サポート文書
必須技術文書

ステートフルトラフィックフィルタ
ファイアウォール cPP の
評価アクティビティ

2015 年 2 月

バージョン 1.0

CCDB-2015-01-002

平成 28 年 1 月 15 日　翻訳 暫定第 0.2 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

序文

本書は、コモンクライテリアバージョン 3 と関連する情報技術セキュリティ評価のための共通評価方法を補足することを意図した、サポート文書である。

サポート文書は、その適用が相互承認上必須ではないような分野に対する具体的なやり方と規格の適用に注目した、それ自体が規格としての性質を持たない「ガイダンス文書」であってもよいし、またはサポート文書の適用範囲によりカバーされる評価において、その適用が必須とされるような「必須技術文書」であってもよい。後者の利用法は必須であるだけでなく、それらの適用の結果として発行される認証書は CCRA の下で承認される。

本サポート文書は、Network International Technical Community (NDFW-iTC) により開発されたものであり、またセクション 1.1 で識別される cPP に適合する製品の評価をサポートするために使用されるよう設計されている。

テクニカルエディタ：Network International Technical Community (NDFW-iTC)

文書履歴：

V1.0, 2015 年 2 月 27 日 (公開バージョン)

V0.4, 2015 年 1 月 26 日 (CCDB レビューから受け取ったコメントによる変更を取り込み)

V0.3, 2014 年 10 月 17 日 (公開レビュー後にリリースされたバージョン、CCDB レビュー用に提出)

V0.2, 2014 年 10 月 13 日 (公開レビューコメントに対応した内部ドラフト、iTC レビュー用)

V0.1, 2014 年 9 月 5 日 (公開レビューのための初期リリース)

一般的な目的：セクション 1.1 を参照されたい。

特定用途分野：本サポート文書は、ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル [FWcPP] に適合主張する TOE の評価に適用される。

謝辞：

本サポート文書は、産業界、政府機関、コモンクライテリア評価機関、及び学術会員からの代表者の参加する、Network international Technical Community によって開発された。

目次

1 序説

1.1 サポート文書の技術分野と適用範囲

1 本サポート文書は、ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル [FWcPP] に関連する評価アクティビティを定義する。[FWcPP] は、[ND-SD] に記述されたネットワークデバイスの評価アクティビティの使用も要求することに注意されたい。本サポート文書は、[ND-SD] の評価アクティビティに加えて、 [FWcPP] のための追加の評価アクティビティのみを定義する。

2 本サポート文書は、以下の cPP への適合を主張する製品の評価に必須となる：

a) ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル [FWcPP]。

3 評価アクティビティは、主に評価者が従うものとして定義されるが、本サポート文書における定義は、開発者、評価者及び利用者に対して、関連する cPP への適合評価において TOE のどの側面がテストされるのか、またどの程度深くテストが実行されるかについての、共通の理解を提供することを目的としている。この共通の理解は、さらに、cPP への適合評価が、比較可能で、透明性のある、再現可能な結果が得られることを保証するという目標に寄与する。一般的に、評価アクティビティの定義は、開発者が、その TOE の具体的な要件を識別することにより、評価の準備に役立てることにもなるだろう。評価アクティビティにおける具体的な要件は、場合によっては SFR の意味を明確化し、またセキュリティターゲット (特に TOE 要約仕様)、利用者ガイダンス文書、及び想定される補足情報 (例、エントロピー分析、または暗号鍵管理アーキテクチャ等) の内容の具体的な要件を識別するかもしれない。

1.2 文書の構成

4 評価アクティビティは、セキュリティ機能要件とセキュリティ保証要件の両方について定義することができる。これらは、本サポート文書の別々のセクションで定義されている。

5 任意の評価アクティビティが評価中に成功裏に完了できなかった場合、その評価の総合判定は「不合格」となる。まれな場合には、評価アクティビティが修正され、または特定の TOE に適用できないとみなされ得る受け入れ可能な理由が存在するかもしれないが、このような場合には、その評価に関して認証機関と合意がなされなければならない。

6 一般的には、すべての評価アクティビティ (SFR と SAR の両方について) が評価中に成功裏に完了した場合、その評価の総合判定は「合格」となる。評価アクティビティが成功裏に完了した時に「不合格」の判定となるためには、その TOE について評価アクティビティがなぜ不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

7 同様に、より粒度の細かい保証コンポーネントのレベルにおいて、ある保証コンポーネントについての評価アクティビティ及びそれに関連する SFR の評価アクティビティのすべてが評価中に成功裏に完了した場合、その評価コンポーネントの判定は「合格」となると期待される。これらの評価アクティビティが

