How to configure Microsoft Windows firewalls for trusted scanning with Vulnerability Manager

Technical Articles ID: KB50878
Last Modified: 11/6/2012
Rated:
★★★★★

Environment

McAfee Vulnerability Manager 7.x

Microsoft Windows

Summary

For Vulnerability Manager to identify a Microsoft Windows host correctly, TCP ports **135** and **445** must be allowed from the IP address of the scan engine. Inbound ICMP access from the engine should be allowed as well. Supplying login credentials in the Vulnerability Manager credential manager allows the scan to authenticate to the system and properly identify it.

Networks using the Windows XP SP2 firewall must take extra steps to allow access by Vulnerability Manager. The quickest way to make Microsoft Windows XP SP2 firewall changes is to use a group policy within Active Directory.

Any of the methods below can be used to allow the Vulnerability Manager scan engines to scan client systems through the Microsoft Windows XP SP2 firewall while still protecting from outside threats.

Solution 1

Update Group Policy Objects in Active Directory
The Group Policy Management Console is the recommended way of updating Group Policy Objects in Active Directory. On a computer that is a member of the domain and has Windows XP SP2 installed, log in with an account that is a member of either the Domain Admins, Enterprise Admins, or Group Policy Creator Owners security groups.

1. Click **Start**, **Run**, type **mmc** and press ENTER.
2. Click **File**, **Add/Remove Snap-in**.
3. Click **Add** and select **Group Policy Object Editor**.
4. Click **Browse** and select the **Default Domain Policy**.
5. Navigate to **Computer Configuration**, **Administrative Templates**, **Network**, **Network Connections**, **Windows Firewall**.

6. Double-click **Allow remote administration exception**. This will bring up a dialog box for creating an exception.
7. Click **Enabled**.
8. In the **Allow unsolicited incoming messages from:** field, type the IP address of the Scan Engine that will be used. If multiple engines are used, a comma-separated list can be entered.

Solution 2

Use the Netsh command

This will enable the MVM engine to authenticate to the client computer, but will only enable that connection from the specified IP addresses.

1. Click **Start**, **Run**, type **cmd** and press ENTER.
2. Type **netsh firewall set service type = REMOTEADMIN mode = ENABLE scope = CUSTOM addresses = SCANRange** (Replace **SCANRange** with the IP address of the Foundstone Scan Engine. This range can be a single IP, comma-separated list or CIDR notation.)

The **netsh** command can be added to a startup script as demonstrated in the next method.

Solution 3

Modify Netfw.inf

If Active Directory cannot be used for creating the policy, modification of **Netfw.inf** can be done manually:

1. Navigate to: **\Windows\inf\Netfw.inf**.
2. Create a backup copy of the **Netfw.inf** file.
3. Right-click **Netfw.inf** and select **Open With**, **Notepad**.
4. Locate **[ICF.AddReg.StandardProfile]**.
5. Create a new line under **[ICF.AddReg.StandardProfile]** and type:

   NTLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\RemoteAdminSettings","Enabled",0x00010001,1

6. On a new line type:

   HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\RemoteAdminSettings","RemoteAddresses",0x00000000,SCANRange

   NOTE: Replace **SCANRange** with the IP or IP range of the scan engines. This can be a single IP, a comma-separated list or CIDR notation.

7. Locate **[ICF.AddReg.DomainProfile]**.
8. Create a new line under **[ICF.AddReg.DomainProfile]** and type:

   HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\RemoteAdminSettings","Enabled",0x00010001,1

9. On a new line type:

   HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\RemoteAdminSettings","RemoteAddresses",0x00000000,SCANRange

   NOTE: Replace **SCANRange** with the IP or IP range of the scan engines. This can be a single IP, a comma-separated list or CIDR notation.

10. Save and Exit the **Netfw.inf** file.
11. Restart the system for the changes to take effect.