Check Point 730/750 Appliance
ローカル管理

R77.20.15

管理ガイド
重要な情報

最新版ソフトウェア

最新版ソフトウェアには、機能や安定性の向上、セキュリティの拡張、新たな脅威や進化する攻撃に対処する最新の保護機能が備えられています。常に最新版をインストールすることをお勧めします。

Check Point R77.20.15

この製品に関する詳細は、R77.20.15 のホームページを参照してください。

最新版ドキュメント

このドキュメントの最新バージョンをダウンロードしてください。

チェック・ポイント製品の詳細な技術情報については、チェック・ポイントのサポート・センター（http://supportcenter.checkpoint.com）を参照してください。

ドキュメントに関するご意見

チェック・ポイントは、わかりやすいマニュアルの作成に日々取り組んでいます。

good意見やご要望がありましたら、ぜひ弊社までお送りください。

改訂履歴

<table>
<thead>
<tr>
<th>日付</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016年6月15日</td>
<td>初版</td>
</tr>
<tr>
<td>タブ</td>
<td>内容</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>ファイアウォール・アクセス・ポリシー</td>
<td>84</td>
</tr>
<tr>
<td>サーバ・オブジェクトの定義</td>
<td>89</td>
</tr>
<tr>
<td>ユーザ認識</td>
<td>92</td>
</tr>
<tr>
<td>QoS の設定 - 帯域幅の制御</td>
<td>94</td>
</tr>
<tr>
<td>QoS の使用</td>
<td>95</td>
</tr>
<tr>
<td>NAT の定義</td>
<td>97</td>
</tr>
<tr>
<td>NAT サーバ・オブジェクトの定義</td>
<td>100</td>
</tr>
<tr>
<td>詳細 - NAT ルールの作成と編集</td>
<td>100</td>
</tr>
<tr>
<td>脅威対策の管理</td>
<td>103</td>
</tr>
<tr>
<td>脅威対策 Blade の設定</td>
<td>103</td>
</tr>
<tr>
<td>IPS 例外の設定</td>
<td>106</td>
</tr>
<tr>
<td>感染ホストの表示</td>
<td>108</td>
</tr>
<tr>
<td>保護リストの表示</td>
<td>109</td>
</tr>
<tr>
<td>脅威対策のエンジン設定</td>
<td>110</td>
</tr>
<tr>
<td>アンチスパム Blade の設定</td>
<td>113</td>
</tr>
<tr>
<td>アンチスパムの例外の設定</td>
<td>114</td>
</tr>
<tr>
<td>VPN の管理</td>
<td>116</td>
</tr>
<tr>
<td>リモート・アクセス Blade の設定</td>
<td>116</td>
</tr>
<tr>
<td>リモート・アクセス・ユーザの設定</td>
<td>118</td>
</tr>
<tr>
<td>リモート・アクセス認証サーバの設定</td>
<td>120</td>
</tr>
<tr>
<td>詳細リモート・アクセス・オプションの設定</td>
<td>123</td>
</tr>
<tr>
<td>サイト間 VPN プレードの設定</td>
<td>125</td>
</tr>
<tr>
<td>VPN サイトの設定</td>
<td>126</td>
</tr>
<tr>
<td>VPNトンネルの表示</td>
<td>129</td>
</tr>
<tr>
<td>サイト間の詳細設定</td>
<td>129</td>
</tr>
<tr>
<td>信頼済み CA の管理</td>
<td>131</td>
</tr>
<tr>
<td>インストール済み証明書の管理</td>
<td>132</td>
</tr>
<tr>
<td>内部証明書の管理</td>
<td>133</td>
</tr>
<tr>
<td>ユーザおよびオブジェクトの管理</td>
<td>135</td>
</tr>
<tr>
<td>ユーザ認識</td>
<td>135</td>
</tr>
<tr>
<td>ローカル・ユーザとユーザ・グループの設定</td>
<td>135</td>
</tr>
<tr>
<td>ローカル・システム管理者の設定</td>
<td>136</td>
</tr>
<tr>
<td>認証サーバの管理</td>
<td>136</td>
</tr>
<tr>
<td>アプリケーションと URL の管理</td>
<td>139</td>
</tr>
<tr>
<td>システム・サービスの管理</td>
<td>140</td>
</tr>
<tr>
<td>サービス・グループの管理</td>
<td>143</td>
</tr>
<tr>
<td>ネットワーク・オブジェクトの管理</td>
<td>144</td>
</tr>
<tr>
<td>ネットワーク・オブジェクト・グループの管理</td>
<td>145</td>
</tr>
<tr>
<td>ログとモニタリング</td>
<td>147</td>
</tr>
<tr>
<td>セキュリティ・ログの表示</td>
<td>147</td>
</tr>
<tr>
<td>システム・ログの表示</td>
<td>148</td>
</tr>
<tr>
<td>外部ログ・サーバの設定</td>
<td>149</td>
</tr>
<tr>
<td>内部ネットワーク内のアクティブ・コンピュータの管理</td>
<td>151</td>
</tr>
<tr>
<td>感染ホストの表示</td>
<td>151</td>
</tr>
<tr>
<td>VPNトンネルの表示</td>
<td>153</td>
</tr>
<tr>
<td>アクティブな接続の表示</td>
<td>153</td>
</tr>
<tr>
<td>モニタリング・データの表示</td>
<td>153</td>
</tr>
<tr>
<td>レポートの表示</td>
<td>155</td>
</tr>
<tr>
<td>システム・ツールの使用</td>
<td>156</td>
</tr>
<tr>
<td>SNMP</td>
<td>157</td>
</tr>
<tr>
<td>詳細設定</td>
<td>159</td>
</tr>
<tr>
<td>USBドライブによるアップグレード</td>
<td>159</td>
</tr>
</tbody>
</table>
Check Point 730/750 Appliance の概要

Check Point 730/750 Appliance は Check Point Software Blade アーキテクチャに対応しており、独立したモジュール型の各セキュリティ保護機能を提供しています。Software Blade を素早く有効化し、個別のセキュリティ要件に応じて設定できます。

Check Point 730/750 Appliance は、Gaia オペレーティング・システムの組み込みバージョンを実行します。これには clish インタフェース、SNMPv2/3、およびルーティング・スタック実装などのコア構成要素が含まれます。Gaia 機能に加えて、組み込み型 Gaia はさらに内蔵ネットワーク・スイッチ、ワイヤレス・ネットワーク、4G/LTE インターネット接続、ハイ・アベイラビリティまたは負荷分散モードでのマルチインターネット接続（2つ以上）、ポリシー・ベースのルーティング、DDNS サポート、および USB によるクイック導入をサポートします。

このガイドでは、ローカル管理モードに関連するすべての特性について説明します。

本書をお読みになる前に、以下のドキュメントの確認をお願いします。

- バージョンのリリース・ノート
- 既知の制限
- 解決済みの問題
- Check Point 730/750 Appliance 導入ガイド

R77.20.15 ホームページのを参照してください。
インストール

このセクションの内容
Check Point 730/750 Appliance のセットアップ .............................................................. 8
ケーブルの接続 ..................................................................................................................... 8

Check Point 730/750 Appliance のセットアップ

1. Check Point 730/750 Appliance を梱包された箱から取り出して卓上に置きます。
2. ネットワーク・インタフェース「LAN1」を確認します。このインタフェースは、IP アドレス 192.168.1.1 でありかじめ設定されています。

ケーブルの接続

1. 電源ユニットをアプライアンスに接続し、電源をコンセントに差し込みます。
   電源ユニットと電源出力がつながると、アプライアンスがオンになります。
   前面パネル（164ページ）にある電源 LED がオンになります。電源 LED が点灯すると、アプライアンスがオンになったことを表わします。
   その後、前面パネルの警告 LED が点滅し始めます。これは、アプライアンスが起動し始めていることを表わします。
   警告 LED ランプが消えたら、アプライアンスの準備が整い、ログインが可能になります。
2. 標準のネットワーク・ケーブルを、アプライアンスの LAN1 ポートと、お使いの PC のネットワーク・アダプタに接続します。
3. アプライアンスの WAN ポートと外部モデム、外部ルータ、またはネットワーク・ポイントを別の標準ネットワーク・ケーブルで接続します。
一般的な設定シナリオ

このセクションの内容

クラウド・サービスの設定........................................................................................................9
ゲスト・ネットワークの設定......................................................................................................10
VPNの設定..................................................................................................................................10
QoSの設定....................................................................................................................................14
クラスタの設定............................................................................................................................15
VoIPトラフィックを有効にする.....................................................................................................16

この章では、一般的な設定シナリオのワークフローについて説明します。
ワークフロー・ステップには、必要に応じて関連するアプライアンス設定セクションへのリンクが含まれます。

クラウド・サービスの設定

はじめに
クラウド・サービスでは、Check Point 730/750 ApplianceをWebベースのアプリケーションを使用するクラウド・サービス・プロバイダに接続して、アプライアンスを管理、設定、およびモニタリングできます。

事前準備
クラウド・サービスに接続する前に、以下を用意しておいてください。

- クラウド・サービス・プロバイダからのアクティベーション・リンクがある電子メールを受信します。このリンクをクリックするとCheck Point 730/750 Applianceが自動的にクラウド・サービスに接続します。
- サービス・センターのIPアドレス、Check Point 730/750 ApplianceゲートウェイID、登録キー。これらの詳細情報を使用してCheck Point 730/750 Applianceを手動でクラウド・サービスに接続します。

クラウド・サービスに自動的に接続するには
1. Check Point 730/750 Applianceが初期設定ウィザードによって設定済みであることを確認してください。「Check Point 730/750 Appliance導入ガイド」を参照してください。
2. セキュリティ・ゲートウェイ所有者がクラウド・サービス・プロバイダから受け取った電子メールのアクティベーション・リンクをクリックします。
   ログイン後、ウィンドウが開いてEメールで送られた有効化の詳細情報が表示されます。
3. 詳細情報が正しいことを確認して[接続]をクリックします。
   詳細については、「クラウド・サービスの設定」(21ページ)を参照してください。