成功裏に完了した時にその評価コンポーネントについて「不合格」の判定となるためには、その TOE について評価アクティビティがなぜ不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

1.3 用語

8 標準的な CC 用語の定義については、 [CC] パート 1 を参照されたい。

9 **cPP—**コラボラティブプロテクションプロファイル

10 **CVE—**Common Vulnerabilities and Exposures (データベース)

11 **iTC—**International Technical Community

12 **SD—**サポート文書

13 **補足情報—**セキュリティターゲットまたはガイダンス文書に必ずしも含める必要のない情報で、公開される必要ないもの。そのような情報の例としては、エントロピー分析、あるいは TOE で (またはそのサポートにおいて) 使用される暗号鍵管理アーキテクチャについての記述であろう。そのような補足情報に関する要件は、関連する cPP で識別される (セクション 4 の記述を参照されたい)。

2 SFR の評価アクティビティ

2.1 利用者データ保護 (FDP)

2.1.1 FDP_RIP.2 十分な残存情報の保護

2.1.1.1 TSS

14 本要件における「資源」とは、TOE を通過して (セキュリティ管理者が TOE へ接続する時のような「へ」の対語として) 送信されるネットワークパケットである。懸念されるのは、一度ネットワークパケットが送信された後も、そのパケットによって使用されたバッファまたはメモリ領域にそのパケットからのデータがまだ含まれており、そしてそのバッファが再利用された場合、それらのデータが残ったまま新たなパケットに入り込むことである。評価者は、ネットワークパケットを処理する時に再利用されるデータが全く存在しないことを決定できるような範囲までのパケット処理が TSS に記述されていることを保証するため、TSS をチェックしなければならない。評価者は、この記述に最低限、どのようにして以前のデータがゼロ化／上書きされるのか、そしてバッファ処理においてどの時点でこれが発生するのかを記述していることを保証しなければならない。

2.2 ファイアウォール (FFW)

2.2.1 FFW_RUL_EXT.1 ステートフルトラフィックフィルタリング

2.2.1.1 TSS

15 評価者は、ネットワークパケット処理の実行をいつ開始するかを明示するような、TOE の初期化／起動プロセスの記述を TSS が提供し、このプロセス中にパケットが流すことができなという主張をサポートする論拠を TSS が提供していることを検証しなければならない。

16 評価者は、ネットワークパケット処理に含まれるコンポーネント (例、プロセスまたはタスク等のアクティブなエンティティ) を識別する説明についても TSS に含まれており、コンポーネントの故障時に規則 (ルールセット) を適用することなしにパケットが TOE を通過して流れることを防止する保護手段について TSS が記述していることを検証しなければならない。これには、プロセスの終了等のコンポーネントの故障、またはメモリバッファが満杯となりパケットが処理できない等のコンポーネント内部の故障が含まれるかもしれない。

2.2.1.2 ガイダンス文書

17 本要件に関連するガイダンス文書は、次のテスト保証アクティビティにおいて評価される。

2.2.1.3 テスト

18 テスト 1 : 評価者は、TOE が初期化されている間、TOE を通過してネットワークトラフィックを流そうと試行しなければならない。初期化中でなければ規則 (ルールセット) によって拒否されたであろうネットワークパケットの定常的なフローが、ホストから、及びホストへ向けて流されるべきである。評価者は、パケットスニファを用いて、生成されたネットワークトラフィックが初期化中にファイアウォールの通過を全く許可されないことを検証しなければならな

い。

19 テスト 2 : 評価者は、TOE が初期化されている間、TOE を通過してネットワークトラフィックを流そうと試行しなければならない。規則 (ルールセット) によって許可されるであろうネットワークパケットの定常的なフローが、ホストから、及びホストへ向けて流されるべきである。評価者は、パケットスニファを用いて、生成されたネットワークトラフィックが初期化中にファイアウォールの通過を全く許可されず、また初期化が完了した後に初めて許可されることを検証しなければならない。

20 注：規則 (ルールセット) の適用に関連する残りのテストは、次のテスト保証アクティビティにおいて対処される。

FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4

TSS

21 評価者は、ステートフルトラフィックフィルタリングポリシー及び以下の属性が、関連するプロトコル用のステートフルトラフィックフィルタリング規則において設定可能なものとして識別されていることを TSS が記述していることを検証しなければならない：

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル
- IPv6
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル、及び ST 作成者によって定義される場合、拡張ヘッダタイプ、拡張ヘッダフィールド
- TCP
  - 送信元ポート
  - 宛先ポート
- UDP
  - 送信元ポート
  - 宛先ポート

