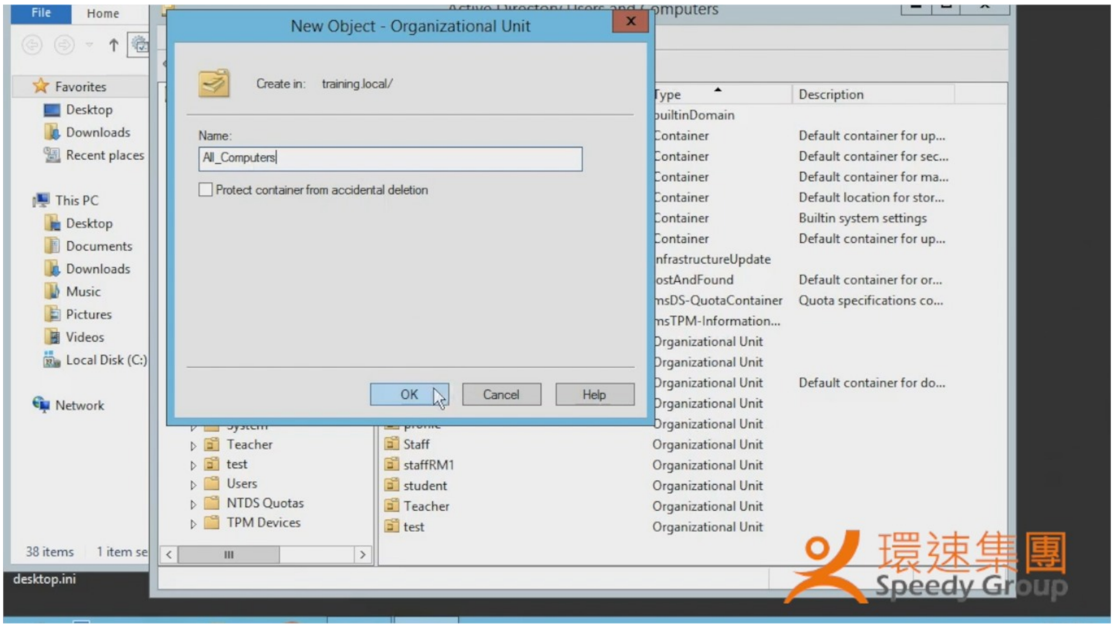
有關 WannaCry 及日後對本港學校具威脅的科技風險資訊分享
環速學校 IT 支援服務已在 Facebook（**www.facebook.com/SpeedyGroupHK**）發佈供本港學校的最新技術訊息，分享學校防範 WannaCry 之實用建議、技術支援資訊及影片，請密切留意。

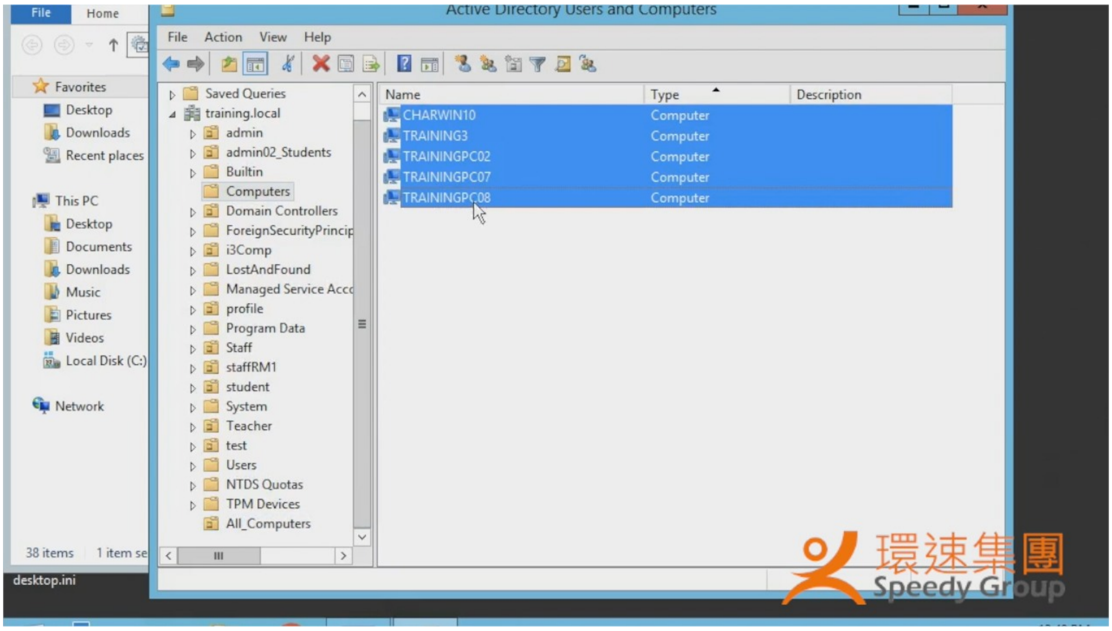
群組原則 (Group Policy) - 封鎖網域電腦 SMB 連接埠

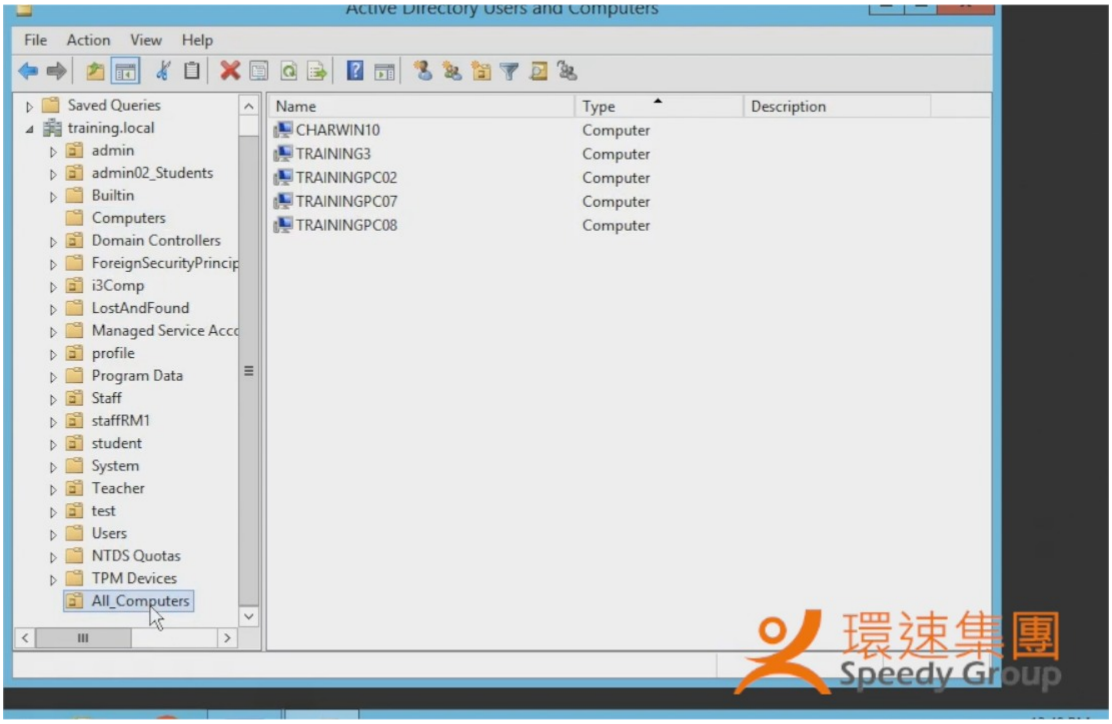
注意：以下教學以 Windows Server 2012 R2 網域控制器為例，請注意 Windows XP 用戶不能經以下教學封鎖 SMB 連接埠，BYOD 用戶亦不適用 *(由於各校網域環境情況不同，以下教學只供參考之用)*

