Firewall/UTM/L3スイッチ

自動ポリシーテスタ

Firewall Tester

取扱説明書

Version 1.1 対応

2018年4月18日

日本シー・エー・ディー株式会社

はじめに

このたびは Firewall/UTM自動テストツールFirewallTester(以下「本製品」)をお買い上げいただき、誠にありがとうございます。

ご注意

- 本ガイドの内容の一部でも無断転載することは禁止されています。
- 本ガイドの内容は、将来予告なく変更することがあります。

本製品に関する最新の情報は、製品サポートサイト

http://firewall-tester.com

をご覧ください。

総販売店・サポート窓口

ネットチャート株式会社

神奈川県横浜市港北区新横浜2-15-10 YS新横浜ビル8F

fwt-sales@ncj.co.jp

開発元

日本シー・エー・ディー株式会社

〒161-0033

東京都新宿区下落合2-14-1　CADビル

http://www.ncad.co.jp/

目次

安全上のご注意

ご使用の前に、安全上のご注意をよくお読みのうえ、正しくお使いください。

 警告	取扱いを誤った場合、死亡もしくは重傷を負う可能性または物的損害の発生が想定されます。

 禁止	付属の電源アダプタ以外を使用しない 発熱、発火、破裂、感電、けが、故障の原因になります。
 禁止	コンセントや配線器具の定格を超える使い方や、AC100V以外で使用しない 発熱により発火の原因になります。
 禁止	電源コード・プラグを破損するようなことをしない 傷んだまま使用すると発火、感電、故障の原因になります。
 指示	電源プラグを根元まで確実に差し込む 差し込みが不完全な場合、感電や発火の原因になります。
 禁止	本機、電源アダプタを分解、修理、改造しない 発熱、発火、破裂、感電、けが、故障の原因になります。
 指示	電源プラグのほこり等は定期的にとる プラグにほこり等がたまると、湿気等で絶縁不良となり、発火の原因になります。
 禁止	内部に金属を入れたりしない ショートや発熱による発火または感電の原因になります。
 禁止	水などの液体にぬらさない 水などの液体にぬれた状態で使用しない ショートや発熱による発火、破裂または感電の原因になります。
 禁止	本機、電源アダプタを落としたり、強い衝撃をあたえない 発熱、発火、破裂、けが、故障の原因になります。
 禁止	ぬれた手で電源プラグの抜き差しはしない 感電の原因になります。

指示

次のような異常があったときは、電源プラグを抜き、使用しない

- 内部に金属や水などの液体が入ったとき
- 落下などで外装ケースが破損したとき
- 煙、異臭、異音が出たとき

そのまま使用するとショートや発熱による発火、破裂または感電の原因になります。

注意

取扱いを誤った場合、傷害を負う可能性または物的損害の発生が想定されます。

 禁止 本機、電源アダプタを異常に温度が高くなるところに置かない 外装ケースや内部部品が劣化するほか、発火の原因になることがあります。	 禁止 本機、電源アダプタの放熱を妨げない 外装ケースや内部部品が劣化するほか、発火の原因になることがあります。
 禁止 本機、電源アダプタを不安定な場所に置かない 落下すると、けが、故障、発火の原因になることがあります。	 禁止 本機、電源アダプタの上に物を置かない 重量で外装ケースが変形し、内部部品の破損、故障や発火の原因になることがあります。

お願いとご注意

- 本製品に使用されているソフトウェアの無断複製・解析は禁止されています。
- 本製品に使用されている意匠、商標の無断使用は禁止されています。
- 本製品のハードウェアの転用は禁止されています。
- 本製品は日本国内の使用を前提として設計・開発・製造されていますので、海外では使用しないでください。
- 本製品は、一般的な情報通信回線用途として設計・製造されています。従って、生命、財産に著しく影響を及ぼすため、高信頼性を要求される制御・監視等のシステム

（原子力発電設備、医療設備等の動作を制御または監視するシステム等）の用途では使用しないください。

VCCI-A対応

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。その場合、使用者が適切な対策を講ずるよう要求されることがあります。

免責事項について

- 本製品の使用または使用不能から生ずる派生的または付随的な損害（情報内容の変化、情報の喪失、事業利益の喪失、事業の中断、他製品・システムへの損害など）に関して、当社は責任を負いかねますので予めご了承ください。

