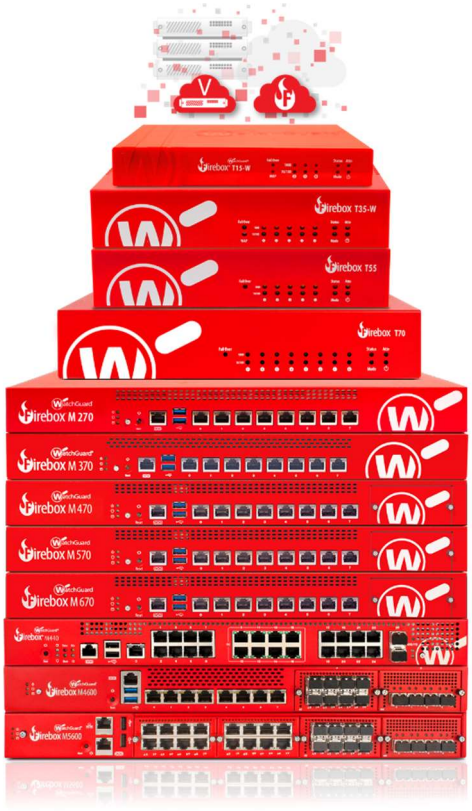
WSM
WatchGuard System Manager
詳細設定ガイド



ウォッチガード・テクノロジー・ジャパン株式会社
2019 年 5 月 Rev 5

目次

はじめに

この度はウォッチガード製品を選定していただきありがとうございます。

本書は、WSM 基本設定ガイドで触れることのできなかった詳細な設定、大規模ネットワークや高負荷な環境に対応するための方法などを、具体的なケースを交えながら解説しています。

前提として WSM 基本設定ガイド レベルの知識が必要ですので、まだお読みになっていない方はご一読されることをお勧めいたします。

なお、本書で使用されている設定画面は、2019 年 5 月時点での最新バージョン Fireware XTM OS v12.4 のものです。

このガイドが、Firebox を自在に使いこなす一助になれば幸いです。

第一章　ネットワーク構成

WSM 基本設定ガイドでは、Firebox のデフォルトの動作モードである「ルーティングモード」での設定を一通り解説しました。

この詳細設定ガイドでは Firebox を透過的に使用するための「ブリッジモード」(トランスペアレントモードとも言います)で運用するケースとそのための設定方法、さらには Firebox のもう一つの動作モードであるドロップインモードでの設定方法についても解説します。

ブリッジモードでの運用

ブリッジモードで構成する場合 Firebox は管理用の IP アドレスのみで運用されます。この場合の Firebox は透過的に動作し、既存のネットワークの構成を変更することなく UTM 機能を適用することが可能になります。

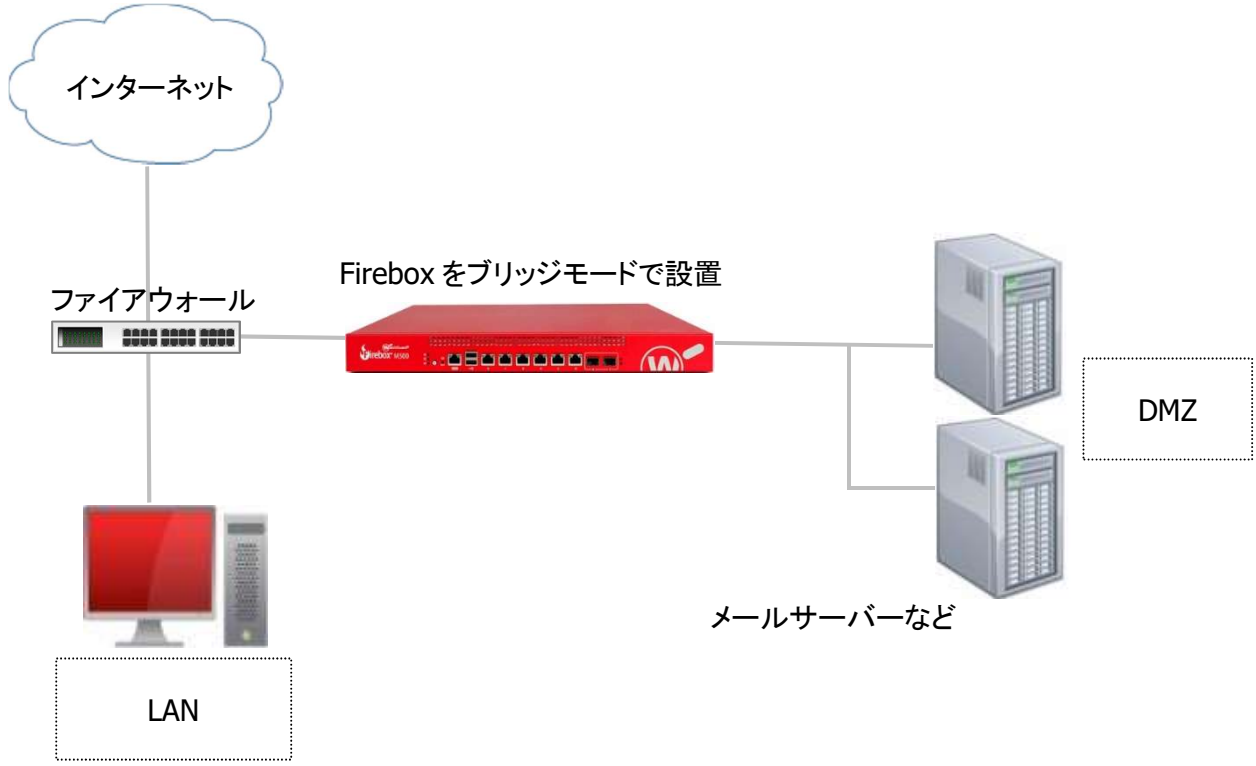
ただしブリッジモードはその名のとおり L2(レイヤー2)で動作するので、下記の機能は使用できなくなります。

- マルチ WAN
- VLAN
- FireCluster (HA 構成)
- セカンダリネットワーク
- DHCP および DHCP リレー
- 1to1NAT およびダイナミック NAT
- ダイナミックルーティング(OSPF,BGP,RIP)
- すべての VPN 機能

構成例

ブリッジモードを利用する実際的な例として、ここではサーバーを保護する UTM として構成する手順をご紹介します。

この例では、既存のファイアウォールと DMZ にあるサーバーの間に Firebox を挟み込む形で設置しています。ブリッジモードで動作させることにより、既存のファイアウォールやサーバーの設定を変更せずに spamBlocker(アンチスパム)や IPS などの UTM 機能を追加することができます。



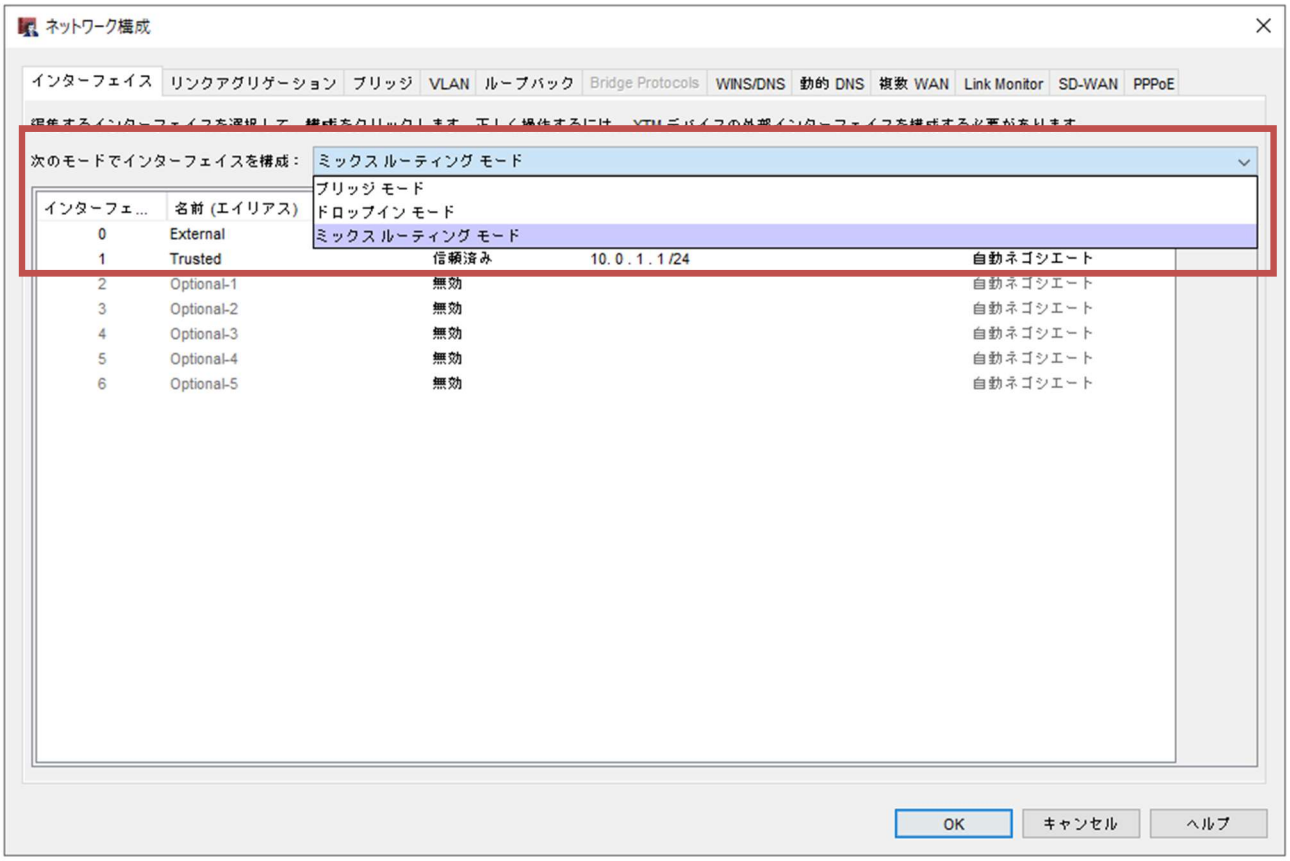
設定するにあたり、このネットワークの設定を以下のように想定します。

ファイアウォールの DMZ 側の IP アドレス	172.16.1.1
Firebox に設定する IP アドレス	172.16.1.254
メールサーバーの IP アドレス	172.16.1.51

ネットワークの設定

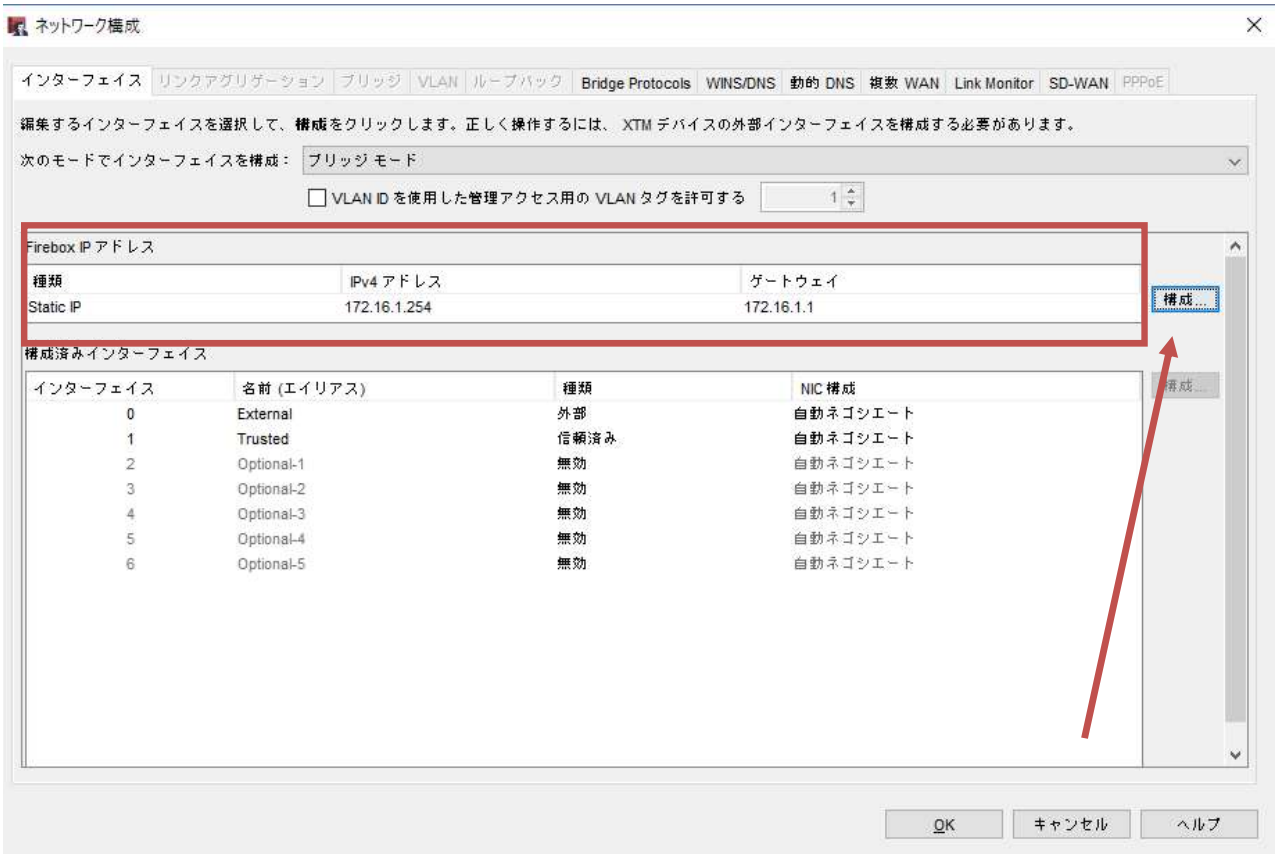
ポリシーマネージャのメニューにある*ネットワーク* ― *構成* をクリックし、ネットワーク構成の画面を開きます。

インターフェイスのモードを指定するリストからブリッジモードを選択します。



IPv4 アドレスは XMT に設定する IP アドレスである 172.16.1.254/24 を入力します。これが WSM で接続する際の管理 IP アドレスになります。

ゲートウェイの欄には上位のファイアウォールの DMZ 側ポートの 172.16.1.1 を指定します。



その横の[構成]ボタンをクリックすると、ブリッジモードのプロパティを設定できます。

とはいえ、設定できる項目はそれほど多くありません。

Firebox は接続されているデバイスの MAC アドレスを自動的に登録し、ルーティングテーブルに保存してゆきますが、それを有効にするチェックが「自動ホストマッピング」です。基本的にはどれもチェックを入れておくべきでしょう。

「関連ホスト」の項では、手動でデバイスの接続を構成する場合、または自動ホスト マッピング機能が正常に動作しない場合、関連するホスト エントリを追加できます。

関連ホスト エントリは、1 つのホストの IP アドレスと 1 つのネットワークインターフェイスの間に静的ルートを作成します。デフォルトでは Firebox の外部インターフェイスとデフォルトゲートウェイとなっているファイアウォールの IP アドレスが関連付けられています。

[OK]をクリックし、設定を保存します。

次にポリシーを設定します。

spamBlocker の設定

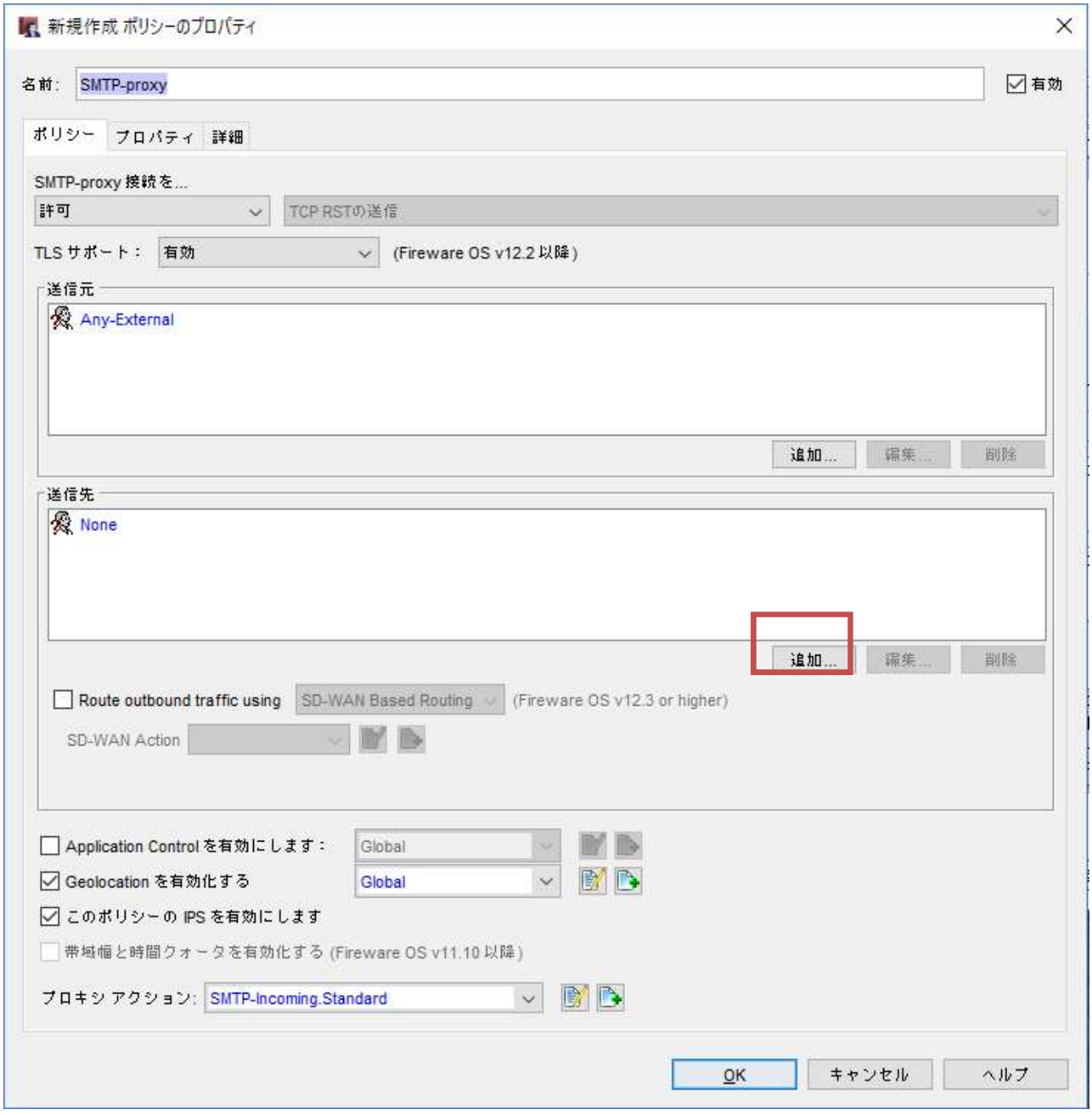
WSM 基本設定ガイドでは、UTM 機能を有効にする際にウィザードを使っていましたが、ここでは手動でポリシーを追加し、spamBlocker を有効にしてみましょう。