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

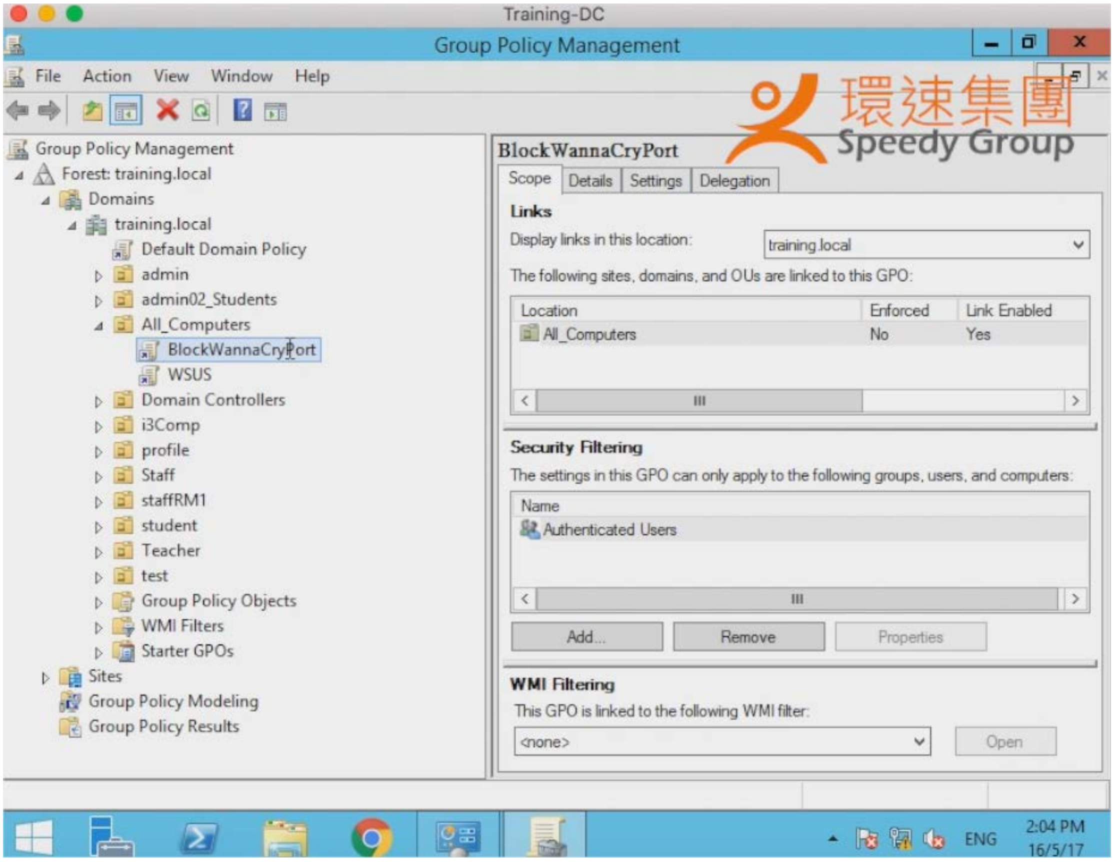


2. 把所有使用者電腦拖延至剛才新建立的 “All_Computers” 內;
(*請勿把有伺服器功能的電腦一起遷移*)





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



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)

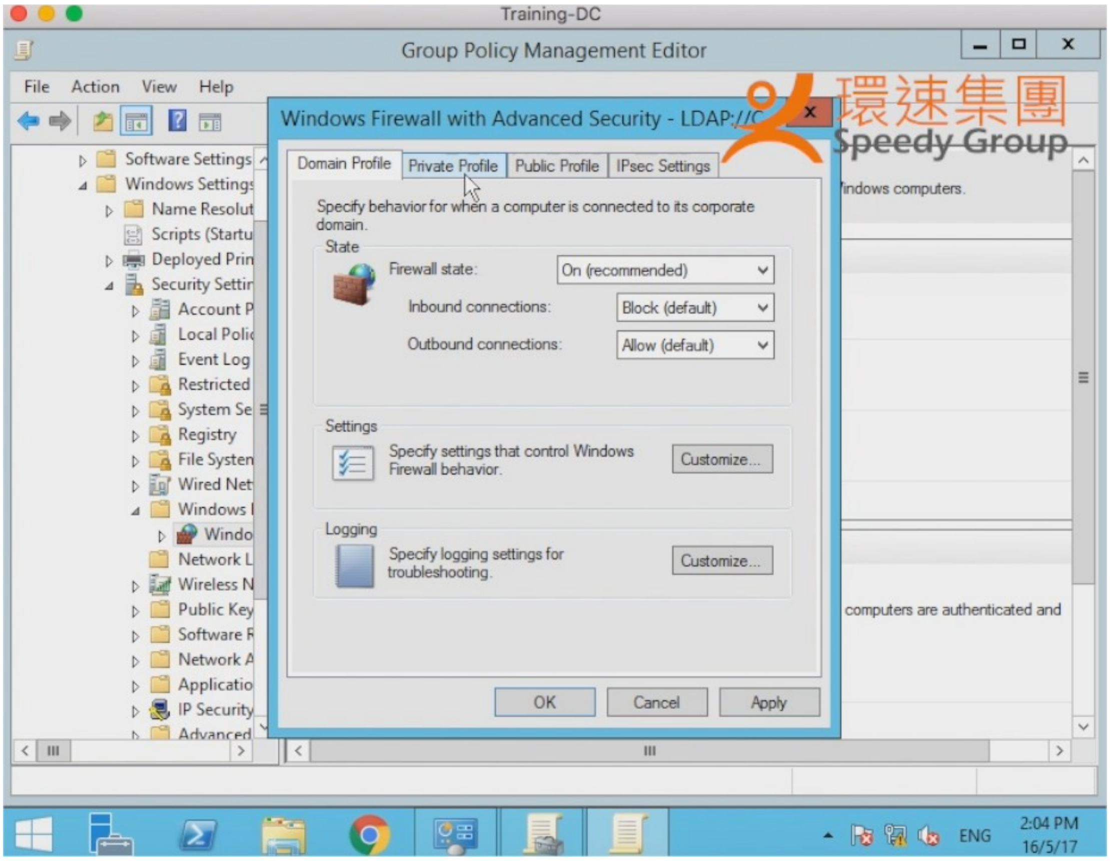
Outbound connections Allow (default)

