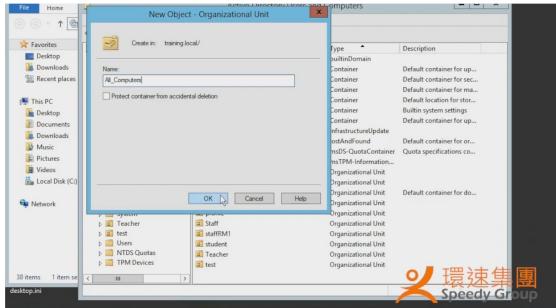
有關 WannaCry 及日後對本港學校具威脅的科技風險資訊分享 環速學校 IT 支援服務已在 Facebook (www.facebook.com/SpeedyGroupHK) 發佈供本港學校的最新技術訊息,分享學校防範 WannaCry 之實用建議、技術支援資訊及影片,請密切留意。



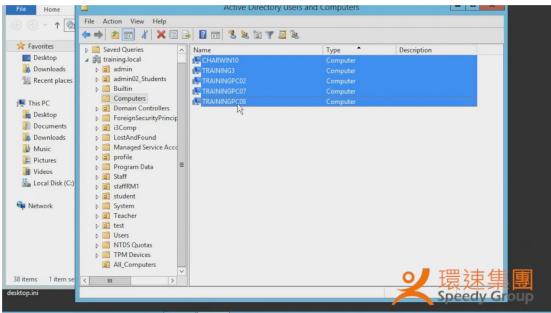
群組原則 (Group Policy) - 封鎖網域電腦 SMB 連接埠

注意:以下教學以 Windows Server 2012 R2 網域控制器為例,請注意 Windows XP 用戶不能經以下教 學封鎖 SMB 連接埠, BYOD 用戶亦不適用 (*由於各校網域環境情況不同 ,以下教學只供參考之用*)

1. 於 "Active Directory Users and Computers"内,新增一個名為 "All_Computers" (名稱可自行定義) 的 "Organization Unit";



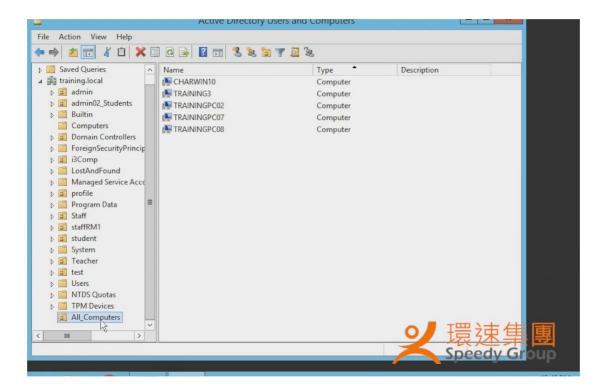
2. 把所有使用者電腦拖延至剛才新建立的 "All_Computers" 内; (*請勿把有伺服器功能的電腦一起遷移*)











3. 於 "Group Policy Management" 內 , 新增一個名為"BlockWannaCryPort" (名稱可自行定義) 的群組 原則物件

• •	Training-DC		
	Group Policy Management		_ 0 X
🔜 File Action View Window Help (====================================	9	環速	集團
Group Policy Management Group Policy Management Gross: Constant Forest: training.local Group Default Domain Policy Constant Domain Policy Constant Domain Policy Constant Constant Consta	BlockWannaCryPort Scope Details Settings Delegation Links Display links in this location: training loca The following sites, domains, and OUs are linked to	al a	√ Group ↓
 admin02_Students ▲ all_Computers ▲ BlockWannaCrytert ₩SUS ▲ Domain Controllers ▲ i3Comp 	Location Al_Computers	Enforced No	Link Enabled Yes
 i3Comp ia profile ia staff ia staffRM1 ia student ia Teacher ia test 	Security Filtering The settings in this GPO can only apply to the follow Name & Authenticated Users	wing groups, use	ers, and computers:
Group Policy Objects	< III		>
▷ IIII WMI Filters ▷ IIIII Starter GPOs	Add Remove	Properties	
 Figure Sites Group Policy Modeling Group Policy Results 	WMI Filtering This GPO is linked to the following WMI filter: (none>)	~	Open
= 占 🛛 🚞 🕥		Re 17 46	ENG 2:04 PM 16/5/17







