

THỰC HÀNH QUẢN TRỊ ATTT TRÊN HỆ THỐNG WINDOWS

Sinh viên: Đinh Thị Hòa

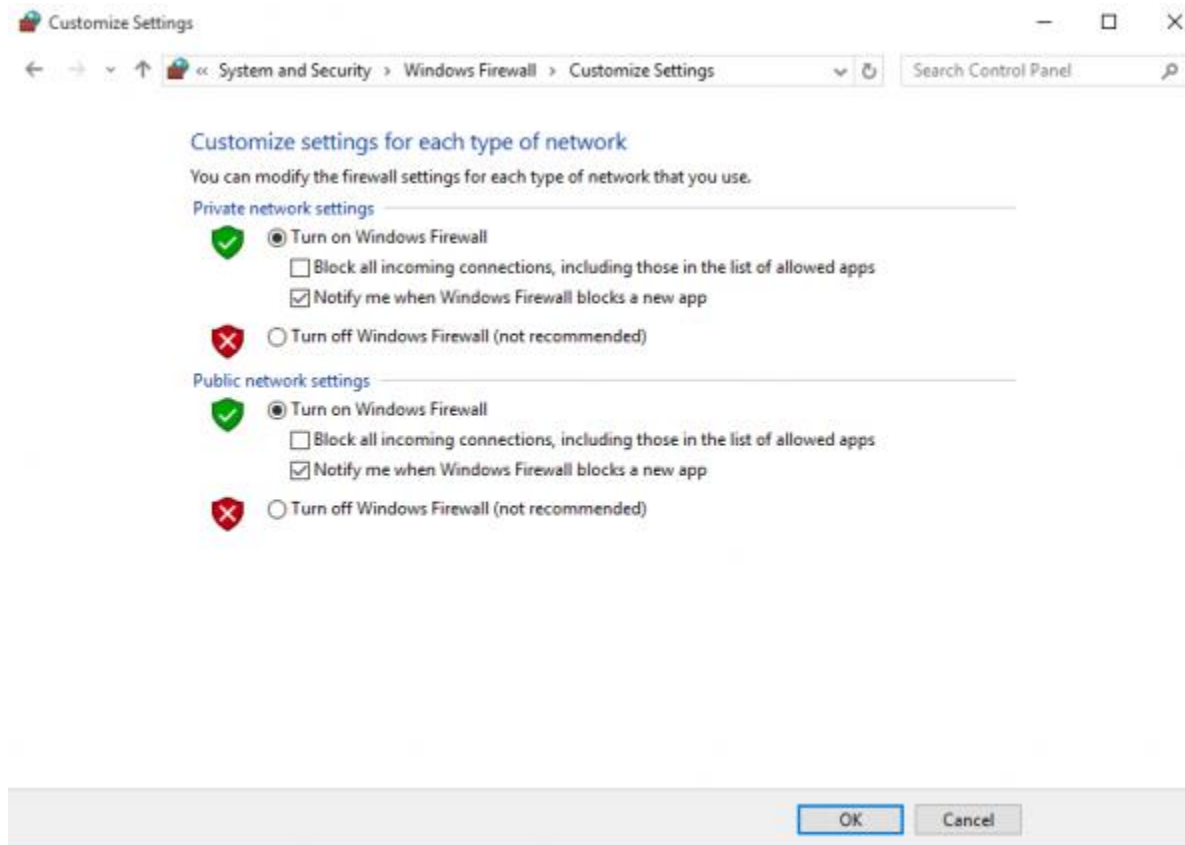
Lớp: CNPM13

Nội dung

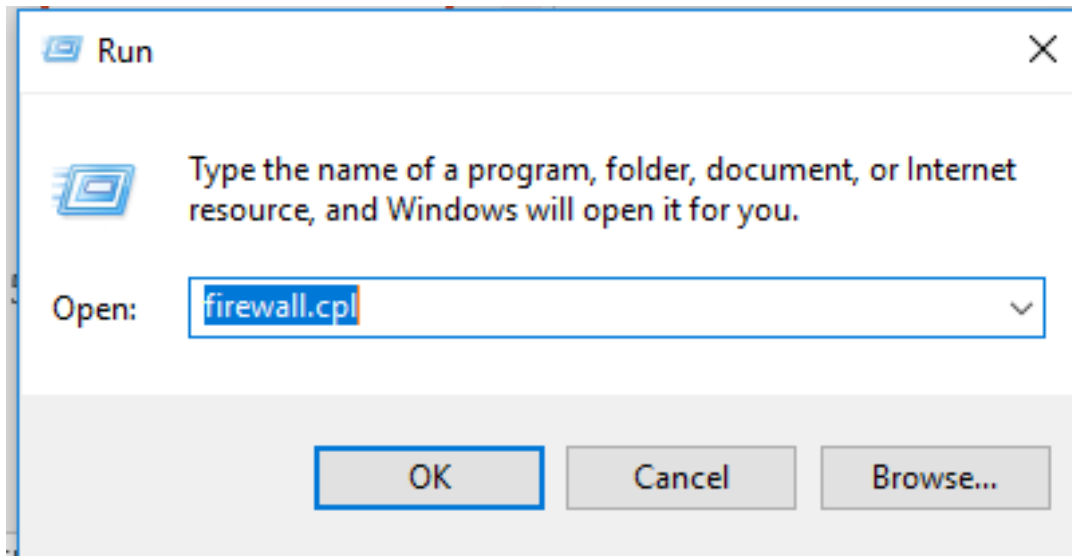
- Windows Firewall
- Các lệnh cmd
- Window powershell

Windows Firewall

- **firewall.cpl**



Window + R -> firewall.cpl



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

Public network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

OK

Cancel

Tập lệnh cmd trong Windows

- Help- hướng dẫn chung (/?)
- Net – thông tin về mạng
- Netsh – cấu hình mạng từ xa (**netsh firewall show config**)
- Netstat – hiển thị các thông tin kết nối TCP
- Ping – kiểm tra, khảo sát kết nối
- Route – hiển thị, điều chỉnh thông tin bảng định tuyến IP table
- Ipconfig – hiển thị cấu hình TCP/IP mạng
- Tracert – hiển thị thông tin truyền tải dữ liệu đến mục tiêu mạng được chỉ định
- Nslookup – hiển thị thông tin để có thể phân tích Domain Name System (DNS)
- Nbtstat – thông tin về các kết nối Netbios
- Arp – hiển thị và chỉnh sửa thông tin về Address Resolution Protocol (ARP)
- Rexec – chạy các lệnh trên máy tính kết nối từ xa
- Call – gọi thực thi một tập lệnh (dạng .bat)

- Lệnh để thoát: **exit**

Window + R -> lệnh help

```
Microsoft Windows [Version 10.0.17134.286]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Hoa DT>help
For more information on a specific command, type HELP command-name
ASSOC      Displays or modifies file extension associations.
ATTRIB     Displays or changes file attributes.
BREAK      Sets or clears extended CTRL+C checking.
BCDEDIT    Sets properties in boot database to control boot loading.
CACLS      Displays or modifies access control lists (ACLs) of files.
CALL       Calls one batch program from another.
CD          Displays the name of or changes the current directory.