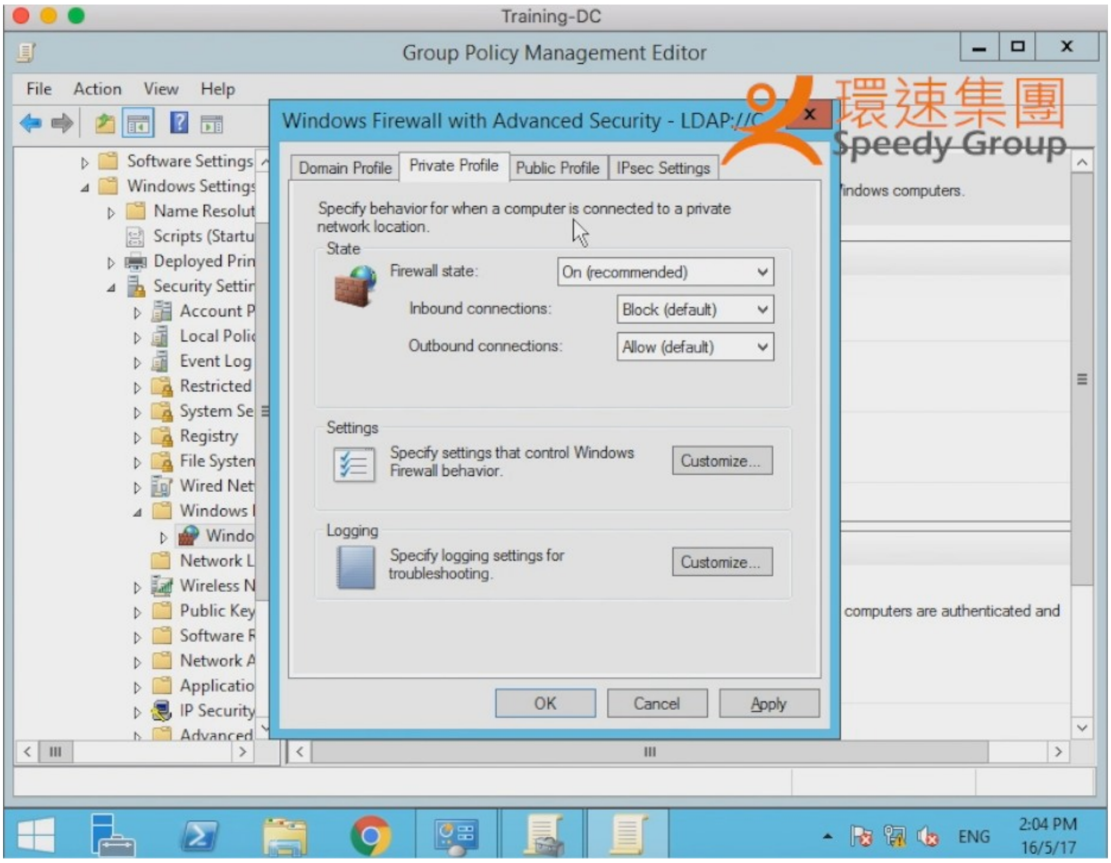
Public Profile:

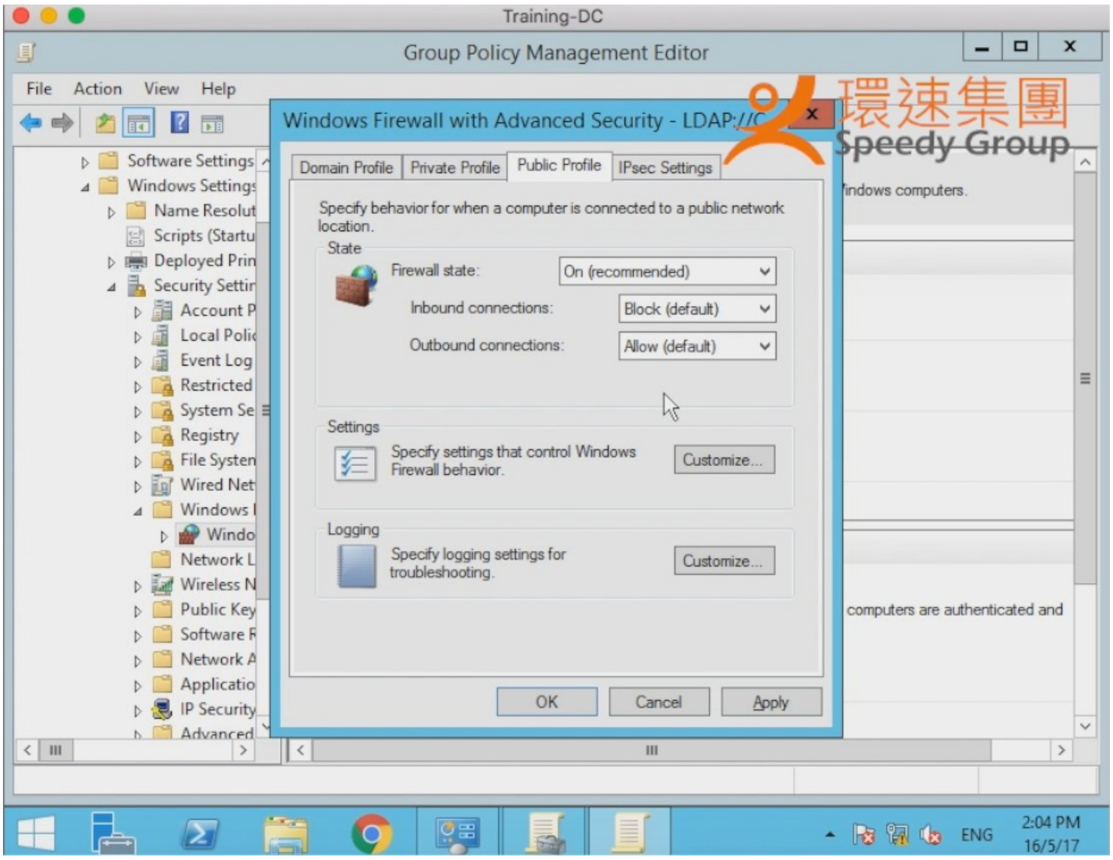
Firewall state: On (recommended)