ポリシーマネージャで[ポリシー追加]ボタンをクリックし、以下の追加画面で SMTP-proxy を選択し、[追加]ボタンをクリックします。

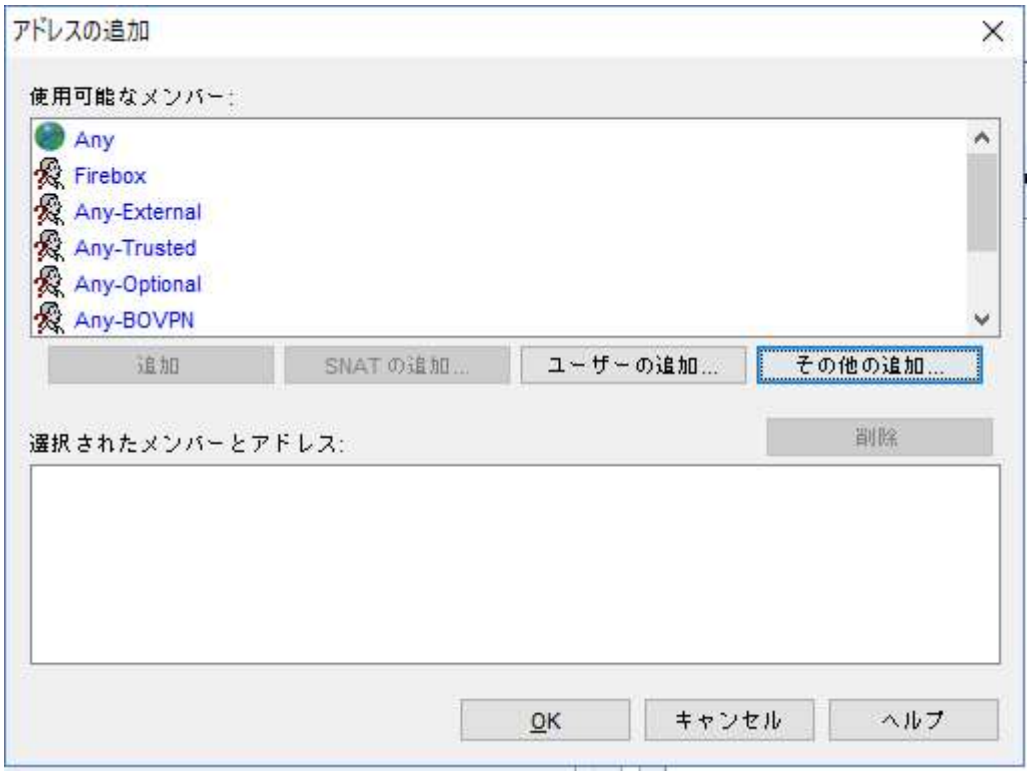
ポリシーの新規作成画面が開きます。

SMTP-proxy は基本的に Incoming のポリシーなので、送信元は Any-External、送信先は未設定の状態になっています。

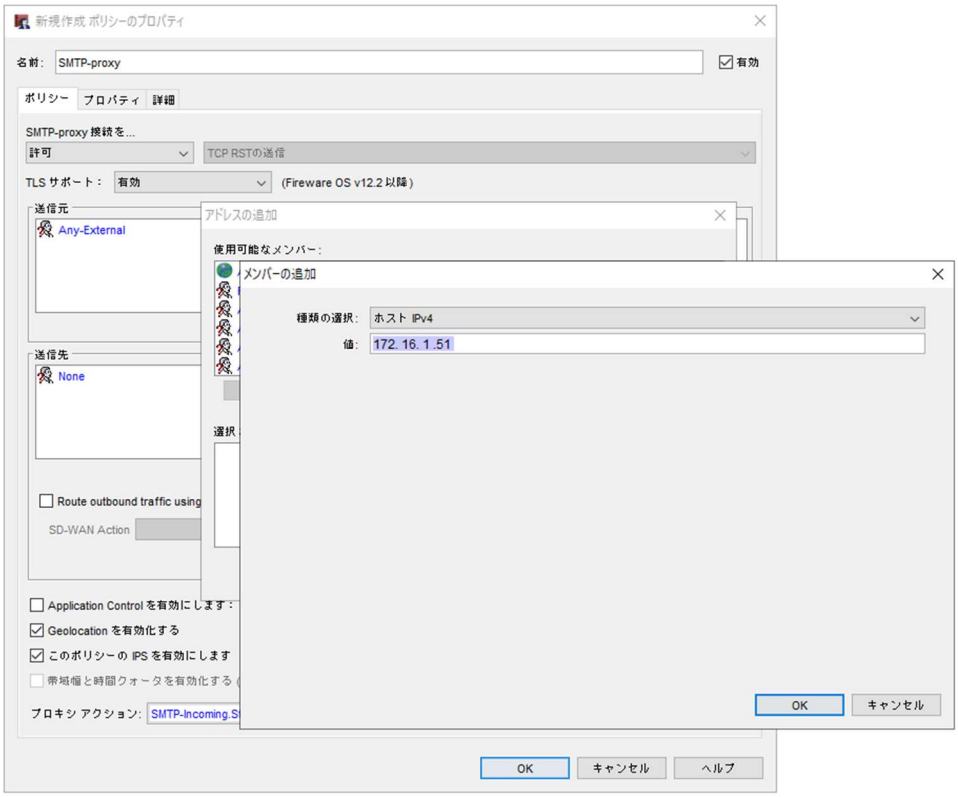
送信先の[追加]ボタンをクリックし、設定しましょう。



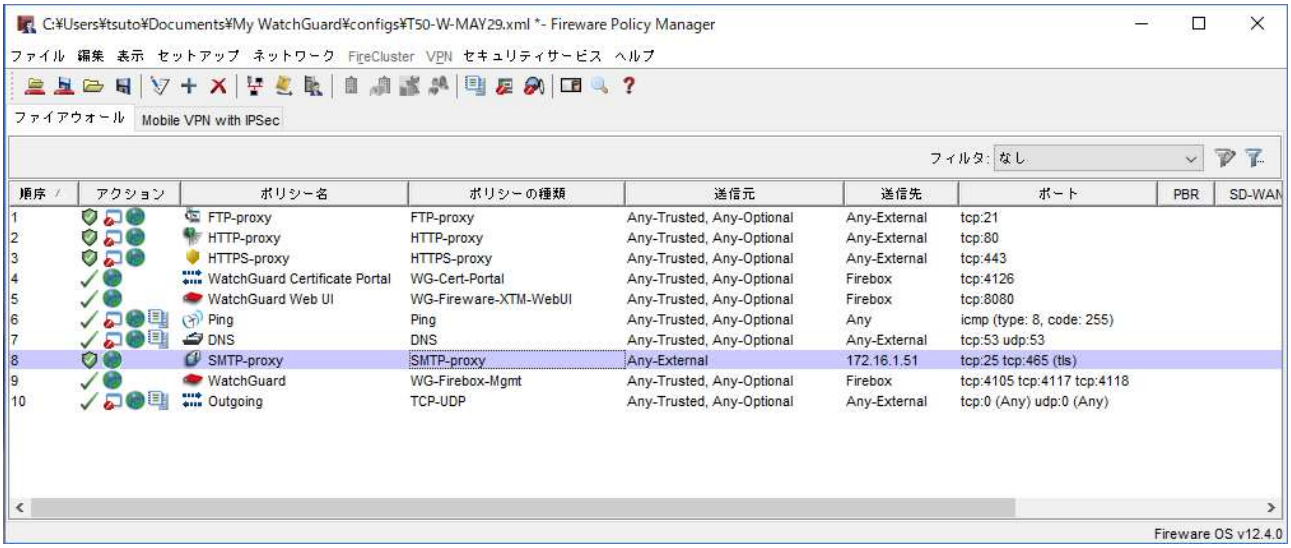
アドレスの追加画面からその他の追加をクリックします。



送信先はメールサーバーの IP アドレスを指定します。



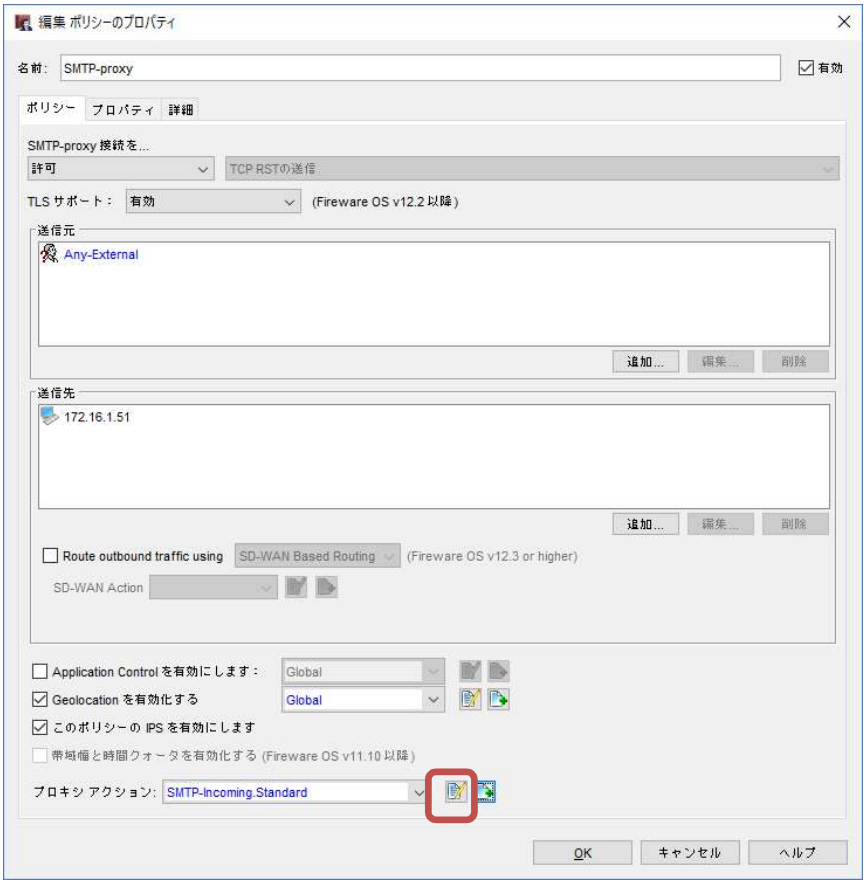
OK をクリックして抜けるとポリシーマネージャに SMTP-proxy が追加されています。



このプロキシに spamBlocker を有効にし、アクションを設定しましょう。

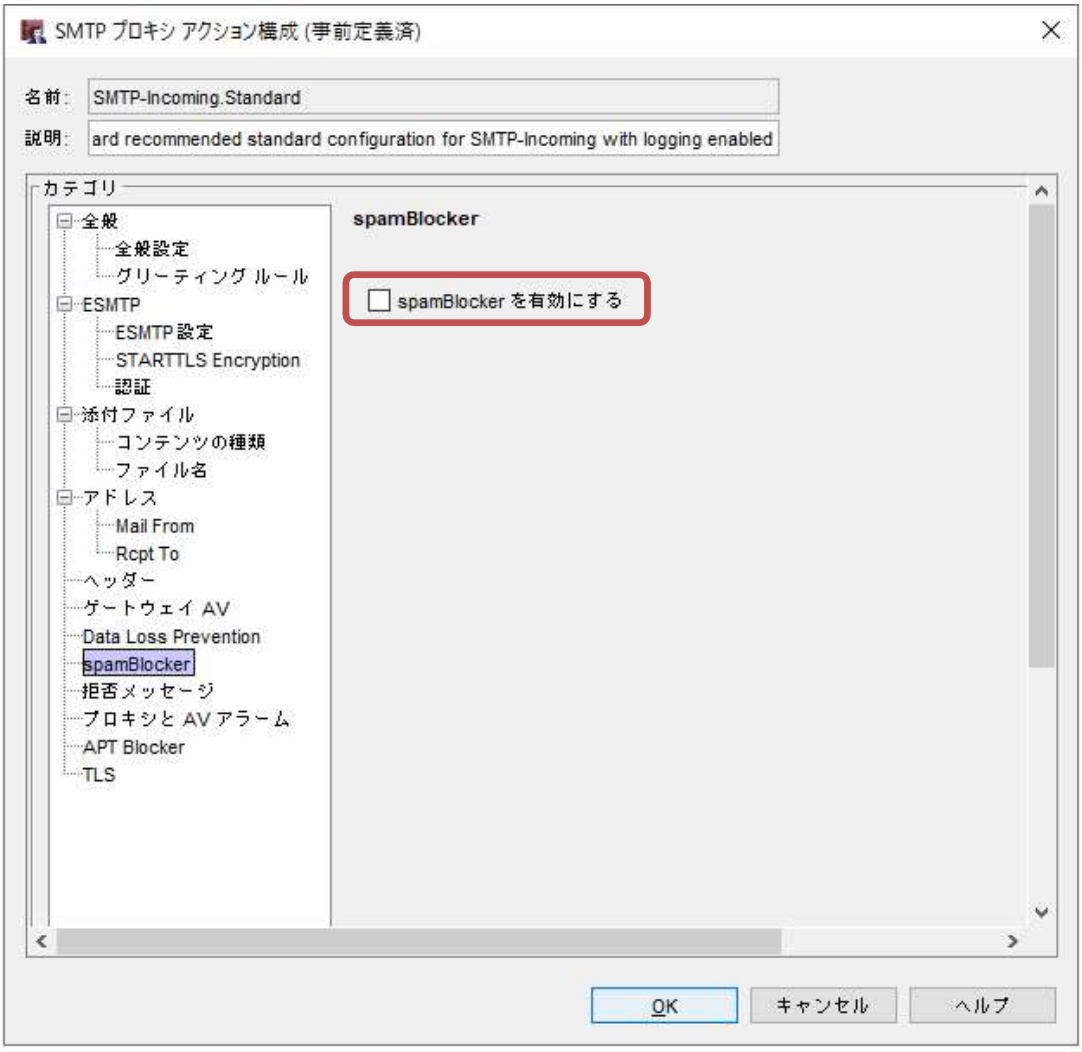
再度 SMTP-proxy のポリシーを開きます。

[プロキシアクションの複製]ボタンをクリックします。



プロキシアクション構成の左メニューの「spamBlocker」をクリックします。

まだ有効になっていないので、spamBlocker を有効にする のチェックを入れます。



すると SMTP 通信を許可する際のアクションを設定する画面が表示されます。

例として 2 通りの設定を以下に挙げます。

例-1：スパムは拒否、広告メールなどのバルクはタグ付け、未確認(疑わしい)は許可の設定

例-2：スパム、バルク、未確認(疑わしい)のどれもタグ付けの設定

設定を Firebox に保存し、動作を確認してください。

ドロップインモードでの運用

ドロップインモードはブリッジモードに似ていますが、より柔軟な運用が可能です。

具体的には、以下のように動作します

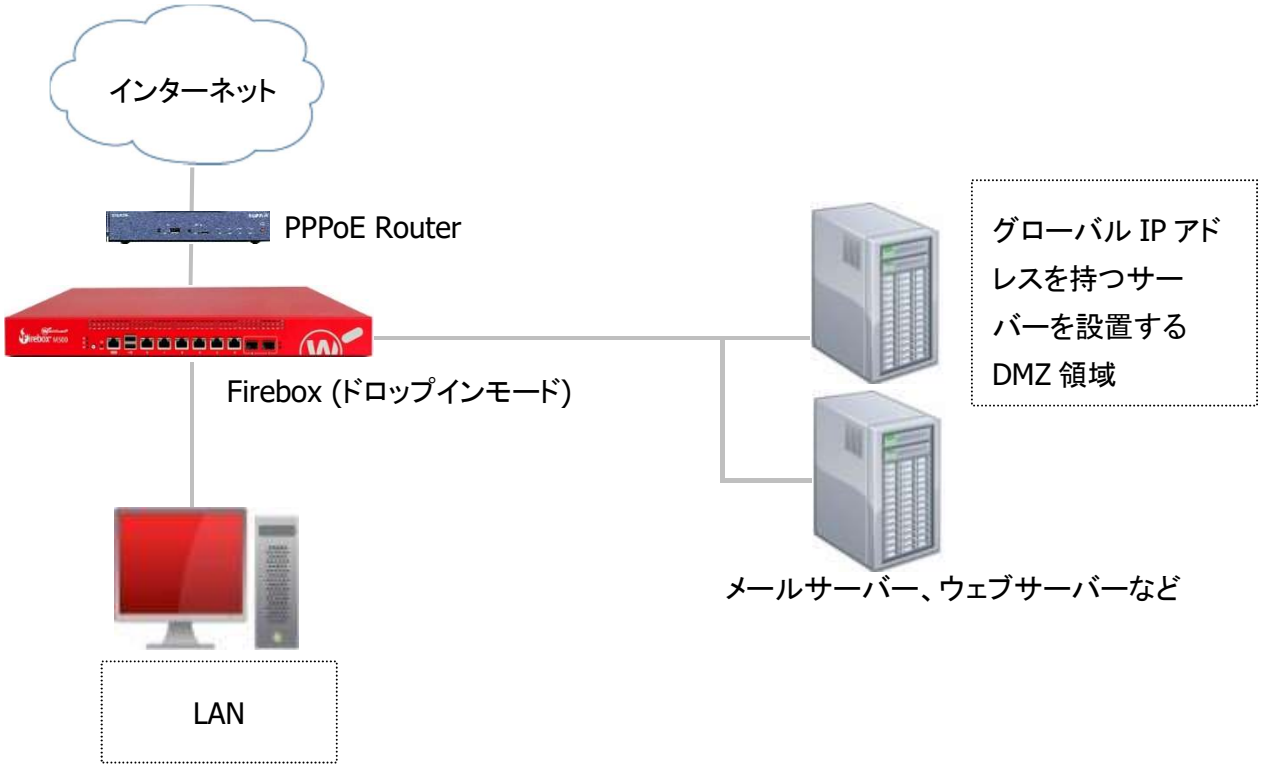
- Firebox のすべてのインターフェイス (外部、信頼済み、および任意) に、同じプライマリ IP アドレスが割り当てられます
- どのインターフェイスにもセカンダリ ネットワークを割り当てることができます。
- 信頼済みネットワークおよび任意ネットワークのホストでは、同じ IP アドレスおよびデフォルト ゲートウェイを保持したまま、セカンダリ ネットワーク アドレスを追加できるため、Firebox はこれらのネットワーク上のホストにトラフィックを正しく送信できます。
- Firebox 配下のパブリック サーバーは、引き続きパブリック IP アドレスを使用できます。 ネットワークの外部からパブリック サーバーにトラフィックをルーティングするときに、ネットワーク アドレス変換 (NAT) は使用されません。

構成例

前述の特長を利用すれば、一例として Unnumbered PPPoE を使ったグローバル IP を持つネットワークを構成することができます。

この例では、Unnumbered PPPoE 対応のルーターの下に Firebox を設置し、グローバル IP アドレスの DMZ 領域を作成します。

同時に Trusted インターフェイスにセカンダリ IP アドレスを設定することにより、クライアント用のセグメントも構成します。



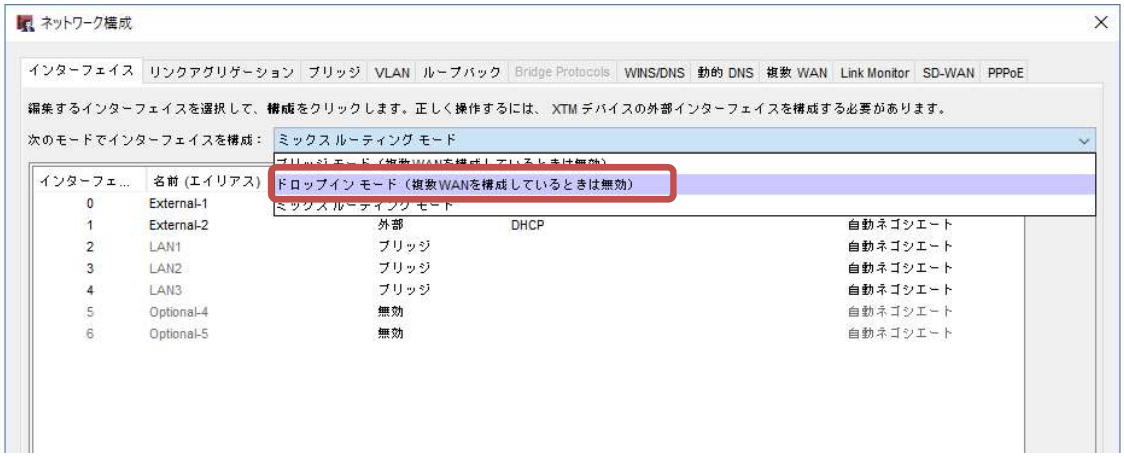
設定するにあたり、このネットワークの設定を仮に以下のように想定します。

固定のグローバル IP 8 個のネットワーク	203.0.113.0 (0-7)/29
PPPoE ルーターの IP アドレス	203.0.113.1
Firebox に設定する IP アドレス	203.0.113.2
サーバーに割り当てる IP アドレス	203.0.113.3～6
LAN 側のネットワーク	192.168.1.0/24

Firebox のインターフェイスは、あらかじめ 0 番ポートは External、1 番ポートは Trusted、2 番ポート以降は Optional で設定しておいてください。(IP アドレスはデフォルトで結構です)

ネットワークの設定

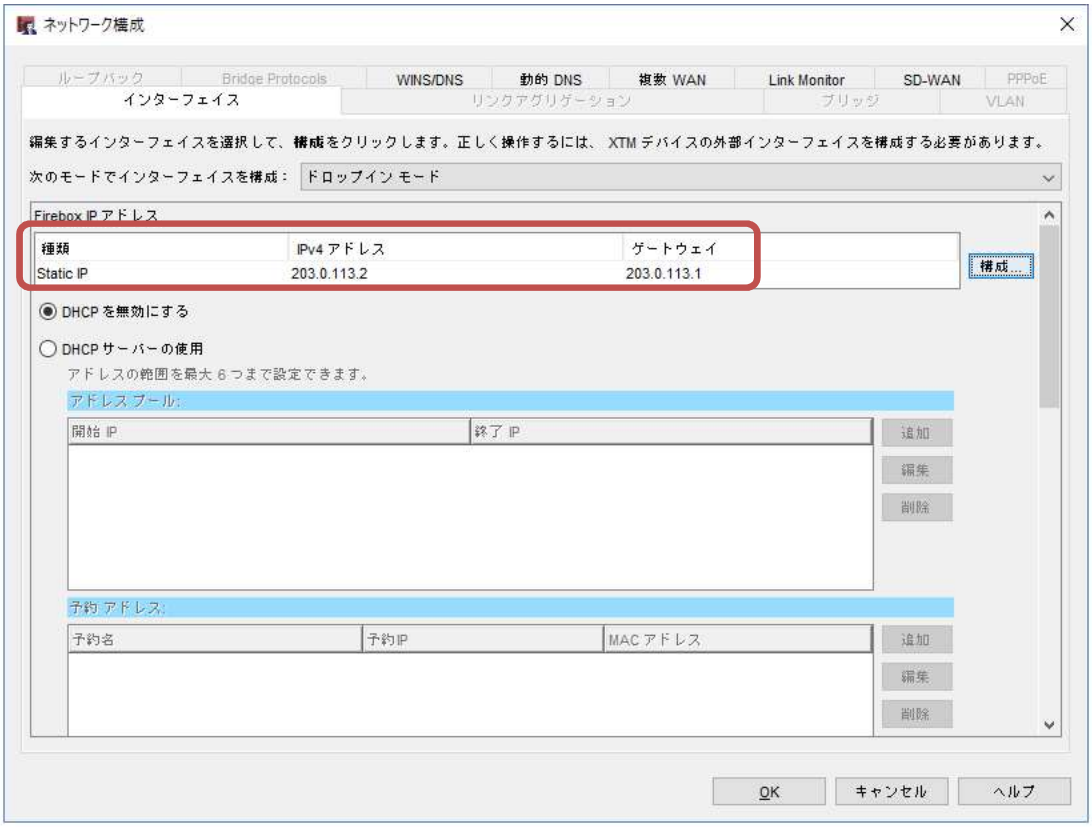
ネットワーク構成の画面のインターフェイスのモードを「ドロップインモード」にします。



すると以下のような画面になります。

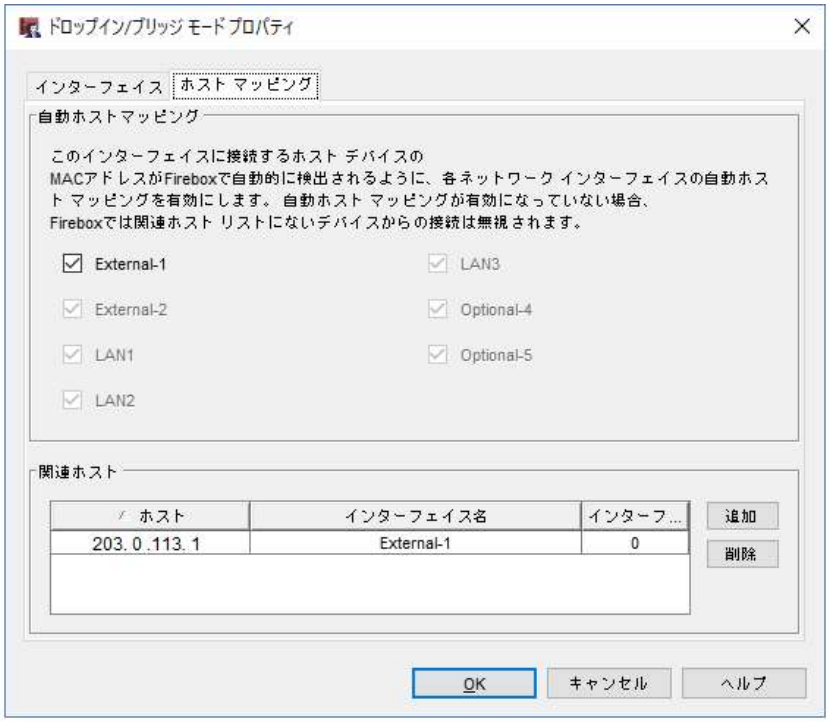
IPv4 アドレスは前述の設定表どおり、203.0.113.2 を設定します。

ゲートウェイは PPPoE ルーターの内側のアドレスである 203.0.113.1 を指定します。



サーバーからは Firebox に割り当てた 203.0.113.2 がゲートウェイアドレスになります。

アドレス欄の横にある構成を開くと、ブリッジモードと同様、自動ホストマッピングの有効/無効および関連ホストのエントリの設定をする画面になります。詳しくはブリッジモードの項をご覧ください。

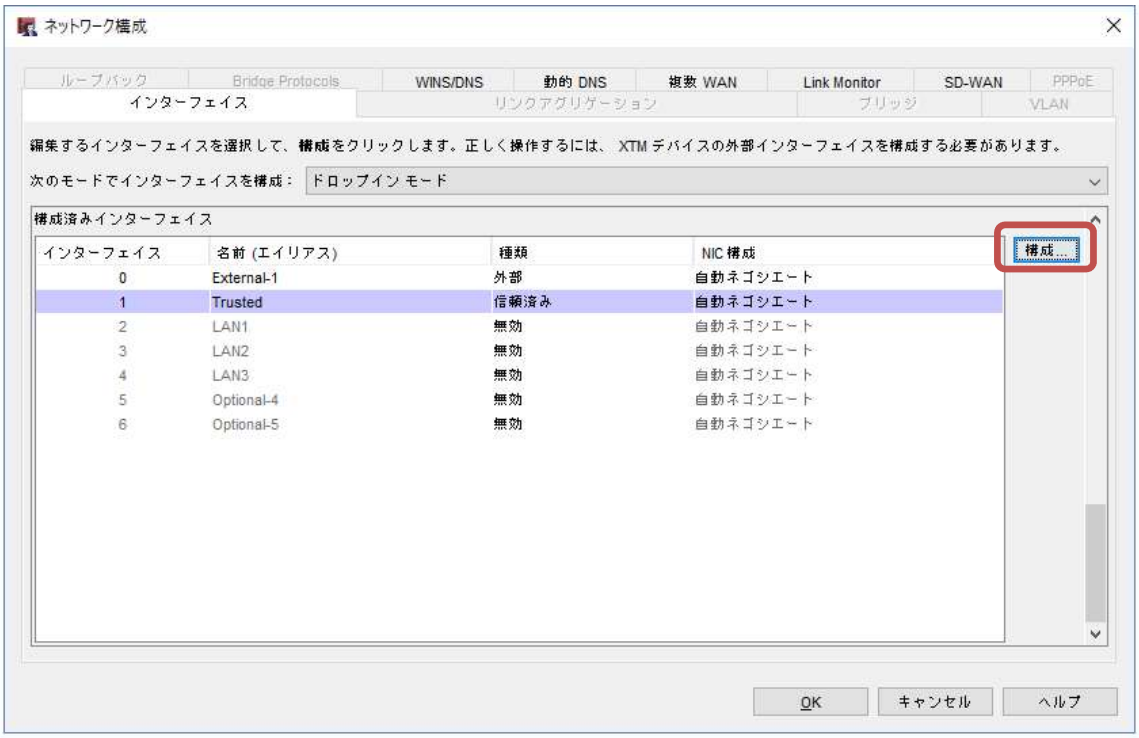


OK ボタンをクリックし、ネットワーク構成の画面に戻ります。

LAN の構成

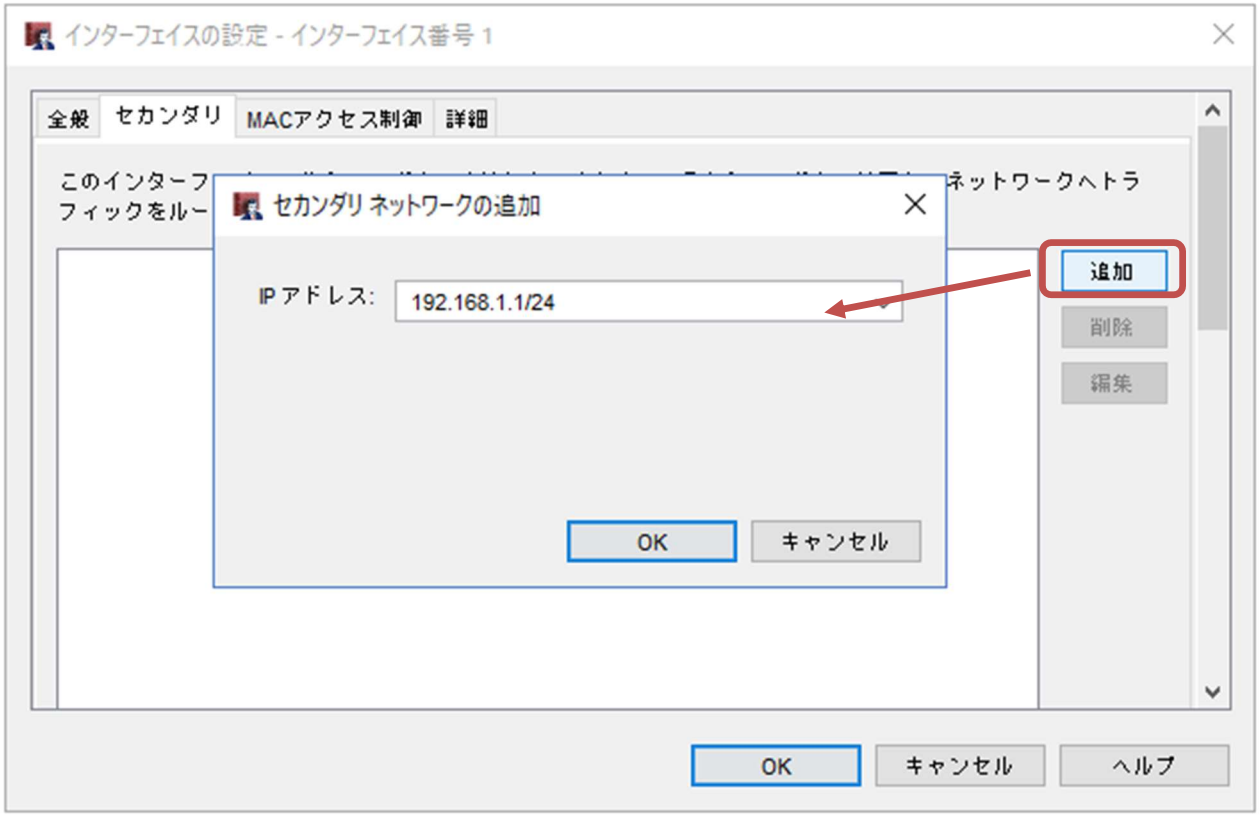
ネットワーク構成の画面をスクロールバーで下に下がると、インターフェイスの一覧があります。

