|  |  |
| --- | --- |
|  | **I-ISMS Implementation Revision** 1 |

**NP Factory, Ltd.**

**Factory Floor**

**Industrial Information Security Management System**

Guide to conducting Windows Firewall hardening

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **I-ISMS Implementation Revision** 1 (1) | **Industrial Information Security Management System**  Guide to conducting Windows Firewall hardening  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**IISMS**

PRIVATE

|  |  |
| --- | --- |
| Document1  Version: 1 Revision 1  Pages: 3 | Path: Document1  Keywords: firewall, hardening, vulnerability, mitigate, remote  Last Saved by on 1/1/1601 12:00 AM |
|  | **NP Factory, Ltd.**  [Company Address]  Factory Floor  I-ISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

Provides high-level guidance on how to configure the Windows Firewall to provide a greater level of security from attack and controlled communications within the LAN.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 13-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 3](#_Toc461537592)

[2 Overview 3](#_Toc461537593)

[1.1 BEWARE! multi-protocol applications 3](#_Toc461537594)

[1.2 Advanced Firewall Configuration Guide 3](#_Toc461537595)

[3 Getting Started 3](#_Toc461537596)

[1.3 Finding open ports (Zenmap/nmap) 3](#_Toc461537597)

[1.4 Launching Windows Firewall 3](#_Toc461537598)

[1.5 Configuration Backup 3](#_Toc461537599)

[1.6 Firewall activation 3](#_Toc461537600)

[4 Modification Methodology 3](#_Toc461537601)

[5 Firewall Configuration – Inbound Rules 3](#_Toc461537602)

[1.7 Remove “obvious” applications that do not need network access 3](#_Toc461537603)

[1.8 Remove Windows Sharing 3](#_Toc461537604)

[1.9 Remove Network Discovery 3](#_Toc461537605)

[1.10 Remote Remote Control 3](#_Toc461537606)

[1.11 Remove SNMP 3](#_Toc461537607)

[1.12 Remove Wi-Fi 3](#_Toc461537608)

[1.13 Remove Media Player / Sharing 3](#_Toc461537609)

[1.14 Removing peer-to-peer collaboration 3](#_Toc461537610)

[1.15 Removing other items 3](#_Toc461537611)

[1.16 Blocking applications 3](#_Toc461537612)

[1.17 Allowing applications 3](#_Toc461537613)

[1.18 Allowing applications with recipient restrictions 3](#_Toc461537614)

[1.19 Allowing specific protocols 3](#_Toc461537615)

[6 Firewall Configuration – Outbound Rules 3](#_Toc461537616)

[1.20 Remove “obvious” applications that do not need network access 3](#_Toc461537617)

[1.21 Removing existing rules 3](#_Toc461537618)

[7 Testing the Firewall Configuration 3](#_Toc461537619)

Figures

**No table of figures entries found.**

# 

# Instructions

This page provides quick instructions for using this guide:

1. Carefully read through the Overview on page 7
2. Plan your intended network communications
3. Understand the Modification Methodology on page 8
4. Execute the Firewall modifications by following all subsequent sections
5. Add your own rules to this document as necessary

Finally, delete this page.

# 

# Overview

The Windows Firewall is a layer of defense that can control network traffic:

* Prevent specific types of communication, e.g. Modbus, HTTP, DNS, NetBIOS, Remote Desktop, etc.
* Allow only specific types of communication, e.g. DNS, HTTP, Modbus, Remote Desktop
* Allow/Prevent only when a specific target and/or source, e.g. accept Modbus when from IP address 1.2.3.4

Windows Firewall is quite powerful and if used properly can provide a significant layer of defense.

IMPORTANT! Before you start configuring Windows Firewall you MUST determine in advance:

* The traffic you will permit, and the traffic you will prevent
* The applications/system services that can connect to the network, and which cannot
* which other systems can the allowed protocols communicate with?

What are we aiming to achieve with Windows Firewall configuration?

* Prevent unauthorized applications on this PC from using the network
* Prevent authorized applications from unauthorized locations from communicating to this PC
* Make the computer appear to be unavailable to unauthorized computers

## BEWARE! multi-protocol applications

Beware, some applications support multiple protocols, e.g. SCADA systems support Modbus, Profinet, OPC, BACnet, and literally dozens of others. This can be a good thing. This can be a bad thing.

Should an application be allowed unlimited access to the network, like a SCADA?

* If so, then the permit the application in the firewall (see *Allowing applications*, below)
* If not, then permit the application and specify the protocol (see *Allowing specific protocols*, below)

## Advanced Firewall Configuration Guide

The United States Department of Defense provides a STIG with very specific instructions for hardening Windows based systems using the Windows Firewall. Some elements are carried into this guide.

