Firewall из командной строки

Настройка брандмауэра windows из командной строки

ПРИМЕР
```
 PS C:\Windows\system32> netsh advfirewall firewall add rule name="HTTP-block" protocol=TCP localport=4427 action=block dir=IN remoteip=87.255.33.131

 netsh advfirewall firewall show rule name="HTTP-block"
 netsh advfirewall firewall delete rule name="HTTP-block"
```

В Windows server 2008 (R2), а также в обычных Windows vista, 7, 8 есть встроенный брандмауэр (firewall). В этой статье расмотрим несколько примеров как создавать правила из командной строки, также эти команды можно использовать при написании своих пакетных сценариев cmd, bat, powershell.

Все команды нужно выполнять из командной строки cmd запущенной с правами администратора.

Включение, выключение

Включить брандмауэр:

```
netsh advfirewall set allprofiles state on
```

Выключить брандмауэр:

```
netsh advfirewall set allprofiles state off
```

Включение отдельных профилей:

```
netsh advfirewall set domainprofile state on
netsh advfirewall set privateprofile state on
netsh advfirewall set publicprofile state on
```

Выключение отдельных профилей:

```
netsh advfirewall set domainprofile state off
netsh advfirewall set privateprofile state off
netsh advfirewall set publicprofile state off
```

Запретить все входящие соединения и разрешить все исходящие:

```
netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound
```

Правила на порты

Разрешить входящие TCP и UDP соединения для 80 порта:

```
netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=allow dir=IN
netsh advfirewall firewall add rule name="HTTP" protocol=UDP localport=80 action=allow dir=IN
```

Запретить входящие на 80 порт:

```
netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=block dir=IN
netsh advfirewall firewall add rule name="HTTP" protocol=UDP localport=80 action=block dir=IN
```

Открыть диапозон портов для исходящего UDP трафика

```
netsh advfirewall firewall add rule name="Port range" protocol=UDP localport=5000-5100 action=allow dir=OUT
```

Удалять правила можно по имени

```
netsh advfirewall firewall delete rule name="HTTP"
```

Ограничения по IP адресам

Правила можно ограничивать для работы только с одним ip:

```
netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=allow dir=IN remoteip=192.168.0.1
```

Или ограничивать по подсетями причем можно использовать разный синтаксис:

```
netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=block dir=IN remoteip=192.168.0.0/24
netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=allow dir=IN
```

```
remoteip=192.168.0.50-192.168.0.70
netsh advfirewall firewall add rule name="HTTP" protocol=TCP
localport=80 action=block dir=IN remoteip=localsubnet
```

Правила для приложений

Разрешить соединения для программы MyApp.exe

```
 netsh advfirewall firewall add rule name="My Application"
dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes
```

Комбинирования параметров

Параметры можно соединять в довольно сложные цепочки:

```
netsh advfirewall firewall add rule name="My Application"
dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes
remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain
```

В данном случае мы создали правило для программы, которое работает при если компьютер подключен к доменну организации (profile=domain) и определенны три диапозона ip адресов.

Подробней о настройках брандмауэра можно прочитать на сайте микрософта там же есть отличия от сторого синтаксиса который использовался на Windows XP и Windows server 2003:

http://support.microsoft.com/kb/947709

Часть примеров были взяты из статьи на английском языке:

http://itblog.gr/213/configuring-windows-firewall-from-the-command-line/