CHCP       Displays or sets the active code page number.
CHDIR      Displays the name of or changes the current directory.
CHKDSK     Checks a disk and displays a status report.
CHKNTFS    Displays or modifies the checking of disk at boot time.
CLS        Clears the screen.
CMD        Starts a new instance of the Windows command interpreter.
COLOR      Sets the default console foreground and background colors.
COMP       Compares the contents of two files or sets of files.
COMPACT    Displays or alters the compression of files on NTFS partitions.
CONVERT    Converts FAT volumes to NTFS. You cannot convert the
           current drive.
COPY       Copies one or more files to another location.
DATE       Displays or sets the date.
DEL        Deletes one or more files.
DIR        Displays a list of files and subdirectories in a directory.
DISKPART   Displays or configures Disk Partition properties.
DOSKEY     Edits command lines, recalls Windows commands, and
           creates macros.
DRIVERQUERY Displays current device driver status and properties.
ECHO       Displays messages, or turns command echoing on or off.
ENDLOCAL   Ends localization of environment changes in a batch file.
ERASE      Deletes one or more files.
EXIT       Quits the CMD.EXE program (command interpreter).
FC         Compares two files or sets of files, and displays the
           differences between them.
FIND       Searches for a text string in a file or files.
FINDSTR    Searches for strings in files.
FOR        Runs a specified command for each file in a set of files.
FORMAT     Formats a disk for use with Windows.
FSUTIL     Displays or configures the file system properties.
FTYPE      Displays or modifies file types used in file extension
           associations.
```