LAN 側のネットワークを構成するために、インターフェイス 1 を選択し、[構成]をクリックします。



インターフェイス 1 の設定画面を開いたら「セカンダリ」タブを選択し、[追加]ボタンをクリックします。

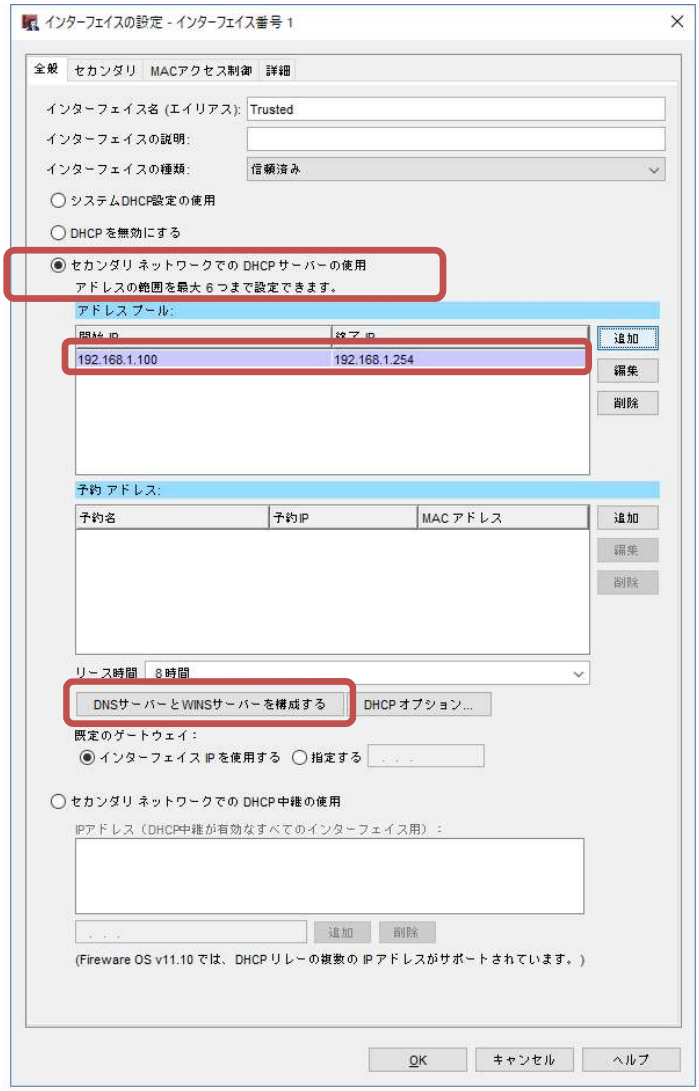
次のように、IP アドレスの欄に LAN 用のネットワークの設定をします。



この設定によって、Trusted インターフェイスに接続されるクライアントからは、192.168.1.1 をゲートウェイとするネットワークを構成できます。

全般タブに戻って、DHCP サーバーの設定もできます。

セカンダリネットワークでの DHCP サーバーの使用にチェックを入れて、クライアントに払い出す IP アドレスプールや DNS サーバーを設定することができます。



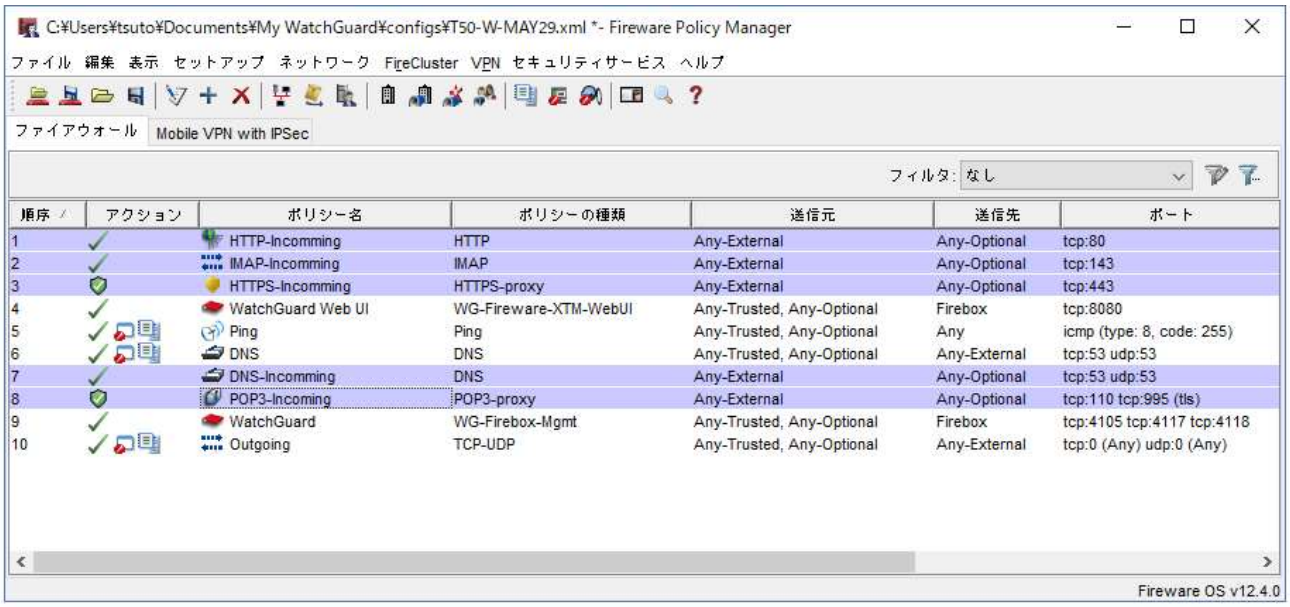
[OK]をクリックします。

インターフェイス 2 から 5 は、サーバー用の Optional(任意)のポートとして設定しています。

ポリシーの設定

下の図はメールサーバー、ウェブサーバー、DNS サーバーへの通信を許可するポリシー(フォーカス当てているもの)を追加した状態です。

いずれも Any-External から Any-Optional を許可するポリシーです。



第二章　負荷分散と冗長構成

Firebox は、内部のサーバーに対して負荷分散する設定、FireCluster とよばれる HA 構成の設定、2 つのポートに External ポートを設定して負荷分散やフェールオーバーを実現するマルチ WAN を設定することができます。

第二章では、これら負荷分散と冗長構成の手法を解説します。

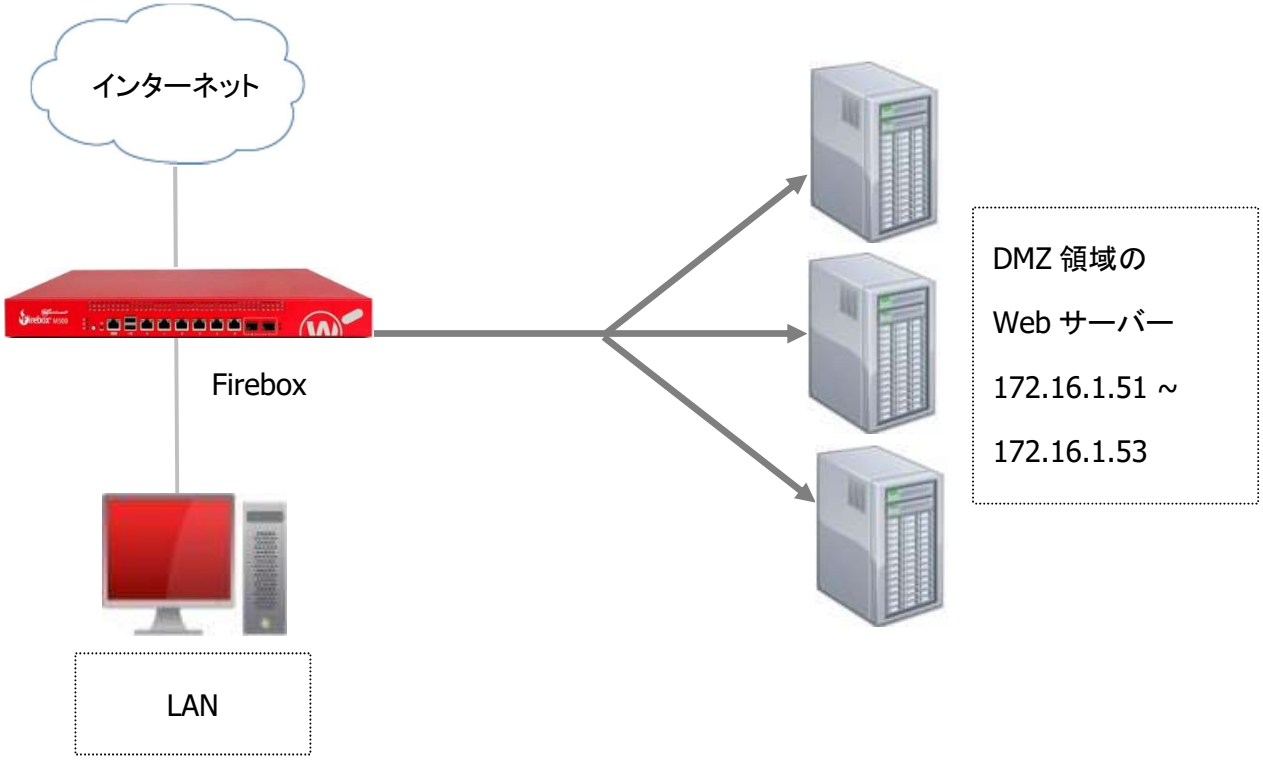
サーバー負荷分散

自社のウェブサイトのレスポンス低下は、機会損失や企業の評判低下に直結します。しかし、ロードバランスの専用機器は高価なものが多く、導入時のコストは企業にとって大きな負担となります。

Firebox は、ルーター、ファイアウォール、UTM の機能に加え、低価格でロードバランスを実現します。

構成例

DMZ に Web サーバーが 3 台あり、それらに負荷分散したいというケースで説明しましょう。



ネットワーク構成は以下のとおりです。

External	PPPoE 接続
LAN 側のネットワーク	192.168.1.0/24
DMZ 側のネットワーク	172.16.1.0/24
サーバーに割り当てる IP アドレス	172.16.1.51 ～ 53

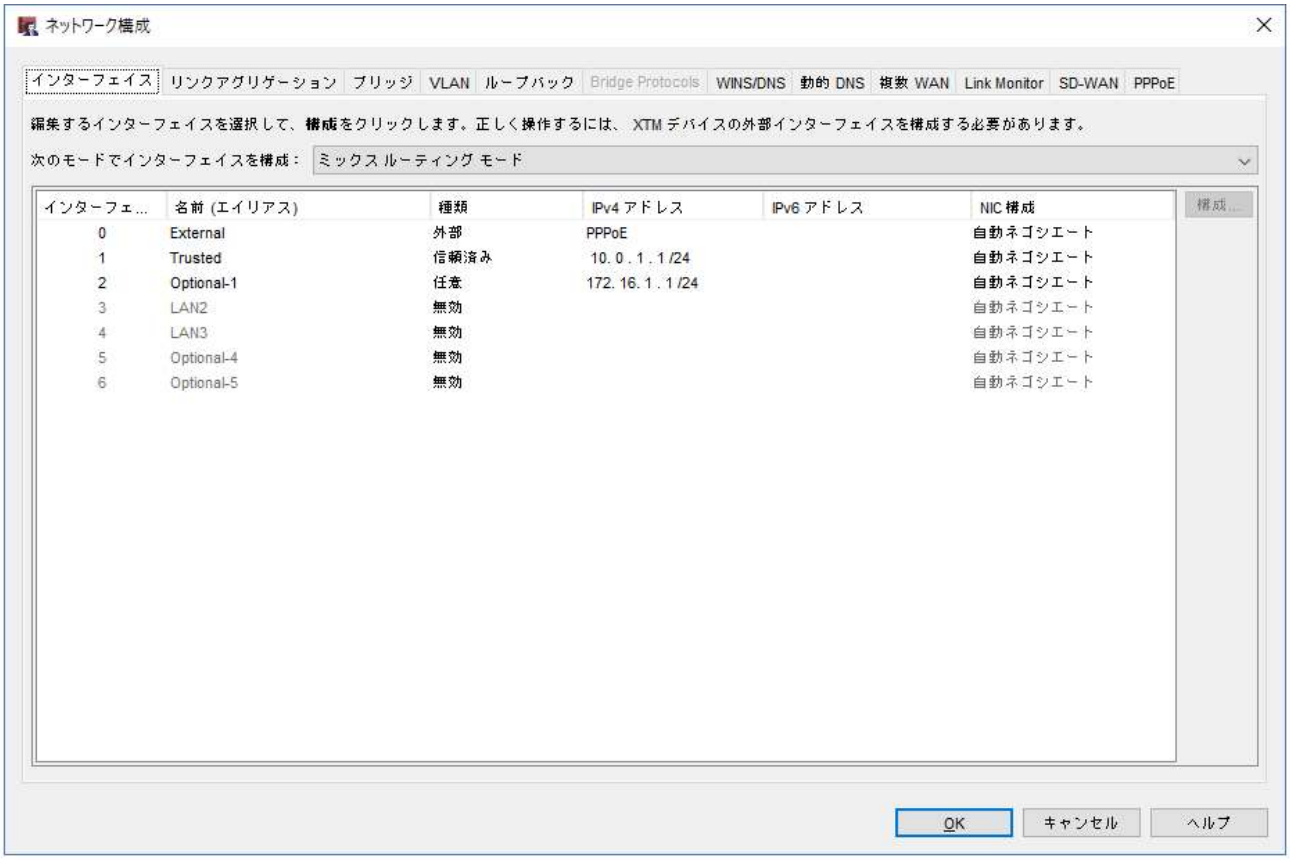
設定の流れとしては、

1. インターフェイスを構成
2. 複数サーバーへの負荷分散用の SNAT を作成する
3. DMZ の Web サーバーに HTTP アクセスを許可するポリシーを作成
4. そのポリシーの送信先を、作成した Web サーバー用の SNAT に指定

となります。

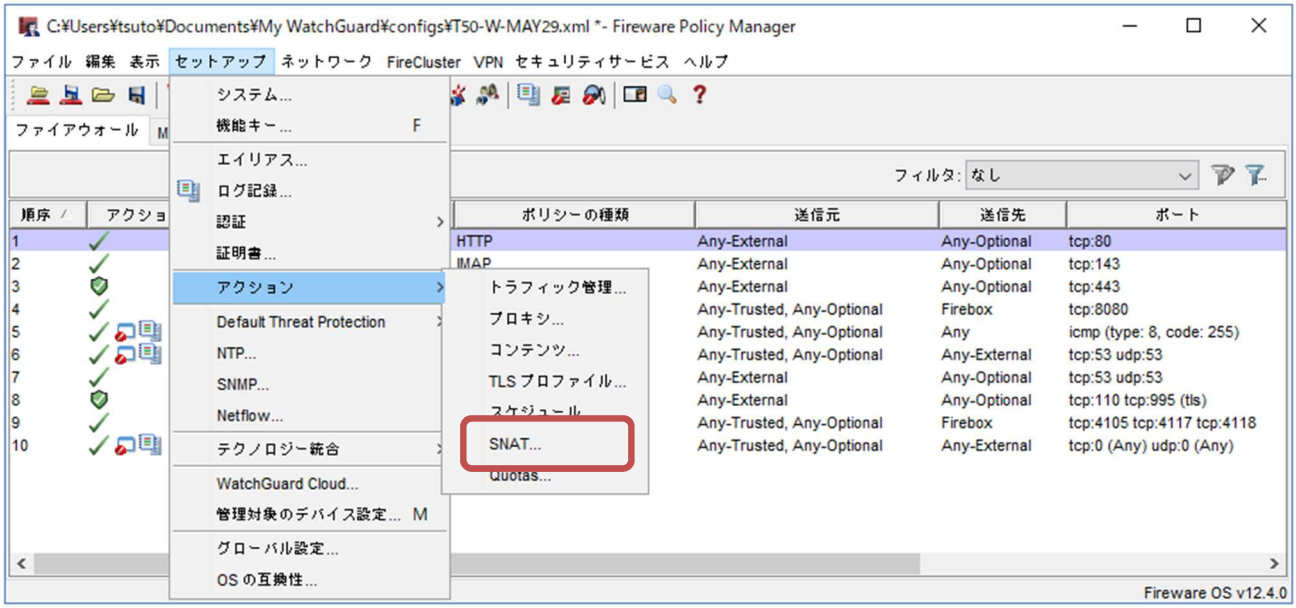
ネットワークの設定

構成にしたがって、以下のように設定します。

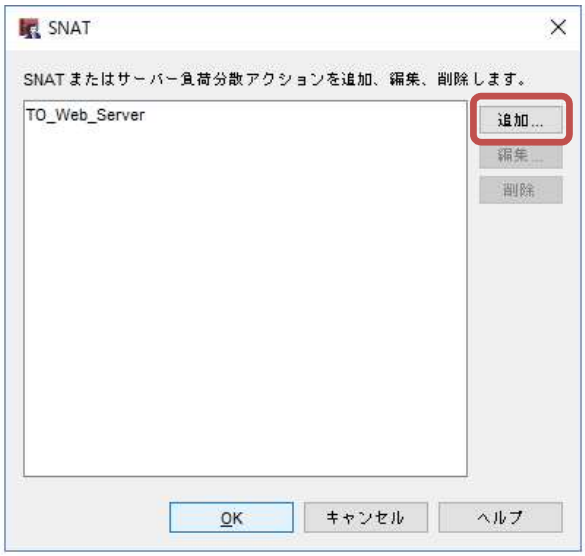


負荷分散用 SNAT の作成

ポリシーマネージャ *セットアップ* ー *アクション* ー *SNAT* をクリックします。



SNAT の画面が起動します。[追加]ボタンをクリックします。

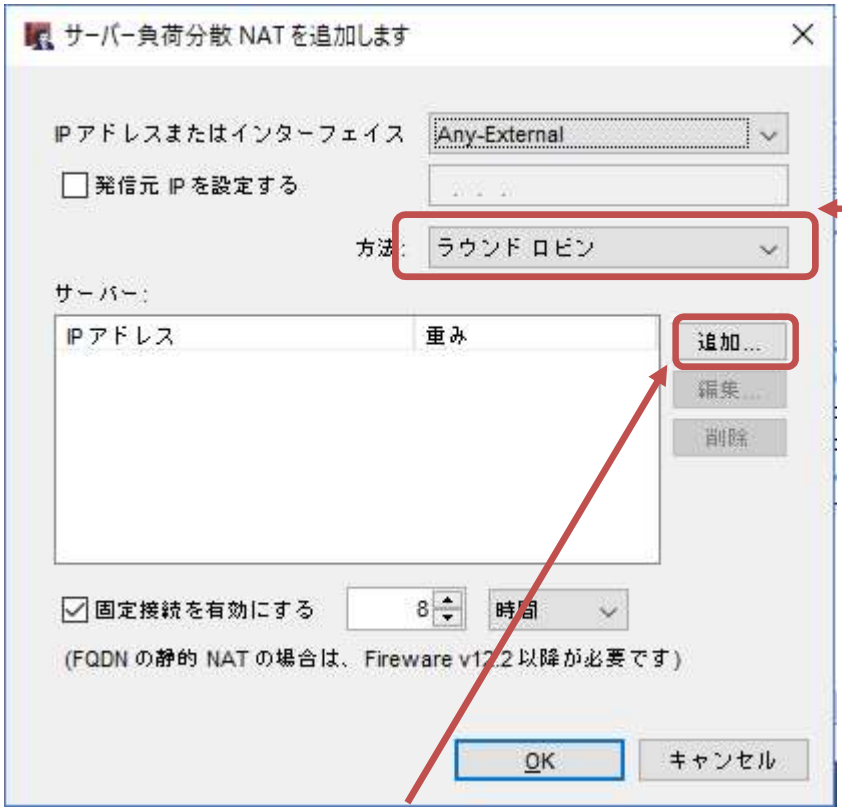


追加画面では「SNAT 名」に分かりやすい名前をつけます。

NAT の種類として「サーバー負荷分散」を選択します。

SNAT メンバーの[追加]をクリックし、SNAT のメンバーを追加します。

するとサーバー負荷分散 NAT の設定画面が開きます。



負荷分散方法では、「ラウンドロビン」と「最小構成」を選択できます。

ラウンドロビン:

接続が順番に (ラウンドロビンで) 割り振られます。 最初の接続は、重みで指定された 1 番目のサーバーに送信されます。

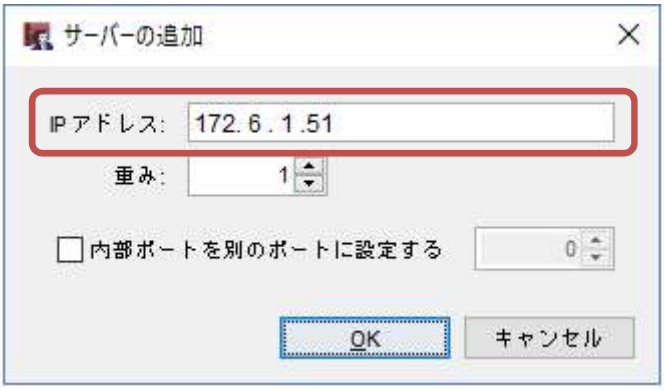
最小接続:

新しいセッション発生時、現時点でオープンな接続数が最も少ないサーバーに送信されます。

負荷分散方法を選択したら、[追加]ボタンをクリックし、サーバーを追加しましょう。

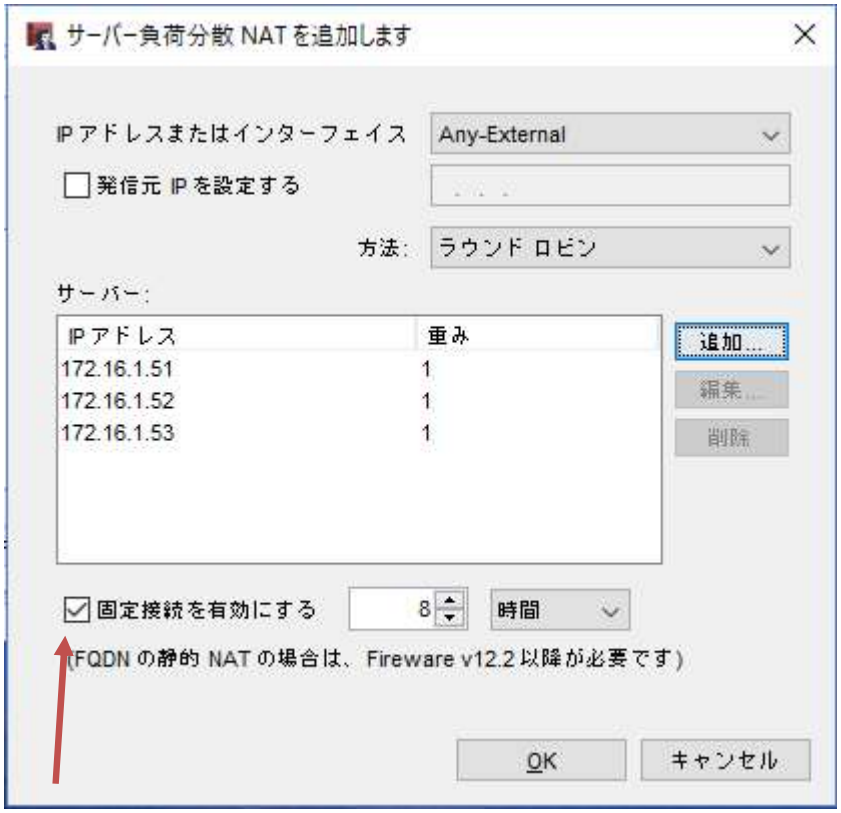
[追加]ボタンをクリックすると、サーバーの追加画面が開きます。

サーバーの IP アドレスを入力します。



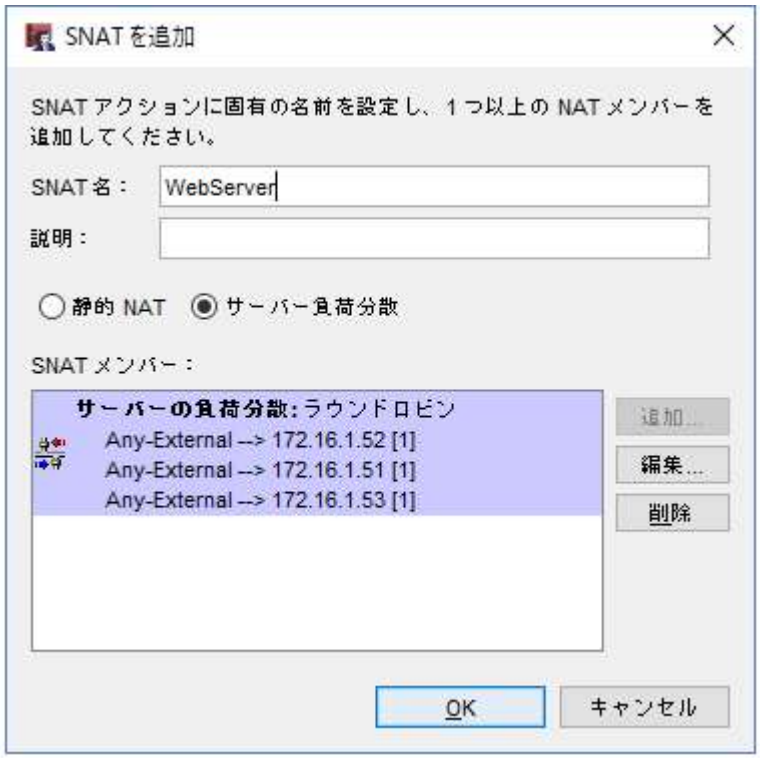
重みは負荷分散の重み付けの設定で、接続の優先順位を表わします。

[OK]をクリックし追加したら、同じように残り 2 台のサーバーを追加します。
以下のような画面になるでしょう。



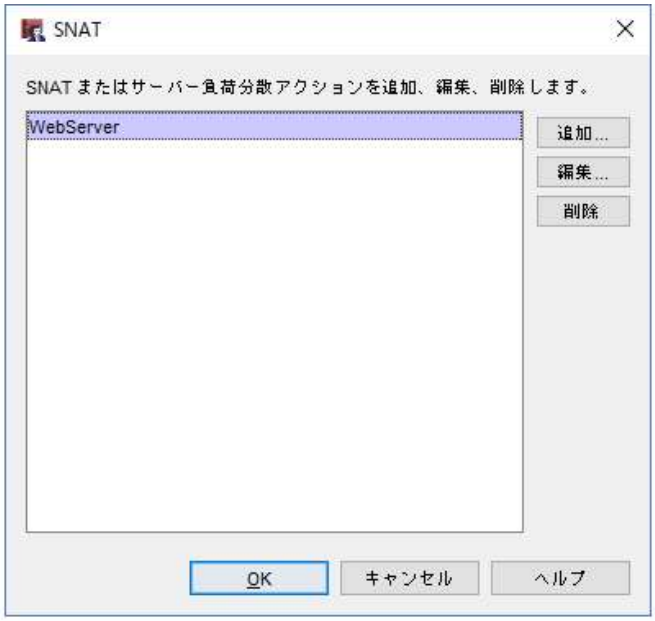
「固定接続を有効にする」のチェックは、指定の期間、継続的に同じサーバーを使用する接続のことです。接続を固定すると、ある発信元アドレスと宛先アドレス ペア間のすべてのパケットは、指定した期間、同じサーバーに送信されます。