- 地震、雷、風水害、当社の責に帰さない火災、第三者による行為、その他の事故、お客様の故意、過失、誤用、その他の異常な条件での使用により生じた損害に関して、当社は責任を負いかねますので予めご了承ください。

- 本ガイドの記載内容を守らないことにより生じた損害に関して、当社は責任を負いかねますので予めご了承ください。

- 当社指定外の機器、ソフトウェアとの組み合わせによる誤動作から生じた損害に関して、当社は責任を負いかねますので予めご了承ください。

知的財産権等

- 本製品に搭載されているFirewallTesterのソフトウェアに関する著作権その他の知的財産権は、日本シー・エー・ディー株式会社が所有するものです。
- Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- Macintosh は米国 Apple Inc の米国およびその他の国における登録商標です。

ソフトウェアの使用許諾条件

日本シー・エー・ディー株式会社（以下、「NCAD」といいます）が提供する本製品上のソフトウェア（以下、「本ソフトウェア」といいます）には、以下の条件が適用されます。お客様は、本製品を使用することにより、以下の条件を承諾したものとみなされます。

1. 使用許諾

① 本ソフトウェアは使用許諾されるものであり、販売されるものではありません。

② お客様には、本製品に組み込まれた形態で本ソフトウェアを使用する非独占的な権利が許諾されます。

③ お客様は、本ソフトウェアを改変または複製できません。本ソフトウェアをベースにしたソフトウェアを作成することもできません。

2. 著作権等

① 本ソフトウェアに関するすべての権利は、NCADおよびそのライセンサーが所有しています。

② 本ソフトウェアに関する著作権その他のいかなる知的財産もお客様に譲渡されるものではありません。

③ お客様は、本ソフトウェアおよび関連資料に使用されている著作権表示、商標その他の表示を除去できません。

3. リバースエンジニアリング

お客様は、自身でまたは第三者をして、本ソフトウェアのリバースエンジニアリング、逆コンパイル、逆アセンブルを行うことができません。

4. サポート契約

本ソフトウェアの更新は、別途締結される本製品のサポート契約で提供されます。

5. 責任の限定

NCAD（そのライセンサーを含む）は、本ソフトウェアの使用または使用不能から生じたお客様の損害等について一切責任を負いません。

6. 輸出管理

お客様は、本ソフトウェアに関し、日本の外国為替及び外国貿易法ならびに関係法令（以下、「法令等」といいます）を順守し、法令等に基づく許可およびNCAD（そのライセンサーを含む）の承認なく、本ソフトウェアを直接または間接的に輸出（海外への持ち出しを含む）しないものとします。

