ウィンドウ サーバのファイアウォールの設定

Windows Server Firewall

Windows ファイアウォールはステートフル ホスト ファイアウォールで、すべての迷惑な着信トラフィックをドロップします。Windows ファイアウォールのこの動作は、迷惑な着信トラフィックを使用してコンピュータを攻撃する悪意のあるユーザやプログラムから保護します。

詳細については、https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guideを参照してください。

サーバ上で Windows ファイアウォールを有効にする場合は、CCE ソリューション コンポーネントに必要なすべてのポートを開きます。

シスコでは、Windows サーバ上の Unified CCE アプリケーションからのすべてのトラフィックを自動的に許可するユーティリティを提供しています。このユーティリティは、Contact Center Enterprise のソリューションで使用する一般的なサードパーティ製アプリケーションのポートを開くことができます。スクリプトは、ファイル `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`のポートのリストを読み取り、ディレクティブを使用してファイアウォールの設定を変更します。

このユーティリティは、アプリケーションからのすべてのトラフィックを許可し、関連するアプリケーションを除くプログラムとサービスのリストに追加します。除外アプリケーションが実行されると、Windows ファイアウォールはプログラムがリッスンするポートをモニタし、これらのポートを除外トラフィックのリストに自動的に追加します。

このスクリプトでは、アプリケーションポート番号を除外トラフィックのリストにアプリケーションポート番号を追加することで、サードパーティアプリケーションからのトラフィックを許可します。これらのポートを有効にするには、`CiscoICMfwConfig_exc.xml` ファイルを編集します。

デフォルトで有効になっているポートとサービス：

- 80/TCP および 443/TCP - HTTP および HTTPS（システムが IIS または TomCat [Web セットアップ用] をインストールする場合）
- Microsoft リモート デスクトップ
- ファイル共有および印刷共有の例外 - https://docs.microsoft.com/en-us/windows-server/storage/file-server/best-practices-analyzer/smb-open-file-sharing-ports を参照してください。

デフォルトで無効になっているファイアウォールのインバウンド：

- IPv6 用のコアネットワーキング
- コアネットワーキング - TCP の IPHTTPS
- コアネットワーキング - UDP 用の Teredo
- プライベートプロファイルのネットワーク検出
- Windows リモート管理 - ドメイン、プライベートプロファイル、およびパブリックプロファイルの HTTP

サービスはデフォルトでは無効：

- ファイルサーバのリモート管理

開くことができるオプションのポート：

- 5900/TCP - VNC
- 5800/TCP - Java ビューア
- 21800/TCP - Tridia VNC Pro（暗号化されたリモートコントロール）
- 5631/TCP および 5632/UDP - pcAnywhere

（注） XML ファイルを編集して、このリスト以外のポートベースの例外を追加できます。

ポートの使用法の完全なリストについては、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html のページにある「*Cisco Unified Contact Center* ソリューションポート使用状況ガイド」を参照してください。

Cisco ファイアウォール設定ユーティリティの前提条件

ファイアウォールの設定ユーティリティを使用する前に、次のソフトウェアをインストールします。

1. オペレーティングシステムの詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「互換性マトリクス」を参照してください。
2. Unified ICM/CCE コンポーネント

（注） Windows ファイアウォールの設定後にコンポーネントをインストールする場合は、Windows ファイアウォールを再設定します。このプロセスでは、前の設定を削除し、Windows ファイアウォールの設定ユーティリティを再び実行します。

Cisco ファイアウォール設定ユーティリティの実行

Cisco ファイアウォール設定ユーティリティは、コマンドラインまたはユニファイド コンタクト センター セキュリティ ウィザードから実行できます。

警告 VNC などのリモートセッションからこのユーティリティを実行しようとすると、ファイアウォールの開始後に「ロックアウト」されることがあります。可能であれば、一部のリモートアプリケーションでネットワーク接続が切断される可能性があるから、コンピュータでファイアウォール関連の作業を実行します。

Unified ICM コンポーネントを実行している各サーバで、Cisco ファイアウォール設定ユーティリティを使用します。ユーティリティを使用するには、次の手順を実行します。

手順

ステップ 1 すべてのアプリケーションサービスを停止します。

ステップ 2 コマンドプロンプトから、`%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat` を実行します。

ステップ 3 初めてスクリプトを実行すると、スクリプトは `configfirewall.bat` を実行します。スクリプトは、同じコマンドを使用してアプリケーションを再設定する必要があります。指示がある場合は、スクリプトを再コマンドします。

ステップ 4 [OK] をクリックします。

スクリプトは、Windows ファイアウォールサービスがインストールされていることを確認してから、実行されていない場合にこのサービスを開始します。

その後、スクリプトは `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml` ファイルで指定されているポートとサービスでファイアウォールを更新します。

ステップ 5 サーバをリブートします。

関連トピック

Windows ファイアウォールの構成

新しい Windows ファイアウォール設定の確認

次の手順に従って、Unified ICM のコンポーネントとポートが Windows ファイアウォール例外リストに追加されたことを確認できます。

手順

ステップ 1 Windows サーバを 使用する場合は、**[開始（Start）]** > **[Windows 管理ツール（Windows Administrative Tools）]** を選択し、**[セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）]** を選択します。または、**[開始（Start）]** > **[コントロールパネル（Control Panel）]** > **[システムとセキュリティ（System and Security）]** > **[Windows ファイアウォール（Windows Firewall）]** を選択します。