22 評価者は、各規則が以下のアクションを識別できることを検証しなければならない：許可または破棄、その操作をログ出力する選択肢と共に。評価者は、ステートフルトラフィックフィルタリングポリシーの対象となるすべてのインタフェース種別が TSS に識別され、規則が個別のネットワークインタフェースとどのように関連付けされているかを TSS が説明していることを検証しなければならない。

ガイダンス文書

23 評価者は、ガイダンス文書が、関連するプロトコル用のステートフルトラフィックフィルタリングの規則において設定可能なものとして、以下の属性を識別していることを検証しなければならない。

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル
- IPv6
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル、及び ST 作成者によって定義される場合、拡張ヘッダタイプ、拡張ヘッダフィールド
- TCP
  - 送信元ポート
  - 宛先ポート
- UDP
  - 送信元ポート
  - 宛先ポート

24 評価者は、各規則が以下のアクションを識別できることをガイダンス文書に示されていることを検証しなければならない：許可、破棄、及びログ出力。

25 評価者は、規則が個別のネットワークインタフェースに関連付けられる方法がガイダンス文書に説明されていることを検証しなければならない。

テスト

26 テスト 1：評価者は、以下の属性のそれぞれについて、パケットを許可、破棄、及びログ出力するようにステートフルトラフィックフィルタファイアウォールの規則が作成可能であることをテストするため、ガイダンス文書における指示を用いなければならない：

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル
- IPv6
  - 送信元アドレス

- 宛先アドレス
- トランスポート層プロトコル、及び ST 作成者によって定義される場合、拡張ヘッダタイプ、拡張ヘッダフィールド

- TCP
  - 送信元ポート
  - 宛先ポート
- UDP
  - 送信元ポート
  - 宛先ポート

27 テスト 2 : 上記のテスト保証アクティビティを繰り返し、TOE によってサポートされる個別のネットワークインタフェース種別それぞれについてステートフルトラフィックフィルタリングの規則が定義可能であることを保証するため、上記のテスト保証アクティビティを繰り返す。

28 これらのテストアクティビティは、その規則の有効性がテストされる FFW_RUL_EXT.1.8 のテストアクティビティと組み合わせて実行されるべきであることに注意されたい。FFW_RUL_EXT.1.8 用のテストアクティビティは、テストする必要のあるプロトコル／属性の組み合わせを定義している。それらの組み合わせが手動で設定される場合、これらのテストアクティビティの目的は達成されるが、それらの組み合わせが別の方法で (例、オートメーションを用いる等) 設定される場合、ガイダンスが正しいこと及び設定の全範囲が TOE 管理者によって達成可能であることを保証するために、これらのテストアクティビティが必要となるかもしれない。

FFW_RUL_EXT.1.5

TSS

29 評価者は、ステートフルなセションの取り扱いをサポートするプロトコルが TSS に特定されていることを検証しなければならない。TSS は、TCP、UDP、及び ST 作成者により選択される場合は ICMP が、識別されなければならない。

30 評価者は、ステートフルなセションが (ハンドシェイク処理を含めて) 確立され維持される方法について、TSS に記述されていることを検証しなければならない。

31 評価者は、TCP について、セションの決定における以下の属性の使用について TSS が識別し記述していることを検証しなければならない : 送信元及び宛先アドレス、送信元及び宛先ポート、シーケンス番号、及び個別のフラグ。

32 評価者は、UDP について、セションの決定における以下の属性について TSS が識別し記述していることを検証しなければならない : 送信元及び宛先アドレス、送信元及び宛先ポート。

33 評価者は、ICMP (選択されている場合) について、セションの決定における以下の属性について TSS が識別し記述していることを検証しなければならない : 送信元及び宛先アドレス、FFW_RUL_EXT.1.5 で選択されたその他の属性。

34 評価者は、確立されたステートフルなセションがどのように削除されるのかについて TSS が記述していることを検証しなければならない。TSS には、通常の完了及び／またはタイムアウト条件に基づいて、各プロトコルのコネクションの削除方法を記述しなければならない。また TSS には、セションの削除が有効

となる時点 (例、そのセションに一致したかもしれない次のパケットが処理される前等) を示されなければならない。

ガイダンス文書

35 評価者は、ステートフルなセションのふるまいについて、ガイダンス文書に記述されていることを検証しなければならない。例えば、TOE は、既存セションの一部として許可されるパケットをログ出力しないかもしれない。

