port <input type="checkbox"/> Set the packet's VLAN ID

Metering	<input type="checkbox"/> Enable	
	Out-of-profile action	<input type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value <input type="checkbox"/> Set Out-Drop Precedence <input type="checkbox"/> Do not drop the matching frame previously marked for dropping

Add Cancel Clear

5. 設定完成後，使用內部電腦開啟 window DOS 視窗輸入 ftp 172.24.78.3。結果因為被阻檔原因顯示將為連線已等候逾時(unknown error number)。

```

C:\Windows\system32\cmd.exe
C:\Users\Jones>ftp 172.24.78.3
> ftp: connect : 連線已等候逾時
ftp> bye
  
```

End of the Document