Window + R -> lệnh Net

```
C:\Users\Hoa DT>net
The syntax of this command is:
```

```
NET
```

```
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |  
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |  
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```


Window + R -> lệnh Netsh

```
C:\Users\Hoa DT>netsh  
netsh>
```

netsh firewall show config

```
C:\Users\Hoa DT>netsh
netsh>firewall show config

Domain profile configuration:
-----
Operational mode           = Enable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Allowed programs configuration for Domain profile:
Mode      Traffic direction  Name / Program
-----
-----

Port configuration for Domain profile:
Port      Protocol  Mode      Traffic direction  Name
-----

ICMP configuration for Domain profile:
Mode      Type      Description
-----
Enable    2          Allow outbound packet too big

Standard profile configuration (current):
-----
Operational mode           = Enable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Service configuration for Standard profile:
Mode      Customized  Name
-----
Enable    No          Network Discovery

Allowed programs configuration for Standard profile:
Mode      Traffic direction  Name / Program
-----
-----

Port configuration for Standard profile:
Port      Protocol  Mode      Traffic direction  Name
-----
```

Netstat - hiển thị các thông tin kết nối TCP

```
C:\Users\Hoa DT>netstat
```

```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	192.168.43.117:57062	a-0001:https	ESTABLISHED
TCP	192.168.43.117:57064	104.18.24.243:http	CLOSE_WAIT
TCP	192.168.43.117:57067	40.100.54.210:https	ESTABLISHED
TCP	192.168.43.117:57071	52.114.132.22:https	ESTABLISHED
TCP	192.168.43.117:57081	52.230.84.0:https	ESTABLISHED

Ping – kiểm tra, khảo sát kết nối

```
C:\Users\Hoa DT>ping google.com

Pinging google.com [172.217.24.206] with 32 bytes of data:
Reply from 172.217.24.206: bytes=32 time=56ms TTL=53
Reply from 172.217.24.206: bytes=32 time=71ms TTL=53
Reply from 172.217.24.206: bytes=32 time=66ms TTL=53
Reply from 172.217.24.206: bytes=32 time=70ms TTL=53

Ping statistics for 172.217.24.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 71ms, Average = 65ms
```

Route – hiển thị, điều chỉnh thông tin bảng định tuyến IP table

```
C:\Users\Hoa DT>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
      [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f          Clears the routing tables of all gateway entries.  If this is
            used in conjunction with one of the commands, the tables are
            cleared prior to running the command.

-p          When used with the ADD command, makes a route persistent across
            boots of the system.  By default, routes are not preserved
            when the system is restarted.  Ignored for all other commands,
            which always affect the appropriate persistent routes.

-4          Force using IPv4.

-6          Force using IPv6.

command     One of these:
            PRINT      Prints  a route
            ADD        Adds    a route
            DELETE     Deletes a route
            CHANGE     Modifies an existing route

destination Specifies the host.
MASK         Specifies that the next parameter is the 'netmask' value.
netmask      Specifies a subnet mask value for this route entry.
            If not specified, it defaults to 255.255.255.255.
gateway      Specifies gateway.
interface    the interface number for the specified route.
METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS.  The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE.  Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.
```