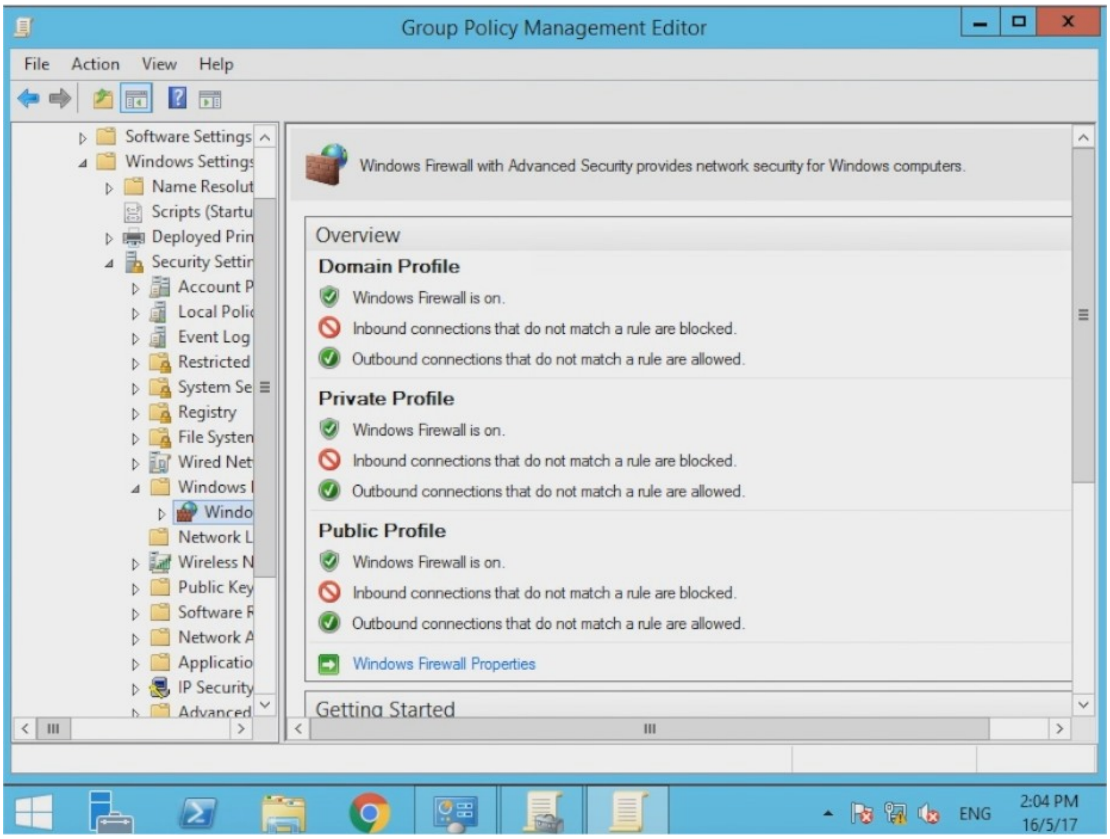
Inbound connections: Block (default)

Outbound connections Allow (default)



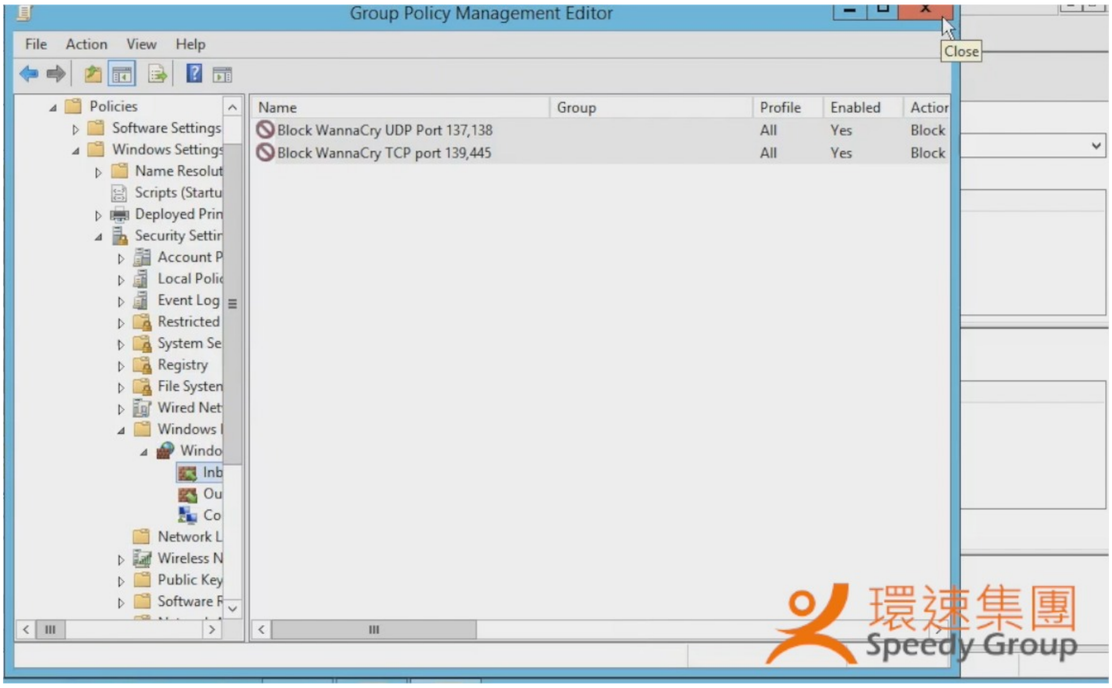

Training-DC
Group Policy Management Editor
File Action View Help
Windows Firewall with Advanced Security - LDAP://C
Domain Profile
Private Profile
Public Profile
IPsec Settings
Specify behavior for when a computer is connected to a private network location.
State
Firewall state:
On (recommended)
Inbound connections:
Block (default)
Outbound connections:
Allow (default)
Settings
Specify settings that control Windows Firewall behavior.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
OK
Cancel
Apply
2:04 PM
16/5/17


Training-DC
Group Policy Management Editor
File Action View Help
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)
Settings
Specify settings that control Windows Firewall behavior.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
OK
Cancel
Apply
2:04 PM
16/5/17

