Windows Firewall Applied

Rob Vinson – ISPO Security Architect
Dan Metzler – ITS-EI Windows Systems Architect

March 2012
Agenda

- Basic concepts – a quick review
- Firewall Profiles
- Network Location Awareness (NLA)
- Rule generation and validation

March 2012
Stateful Firewall - Basics

- Rules are for the traffic that initiates a connection/session
- Subsequent traffic belonging to that connection/session is allowed through

Example allow rule for HTTP: 10.0.0.1 → 10.0.0.2:80

The response traffic 10.0.0.2:80 → 10.0.0.1 is automatically allowed
Application Firewall - Basics

Based on the application/program creating the network communication socket.

Example allow rule:

any ➔ instant_messenger.exe

Allows any host to communicate to ports opened by instant_messenger.exe
Profiles

- Allow different firewall rules to be applied in different environments

- Domain – Corporate Environment
- Private – Trusted/home network
- Public – Coffee Shops, Airport, etc.
Settings - Profiles

- Allow outbound connections by default.
- Inbound connections are allowed if there is an allow rule that matches the connection.
- Public profile – Network discovery is off.
How Profiles are Chosen

- Network Location Awareness (NLA)
- Domain Profile – Computer can reach Domain Controller
- Private/Public Profiles – Pop-up window asks which to apply

Rule Development - Tools

- Command line: netstat -noa

  - TCPView
  - Process Monitor
Rule Validation

- Verify that you can get an open port when you should, and don’t when you shouldn’t.

- Tools:
  - Logs, netcat, nmap (port scanners), telnet, web browser, etc.
Demo
Windows Firewall GPO
Agenda

- Managing Firewall GPOs
  - Tools
  - Concepts
- Troubleshooting Tools
- Things to Think About
- Strategy
Managing Firewall GPOs

Tools
Tools

- Group Policy Management Console (GPMC)
- Group Policy Editor (GPEdit)
- NetSH
- Powershell
NetSH (local and GPO)
Powershell

- **GroupPolicy Module**
  - Import-module GroupPolicy
  - New-GPO
  - Get-gpregistryvalue
  - New-gplink
  - Set-gpregistryvalue
  - Set-gppermissions
  - Remove-gpregistryvalue

- **Netsh**
  ```powershell
  $stream = [System.IO.StreamWriter] 'netshinput.txt'
  $stream.WriteLine('advfirewall')
  $stream.WriteLine('set store gpo=' + $domainfqdn + '\gponame')
  $stream.WriteLine('import myfirewallsettings.wfw')
  $stream.WriteLine('exit')
  $stream.Close()
  Get-content 'netshinput.txt' | netsh
  ```
Managing Firewall GPOs
Some Concepts
GPO Processing Order

- Local GPO
- Site
- Domain
- OU (Top to Bottom)
GPO Processing

- Some settings overwrite
- Some settings accumulate
Filtering

- Computer Group – only certain groups have permissions to apply the GPO

- WMI - If the filter evaluates to true the GPO applies

Examples

- Certain OS versions
  SELECT Version FROM Win32_OperatingSystem WHERE Version >= "6"

- Certain Server Features installed
  SELECT Name FROM Win32_ServerFeature WHERE Name = "Web Server (IIS)"

- Certain Program Installed
  SELECT Name FROM Win32_Product WHERE Name = "Cisco AnyConnect VPN Client"
Local GPO and Local Settings

- If you don’t block these, Domain GPO firewall rules and local settings are cumulative.

- If you want to prevent Domain GPOs from being overridden, then you have to block local settings and local GPO processing.

