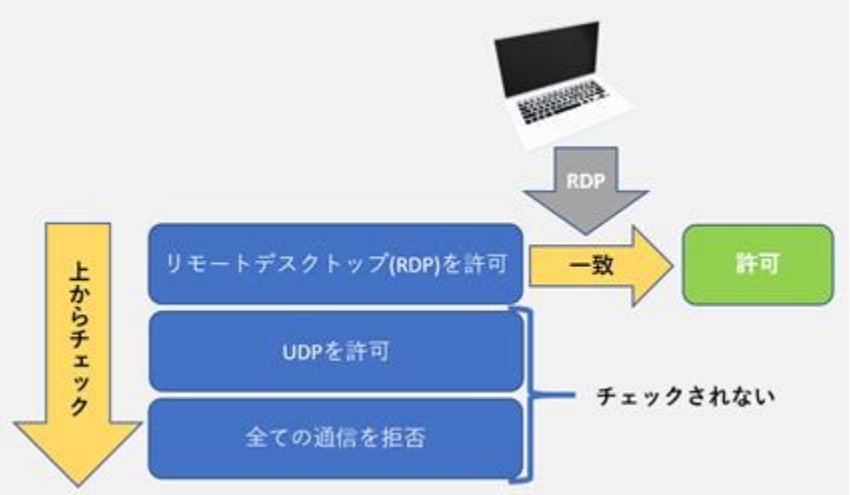
ClientSecurity/ ServerSecurity(Protection) 14 以降 のファイヤーウォール機能について

Client Security14/15、Server Protection(Server Security14 以降)に搭載されているファイヤーウォール(FW)機能は、Windows FW 機能をコントロールする「管理機能」となります。例えば、Windows FW を有効/無効化したり、ルールを追加/削除/無効化する等です。その為、独自の F-SecureFW が搭載されていた Client Security(CS)13/Server Security(SS) 12 以前とは FW ルールメカニズムが異なりますので、当記事にて解説させていただきます。
CS14/CS15 へのアップグレードインストールの際、既存 FW ルールは引き継がれません。
PolicyManager へのルール新規登録が必要となります。

［ファイヤーウォール適用順の違いについての解説］

CS13/SS12 以前の F-secure ファイヤーウォールは順序を考慮します。ルールは上から下へ順番にチェック/適用され、例えば下図のようにルールを設定した場合、RDP 通信(TCP:3389 使用)は、最上段の RDP 許可ルールに一致し、その時点で通信許可されます。それ以降のルールはチェックされません。ルール最下部に「全ての通信を拒否」(暗黙の Deny)が存在していてもルールはチェックされず、リモートデスクトップ通信は成功します。

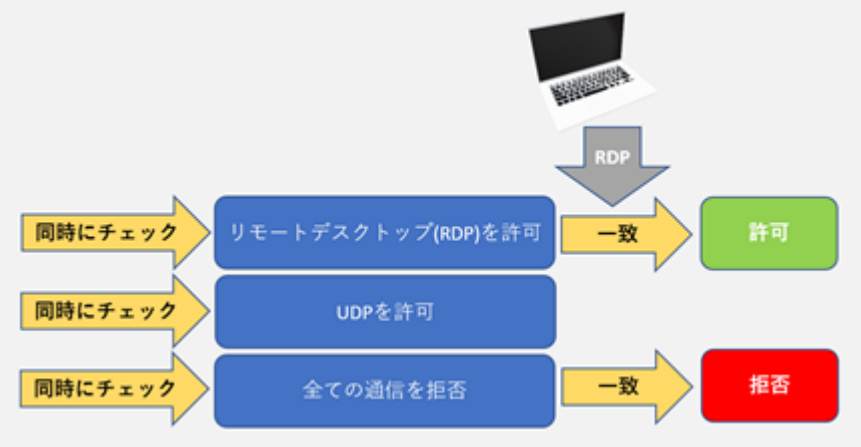
・CS13/SS12 以前(F-secure 製ファイヤーウォール)



・CS/ SS(SP) 14 以降(Windows ファイヤーウォール)

一方、ClientSecurity/ ServerSecurity(Protection) 14 以降が利用する Windows ファイヤーウォールは、設定されたルールの順序を考慮せず全てのルールをチェックします。通信に対して複数のルールが一致した場合、**拒否が優先**されます。その為、ルール最下部に「全ての通信を拒否」(暗黙の deny)がある場合、RDP 通信施行は失敗します。また、Windows FW に既存の拒否ルールが存在

している場合も RDP 通信施行は失敗します。当手順では、そういった Windows ファイヤーウォール既存ルールついて無効化を行います。



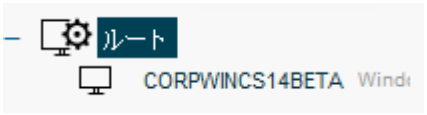
つまり、CS13/SS12 以前のルールをそのまま CS/SS(SP) 14 以降に設定しても狙った動作は見込めません。