7. ライセンサーの権利

お客様は、本ソフトウェアに関するNCADのライセンサーが自己の名義で本契約書に基づき権利を行使できることを了承します。

8. 管轄裁判所

本ソフトウェア契約に関し紛争が生じた場合には、東京地方裁判所を管轄裁判所とするものとします。

以上

1　本製品概要

1.1　本製品について

本製品は構築したFirwall/UTM/L3スイッチのACLやFirewallポリシーを自動的にテストし、結果をCSVで保存するためのツールです。

1.2　本製品の機能

1.2.1　Firewallテスト機能

決められた通信を本製品で実行し、通信が疎通する、疎通しない、意図しない通信をするなどの結果を取得します。

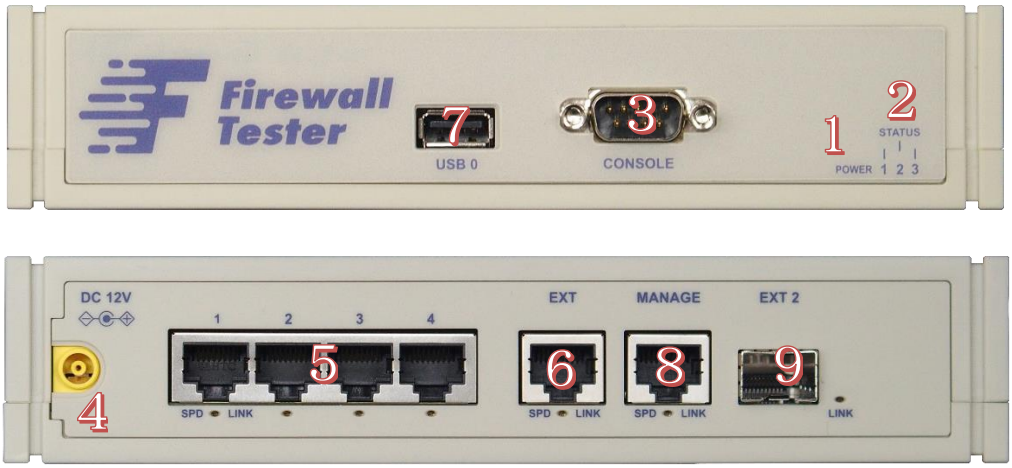
1.2.2　PPPoEサーバ機能

本製品のLANインターフェース一つにPPPoEサーバを設定することで、プロバイダに接続している状態と同じ状態で試験を行うことが可能です。

2　ご使用の前に

本製品をご使用いただく前に必要な、各部の名称や接続方法を解説します。

2.1　各部の名称



1	電源LED
2	ステータスLED
3	シリアルポート(メンテナンス用につき、使用しないでください)
4	電源ジャック
5	試験用untag LANポート
6	試験用VLAN tag LANポート
7	USB端子 (メンテナンス用につき、使用しないでください)
8	管理用LANポート
9	拡張用SPFポート(現在は使用できません)

✴ 3.7.9.はメンテナンスと修理のために、指定された技術者のみが使用する端子です。お客様がこれらの端子を使用することで機器の不具合が起きた場合、弊社はその不具合または不具合によって引き起こされた他の機器、システムへの不具合については一切責任を負いかねます。

2.2　準備するもの

機器本体	本製品
ACアダプタ	本製品に同梱
LANケーブル(ストレート)	1mのケーブルを同梱してあります。
管理用PC	お客様でご用意ください。

✴ 管理用PCは、イーサネットのLANポートがあり(無線LANは不可)、かつ一般的なWebブラウザが動作すれば運用可能することができます。また、管理用PCに本製品専用の特別なソフトをインストールする必要はありません。

2.3　電源ケーブルの接続

付属のアダプタを電源コネクタに接続してください。本製品に電源が接続されると自動的に起動し、電源LED（緑）が点灯します。起動処理中はステータスSTATUS1が赤く点滅します。その後1分程度で起動が完了するとステータスLED1が緑色の点滅に変わり、動作可能な状態になります。

2.4　動作の終了

本製品は、接続されているACアダプタの電源ケーブルを抜くと動作を終了します。

※設定情報の書き込みを行なっている最中に終了してしまうと設定情報が正しく保存されない事がありますので、LEDが1個でも赤く”点灯”している時は電源ケーブルを抜かないでください。

3　ネットワーク接続の設定

本製品をネットワークに接続するための設定を行います。
本装置の初期IPは192.168.20.1/24となっておりますので、適切なIPアドレスをパソコンに設定しブラウザでアクセスを行ってください。