Route PRINT

```
C:\Users\Hoa DT>route PRINT
=====
Interface List
16...ec f4 bb 67 84 59 .....Intel(R) 82579LM Gigabit Network Connection
6...2e 33 7a 43 e8 56 .....Microsoft Wi-Fi Direct Virtual Adapter
7...2e 33 7a 43 e0 56 .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...2c 33 7a 43 e8 56 .....Broadcom 802.11n Network Adapter
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.43.1      192.168.43.117   55
127.0.0.0                  255.0.0.0        On-link           127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link           127.0.0.1        331
127.255.255.255            255.255.255.255  On-link           127.0.0.1        331
192.168.43.0                255.255.255.0    On-link           192.168.43.117   311
192.168.43.117              255.255.255.255  On-link           192.168.43.117   311
192.168.43.255              255.255.255.255  On-link           192.168.43.117   311
224.0.0.0                  240.0.0.0        On-link           127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link           192.168.43.117   311
255.255.255.255            255.255.255.255  On-link           127.0.0.1        331
255.255.255.255            255.255.255.255  On-link           192.168.43.117   311
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331 ::1/128                      On-link
14   311 fe80::/64                      On-link
14   311 fe80::4540:87e3:7ad3:d151/128 On-link
1    331 ff00::/8                      On-link
14   311 ff00::/8                      On-link
=====
Persistent Routes:
None
```

Fore using Ipv4

```
C:\Users\Hoa DT>route PRINT -4
=====
Interface List
16...ec f4 bb 67 84 59 .....Intel(R) 82579LM Gigabit Network Connection
 6...2e 33 7a 43 e8 56 .....Microsoft Wi-Fi Direct Virtual Adapter
 7...2e 33 7a 43 e0 56 .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...2c 33 7a 43 e8 56 .....Broadcom 802.11n Network Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.43.1     192.168.43.117   55
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
192.168.43.0                255.255.255.0    On-link          192.168.43.117   311
192.168.43.117              255.255.255.255  On-link          192.168.43.117   311
192.168.43.255              255.255.255.255  On-link          192.168.43.117   311
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.43.117   311
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.43.117   311
=====
Persistent Routes:
None
```

Ipconfig – hiển thị cấu hình TCP/IP mạng

```
C:\Users\Hoa DT>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::4540:87e3:7ad3:d151%14
    IPv4 Address. . . . . : 192.168.43.117
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.1
```


Tracert – hiển thị thông tin truyền tải dữ liệu đến mục tiêu mạng được chỉ định

```
C:\Users\Hoa DT>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d                Do not resolve addresses to hostnames.
  -h maximum_hops   Maximum number of hops to search for target.
  -j host-list       Loose source route along host-list (IPv4-only).
  -w timeout         Wait timeout milliseconds for each reply.
  -R                Trace round-trip path (IPv6-only).
  -S srcaddr         Source address to use (IPv6-only).
  -4                Force using IPv4.
  -6                Force using IPv6.
```

Nslookup – hiển thị thông tin để có thể phân tích Domain Name System (DNS)

```
C:\Users\Hoa DT>nslookup  
Default Server: UnKnown  
Address: 192.168.43.1  
>
```

Nbtstat – thông tin về các kết nối Netbios

```
C:\Users\Hoa DT>Nbtstat
```

```
Displays protocol statistics and current TCP/IP connections using NBT  
(NetBIOS over TCP/IP).
```

```
NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]  
          [-r] [-R] [-RR] [-s] [-S] [interval] ]
```

```
-a  (adapter status) Lists the remote machine's name table given its name  
-A  (Adapter status) Lists the remote machine's name table given its  
                        IP address.  
-c  (cache)          Lists NBT's cache of remote [machine] names and their IP addresses  
-n  (names)          Lists local NetBIOS names.  
-r  (resolved)       Lists names resolved by broadcast and via WINS  
-R  (Reload)         Purges and reloads the remote cache name table  
-S  (Sessions)       Lists sessions table with the destination IP addresses  
-s  (sessions)       Lists sessions table converting destination IP  
                        addresses to computer NETBIOS names.  
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh
```

```
RemoteName  Remote host machine name.  
IP address  Dotted decimal representation of the IP address.  
interval    Redisplays selected statistics, pausing interval seconds  
              between each display. Press Ctrl+C to stop redisplaying  
              statistics.
```

