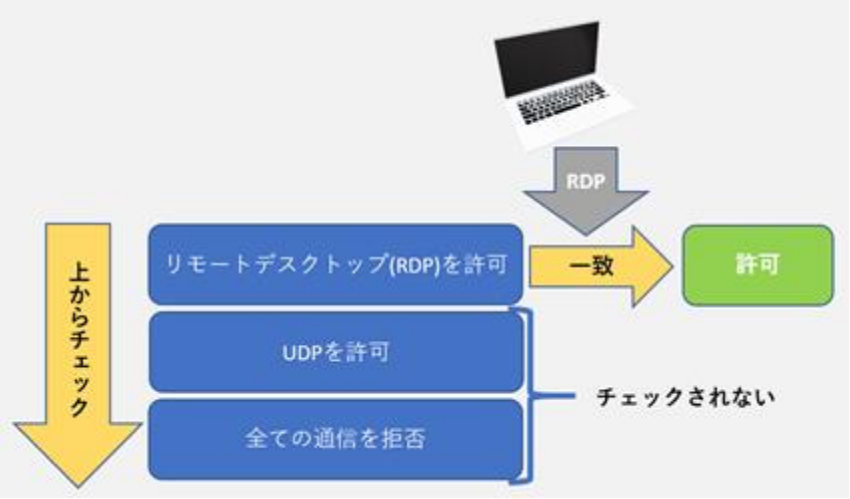
ClientSecurity/ ServerSecurity(Protection) 14/15 のファイヤーウォール機能について

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、ルールの再検討をせずにバージョンアップを実施した場合、想定通りの動作が見込めません。また CS13 以前の既存 FW ルールは引き継がれない為、PolicyManager へルール移行を行うか、PolicyManger でのファイヤーウォール管理を停止する必要があります。

［ファイヤーウォール適用順の違いについての解説］

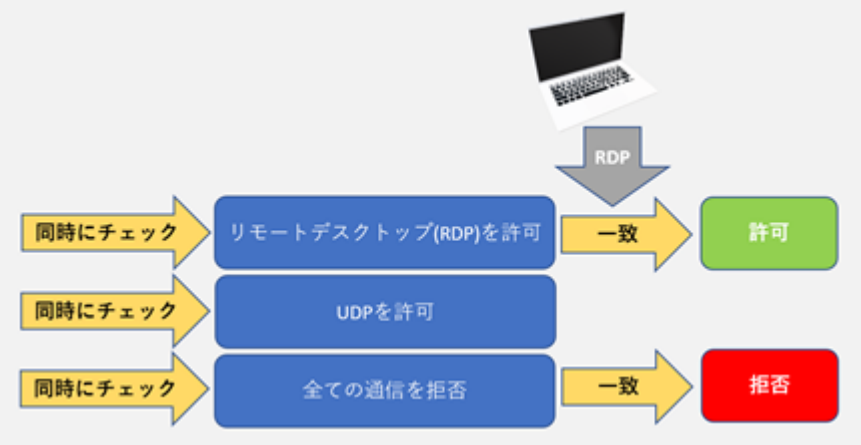
CS13/SS12 以前の F-secure ファイヤーウォールは順序を考慮します。ルールは上から下へ順番にチェック/適用され、例えば下図のようにルールを設定した場合、RDP 通信(TCP:3389 使用)は、最上段の RDP 許可ルールに一致し、その時点で通信許可されます。それ以降のルールはチェックされません。ルール最下部に「全ての通信を拒否」(暗黙の Deny)が存在していてもルールはチェックされず、リモートデスクトップ通信は成功します。

・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) 14/15 以降に設定しても狙った動作は見込めません。

[対処方法] 下記のどちらかを実施してください。

- PolicyManger で Windows FW 機能コントロール機能を無効にする。
  → **“Windows FW 機能コントロール無効化手順“を実施**

- Window FW ルール設定を Policy Manager 経由で行うように設定し、FW ルールを全て移行する。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 に許可ルールのみ登録する手法を採用しております。
  → **“Policy Manger での FW ルール管理手順“を実施**

[Windows FW 機能コントロール無効化手順]

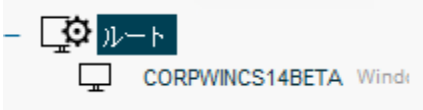
CS/SS が所属するポリシードメインで下記 2 点を無効化(チェック解除)してポリシー配布する。
「ポリシーマネージャを使用してファイヤーウォール構成を有効にする」
「Windows firewall を有効にする」

※インストーラにポリシーを含めるとバージョンアップ直後に WindowsFW が無効化できます。

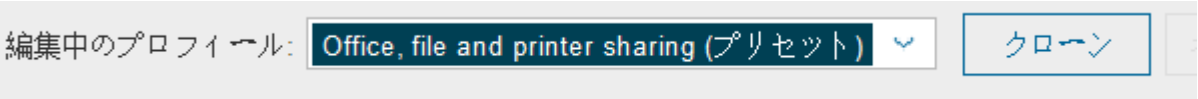
インストールパッケージ作成ウィザードで「初期ポリシー」に FW 無効化ポリシーを指定。