3.1　本製品の接続

本製品のLANコネクタ(MNG)と管理用PCをLANケーブルで直接繋いでください。

3.2　本製品の管理画面にアクセス

本製品は管理用にWebインタフェース(以下、管理画面といいます)を備えています。
ここでは、管理画面にアクセスする方法を解説します。

3.2.3　Webブラウザの起動

管理画面にアクセスするために、管理用PCでWebブラウザ（以下、ブラウザ）を起動します。

3.2.4　ケーブルの接続

管理用のPCとFirewallTesterのMANAGEポートをLANケーブルで接続します。

3.2.5 本製品の初期IPアドレスを入力

本製品は、出荷時に固定の初期IPアドレスが設定されています。

ブラウザのアドレス欄に以下の初期IPアドレスを入力して本製品にアクセスします。

多くの情報を表示するため、画面解像度はFULL-HDを推奨いたします。

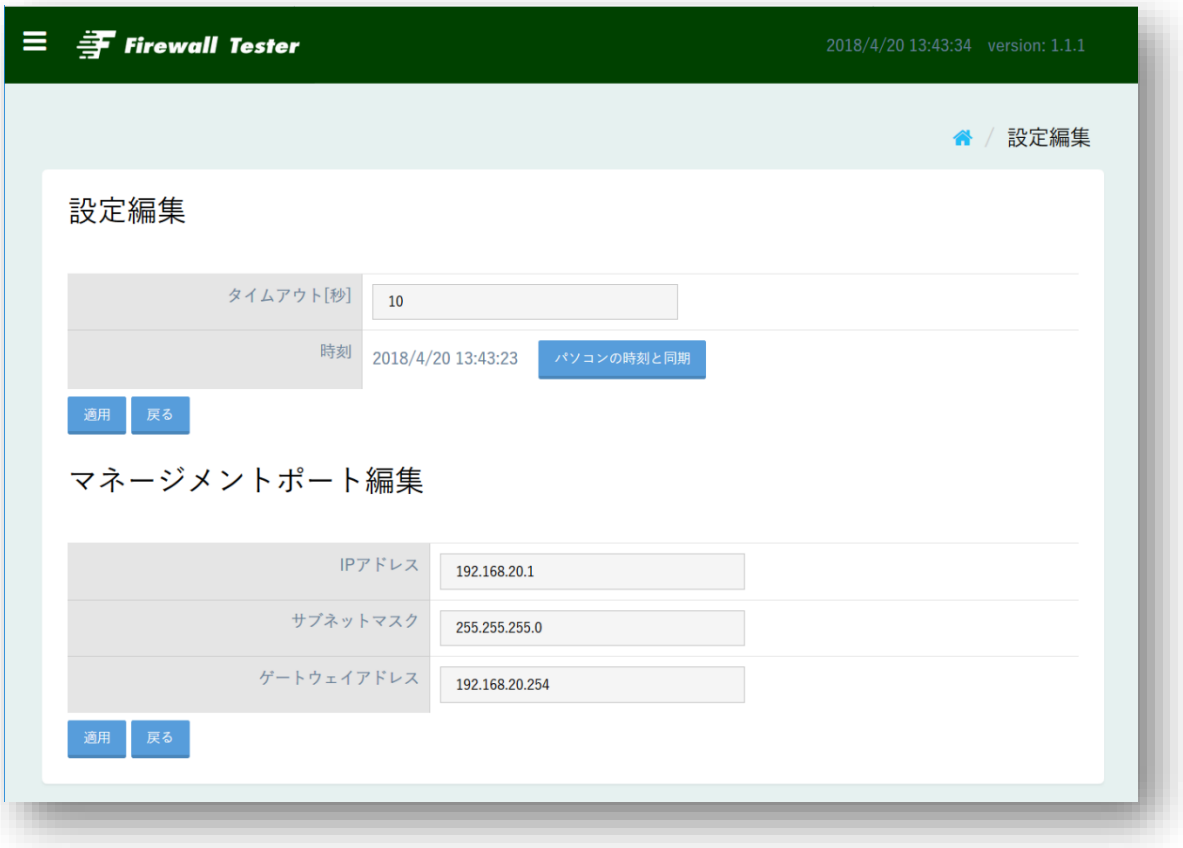
初期アドレス	http://192.168.20.1

ログインのための、ID、パスワードはありません。

3.3　メニュー項目

3.3.1設定編集

試験時のタイムアウト時間や管理ポートのIPアドレスを変更する場合は、メインメニューの「設定変更」を選択し、設定を投入後「適用」ボタンをクリックします。



3.3.2 サービス定義

本製品はFirewallが使用する各種管理サーバ機能として以下のサービスを内部に作成することが可能です。

(1)　Syslog

Firewallから送信されるSyslogを記録し表示させることが可能です。

(2)　DNS

bindのゾーンファイルの内容を書き込むことでDNSサーバとして動作し、Firewallからの名前解決が可能になります。

(3)　メール

SMTPサーバとして動作し、Firewallが送信したメールを表示することが可能です。

(4)　SNMP

SNMPTrapを受信し、メッセージを表示します。

(5)　NTP

FirewallからのNTPリクエストに応答し、本製品の時刻と同期させます。

各サービスはサービスを起動するインターフェース上で動作します。

制限事項：立ち上げるインターフェースと同じサブネットのIPアドレス以外では正常に動作いたしません。

3.3.3 ファームウェアアップデート

本製品のファームウェアをアップデートするときは、ファームウェアアップデート画面を選択し、アップデートファイルを指定後「アップデート」ボタンをクリックします。しばらくすると本体が再起動されるので、再起動が終了したら再びブラウザ画面で接続してください。