クラウド・サービスに手動で接続するには
1. WebUIから[ホーム]→[クラウド・サービス]ページに移動します。
2. 「クラウド・サービスの設定」(21ページ)のクラウド・サービスへの接続手順に従います。
ゲスト・ネットワークの設定

一部の状況では、ゲストによる組織内からインターネットへのアクセスを許可する必要がある場合があり、一部の状況では、ゲストによる組織内からインターネットへのアクセスを許可する必要がある場合もあります。また、それと同時に内部ネットワーク・リソースへのアクセスを制限する必要がある場合もあります。ホットスポットでゲスト・ネットワークを設定するとネットワーク・アクセサをコントロールできるようになります。ユーザ認証オプションを設定すると、ネットワークに接続しているユーザを監視できます。

事前準備
- アプライアンスでワイヤレス・ネットワークが有効である必要があります。ゲスト・ネットワークは、実際には仮想アクセスポイント（VAP）です。
- インタフェースから閲覧を行うユーザをホットスポット・ポータルにリダイレクトするネットワーク・インタフェースを定義する必要があります。

設定
1. [デバイス] → [ワイヤレス・ネットワーク]に移動します。
2. [ゲスト]をクリックしてウィザードの指示に従います。「ワイヤレス・ネットワーク設定」（33ページ）を参照してください。
   a) ウィザードで[ホットスポットを使用]チェックボックスを選択します。
   b) ネットワーク保護を設定します（保護されていないネットワークまたは保護されたネットワーク）。
   c) [アクセス・ポリシー]タブでアクセスとログ・ポリシーのオプションを設定します。
3. このとき、ホットスポット用のネットワーク・インタフェースを定義するように注意してください。「ローカル・ネットワークの設定」（36ページ）を参照してください。
4. ホットスポットの設定 - [デバイス] → [ホットスポット]に移動します。「ホットスポットの設定」（41ページ）を参照してください。
5. アクセス・セクションで必要に応じて指定のユーザ・グループのホットスポットへのアクセスを制限できます。

モニタリング
ネットワークに接続してブラウザ・セッションを開きます。カスタマイズされたホットスポット・ポータルが表示されます。このホットスポット・ポータルは所定のタイムアウト時間中に1回表示されます。デフォルトのタイムアウト時間は4時間です。
ログ・トラフィック・オプションが選択されている場合、このネットワーク上のユーザ・アクティビティはユーザ名で記録されます。

VPN の設定
このセクションでは、これらのVPN設定シナリオの設定方法について説明します。
- リモート・アクセスVPN
- 事前共有秘密を使用するサイト間VPN
- 証明書を使用するサイト間VPN

リモート・アクセスVPN の設定

はじめに
リモート・アクセスには次のオプションを使用します。
Check Point VPN クライアント
Check Point モバイル・クライアント
Check Point SSL VPN
L2TP VPN クライアント

事前準備
- [VPN]→[ブレード・コントロール]で、以下の設定を確認します。
  - リモート・アクセス制御をオンに設定し、[リモート・アクセス・ユーザからのトラフィックを許可（デフォルト）]オプションを選択します。
  - 適切な接続方法を選択します。
  - 詳細については、「リモート・アクセス Blade の設定」（116ページ）を参照してください。
- ゲートウェイが動的 IP アドレスを使用している場合は、DDNS 機能の使用をお勧めします。「DDNS アカウント詳細の設定」（55ページ）を参照してください。
- Check Point VPN クライアントまたはモバイル・クライアント・メソッドでは、適切なクライアントをホストにインストールする必要があります。詳細については、「接続方法」をクリックしてください。

リモート・アクセス設定
リモート・アクセス・ユーザを設定するには3つの方法があります。
- ローカル・ユーザ
- RADIUS ユーザ
- AD ユーザ

特定のユーザにのみリモート・アクセス・プライアントへの接続を許可するには、適切なユーザ・タイプにグループ権限を設定します。[追加]オプションの横にある矢印を選択して、関連するグループ・オプションを選択します。「リモート・アクセス・ユーザの設定」（118ページ）を参照してください。

ローカル・ユーザを設定するには
1. 新規ユーザの場合
   a) [VPN]→[リモート・アクセス・ユーザ]に移動します。
   b) [追加]をクリックしてローカル・ユーザを追加します。
   c) [リモート・アクセス権限]チェックボックスが選択されていることを確認します。
   d) 詳細については、「リモート・アクセス・ユーザの設定」（118ページ）を参照してください。
2. 既存のユーザの場合
   a) [VPN]→[リモート・アクセス・ユーザ]に移動します。
   b) [編集]をクリックして[リモート・アクセス権限]チェックボックスを選択します。
   c) 詳細については、「リモート・アクセス・ユーザの設定」（118ページ）を参照してください。

RADIUS ユーザを設定するには
1. [VPN]→[認証サーバ]に移動します。
2. [設定]をクリックしてRADIUS サーバを追加します。「リモート・アクセス認証サーバの設定」（120ページ）を参照してください。
3. [RADIUS ユーザの権限]をクリックしてアクセス権限を設定します。
AD ユーザを設定するには

1. [VPN]→[認証サーバ]に移動して新規をクリックしてADドメインを追加します。「リモート・アクセス認証サーバの設定」(120ページ)を参照してください。
2. [Active Directory ユーザの権限]をクリックしてアクセス権限を設定します。

L2TP VPN クライアント設定

L2TP VPN クライアントを設定するには、[L2TP 事前共有キー]をクリックして L2TP VPN クライアントメソッドを有効にした後、キーを入力します。

詳細オプション

オフィス・モード・ネットワークなど詳細リモート・アクセス・オプションの詳細については、「詳細リモート・アクセス・オプションの設定」(123ページ)を参照してください。

モニタリング

リモート・アクセスを動作させるには

リモート・ホストから内部リソースに接続するには、設定済みのクライアントを使用します。

共有秘密を用いるサイト間 VPN の設定

はじめに

このサイト間 VPN 設定メソッドでは、認証に共有秘密を使用します

事前準備

- サイト間 VPN のブレードがオンに設定され、[リモート/サイトからのトラフィックを許可 (デフォルト)]が選択されていることを確認します。「サイト間 VPN のブレードの設定」(125ページ)を参照してください。
- 接続するピア・デバイスは設定済みでネットワークに接続されている必要があります。DAIP ゲートウェイの場合、ホスト名を解決する必要があります。

設定

ホスト名と IP アドレスを入力し、事前共有秘密情報を入力します。詳細については、「VPN サイトの設定」(126ページ)を参照してください。

モニタリング

VPN を動作させるには

1. ローカルおよびピア・ゲートウェイ間でトラフィックを送信します。
2. [VPN]→[VPNトンネル]に移動してトンネル・ステータスをモニタリングします。「VPN トンネルの表示」(129ページ)を参照してください。

証明書を用いるサイト間 VPN の設定

はじめに

このサイト間 VPN 設定メソッドでは、認証に証明書を使用します。
事前準備

- サイト間 VPN のブレードがオンに設定され、[リモート/サイトからのトラフィックを許可 (デフォルト)] が選択されていることを確認します。「サイト間 VPN のブレードの設定」 (125 ページ) を参照してください。

- 接続するピア・デバイスは設定済みでネットワークに接続されている必要があります。DAIP ゲートウェイの場合 は、ホスト名を解決する必要があります。

- ご使用の IP アドレスを使って証明書を再初期化するか、またはホスト名を解決します。証明書が双方から信頼されていることを確認します。

- VPN 暗号化設定は双方（ローカル・ゲートウェイとピア・ゲートウェイ）で同一である必要があります。これはスタム暗号化オプションを使用する場合には特に重要となります。

設定

1. 証明書の再初期化 - 「内部証明書の管理」 (133 ページ) に記載の [証明書の再初期化] オプションを使用します。これはローカル・ゲートウェイとピア・ゲートウェイの両方で行う必要があります（両方ともローカルに管理された Check Point アプライアンスを使用する場合）。

2. ローカル・ゲートウェイとピア・ゲートウェイの両方で CA を信頼します - 次の手順のいずれかを実行します。
   - ゲートウェイ間で CA を交換する
   - ゲートウェイの CA のひとつを使用してリクエストに署名する
   - サードパーティ CA を使用して認証する
   - 既存のサードパーティ証明書を使用して認証する

以下の信頼手続きセクションに記載の適切な手続きの手順に従います。

3. 証明書認証を使用して VPN サイトを作成します。
   a) 「VPN サイトの設定」 (126 ページ) の指示に従います。
   b) 指定の証明書を使用するように注意してください。 [詳細] → [証明書の照合] にピア・ゲートウェイの証明書情報を入力します。

信頼手続き

ゲートウェイ間で CA を交換する

ゲートウェイの CA のひとつを使用してリクエストに署名する

ピア・ゲートウェイの CA により署名されたゲートウェイからリクエストを作成します。

1. 「インストール済み証明書の管理」 (132 ページ) の [新しい署名リクエスト] オプションを使用します。
2. [エクスポート] オプションを使用してこのリクエストをエクスポートします。
3. 詳細については、「信頼済み CA の管理」 (131 ページ) を参照してください。
4. 署名したリクエストをローカル・ゲートウェイにアップロードします。
   a) [VPN] → [インストール済み証明書] ページに移動します。
   b) リモート・ピアに署名を要求したインストール済み証明書を選択します。
   c) [署名済み証明書のアップロード] オプションを使用して証明書をアップロードします。「インストール済み証明書の管理」 (132 ページ) を参照してください。
5. CA が両方のゲートウェイにインストールされていることを確認してください。 [信頼済み CA の管理] (131 ページ) の [追加] オプションを使用します。
サードパーティーCAを使用して認証する