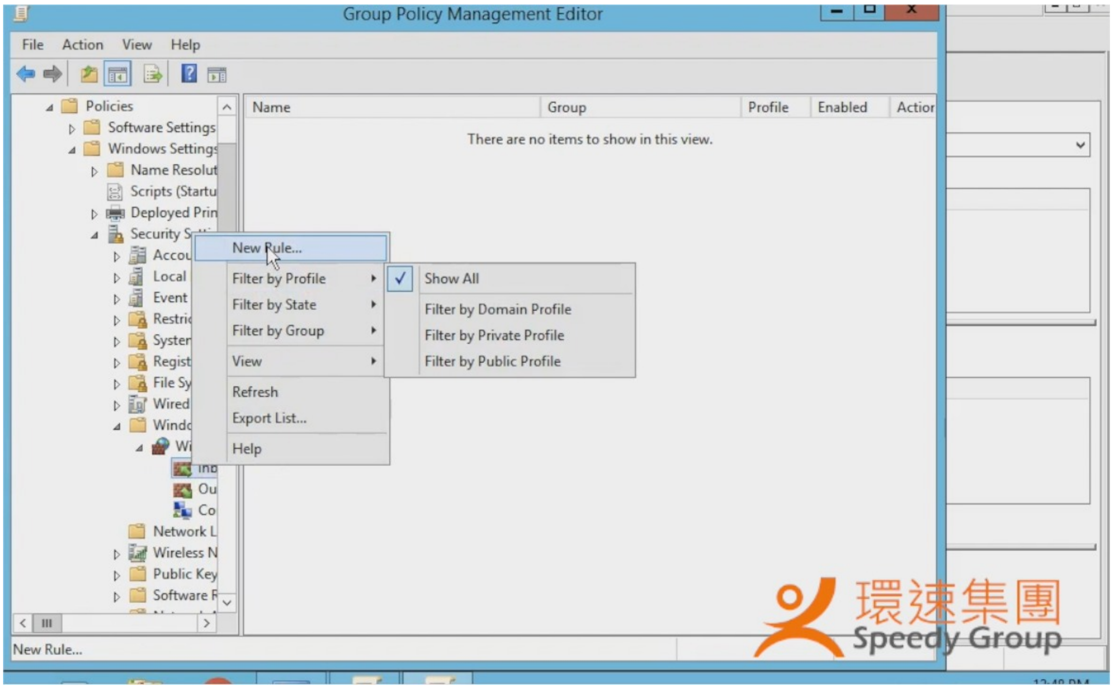


5. **[防止 WannaCry 經 SMB 連接埠進入]**

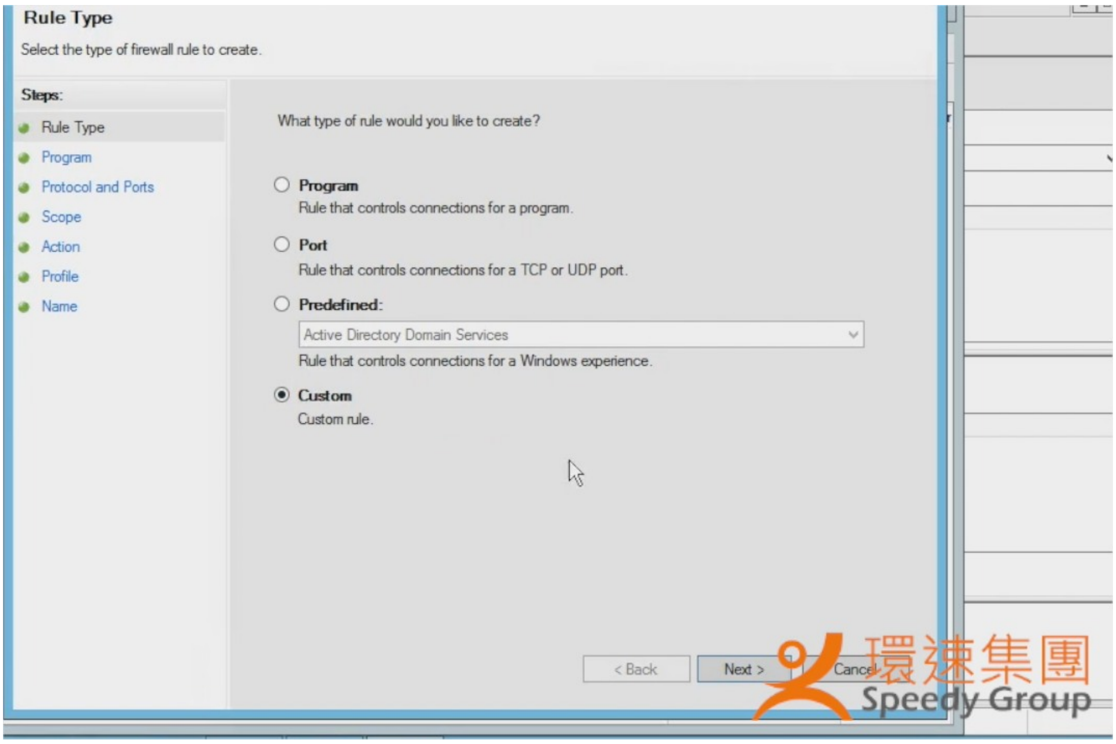
新增兩個 “Inbound Rules”，分別阻擋以下連接埠: TCP 139,445 UDP 137,138



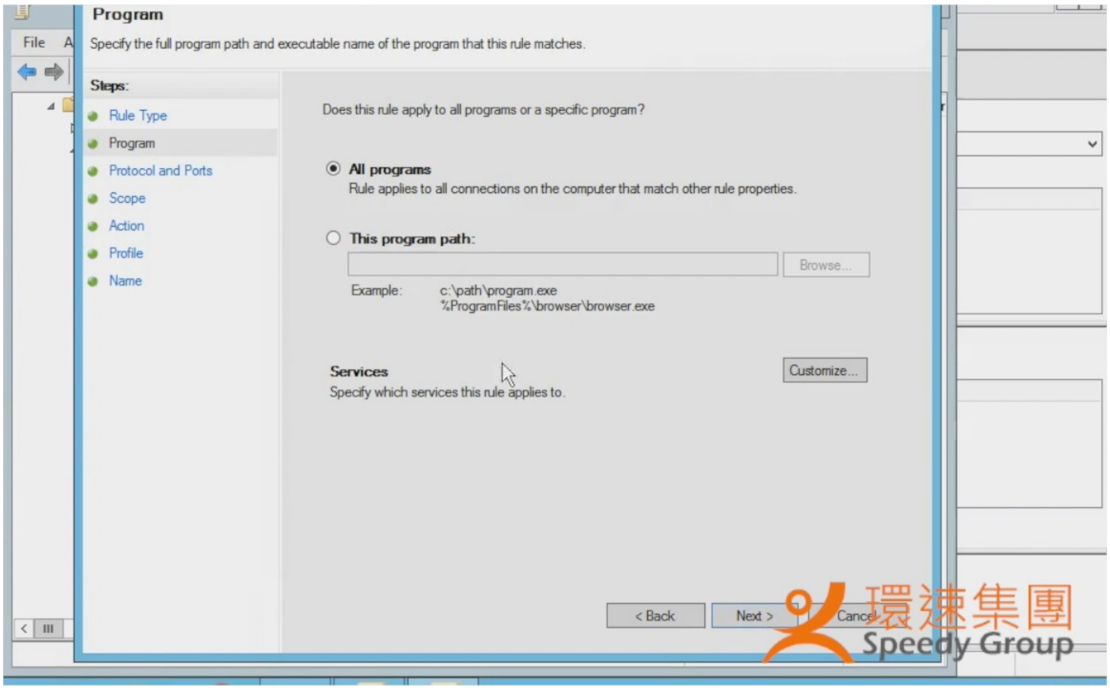
5. i)


Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security S
Accou
Local
Event
Restric
Syster
Regist
File Sy
Wired
Windo
Wi
Inb
Ou
Co
Network L
Wireless N
Public Key
Software R
Name
Group
Profile
Enabled
Action
There are no items to show in this view.
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Show All
Filter by Domain Profile
Filter by Private Profile
Filter by Public Profile
New Rule...
環速集團
Speedy Group

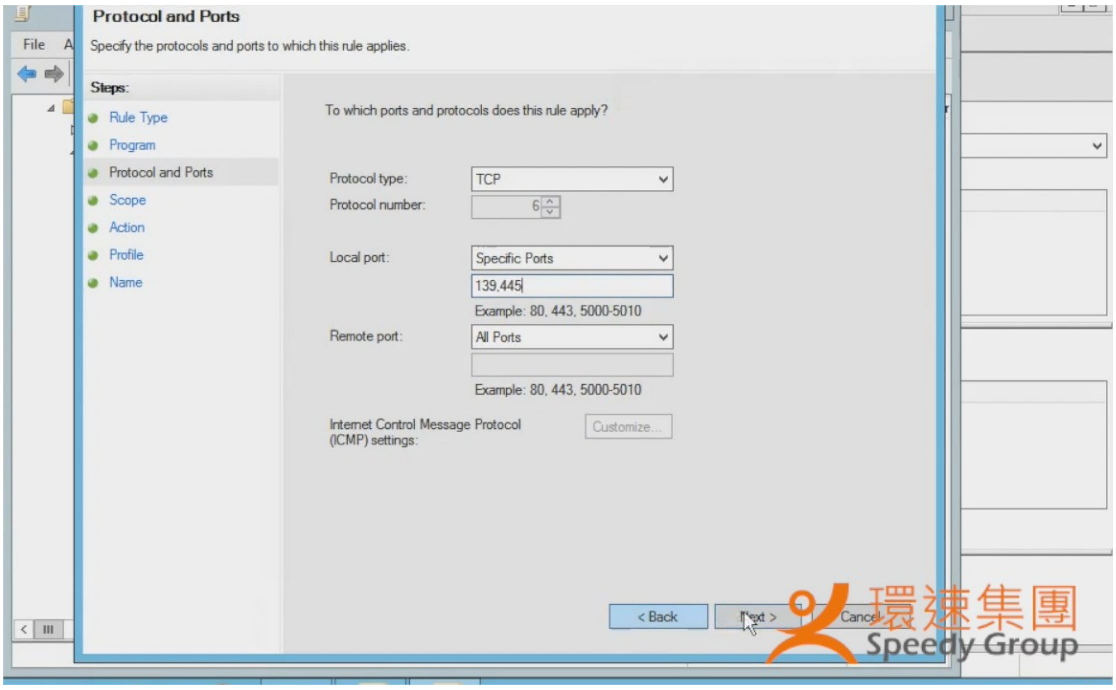
5. ii)


Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Active Directory Domain Services
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
環速集團
Speedy Group

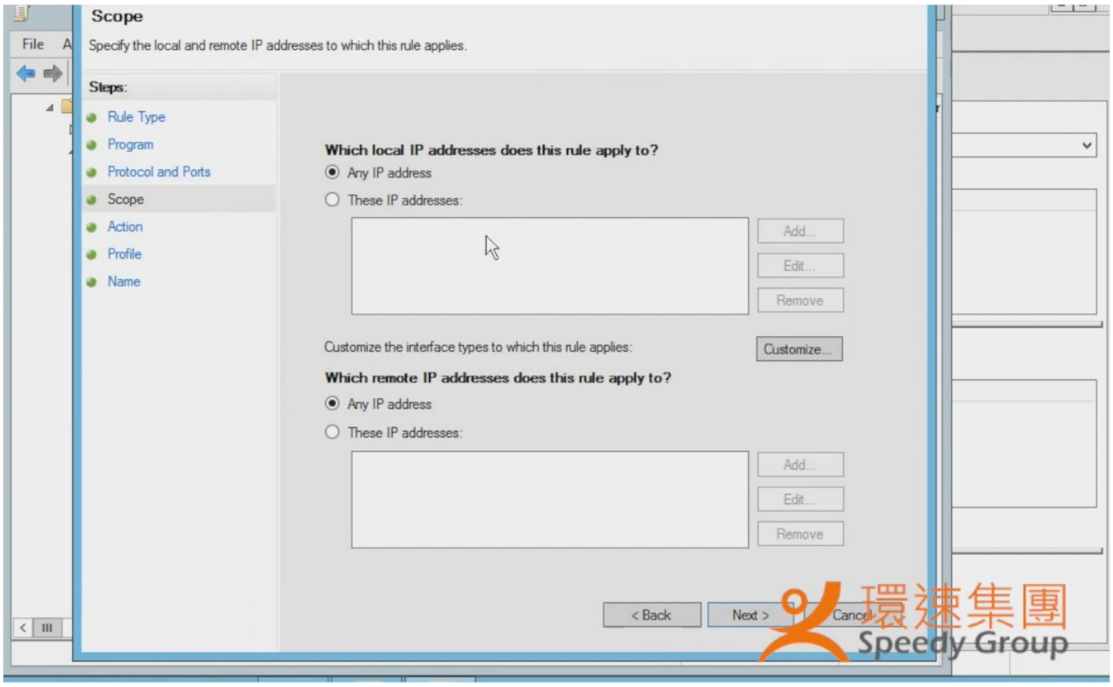
5. iii)