3.4　テスト環境の設定

テスト環境は以下の流れで設定を行います。

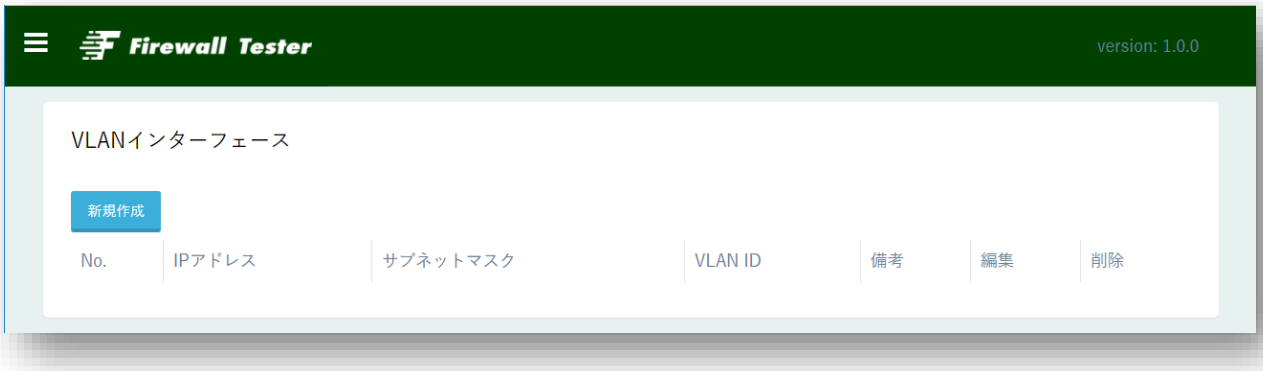
(1)　各インターフェースのIPアドレス設定

FirewallTesterのインターフェースはFirewall/UTMから見たとき、NextHopRouterアドレスになります。NextHopRouterが無い場合はFirewallのインターフェースと同じサブネット内の任意のIPアドレスを指定してください。

(2)　VLANインターフェース設定

VLANインターフェースは任意のVLAN IDを指定しインターフェースを作成することが可能になります。

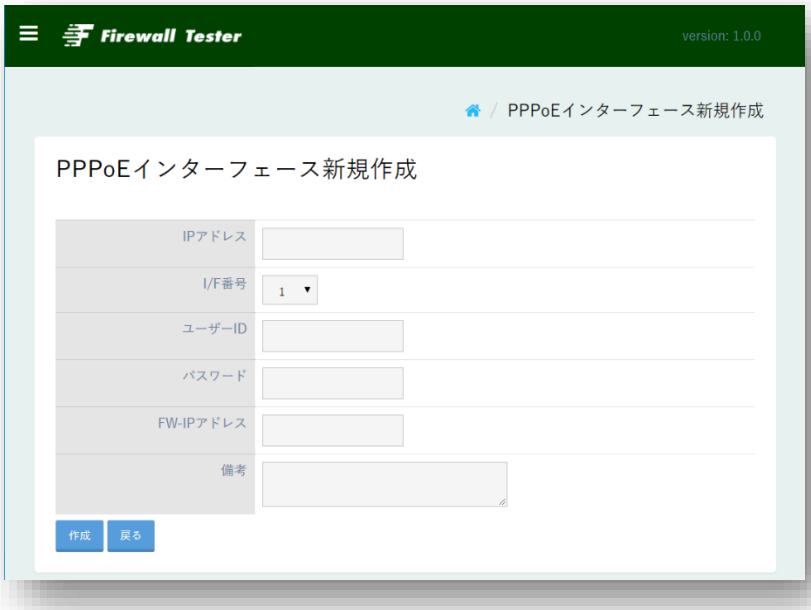
VLANインターフェースは任意の数が作成可能で、すべてEXTインターフェースに割り当てられます。