3 台分のサーバーを設定し、負荷分散 NAT 画面を OK で抜けると、SNAT 画面は次のようになっています。



この画面で[OK]をクリックし設定を保存しましょう。

SNAT 画面に設定が追加されたことが分かります。

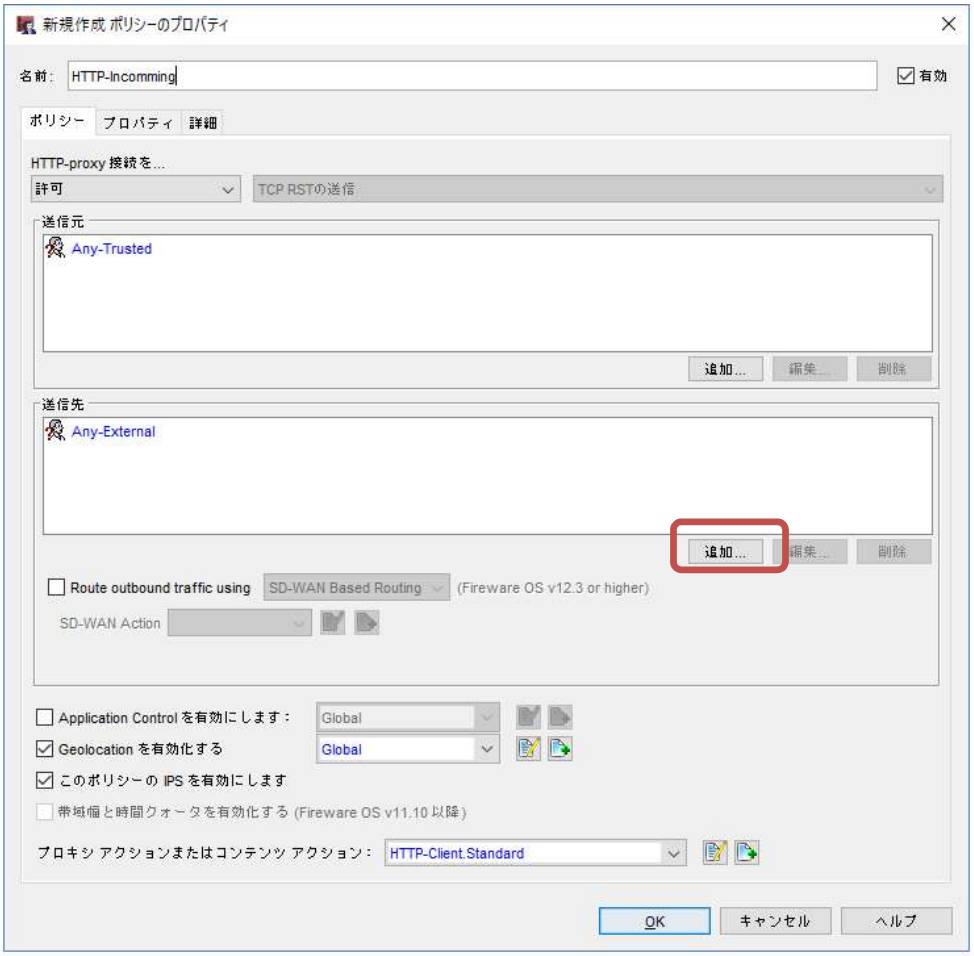


ポリシーの追加

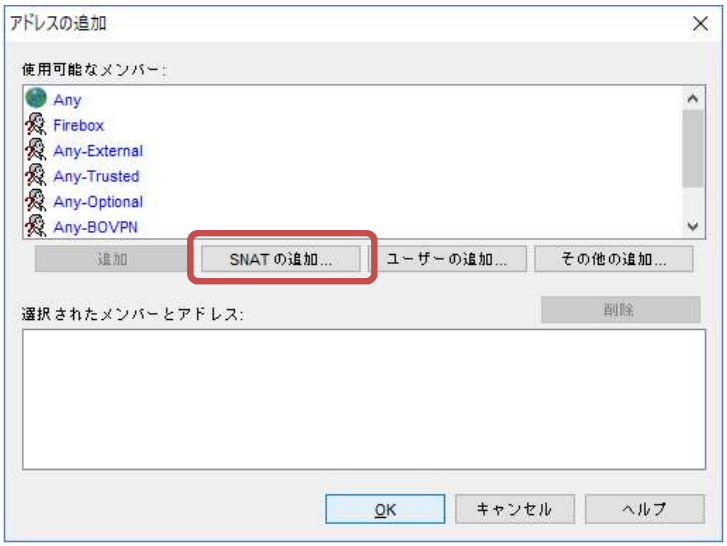
ポリシーの追加から、HTTP の許可ポリシーを追加します。

ポリシー名は分かりやすいように「HTTP-Incoming」としておきましょう。送信元は Any-External です。

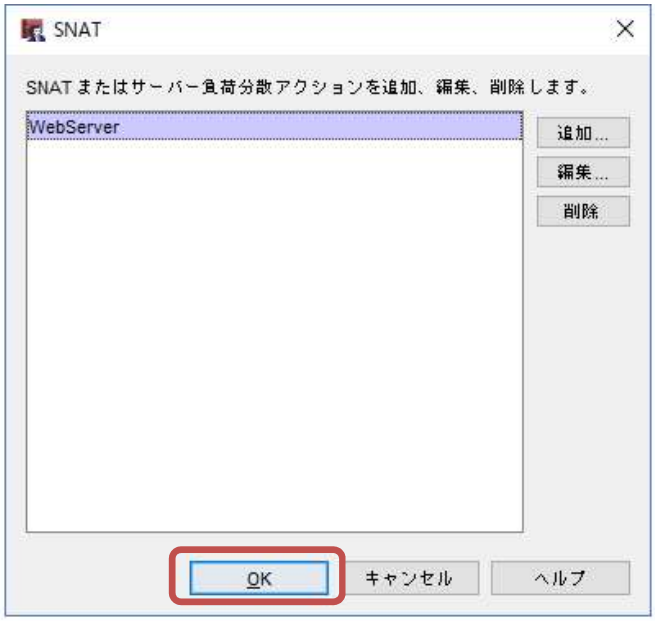
送信先のデフォルト設定を削除し、送信先の[追加]ボタンをクリックし追加します。



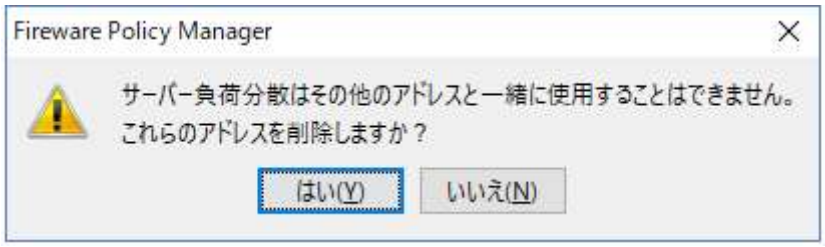
SNAT の追加ボタンをクリックします。



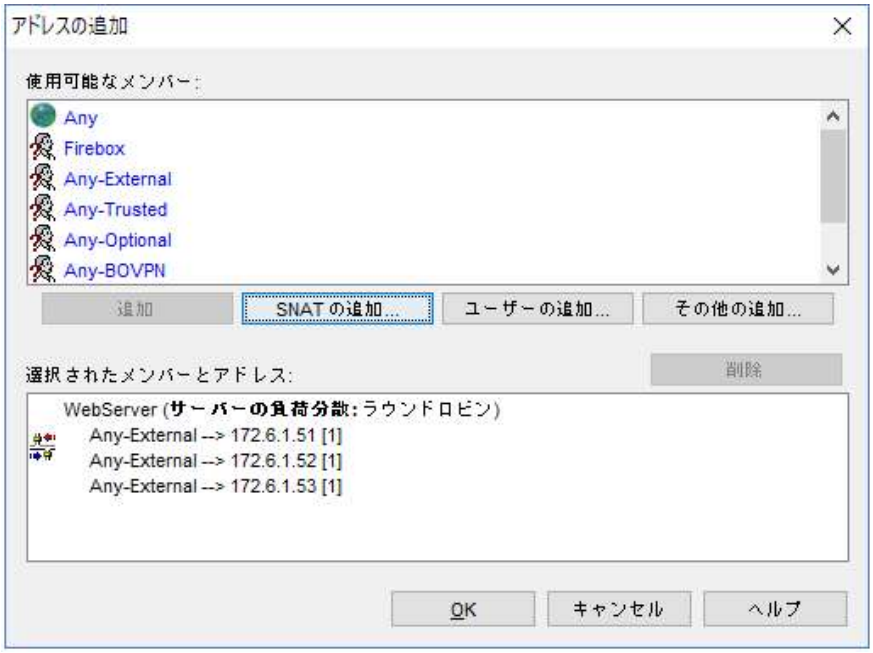
SNAT 画面で、先ほど作成した負荷分散 NAT である「WebServer」を選択し、OK ボタンをクリックします。



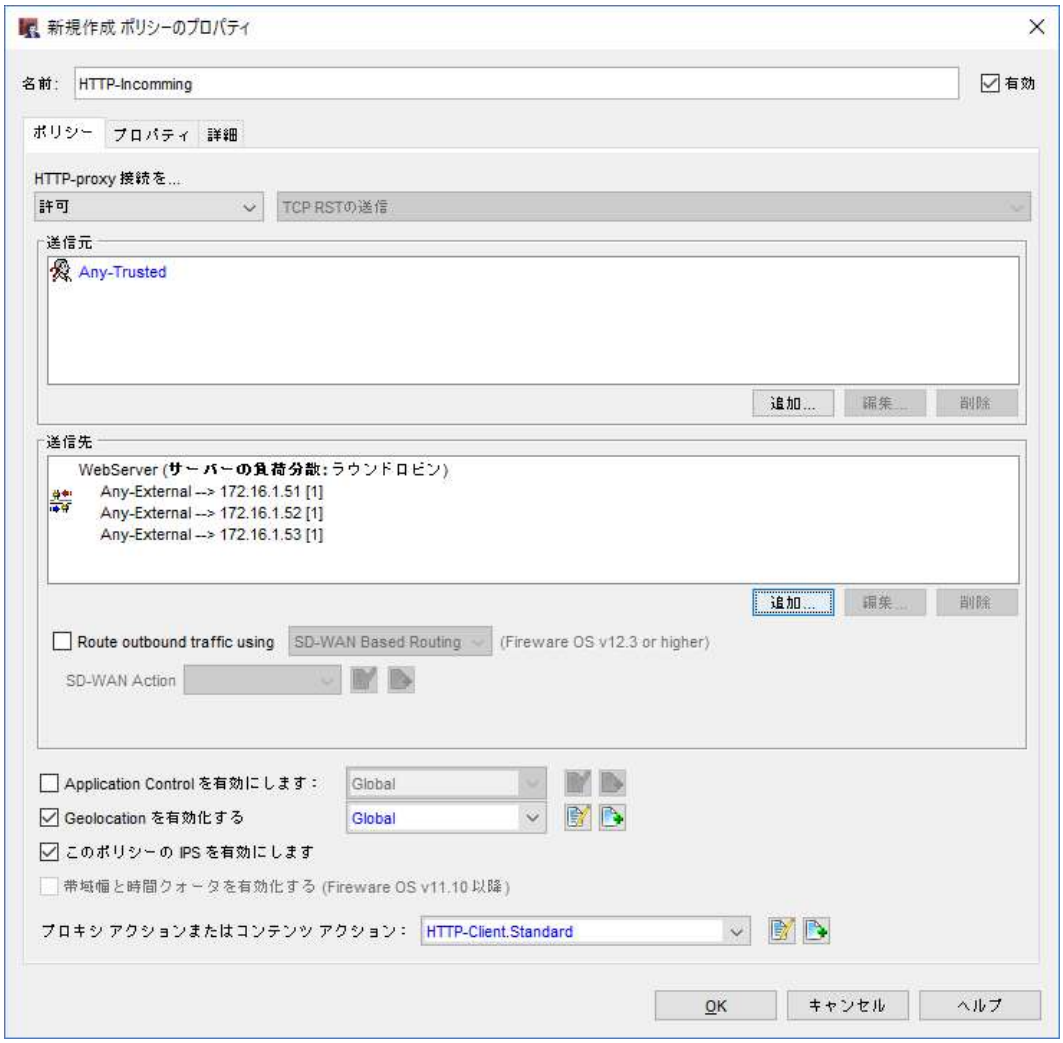
以下のアラートが出たら[はい]をクリックします。（他の送信先が入っていると削除されます）



送信先が選択できたので OK ボタンをクリックします。

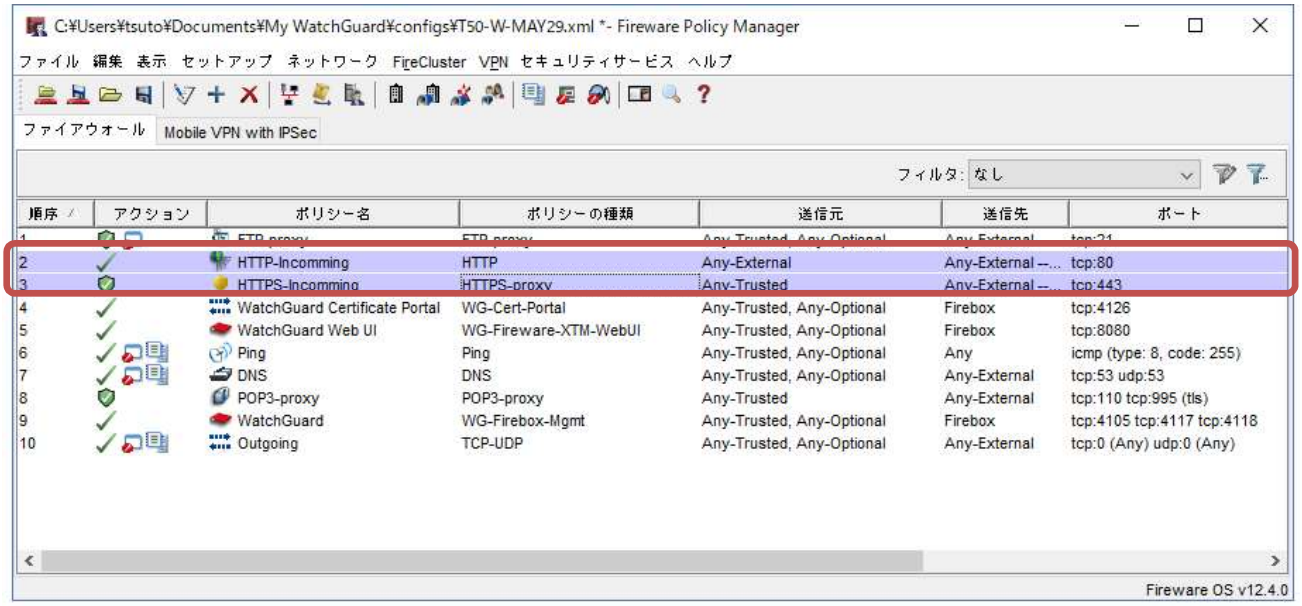


ポリシーは以下のようになります。



必要なら HTTPS ポリシーも同様に設定します。

ポリシーマネージャでは、追加された設定が以下のように表示されています。



以上で負荷分散の設定は完了です。

複数 WAN

Firebox は外部ポートを複数(最大で 4 つのインターフェイス)構成することにより、負荷分散、可用性の向上を図ることができます。

たとえば、

- インターネット閲覧の際のもたつきを解消したい
- VPN 接続のスループットの向上を図りたい
- 外部インターフェイスの接続が切れた際に別のインターフェイスにフェールオーバーしたい
- 片方のインターフェイスを外部からサーバーへのアクセスにし、もう片方を社内用と分けたい

といった場合のソリューションになります。

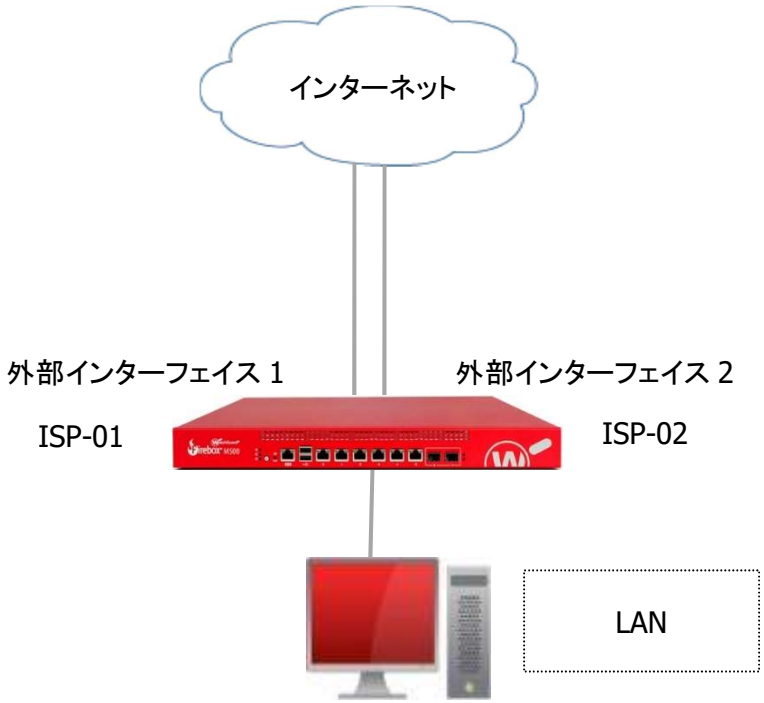
要件

- 複数 WAN に割り当てる外部インターフェイスにそれぞれの接続先があること
  - 2 つ(以上)の ISP 接続契約、IP アドレスなど
- ミックスルーティングモードで構成すること

構成例

2 社の ISP(インターネット・サービス・プロバイダー)と契約し、Firebox のインターフェイス 1 と 2 を外部ポートとして複数 WAN を構成します。

動作モードはラウンドロビンで、負荷分散を行ないます。



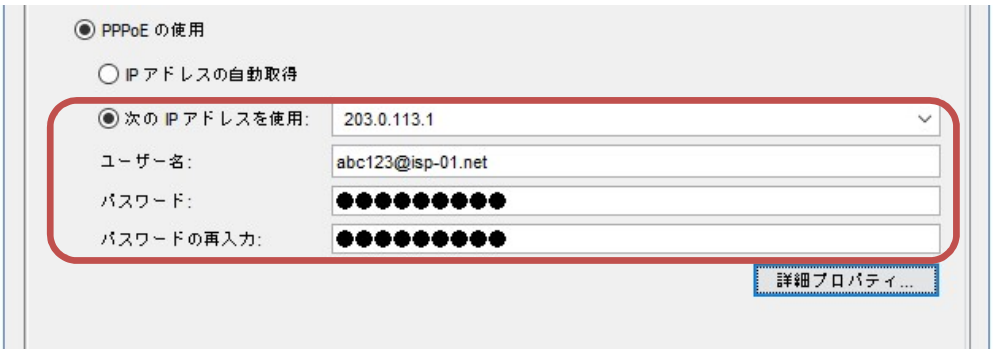
インターフェイス 0(External-1)の接続	PPPoE (100Mbps 回線)
External-1 のアカウント	abc123@isp-01.net
External-1 のパスワード	xxxxxxxxxx
インターフェイス 1(External-2)の接続	PPPoE (ギガビット回線)
External-2 のアカウント	xyz789@isp-02.net
External-2 のパスワード	yyyyyyyyyy
インターフェイス 2-5	ブリッジで Trusted (インターフェイス：10.0.1.1)
Trusted のネットワーク	10.0.1.0/24
インターフェイス 6	DMZ のための Optional (インターフェイス：10.0.6.1)
DMZ のネットワーク	10.0.6.0/24