4. [強制電腦防火牆開啟]

修改"BlockWannaCryPort"內的防火牆設置: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security

設置如下:

Domain Profile: Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections Allow (default)

Private Profile:

Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections Allow (default)

Public Profile:

Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections Allow (default)

	Training-DC
<u>.</u>	Group Policy Management Editor
File Action View Help	の上理法住国
🗢 🄿 🙍 📰 🚺	Windows Firewall with Advanced Security - LDAP://C × 农 本 完 巨
 ▷ ○ Software Settings △ ○ Windows Settings ▷ ○ Name Resolut ○ Scripts (Startu ▷ ○ Deployed Prin △ ○ Security Settir ▷ ○ Account P ▷ ○ Event Log ▷ ○ Restricted ▷ ○ System Se ■ ▷ ○ Restricted ▷ ○ File System ▷ ○ File System ▷ ○ Wired Net 	Domain Profile Private Profile Public Profile IPsec Settings Indows computers. Specify behavior for when a computer is connected to its corporate domain. State Indows computers. Indows computers. State On (recommended) Inbound connections: Block (default) Image: Display the private pri
 ↓ Windows I ↓ Windo ↓ Network L ↓ Wireless N ↓ Public Key ↓ Software F ↓ Network A ↓ Applicatio ↓ P Security 	Logging Specify logging settings for troubleshooting. Customize OK Cancel Apply
< III >	
	🚔 📀 📴 🛃 🧾 🔹 🕞 2:04 PM 16/5/17

