

題目	【網路控制措施】 (1)與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以符合一致性與單一性之安全要求。 (2)宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。
辦理方式	1. 本校與外界的網路連線，是使用教育局所配發之網段與外網相連。 2. 檢附本校網路邏輯架構及業務與網段對應資料。
佐證資料	本校實體網路對應資料 1.由機房網路拓模圖，本校網路連線全部透過教育局配發之 210.243.8.X/24 網段與外網連接，並無使用其他 ISP 所提供之電線線路。 2.本校依電腦用途區分為各網路區域，防火牆上使用不同介接孔，由於本校骨幹連接，未避免區域之間的混用，於是於骨幹交換器上切虛擬 VLAN，用以區分各區域用途之電腦。

本校防火牆 Fortinet 200D 區域對應資料

1. 本校內部網路於防火牆區分為 DMZ、LAN、WIFI、CLASS 等區域。
2. DMZ 區域放置伺服器，於防火牆上屬於 dmz 群組，所有群組均可存取 DMZ，網路區域為 192.168.108.X/24。
3. WIFI 區域為無線網路基地台所在區域，於防火牆上屬於 LAN2 群組，該群組無法存取行政與教師電腦所在之 LAN 群組，網路網域為 192.168.254.X/24。
4. LAN 區域為行政與教師電腦所使用之區域，於防火牆屬於 LAN 群組，該群組無法被其他群組所存取，網路網域為 10.108.X.X/16。
5. CLASS 為班級教室所使用區域，於防火牆屬於 LAN5 群組，該群組無法存取行政與教師電腦所在之 LAN 群組，網路網域為 172.16.X.X/16。

FORTINET FortiGate 200D

Video Help Logout

防火牆網域配置設定

System

- Dashboard
 - Status
- FortiView
 - Sources
 - Applications
 - Cloud Applications
 - Destinations
 - Web Sites
 - Threats
 - All Sessions
 - System Events
 - Admin Logins
 - VPN
- Network
 - Interfaces**
 - Routing
 - DNS
 - Packet Capture
- Config
- Admin
- Monitor

Policy & Objects

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

FortiGate 200D

WAN1 1 3 5 7 9 11 13 15 DMZ1

MGMT 2 4 6 8 10 12 14 16 DMZ2

WAN2 2 4 6 8 10 12 14 16 DMZ2

View

Group by Type ON

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (5)						
dmz1			10.10.10.1 255.255.255.0	Physical	PING HTTPS HTTP FMG-Access CAPWAP	0
dmz2			0.0.0.0 0.0.0.0	Physical	PING FMG-Access CAPWAP	0
mgmt			192.168.1.99 255.255.255.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	1
port15			0.0.0.0 0.0.0.0	Physical		0
port16			0.0.0.0 0.0.0.0	Physical		0
VLAN Switch (1)						
lan	(VLAN ID: 0)		192.168.100.99 255.255.255.0	VLAN Switch (9)	PING HTTPS HTTP FMG-Access CAPWAP	1
Zone (14)						
LAN1				Zone		27
port1			10.108.0.254 255.255.0.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	2
LAN2				Zone		13
port2 (Cisco Wireless)			192.168.254.1 255.255.255.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	3
LAN3				Zone		2
port3			192.168.3.254 255.255.255.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	1
LAN4				Zone		1
port4			192.168.4.254 255.255.255.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	1
LAN5				Zone		5
port5			172.16.0.254 255.255.0.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	2
dmz				Zone		35
wan2			192.168.108.254 255.255.255.0	Physical	PING HTTPS SSH SNMP HTTP FMG-Access	1
untrust				Zone		27