**Warning:** This significantly impacts the the number of rules required in Domain GPOs.
## Must Have Rules

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Domain</th>
<th>Allow</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Networking - Group Policy (LSASS-Out)</td>
<td>Domain</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Group Policy (NP-Out)</td>
<td>Domain</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Group Policy (TCP-Out)</td>
<td>Domain</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Internet Group Management Protocol (IGMP-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Internet Group Management Protocol (IGMP-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - IPv6 (IPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - IPv6 (IPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Done (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Done (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Query (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Query (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Report (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Report (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Report v2 (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Multicast Listener Report v2 (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Neighbor Discovery Advertisement (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Neighbor Discovery Solicitation (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Packet Too Big (ICMPv6-In)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
<tr>
<td>Core Networking - Packet Too Big (ICMPv6-Out)</td>
<td>All</td>
<td>Allow</td>
<td>No</td>
</tr>
</tbody>
</table>
Firewall Rule Precedence

- Authentication Bypass
- Block Rule
- Allow Rule
- Default Rule
Troubleshooting
Netstat

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5357</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>528</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>280</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49160</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>520</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>844</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5357</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>528</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>280</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49160</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>520</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>844</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5357</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>528</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>280</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49160</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>520</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>844</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5357</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>528</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>280</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49160</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>520</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>844</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5357</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>444</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>528</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>280</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49160</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>520</td>
</tr>
</tbody>
</table>
Firewall logging
Event Viewer
Event Viewer (Cont.)

Event 5152, Microsoft Windows security auditing.

The Windows Filtering Platform has blocked a packet.

Application Information:
- Process ID: 9544
- Application Name: \device\harddiskvolume1\windows\system32\telnet.exe

Network Information:
- Direction: Outbound
- Source Address: 172.31.6.133
- Source Port: 57715
- Destination Address: 128.255.56.81
- Destination Port: 34523
- Protocol: 6

Log Name: Security
Source: Microsoft Windows security
Logged: 3/11/2012 9:10:04 PM
Event ID: 5152
Task Category: Filtering Platform Packet Drop
Level: Information
Keywords: Audit Failure
User: N/A
Computer: ITS-SPA-056LT2.iowa.uiowa.edu
OpCode: Info
More Information: Event Log Online Help
Event Viewer (Cont.)
Event Viewer (Cont.)
Packet Sniffing (Netmon and Wireshark)
Windows Firewall with Advanced Security Snap-in
Things to Think About
It’s A Balance?

- Security requirements tend to drive the need for restricting traffic with firewall rules.
- Software requirements drive the need to allow traffic through the firewall.
Part of Software Deployment

- Installation time is when the firewall rule change happens.
- Vendor documentation is sparse with regard to firewall requirements
  - Common statements
    - “Allow the following ports both ways: x,y,z”
    - “Application uses the following ports both TCP and UDP: x,y,z”
Who Manages The Rules?

- Typically those who have admin permissions are likely the group that installs software.
- Often the owner, (not necessarily the user of the computer), determines who has admin rights, and who controls firewall rules.
- Security office implements policy that often dictates rules.
- Auditors may need to audit rules on occasion.
Strategy
Level Of Control
Loose Management Scenario

- Environment
  - End user has admin rights to the computer.
  - End user often installs software
  - Software installs often open up rules in the process of installing.

- IT only might add a few rules through GPO
Strict Management Scenario 1

- **Environment**
  - Users don’t have admin permissions:
  - IT controls local firewall settings
  - IT controls local gpo settings.
  - Users request software not firewall settings.

- IT might use GPOs or just manage settings locally.
Strict Management Scenario 2

- Environment
  - Users have admin permissions:
  - IT wants to manage firewall rules centrally.
  - Users need to request firewall rules.

- IT must use GPOs in this situation.
  - Disable local firewall settings
  - Disable local GPO processing
Strategy
Level Of Security
Default Security

- Inbound Default rule: Block
- Outbound Default rule: Allow
- Only Inbound exceptions must be defined.
High Security/High Maintenance

- Inbound Default rule: Block
- Outbound Default rule: Block
- All exceptions must be defined.
Account For Your Environment

- Inbound Exception Rules
  - Program or Service
  - Protocol
  - Local Ports
  - Remote Address Scope (Any, Campus, Trusted Nets)

- Outbound Exception Rules (High Security)
  - Program or Service
  - Protocol
  - Remote Ports (maybe)
  - Remote Address Scope (Any, Campus, Trusted Nets)
Questions?