ネットワークの設定

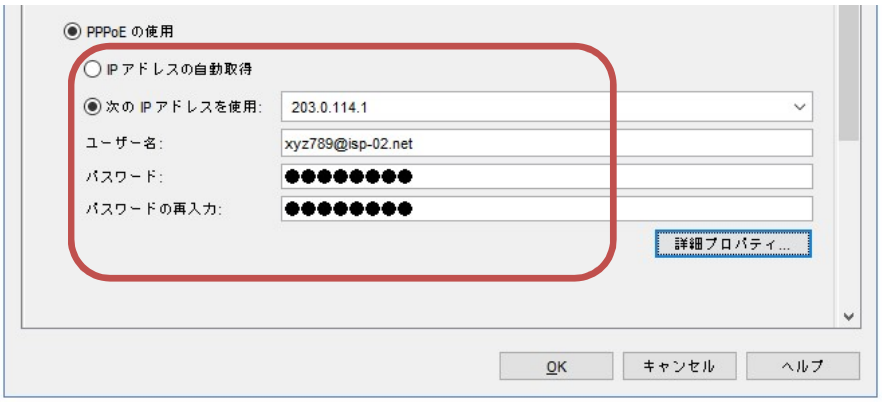
まずは構成例に基づいて、一つ目の外部インターフェイスを設定します。

インターフェイス名に他の外部インターフェイスと区別がつくように命名します。

インターフェイス設定画面の下方に PPPoE 設定の箇所がありますので、PPPoE の使用にチェックを入れ、ISP から提供された接続情報を入力します。

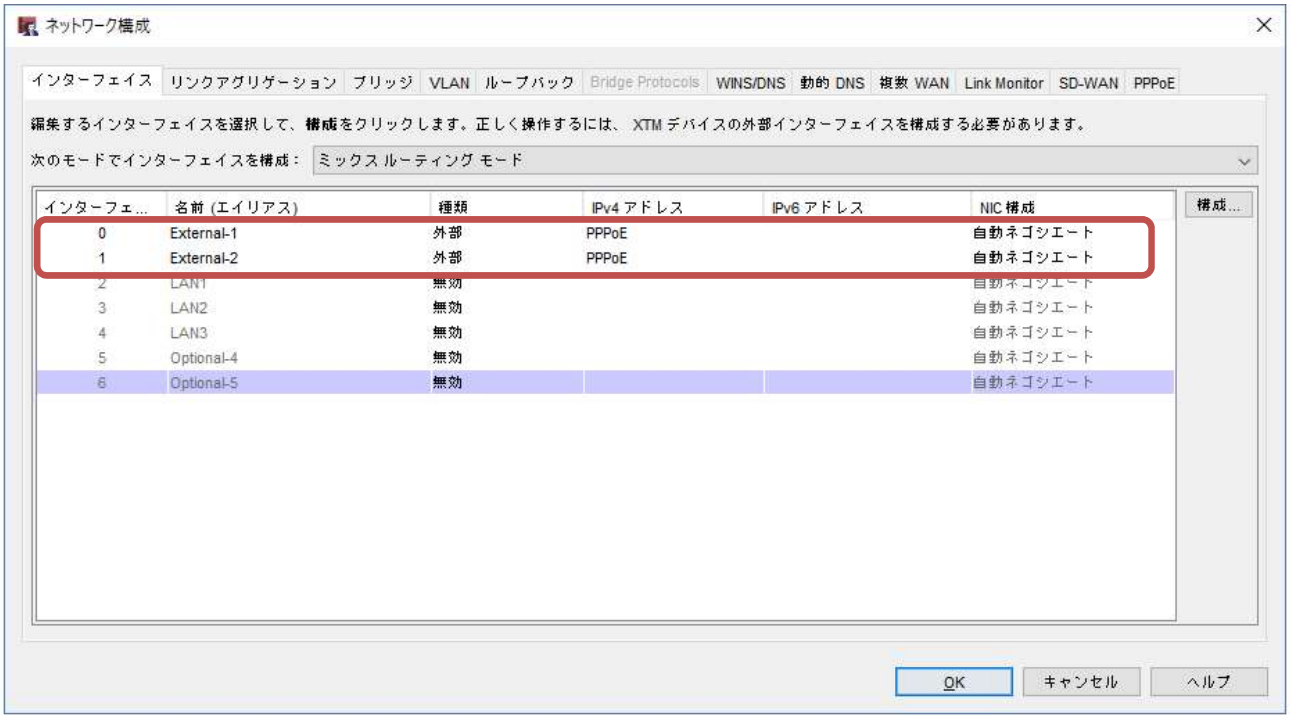


インターフェイス 1 に 2 つ目の外部インターフェイスを同様に設定します。



Trusted と Optional も設定すると、ネットワーク構成の画面は次のようになります。

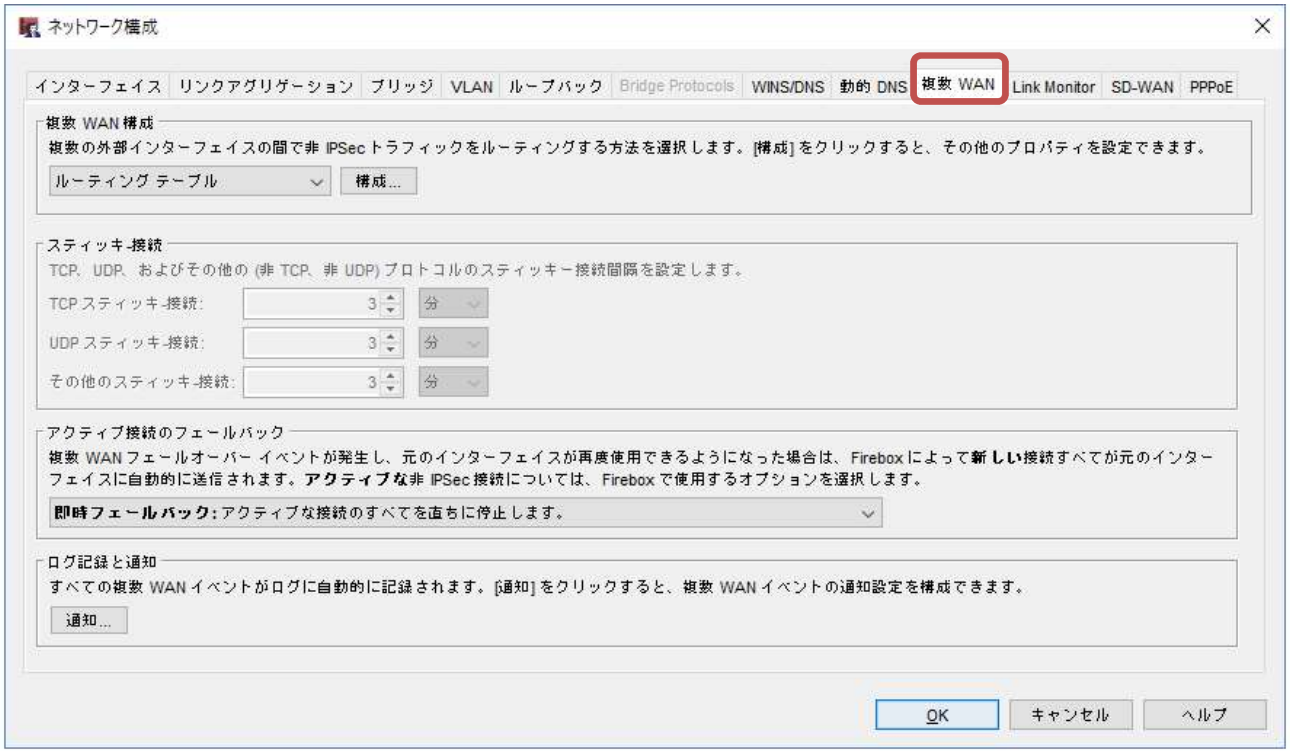
上記の設定で外部インターフェイスも 2 つ構成されています。



以上で複数 WAN を設定する準備ができました。

複数 WAN の設定

同じくネットワーク構成の「複数 WAN」のタブを選択します。

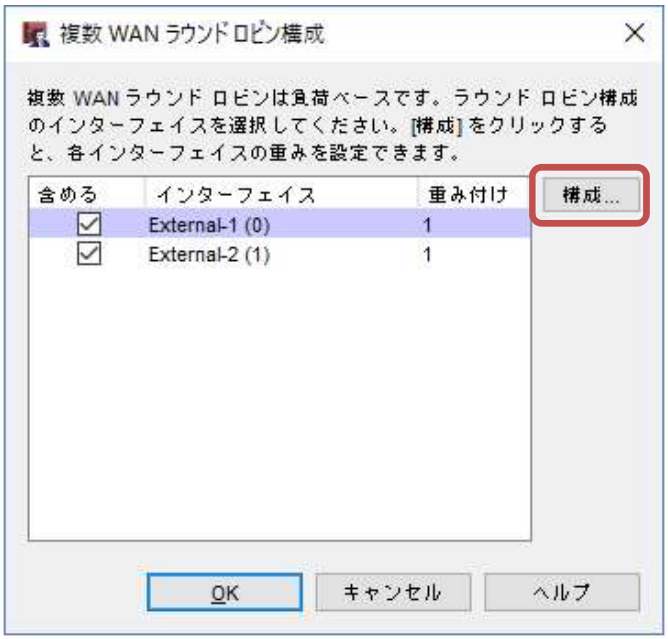


複数 WAN 構成のセクションでラウンドロビンを選択します。

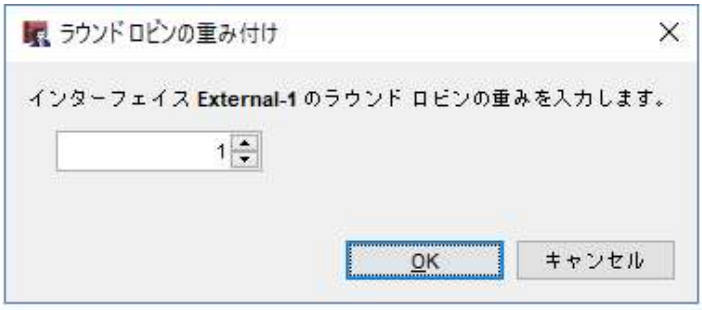
ラウンドロビンの振る舞いを設定するために、構成ボタンをクリックします。

複数 WAN ラウンドロビン構成が開きます。ここではインターフェイスの重み付けの設定ができます。

構成ボタンをクリックします。



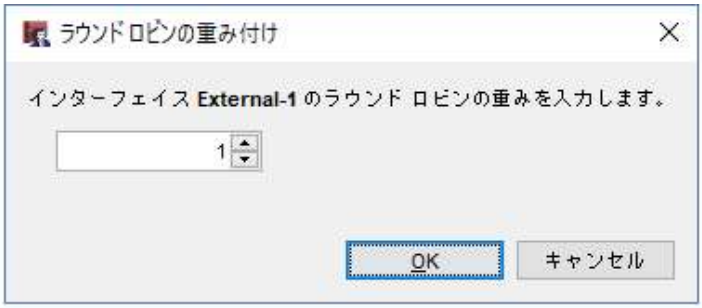
ラウンドロビンの重み付けの画面が開きます。



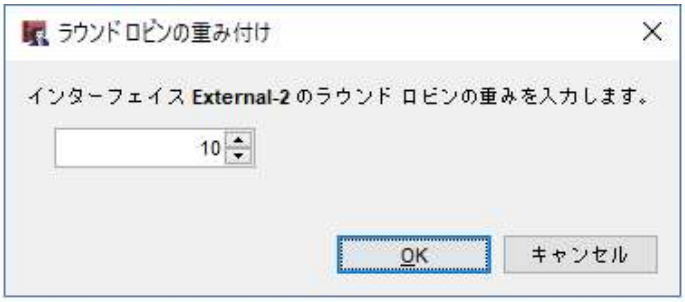
重み付けの計算方法は以下のとおりです。

1. 構成例ですと一つは 100Mbps、もう一つは 1Gbps なので、整数にならして単位をそろえます
   - インターフェイス 0 は 100Mbps、インターフェイス 1 は 1000Mbps です
2. 比例式で最小通信速度を 1 とした比率を割り出します
   - [100：1000]なので[1：10]という比率になります
3. 重み付けは External-1 が 1、External-2 が 10 になります

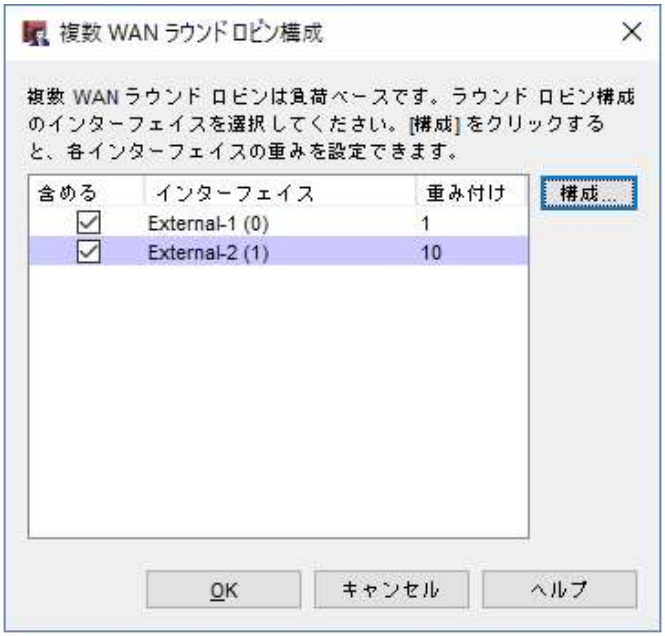
External-1 の重み付け



External-2 の重み付け



設定後、ラウンドロビンの構成は以下のようになっています。

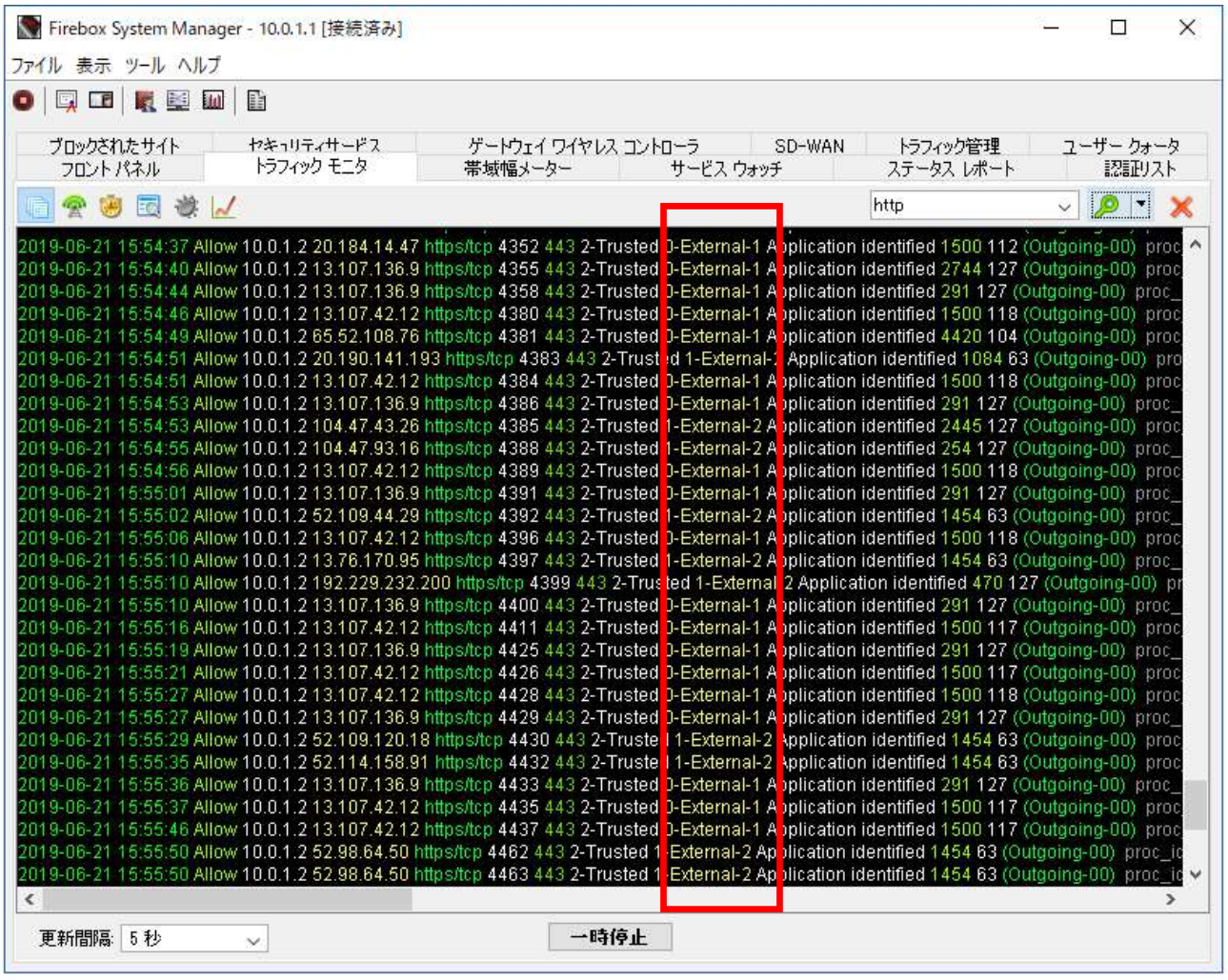


動作確認

Firebox System Manager のトラフィックモニタで確認することができます。

http でフィルタリングして、クライアント PC から Web アクセスします。下の図は負荷テストツールで大量の HTTP アクセスを生成した際のログです。

パケットが通過する際に、外部インターフェイスの External-1 と External-2 の両方が使用されていることが分かります。



第三章 UTM 機能

WSM 基本設定ガイドでは WebBlocker、Gateway Anti-Virus、spamBlocker、Intrusion Prevention Service(IPS)、Reputation Enabled Defense (RED) について解説しましたが、本書では Application Control の設定方法について紹介します。

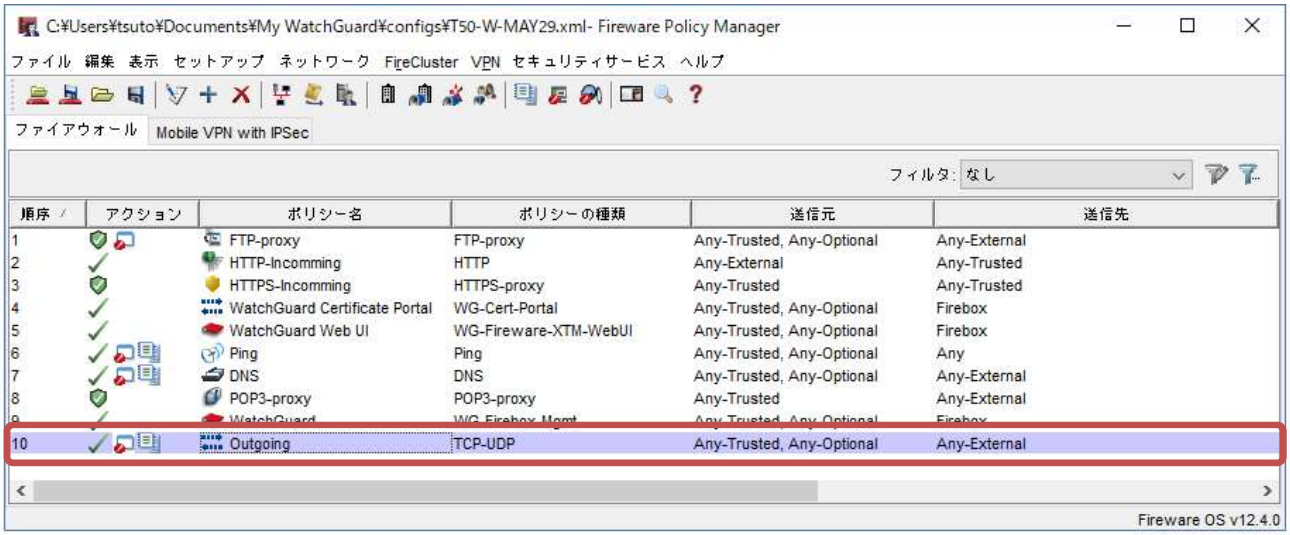
Application Control

アプリケーション・コントロールは、文字通り、社内で使用される可能性があるアプリケーションを制御します。プロトコルは何か、ブラウザベースか否かに関係なく、アプリケーションの振る舞いや特徴を検知して、その利用方法を細かく管理することができます。これにより、私的目的のネットワーク利用を制限したり、情報漏洩を防いだりすることができます。

このセクションでは、ファイル転送サービスの制御を想定し、設定方法を解説します。

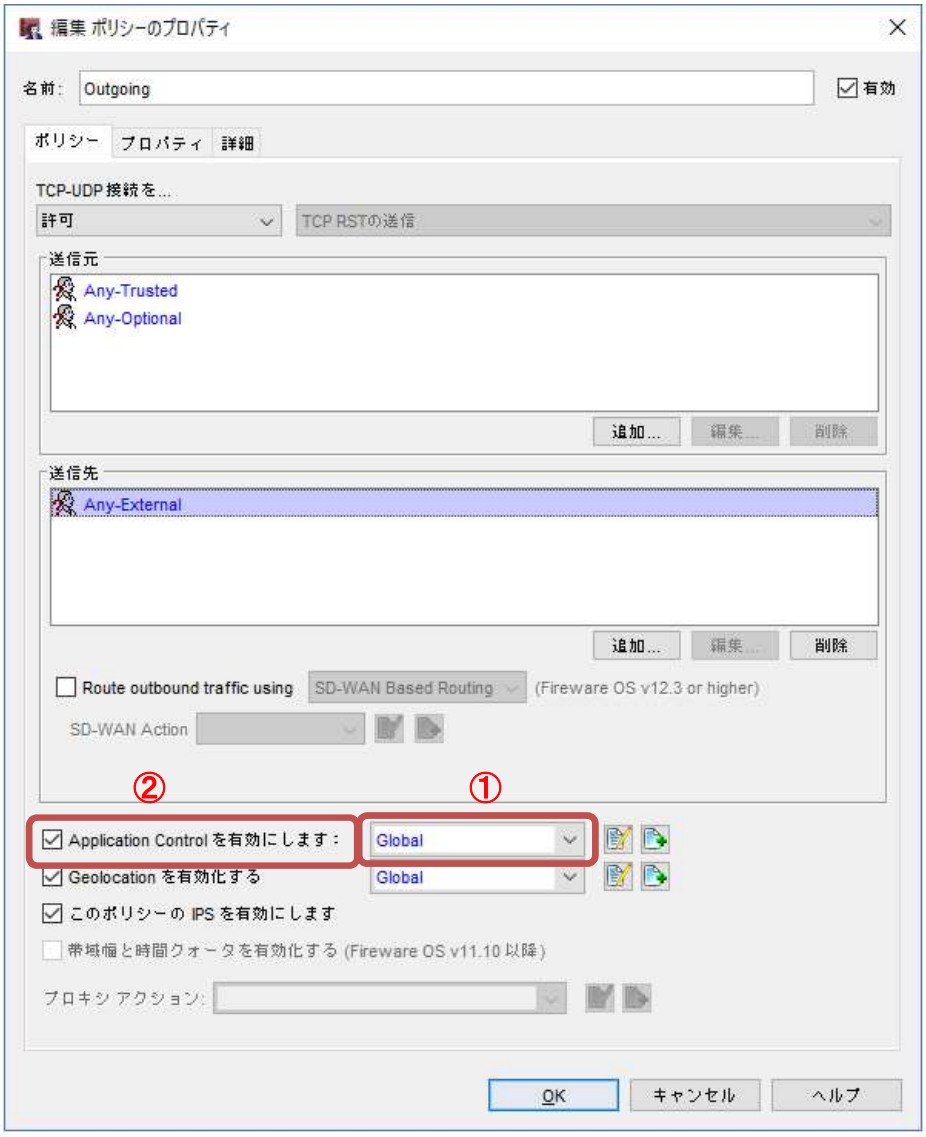
ポリシーと Application Control アクションの紐付け

ポリシーマネージャから Outgoing ポリシーをダブルクリックして開きます。



「Application Control を有効にします」のチェックを入れます(①)。

このポリシーに、後で作成する Application Control のアクションを横のドロップダウンリスト(②)をから選択することによってポリシーとアクションが紐付き、目的のアプリケーションを制御ようになります。



Outgoing ポリシーと紐付けるのは、Application Control の機能がプロトコル(ポート番号)に関係なく、全通信を対象にしてアプリケーションを判別し、制御するからです。

どのプロトコルか確定していれば、その特定のポリシーで Application Control を有効にすることもできます。

特に Outgoing よりも上位に定義されているポリシーがあれば、そのポリシーでも Application Control を有効にする必要があります。

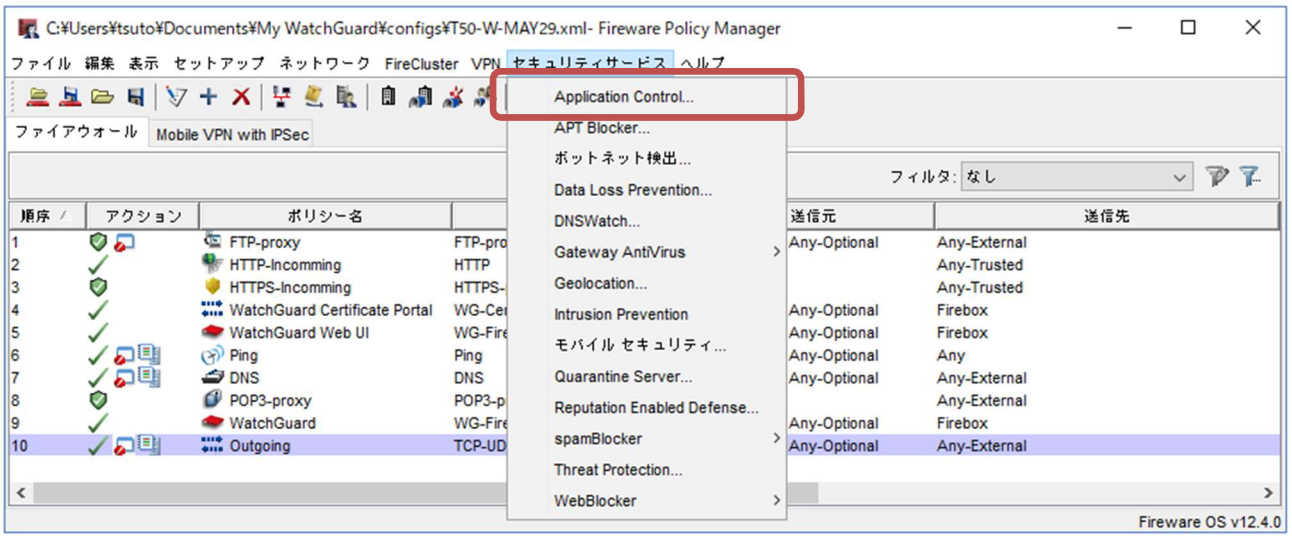
では実際に Application Control のアクションを作成してみましょう。

