Windows Firewall with Advanced Security

Table of Contents

Configuring Advanced Settings Wizard.................................................................................. 2
Windows Firewall Advantages ................................................................................................. 3
Windows Firewall Disadvantages ............................................................................................... 6
Windows Firewall Configurations ............................................................................................ 8
Windows Firewall Advanced Security Netsh ........................................................................... 9
Windows Firewall Advanced Security PowerShell ................................................................. 10
Netsh vs. PowerShell ............................................................................................................... 11
Notices .................................................................................................................................. 12
**015 So, in this particular case, we're adding a rule.
Windows Firewall Advantages

Provides very granular customization of application and network behavior

Supports defense-in-depth
  • An action might be allowed on the network, but not on this particular system.

Consistency! One of the few things that is exactly the same between Windows 7, Windows 8, and Server 2012.

**016 We’ll take a look at the advanced firewall settings a little bit more in a moment. You can be as granular as you want to be, so as in-depth or at any level. You can be low level or high level when it comes to rule sets. Yes?

Student: I thought that was really nice. You could get on and talk about a specific port. Now, my question is can I have a rule that says if this specific port-- if someone tries to connect to it, I’d like to go and log it.

Mark Williams: Mm-hmm.

Student: Okay.
Mark Williams: Yep. So, you can create a rule that would be effectively a deny rule. And then you can say here’s what I want to do, deny it, but put an entry in the log.

Student: Okay.

Mark Williams: Mm-hmm.

Student: The second question related to that is can I use rules to limit the unassigned ports? Know how you have your assigned ones, if I’m trying to manage all the ports and there’s-- I mean there’s tons of them.

Mark Williams: There’s sixty-five thousand plus.

Student: Right. So, if I can squeeze them down to a smaller area, that's fewer for me to monitor and also reduces the overhead on my machine.

Mark Williams: Well, one thing to note-- and I probably should have said this earlier. One thing to note is the default posture is deny. So, if I put in a rule to allow port eighty, and that's the only rule I have in the inbound rule set, allow port eighty in, and I get rid of all the other inbound allows, then everything else, by default, is going to be shut down.

So, I don’t really-- I can be specific and put a deny rule in that says if it's between port five thousand and five thousand, one hundred and twenty-- maybe that’s the set that I've
identified as absolutely not acceptable, I could have a rule that says, if it’s in that range of ports do not allow it. I could have rule sets that are-- if it’s from a particular IP address or a block of IP addresses, I can say explicitly, do not allow this and then have it logged as well. But the default posture is, if it’s not allowed, if it’s not explicitly allowed, then it's implicitly denied. All right? So, yes sir?

Student: When you say on your machine allow remote desktop connections, it's going to set the rule for that automatically?

Mark Williams: Yep. There are a number of configurations that will go in and modify the firewall behind the scenes for us, yeah.

Student: Okay. Thanks.

Mark Williams: One of the cool things about Windows firewall is consistency. You guys are probably aware, when you go from one flavor of OS to another flavor of OS within Windows, things don't look or operate exactly the same way. The firewall is one of those areas where Windows 7, Windows 8, Server 2012 looks the same way, feels the same way, is the same way. So that's kind of nice about it.
Windows Firewall Disadvantages

More than a bit of “know how” is required to go beyond the basics.

Misconfigured rules could create a denial of service.

Misconfigured rules could allow unauthorized applications to run and users access.

**017 Disadvantages, it takes more than a bit of know how. It does take a bit of intelligence and understanding to create the proper rules for the firewall. And that's not just Windows firewall. That's all firewalls, in general.

Often times, because people, administrators, do not necessarily understand what they're doing, they often times end up opening up the firewall with these big, gaping holes. And one of the things that I like to point out to people that every opening through a firewall, even if it's a small one, but every opening through a firewall is a potential point of ingress and attack for you.
So, it would be better for us if we knew a little bit more, if we had a better understanding of what we were trying to accomplish. And then I could open up fewer holes and smaller more precision holes to allow the appropriate tasks.

So, they say that more than a bit of know how is required. Yes, but that's with any firewall that's out there. That's not just Windows firewall. Actually, these are all issues with all firewalls.

Misconfiguration could either allow or deny things that you don't want to allow or deny. Right? So, those are some of the disadvantages of any firewall.
Windows Firewall Configurations

Turned **on by default**

Can create profiles for Home or Work (Private) and Public networks

![Control Panel](control_panel_icon) → **Control Panel** → Type **firewall** in the search window

To change settings, select Allow a program or feature through Windows Firewall.

**018** The configuration, we don't have to worry about turning it on. It is on by default. I did say that we can set up different rules for different profiles. Right? Excuse me. And we've already kind of explored how we go through and allow programs and features through the firewall.
Netsh command line is the same with
- Windows 7, 8, and Server 2008

**Netsh advfirewall** is the command line tool.

**019 Now the GUI is nice, but I can also configure the firewall through command line, as well. Net shell, Net shell, many administrators are probably familiar with the Net shell utility. It gives a lot of capabilities. Net shell advanced firewall, if I do Net shell advanced firewall, as we're showing you in the display, with the question mark, it is going to give me help. It tells me what are some of the options available to us.

So, we'll give you some of the basic commands in Net shell that you can use. And our goal here is not to help you understand the syntax. Our goal
is just to show you the same types of things we could do in the GUI, we can also do with actually multiple different command tools.

Windows Firewall Advanced Security PowerShell

Windows Firewall Advanced Security PowerShell

Object-oriented cmdlets in Server 2008 and Server 2012 make it easier to manage policies and network connections through PowerShell.

Netsh is still available on Windows 7 and Server 2008.

On Server 2008, it is recommended that you transition to PowerShell as Netsh is likely to disappear in the future.

Netsh and PowerShell commands are similar… yet distinctly different between the two.

**020 PowerShell, we have an entire module on PowerShell that we will be discussing in another section. But we can configure our firewall with Net shell-- I’m sorry with PowerShell, as well. So, when we think about the differences between Net shell and PowerShell, Net shell is available on Windows 7 and Server 2008. But PowerShell is primarily what I’m going to be using if I’m talking about Windows 8 and Server 2012.**
They-- the commands accomplish the same task, effectively, but the syntax behind those commands actually is quite different.

**Netsh vs. PowerShell**

Adding a firewall rule to allow Telnet to listen on the network would look like

**Netsh**

```
netsh advfirewall firewall add rule name="Allow Inbound Telnet" dir=in program=%SystemRoot%\System32\tlntsvr.exe remoteip=localsubnet action=allow
```

**PowerShell**

```
New-NetFirewallRule -DisplayName “Allow Inbound Telnet” -Direction Inbound -Program %SystemRoot%\System32\tlntsvr.exe -RemoteAddress LocalSubnet -Action Allow
```

**021 And we’ll give you an example here. At the top, we’re showing you how to create a rule to allow Telnet to listen on the-- to be a listener on the program. So, the top command is the Net shell command. And the bottom command is the PowerShell command.

When I think about comparing these, I guess the only thing to keep in mind is they both get the same job
done. You just have to figure out the syntax. One thought for us with both of them, scripting. I can script either one of these in order to get the job done. Right? So, we have more on PowerShell coming up.

Actually we have a lot of PowerShell configuration commands that we will be discussing how to configure the firewall through PowerShell in module eight.

Notices

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.