テスト

36 テスト 1： 評価者は、TCP トラフィックを許可し、ログ出力するように TOE を設定しなければならない。 評価者は、TCP セションを開始しなければならない。 TCP セションが確立されている間、評価者は、改変されたトラフィックがセションの一部として受け入れられない (すなわち、規則 (ルールセット) が適用されたことを示すログ事象が生成される) ことを決定するため、不正確なフラグを持つセション確立パケットを取り入れなければならない。 TCP セションの確立が成功した後、改変されたパケットが確立されたセションの一部として受け入れられないことを検証するために、評価者はセションを決定する属性 (送信元及び宛先アドレス、送信元及び宛先ポート、シーケンス番号、フラグ) のそれぞれを一度にひとつずつ改変しなければならない。

37 テスト 2： 評価者は、テスト 1 で確立された TCP セションを TSS に記述されるように終了させなければならない。 その直後に、規則 (ルールセット) が適用されることなく以前のセション定義に一致するパケットが TOE を通過して転送されないことを保証するために、評価者はそのようなパケットを送信しなければならない。

38 テスト 3： 評価者は、テスト 1 で確立された TCP セションを TSS に記述されるように有効期限切れ (すなわち、タイムアウトに到達する) とさせなければならない。規則 (ルールセット) が適用されることなく以前のセションに一致するパケットが TOE を通過して転送されないことを保証するために、評価者はそのようなパケットを送信しなければならない。

39 テスト 4： 評価者は、UDP トラフィックを許可し、ログ出力するよう TOE を設定しなければならない。 評価者は、UDP セションを開始しなければならない。 UDP セションが確立した後、改変されたパケットが確立されたセションの一部として受け入れられないことを検証するために、評価者は、セションを決定する属性 (送信元及び宛先アドレス、送信元及び宛先ポート) のそれぞれを一度にひとつずつ改変しなければならない。

40 テスト 5： 評価者は、テスト 4 で確立された UDP セションを TSS に記述されるように有効期限切れ (すなわち、タイムアウトに到達する) とさせなければならない。規則 (ルールセット) が適用されることなく以前のセションに一致するパケットが TOE を介して転送されないことを保証するために、評価者はそのようなパケットを送信しなければならない。

41 テスト 6： ICMP が選択されている場合、評価者は、ICMP トラフィックを許可し、ログ出力するよう TOE を設定しなければならない。 評価者は、TSS に定義されるように ICMP のセションを確立しなければならない。 ICMP セションが確立した後、改変されたパケットが確立されたセションの一部として受け入れられないことを検証するために、評価者は、セションを決定する属性 (送信元及び宛先アドレス、FFW_RUL_EXT.1.5 で選択されたその他の属性) のそ

れぞれを一度にひとつずつ改変しなければならない。

42 テスト 7： 該当する場合、評価者は、テスト 6 で確立された ICMP セションを TSS に記述されるように終了させなければならない。その直後に、規則 (ルールセット) が適用されることなく以前のセション定義に一致するパケットが TOE を通過して転送されないことを保証するために、評価者はそのようなパケットを送信しなければならない。

43 テスト 8： 評価者は、テスト 6 で確立された ICMP セションを TSS に記述されるように有効期限切れ (すなわち、タイムアウトに到達する) とさせなければならない。規則 (ルールセット) が適用されることなく以前のセションに一致するパケットが TOE を介して転送されないことを保証するために、評価者はそのようなパケットを送信しなければならない。

FFW_RUL_EXT.1.6

TSS

44 評価者は、TSS が、自動的に破棄され、カウントまたはログ出力されるパケットとして、以下のものを識別していることを検証しなければならない：

a) 無効なフラグメントであるパケット、何が無効なフラグメントとなるのかという記述を含む
b) 完全な再構成が不可能なフラグメント
c) 送信元アドレスがブロードキャストネットワーク上にあると定義されるようなパケット
d) 送信元アドレスがマルチキャストネットワーク上にあると定義されるようなパケット
e) 送信元アドレスがループバックアドレスであると定義されるようなパケット
f) TSF は、ネットワークパケットの送信元または宛先アドレスが、IPv4 について RFC 5735 に特定されるとおり、未指定 (すなわち 0.0.0.0) または「将来のために予約された」アドレス (すなわち 240.0.0.0/4) であると定義されるようなネットワークパケットを拒否し、またそのログ出力ができなければならない；
g) TSF は、ネットワークパケットの送信元または宛先アドレスが、IPv6 について RFC 3513 に特定されるとおり、「未指定アドレス」または「将来のために予約された」アドレス (すなわち、以下のアドレス範囲：2000::/3 にないユニキャストアドレス) であると定義されるようなネットワークパケットを拒否し、またそのログ出力ができなければならない；
h) IP オプションを持つパケット：ルーズソースルーティング (Loose Source Routing)、ストリクトソースルーティング (Strict Source Routing)、またはレコードルート(Record Route)
i) FFW_RUL_EXT.1.6 に定義されるその他のパケット