<http://iase.disa.mil/stigs/Pages/index.aspx>

# Modification Methodology

To avoid the misconfiguration of your computer system and essentially breaking all communications capabilities, it is recommended that you follow these steps:

1. Backup the firewall configuration
2. Make a few changes
3. Reboot
4. Test the general behavior of the computer and the applications that must have network connectivity
5. If problems arise, restore a firewall backup

# Getting Started

Talk to your IT dept. to see if they already have a Windows Firewall policy; if so, request a copy and discuss with them to determine which parts should apply to industrial automation. Seek expertise if it is available.

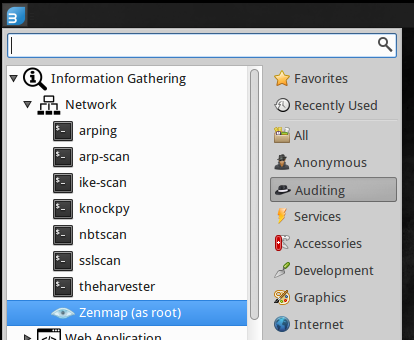
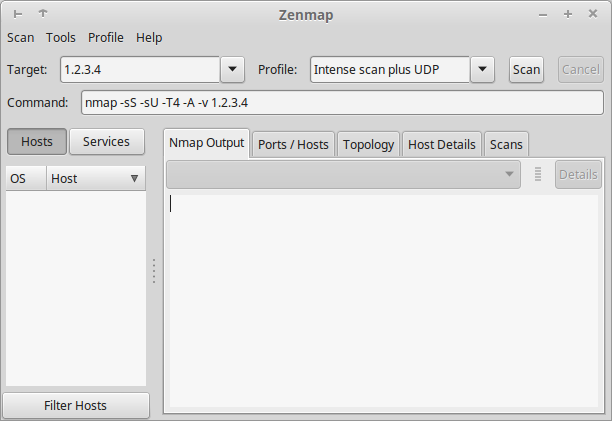
Windows Firewall is quite powerful, and the options available may vary slightly in each variation of Windows operating system. This document assumes Windows 7.

## Finding open ports (Zenmap/nmap)

Before modifying the Windows Firewall, we should first determine what traffic can traverse through the firewall. The easiest way to do this is by using a port-scanner.

Using a different computer, launch “Zenmap” from the BackBox VM – or alternatively you can download it to a separate Windows PC from here: <https://nmap.org/download.html> (search for the “Microsoft Windows binaries” section).

The following instructions show Zenmap (the nmap GUI) with screenshots from Linux:

1. Launch Zenmap (BackBox O/S shown):   
   
2. Enter the IP address of the Target and specify an *Intense scan plus UDP*:   
   
3. Click “Scan” and wait. This may take several minutes.
4. Save the output file by clicking SAVE > Save Scan.
5. Review the results to determine which ports are open; sometimes nmap can determine the application and version that is listening. This is useful information to an attacker.

The nmap findings can help you to identify if more applications are listening for connections than what you expect, and that the right applications are listening.

## Launching Windows Firewall

As a system administrator:

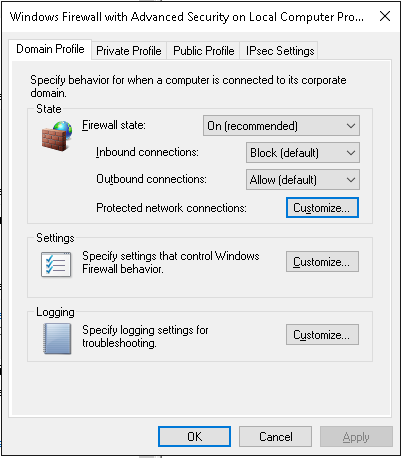
1. Open Control Panel > System and Security > Windows Firewall
2. Click “Advanced settings” in the left-side navigation bar
3. The main firewall configuration application will open.

## Configuration Backup

Before we make any changes to the firewall we will take a backup of the configuration that can be restored:

1. In the left-side navigation right-click on the “Windows Firewall with Advanced Security on Local Computer” node and choose “Export Policy”.
2. Specify a filename and location to save the \*.WFW file.