[Windows ファイアウォール（Windows Firewall）] ダイアログボックスが表示されます。

ステップ 2 **[例外（Exceptions）]** タブをクリックします。次に、Windows Server の [Windows ファイアウォール（Windows Firewall）] ダイアログボックスの **[インバウンドルールとアウトバウンドルール（Inbound and Outbound Rules）]** タブをクリックします。

ステップ 3 例外アプリケーションのリストをスクロールします。リストと、構成ファイルで定義されているポートまたはサービスに、いくつかの Unified ICM 実行ファイルが表示されます。

Windows Server ファイアウォールと Active Directory の通信

ドメインコントローラ（DC）が LDAP や他のプロトコルとの通信に使用するポートを開いて、Active Directory がファイアウォール経由で通信可能か確認します。

ドメインと信頼関係のファイアウォールの設定に関する重要な情報については、Microsoft サポート技術情報の KB179442 の項目を参照してください。

DC と Unified ICM サービス間のセキュアな通信を確立するには、ファイアウォール上のアウトバウンドおよびインバウンドの例外に対して次のポートを定義します。

- すでに定義されているポート
- リモートプロシージャコール（RPC）で使用する変数ポート（高ポート）

ドメイン コントローラ ポートの設定

外部 DC に対して複製可能な、緩衝地帯（DMZ）内のすべての DC に対して、以下のポート定義を定義します。ドメイン内のすべての DC 上のポートを定義します。

特定のスタティックポートへの FRS トラフィックの制限

特定の静的ポートへのファイル複製サービス（FRS）トラフィックの制限の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

手順

ステップ 1 **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

ステップ 2 位置を確認して、次のキーをレジストリにクリックします。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters

ステップ 3 次のレジストリ値を追加します。

- 新規：**Reg_DWORD**
- 名前：**RPC TCP/IP ポートの割り当て**
- 値：**10000（10 進数）**

特定のポートへの Active Directory 複製トラフィックの制限

特定のポートへの Active Directory 複製トラフィックの制限の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

手順

ステップ 1 **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

ステップ 2 位置を確認して、次のキーをレジストリにクリックします。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

ステップ 3 次のレジストリ値を追加します。

- 新規：**Reg_DWORD**
- 名称：**RPC TCP/IP Port**
- 値：**10001**（**10 進数**）

リモートプロシージャコール（RPC）ポートの割り当ての構成

RPC ポート割り当ての設定の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

手順

ステップ 1 **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

ステップ 2 特定して、次のキーをレジストリでクリックします：
HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc

ステップ 3 **インターネット**キーを追加します。

ステップ 4 次のレジストリ値を追加します。

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

Windows ファイアウォールポート

ドメインと信頼のファイアウォールの設定に使用するポートの詳細については、Microsoft サポート技術情報の KB179442 の項目を参照してください。

表 *1 : Windows Server* ファイアウォールポート

サーバ ポート	[プロトコル（Protocol）]	プロトコル	サービス
135	[TCP]	RPC	RPC コネクタ ヘルパー（どの高いポートを使用するかを特定するために接続するマシン)
137	TCP	UDP	[NetBIOS 名（NetBIOS Name）]
138		UDP	NetBIOS NetLogon とブラウズ

サーバ ポート	[プロトコル（Protocol）]	プロトコル	サービス
139			NetBIOS セッション
123		UDP	NTP
389	TCP		LDAP
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
54			WINS 複製
53	TCP	UDP	DNS
88	TCP	UDP	Kerberos
445	TCP	UDP	IP の SMB（Microsoft-DS）
10000	TCP		RPC NTFRS
10001	[TCP]		RPC NTDS
10002 ～ 10200	[TCP]		RPC - 動的ハイオープンポート
適用外	ICMP		TCP/IP スイート内のレイヤ 3 プロトコルスイート。これは、ping やトレースで使用されます。ポート 7 を閉じるとエコー応答をブロックできます。

接続のテスト

接続をテストし、Active Directory で FRS の設定を表示するには、Ntfrsult ツールを使用します。

手順

コマンドラインから、Windows ファイル複製ユーティリティを実行します：`Ntfrsutl version <server_name>`。

ドメインコントローラ間の通信が適切に設定されている場合、Ntfrtl 出力には Active Directory の FRS 設定が表示されます。

接続の検証

ドメインコントローラ間の接続を検証するには、Portqry ツールを使用します。

Portqry ユーティリティをダウンロードし、詳細について知りたい場合は、https://support.microsoft.com/en-in/help/310099/description-of-the-portqry-exe-command-line-utility を参照してください。