1. 適切なアップロード・オプションを使用して証明書をアップロードします。
   a) [VPN]→[インストール済み証明書]ページに移動します。
   b) リモート・ピアに署名を要求したインストール済み証明書を選択します。
   c) [署名済み証明書のアップロード]または[P12証明書のアップロード]オプションを使って証明書をアップロードします。「インストール済み証明書の管理」(132ページ)を参照してください。

2. サードパーティーCAが両方のゲートウェイにインストールされていることを確認します。[信頼済みCAの管理](131ページ)の[追加]オプションを使用します。

既存のサードパーティー証明書を使用して認証する

1. ローカル・ゲートウェイとピア・ゲートウェイにP12証明書を作成します。
2. 各ゲートウェイの[P12証明書のアップロード]を使用してP12証明書をアップロードします。
3. サードパーティーCAが両方のゲートウェイにインストールされていることを確認します。[信頼済みCAの管理](131ページ)の[追加]オプションを使用します。

モニタリング

VPNを動作させるには

1. ローカル・ゲートウェイとピア・ゲートウェイ間にトラフィックを通します。
2. [VPN]→[VPNトンネル]に移動してトンネル・ステータスをモニタリングします。「VPNトンネルの表示」(129ページ)を参照してください。

QoSの設定

はじめに

QoS（帯域幅制御）ポリシーは、ネットワークを行き来するトラフィックの流れを制御する帯域幅パラメータを設定するための一連のルールです。これによりネットワークが混雑したときに重要なトラフィックを優先して、ビジネスの混雑を最小限に抑えることができます。

QoSはインターネット接続で作動します。したがって、最大ダウンロード/アップロード速度を設定するインターネット接続が少なくともひとつ必要です。速度情報はご利用のISPから入手できます。

QoSポリシー・ルールは設定されたインターネット接続ごとに個別に適用されます。

事前準備

[アクセス・ポリシー]→[QoS]→[ブレード・コントロール]ページからQoS Bladeをオンにします。

設定

1. [デバイス]→[インターネット]で、インターネット接続を選択して[編集]をクリックします。
2. [詳細]タブで[QoS設定]を編集します。
   これらの値は、QoSウェイトを計算するときの100％ベースラインとして使用されます。詳細については、「インターネット接続の設定」(30ページ)を参照してください。
3. 以下のオプションを使用できます。
   - いくつかのパラメータのみを定義するデフォルトのQoSポリシー「サービスの品質の設定」(94ページ)を参照してください。
クラスの設定

はじめに

2つのアプライアンスをクラス構成に設定することで高い可用性が実現します。ハイ・アベイラビリティでは、クラスメンバのひとつが故障しても組織のネットワークの接続が維持されます。ゲートウェイは1つだけアクティブになります。フェイルオーバーが発生すると、スタンバイ・メンバがアクティブになります。
サポートされるのはクラスタ・ハイ・アベイラビリティのみです。クラスタのメンバ間での負荷分散はありません。

事前準備

- クラスタ構成では、ブリッジおよびスイッチ構成はサポートされません。それらをクラス構成する前に([WebUI]→[デバイス]→[ローカル・ネットワーク]ページ)で削除する必要があります。
- クラスタ・メンバとして使用するために指定されるアプライアンスは、両方とも同じハードウェア、ファームウェア、およびライセンスを持つ必要があります。
- さらに同期インタフェースには同じLANポートを指定することをお勧めします。デフォルトの同期インタフェースはLAN2/SYNCです。

注 - Syncケーブルは、初期設定ウィザードが完了し両方のアプライアンスからスイッチが除去された後に接続してください。両方のメンバ共に追加の設定は必要ありません。

設定

1. 両方のアプライアンスの初期設定ウィザードを完了します。ステップ5(ウィザードのローカル・ネットワーク・ページ)で、[LANポートのスイッチを有効にする]チェックボックスの選択を解除します。この操作を忘れた場合は、[WebUI]→[デバイス]→[ローカル・ネットワーク]ページでスイッチを削除できます。
2. プライマリ・メンバにするアプライアンスでネットワーク設定を行います。
3. アプライアンス間を同期ケーブルで接続します。
4. プライマリ・クラスタ・メンバ:
   a) プライマリ・クラスタ・メンバにするアプライアンスを接続します。
   b) WebUIで、[デバイス]→[ハイ・アベイラビリティ]ページに移動し[クラスタの設定]をクリックします。
   c) プライマリ・メンバ・オプションのウィザード・ステップを実行します。詳細については、「ハイ・アベイラビリティの設定」(58ページ)を参照してください。
5. セカンダリ・クラスタ・メンバ:
   a) セカンダリ・クラスタ・メンバにするアプライアンスを接続します。
   b) [デバイス]→[ハイ・アベイラビリティ]ページに移動して[クラスタの設定]をクリックします。
   c) セカンダリ・メンバ・オプションのウィザード・ステップを実行します。詳細については、「ハイ・アベイラビリティの設定」(58ページ)を参照してください。
6. アクセス・ポリシー、VPN、脅威対策パラメータなど必要なその他の設定を完了します。これによりアクティブ・メンバが設定され、スタンバイ・メンバに同期されます。フェイルオーバーが発生すると、スタンバイ・メンバがアクティブ・メンバになります。
モニタリング
クラスタの設定が正常に完了した後に、my.firewallに接続することをお勧めします。my.firewallは接続をアクティブ・クラスタ・メンバにリダイレクトします。

https://<IP>:4434に移動して各アプライアンスにログインします。ただし、<IP>は指定のメンバのIPアドレスです。
スタンバイ・クラスタ・メンバのWebUIには、ひとつのタブ（デバイス・タブ）しかありません。デバイスアクティブ・メンバを通じてすべてのクラスタ設定が完了しても一部のオプションは利用できません。
WebUIの[デバイス]→[ハイ・アベイラビリティ]ページに各メンバのステータスが表示されます。

VoIPトラフィックを有効にする

はじめに
この設定手続きに従うことにより、次の場合にSIPトラフィックがゲートウェイを通過できるようになります。
- サーバが外部ネットワークにある場合
- ゲートウェイのNAT設定がデフォルトに設定されている（内部ネットワークがその外部IPアドレスに隠れている）場合

設定
アプリケーション・レベルの検査およびSIPプロトコルのNATを許可するには
1. [ユーザ&オブジェクト]→[サービス]ページに移動します。
2. 両方のサービスのSIP検査を有効にして、サービスのSIP_UDPおよびSIP_TCPビルドを編集します。各サービス・オブジェクトの[このサービスのインスペクションを無効にする]チェックボックスの選択を解除します。詳細については、「システム・サービスの管理」（140ページ）を参照してください。

SIPサーバがインターネットから内部電話にアクセスできるようにするには
1. [アクセス・ポリシー]→[ポリシー]ページへ移動します。
2. [着信、内部およびVPNトラフィック]ルール・ベースに、SIPトラフィックを許可するルールを追加します。例えば、次のように入力します。
   ソース - Any
   宛先 - Any
   サービス - SIP
   アクション - 許可
   詳細については、「ファイアウォール・アクセス・ポリシーとの連携」（84ページ）を参照してください。
3. SIPサーバのIPアドレスが分かっている場合は、それをこのルールのソースとして使用できます。
4. オプション: このルールのログを設定します。
アプライアンスの設定

このセクションの内容

WebUI アプリケーションの概要 ................................................................. 18
ホーム・タブ ........................................................................ 19
デバイスの管理 ........................................................................ 30
アクセス・ポリシーの管理 .......................................................... 80
脅威対策の管理 ........................................................................ 103
VPN の管理 ................................................................................ 116
ユーザおよびオブジェクトの管理 .................................................. 135
ログとモニタリング ...................................................................... 147

この章では特別な Check Point 730/750 Appliance 機能について説明します。
WebUI アプリケーションの概要

Check Point 730/750 Appliance では、アプライアンスの設定に Web アプリケーションを使用します。

初期設定ウィザードの使用後（『Check Point 730/750 Appliance 導入ガイド』参照）、ブラウザで（アプライアンスのIPを使用して、またはアプライアンスをDNSプロキシまたはDHCPサーバとして使用している場合は"my.firewall"で）アプライアンスに接続すると、Webページが安全なhttpsサイトにリダイレクトされ管理者認証情報が要求されます。ログイン時に[ユーザ名を保存]チェックボックスを選択すると管理者のユーザ名を保存できます。この名前はブラウザのcookieがクリアされるまで維持されます。

左ペインで以下の各タブのページ間を移動できます。

- ホーム
- デバイス
- アクセス・ポリシー
- 脅威対策
- VPN
- ユーザ&オブジェクト
- ログ&モニタリング

別の言語でWebUIにログインするには

ログイン・ウィンドウが表示されているブラウザ・ページで、ページ下部にある言語リンクから必要な言語を選択してください。

直ちにログイン・ページが選択した言語に変更されます。同じコンピュータで次にログインするときは選択した言語が使用されます（ブラウザcookieに保存）。この言語はブラウザのcookieがクリアされるまで維持されます。

注 - ユーザのロケールとローカライズされたWebUIが一致する場合、ログイン・ウィンドウは自動的に指定の言語をロードします。入力言語は英語のみサポートされます。
ホーム・タブ

システム情報の確認

[ホーム]→[システム]ページには、Check Point 730/750 Appliance の概要が表示されます。

Check Point Check Point 730/750 Appliance でユーザによる設定が必要なのは、IP アドレスやルーティング情報、Software Blade 設定などごく少数の基本項目だけでです。Check Point 730/750 Appliance の初期設定は、初期設定ウィザードで行うことができます。初期設定の完了後は、http://my.firewall からログインするたびに、WebUI の[ホーム]→[システム]ページが表示されます。