ガイダンス文書

45 評価者は、デフォルトで廃棄されると共にログ出力される可能性のあるパケットについてガイダンス文書に記述されていることを検証しなければならない。該当するプロトコルが識別されている場合、それらの記述は TSS と一貫している必要がある。ログ出力が設定可能な場合、評価者は自動的に拒否されたパケットの監査について設定するために、適用可能な指示が提供されていること

を検証しなければならない。

テスト

46 テスト 1： 評価者は、自動的なパケット拒否の各条件を順番にテストしなければならない。それぞれの場合において、TOE はすべてのネットワークトラフィックを許可するよう設定されるべきであり、また評価者は、拒否されるべきパケットまたはパケットフラグメントを生成しなければならない。評価者は、容認できないパケットまたはパケットフラグメントが TOE を通過しないことを保証するため、パケットキャプチャを利用しなければならない。

47 テスト 2： 上記のそれぞれの場合について、評価者は、破棄されたパケットのログ出力またはカウントを有効化するため、あらゆる適用可能なガイダンスを使用しなければならない。 上記のそれぞれの場合において、評価者は、拒否されたパケットまたはパケットフラグメントが記録された (ログ出力されたか、適切なカウンタがインクリメントされたかのいずれか) ことを保証しなければならない。

FFW_RUL_EXT.1.7

TSS

48 評価者は、以下のトラフィックが破棄されると共にカウントまたはログ出力できる方法について、TSS に説明されていることを検証しなければならない。

a) 送信元アドレスが、そのネットワークパケットが受信されたネットワークインタフェースのアドレスと等しいようなパケット
b) ネットワークパケットの送信元または宛先アドレスがリンクローカルアドレスであるようなパケット
c) 送信元アドレスが、そのネットワークパケットが受信されたネットワークインタフェースと関連するネットワークに属さないようなパケット、送信元アドレスが、所与のネットワークインタフェースと関連するネットワークに属するかどうか TOE が決定する方法の記述を含むこと。

ガイダンス文書

49 評価者は、要求されるルールを実装するように TOE が設定できる方法についてガイダンス文書に記述されていることを検証しなければならない。 ログ出力が設定可能な場合、評価者は、自動的に拒否されたパケットの監査について設定するために適用可能な指示が提供されていることを検証しなければならない。

テスト

50 テスト 1： 評価者は、トラフィックが受信された TOE ネットワークインタフェースとパケットの送信元アドレスが一致するようなネットワークトラフィックを破棄し、ログ出力するように TOE を設定しなければならない。評価者は、設定されたルールに一致するような適切なネットワークトラフィックを生成しなければならず、トラフィックが破棄されログメッセージが生成されることを検証しなければならない。

51 テスト 2： 評価者は、パケットがターゲットとするインタフェースのネットワーク到達性情報とパケットの送信元 IP アドレスが一致しないようなネットワークトラフィックを破棄し、ログ出力するように、TOE を設定しなければならない。 例えば、ネットワーク 192.168.1.0/24 がインタフェース 2 を介して到達

可能であると TOE が確信している場合、192.168.1.0/24 ネットワークからの送信元アドレスを持つネットワークトラフィックが生成され、インタフェース 2 以外のインタフェースへ送信されるべきである。 評価者は、ネットワークトラフィックが破棄されログメッセージが生成されることを検証しなければならない。

FFW_RUL_EXT.1.8

TSS

52 評価者は、デフォルトルールの処理、パケットが確立されたセションの一部であるかどうかの決定、及び管理者定義の順序付けられた規則 (ルールセット) の適用を含めて、着信パケットに適用されるアルゴリズムについて、TSS に記述されていることを検証しなければならない。

ガイダンス文書

53 評価者は、ステートフルトラフィックフィルタリングのルールの順序が決定される方法についてガイダンス文書に記述され、管理者がルールの処理順序を設定できるように必要な指示が提供されていることを検証しなければならない。

テスト

54 テスト 1： 評価者は、許可及び破棄 － という別の操作を行う以外は同一の 2 つのステートフルトラフィックフィルタリングのルールを考案しなければならない。 そして、ルールは、2 とおりの異なる順序で適用されるべきであり、どちらの場合についても評価者は、該当するパケットを生成してパケットキャプチャ及びログ出力により確認を行うことによって、両方の場合で最初のルールが適用されることを保証しなければならない。

