All About Windows Firewalls w/ Powershell

A guide to Windows Firewall for Umsec.

Firewall Profiles

There are three different firewall profiles in Windows, “Public”, “Private”, and “Domain”. These are to be used when connected to different networks. The profiles each contain settings and rules.

View profiles
> Get-NetFirewallProfile

Enable a profile
> Set-NetFirewallProfile -Name <Private | Public | Domain> -Enabled <True | False>

Default Actions

A firewall profile has a default action for both inbound and outbound traffic. See Defaults.

Defaults

By default, the firewall will

- Allow all new outbound traffic
- Allows all established inbound traffic
- Allows traffic to programs configured in the “exception” list
- Allows traffic to ports in the “exceptions” list

You can easily change some of these defaults by modifying the firewall profiles that are enabled.
> Set-NetFirewallProfile -DefaultInboundAction Block

If you use the `Set-NetFirewallProfile` command without specifying a profile name (which you can do with -name), then only the enabled profiles will be modified.

Disable the firewall:

```
> Set-NetFirewallProfile -Enabled false
```

This functions by disabling all 3 profiles at once.

Settings

By modifying global firewall settings (which apply to any and all profiles), you can change firewall behaviour. See Get-NetFirewallSettings. Some defaults are:

- Stateful firewalling for TCP is enabled (EnableStatefulFtp)
- DHCP is exempt from all firewall rules (Exemptions: Dhcp)
- On a server, ActiveProfile will say “NotApplicable”, meaning all profiles are active.

Some Default Rules

The following are some default rules are observed on new Windows 10 installs. It is recommended that you disable the rules instead of deleting them. Since default rules often have bizarre names, the display name is shown instead.

Allowed outbound traffic

Display Name	Profile	Action	Note

Allowed inbound traffic

Display Name	Profile	Action	Note
Java(TM) Platform SE binary	Private	Allow all incoming tcp and udp (two different rules)	If you need Java, please disable this rule.
Groove Music	Private, Domain	Allow all traffic	Disable this (wtf Microsoft)
Firefox (C:\Program Files\Mozilla Firefox)	Private	Allow all traffic	Why would Firefox need to listen?.

Powershell

For a list of all commands:

```
> Get-Command *NetFirewall*
```

The major objects are:

Profile	The three possible firewall chains, Public, Private, Domain.
Rule	Profiles contain rules.
Setting	Global Firewall settings that apply to all profiles

Firewall rules can be modified by extra commands that do not apply to the other objects: Copy-NetFirewallRule, Disable-NetFirewallRule, Enable-NetFirewallRule, Remove-NetFirewallRule, Rename-NetFirewallRule, Show-NetFirewallRule. These all take the rule name as an argument.

Here's a few quick examples:

Allow a Windows host to be pinged

> New-NetFirewallRule -DisplayName "Allow inbound ICMPv4" -Direction Inbound -Protocol

ICMPv4 -IcmpType 8 -Action Allow

Logging

Firewalls can create a logging event when they allow or block traffic. You can use this as a way to look for malicious traffic.

By default, nothing is logged. Enable the logs with
> Set-NetFirewallProfile -LogBlocked True
Or to log allowed traffic (my produce many logging events!)
> Set-NetFirewallProfile -LogAllowed True

Once logs are enabled, a log file will be created at `%systemroot%\system32\LogFiles\Firewall\pfirewall.log`, unless you change the settings. Note that only 4MB of logs will be retained at a time unless you change the `LogMaxSizeKilobytes` setting of the firewall profile.

Logs of traffic are not set to WinEvent. However, there are WinEvent logs when the firewall is changed or modified.

Firewall Rules

All Windows Firewall rules have:

- A name, which can be used to identify the rule in Powershell commands
- A display name, usually a few words
- A description
- The Enabled property
- A group
- A direction, either “inbound” or “outbound”
- Action, either “accept” or “block”
- Filters, which define which traffic is blocked or allowed. Address, (Windows) Service, Application, Interface, InterfaceType, Port (which includes network protocol), and Security (deals with IPSEC-enabled traffic).

Specific rules will usually require specify filters to be created.

Listing Firewall Rules

You can list firewall rules with
> Get-NetFirewallRule

The Get-FirewallRule command does not include information on filters by default. This means that to really understand what a firewall rule does, the Show-NetFirewallRule command will be required.

The look for rules with a specific display name or description, use the -DisplayName or -Description arguments with wildcards. Here is an example about finding all rules for Java applications:
> Get-NetFirewallRule -DisplayName “*java*”

Rule Details

The Show-NetFirewallRule automatically pipes the output of Get-NetFirewallRule though filter viewing commands, so that all the filters attached to a rule can actually be seen.

A firewall rule

```
> Show-NetFirewallRule | where {$_.enabled -eq 'true' -AND $_.direction
      -eq 'Outbound'}
```

Creating New Rules

Create a new firewall rule with
> New-NetFirewallRule -Name <name> -DisplayName <name> -Action <block | allow>
-Direction <inbound | outbound>

Other options
-Program <exe path> # Refer to a program by path in the rule
-Protocol <TCP | UDP | ANY> # the network protocol to which the rule applies
-LocalPort <port> # the port on this machine used by traffic. Protocol must be set to TCP or UDP, so you may need multiple rules to get both.
-RemotePort <port>
-RemoteAddress <address (optionally with cidr)> # seperate many addresses with commas

You can also edit existing firewall rules with many of the same options as above:
> Set-NetFirewallRule

IPSEC

Windows Firewall has the ability to authenticate individual network connections using IPSEC and Kerberos. This can be used to tie low-level network traffic with a domain identity.

Recommendations

What Windows ports can we block for incoming traffic?

Since Windows opens so many damn ports by default, we need to know what incoming traffic we can restrict without breaking things.

Port	Service	Status
50, 500, 4500 UDP	IPSEC	Block unless using ipsec within the domain
53 UDP	DNS	If server is used for DNS, **do not block**
67 UDP	DHCP	If server is used for DHCP, **do not block**
135, 593 TCP/UDP	RPC	If domain-connected, restrict to local DC. If on the DC or cert authority, allow local networks. Otherwise, block.
137, 138, 139 TCP/UDP	Netbios	Not necessary in 2019, block access
389, 636 TCP	LDAP	Necessary on DC
445 TCP	SMB, remote named pipes	SMB is mostly used for file sharing. If the server is not supposed to be hosting file shares, block access.
1801, 2101 TCP	MSMQ	Can probably block
2179 TCP	Hyper-V management	Block unless you need to remotely manage a HyperV server
3389 TCP	RDP	If RDP is necessary for local management but not for scoring, restrict to local network.
5985, 5986 TCP	Windows Remote	Best to ignore these, if they

	Management	are present than you will break stuff by blocking them

References

https://medium.com/@cryps1s/endpoint-isolation-with-the-windows-firewall-462a795f4cfb

https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows

UMCST Firewall

- TCP 88 (Kerberos Key Distribution Center)
- TCP 135 (Remote Procedure Call)
- TCP 139 (NetBIOS Session Service)
- TCP 389 (LDAP)
- TCP 445 (SMB, Net Logon)
- UDP 53 (DNS)
- UDP 389 (LDAP, DC Locator, Net Logon)
- TCP 49152-65535 (Randomly allocated high TCP ports)

- TCP 3389 (RDP)
- TCP 5985 (WinRM)
- TCP 5986 (WinRM)