・[システム情報] - アプライアンスのモデル、インストールされているソフトウェアのバージョン、名前、MAC アドレス、システム時刻（GMT）、システムの起動時間が表示されます。
・[ネットワーク] - インターネット情報とダイヤル・アップ接続のステータスが表示されます。各リンクをクリックすると、必要な設定が確認できます。
・[統計] - パッケージ・レートやルート・ネットワークなど実際のデータに基づくグラフが表示されます。

Software Blade の制御とモニタリング

[ホーム]→[セキュリティ・ダッシュボード]ページには、有効にされている Software Blade が表示され、ここから各 Software Blade の設定ページに直接移動できます。

また以下の操作を行うことができます。

・[設定]ボタン（歯車のアイコン）をクリックすると、各 Software Blade の基本設定にアクセスし、Software Blade を有効にすることができます。
・各 Software Blade の統計にアクセスできます（グラフのアイコン）。
・ライセンスが適用されていない Software Blade、最新の状態でない Software Blade、追加設定が必要な Software Blade（サイト間 VPN など）に関する警告を確認できます。これらの設定を有効にする場合、その Software Blade のアイコンの右上隅に三角形が表示されます。

このページでは、Software Blade は以下の 3 つのグループに分類されています。この分類は、WebUI での設定場所に基づいています。

・【アクセス・ポリシー】 - Firewall、Applications & URL Filtering、User Awareness、QoS の各 Software Blade が表示されます。
・【脅威対策】 - Intrusion Prevention（IPS）、Anti-Virus、アンチポット、Anti-Spam の各 Software Blade が表示されます。
・【VPN】 - Remote Access と Site to Site VPN の各 Software Blade が表示されます。ここには証明書に関するオプションも表示されます。

タブ名のリンクまたは Software Blade のリンクをクリックすると、詳細設定を行うためのタブにアクセスできます。

Software Blade を有効/無効にするには

注 - クラウド・サービスで管理されているSoftware Bladeには鍵のアイコンが表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。

設定情報を表示または編集するには
1. オン/オフ・スイッチの隣にある歯車のアイコンをクリックします。
   Software Bladeの設定ウィンドウが表示されます。
2. 詳細を確認します。現在の設定を変更する場合は適切なオプションを選択します。
3. [適用]をクリックします。

統計を表示するには
1. 棒グラフのアイコンをクリックします。
   Software Bladeの統計ウィンドウが表示されます。
2. Software Bladeが有効である場合
   a) グラフと詳細を確認します。
   b) 他のSoftware Bladeの統計を確認するには、ヘッダの矢印をクリックします。
3. Software Bladeが無効になっている場合
   a) [デモの表示]をクリックすると、統計の例を表示できます。
   b) デモを終了するにはXのアイコンをクリックします。

警告を表示するには
1. 警告を示す三角形にカーソルを合わせます。
2.
クラウド・サービスの設定

ホーム]→[クラウド管理]ページでは、Check Point 730/750 Applianceをクラウド・サービスに接続します。クラウド・サービス・プロバイダはWebベースのアプリケーションを使ってCheck Point 730/750 Applianceを管理、設定、モニタリングします。

Check Point 730/750 Applianceをクラウド・サービスに接続する方法は、以下のいずれかです。

- セキュリティ・ゲートウェイの所有者がクラウド・サービス・プロバイダから受信するEメールにある、有効化するリンクをクリックします。ログイン後、ウィンドウを開いてEメールで送られた有効化の詳細情報を表示されます。情報が正しいことを確認し、[接続]をクリックします。アプリケーションが別のクラウド・サービス・プロバイダに接続している場合は、そのまま続行するかどうか確認メッセージが表示されます。
- ページに入力して下の接続手順に従います。

接続すると、セキュリティ・ポリシーとその他の設定がアプリケーションにプッシュされます。クラウド・サービスで定義された設定には、有効になったブレード、セキュリティ・ポリシー、サービスの各設定が含まれます。

クラウド・サービスをオンにすると、これらの識別詳細情報がWebUIに表示されます。

- ログインページの下部 - クラウド・サービス・プロバイダで定義されたセキュリティ・ゲートウェイの名前とCheck Point 730/750 ApplianceのMACアドレス。
- WebUIアプリケーションの上部（検索ボックスの近く）- Check Point 730/750 Applianceの名前。

このページには3つのセクションがあります。

- クラウド・サービス - クラウド・サービスの詳細が表示されます。
  - 設定オプションで、初期の接続を設定できます。
  - 接続している状態で[詳細]をクリックすると接続の詳細が表示され、[互換性]と接続すると有効化したブレード、セキュリティ・ポリシー、サービス設定がクラウドと同期されます。
  - 接続が切断された場合は、[更新]をクリックしてクラウド・サービスと再接続を試みることができます。

- Managed Security Blades - 定義された各ブレードがカラーやまたはモノクロで表示されます。アイコンのテキストをクリックして、該当ページをWebUIで開くことができます。
  - カラー・アイコン - クラウド・サービスでリモート管理されているブレードです。カラーで表示されるブレードはオンになっています。
    オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。
  - グレー・アイコン - クラウド・サービスでリモート管理されているブレードです。グレーで表示されるブレードはオフになっています。
  - 非表示アイコン - Check Point 730/750 Appliance上でローカル管理されているブレードです。このブレードはクラウド・サービスで管理されていません。

どのブレードもリモート管理されていない場合は、すべてのブレードのアイコンはグレー表示されます。

- 利用可能なサービス - クラウド・サービス・プロバイダで管理されるサービスが表示されます。サービスに[設定]ボタンがある場合は、クリックして読み取り専用の設定情報を確認できます。設定情報は変更できません。グレー表示されているサービスは、クラウド・サービスから提供されていないサービスです。

利用可能なサービスは以下のとおりです。
アプライアンスの設定

- レポート - ネットワークとセキュリティのレポートが定期的にEメールで送られます。 [設定]をクリックすると、ゲートウェイに設定されたレポートの間隔を確認できます。
- ログ - ログはクラウド・サービス・プロバイダに格納されます。
- ダイナミックDNS - クラウド・サービスで設定された永続的なドメイン名。
- ファームウェア・アップグレード - ファームウェアのアップグレードはクラウド・サービスでリモート管理されます。
- 定期的バックアップ - アップはクラウド・サービスでスケジュールされます。

クラウド・サービスに接続する前に、以下を用意してください。

- クラウド・サービス・プロバイダから受信したEメール。Check Point 730/750 Appliance の有効化キーと有効にするリンクが記載されています。

または

- サービス・センターのIPアドレス、Check Point 730/750 Appliance ゲートウェイID、登録キー。

クラウド・サービスへの接続は、以下の手順を実行します。

1. ゲートウェイ登録情報が正しいことを確認する
2. セキュリティ・ポリシーと各設定を取得する
3. セキュリティ・ポリシーと各設定を取得する

初めて接続する場合は、クラウド・サービス・プロバイダの証明書をトラスト認証局で検証する必要があります。検証が失敗すると、通知メッセージが表示されます。検証メッセージは停止/無視してそのまま続行することができます。

クラウド・サービス・プロバイダへ接続するには

2. [有効化キー]または[有効化の詳細]を選択して指定の情報を入力します。
3. [適用]をクリックします。 Check Point 730/750 Appliance からクラウド・サービス・プロバイダに接続を開始します。クラウド・サービスセクションに、進捗状況のインジケータと接続のステップが表示されます。
4. クラウド・サービス・プロバイダの識別情報が正しいにも関わらず、識別されないというメッセージが表示された場合は、[解決]をクリックして[無視して再接続]をクリックします。

接続が成功すると、ページの上部にあるクラウド・サービスセクションに以下の情報が表示されます。

- 同期した日付
- クラウド・サービスの状態を表わす[オン] [オフ]レバー
- クラウド・サービス・サーバウィジェットがステータスバーに表示され、「接続」状態になります。このウィジェットをクリックするとクラウド・サービスページを開くことができます。

注 - クラウド・サービスへの接続をテストするには、コンソールの接続を開いてログインし、以下のCLIコマンドを入力します。

```
test cloud-connectivity
```
ライセンスの管理

[ホーム]→[ライセンス]ページには、各 Software Blade のライセンスの状態が表示されます。このページでは、アプライアンスから、認証情報を用いて Check Point のユーザ・センターに接続し、ライセンス情報を確認したり、アプライアンスを有効にしたりできます。

通常は、初めてチェック・ポイントのユーザ・センター・アカウントでアプライアンスを登録する必要があり、ユーザ・センターのアカウントがない場合は、サポートやアップデートを受け取るためにも、新しく作成する必要があります。

インターネット接続が設定されている場合:
1. [ホーム]→[ライセンス]に移動します。
2. [ライセンスの有効化]をクリックします。

アプライアンスが有効になったことが通知されます。

ライセンスを有効にできない場合は、以下の原因が考えられます。
- アプライアンスとインターネット間のプロキシなどの接続問題がある。
- アプライアンスとインターネットを接続していない場合
- アプライアンスが登録されていない。

アプライアンスとインターネット間でプロキシがある場合、ライセンスをアクティブにする前にプロキシの詳細を設定する必要があります。

プロキシの詳細を設定するには
1. [プロキシの設定]をクリックします。
2. [プロキシを設定する]を選択し、プロキシのアドレスとポートを入力します。
3. [適用]ボタンをクリックします。
4. [ライセンスの有効化]をクリックします。

アプライアンスが登録されていない場合
2. 以下のフィールドに入力します。
   - MAC アドレス
   - 登録キー
   -これらの情報は[ホーム]→[ライセンス]にあります。
3. [ハードウェア・プラットフォーム]をクリックします。
4. [ハードウェア・モデル]で、[Check Point 730/750 Appliance]を選択します。
5. [ライセンスの有効化]をクリックします。