ファイル転送サービスを制御する

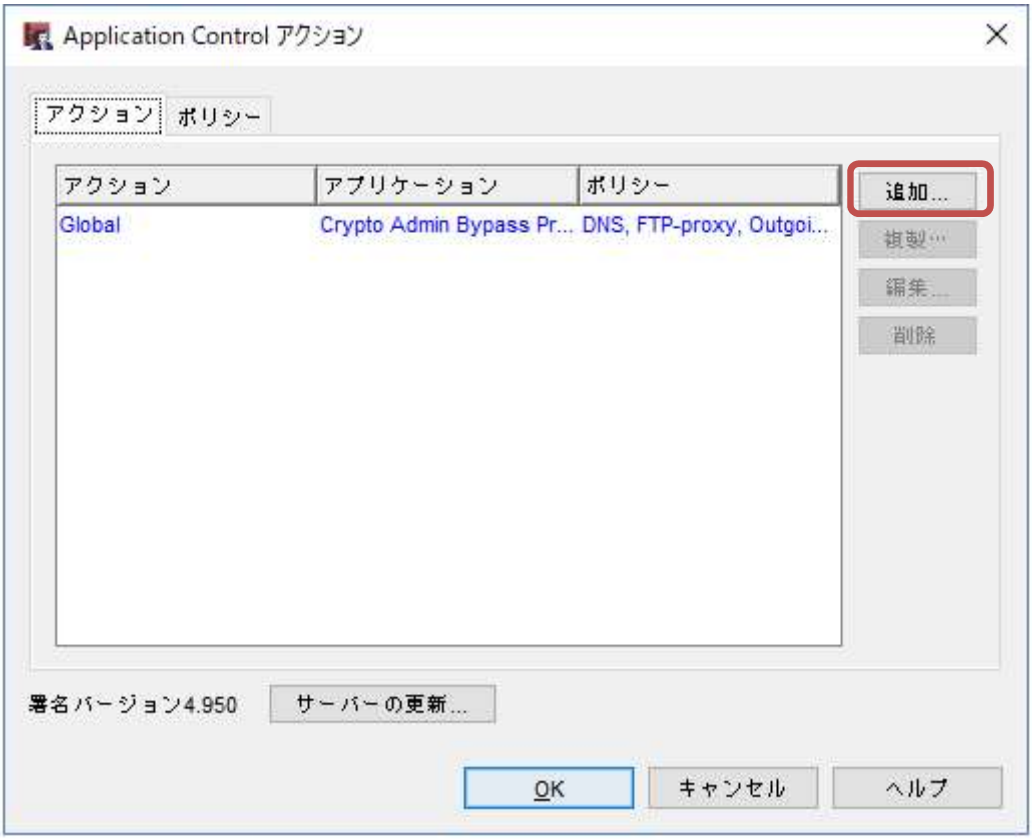
ファイル転送サービスは便利ですが、情報漏えいにつながるリスクもあります。

この項では、ファイル転送サービスは原則禁止、しかし顧客とのファイルのやりとりに Dropbox を使うということになり、それだけを許可するケースを想定し、設定します。

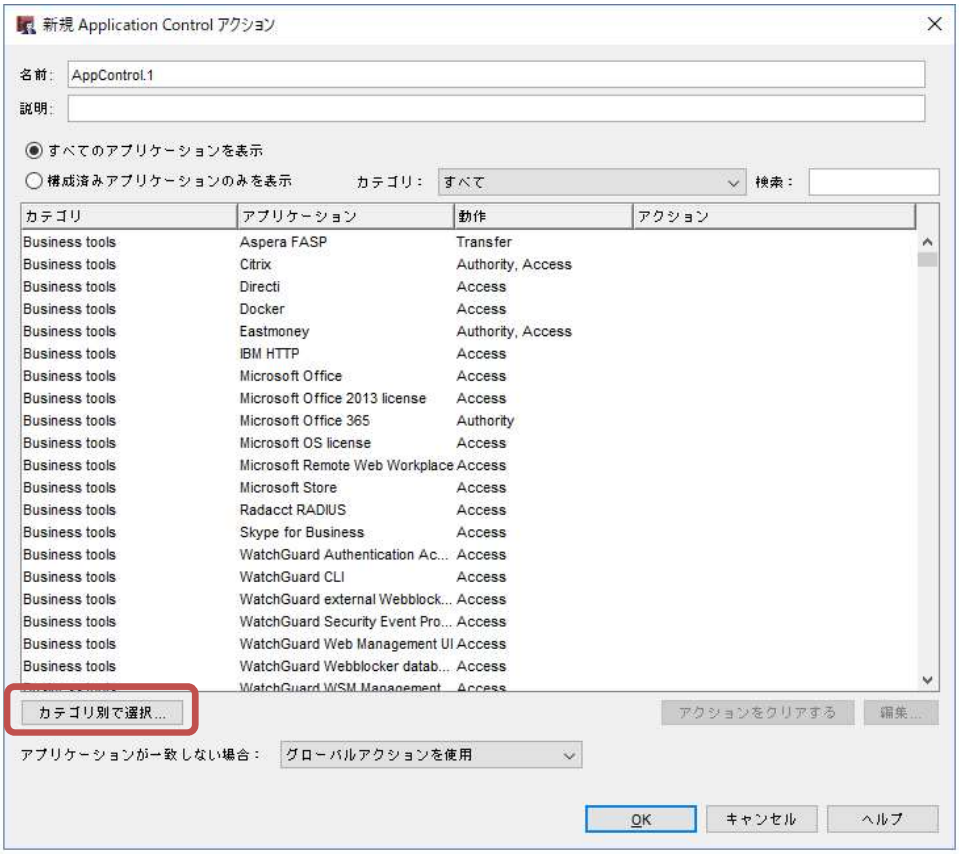
ポリシーマネージャのメニュー *セキュリティサービス* ー *Application Control* をクリックします。



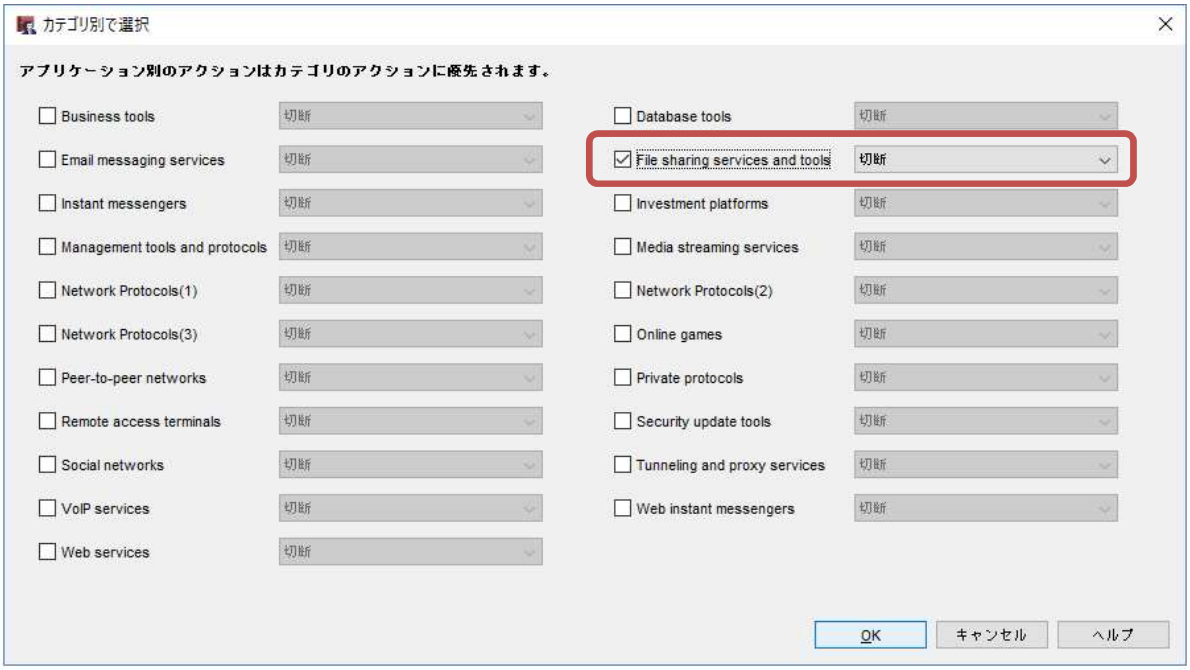
アクションの一覧画面が開きます。[追加]をクリックして、アクションを作成しましょう。



ここではファイル共有サービスすべてが対象になりますので、カテゴリ別の表示に切り替えます。



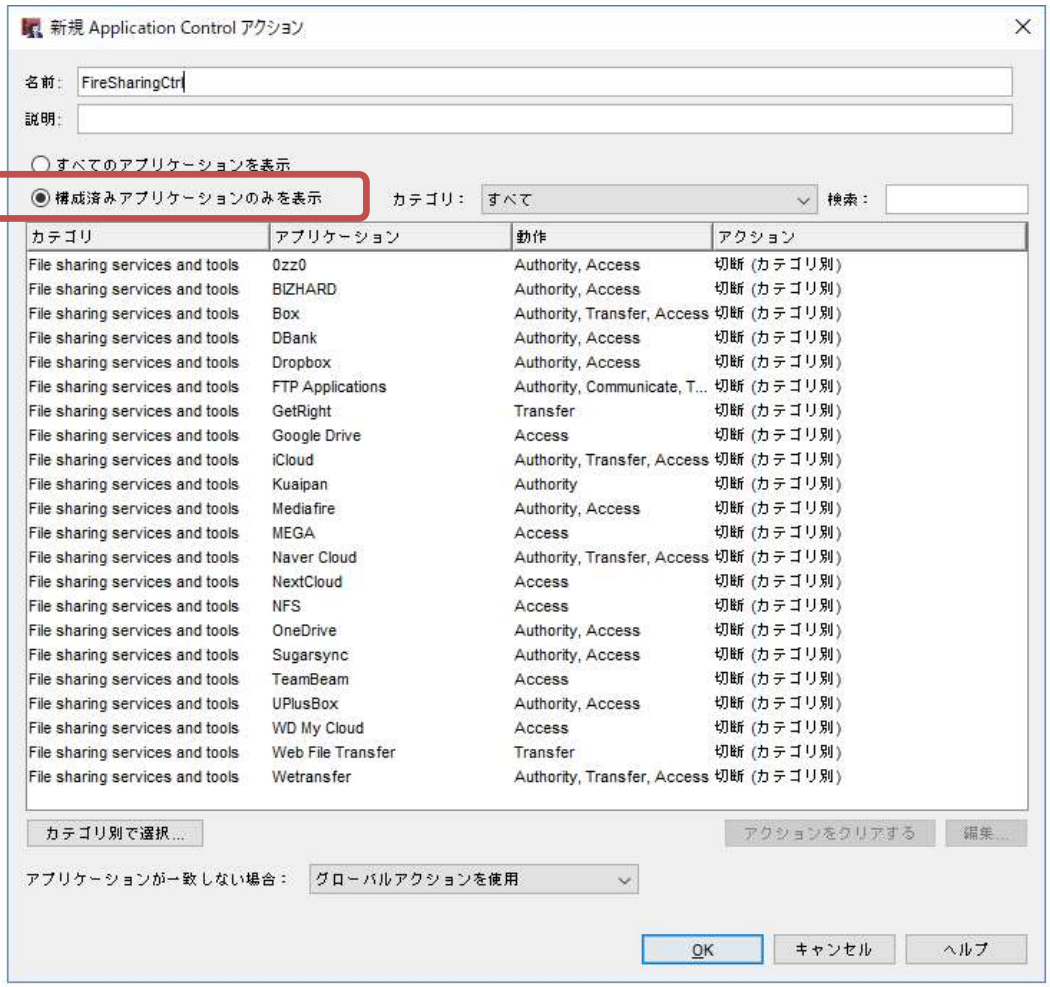
カテゴリで File Sharing services and tools をチェックし、切断を選択します。



OK をクリックして、新規アクションの追加画面に戻ります。

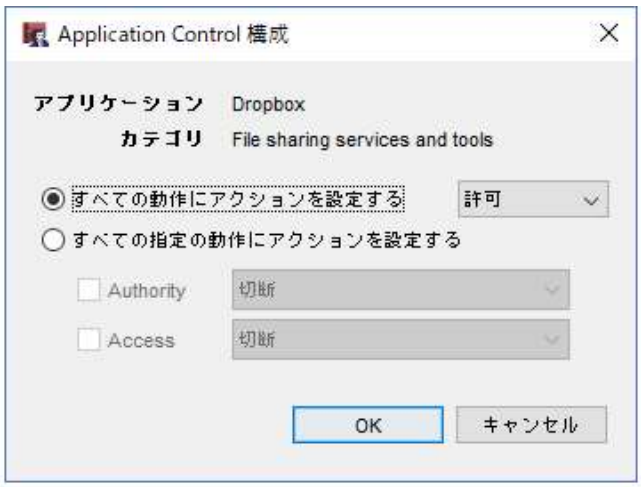
構成済みのアプリケーションのみを表示 をクリックすると、ファイル転送サービス関連のアプリケーションすべてが切断になっていることが確認できます。

名前はアクションの内容を表わすわかりやすいものに編集してください。ここでは「FileTransferCtrl」とします。



では、Dropbox だけ使用可能にしましょう。Dropbox をダブルクリックし、構成画面を開きます。

「すべての動作にアクションを設定する」にチェックを入れ、許可を選択します。



この画面では更に細かい制御も可能で、例えば「ファイルのアップロードは禁止し、受け取り（ダウンロード）のみ許可する」といった設定もできます。

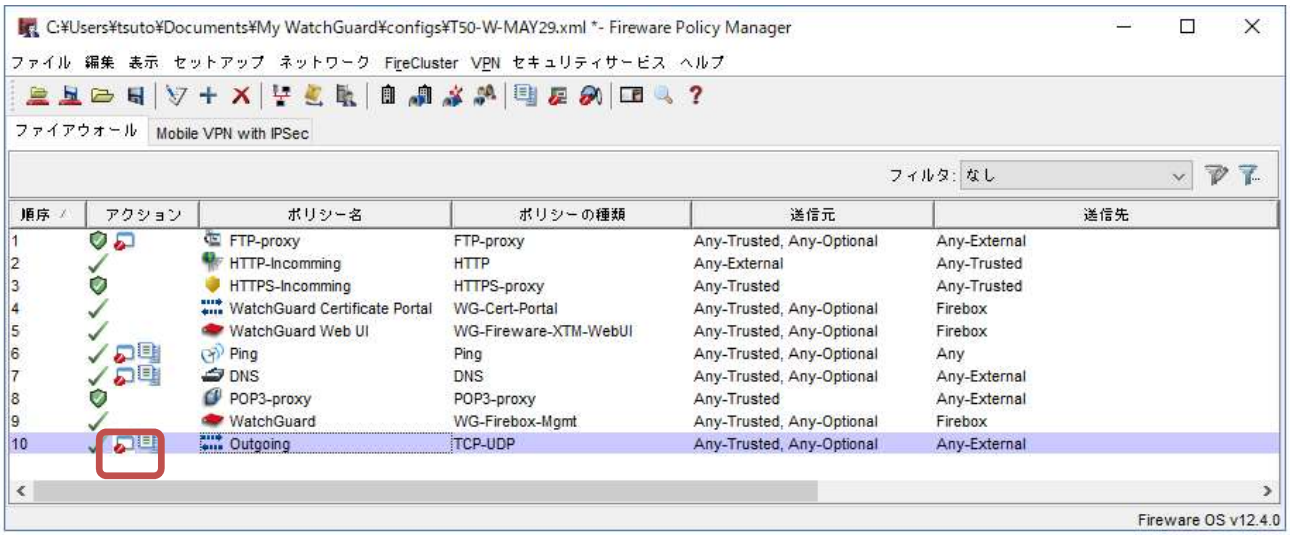
Authority を許可するとフィアルのアップロードが可能になってしまいますので切断、そしてダウンロードは可能にするため、Access を許可の設定にします。

このように必要に応じて、きめ細かな制御をすることが可能です。

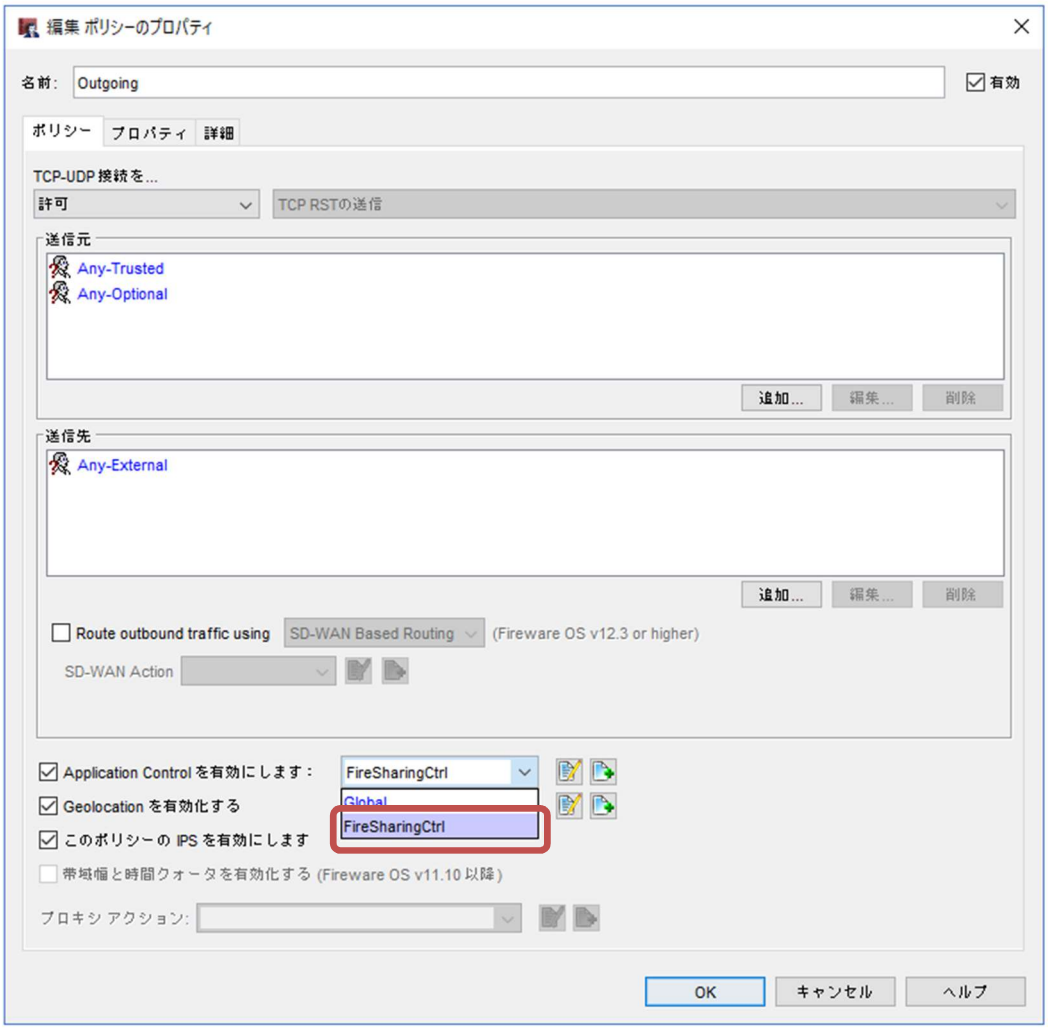
すべて OK で抜けて、ポリシーマネージャの画面に戻ります。

アクションのカラムに Application Control が有効になったことを示すアイコンが表示されています。

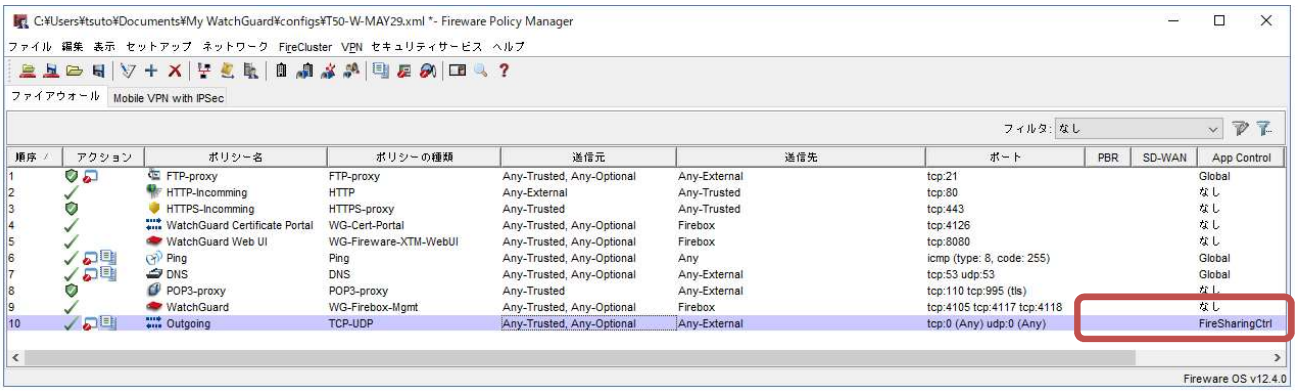
この状態で Outgoing ポリシーをダブルクリックして開きます。



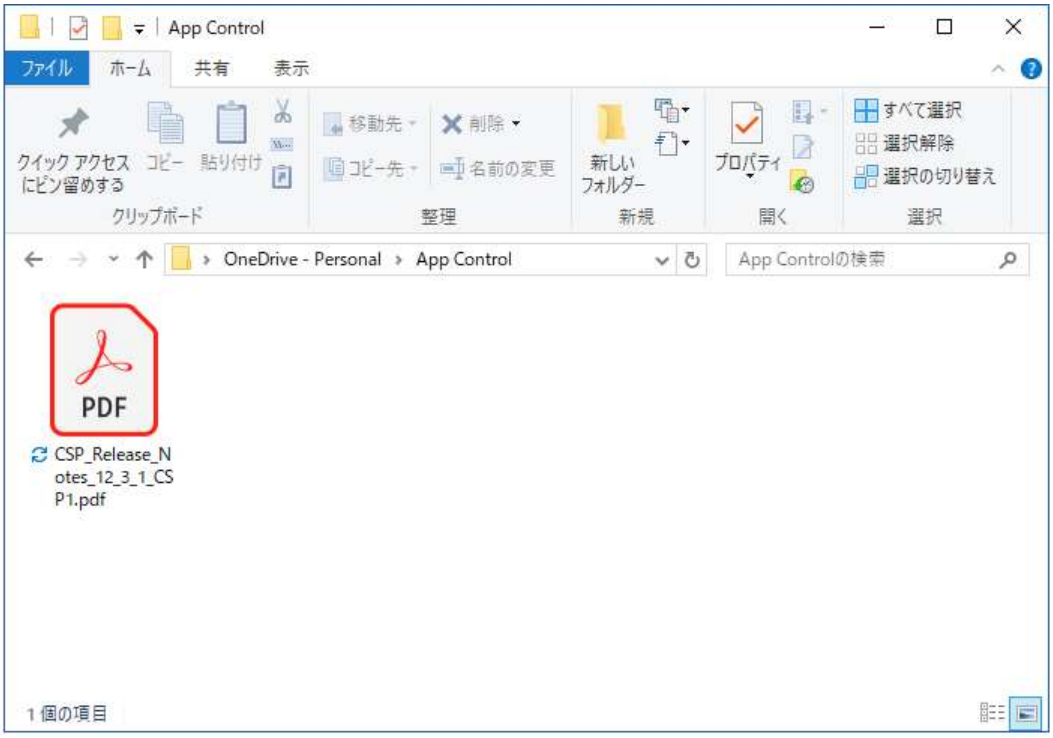
Application Control を有効にします のチェックの横のドロップダウンリストで、先ほど作成したアクションを選択します。



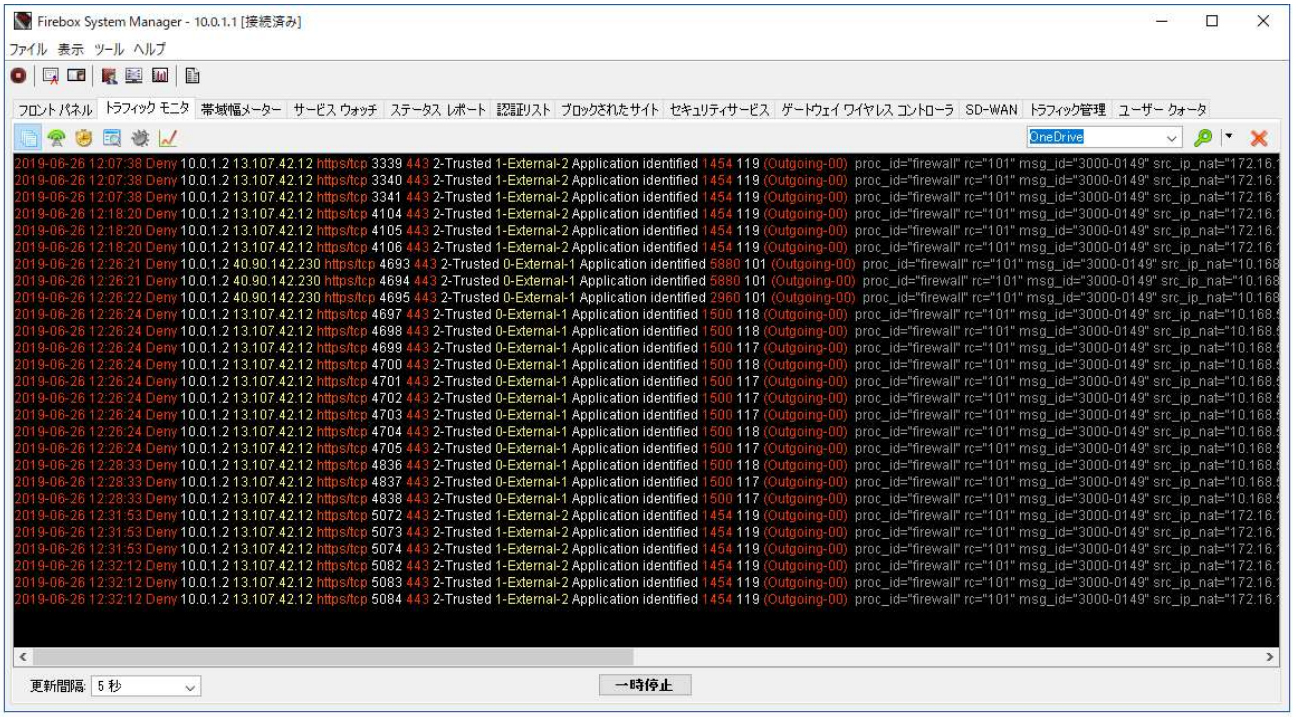
[OK]で抜けてポリシーマネージャに戻ると Outgoing ポリシーの App Control の列に選択したアクション名が表示されています。この状態で設定を保存すると、ファイル転送サービスに対する制御が動作します。