55 テスト 2： 評価者は、一方が他方の部分集合 (例えば、特定のアドレスとネットワークセグメント) となるように 2 つのルールを考案するべきことを除き、上記の手順を繰り返さなければならない。ここでも、評価者は、ルールの特異性にかかわらず、最初のルールが適用されることを保証するため、両方の順序でテストすべきである。

FFW_RUL_EXT.1.9

TSS

56 評価者は、ステートフルトラフィックフィルタリングのルールが適用されるプロセスについて TSS に記述されていること、そしてそのふるまい (デフォルトで、または管理者の設定によりのいずれか) が、別の必要条件がネットワークトラフィックを許可することなしに一致するルールのない場合にはパケットを拒否することについても検証しなければならない (すなわち、FFW_RUL_EXT.1.5 または FFW_RUL_EXT.2.1)。

ガイダンス文書

57 評価者は、ガイダンス文書に、ネットワークトラフィックに対してルールや特別な条件が適用されない場合のふるまいが記述されていることを検証しなければならない。そのふるまいが設定可能な場合、一致するルールのない場合にはパケットを拒否するふるまいを設定するための適切な指示が、ガイダンス文

書に提供されていることを評価者は検証しなければならない。

テスト

58 FFW_RUL_EXT.1.2 の各属性について、評価者は、TOE がパケットヘッダからの属性を規則 (ルールセット) と正しく比較できることを実証するためのテストを構築しなければならず、またそれぞれの場合について許可と拒否の両方の場合について実証しなければならない。 評価者は、該当するルールが適用されたことを確認するために、それぞれの場合のログをチェックしなければならない。 評価者は、それぞれの場合について、正しい TOE のふるまいを実証するため、パケットキャプチャを記録しなければならない。

FFW_RUL_EXT.1.10

TSS

59 評価者は、ハーフオープンした TCP コネクションの数に関する情報を TOE が追跡し、保持する方法について、TSS に記述されていることを検証しなければならない。TSS には、管理者が定義した制限に達した時に、TOE がどのようにふるまうかについて識別されるべきであり、またどの条件でハーフオープンしたコネクションが削除されるのか (例、タイマーが時間切れになった後等) について記述されるべきである。

ガイダンス文書

60 評価者は、TCP のハーフオープンしたコネクションの制限が課されるふるまいと、未設定の場合のデフォルトの状態について、ガイダンス文書に記述されていることを検証しなければならない。 評価者は、例、宛先毎またはクライアント毎等、新しいコネクションが破棄される条件がガイダンスに明示されていることを検証しなければならない。

テスト

テスト 1： 評価者は、TOE 上で TCP のハーフオープンしたコネクションの制限を定義しなければならない。 評価者は、TOE を通過してターゲットシステムへ至る TCP SYN 要求を、ランダム化された送信元 IP アドレスと共通の宛先 IP アドレスを用いて生成しなければならない。 SYN 要求の数は、TOE 上で定義された TCP のハーフオープンの閾値を超えるべきである。 TCP SYN-ACK メッセージは、アクノリッジされるべきではない。評価者はパケットキャプチャによって、定義された TCP のハーフオープンの閾値に達すると、その後の TCP SYN パケットがターゲットシステムへ送信されないことを検証しなければならない。 評価者は、設定された閾値に達した時、選択に応じて、ログのエントリが生成されるか、カウンタが増加するかのどちらかであることを検証しなければならない。

2.2.2 FFW_RUL_EXT.2 動的プロトコルのステートフルフィルタリング

FFW_RUL_EXT.2.1

TSS

61 評価者は、動的パケットフィルタリングルールを自動作成させることが可能なプロトコルが TSS に特定されていることを検証しなければならない。場合によっては、動的ルールを作成するのではなく、一部の特定されたプロトコルのふるまいをサポートするために TOE がステートフルなセションを確立するこ

ともあるかもしれない。

62 評価者は、セション確立及び削除の動的な性質について TSS にて説明されていることを検証しなければならない。また TSS には、任意のログ出力の波及についても説明されなければならない。

63 評価者は、選択された各プロトコルについて、プロトコル特有のセション確立及び削除の動的な性質について TSS に説明されていることを検証しなければならない。

ガイダンス文書

64 評価者は、動的なセション確立機能について、ガイダンス文書に説明されていることを検証しなければならない。

65 評価者は、TSS と一貫した動的セションのログ出力について、ガイダンス文書に記述されていることを検証しなければならない。

テスト

66 テスト 1： 評価者は、サポートされるそれぞれのプロトコルについて、トラフィックを許可及びログ出力し、1024 を超える TCP 及び UDP ポートを破棄及びログ出力するようなトラフィックフィルタリングのルールを定義しなければならない。 その後、評価者は、選択されたプロトコルのそれぞれについて、コネクションを確立し、それが成功することを保証しなければならない。評価者は、それらがガイダンス文書と一貫していることを検証するため、生成されたログを検査しなければならない。