## Firewall activation

1. In the left-side navigation right-click on the “Windows Firewall with Advanced Security on Local Computer” node and choose Properties.
2. A tabbed-dialog will open
3. Select the “Domain Profile” tab; this ONLY applies if the computer is within a domain. Set the options as follows:
   1. Main settings:   
      
   2. Click “Customize” beside “Protected network connections” and ensure all network adapters are selected.
   3. Click “Customize” beside “Settings” and then:
      1. enable notifications
      2. block unicast response to multicast traffic (unless required by a needed protocol)
      3. Click OK to save and close the window.
   4. Click “Customize” beside the “Logging” option and then:
      1. ensure the log size is at least 4096 kb; also check the location of the log file is acceptable.
      2. Log dropped packets becomes “Yes”
      3. Log successful connections becomes “Yes”
      4. Click OK to save and close the window.
4. Click the “Private Profile” tab and repeat steps 3.a to 3.c.iii
5. Click the “Public Profile” tab and repeat steps 3.a to 3.c.iii
6. Click the “IPsec Settings” tab and select the “None” option at the bottom, unless IPSEC is permitted.
7. Click OK to save and close the dialog.

# Firewall Configuration – Inbound Rules

Inbound rules are evaluated when traffic reaches the computer from the network/internet. Such information may be to establish a connection with a hosted application, e.g. web-server, OPC Server, or database etc.

## Remove “obvious” applications that do not need network access

The following steps will specify which installed applications are permitted to use the network:

1. Click the “Inbound Rules” to view the rules that permit incoming traffic.  
   **Note**: by default, Windows allows a lot of services to access network resources.
2. Remove obvious applications that should not have network access, e.g. “Notepad” or “Solitaire” etc.
3. If you see applications that you are not familiar with, or have never heard of before, then now is a good time to research them.

## Remove Windows Sharing

Does the computer share resources such as a files/folders or printers? Hopefully not, because that’s what servers are for. Unless required, remove all entries that start with “File and Printer Sharing”.

## Remove Network Discovery

Unless absolutely necessary to *discover* resources on the network, of which there really shouldn’t be a need, you should disable discovery since it can present greater exposure to vulnerabilities. Locate and delete all entries starting with “Network Discovery”; there could be a lot.

## Remote Control

Unless absolutely necessary, remove any capability to remotely control the computer. Locate and delete any entry starting with “Remote Assistance” or “Remote Desktop”.

## Remove SNMP

Unless absolutely necessary, an SNMP service may expose sensitive information over the network about the computer system, or accept requests from other devices for logging purposes. This poses a security risk of potential vulnerabilities. Locate and delete any entry starting with “SNMP”.

## Remove Wi-Fi

Unless absolutely necessary, do not allow the direct discovery and utilization of Wi-Fi networks. Locate and delete any entry starting with “Wi-Fi Direct”.

## Remove Media Player / Sharing

Unless absolutely necessary, and it really shouldn’t be, remove any entry starting with “Windows Media Player”.

## Removing peer-to-peer collaboration

Unless absolutely necessary for peer-to-peer communications, delete any entry starting with “Windows Peer to Peer Collaboration”.

## Removing other items

As previously stated, there are a lot of applications already permitted by the default Windows policy scheme.

If in doubt, right-click and export the setting so that you can import it back later.

## Blocking applications

If there are any applications that \*might\* use network resources, but should never have the ability to do so, then block them as follows:

1. Right-click the *Inbound Rules* node and choose *New Rule*, and then:
   1. Select “Program” from the selection and then click NEXT.
   2. Browse to the program executable and choose NEXT.
   3. Select “Block the connection” and choose NEXT.
   4. The rule should apply to Domain, Private, and Public profiles.
   5. Give the rule a name and [optional] description and click FINISH.
2. Right-click the *Outbound Rules* node and choose *New Rule* and then repeat steps 1.1 to 1.5 above.

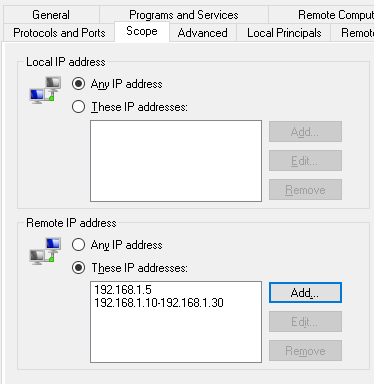
## Allowing applications

Here, we can allow specific applications access to the network without any restriction to which protocols they use;

1. If the application is a server, e.g. Database, Web-Server, OPC Server, etc. then right-click the *Inbound Rules* node and choose *New Rule*, and then:
   1. Select “Program” from the selection and then click NEXT.
   2. Browse to the program executable and choose NEXT.
   3. Select “Allow the connection” and choose NEXT.
   4. The rule should apply to Domain, Private, and Public profiles.
   5. Give the rule a name and [optional] description and click FINISH.

## Allowing applications with recipient restrictions

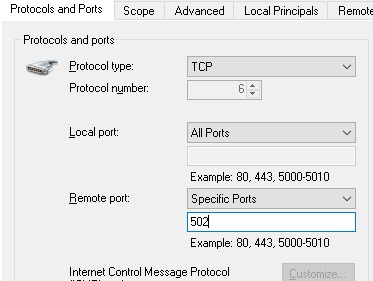
Here, we can allow specific applications access to the network while restricting which other devices they can communicate with.