アプライアンスが有効になったことが通知されます。

有効にした後は、[ライセンスの有効化]ボタンが[再有効化]になります。ライセンスに変更があった場合は、[再有効化]をクリックして最新のライセンス情報を取得してください。

オフライン状態でアプライアンスを設定している場合:
1. https://usercenter.checkpoint.com（http://usercenter.checkpoint.com）へアクセスし、必要な情報を入力します。入力が必要な情報は、アプライアンスの認証情報、MAC アドレス、登録キーです。これらの情報は[ホーム]→[ライセンス]にあります。
2. 登録のウィザードが完了すると、アクティベーション・ファイルをダウンロードするようにメッセージが表示されます。ローカルにファイルをダウンロードします。次のステップに進む前に必ずダウンロードしてください。
3. [ホーム]→[ライセンス]ページで[オフライン]をクリックします。
   [有効化ファイルのインポート]ウィンドウが開きます。
4. ダウンロードしたアクティベーション・ファイルを探して、[インポート]をクリックします。
   有効化プロセスが始まります。

サイト・マップの表示
[ホーム]→[サイト・マップ]ページには、WebUI のサイト・マップが表示されます。このページには、WebUI を構成するすべてのタブとページが表示されます。
このページに表示されているリンクから、任意のページに直接移動できます。

内部ネットワーク内のアクティブ・コンピュータの管理
[アクティビナコンピュータ]ページには、内部ネットワークで確認されたデバイスのリストが表示されます。
情報には次のものが含まれます。
- オブジェクト名
- IP/MAC アドレス
- デバイス/ユーザ名 - DHCP またはユーザ認識により Check Point 730/750 Appliance が情報を確認できた場合、デバイス/ユーザ名が表示されます。
- サービス - 着信および発信サービスが表示されます。着信サービスは主にサーバを示します。
- ゾーン - アプライアンスがケーブルで接続されているかワイヤレスで接続されているかが示されます。
- トラフィック - トラフィックのモニタリングが有効な場合、アップロードおよびダウンロードのパケット・レートが表示されます。
以下の操作ができます。
- [名前を付けて保存] - 選択したデバイスをネットワーク・オブジェクトまたはサーバとして保存します。このオプションを選択すると、[新しいネットワーク・オブジェクト]ウィンドウまたは新しいサーバ・ウィンドウが開きます。各フィールドに必要な情報を入力して、[適用]をクリックします。これらのオブジェクトを使用すると、DHCP サーバで IP アドレスを MAC アドレスに予約したり、オブジェクト名をホストとしてローカル DNS サービスに追加したりできます。ネットワーク・オブジェクトとサーバ・オブジェクトは、アクセス・ポリシーや IPS の例外などのセキュリティ設定に使用できます。
また可能な場合には、サーバ・オブジェクトの一部としてアクセスや NAT を設定することもできます。
- [絞り込み] - サーバ、アクティブなデバイス、既知のデバイスに基づいてリストをフィルタリングします。
- [詳細] - リストで行を選択して[詳細]をクリックすると、デバイスの追加プロパティが表示されます。
- [更新] - リストの情報を更新します。
- [トラフィック・モニタリングの開始/停止] - アクティブなコンピュータのアップロードおよびダウンロードのパケット・レートを収集します。この情報は、表に追加表示される[トラフィック]カラムに表示されます。
この操作はパフォーマンスに影響を与える場合があります。モニタリングを停止するには、[トラフィック・モニタリングの停止]をクリックします。

注 - このページには、[ホーム]および[ログ&モニタリング]タブからアクセスできます。
モニタリング・データの表示

[モニタリング] ページには、ネットワーク、セキュリティ、トラブルシューティング情報が表示されます。このページにアクセスするごとに、データは更新されます。[更新]をクリックして情報をアップデートできます。

モニタリング・レポートのサンプルを見る場合は[デモ]をクリックします。サンプル・レポートを閉じるには[戻る]をクリックします。

システムの現在の接続数は[VPN トンネル]、[アクティブなコンピュータ]、[接続]に表示されます。リンクをクリックして WebUI ページを開くことができます。

[モニタリング] ページは、次のセクションに分かれています。

- ネットワーク
- セキュリティ
- トラブルシューティング

各セクションのタイトル・バーにある矢印アイコンをクリックして、セクションを展開したり折り畳んだりすることができます。

ネットワーク

デフォルトでは過去 1 時間のネットワーク統計が表示されます。過去 1 日の統計も確認できます。ネットワーク・セクションのタイトル・バーから[過去 1 時間]または[過去 24 時間]を選択します。

データは指定時間ごとに自動的に更新されます。
過去 1 時間の場合、1 分毎の間隔で処理されます。たとえば、10:15:45 AM にレポートを生成した場合、レポートの内容は 9:15 から 10:15 AM のデータになります。
過去 24 時間の場合、1 時間毎に処理されます。たとえば、10:15 AM にレポートを生成した場合、レポートの内容はその日の 10:00 AM から 24 時間前まで遡った 24 時間分のデータになります。

- 帯域幅の使用量 - 円グラフに、指定期間（過去 1 時間/過去 24 時間）で最も帯域を消費したトップ 10 のアプリケーション/ユーザが表示されます。[アプリケーション]または[ユーザ]リンクをクリックして統計を切り替えます。ユーザ情報を確認するには、ユーザ認識ブレードを有効にする必要があります。

- 帯域消費の上位ランク - 帯域消費の上位アプリケーション、カテゴリ、サイト、ユーザのパーセンテージとトラフィック量（MB/GB）の統計が表示されます。

- トラフィック - デフォルトでは、領域グラフで受信および送信したトラフィックの合計量が表示されます。時間軸は、ネットワーク・セクションで選択した期間（過去 1 時間または過去 1 日）を反映します。過去 1 時間の場合グラフには 5 分間隔で表示され、過去 24 時間の場合は 1 時間間隔で表示されます。受信と送信の各リンクをクリックして、受信または送信のトラフィック量だけを確認できます。グラフのオレンジ色の領域は送信トラフィックを表わします。青色の領域は受信トラフィックを表わします。時間間隔の上をポイントすると、ポップアップ・ボックスが表示されます。
  - 日付と時刻
  - 送信または受信トラフィック
  - 時間間隔の合計トラフィック

- 合計トラフィック統計 - 領域グラフの隣に過去 1 時間または過去 1 日の合計トラフィックの統計を確認できます。

セキュリティ

- 感染ホスト - 以下の数が表示されます。
  - 感染ホスト
アプライアンスの設定

- 感染サーバ
- 最近アクティブな感染ホスト
[すべての感染ホスト]をクリックして、[ログ&モニタリング]→[感染ホスト]ページを開くことができます。

- 高リスク・アプリケーション - 以下が表示されます。
  - 高リスク・アプリケーションの数
  - 使用頻度が最も高い高リスク・アプリケーション
  - 高リスク・アプリケーションを使用する上位ユーザ
[アプリケーション・ブレード・コントロール]をクリックして、[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページでアプリケーションと URL サイレントの設定を確認できます。

- セキュリティ・イベント - 以下の数が表示されます。
  - セキュリティ・ゲートウェイで検出されたアンチボット・マルウェア
  - セキュリティ・ゲートウェイで検出されたアンチウイルスマルウェア
  - IPS の数
リンクをクリックして[脅威対策]→[ブレード・コントロール]ページを開くことができます。

トラブルシューティング

- システムのリソース - [CPU、メモリ、ディスク使用量]をクリックして CPU、メモリ、ディスク使用量の情報を確認します。

- デバイス情報 - セキュリティ・ゲートウェイ情報が表示されます。

- モニタリングおよびトラブルシューティングに役立つページへのリンク

注 - このページには、[ホーム]および[ログ&モニタリング]タブからアクセスできます。

レポートの表示

[レポート]ページには、ネットワーク分析、セキュリティ分析、感染ホスト・レポートが指定した期間（毎月、毎週、毎日、每時間）ごとに表示されます。

レポートには、表示される時間に関係する重要な 2 つの要素があります。

- 時間の丸め処理
- システムの再起動

時間の丸め処理

生成レポートに表示される時間は丸め処理されます。

- レポート（毎時）の場合 - 1 分毎の間隔で処理されます。たとえば、10:15:45 AM にレポートを生成した場合、レポートの内容は 9:15 から 10:15 AM のデータになります。

- レポート（毎日）の場合 - 1 時間毎の間隔で処理されます。たとえば、10:15 AM にレポートを生成した場合、レポートの内容はその日の 10:00 AM から 24 時間前まで遡った 24 時間分のデータになります。

- レポート（毎週）の場合 - 2 時間毎の間隔で、00:00、02:00、04:00、06:00 といった偶数間隔で処理されます。たとえば、9:55 AM にレポートを生成した場合、レポートの内容はその日の 8:00 AM から 1 週間遡った 1 週間分のデータになります。
レポート（毎月）の場合 - 4 時間毎の間隔で、00:00、4:00、8:00、12:00といった偶数間隔で処理されます。たとえば、11:15 AM にレポートを生成した場合、レポートの内容はその日の 8:00 AM から 1か月間遡った 1か月分のデータになります。

システムの再起動
アプライアンスの起動後（インストール後/アップデート後）最初の 24 時間は、次回のレポート生成までの時間にもう一回分の間隔がシステムで追加されます。
たとえば、対の時間間隔でレポート（毎週）を生成する場合、アプライアンスでは追加の 2 時間と、更に最初の対時間のデルタ（差分）が必要になります。