67 テスト 2： テスト 1 に引き続き、評価者は、制御プロトコルによって 1024 を超えるどのポートがオープンされるのかを (例、パケットスニファを用いて) 決定し、コネクションセションを終了し、そして同一の送信元及び宛先アドレス及びポートを用いて TCP または UDP (プロトコルの選択に応じて) パケットが TOE を通過して送信できないことを検証しなければならない。

68 テスト 3： 追加的にサポートされるプロトコルそれぞれについて、評価者は、上記の手順をそのプロトコルについて繰り返さなければならない。それぞれの場合について、評価者は、動的なルールが作成され、有効化されることを保証するため、どのポート範囲をブロックすればよいかを決定するために、該当する RFC または規格を使用しなければならない。

3 SAR の評価アクティビティ

69 SAR の追加の評価アクティビティ ([ND-SD]に加えて) は、ここでは定義されていない。

70 しかし、ステートフルトラフィックフィルタファイアウォールの脆弱性分析アクティビティに関する追加の詳細が、現文書の附属書 A に与えられている。

4 必須の補足情報

71 追加の必須の補足情報 ([ND-SD] の補足情報に加えて) は、ここでは定義されていない。

5 参考資料

[CC1] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 1：概説と一般モデル
CCMB-2012-09-001、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CC2] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 2：セキュリティ機能コンポーネント
CCMB-2012-09-002、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CC3] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 3：セキュリティ保証コンポーネント
CCMB-2012-09-003、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CEM] 情報技術セキュリティ評価のための共通方法、
評価方法
CCMB-2012-09-004、バージョン 3.1 改訂第 4 版、2012 年 9 月

[FWcPP] ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル
バージョン 1.0、2015 年 2 月 27 日

[NDcPP] ネットワークデバイスのコラボラティブプロテクションプロファイル
バージョン 1.0、2015 年 2 月 27 日

[ND-SD] ネットワークデバイス cPP の評価アクティビティ
バージョン 1.0、2015 年 2 月 27 日

[VAWP] ドラフト cPP 脆弱性分析ホワイトペーパー
バージョン 0.2 ドラフト

A. 脆弱性分析

A.1 序説

72 [ND-SD] には、従うべき脆弱性分析プロセスの詳細が含まれている ; その情報はここで繰り返さない。[FWcPP] に適合する TOE の脆弱性分析に必要とされる追加情報が、以下のセクションに含まれる。

A.2 追加の文書

73 [VAWP] には、TOE 開発者によって評価チームへ提供されることになる適切な追加文書を、技術種別に基づいて iTC が決定することが示されている。この文書は、cPP 評価アクティビティ及びその他の SAR において指示されるものへの追加である。

74 [ND-SD] に現在特定されているものに加えて、追加の文書は必要とされない。

A.3 脆弱性情報の情報源

75 [ND-SD] には、評価チームによって考慮されるべき 4 種類の欠陥が特定されている。種類のそれぞれについて、以下の追加情報が [FWcPP] に適合する TOE に提供される。

A.3.1 タイプ 1 仮説—公開脆弱性データベースに基づくもの

76 本サポート文書のセクション A.6 には、公開された脆弱性情報源のリスト、及びこれらの情報源のエントリ、[FWcPP] に適合する TOE において考慮されるべきタイプ 1 の欠陥仮説とみなされるべきものが含まれている。本リストを補足するために、評価者は、セクション A.6 の情報源であって cPP の公開日付よりも新しいもの、及び上記の追加の文書により特定されるとおり、TOE 及びそのコンポーネントに特有なものについても検索を行わなければならない。特定のエントリ、あるいは同一または異なる情報源からのエントリから生成された欠陥仮説に重複があれば、評価チームは、それを記録した上で考慮から外すことができる。

77 cPP の公開日以降に公開された CVE を検索する時に用いられるべき検索基準には、以下のものが含まれなければならない :

- 「ファイアウォール (firewall)」という用語
- 以下のプロトコル : TCP、UDP、IPv4、IPv6
- TOE によって (SFR を介して) サポートされる、上に列挙されていない任意のプロトコル。