［対処方法］

下記手順で、Window FW ルールを Policy Manager 経由で行うように設定してください。当シナリオでは、「暗黙の Deny」（"許可条件に合致しない通信は全ブロック"）を Windows ファイヤーウォールに担当させ、Policy Manager から許可ルールのみ登録する手法を採用しております。

［Window ファイヤーウォールのルール無効化手順］

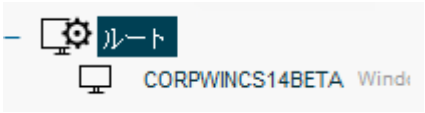
1. ポリシーマネージャコンソールの左ペインで設定したいドメインを選択します。



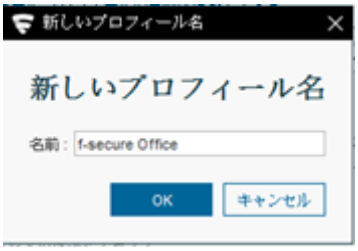
2. 「設定」→「ファイヤーウォール」→「プロフィールにないファイヤーウォールルールをすべて無視する」を有効(チェックを入れる)にしてください。この変更により、Window FW に設定されている既存ルールが無効化されます。

［Policy Manger でのファイアルール追加手順］

1.ポリシーマネージャコンソールの左ベインで設定したいドメインを選択します。



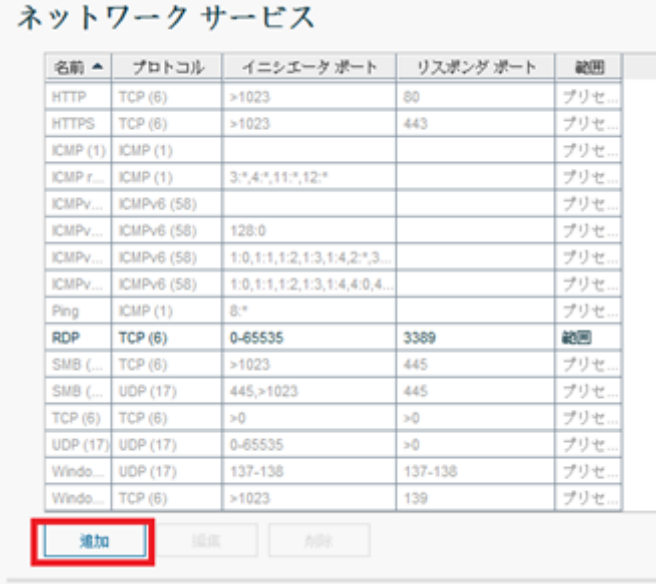
2.右ベインの「設定」→「ファイヤーウォール」に移動し、「クローン」をクリックして自由にカスタムできる新しいプロフィールを作成します。