- 00:00 AM に起動したアプライアンスの場合 - 最初のレポート（毎週）は 04:00 AM に生成されます。合計の 4 時間は、最初の対時間のデルタ時間である 02:00 に、追加の 2 時間を足した時間です。待ち時間は 4 時間です。
- 01:59 AM に起動したアプライアンスの場合 - 最初のレポート（毎週）は 04:00 AM に生成されます。合計の 2 時間は、最初の対時間のデルタ時間である 02:00 に、追加の 2 時間を足した時間です。待ち時間は 2 時間です。

レポートを生成するには
ページの上部にある該当する期間のリンクをクリックします（「毎月」「毎週」「毎日」「毎時」）。
リンクの下の行には、選択したレポートとその時間間隔が表示されます。表示データを更新するには、[生成]をクリックします。
レポートには以下のセクションがあります。
- サマリ
- 目次
- レポート・ページ

サマリ
レポートの最初のページにはサマリと以下が表示されます。
- セキュリティ・ゲートウェイで検出されたアンチボットとアンチウイルスのマルウェア数と IPS 攻撃の数。
- カテゴリ、サイト、ユーザ別の帯域幅上位使用率の統計。上位ランク・カテゴリー、上位ランク・サイト、上位ランク・ユーザの各リンクをクリックして該当するレポートのページを表示できます。上位 5 つのアプリケーション（円グラフ）と、受信および送信トрафィックの合計のアプリケーション別の帯域消費統計も表示されます。
- 感染ホスト、サーバ、最近アクティブな感染ホストの数。
- 高リスク・アプリケーションの数、使用頻度が最も多い高リスク・アプリケーション、高リスク・アプリケーションを使用する上位ユーザ。
- セキュリティ・ゲートウェイ名、バージョン、MAC アドレス。
目次

目次には、ネットワーク分析、セキュリティ分析、感染ホストの各レポートへのリンクがあります。リンクをクリックすると、選択したセクションへ直接移動できます。

レポート・ページ

各レポート・ページには、詳細グラフと表、説明があります。

注 - このページには、[ホーム]および[ログ&モニタリング]タブからアクセスできます。

システム・ツールの使用

[ツール]ページでは以下を行うことができます。

- システム・リソースのモニタリング
- ルーティング・テーブルの表示
- CPInfoファイルの生成
- IPアドレスのPingまたはトレース
- DNSルックアップの実行
- パケットのキャプチャ

システムのリソースをモニタリングするには

1. [システムリソースのモニタリング]をクリックします。[システムのリソース]ページが開き、以下の情報が表示されます。
   - [CPU使用履歴](自動的に更新されます)
   - [メモリ使用履歴] - メモリの計算は、トラフィック処理のために事前割り当てられたメモリとキャッシュ・メモリを除外して行われます。このため、アプライアンスにおける実際のメモリ使用状況を正確に把握できますが、Linuxツールによる計算とは数値が異なる場合があります。情報は自動的に更新されます。
   - [ディスク使用量] - 最新のディスク使用状況を表示するには、[更新]ボタンをクリックします。
2. [閉じる]をクリックすると、[ツール]ページに戻ります。

ルーティング・テーブルを表示するには

1. [ルーティング・テーブルの表示]をクリックします。出力が[コマンド出力]ウィンドウに表示されます。
2. [閉じる]をクリックすると、[ツール]ページに戻ります。

CPInfoファイルを生成するには

1. [CPInfoファイルの生成]をクリックします。進捗状況を示すメッセージがボタンの隣に表示されます。
2. [CPInfoファイルのダウンロード]をクリックして、CPInfoファイルを表示するか保存します。

IPアドレスのpingまたはトレースを実行するには

1. [ホスト名/IPアドレス]フィールドにホスト名またはIPアドレスを入力します。
2. [Ping]または[トレース・ルート]をクリックします。出力が[コマンド出力]ウィンドウに表示されます。
3. [閉じる]をクリックすると、[ツール]ページに戻ります。
DNS ルックアップを実行するには
1. [ホスト名/IP アドレス]フィールドにホスト名または IP アドレスを入力します。
2. [ルックアップ]をクリックします。出力が[コマンド出力]ウィンドウに表示されます。
3. [閉じる]をクリックすると、[ツール]ページに戻ります。

パケットをキャプチャするには

パケット・キャプチャ・ファイルがすでに存在する場合はそのファイルの日付が表示され、ファイルをダウンロードできます。パケット・キャプチャを新たに開始すると、既存のパケット・キャプチャ・ファイルは上書きされます。
1. ネットワークの選択リストからオプションを選択します。
2. [開始]をクリックしてパケット・キャプチャを開始し、停止する場合は[停止]をクリックします。
3. [ファイルのダウンロード]をクリックして、キャプチャ・ファイルを表示するか保存します。

パケット・キャプチャを開始した後、WebUI アプリケーションの別のページに移動しても、パケット・キャプチャはバックグラウンドで続行されます。ただし、WebUI セッションを終了するとパケット・キャプチャは自動的に停止します。WebUI セッションを終了する前にパケット・キャプチャ・ページに戻り、パケット・キャプチャを停止して結果をダウンロードしてください。

注 - キャプチャ・ユーティリティは tcpdump を使用します。「fw monitor」は、コマンドライン・インタフェースで使用できます。

このページには、[ホーム]タブ、[デバイス]タブ、[ログ&モニタリング]タブからアクセスできます。
デバイスの管理

このセクションでは、Check Point 730/750 Appliance のセットアップおよび管理の方法について説明します。

インターネット接続の設定

このセクションでは、Check Point 730/750 Appliance のインターネット接続情報が表示されます。ここでは、単一のインターネット接続を設定することも、ハイ・アベイラビリティまたはロード・バランス構成の複数接続を設定することもできます。複数のインターネット接続が定義されると、このページにテーブル形式で表示されます。ここで、新しい接続を追加したり、既存の接続の編集、削除、無効化などを実行できます。複数のインターネット接続がある場合は、使用するモードを「ハイ・アベイラビリティ」と「負荷分散」から選択できます。

ローカル IPS（インターネット・サービス・プロバイダ）に問い合わせて、特定のインターネット接続の設定について理解を深めることをお勧めします。

インターネット接続を設定するには

1. [[インターネットの接続]]（初めてインターネット接続を設定する場合）、[[追加]]（インターネット接続を追加設定する場合）、または[[編集]]をクリックします。
   [[新しいインターネット接続]]または[[インターネット接続の編集]]ウィンドウが開きます。
2. タブのフィールドを設定します。
   [設定]タブ

注 - 接続の種類を変更すると、アプライアンスがいったんインターネットから切断される可能性があります。

- [[接続名]] - 接続の名前を入力するか、デフォルトの「InternetN」ラベルをそのまま使用します（N は変数のインクリメント）。
- [[接続タイプ]] - 接続タイプを以下の中から選択します。
  - [DHCP] - DHCP（Dynamic Host Configuration Protocol）は、指定された範囲の IP アドレスをネットワーク上のデバイスに自動発行します。デバイスは、管理者が指定した期間、割り当てられたアドレスを使用します。
  - [静的 IP] - 固定の（ダイナミックでない）IP アドレスです。
  - [PPPoE] - PPP（Point-to-Point Protocol）フレームをイーサネット・フレームにカプセル化するネットワーク・プロトコルです。このプロトコルは主に、個人ユーザがイーサネット経由で DSL モデムに接続する DSL サービスや、シンプルなメトロ・イーサネット・ネットワークで使用されます。
  - [PPTP] - PPTP（Point-to-Point Tunneling Protocol）は、VPN（バーチャル・プライベート・ネットワーク）を構築するためのプロトコルです。PPTP では、TCP 上のコントロール・チャネルと GRE トンネルを使用して PPP パケットをカプセル化します。
  - [L2TP] - L2TP（Layer 2 Tunneling Protocol）は、VPN をサポートするために使用されるトンネリング・プロトコルです。L2TP 自体は、暗号化や機密保持のための機能を備えていません。トンネル内で別の暗号化プロトコルを使用することにより通信のプライバシーを保護します。
  - [ブリッジ] - データ・リンク層（レイヤ 2）で複数のネットワーク・セグメントを接続します。
アプライアンスの設定

- セルラー・モデム - セルラー・モデムを使用して、3G/4Gネットワークの通信事業者経由でインターネットに接続します。このオプションを使用する場合は、[インタフェース名]で[USB/Serial]を選択します。
- アナログ・モデム - USBポートやシリアルポートに接続したアナログ・モデムを使用してインターネットに接続します。このオプションを使用する場合は、[インタフェース名]で[USB/Serial]を選択します。
- 注 - シリアルポート経由のアナログ・モデムを使用する場合、シリアルポートを使ったアプライアンスへの接続や端末サーバ機能へのアクセスはできなくなります。端末サーバの詳細については、[デバイス]→[詳細設定]を参照してください。

注 - パスワードや共有キーを入力する際は、{ } [ ] ` ~ | の文字は使用できません。

- VLAN接続を使用 - インターネットの仮想インターフェースを追加するにはこのチェック・ボックスをオンにします。WAN/DMZインターフェース、スタティック、DHCP、PPPoE、PPTP、L2TP接続タイプのみに関連します。
- VLAN ID - VLAN IDとして1〜4094の値を入力します。

接続モニタリングタブ

- デフォルト・ゲートウェイ接続の切断を自動的に検知 - このオプションを選択すると、ARP要求（ping）をデフォルト・ゲートウェイに送信し、応答を待機することで、接続の切断を検出できます。
- プローブ・パケットをインターネット上の1つ以上のサーバに送り接続状況をモニタリング - このオプションを選択すると、複数の方法とサーバを使用して接続の切断を検出できます。
- 接続のプロービング・メソッド - 以下のいずれかのオプションを選択します。
  - [アドレスのping] - このオプションを選択すると、IPアドレスまたはホスト名を使用して最大3台のサーバを指定できます。
  - [DNSサーバの確認] - このオプションを選択した場合、アプライアンスは、インターネット接続設定で定義されたDNSサーバにプローブして応答を待機します。