手順

ステップ 1 **PortQryV2.exe** をダウンロードし、ツールを実行します。

ステップ 2 宛先 CD または PDC を選択します。

ステップ 3 **[ドメインと信頼（Domains and Trusts）]**を選択します。

ステップ 4 PortQry からの応答を使用して、ポートが開いているか確認します。

PortQry の機能の詳細については、Microsoft サポート技術情報の KB832919 の項目を参照してください。

CiscoICMfwConfig_exc.xml File

CiscoICMfwConfig_exc.xml ファイルは、Cisco ファイアウォールスクリプトが Windows ファイアウォールの変更に使用するアプリケーション、サービス、およびポートのリストを含む標準 XML ファイルです。この変更により、ファイアウォールが Unified ICM/Unified CCE 環境で正常に機能します。

ファイルは、次の 3 つの主要な部分で構成されています。

- **サービス**：ファイアウォール経由でのアクセスが許可されているサービス。
- **ポート**：ファイアウォールが開くポート。

  この設定は、TCP/80 と TCP/443 の場合の IIS のインストールに応じた条件付きの設定です。
- **アプリケーション**：ファイアウォールを介したアクセスが許可されていないアプリケーション。

  スクリプトは、`CiscoICMfwConfig_exc.xml` ファイルにリストされているすべてのアプリケーションを自動的に除外します。

（注） [アプリケーション（Applications）] セクションの動作は、ファイル内の他の2つのセクションの動作とは逆です。[ポートとサービス（Ports and Services）] セクションでは、アクセスが許可されていますが、[アプリケーション（Application）] セクションではアクセスが拒否されています。

CiscoICMfwConfig_exc.xml ファイルにさらに多くのサービスまたはポートを手動で追加し、スクリプトを再実行して Windows ファイアウォールを再設定できます。たとえば、**Jaguar** サーバへのポート 9000（CORBA）からの接続を許可するには、[ポート（Ports）] セクションに回線を追加して、Windows ファイアウォール上のポート 9000 を開きます。

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

（注） この変更は、リモート Jaguar 管理が求められている場合にのみ必要です。通常、この変更は不要です。

[セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）] を使用して、ポートまたはアプリケーションを追加または拒否できます。

このファイルには、一般に使用されるポートが XML コメントとしてリストされています。これらのポートの 1 つをすばやく有効にするには、ポートをコメントから **[ポート（Ports）]** タグの前の場所に移動します。

Windows ファイアウォールのトラブルシューティング

Windows ファイアウォールで問題が発生した場合は、次のメモとタスクを参照してください。

Windows ファイアウォール一般トラブルシューティング ノート

Windows ファイアウォールに関する一般的なトラブルシューティング ノート：

1. CiscoICMfwConfig アプリケーションを初めて実行する場合は、アプリケーションを 2 回実行すると、FirewallLib.dll の登録に成功します。場合によっては、特にシステムの速度が低下している場合、登録の完了に遅延が生じます。
2. 登録が失敗した場合は、.NET フレームワークが正しくインストールされていない可能性があります。次のパスとファイルが存在するかを確認します。

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

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

3. 環境に合わせて、必要に応じて `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\Register.bat` を変更します。

Windowsファイアウォールがルータのプライベートインターフェイス通信に干渉する

問題 MDS は、Windows ファイアウォールが有効になっている場合のみ、サイド A ルータからプライベート インターフェイスの IP アドレス（分離）上のサイド B ルータへの接続に失敗します。

考えられる原因 Windows ファイアウォールにより、アプリケーション（mdsproc.exe）がトラフィックをプライベートネットワーク上のリモートホストに送信するのを妨げている可能性があります。

解決法 プライベートアドレス（ハイ およびハイ以外）用に、サイド A ルータおよびサイド B ルータの両方にスタティックルートを設定します。

Windows ファイアウォールで Unified CCE 障害のないドロップされたパケットが表示される

問題 Windows ファイアウォールログにドロップされたパケットが表示されますが、Unified ICM および Unified CCE アプリケーションではアプリケーション の障害が発生しません。

考えられる原因 Windows ファイアウォールは、トラフィックが許可されていないか、許可されたアプリケーションがポートをリッスンしない場合に、ホストのトラフィックを記録します。

解決法 pfirewall.log ファイルを詳しく確認して、送信元と宛先の IP アドレスとポートを確認します。`netstat` または `tcpview` を使用して、どのプロセスがリッスンし、どのポートで接続されるのか確認します。

ファイアウォール設定の取り消し

ファイアウォール設定ユーティリティを使用すると、最後のファイアウォール設定の適用を元に戻すことができます。`CiscoICMfwConfig_undo.xml` ファイルが必要です。

（注） 元に戻すファイルは、設定が正常に完了した場合にのみ書き込まれます。このファイルが存在しない場合は、コントロールパネル経由の Windows ファイアウォールを使用して手動でクリーンアップする必要があります。

ファイアウォール設定を元に戻すには、次の操作を実行します。

手順

ステップ 1 すべてのアプリケーションサービスを停止します。

ステップ 2 コマンドウィンドウを開きます。ダイアログウィンドウで **[開始（Start）]** > **[実行（Run）]** を選択し、CMD と入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 次のコマンドを入力します。`cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig`

ステップ 5 Windows Server の `UndoConfigFirewall.bat` を入力します。

ステップ 6 サーバをリブートします。