1. If the application is a server, e.g. Database, Web-Server, OPC Server, etc. then right-click the *Inbound Rules* node and choose *New Rule*, and then:
   1. Select “Program” from the selection and then click NEXT.
   2. Browse to the program executable and choose NEXT.
   3. Select “Allow the connection” and choose NEXT.
   4. The rule should apply to Domain, Private, and Public profiles.
   5. Give the rule a name and [optional] description and click FINISH.
   6. Locate the rule in the list and then open its Properties.
   7. Click the *Scope* tab and then enter the IP addresses of the other computers/devices that are allowed/blocked, e.g.:   
      
   8. If there are specific users that must be logged in for the application to have network access (e.g. prevent normal users from using the network with the selected application) then do this:
      1. If the application will make outbound connections, then:
         1. Click “Local Principles” tab
         2. Add the appropriate users to the “Authorized users” list
      2. If the application will receive connections from remote computers/users, then:
         1. Click “Remote Users” tab
         2. Add the appropriate users to the “Authorized users” list.
   9. Note: The “Remote Computers” tab is useful if you plan to link to computers managed in a Domain.
   10. Click OK to save and close the dialog.
2. If the application is a Client that is making a connection to an external server then right-click the *Outbound Rules* node and choose *New Rule*, and then:
   1. Repeat steps 1.1 through 1.10 above.

## Allowing specific protocols

If an application supports multiple protocols, then we don’t want to blanket allow all protocols. For example, we may permit our SCADA to only use Modbus TCP through our firewall.

The following steps will restrict the protocol use for an application:

1. If the application is a server, e.g. Database, Web-Server, OPC Server, etc. then right-click the *Inbound Rules* node and choose *New Rule*, and then:
   1. Select “Program” from the selection and then click NEXT.
   2. Browse to the program executable and choose NEXT.
   3. Select “Allow the connection” and choose NEXT.
   4. The rule should apply to Domain, Private, and Public profiles.
   5. Give the rule a name and [optional] description and click FINISH.
   6. Locate the rule in the list and then open its Properties.
   7. Click the *Protocols and Ports* tab and complete the fields as required by the protocol.
2. If the application is a Client that is making a connection to an external server then right-click the *Outbound Rules* node and choose *New Rule*, and then:
   1. Perform steps 1.a through 1.f, above.
   2. Click the *Protocols and Ports* tab and complete the fields as required by the protocol.  
      The following screenshot shows a typical Modbus configuration for an application connecting to a PLC:   
      
3. Click OK to save and close the rule.

Note: you can combine these steps with the steps defined in *Allowing applications with recipient restrictions*, above.

# Firewall Configuration – Outbound Rules

Outbound rules are evaluated when an application attempts to send information over the network. Ideally, only applications you trust will be allowed to communicate. Just as before, it is advisable to have a map of your network infrastructure with a relationship diagram showing which devices/computers should be allowed to communicate with each other.

## Remove “obvious” applications that do not need network access

The following steps will specify which installed applications are permitted to use the network:

1. Click the “Outbound Rules” to view the rules that permit incoming traffic.  
   **Note**: by default, Windows allows a lot of services to access network resources.
2. Remove obvious applications that should not have network access, e.g. “Notepad” or “Solitaire” etc.
3. If you see applications that you are not familiar with, or have never heard of before, then now is a good time to research them.

## Removing existing rules

By default, the Windows Firewall contains a large list of rules that permit many applications and core operating system services to communicate over the network. Depending on your hardening needs for the specific computer this could pose a security problem. Generally speaking, only permit REQUIRED services.

As before, be sure to back-up your configuration before making any changes. See *Modification Methodology*, above.

The goal here is to reduce the rules to the fewest number needed.

Go through the same processes as described by all sub-sections of *Firewall Configuration – Inbound Rules*, above.

# Testing the Firewall Configuration

Firewalls are complicated because they manage the traffic to/from the operating system as well as applications. Therefore, the testing of the firewall can be a little time-consuming as many elements may require specific testing.

This section provides some general tips on how to test the firewall.

First, use Zenmap/nmap (see *Finding open ports (Zenmap/nmap)*, above) to identify open ports and to verify that the ONLY open-ports are those that you expect. Unexpected ports should be researched and shutdown.

Second, use Windows as a user:

* Can you get online?
* Can you browse the network or access network resources (shares/printers)?

Third, launch your applications HOSTED on the PC and make sure they work.

Fourth, from a different computer/device, establish connections to shared resources that you expect to be available.