[Policy Manger での FW 許可ルール管理手順]

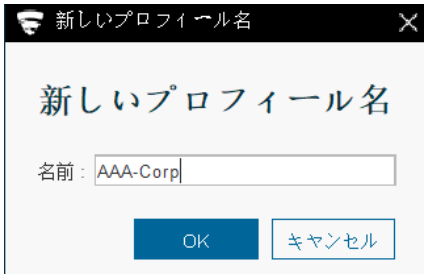
1. ポリシーマネージャコンソールの左ペインで設定したいドメインを選択します。



2. 右画面の「設定」→「ファイヤーウォール」に移動します。
「Office,File and printer sharing」から「クローン」をクリックし、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。

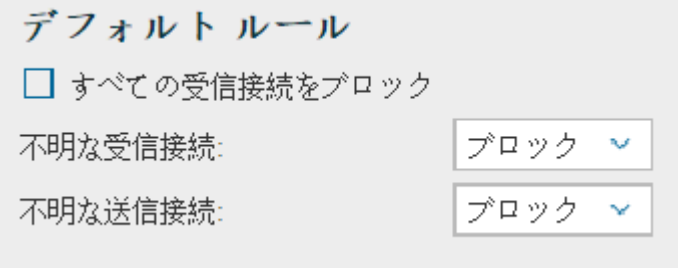


※新しいプロフィールとして「AAA-Corp」を作成

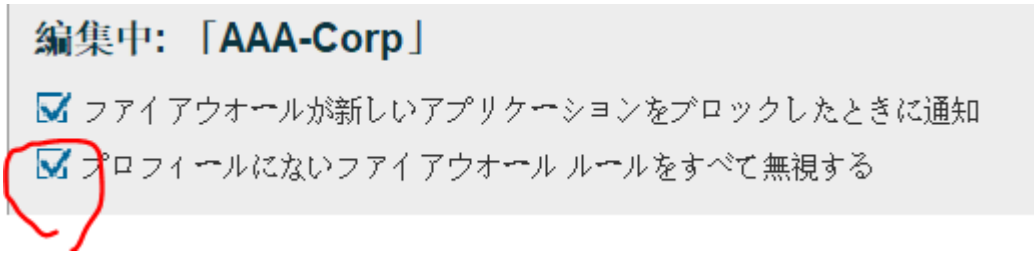


3. 「編集中のプロフィール」を「AAA-Corp（範囲)」に切り替えます。

4. デフォルトルールが下記になっている事を確認します。

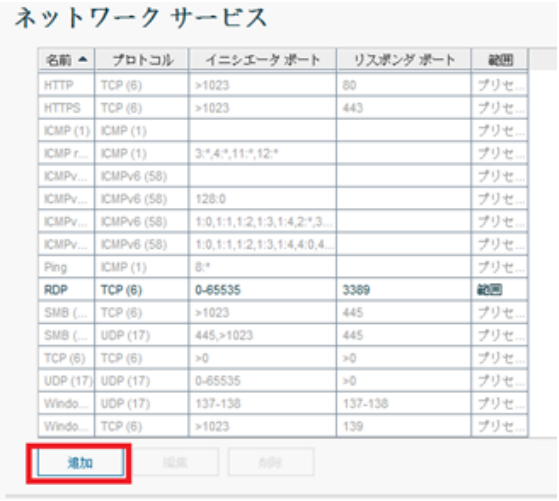


5. 「プロフィールにないファイヤーウォールルールをすべて無視する」を有効(チェックを入れる)します。この設定により Window FW の既存ルールが無効化されます。