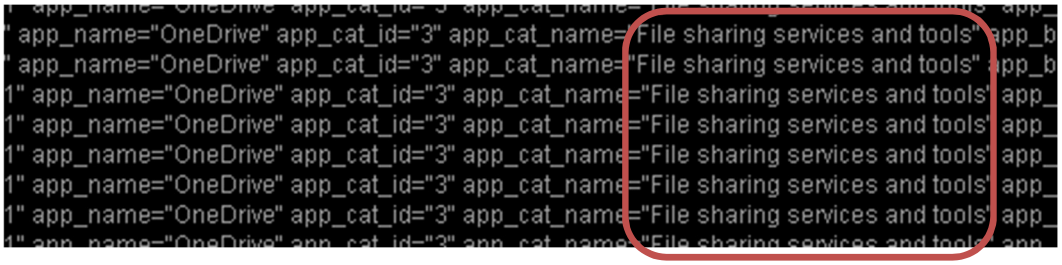
動作確認です。OneDrive ではアップロードできません。



ログを見ればファイル転送を切断していることが分かります。



行末のほうを見ると、ファイル転送であると検知してブロックしていることが確認できます。



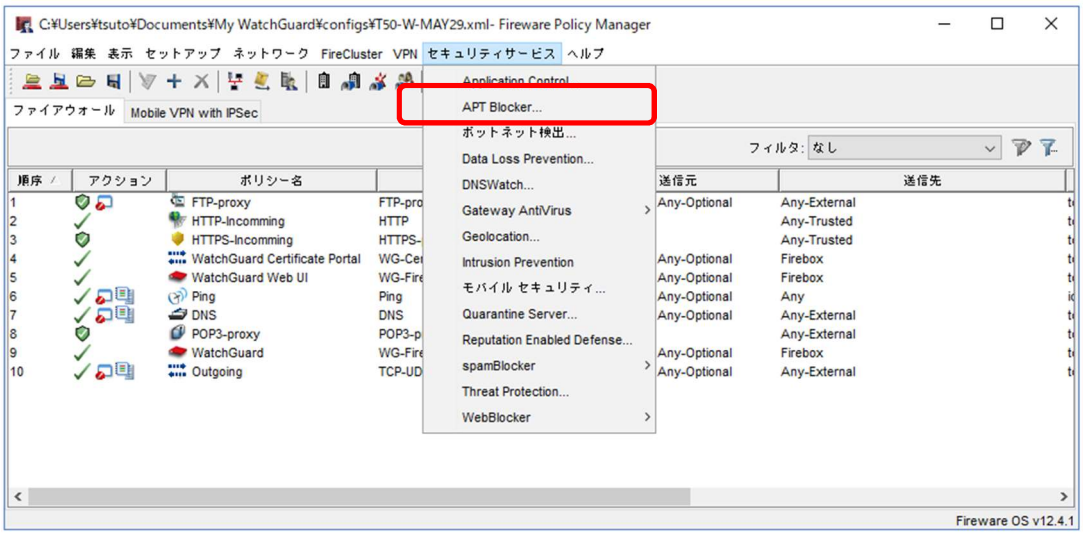
Dropbox では設定で許可したので、ファイルのアップロードができています。

APT Blocker

今日、サイバー攻撃はますます複雑で巧妙になっており、特定の組織の情報や資産を狙って行なわれる攻撃は標的型攻撃と呼ばれています。攻撃方法も多様であり、攻撃に使われるウィルスやマルウェアも無数の亜種が存在します。攻撃が来た時点で未知のものであることも珍しくありません。そうした新たな脅威に対応するために、APT Blocker は非常に効果的なソリューションです。

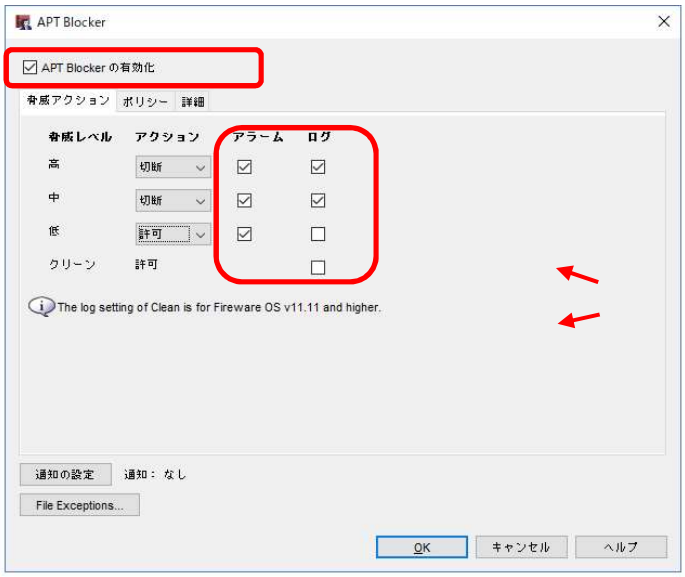
APT Blocker の有効化

Policy Manager のメニュー *セキュリティサービス* — *APT Blocker* をクリックします。



まず、APT Blocker の有効化にチェックを入れます。

するとグレーアウトしていた画面がアクティブになるので、脅威レベルに応じたアクションを設定してください。必要に応じてログとアラームのチェックを入れます。



図の例では、脅威レベルが高および中の場合に通信を切断するアクションにしています。

また、切断の時にログを出力するようにチェックを入れています。

ポリシーへの適用

どのポリシーで APT Blocker を有効にするかは、ポリシー タブで設定できます。

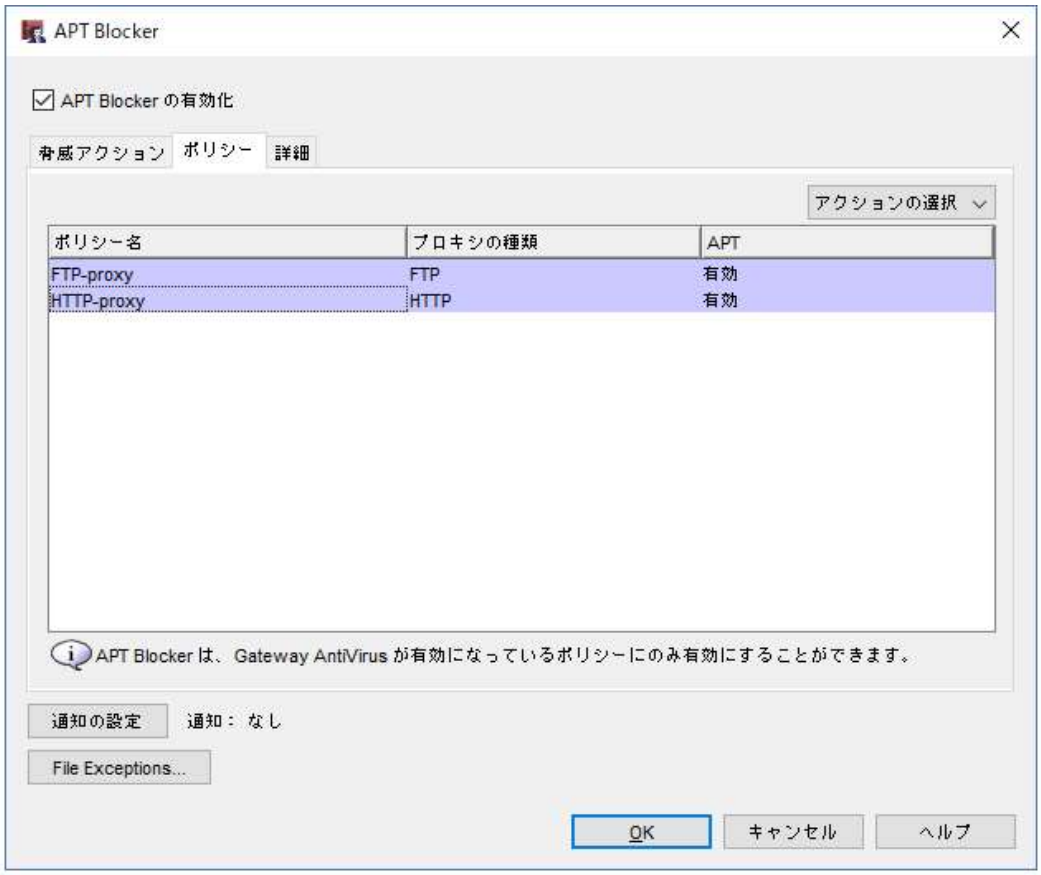
デフォルトでは、すべてのポリシーで無効[1]になっていることが確認できます。

ポリシーに適用するには、有効にしたいポリシーを選択し、右上のアクションの選択 ドロップダウンリストから「有効」をクリックします。

[1] 12.4.1 ではあらかじめすべて有効になっています。この例ではすべて無効になっています。

※　この一覧に表示されていないポリシーは、Proxy ポリシーが作成されていないか、Proxy ポリシーがあっても Gateway AntiVirus が有効になっていません。再度設定を見直してください

目的のポリシーで有効化したら、OK ボタンをクリックし、Policy Manager で設定を保存してください。



設定を保存すると、APT Blocker が有効になります。

第四章　ユーザーインターフェイス

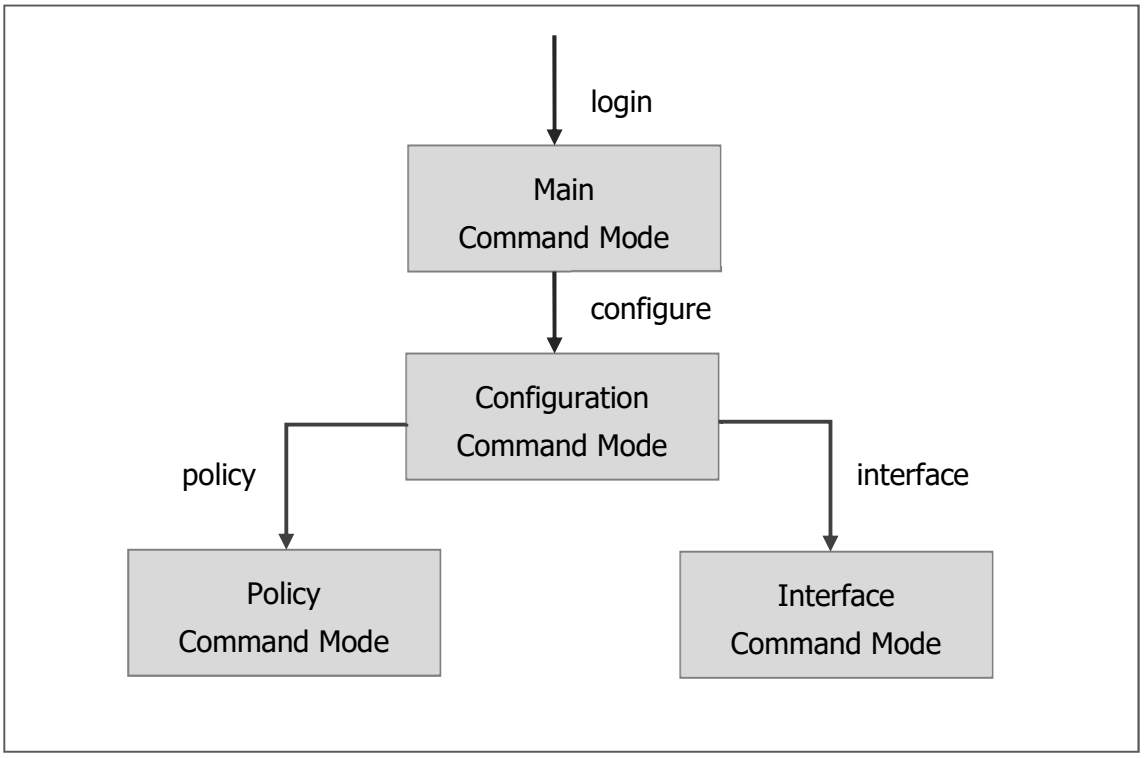
Firebox を管理するためのインターフェイスは 3 種類あります。管理者の方には、設定項目に制限がなく周辺ツールも充実した WSM を推奨しています。

しかし、本格的な WebUI と CLI も備えています。

この章では CLI の使い方を解説します。WebUI については、別途 WebUI ガイドをご覧いただきたいと思いますが、ここでは WebUI ガイドで触れていない Tips と便利な使い方をご紹介します。

CLI

CLI ではターミナルソフトでログイン後、それぞれのモードに入り、設定情報の取得や各種設定ができます。



次に接続方法、設定方法を解説します。

接続方法

TeraTerm、putty など、ターミナルソフトを以下の設定で接続することができます。

- シリアルケーブル

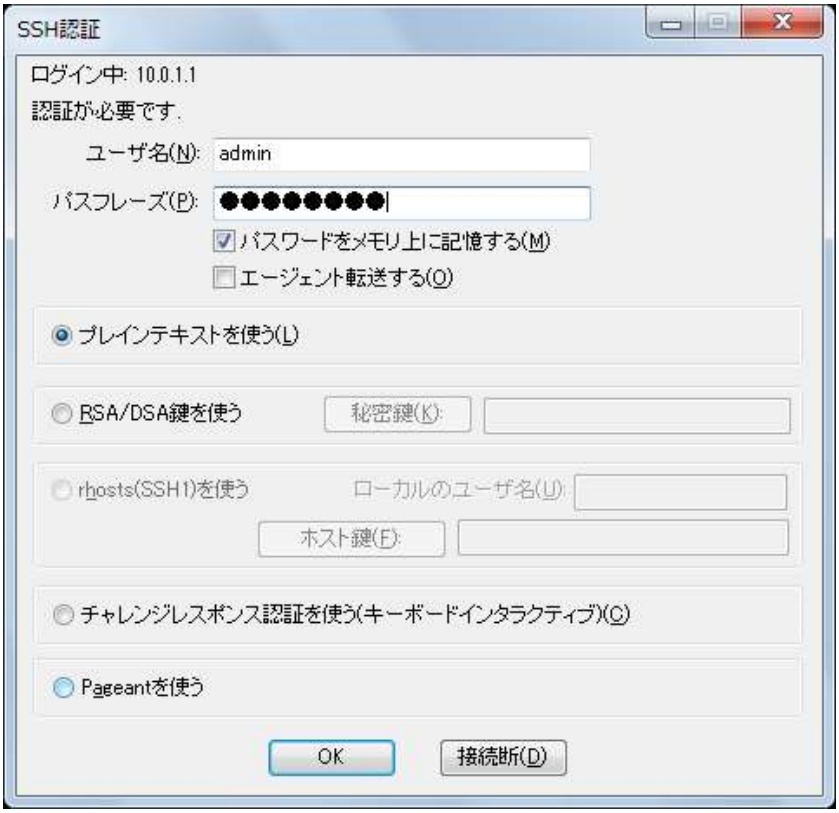
設定	値
Port	シリアルポート(通常は COM1)
Baud Rate	115200
Date Bits	8
Stop Bits	1
Parity	No
Flow Control	None

- TCP/IP

設定	値
Host	Firebox の Trusted または Optional の IP アドレス
TCP Port	4118
Service	SSH(Version SSH2)
Protocol	IPv4

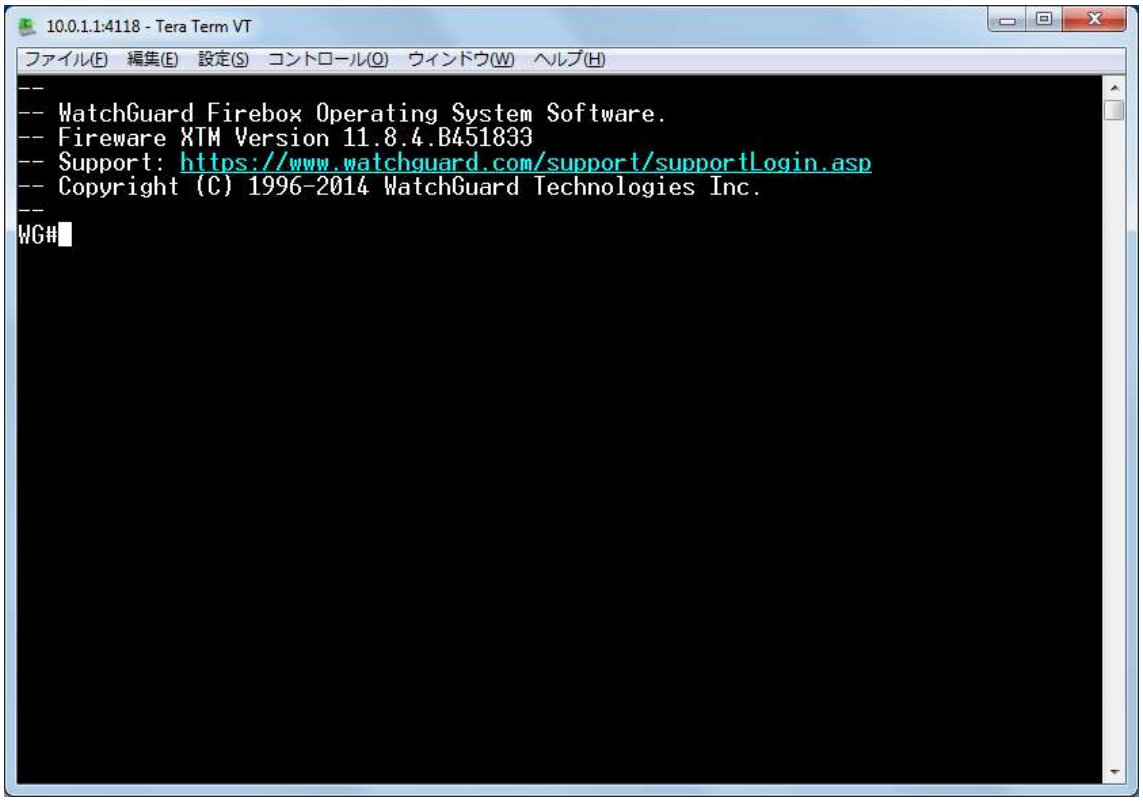
設定表どおり、ターミナルソフトで Firebox の IP アドレスとポート番号 4118 を指定して接続します。

ユーザ名は admin、パスフレーズは構成パスフレーズでログインします。



ログインするとプロンプトが表示されます。

WG# が表示されたメインコマンドモードとなります。



ログインしている間は排他制御がかかり、他の端末から CLI のログインや WebUI のログインができなくなるので注意してください。

設定手順

では設定例として、インターフェイス 1 の DHCP サーバーを構成するケースを見てみましょう。

configure コマンドで Configuration Command Mode に入ります。

```
WG#configure
```

プロンプトが変わります。

```
WG(config)#
```

インターフェイスを設定する場合、Interface Command Mode に入る必要があるので interface コマンドを入力します。interface に続いてスペースを入力し、次に何を入力してよいか分からない場合は「?」を入力します。

```
WG(config)#interface ?
  FastEthernet   FastEthernet IEEE 802.3
```

イーサネットポートを設定したいので FastEthernet を入力すればよいことが分かります。

コマンドは途中まで入力して TAB キーを押すと、補完する機能が働きます。

```
WG(config)#interface F<tab>
WG(config)#interface FastEthernet
```

エンターキーを押すと% Incomplete command.と表示されました。

```
WG(config)#interface FastEthernet
% Incomplete command.
```

これはまだ入力しなければならないパラメータがあるという意味です。

interface FastEthernet に続けて?を入力すると、インターフェイス番号を入力する必要があることが分かります。

```
WG(config)#interface FastEthernet ?
  <int>   FastEthernet interface number <0-5>
WG(config)#interface FastEthernet 1
```

インターフェイス 1 を指定していしてエンターを押します。

するとプロンプトが変わり、Interface Command Mode に入ったことが分かります。

？を入力すると、インターフェイスを設定するためのコマンド一覧が取得できます。

```
WG(config/if-fe1)#?
Trusted interface configuration commands:
  dhcp                 Dynamic host configuration protocol
  enable               Enable/Disable current physical interface
  exit                 Exit from interface configuration mode
  help                 Description of the interactive help system
  history              Display the command history list with line numbers
  ip                   Internet protocol
  link-speed           Link operation speed property
  mac-access-control   Restrict access by MAC address
  mac-ip-binding       Static MAC/IP binding in arp table
  mtu                  Set the interface maximum transmission unit (MTU)
  name                 Name of the entity
  no                   Negate a command or set its defaults
  qos                  Quality of service, be sure to enable settings by the command global-
setting
  secondary            Secondary ip address
  show                 Show running system information
  type                 Network interface type
  v6                   Configure the ipv6 interface
```

DHCP サーバーを構成するには dhcp コマンドが使えることが分かります。

それでは dhcp のあとにスペースと？を入れながら、パラメータ名を確認しつつ、設定してゆきます。

```
WG(config/if-fe1)#dhcp server ?
  <int>           Lease time, in hour <1-596523>
  dns-server      Dns server
  domain          Domain name e.g. foo.com
  reservation     Reservation name, e.g. a host name
  start-addr      Start ip address
  wins            Specific the wins server's ip address

WG(config/if-fe1)#dhcp server start
WG(config/if-fe1)#dhcp server start-addr 10.0.1.100 ?
  <ipaddr>    End ip address <A.B.C.D>

WG(config/if-fe1)#dhcp server start-addr 10.0.1.100 10.0.1.199 ?
  <cr>            Carriage return
  <int>           Lease time, in hour <1-596523>
  dns-server      Dns server
  domain          Domain name e.g. foo.com
  reservation     Reservation name, e.g. a host name
  start-addr      Start ip address
  wins            Specific the wins server's ip address

WG(config/if-fe1)#dhcp server start-addr 10.0.1.100 10.0.1.199
WG(config/if-fe1)#
```

同じように DNS サーバーも設定します。

```
WG(config/if-fe1)#dhcp server dns
WG(config/if-fe1)#dhcp server dns-server ?
  <ipaddr>    Dns server <A.B.C.D>

WG(config/if-fe1)#dhcp server dns-server 8.8.8.8
WG(config/if-fe1)#
```

コマンドが成功すると、プロンプトに戻るだけです。設定し、それが即反映となる点にご注意ください。

設定が反映されていることをポリシーマネージャから確認してみてください。

CLI を終了するには、exit コマンドで各モードを抜けて終了させます。

```
WG(config/if-fe1)#exit
WG(config)#exit
WG#exit
```

CLI についてのより詳細な情報は WatchGuard(US)のサイトより得ることができます。

http://www.watchguard.com/help/documentation/xtm.asp (英語)

