Window Server Firewall Configuration

Windows Server Firewall

Windows Firewall is a stateful host firewall that drops all unsolicited incoming traffic. This behavior of Windows Firewall provides some protection from malicious users and programs that use unsolicited incoming traffic to attack computers.

For more information, see Microsoft documentation for details.

When you enable Windows Firewall on the servers, open all ports that the CCE solution components require.

Cisco provides a utility to automatically allow all traffic from Unified CCE applications on Windows Server. The utility can open ports for common third-party applications, that the contact center enterprise solution uses. The script reads the list of ports in the file `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml` and uses the directive to modify the firewall settings.

The utility allows all traffic from the applications, it adds the relevant applications to the list of excepted programs and services. When the excepted application runs, Windows Firewall monitors the ports on which the program listens and automatically adds those ports to the list of excepted traffic.

The script allows traffic from the third-party applications, by adding the application *port number* to the list of excepted traffic. Edit the `CiscoICMfwConfig_exc.xml` file to enable these ports.

Ports and Services that are enabled by default:

- 80/TCP and 443/TCP - HTTP and HTTPS (when the system installs IIS or TomCat [for Web Setup])
- Microsoft Remote Desktop
- File and Print Sharing Exception - see https://docs.microsoft.com/en-us/windows-server/storage/file-server/best-practices-analyzer/smb-open-file-sharing-ports.

Firewall inbound rules that are disabled by default:

- Core Networking for IPv6
- Core Networking - IPHTTPS for TCP
- Core Networking - Teredo for UDP
- Network Discovery for Private Profile
- Windows Remote Management - HTTP for domain, private, and public profiles

Service disabled by default:

- File Server Remote Management

Optional ports that you can open:

- 5900/TCP - VNC
- 5800/TCP - Java Viewer
- 21800/TCP - Tridia VNC Pro (encrypted remote control)
- 5631/TCP and 5632/UDP - pcAnywhere

Note You can edit the XML file to add port-based exceptions outside of this list.

For a complete list of port usage, see *Port Utilization Guide for Cisco Unified Contact Center Solutions*, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Cisco Firewall Configuration Utility Prerequisites

Install the following software before using the Firewall configuration utility:

1. For information on operating system, see the Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
2. Unified ICM/CCE components

Note If you install any more components after configuring the Windows Firewall, reconfigure the Windows Firewall. This process involves removing the previous configuration and rerunning the Windows Firewall configuration utility.

Run Cisco Firewall Configuration Utility

You can run the Cisco Firewall Configuration Utility either from the command line or from the Unified Contact Center Security Wizard.

Warning If you attempt to run this utility from a remote session, such as VNC, you can be "locked out" after the firewall starts. If possible, perform any firewall-related work at the computer because network connectivity can be severed for some remote applications.

Use the Cisco Firewall Configuration Utility on each server running a Unified ICM component. To use the utility, follow these steps:

Procedure

Step 1 Stop all application services.

Step 2 From a command prompt, run `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat`.

Step 3 When you first run the script, the script runs `configfirewall.bat`. The script then asks you to rerun the application using the same command. Rerun the script if instructed to do so.

Step 4 Click **OK**.

The script verifies that the Windows Firewall service is installed, then starts this service if it is not running.

The script then updates the firewall with the ports and services specified in the file `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`.

Step 5 Reboot the server.

Related Topics

Windows Firewall Configuration

Verify New Windows Firewall Settings

You can verify that the Unified ICM components and ports were added to the Windows Firewall exception list by following these steps:

Procedure

Step 1 Choose **Start** > **Windows Administrative Tools** and select **Windows Firewall with Advanced Security** when using Windows Server. Alternatively, choose **Start** > **Control Panel** > **System and Security** > **Windows Firewall**.

The Windows Firewall dialog box appears.

Step 2 Click the **Exceptions** tab. Then click the **Inbound and Outbound Rules** tab of the Windows Firewall dialog box for Windows Server.

Step 3 Scroll through the list of excepted applications. Several Unified ICM executables now appear on the list and any ports or services defined in the configuration file.

Windows Server Firewall Communication with Active Directory

Open the ports that the domain controllers (DCs) use for communication by LDAP and other protocols to ensure that Active Directory can communicate through your firewall.

Consult the Microsoft Knowledge Base article KB179442 for important information about configuring firewall for Domains and Trusts.

To establish secure communications between DCs and Unified ICM Services, define the following ports for outbound and inbound exceptions on the firewall:

- Ports that are already defined
- Variable ports (high ports) for use with Remote Procedure Calls (RPC)

Domain Controller Port Configuration

Define the following port definitions on *all* DCs within the demilitarized zone (DMZ) that can replicate to external DCs. Define the ports on all DCs in the domain.

Restrict FRS Traffic to Specific Static Port

For more information about restricting File Replication Service (FRS) traffic to a specific static port, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

Procedure

Step 1 Start **Registry Editor** (regedit.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters**.

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port Assignment**
- Value: **10000 (decimal)**

Restrict Active Directory Replication Traffic to Specific Port

For more information about restricting Active Directory replication traffic to a specific port, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

Procedure

Step 1 Start **Registry Editor** (regedit.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**.

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port**
- Value: **10001 (decimal)**

Configure Remote Procedure Call (RPC) Port Allocation

For more information about configuring RPC port allocation, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

Procedure

Step 1 Start **Registry Editor** (regedit.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc**

Step 3 Add the **Internet** key.

Step 4 Add the following registry values:

- Ports: **MULTI_SZ: 10002-10200**
- PortsInternetAvailable: **REG_SZ: Y**
- UseInternetPorts: **REG_SZ: Y**

Windows Firewall Ports

Consult the Microsoft Knowledge Base article KB179442 for a detailed description of the ports that are used to configure a firewall for domains and trusts.