File
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
環速集團
Speedy Group

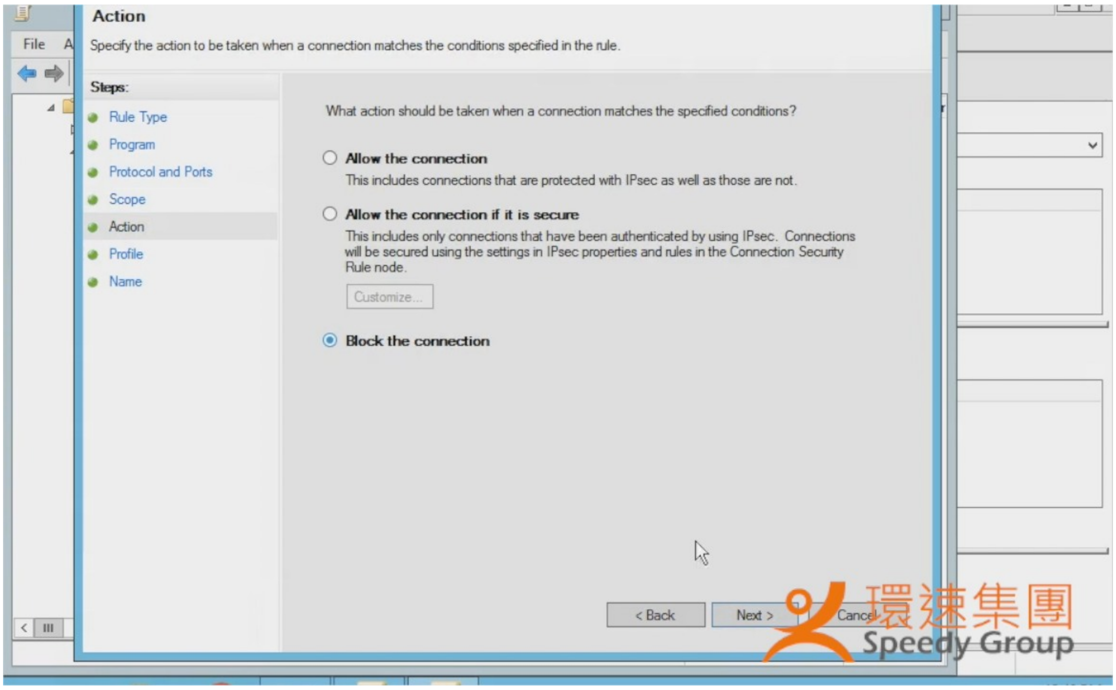
5. iv)


File
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type: TCP
Protocol number: 6
Local port: Specific Ports
139,445
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
環速集團
Speedy Group

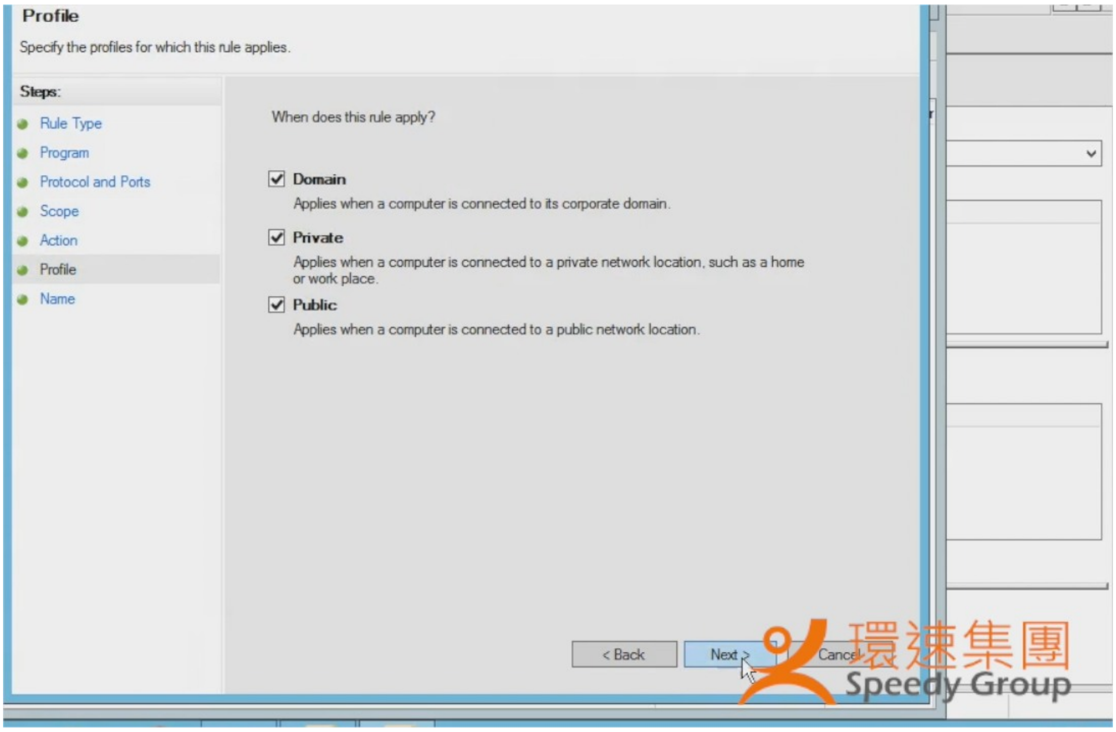
5. v)


Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
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:
Add...
Edit...
Remove
< Back
Next >
環速集團
Speedy Group