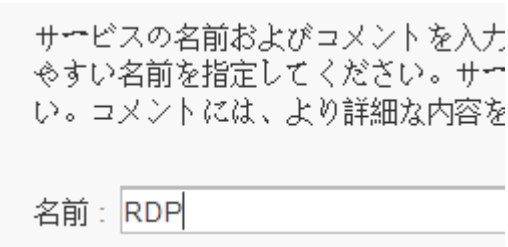


6. 「ネットワークサービスを設定する」をクリックします。

7. 「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。



8. 「サービス名」を入力します。
※RDP と入力しています。



9. 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、RDP の場合 TCP です。

10. 「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。

11. 「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。

12. 「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。

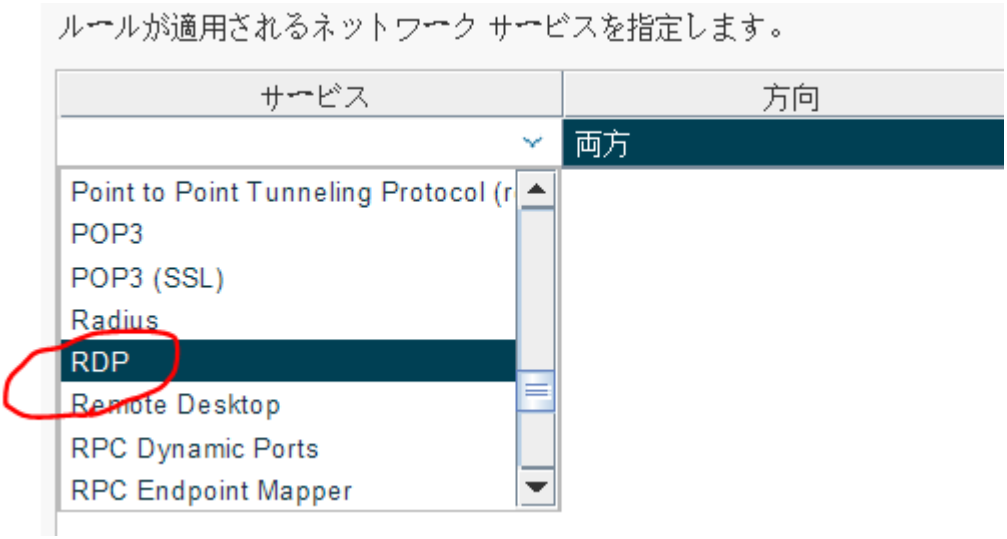
13. 「ファイヤーウォールルール」の画面で、「ルールを追加」をクリックします。

14. 「名前」(RDP)「タイプ」(許可)を入力し、「次へ」をクリックします。

15. 「追加」をクリックします。

16. 空白のサービスが追加されます。

17. 「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「RDP」を選びます。



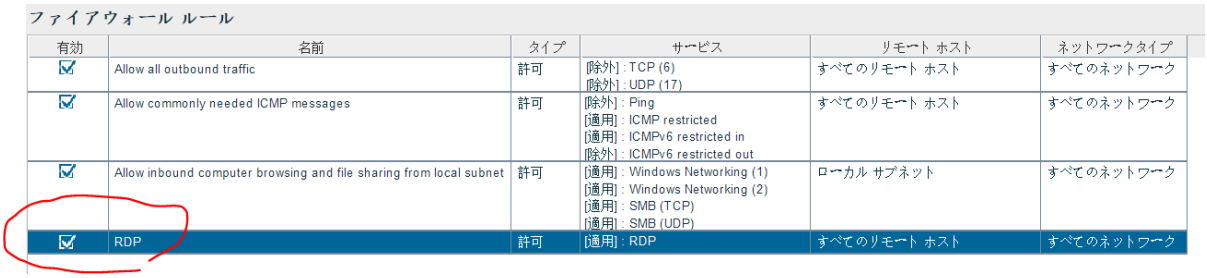
18. 「方向」フィールドで[着信/発信/両方]のどれかを選択し、「次へ」をクリックします。

※RDP 接続を受ける側は「着信」を選びます。

19. 「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。

20. デフォルト設定のまま、「完了」をクリックします。

21. 「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。

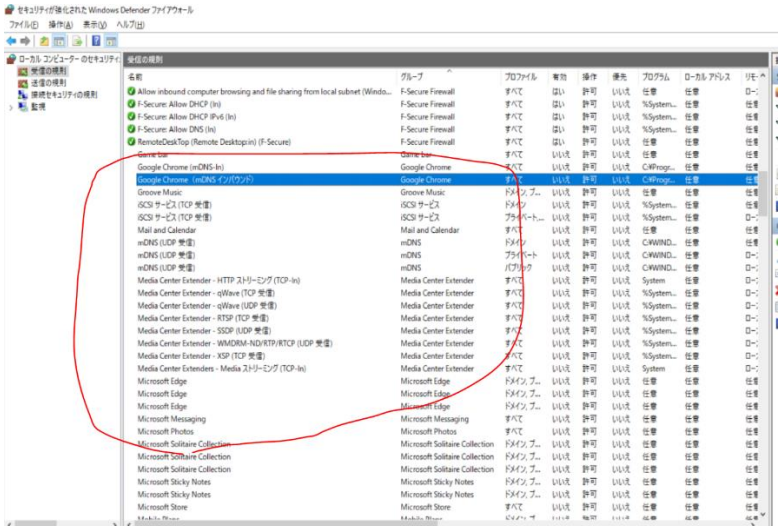


22. デバイスに適用するファイヤーウォールプロフィールを指定します。
※ 今回作成した「AAA-Corp」を選びますが既に切り替わっている場合は不要です。

23. ポリシーを配布します。

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

25. 「F-Secure Firewall」グループ以外が無効(緑色のチェックが無い)である事を確認する。



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。また、遠隔地での操作の場合、誤ったファイヤーウォール設定を行うことで操作ができなくなる可能性があります。現地での作業をお勧め致します。

(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。