Arp – hiển thị và chỉnh sửa thông tin về Address Resolution Protocol (ARP)

```
C:\Users\Hoa DT>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
             protocol data. If inet_addr is specified, the IP and Physical
             addresses for only the specified computer are displayed. If
             more than one network interface uses ARP, entries for each ARP
             table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
             entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
             by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
             wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
             with the Physical address eth_addr. The Physical address is
             given as 6 hexadecimal bytes separated by hyphens. The entry
             is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
             interface whose address translation table should be modified.
             If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

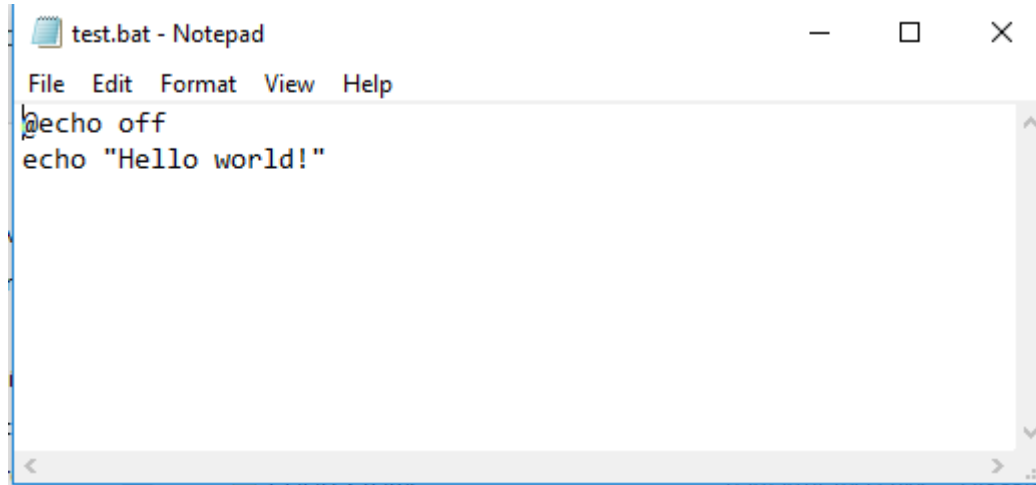
C:\Users\Hoa DT>arp -a

Interface: 192.168.43.117 --- 0xe
Internet Address    Physical Address    Type
192.168.43.1        44-78-3e-49-c8-0e   dynamic
192.168.43.255      ff-ff-ff-ff-ff-ff   static
224.0.0.22          01-00-5e-00-00-16   static
224.0.0.251         01-00-5e-00-00-fb   static
224.0.0.252         01-00-5e-00-00-fc   static
239.255.255.250     01-00-5e-7f-ff-fa   static
```

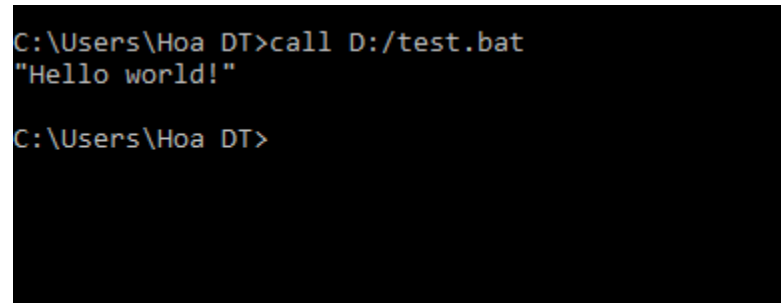
Rexec – chạy các lệnh trên máy tính kết nối từ xa

```
C:\Users\Hoa DT>rexec  
'rexec' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\Hoa DT>
```

Call – gọi thực thi một tập lệnh (dạng .bat)



```
test.bat - Notepad
File Edit Format View Help
echo off
echo "Hello world!"
```



```
C:\Users\Hoa DT>call D:/test.bat
"Hello world!"
C:\Users\Hoa DT>
```