このページにある「Command Line Interface Reference」のリンクから、最新バージョンの CLI リファレンスを参照できます。

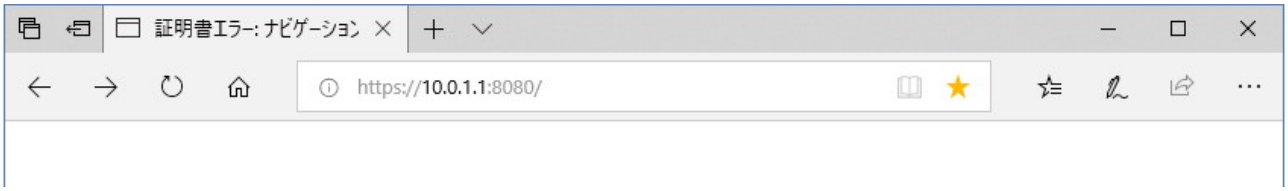
WebUI

WebUI についての詳しい情報は別途「WebUI ガイド」をご覧ください。

ここでは WebUI での接続方法と、WebUI ガイドには記載されていない便利な機能や使い方について解説します。

接続方法

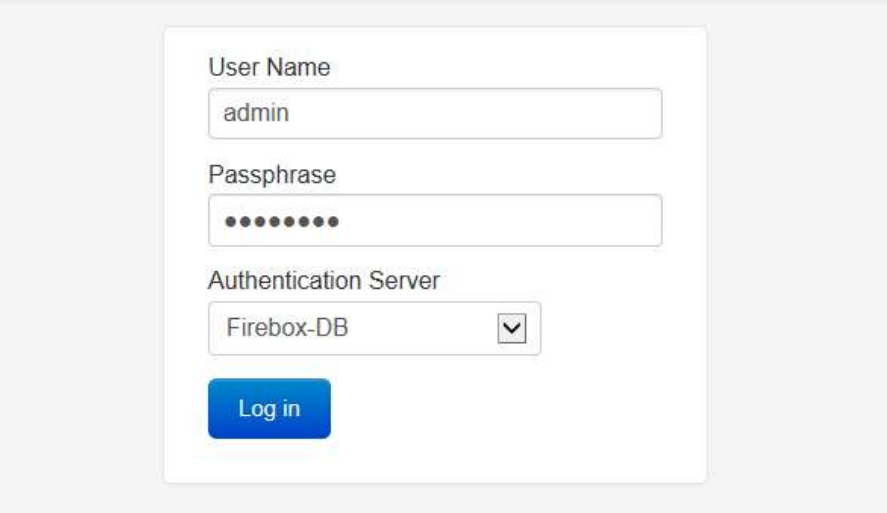
https://Firebox の IP アドレス:8080 で接続します。



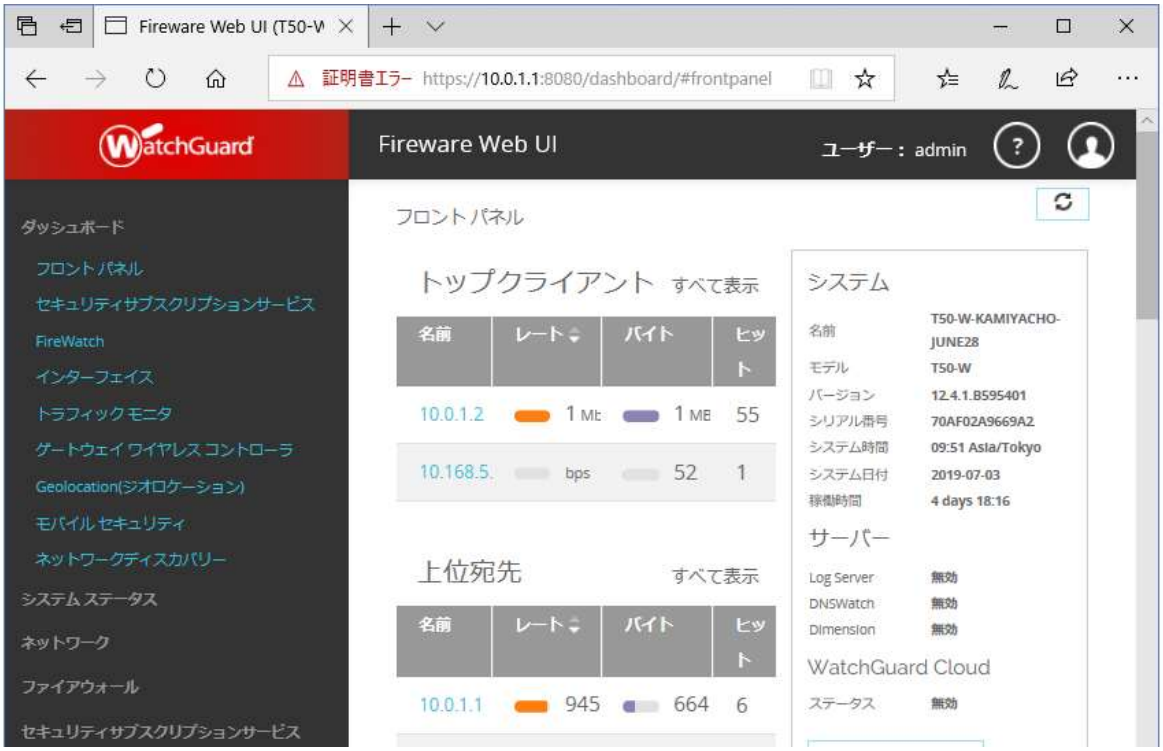
セキュリティ証明書の警告が出ますが、「詳細」—「Web ページへ移動」をクリックして閲覧を続行します。

ログインはステータスパスフレーズ(status)、構成パスフレーズ(admin)のどちらでも可能です。

ただ、admin でログインすると排他制御がかかり、他の WebUI の admin ログインや CLI から接続できなくなります。また、WSM で接続しているクライアントからも設定の保存ができなくなるので注意してください。



ログインするとダッシュボードが表示され、接続した Firebox の状態のサマリーが表示されます。

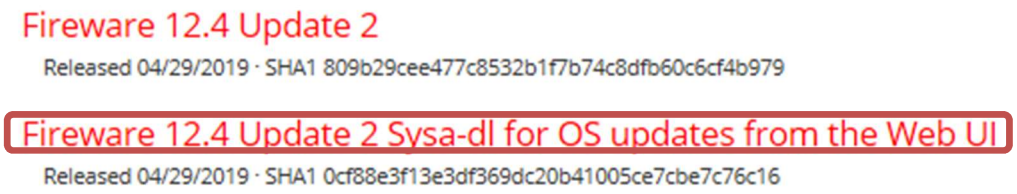


左側の各メニューから、インターフェイスやポリシーの設定ができます。

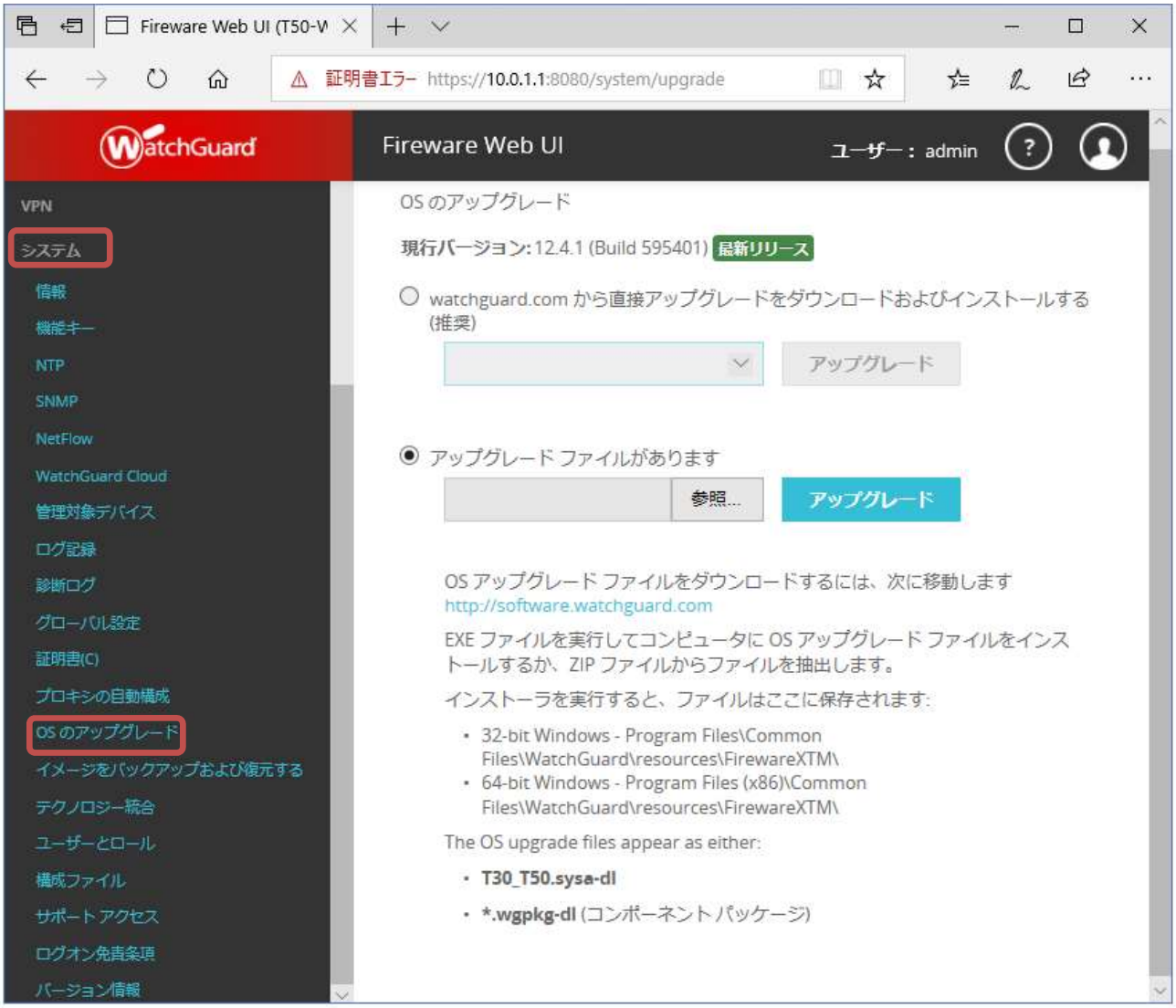
Fireware のアップグレード/ダウングレード

WebUI ではファームウェアのアップグレード画面から、バージョンアップはもちろんの事、ダウングレードもできるようになっています(但しファクトリーリセット状態になります)。

あらかじめ WebUI 用のファームウェア(exe 形式ではなく zip 形式のものを展開)を用意しておきます。Software Download のページにも「Fireware 12.4 Update 2 Sysa-dl for OS updates from the Web UI」という名称でダウンロードできるようになっています。

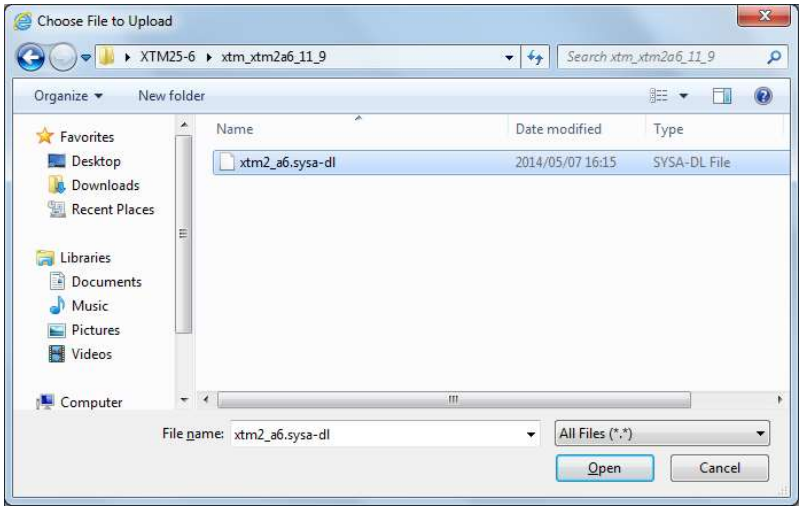


WebUI 左側メニューの *システム* － *アップグレード OS* とクリックします。



ファイルの選択で [Browse...] ボタンをクリックします。

あらかじめ用意しておいたファームウェアのファイルを指定します。



[アップグレード] をクリックします。

ボタンがアップグレード中...となるのでしばらく待ちます。

ダウングレードの場合、Firebox が工場初期出荷状態になる旨、警告が表示されますが、Yes で進みます。

イメージがアップロードされると、再起動が促されますので、[Yes]をクリックします。

ログイン画面に戻ります。

Firebox が再起動されたら、再度ログインし、動作を確認してください。

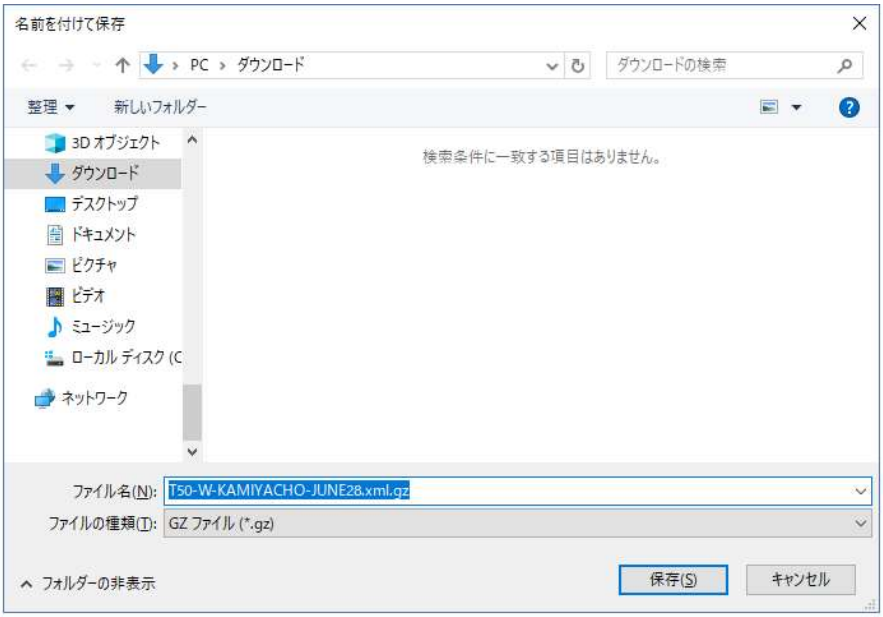
ダウングレードの場合は、Quick Setup Wizard を実施してください。

コンフィグファイルの保存とレポート表示

WSM であれば、コンフィグはポリシーマネージャの「ファイルとして保存」で保存し、設定ファイルを保存できます。しかし WebUI の場合どうすればよいでしょうか。

左側メニュー *システム* ー *構成ファイル* をクリックします。
「Download the Configuration File」のリンクをクリックすると、設定ファイルが取得できます。

保存先を指定して保存します。



gzip 形式で保存されるので、対応した解凍ソフトで取り出します。

WebUI では、コンフィグのダウンロードだけでなく、コンフィグを分かりやすいレポート表示で閲覧することが可能です。「Firebox Configuration Report」リンクをクリックします。

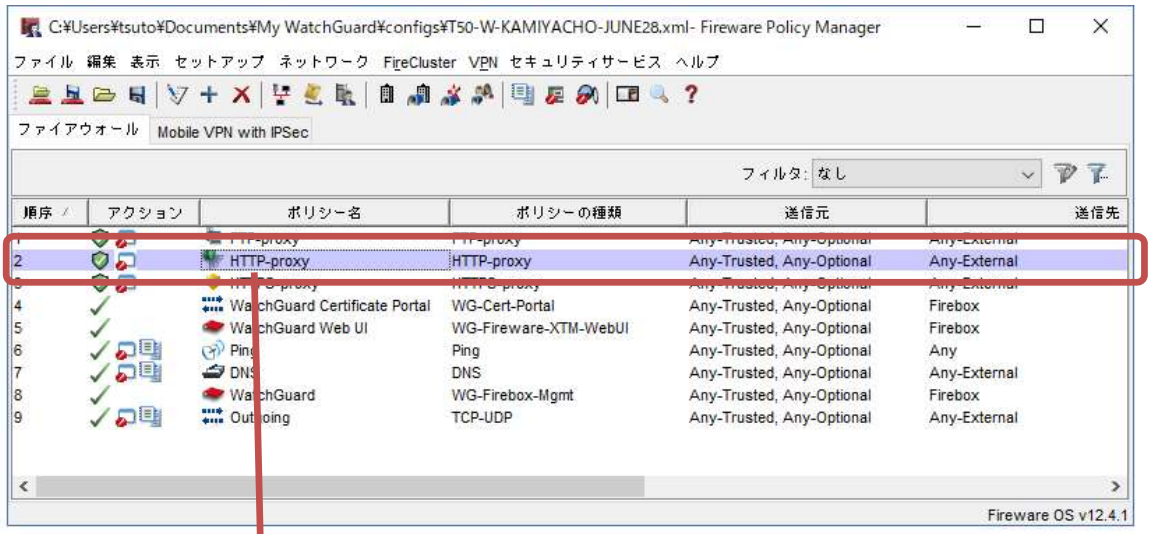
別窓でレポートが表示されます。設定の閲覧や、PDF 作成ソフトなどで設定ドキュメントとして保存するなどの用途でお使いいただけます。

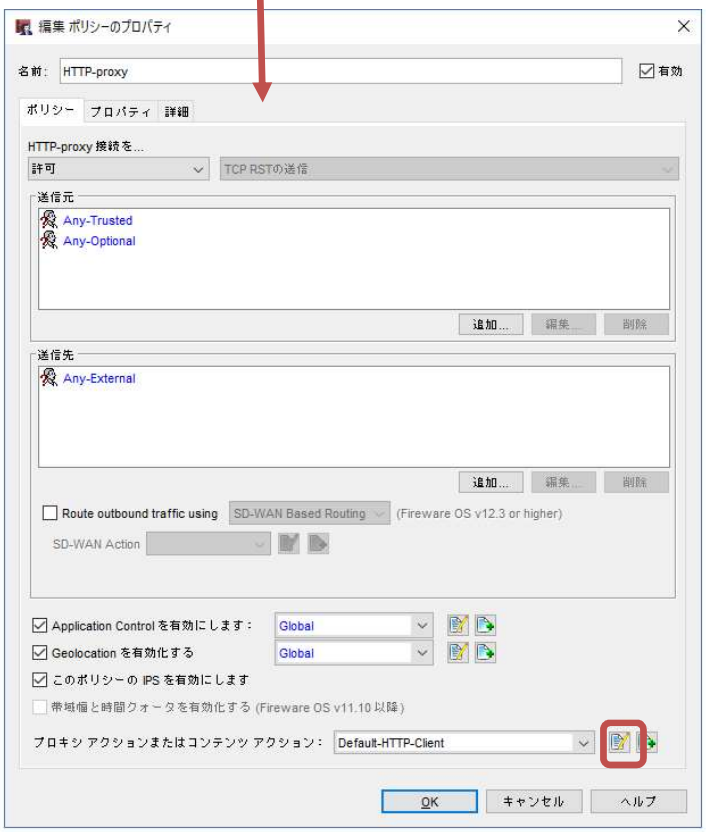

空白のページ
検索または Web アドレスを入力
Firebox 構成レポート
[印刷]
目次
1 ネットワーク
1-1 インターフェイス
1-2 ARP エントリ
1-3 リンクアグリゲーション
1-4 VLAN
1-5 ブリッジ
1-6 Loopback
1-7 複数WAN
1-8 SD-WAN
1-9 リンク モニー
1-10 動的DNS
1-11 NAT
1-12 ルート
1-13 動的ルーティングに
1-14 Multicast Routing
1-15 ゲートウェイ ワイヤレス コントローラ
1-16 モデム
1-17 認証方法
2 ファイアウォール
2-1 ファイアウォール ポリシー
2-2 Firewall Policies Details
2-3 Mobile VPN ポリシー
Firebox 構成レポート
モデル: T50-W
日付: 7/3/2019
構成
1. ネットワーク
1-1 インターフェイス
ネットワーク構成
構成インターフェイスでミックス ルーティング モード.
インターフェイス 種類 名前 (エイリアス) IPv4 アドレス IPv6 アドレス 説明
0 External External DHCP Auto
1 Trusted Trusted 10.0.1.1/24
2 無効 Optional-1 0.0.0.0/24
3 無効 Optional-2 0.0.0.0/24
4 無効 Optional-3 0.0.0.0/24
5 無効 Optional-4 0.0.0.0/24
6 無効 Optional-5 0.0.0.0/24
ドメイン名前 なし
DNSサーバー なし
WINSサーバー なし
Copyright © 2012-2015 WatchGuard Technologies, Inc. All Rights Reserved.

クライアント側の UI カスタマイズ

この項では管理者向けのインターフェイスではなく、クライアントがウェブブラウザで見ることになる拒否画面のカスタマイズについて触れておきます。

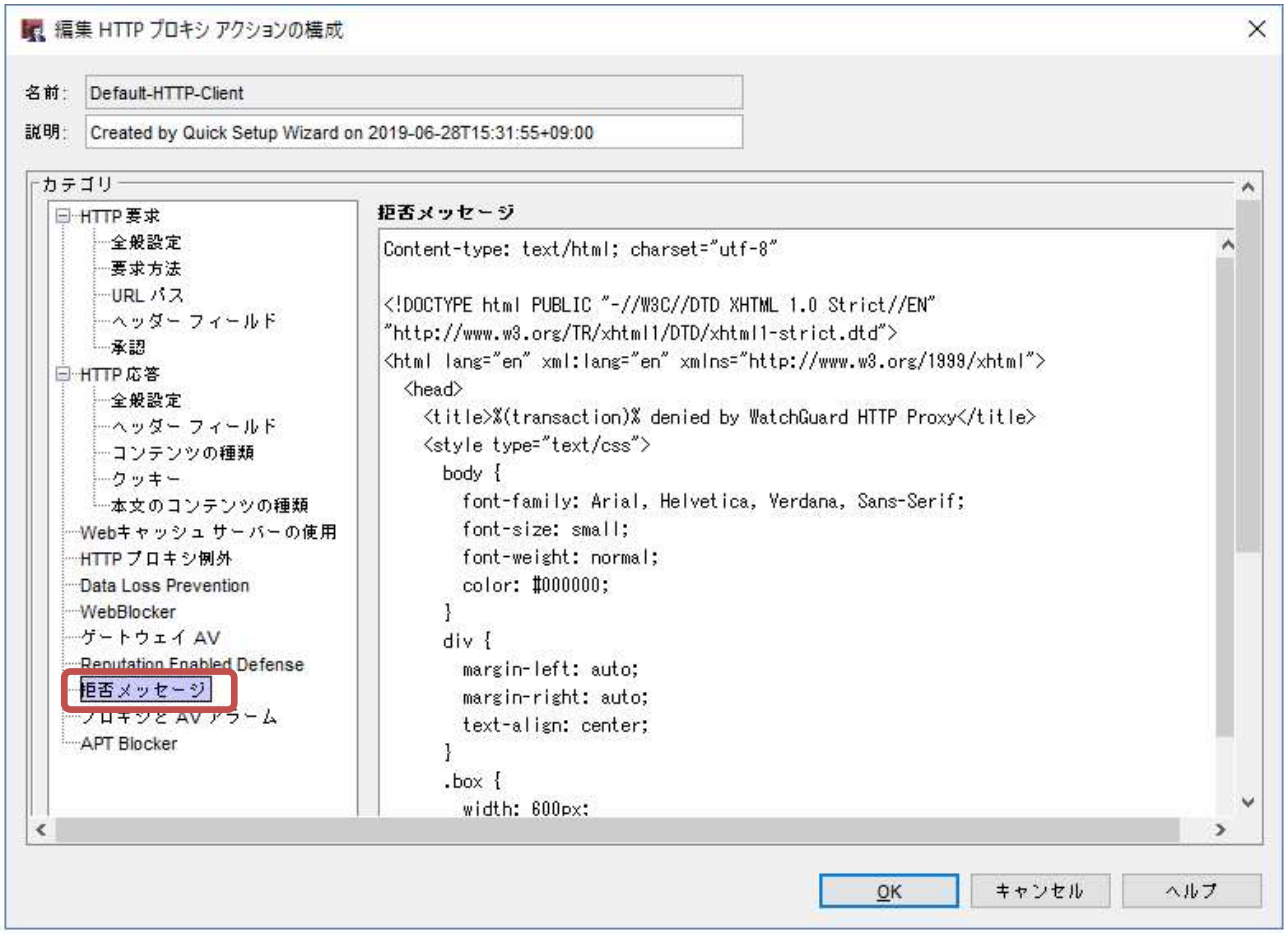
WebBlocker、Gateway Anti-Virus、RED などで拒否された際に表示されるセキュリティ警告のメッセージはデフォルトで英語になっています。その警告ページのテンプレートはポリシーマネージャの HTTP-proxy ポリシーのプロパティにあります。まず HTTP-proxy ポリシーを開きます。





[プロキシの表示/編集]ボタンをクリックします。

プロキシの表示/編集画面の「拒否メッセージ」に表示のテンプレートの設定があります。



このテンプレートの HTML を編集すれば日本語のページにすることができます。
テンプレート中で使用されている%(...)%で囲まれた Firebox のメッセージを格納する変数部分ですので、必ず残してください。

次頁にそのままコピー＆ペーストとして使える HTML ソースを掲載しておきます。

(72 ページで使用したセキュリティ警告画面の HTML です)

ソース中のメールアドレスや連絡先の部分は実際のものに書き換えてください

```
Content-type: text/html; charset="utf-8"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>%(transaction)%   denied by WatchGuard HTTP Proxy</title>
    <style type="text/css">
      body {
        font-family: Arial, Helvetica, Verdana, Sans-Serif;
        font-weight: normal;
        color: #000000;
      }
      div {
        margin-left: auto;
        margin-right: auto;
        text-align: center;
      }
      .box {
        width: 640px;
        background-color: #F2F2F2;
        border-left: solid 1px #C2C2C2;
        border-right: solid 1px #C2C2C2;
        vertical-align: middle;
        padding: 20px 10px 20px 10px;
      }
      p {
        text-align: left;
        font-size: small;
      }
      .red {
        font-weight: bold;
        font-size: large;
        color: Red;
        text-align: center;
      }
      .band {
        height: 20px;
        color: White;
        background: #333333;
```

```
        width: 640px;
        border-left: solid 1px #333333;
        border-right: solid 1px #333333;
        padding: 3px 10px 0px 10px;
      }
      div#wrap {
        margin-top: 50px;
      }
      .center{
        text-align: center;
            }
      .blue {
        font-weight: bold;
        font-size: large;
        color: blue;
        text-align: center;
      }
    </style>
  </head>
  <body>
    <div id="wrap">
      <div class="band">Security Alert !</div>
      <div class="box">
        <p class="red">セキュリティ機能によってアクセスは拒否されました</p>
        <p class="blue">お問い合わせは情報システム部(内線 1000)まで。</p>
        <p class="center">アクセス許可を希望される場合は、以下のメッセージをコピーして<br/>
        <a href="mailto:info@joho-system.domain">info@joho-system.domain</a>までメールでご連絡ください</p>
        <hr/>
        <p><b>  理由: </b> %(reason)% </p>
        <p><b>アクセスメソッド:</b> %(method)%</p>
        <p><b>アクセス先のサーバー:</b> %(url-host)%</p>
        <p><b>URL パス:</b> %(url-path)%</p>
      </div>
      <div class="band">WatchGuard Technologies, Inc.</div>
    </div>
  </body>
</html>
```

終わりに

WSM 詳細設定ガイドをご活用いただきありがとうございます。

WatchGuard Firebox がいかに多様なセキュリティ要件に適用できるか、実感いただけたと存じます。

今後も弊社の製品が、御社のセキュリティの要としてお役に立てれば幸いです。