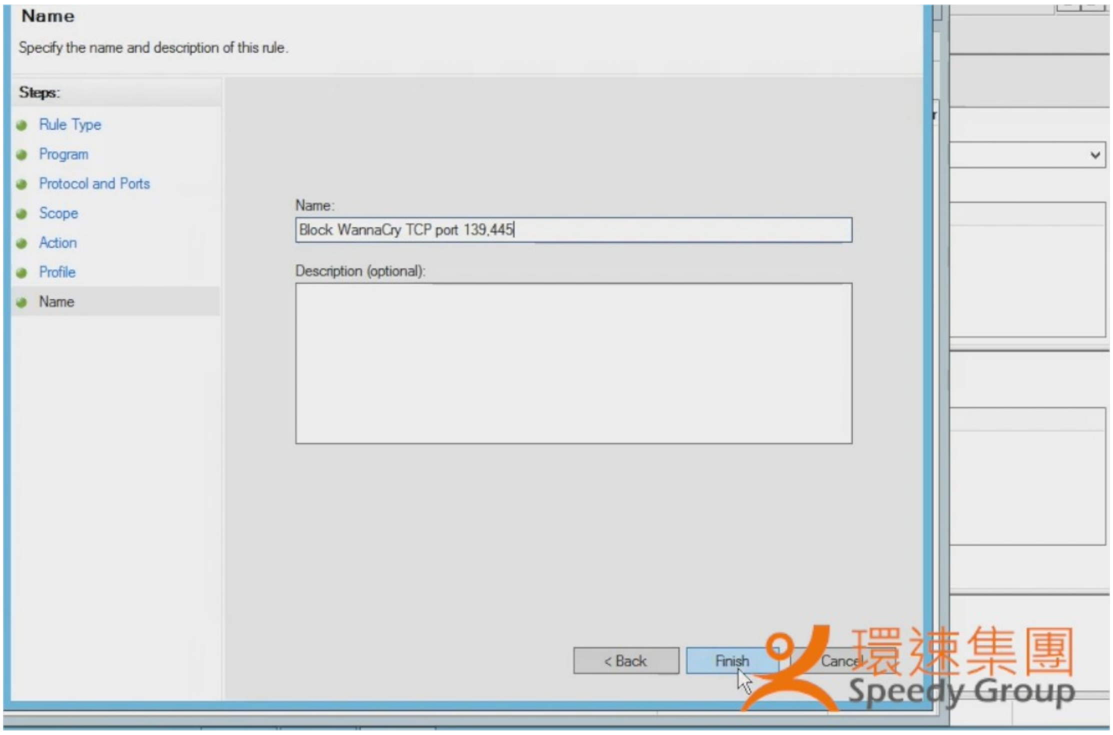
5. vi)


Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
環速集團
Speedy Group

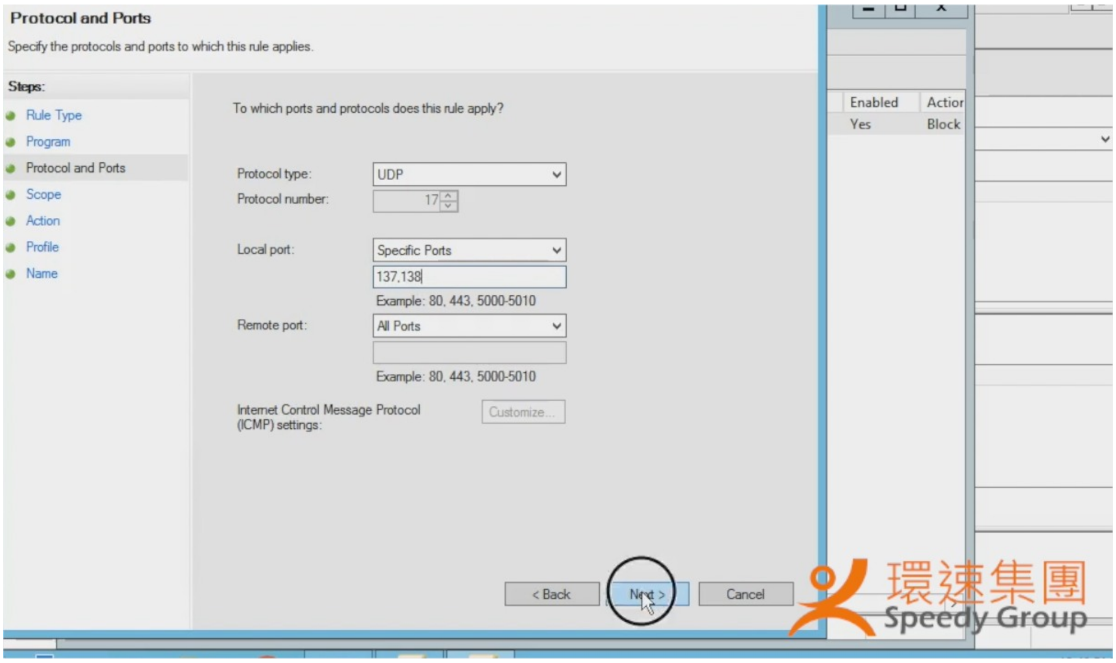
5. vii)


Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
環速集團
Speedy Group

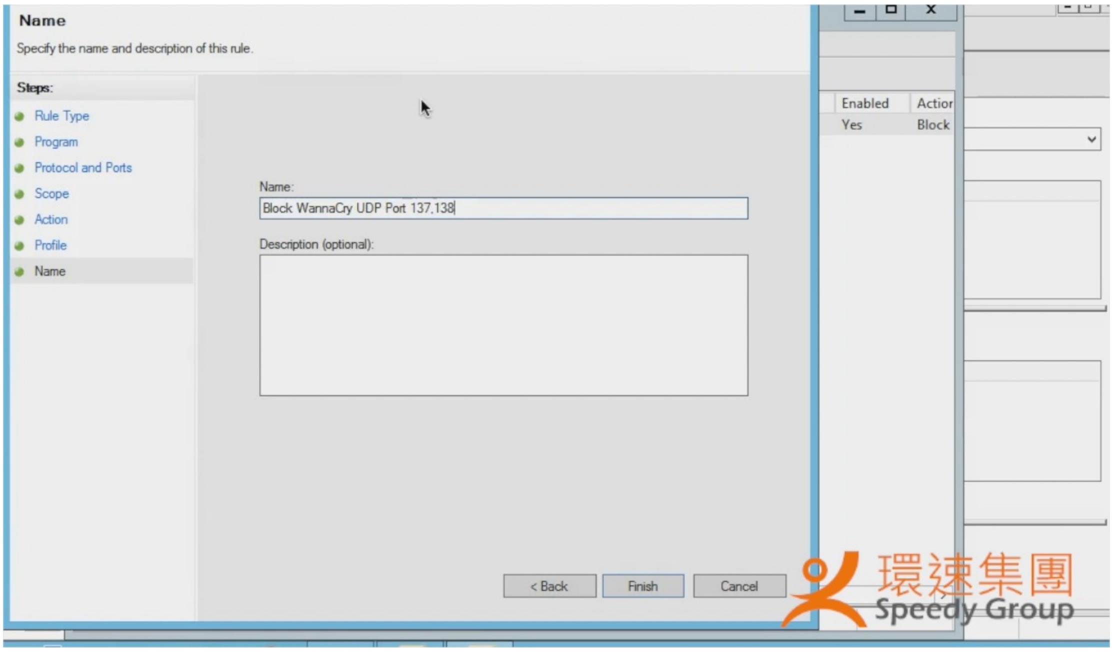
5. viii)


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):
< Back
Finish
環速集團
Speedy Group

5. ix)


Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
UDP
Protocol number:
17
Local port:
Specific Ports
137,138
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel
Enabled
Yes
Block
環速集團
Speedy Group

5. x)


Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
Block WannaCry UDP Port 137,138
Description (optional):
< Back
Finish
Cancel
Enabled
Yes
Block
環速集團
Speedy Group

完