詳細タブ

PPPoEの場合

- IPアドレスの割り当て - [ローカル・トンネルのIPアドレス]で、IPアドレスを自動的に取得するか手動で設定するかどうかを選択します。手動設定の場合は、IPアドレスを入力します。
- サービス・プロバイダ設定 - [サービス]で、サービス名（必須ではない）を入力して認証メソッドを選択します。
- オンデマンド接続 - 必要に応じて、[オンデマンド接続]チェックボックスをオンにします。このオプションは、ハイ・アベイラビリティ・モードを使用している場合のみ関係してきます。

PPTPとL2TPの場合

- IPアドレスの割り当て -
  - [ローカル・トンネルのIPアドレス]で、IPアドレスを自動的に取得するか手動で設定するかどうかを選択します。手動設定の場合は、IPアドレスを入力します。
  - [WAN IPアドレスの割り当て]で、WAN IPアドレスを自動的に取得するか手動で設定するかどうかを選択します。手動設定の場合は、IPアドレス、サブネット・マスク、デフォルトのゲートウェイを入力します。
- サービス・プロバイダ設定 - [サービス]で、サービス名（必須ではない）を入力して認証メソッドを選択します。
- オンデマンド接続 - 必要に応じて、[オンデマンド接続]チェックボックスをオンにします。このオプションは、ハイ・アベイラビリティ・モードを使用している場合のみ関係してきます。

ポート設定
アプライアンスの設定

- 必要に応じて[カスタムMTU値を使用]を選択し、[MTUサイズ]を設定します。DMZインテフェースを使用する場合、このMTU値はすべてのLANポートに適用されます。

- [MACアドレスの複製] - [デフォルトMACアドレスを上書き]を選択すると、インターネット接続で使用されているデフォルトのMACアドレスを上書きできます。この設定は、アプライアンスを別のデバイスの代わりに使用し、そのデバイスと同じMACアドレスを使用したい場合に便利です。

- 必要に応じて[自動ネゴシエーションを無効にする]を選択します。このオプションを選択すると、インターネット接続のリンク速度を手動で設定できます。

- [リング・スピード]を選択します。

QoS設定（帯域幅制御）

特定の接続に対してダウンロードまたはアップロードのQoS（帯域幅制御）を有効にするには、該当する[QoSを有効にする（ダウンロード）]チェック・ボックスまたは[QoSを有効にする（アップロード）]チェック・ボックス（あるいはその両方）をオンにします。ISPから割り当てられているアップロードおよびダウンロードの帯域幅に合わせ、選択したオプションの最大Kbpsレートを入力します。

QoSを設定する場合は、あらかじめQoSSoftwareBladeを有効にしておく必要があります。QoSSoftwareBladeを有効にするには、[ホーム]→[セキュリティ・ダッシュボード]→[QoS]→[オン]を設定します。

ISP冗長性

複数のインターネット接続をハイ・アベイラビリティ・モードまたは負荷共有モードで構成できます。複数のインターネット接続を設定する場合は、[デバイス]→[インターネット]ページでこれらのモードを切り替えることができます。各インターネット接続の[詳細]設定では、モードに応じて、各接続の優先度または重み付けを設定できます。

- 該当のインターネット接続を、このゲートウェイのデフォルト・ルートとして使用しない場合は、[デフォルトでこの接続にトラフィックをルーティング]チェック・ボックスをオフにします。このような接続は、特定の（通常はサービスベースの）ルーティング・ルールが定義されるデバイスでのみ必要となります。一般に、このようなデバイスは、特定トラフィック用の接続を用意するといった場合に使用されます。このチェック・ボックスをオフにした場合、その接続はハイ・アベイラビリティやロード・バランスには参加しません。

- [ハイ・アベイラビリティ] - [優先度] - 接続の優先度を選択します。優先度の低い接続は、優先度の高い接続が利用できない場合にのみ使用されます。
アプライアンスの設定

- [負荷分散] - [重み付け] - インターネットへのトラフィックは、重み付けの設定に従ってすべての利用可能な接続間で分散されます。

ワイヤレスの設定

[デバイス]→[ワイヤレス]ページには、ワイヤレス・ネットワークの設定が表示されます（ワイヤレス・ネットワークが利用可能な場合）。メインのワイヤレス・ネットワークに加え、ゲスト・ワイヤレス・ネットワークと標準ワイヤレス・ネットワーク（VAP：仮想アクセス・ポイント）を設定できます。

- ゲスト・ワイヤレス・ネットワーク - デフォルトでホットスポットを使用します。セキュリティで保護されず、パスワードなしでアクセスできます。
- 標準ワイヤレス・ネットワーク - アクセスにパスワードが必要なる保護されたワイヤレス・ネットワークです。デフォルトではホットスポットを使用しません。

ワイヤレス・ネットワークを削除するには、[デバイス]→[インターネット]へ移動します。

複数のワイヤレス・ネットワーク（VAPS）を定義すると、表に各ワイヤレス・ネットワークが表示されます。この表で、新しいゲスト・ワイヤレス・ネットワークまたは標準ワイヤレス・ネットワークの追加や、既存のワイヤレス・ネットワークの編集、削除、無効化を行うことができます。

ワイヤレス・ネットワークをオン/オフにするには

- [オン]または[オフ]オプションを選択します。以前の設定が保存されます。複数の VAP を設定している場合は、[オフ]を選択するとすべての VAP が無効になります。
  注 - ワイヤレス・ラジオをオフにした場合、再度オフにしてもVAPは無効のままになります。VAPを有効にするには、この表で該当のエントリを選択し、[有効にする]をクリックします。
- インターネットに有効または無効にするには、[有効/無効]をクリックします。

ラジオ設定を編集するには

1. [ラジオ設定]をクリックします。
アプライアンスの設定

2. 適切な操作モード、チャネル、チャネル（幅）、送信出力を選択します。
4. [適用]をクリックします。

この設定は、すべてのワイヤレス・ネットワークに共通して適用されます。国によっては、ワイヤレス通信に関する規制のため一部のオプションが使用できない、または許可されない場合があります。

[471x41]Check Point 730/750 Appliance Locally Managed Administration Guide R77.20.15

ホットスポットをカスタマイズするには

[ホットスポット]リンクをクリックします。詳細については、[デバイス]→[ホットスポット]ページを参照してください。

ワイヤレス・ネットワークを追加または編集するには

1. メインのワイヤレス・ネットワークを編集するには、[ワイヤレス・ネットワーク設定の編集]をクリックします。
2. メインのネットワークにゲスト・ネットワークまたは標準ネットワークを追加するには、ページの[ゲスト]リンクまたは[標準]リンクをクリックします。定義したネットワークは、ページの表に表示されます。この表で[新規]をクリックして、新しいネットワークを作成することもできます。追加したゲスト・ネットワークや標準ネットワーク（VAP）を編集するには、表で該当のエントリを選択し、[編集]をクリックします。

[New/Edit Wireless Network]ウィンドウが開きます。

3. 以下のフィールドを設定します。

[設定]タブ

- [ネットワーク名（SSID）] - ワイヤレス・ネットワークの名前を入力するか、デフォルトの名前を使用します。通信範囲内のアクセス・ポイントを探すクライアントには、この名前が表示されます。
- [ホットスポット使用] - このインタフェースからのアクセスを許可する前に、ユーザをホットスポット・ポータルにログインするには、このチェック・ボックスをオンにします。ホットスポットの設定は、[デバイス]→[ホットスポット]ページで行います。

[設定]タブ→[ワイヤレス・セキュリティ]

- [保護されているネットワーク（推奨）] - ワイヤレス・ネットワークではこのセキュリティ設定を使用することをお勧めします。
- [セキュリティタイプ] - ワイヤレス・ネットワークで使用するセキュリティ技術を選択します。最も互換性が高いのは WPA/WPA2 です。また WPA2 ではセキュリティの強度が最も高くなります。
- [暗号化タイプ] - 暗号化方式を選択します。
- [認証方式] - ユーザが認証する方法として、パスワードまたは RADIUS サーバ（エンタープライズ・モード）を選択します。

[パスワード]オプションを選択すると、すべてのユーザで共通のパスワードを使用できます。このオプションは「WPA パーソナル」と呼ばれるものです。

[RADIUS サーバ（エンタープライズ・モード）]オプションは、[ユーザ&オブジェクト]→[サーバ認証]ページで、RADIUS サーバを定義する必要があります。ワイヤレス・ネットワークに接続しようとする各ユーザは、RADIUS サーバを通じて認証されます。このオプションは「WPA エンタープライズ」とも呼ばれます。

- [ネットワーク・パスワード] - 認証にパスワードを使用する場合は、パスワードを使用するか[生成]をクリックして自動生成します。
アプライアンスの設定

- [表示] - パスワードを表示するにはこのチェック・ボックスをオンにし、非表示にするにはオフにします。
- [保護されていないネットワーク(推奨されません)] - パスワードを設定しない場合、すべてのワイヤレス・クライアントがこのネットワークにアクセス可能となります。このオプションは選択しないことをお勧めします。

[設定]タブ→[詳細設定]
- [ネットワーク名を隠す（SSID）] - オンにした場合、ワイヤレス・ネットワーク名は、ワイヤレス・ネットワークをスキャンするユーザに自動的には表示されなくなります。このワイヤレス・ネットワークに接続するには、ネットワーク名を手動で指定する必要があります。
- [ステーション間のトラフィックを許可] - オンにすると、このネットワーク上の各ワイヤレス・ステーションが相互に通信できるようになります。オフにした場合、ワイヤレス・ステーション間のトライフォックは遮断されます。
- [MAC アドレス・フィルタリングを有効にする] - オンにした場合、ワイヤレス・デバイスによるワイヤレス・ネットワークへの接続がデフォルトで禁止されます。特定のデバイスによる接続を許可するには、この表にデバイスのMAC アドレスを追加します。[新規]をクリックし、そのデバイスのMAC アドレスを入力してから[適用]をクリックします。