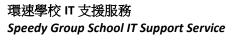






• • •	Training-DC	
J	Group Policy Management Editor	_ 🗆 X
File Action View Help		四法住国
🗢 🔿 🙍 🖬 🚺 🖬	Windows Firewall with Advanced Security - LDAP://	限述 乐园
Software Settings A	Domain Profile Private Profile Public Profile IPsec Settings	peccay croup
⊿ Image: A setting windows Setting ▷ Image: A setting Name Resolut	Specify behavior for when a computer is connected to a private	Indows computers.
🚊 Scripts (Startu	network location.	
 Deployed Prin Security Settir 	Firewall state: On (recommended)	
Security Setting B Account P	Inbound connections: Block (default)	
b Local Polic	Outbound connections: Allow (default)	
Event Log Restricted		=
▷ → System Se ≡		
D 🔂 Registry	Settings Specify settings that control Windows	
▷ 📴 File Systen ▷ 🔯 Wired Net	Firewall behavior.	
🔺 🧮 Windows I	Lucia -	
Windo Network L	Logging Specify logging settings for Customize	
Wireless N	troubleshooting.	
Public Key		computers are authenticated and
Software F Metwork A		
Applicatio		
▷ 🐻 IP Security ► 🦳 Advanced	OK Cancel Apply	~
	II €	>
	🗎 👩 📰 🛃 🚺 🔹	R R ENG 2:04 PM
	Training DC	16/5/17
•••	Training-DC	
	Training-DC Group Policy Management Editor	
File Action View Help	Group Policy Management Editor	
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP://c	
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP://C	
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP://c	- □ × 環速集團 Speedy Group
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP://c × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State	- □ × 環速集團 Speedy Group
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended)	- □ × 環速集團 Speedy Group
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:///C Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default)	- □ × 環速集團 Speedy Group
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended)	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP://c Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default)	- □ × 環速集團 Speedy Group
File Action View Help 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) × Outbound connections: Allow (default) × Settings	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:///C Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default)	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help Image: Software Settings Image: Software Settings Image: Software Settings Image: Image: Software Settings Image: Software Settings Image: Software Settings Image: Image: Image: Software Settings Image: Software Settings Image: Software Settings Image: Image: Image: Image: Image: Image: Software Settings Image: I	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Settings Specify settings that control Windows Outbound	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help Software Settings Windows Settings Scripts (Startu Scripts (Startu Scripts (Startu Security Settin Security Settin Local Polic Event Log Restricted System Se Registry Registry File Systen Windows 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Specify settings that control Windows Firewall behavior. Logging	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help Software Settings Windows Settings Scripts (Startu Scripts (Startu Scripts (Startu Security Settin Security Settin Security Settin Local Polis Event Log System Se Registry Registry Registry Windows Windows Windows Windows Windows Windows Windows Windows Windows Network L 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Specify settings that control Windows Firewall behavior.	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help Software Settings Windows Settings Scripts (Startu Scripts (Startu Scripts (Startu Security Settin Security Settin Local Polic Event Log Restricted System Se Registry Registry File Systen Windows 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Settings Specify settings that control Windows Firewall behavior. Logging Specify logging settings for Customize	- □ × 表生集団 Speedy Group Indows computers.
File Action View Help Software Settings Windows Settings Name Resolut Scripts (Startu Exert Log Security Settir Account P Event Log Restricted System Se Registry Registry Registry Windows Windows Windows Windows Windows Windows Public Key Software F	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Settings Specify settings that control Windows Firewall behavior. Logging Specify logging settings for Customize	□ × 定ま集団 Speedy Group indows computers.
File Action View Help Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Settings Specify settings that control Windows Firewall behavior. Logging Specify logging settings for Customize	□ × 定ま集団 Speedy Group indows computers.
File Action View Help Software Settings Windows Settings Scripts (Startu Scripts (Startu Scripts (Startu Security Setting Security Setting Security Setting Coal Polic Event Log Event Log Restricted System Set Windows I Windows I Windows I Windows I Software F Network A Software F Network A Software F Network A Software F 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Firewall state: On (recommended) Inbound connections: Block (default) Outbound connections: Allow (default) Settings Settings Specify settings that control Windows Firewall behavior. Logging Specify logging settings for Customize	□ × 天子中の中での中では、 Indows computers.
File Action View Help Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Settings Image: Software Setings Image: Software Settings <td>Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Infound connections: Block (default) State On (recommended) v Inbound connections: Block (default) v Outbound connections: Allow (default) v Settings Specify settings that control Windows Customize Logging Specify logging settings for roubleshooting. Customize</td> <td>□ × 定ま集団 Speedy Group indows computers.</td>	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Infound connections: Block (default) State On (recommended) v Inbound connections: Block (default) v Outbound connections: Allow (default) v Settings Specify settings that control Windows Customize Logging Specify logging settings for roubleshooting. Customize	□ × 定ま集団 Speedy Group indows computers.
File Action View Help Software Settings Windows Settings Name Resolut Scripts (Startu Scripts (Startu Scripts (Startu Scripts (Startu Event Log Local Polic System Se Registry Registry File Systen Windows Windows Network L Windo Network A Software F Software F Security Active Advanced 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Pace Settings Specify behavior for when a computer is connected to a public network location. State On (recommended) State Firewall state: On (recommended) V Inbound connections: Block (default) V Outbound connections: Allow (default) V Settings Specify settings that control Windows Customize Logging Specify logging settings for troubleshooting. Customize OK Cancel Apply	□ ×
File Action View Help Software Settings Windows Settings Name Resolut Scripts (Startu Scripts (Startu Scripts (Startu Scripts (Startu Event Log Local Polic System Se Registry Registry File Systen Windows Windows Network L Windo Network A Software F Software F Security Active Advanced 	Group Policy Management Editor Windows Firewall with Advanced Security - LDAP:/// × Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to a public network location. State Inbound connections: Block (default) v Outbound connections: Block (default) v Outbound connections: Allow (default) v Settings Specify settings that control Windows Customize Logging Specify logging settings for troubleshooting. Customize OK Cancel Apply	□ ×

父環速集團 Speedy Group







5. [防止 WannaCry 經 SMB 連接埠進入]

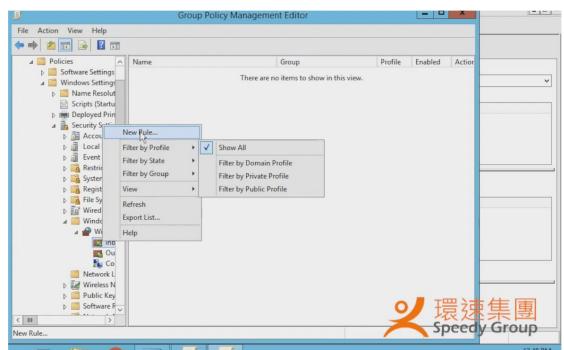
新增兩個 "Inbound Rules", 分別阻擋以下連接埠: TCP 139,445 UDP 137,138