(3)　PPPoEインターフェース

PPPoEサーバ機能を有効にします。

FirewallからPPPoEの接続要求があると、PPPoE接続が行われます。

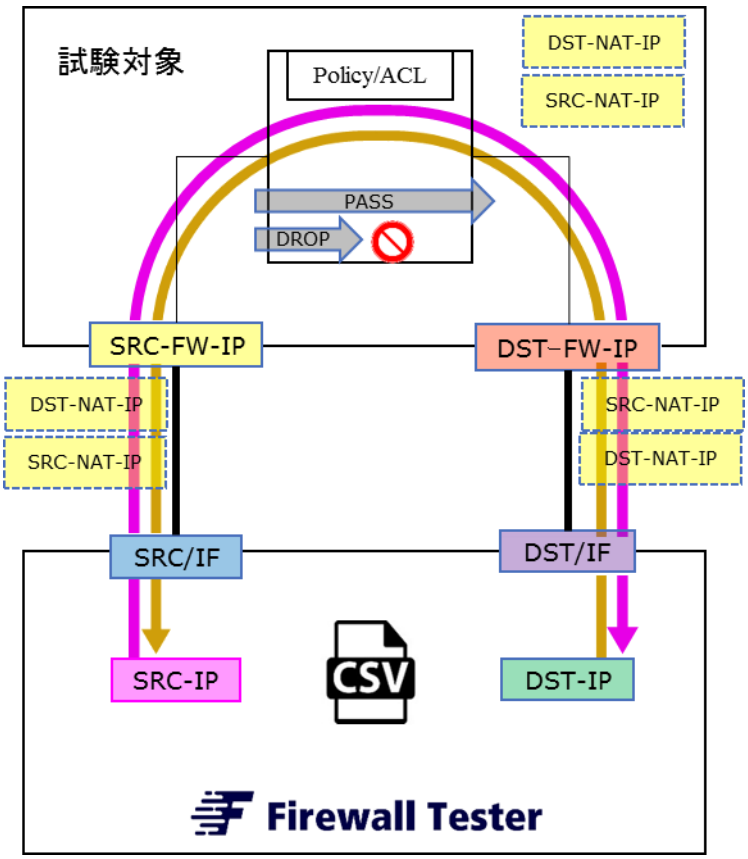


※PPPoEはNumberedモードにのみ対応しており、UnNumberedのサービスには対応しておりません。

4．ポリシー設定

4.1 テストポリシーと、ネットワーク構成の関係

テストポリシーの各カラムと、実際に通信するアドレスの位置の関係は以下の通りとなります。Firewallと本器のインターフェースは同じサブネットとなりますが、SRC-IPとDST-IP、NAT-IPは任意のIPを指定することが可能です。