3.「編集中のプロフィール」で、先程作成したプロフィール「f-secure Office(範囲)」に切り替えます。

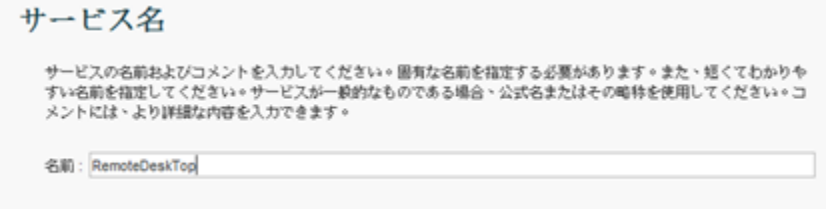
4.「ネットワークサービスを設定する」をクリックします。

5.「ネットワークサービス」が開きます。「追加」をクリックします。



6.「サービス名」を入力します。

※RemoteDeskTop と入力しています。



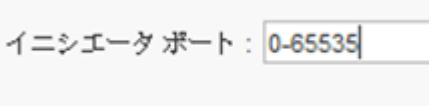
7.プロトコルを選択し、「次へ」をクリックします。

※一般的には TCP か UDP となります。

8.「イニシエータポート」を入力し、「次へ」をクリックします。

※イニシエータポートは送信(開始)ポートとなります。

※指定されていない場合、0-65535 を入力してください。RDP の場合は指定は不要。



7.「リスポンダポート」を入力し、「完了」をクリックします。

※リスポンダポートは受信ポートとなります。RDP の場合は 3389 となります。

8.「ネットワークサービス」にサービスが追加された事を確認し、この画面を閉じます。

8.「ファイヤーウォールルール」の画面で、「ルールを追加」をクリックします。

9.「名前」「タイプ」を入力し、「次へ」をクリックします。

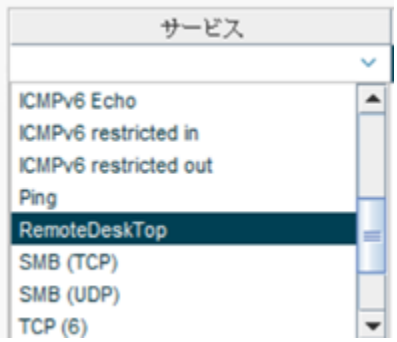
10.「追加」をクリックします。

11.空白のサービスが追加されます。

12.「サービス」フィールドを**ダブルクリック**し、追加したいサービスを選択します。

※先程追加したサービスを選びます。

※プリセットされたサービスも表示されます。



13.「方向」フィールドで着信/発信/両方のどれかを選択し、「次へ」をクリックします。

14.「全てのリモートアドレス」を選択し、「次へ」をクリックします。

15.デフォルト設定のまま、「完了」をクリックします。

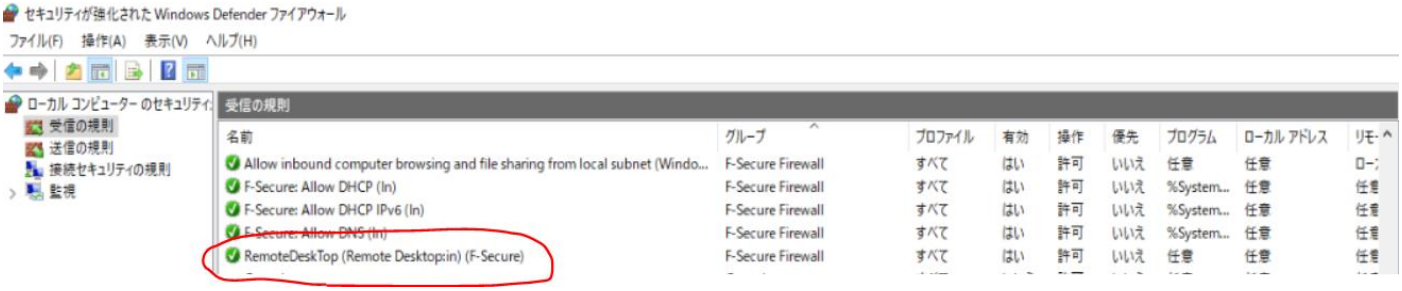
16.「ファイヤーウォールルール」にルールが追加された事を確認します。

17.ファイヤーウォールプロフィールを切り替えます。

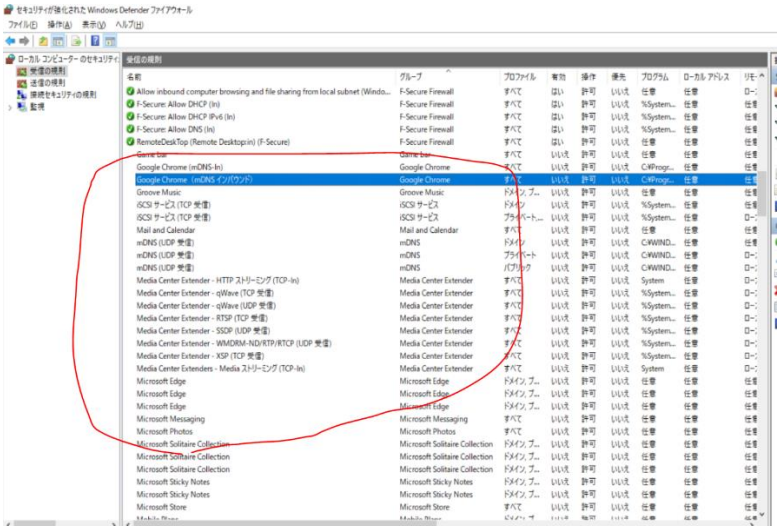
※今回作成した「F-secure Office」を選んでいます。既に切り替わっている場合は不要です。

18.ポリシーを配布します。

19.管理クライアント(CS/SS)の Window ファイヤーウォール管理画面-詳細設定-受信の規則に、RemoteDeskTop(Remote Desktop in)が存在している事を確認してください。



20.グループが「F-Secure Firewall」以外のルールが無効(緑色のチェックが無い状態)である事を確認してください。
※「Window ファイヤーウォールのルール無効化手順」で WindowsFW を無効化しています。



補足事項

(補足事項 1)当手法を行うことで既存の Windows ファイヤーウォールルールの設定を変更し、既存のアプリケーション通信に影響を与える可能性がございます。あらかじめお使いのコンピュータに必要な通信(IP アドレス/ポート番号/etc)を把握した上で当手法をお試しください。

(補足事項 2) Windows ファイヤーウォールはポリシーのインポート/エクスポート、既定のポリシーの復元機能を備えております。Computer Protection での設定変更前のポリシーをエクスポートしておく事で設定ミスが発生した場合でも設定の復元が可能です。

※コントロールパネル→ファイヤーウォール→詳細設定→ポリシーのエクスポート/インポート
※「Window ファイヤーウォールのルール無効化手順」をチェックした、「プロフィールにないファイヤーウォールルールをすべて無視する」のチェックを解除する事でも既存 WindowsFW を再度有効化できます。

(補足事項 3) Windows Firewall は Microsoft 社製品のコンポーネントとなります。詳細なご案内については Microsoft 様でのサポートを受けていただくようお願いいたします。

(補足事項 4) Active Directotry のグループポリシーや Windows のローカルポリシー(GPO)で Windows ファイヤーウォールを有効/無効に設定している場合、Client Security は Windows ファイヤーウォールをコントロールできません。ActiveDirectory やローカルポリシー(GPO)での管理をお願いします。