Action View Help Action View				
▲ Policies ∧ ▷ Software Settings ∧ ▷ Windows Setting > ▷ Name Resolut > ○ Scripts (Starture > ▷ Deployed Prin > ▷ Account P > ▷ ∴ Local Polic ▷ ∴ Event Log ▷ ∴ Kestricted ▷ … Windows △ … Windows △ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … ○ … … …			Clo	ose
 Software Settings Windows Setting Name Resolut Scripts (Startu Scripts (Startu Security Settin Security Sett				
 Windows Settings Name Resolut Scripts (Startu Deployed Prin Sceurity Settin Account P Local Polic Local Polic Event Log = System Se Registry Site System Windows Public Key 	Profile	Enabled	Actior	
 Name Resolut Scripts (Startu Deployed Prin Security Settin Account P Local Polic Local Polic Event Log = Registry System Se Registry Rile System Windows I Public Key 	All	Yes	Block	
Scripts (Startu Deployed Prin Security Settir Deployed Prin Security Settir Deployed Polie Deployed Polie Depl	All	Yes	Block	
 Deployed Prin Security Settir Account Polic Local Polic Local Polic Event Log Event Log Restricted Resistry Registry Registry Registry Registry Wired Net Windows I Windows I Windows I Windows I Co Network L Wireless N Public Key 				
▲ Security Settin ▷ Account P ▷ Local Polic ▷ Event Log = ▷ Restricted ▷ Restricted ▷ Restricted ▷ Restricted ▷ Restricted ▷ Registry ▷ File System ▷ Windows △ Windows △ Windows ▲ Ou ▲ Ou ▲ Ou ▲ Windows ▲ Public Key				
 Account P Local Polic Local Polic Local Polic Restricted System Se System Se Registry Registry Registry File Systen Windo will Windows Windo Windo Windo Windo Windo Windo Windo Windo Windo Public Key 				
 Local Polic Event Log ≡ Event Log ≡ System Se System Se Registry File System Windows Windows Windows Windows Windows Ou Co Network L Wireless N Public Key 				
 Event Log Event Log Restricted Restricted Registry File System Windows I Windows I Windows I Windows I Co Network L Wireless N Public Key 				
 Restricted System Se Registry Registry Wired Net Windows Windows Windo Inb Ou Co Network L Wireless N Public Key 				
 System Se Registry Rejistry Wired Net Windows I Windo Public Key 				
 ▷ Kegistry ▷ File Systen ▷ Wired Net ▲ Windows ▲ Windows ▲ Windo Windo ▲ Windo ■ Windo <l< td=""><td></td><td></td><td></td><td></td></l<>				
 ▷ Kite System ▷ Wired Net ▲ Windows I ▲ Windows I ▲ Windo Windo ■ Inb ■ Ou ■ Co ■ Ketwork L ▷ Wireless N ▷ ■ Public Key 				
 Wired Net Windows Windo Inb Ou Co Network L Wireless N Public Key 				
✓ Windows Windo Windo Inb Co Network L Wireless N Public Key				<u> </u>
 Windo Inb Ou Ou Co Metwork L Wireless N Public Key 				
Co Metwork L ▷ Wireless N ▷ □ Public Key				
E Co Ketwork L ▷ Wireless N ▷ Public Key				
Network L K Wireless N Public Key				
þ 🧱 Wireless N þ 🧰 Public Key				
👂 🧰 Public Key				
Software R	0	I	<u></u>	6 住 国
			えど	「法国
		SI	peed	y Group

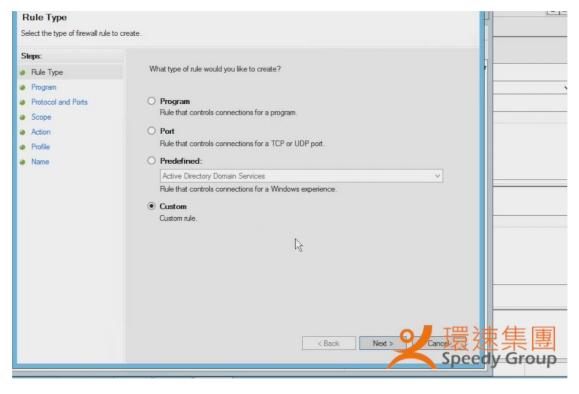








5. ii)