4.2 ポリシーの作成

ポリシーは3つの方法で作成が可能です

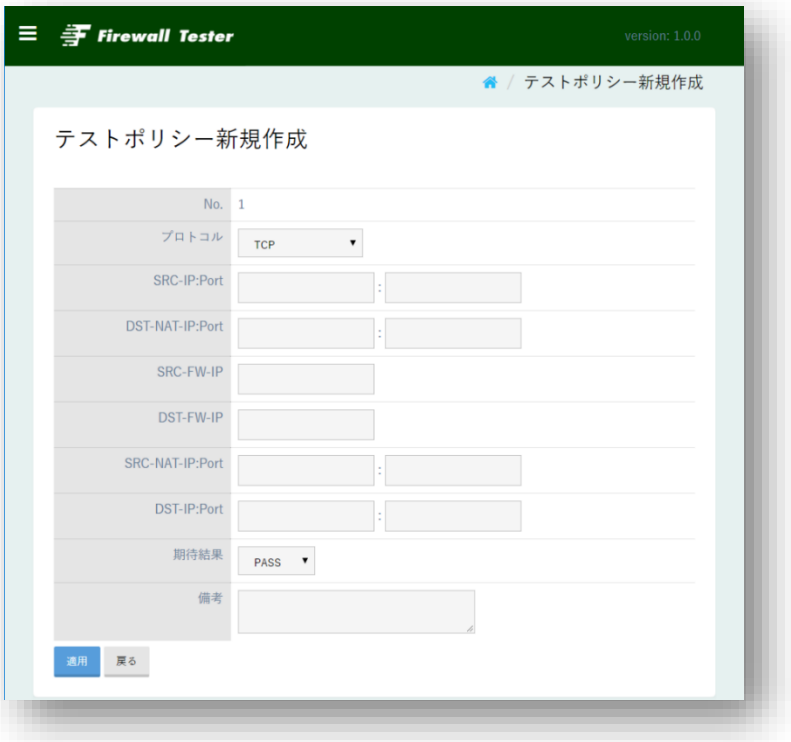
(1)　GUIから個別に作成する

(2)　Excelやテキストエディタを使用して CSVかTSVファイルをアップロードする

(3)　Excelで作成したセルをペーストする

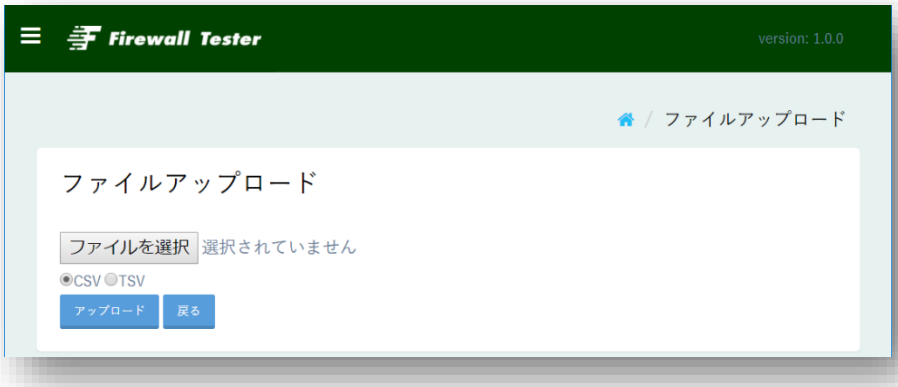
（※ CSV　カンマ区切りのテキスト、TSV　タブ区切りのテキスト）

・GUIによる個別作成



・CSV/TSVによるアップロード

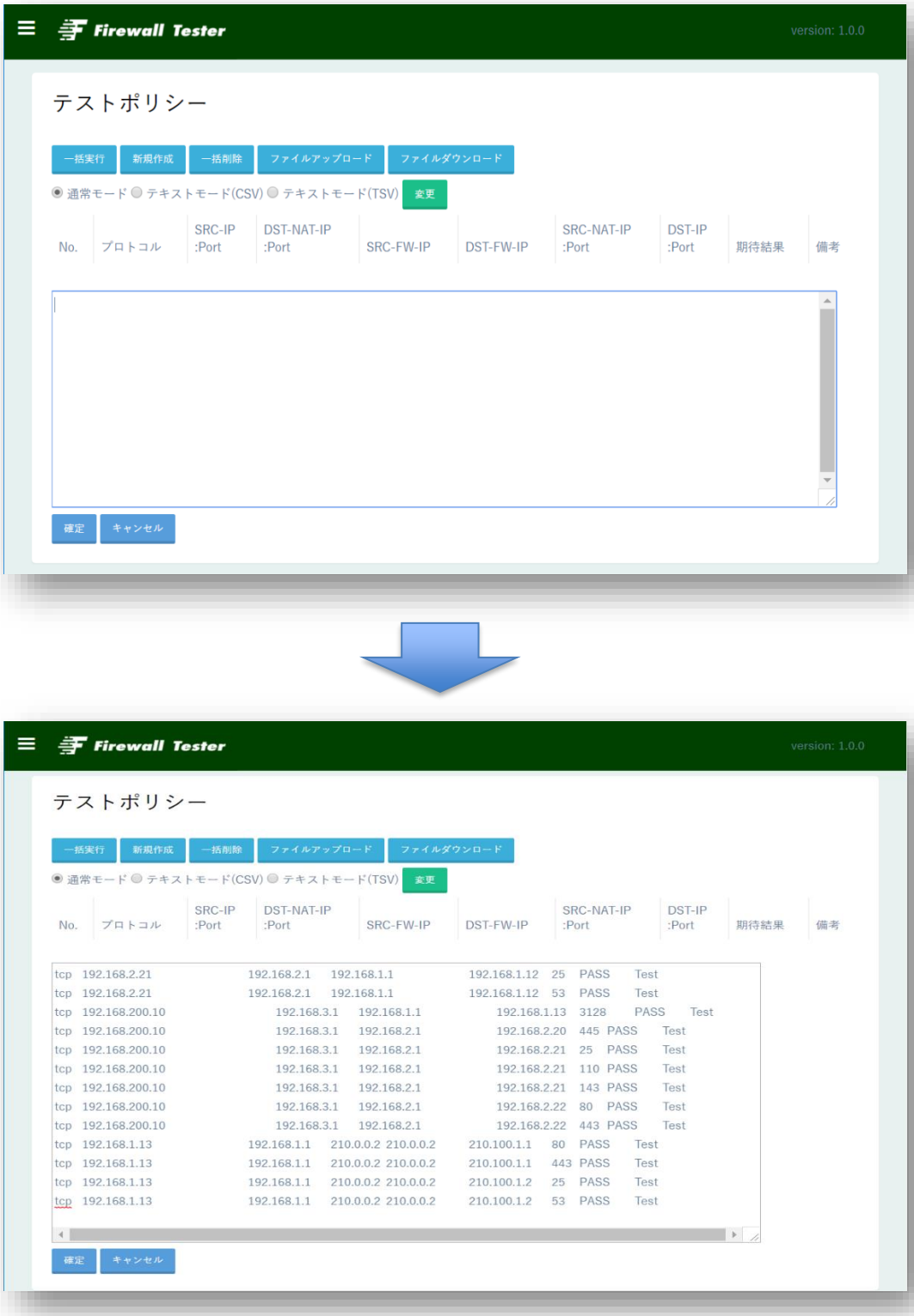
CSV/TSVによるアップロードを行う場合は、あらかじめ、ファイルダウンロードメニューから、空のファイルをダウンロードすると、カラム名だけの入ったファイルを入手できますので、そのファイルを編集していただくことが可能です。



