Article: Blocking Bad Hosts (CLI Version)
Date: 02/03/2012
Posted by: HeelpBook Staff
Source: Link
Permalink: Link

Microsoft Windows – Blocking Bad Hosts (Command Line Version)

In this article you will learn how to block bad hosts (client) from connecting to your workstation / server using ipsec filtering rules.

By following the steps below, you will be able to create a ***new policy*** and manage the filter lists and actions. The goal here will be to put all these pieces together into a nice tidy package that is fully automated.

The policy you create in this tutorial will not be applied to the system until you "**Assign**" the policy in **Step 6**.

As long as the policy is not assigned, you can safely ***edit, add, remove***, etc. rules and sets to the policy without affecting the system. ***Note: double and triple check your sets to ensure you do not block legitimate traffic before assigning the policy.***

To begin this tutorial, open the command prompt. If you don't know how, you probably shouldn't be doing this.

All commands meant to be typed are in ***italics***.

Step 1: Create IP Security Policy

```
netsh ipsec static add policy description="This policy blocks all traffic to
hosts/nets associated with it."
```

Step 2: Create an IP Filter List

```
netsh ipsec static add filterlist description="This filter list contains hosts
and networks known to host malware, criminal activity, etc."
```

Step 3: Create IP Filters and Associate them with the Filter List (Repeat this step until all hosts you wish to block have been entered)

Single IP (**10.254.254.254/32**)

```
netsh ipsec static add filter filterlist="Bad Hosts" srcaddr=10.254.254.254
dstaddr=any description="John Smith. 12/31/2015. Brute force logon attempts to:
SERVER01"
```

Subnet (**10.254.254.0/24**)

```
netsh ipsec static add filter filterlist="Bad Hosts" srcaddr=10.254.254.0
dstaddr=any srcmask=24 description="John Smith. 12/31/2015. Brute force logon
attempts to: SERVER01"
```

Network Range (**10.254.254.2-10**)

```
netsh ipsec static add filter filterlist="Bad Hosts" srcaddr=10.254.254.2-
10.254.254.15 dstaddr=any description="John Smith. 12/31/2015. Brute force logon
attempts to: SERVER01"
```

Step 4: Create a Filter Action

```
netsh ipsec static add filteraction description="This action blocks all
traffic." action=block
```

Step 5: Create Policy Rule to apply Filter Action to Filter List

```
netsh ipsec static add rule policy="Blocked Traffic" filterlist="Bad Hosts"
filteraction="Block All Traffic" activate=yes
```

Step 6: Assigning (and un-assigning) the Policy

This step will apply all the settings you have created up to this point. Double and triple check that you did not enter a valid host or network or it will be blocked. If fact, if you have any doubts in your mind, do not do this step until another person (***who knows what they are doing***) looks over your work too!

Note: This is one place MS will not give you a little "***are you sure you want to do this***" type of warning.

As soon as you assign the policy, it is done.

Assign

```
netsh ipsec static set policy name="Blocked Traffic" assign=yes
```

Un-assign

```
netsh ipsec static set policy assign=no
```