5. iii)

Steps:	
 Rule Type Program 	Does this rule apply to all programs or a specific program?
 Protocol and Ports Scope Action 	All programs Rule applies to all connections on the computer that match other rule properties. This program path:
 Profile Name 	Example: c:\path\program.exe %Program.Files %\browser\browser.exe Services Specify which services this rule applies to.
	K Next Speedy Group

5. iv)

IJ	Protocol and Ports				
File A	Specify the protocols and ports to	which this rule applies.			
*	Steps:				
4	Rule Type	To which ports and pro	ptocols does this rule apply?		r
	Program				~
	Protocol and Ports	Protocol type:	TCP	~	
	Scope	Protocol number:	6		
	Action				
	Profile	Local port:	Specific Ports	~	
	Name		139,445		
			Example: 80, 443, 5000-5010	0	
		Remote port:	All Ports	~	
			Example: 80, 443, 5000-5010	0	
		Internet Control Mess (ICMP) settings:	age Protocol Customi	ize	
		(ICIVIF) settings.			
					油作面
< 111				< Back Cancel	本未団
				Spe	edy Group



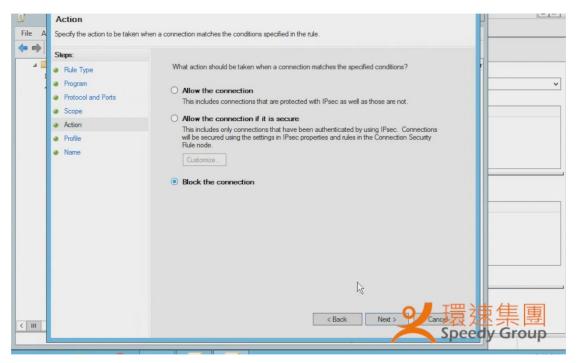




5. v)

File A	Scope Specify the local and remote IP a	addresses to which this rule applies.	<u></u>
	Steps: Pule Type Program Protocol and Ports Scope	Which local IP addresses does this rule apply to? Any IP addresses These IP addresses:	~
	Action Profile Name	Add Edt Remove Customize the interface types to which this rule applies: Customize Which remote IP addresses does this rule apply to? • Any IP address These IP addresses:	
< 111		<pre>Add Edt Remove </pre>	王 J Foup

5. vi)

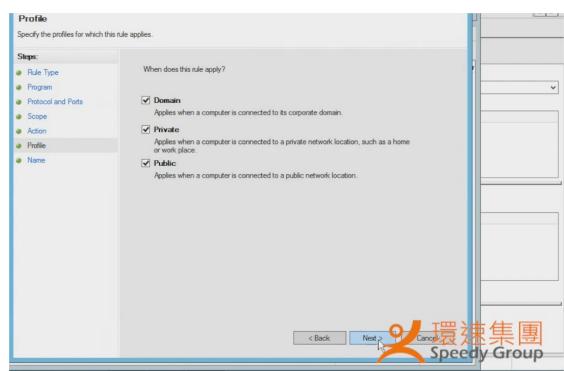








5. vii)



5. viii)

Name Specify the name and description	of this rule.
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	Name: Block WannaCry TCP port 139,445 Description (optional):
	Speedy Group







5. ix)

Steps:				
 Rule Type 	To which ports and pr	otocols does this rule apply?	Enabled Action	
 Program 			Yes Block	
 Protocol and Ports 	Protocol type:	UDP V		
Scope	Protocol number:	17		
Action	Trococornamocr.			
Profile	Local port:	Specific Ports		
Name		137,138		
		Example: 80, 443, 5000-5010		
	Remote port:	All Ports V		
		Example: 80, 443, 5000-5010		
	Internet Control Mess (ICMP) settings:	age Protocol Customize		
		-		三国

5. x)

Name			- 0
Specify the name and description	of this rule.		
Steps:			
Rule Type	h	Enabled Action Yes Block	
Program		DIOCK	~
Protocol and Ports			
Scope	Name: Block WannaCry UDP Port 137,138		
Action			
Profile	Description (optional):		
Name			
	(住面
	< Back Finish Cancel	~ 坂汉	同志
	/	Speed	y Group

完