※ファイルにはBOMは入れない様に、UTF-8Nで保存をお願いします。Windowsのメモ帳を使用すると、BOMが強制的に挿入され、正常に動作しない場合があります。

・TSV/CSVの貼り付け

Excelでテストパターンを作成してテストする場合は、TSVを使用してください。



ポリシー投入完了

一括実行	すべてのテストパターンを一括で実行します。
新規作成	新規にテストパターンを１つ作成します。
一括削除	すべてのテストパターンを削除します。
ファイルアップロード	テストポリシーの書かれたCSVまたはTSVファイルをアップロードします。
ファイルダウンロード	テストパターンデータ及び、テスト結果を含むCSVまたはTSVファイルをダウンロードします。
変更	ポリシーの表示モードを切り替えます。

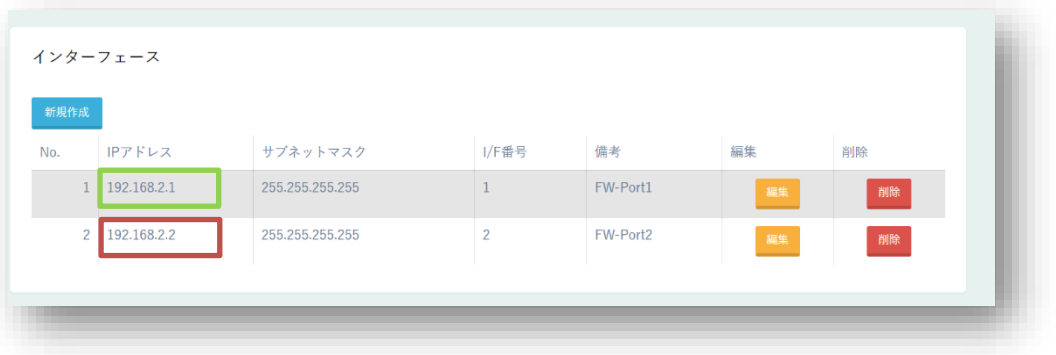
編集	指定のポリシーをGUIで編集します。
削除	指定のポリシーを1行削除します。
実行	指定したポリシーを個別に実行します。

5．L1/L2モードによる試験

本製品はルータモードのFirewall以外に、Paloaltoのバーチャルワイヤ、各種Firewallのブリッジモードにも対応します。

その際は以下の様な設定を行ってください。

（1）FirewallTesterのインターフェースの設定を任意の32ビットマスクのIPで設定します。このIPはFirewallTesterがパケットの送受信を行うインターフェースを決めるためのものなので、任意のIPを設定することができます。



（2）ポリシー作成時にSRC-FW-IPとDST-FW-IPにSource側とDestination側のインターフェースを指定するために、FirewallTesterのインターフェースのIPを入力します。

（3）この設定を行うことで、FirewallTesterのSRC-FW-IPの設定されたインターフェースからDST-FW-IPの設定されたインターフェースに向けて試験パケットを送信します。IPアドレスは任意のアドレスを使用することが可能です。

Firewall Tester

2018年４月18日

総販売店・サポート窓口

ネットチャート株式会社

神奈川県横浜市港北区新横浜2-15-10 YS新横浜ビル8F

fwt-sales@ncj.co.jp

開発元

日本シー・エー・ディー株式会社

〒161-0033 東京都新宿区下落合2-14-1 CADビル

http://www.ncad.co.jp/