Table 1: Windows Server Firewall Ports

Server Port	Protocol	Protocol	Service
135	TCP	RPC	RPC Connector Helper (machines connect to determine which high port to use)
137	TCP	UDP	NetBIOS Name

Server Port	Protocol	Protocol	Service
138		UDP	NetBIOS NetLogon and Browsing
139			NetBIOS Session
123		UDP	NTP
389	TCP		LDAP
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
42			Wins Replication
53	TCP	UDP	DNS
88	TCP	UDP	Kerberos
445	TCP	UDP	SMB over IP (Microsoft-DS)
10000	TCP		RPC NTFRS
10001	TCP		RPC NTDS
10002 to 10200	TCP		RPC - Dynamic High Open Ports
NA	ICMP		A layer 3 protocol suite in the TCP/IP suite. This is used in pings and traces. You can block echo replies by closing port 7.

Test Connectivity

To test connectivity and show the FRS configuration in Active Directory, use the Ntfrsult tool.

Procedure

From the command line, run the Windows File Replication utility: `Ntfrsutl version <server_name>`.

When communications between the domain controllers are configured properly, the Ntfrsutl output shows the FRS configuration in Active Directory.

Validate Connectivity

To validate connectivity between the domain controllers, use the Portqry tool.

To download Portqry utility and to learn more about it, see https://support.microsoft.com/en-in/help/310099/description-of-the-portqry-exe-command-line-utility.

Procedure

Step 1 Download the **PortQryV2.exe** and run the tool.

Step 2 Select the destination CD or PDC.

Step 3 Select **Domains and Trusts**.

Step 4 Use the response from PortQry to verify that the ports are open.

Consult the Microsoft Knowledge Base article KB832919 for more information about PortQry features and functionality.

CiscoICMfwConfig_exc.xml File

The CiscoICMfwConfig_exc.xml file is a standard XML file that contains the list of applications, services, and ports that the Cisco Firewall Script uses to modify the Windows Firewall. This modification ensures that the firewall works properly in the Unified ICM/Unified CCE environment.

The file consists of three main parts:

- **Services:** The services that are allowed access through the firewall.
- **Ports:** The ports for the firewall to open.

  This setting is conditional depending on the installation of IIS in the case of TCP/80 and TCP/443.
- **Applications:** The applications that are *not* allowed access through the firewall.

  The script automatically excludes all the applications listed in the `CiscoICMfwConfig_exc.xml` file.

Note The behavior of the Applications section is opposite to that of the other two sections in the file. The Ports and Services sections *allow* access, whereas the Application section *denies* access.

You can manually add more services or ports to the CiscoICMfwConfig_exc.xml file and rerun the script to reconfigure Windows Firewall. For example, to allow your **Jaguar** server connections from port 9000 (CORBA), add a line in the `<Ports>` section to open port 9000 on the Windows Firewall:

```
<Port Number="9000" Protocol="TCP" Name="CORBA" />.
```

Note This change is only needed if remote Jaguar administration is required. Usually, this change is not needed.

You can use **Windows Firewall with Advanced Security** to add or deny the ports or applications.

The file lists some commonly used ports as XML comments. You can quickly enable one of these ports by moving the port out of the comments to a place before the **</Ports>** tag.

Windows Firewall Troubleshooting

The following notes and tasks can aid you if you have trouble with Windows Firewall.

Windows Firewall General Troubleshooting Notes

Some general troubleshooting notes for Windows Firewall:

1. When you run the CiscoICMfwConfig application for the first time, run the application twice to successfully register of FirewallLib.dll. Sometimes, especially on a slower system, you need a delay for the registration to complete.
2. If the registration fails, the .NET framework might not be installed correctly. Verify that the following path and files exist:

   ```
   %windir%\Microsoft.NET\Framework\v2.0.50727\regasm.exe
   ```

   ```
   %windir%\Microsoft.NET\Framework\v1.1.4322\gacutil.exe
   ```

3. Change `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\Register.bat` as necessary to meet the environment.

Windows Firewall Interferes with Router Private Interface Communication

Problem The MDS fails to connect from the Side-A router to Side-B router on the private interface IP Addresses (Isolated) only when the Windows Firewall is enabled.

Possible Cause Windows Firewall is preventing the application (mdsproc.exe) from sending traffic to the remote host on the private network.

Solution Configure static routes on both Side-A and Side-B routers for the private addresses (high and nonhigh).

Windows Firewall Shows Dropped Packets Without Unified CCE Failures

Problem The Windows Firewall Log shows dropped packets but the Unified ICM and Unified CCE applications do not exhibit any application failures.

Possible Cause The Windows Firewall logs traffic for the host when the traffic is not allowed or when no allowed application listens to that port.

Solution Review the pfirewall.log file closely to determine the source and destination IP Addresses and Ports. Use `netstat` or `tcpview` to determine what processes listen and connect on what ports.

Undo Firewall Settings

You can use the firewall configuration utility to undo the last application of the firewall settings. You need the `CiscoICMfwConfig_undo.xml` file.

Note The undo file is written only if the configuration is completed successfully. If this file does not exist, manual cleanup is necessary using the Windows Firewall via Control Panel.

To undo the firewall settings:

Procedure

Step 1 Stop all application services.

Step 2 Open a command window by choosing **Start** > **Run** and entering `CMD` in the dialog window.

Step 3 Click **OK**.

Step 4 Enter the following command `cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig`.

Step 5 Enter `UndoConfigFirewall.bat` for Windows Server.

Step 6 Reboot the server.