78 TOE の特定コンポーネントのタイプ 1 欠陥仮説生成の一部として、評価者は、コンポーネント製造業者のウェブサイトについても検索し、これを基盤として欠陥仮説が作成できるかどうかを決定しなければならない (例えば、評価中のコンポーネントのバージョンにセキュリティパッチがリリースされている場合、これらのパッチの対象が欠陥仮説の基盤を形成するかもしれない)。

A.3.2 タイプ 2 仮説—iTC によって作成されたもの

79 セクション **A.7** には、iTC によって本 cPP のために作成された欠陥仮説のリストが含まれる。タイプ 3 またはタイプ 4 の欠陥であって、本 cPP の将来のバージョンでは、セクション A.7 に含めることを考慮されるべきと評価者が確信するものを発見した場合、評価者は、iTC による検討のため、非独占的な欠陥の追加事項を提出すること。

A.3.3 タイプ 3 仮説—評価チームによって作成されたもの

80 [ND-SD] に含まれるものに加えて、追加のガイダンスは提供されない。

A.3.4 タイプ 4 仮説—ツールによって作成されたもの

81 評価者は、タイプ 4 欠陥仮説を生成するために、以下のアクティビティを実行しなければならない：

- ファジングテスト
  - 以下の送信の影響を検査する：
    - 各「Type」と「Code」の値が、ICMPv4 (RFC 792) 及び ICMPv6 (RFC 4443) のそれぞれに対応する RFC において未定義であるような、変形したパケット
    - 各「トランスポート層プロトコル」の値が、IPv4 (RFC 791) 及び IPv6 (RFC 2460) のそれぞれに対応する RFC において未定義であるような、変形したパケット。

    これらのパケットがいずれも、ルールに一致したり、または許可されたセションに属したりすることはないため、パケットは破棄されるべきである。 評価者は、これらのパケットが TOE を通過して流れることをファイアウォールが許可しないことを保証しなければならない。
  - 要求されるプロトコルヘッダの残りのフィールドについての変形ファジングテスト。このテストには、注意深く選択された値とランダムな値の両方が各ヘッダフィールドへ順番に挿入された整形されたパケットの変形したものを送信することを要求する (すなわち、テストには注意深く選択されたテストケースとランダムに挿入されたテストケースの両方が含まれる)。元の整形されたパケットは、通常の既存の通信ストリームの一部として受け入れられるであろうし、注意深く選択された変形が行われた際にも依然として有効なパケットとして受け入れられるかもしれない (個別のパケットだけでは有効となるだろうが、その内容は前後のパケットでは有効でないかもしれない) が、ランダムな値がフィールドへ挿入された際には有効なパケットではなくなることが多い。注意深く選択された値には、そのフィールドが表すデータの種別から決定できるような意味のある重要な値、例えば正負の整数、境界条件、無効な 2 値の組み合わせ (例、ビット間に依存関係のある一連のフラグ) を示す値、及び開始値または終了値を欠いたもの等が含まれるべきである。ランダムに選択された値によって整形されたパケットを得られないかもしれないが、それでもなお、それによってデバイスがセキュアでない状態になるかどうかを確認するために含まれている。予期されない結果 (例、コアダンプ等) は、

欠陥仮説の候補となる。

82 iTC は、上記の欠陥仮説の作成アクティビティを達成するために用いられる具体的なツールを識別していないため、評価チームによって用いられる任意のツールが受け入れ可能である。評価チームは、このアクティビティで使用されたすべてのテストツールの名称、バージョン、パラメタ、及び結果をテスト報告書に記録しなければならない。

A.4 評価者脆弱性分析のプロセス

83 従うべきプロセスは、[ND-SD] に記述されている。

A.5 報告

84 報告アクティビティは、[ND-SD] に記述されている。

A.6 欠陥仮説のための CVE エントリ

85 このリストには、現在のところエントリが定義されていない。

A.7 追加の欠陥仮説

86 このリストには、現在のところエントリが定義されていない。

A.8 iTC のアクティビティ—cPP 及びサポート文書の維持管理

87 [ND-SD] の附属書 A に示されるように、何が公的に報告されるのかに関して脆弱性分析の適用範囲を決定するにあたって iTC が重要な役割を果たす。[ND-SD] のセクション A.8 では、評価チームにより調査されるべき欠陥が識別され、本 PP に適合する TOE の全般的な保証レベルと同等であり、かつこの技術について iTC によって懸念される領域を網羅することを保証するために iTC が行わなければならないアクティビティが詳述されている。

B. ファイアウォールの等価性の考察

88 追加の等価性の考察 ([ND-SD] に加えて) はここでは定義されない。