Các cổng kết nối thường dùng

- PORT NUMBER 80 - Internet Access (HTTP)
- Port Number 443 - Secure Internet Access (HTTPS)
- Port Number 25 - emails (SMTP)
- Ví dụ về chính sách: **firewall.cpl**
- **netsh advfirewall firewall add rule name="mở cổng https" dir=in/out action=allow/block protocol=TCP localport/remoteport=443**

Block vnexpress.net & all

- netsh advfirewall firewall add rule
name="ngoc" dir=out action=block
remoteip=111.65.248.132 enable=yes
- **netsh advfirewall firewall add rule
name="ngoc" dir=out action=block
protocol=TCP**
- **netsh advfirewall firewall add rule
name="ngoc" dir=out action=block**


```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name="ngoc" dir=out action=block remoteip=111.65.248.132 enable=yes  
Ok.
```

```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name="ngoc" dir=out action=block protocol=TCP  
Ok.
```

```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name="ngoc" dir=out action=block  
Ok.
```

Một số lệnh netsh

- *netsh -f <scriptfile>*
- netsh advfirewall set allprofiles state on
- netsh advfirewall reset
- <http://windowsitpro.com/windows-server/top-10-windows-firewall-netsh-commands>

```
C:\WINDOWS\system32>netsh advfirewall set allprofiles state on  
Ok.
```

```
C:\WINDOWS\system32>netsh advfirewall reset  
Ok.
```

Windowpowershell



```
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe
PS C:\> Get-PSProvider

Name                Capabilities                Drives
----                -
Alias                ShouldProcess                {Alias}
Environment          ShouldProcess                {Env}
FileSystem            Filter, ShouldProcess        {C, D, WIN, Fav...}
Function              ShouldProcess                {Function}
Registry              ShouldProcess                {HKLM, HKCU}
Variable              ShouldProcess                {Variable}
Certificate           ShouldProcess                {cert}

PS C:\> Get-WmiObject Win32_ComputerSystem

Domain                : ntdev.corp.microsoft.com
Manufacturer          : Dell Inc.
Model                 : Inspiron 9300
Name                  : JPSVISTA1
PrimaryOwnerName      : jsnover
TotalPhysicalMemory   : 2146279424

PS C:\> 
```

Tập lệnh dạng ngôn ngữ kịch bản

- `$NIC = Get-WMIObject Win32_NetworkAdapterConfiguration`
| `where{$_.IPEnabled -eq "TRUE"}`
 - `$NIC.EnableStatic("192.168.100.66", "255.255.255.0")`
 - `$NIC.SetGateways("192.168.100.1")`
 - `$NIC.SetDNSServerSearchOrder("8.8.8.8", "8.8.4.4")`
 - `$NIC.SetDynamicDNSRegistration("FALSE")`

Hỗ trợ quản trị ATTT

- `Gwmi win32_process | select name | sort name`
- `(Gwmi win32_process | where {$_.name - (match "processname.exe")}.terminate(1)`

`Get-Process | Where { $_.handles -gt 500 } | Sort handles | Format-Table`

Tập lệnh cơ bản

- **Get-Help**
- Hướng dẫn chung về các lệnh
- **Get-Command**
- Hướng dẫn cụ thể
- **Get-Member**
- Chi tiết về một đối tượng
- **Get-Module**
- Chi tiết về tập lệnh bên trong

Các thao tác trên dữ liệu

- **Compare**
- So sánh
- **Foreach**
- Duyệt qua từng thành phần
- **Group**
- Nhóm dữ liệu
- **Select**
- Chọn lựa một số thuộc tính
- **Sort**
- Sắp xếp các đối tượng
- **Tee**
- Copy dữ liệu
- **Where**
- Điều kiện khi chọn lựa

Ví dụ quản trị truy cập USB

- Tạo file kịch bản “Block-USB.ps1”
- Powershell
- PS C:\> Set-ExecutionPolicy Unrestricted
- PS C:\> .\Block-USB.ps1 -Enable