[ワイヤレス・ネットワーク]タブ→[インタフェース設定]
- [割り当て先] - [別のネットワーク]を選択するか、設定済みの既存のネットワークを選択します。[別のネットワーク]を選択した場合は、以下の情報を設定します。
  - IP アドレス
  - サブネット・マスク

[ワイヤレス・ネットワーク]タブ→[DHCP サーバ]
いずれかのオプションを選択します。
- 有効 - IP アドレス範囲を入力し、必要な場合はIP アドレスの除外範囲を入力します。アプライアンス自体のIP アドレスは自動的にこの範囲から除外されます。[ユーザ & オブジェクト]→[ネットワーク・オブジェクト]ページでネットワーク・オブジェクトを定義して、特定のIP アドレスを除外または予約することは可能です。特定のIP アドレスを予約するには、デバイスのMAC アドレスが必要です。
- リレー - DHCP サーバのIP アドレスを入力します。
- 無効

[アクセス・ポリシー]タブ
以下のオプションを使用して自動ルールを作成できます。自動ルールは、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページに表示されます。
- [このネットワークからローカル・ネットワークへのアクセスを許可（ワイヤレス・ネットワークは信頼）]
- [このネットワークからローカル・ネットワークへのトラフィックをログ記録]

[DHCP サーバ・オプション]タブ
このタブで設定されるDHCPオプションの値は、DHCP サーバからDHCP クライアントへ配布されます。
このタブは、ワイヤレス・ネットワークが別にあり、そこにDHCP サーバが設定されている場合のみ利用できます。

DNS サーバ
いずれかのオプションを選択します。
- 自動 - [デバイス]→[DNSとデバイス]→[インターネット]のページで設定されたアプライアンスのDNS設定を使います。
次のIPアドレスを使用 - 最初のDNSサーバ、2番目のDNSサーバ、3番目のDNSサーバのIPアドレスを入力します。

デフォルト・ゲートウェイ
いずれかのオプションを選択します。
- このゲートウェイのIPアドレスをデフォルトゲートウェイとして使用
- 次のIPアドレスを使用 - デフォルトゲートウェイとして使うIPアドレスを入力します。

WINS
いずれかのオプションを選択します。
- インターネット接続に設定されたWINSサーバを使用
- 次のWINSサーバを使用 - 1番目と2番目のWINSサーバのIPアドレスを入力します。

リース
- リース時間 - 1台のデバイスで、動的に取得するIPアドレスを保持する際のタイムアウトを設定します（時間）。

その他の設定
次の追加パラメータを設定して、DHCPクライアントへ配布することができます（オプション）。
- Timeサーバ
- Callマネージャ
- TFTPサーバ
- TFTPブート・ファイル
- X-Windowsディスプレイ・マネージャ
- AvayaIPphone
- NortelIPphone
- ThomsonIPphone

カスタム・オプション
上記以外のカスタム・オプションを追加することができます。各オプションには、名前、タグ、タイプ、データ・フィールドを設定する必要があります。

ワイヤレス・クライアントはリンクとして表示されます。[設定の編集]をクリックして編集します。[無効/有効]をクリックしてワイヤレス・クライアントを有効または無効にします。

ローカル・ネットワークの設定
[デバイス]→[ローカル・ネットワーク]ページでは、ローカル・ネットワーク接続、スイッチ、ブリッジ、ワイヤレス・ネットワーク(ワイヤレス・ネットワーク・モデルのみ)を設定、有効化できます。

[ネットワーク]表には、使用可能なすべてのネットワーク接続が表示されます。
このページでは、以下の操作を行うこともできます。
- 使用可能なローカルLANインターフェースとワイヤレス・ネットワーク間に複数のスイッチ（ポートベースのVLAN）を設定する。スイッチのLANポート間でトラフィックのモニタリングや検査を行うことはできません。
- インタフェース間に複数のブリッジを設定する。ブリッジのトラフィックは、アプライアンスによって常にモニタリングおよび検査されます。
アプライアンスの設定

- 任意のLANインタフェースまたはDMZにタグベースのVLAN(802.1q)を作成、設定する。
- VPNトンネル(VTI)を作成、設定する。VPNトンネルを使用すると、トンネルにルーティングして暗号化するトラフィックを決定するルーティングルールを作成できます(ルートベースのVPN)。
- 新しいワイヤレスネットワーク(仮想アクセスポイント)を追加する(ワイヤレスネットワーク・モデルのみ)。この操作は、[デバイス]→[ワイヤレスネットワーク]ページで行うこともできます。

上記のいずれかのオプションを作成するには
[新規]をクリックし、該当のオプションを選択します。

上記のいずれかのオプションを編集、削除、有効化/無効化するには
該当の行を選択し、[編集]、[削除]、[有効]、[無効]のいずれかをクリックします。
以下のことに注意してください。
- 物理インタフェースは削除できません。
- スイッチまたはブリッジの一部であるインタフェースを編集すると、そのインタフェースはスイッチまたはブリッジから削除されます。
- インターネット接続の一部であるLANインタフェースやDMZインタフェースもこのページに表示されますが、設定は[デバイス]→[インターネット]ページで行う必要があります。
- このページの表には、ネットワークごとに以下の情報が表示されます。
  - 名前・ネットワーク名、使用するインタフェース(複数ある場合)、説明(オプション)
  - ローカルIPアドレス
  - サブネット・マスク
  - MACアドレス
  - ステータス - 物理インタフェースとワイヤレスネットワークのステータスが表示されます。
    - 物理インタフェース - 有効な各物理インタフェースのケーブル接続の状態が表示されます。有効にされていない物理インタフェースについては無効と表示されます。
    - ワイヤレスネットワーク - ワイヤレスネットワークが有効かどうかが表示されます。

スイッチを作成または編集するには
注 - スイッチのLANポート間でトラフィックのモニタリングや検査を行うことはできません。

タブのフィールドを設定します。
[設定]タブ
1. [スイッチの設定]で、スイッチの一部とするインタフェースのチェックをオン/オフに設定します。表には、すでにスイッチの一部となっているインタフェース(チェックマーク付き)と、まだ割り当てられておらずスイッチに追加可能なインタフェース(チェックマークなし)が表示されます。すでに別のスイッチの一部となっているインタフェースは、この表には表示されません。
2. [割当先]オプションを選択します。
   - [未割り当て] - 物理インタフェースはいずれのネットワークの一部にもならず、使用することはできません。
   - [別のネットワーク] - 別のネットワークを選択した場合は、以下の情報を設定します。
3. スイッチが使用するIPアドレスとサブネット・マスクを選択します。
4. [ホットスポットを使用] - このインタフェースからのアクセスを許可する前に、ユーザをホットスポット・ポータルにリダイレクトするには、このチェックボックスをオンにします。ホットスポットの設定は、[デバイス]→[ホットスポット]ページで行います。
5. [DHCP サーバ]で以下の設定を行います。

いずれかのオプションを選択します。

- 有効 - IP アドレス範囲を入力し、必要な場合は IP アドレスの除外範囲を入力します。アプライアンス自体の IP アドレスは自動的にこの範囲から除外されます。[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]ページでネットワーク・オブジェクトを定義して、特定の IP アドレスを除外または予約することも可能です。特定の IP アドレスを予約するには、デバイスの MAC アドレスが必要です。

- リレー - DHCP サーバの IP アドレスを入力します。

- 無効

[DHCP サーバ・オプション]タブ

後述する「[DHCP サーバ・オプション]タブ」を参照してください。

物理インタフェースを編集するには

タブのフィールドを設定します。DMZ インタフェースの場合、[アクセス・ポリシー]というタブも表示されます。

[設定]タブ

- [割当先] - 以下の必須オプションを選択します。
  - [未割り当て] - 物理インタフェースはいずれのネットワークの一部にもならず、使用することはできません。
  - 設定済みのいずれかのスイッチまたはブリッジ。
  - [別のネットワーク] - このオプションを選択する場合は、以下の情報を設定します。
    - IP アドレス
    - サブネット・マスク
    - DHCP サーバ

いずれかのオプションを選択します。

- 有効 - IP アドレス範囲を入力し、必要な場合は IP アドレスの除外範囲を入力します。アプライアンス自体の IP アドレスは自動的にこの範囲から除外されます。[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]ページでネットワーク・オブジェクトを定義して、特定の IP アドレスを除外または予約することも可能です。特定の IP アドレスを予約するには、デバイスの MAC アドレスが必要です。

- リレー - DHCP サーバの IP アドレスを入力します。

- 無効

[詳細]タブ

このタブに表示されるオプションは、インタフェースの種類とステータスによって異なります。使用可能なオプションを以下のように設定します。

- [説明] - 説明を入力します(オプション)。説明は、名前の横のローカル・ネットワークのテーブルに表示されます。

- [MTU サイズ] - インタフェースの最大転送単位のサイズを設定します。Check Point 730/750 Applianceでは、この値はすべての物理 LAN ポートおよび DMZ ポートで共通となります。

- [自動ネゴシエーションを無効にする] - インタフェースのリンク速度を手動で設定する場合は、このオプションを選択します。

[アクセス・ポリシー]タブ（DMZ インタフェースのみ）
以下のオプションを使用して自動ルールを作成できます。自動ルールは、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページに表示されます。

- このネットワークからローカル・ネットワークへのアクセスを許可
- このネットワークからローカル・ネットワークへのトラフィックをログ記録

【DHCP サーバ・オプション】タブ

後述する「[DHCP サーバ・オプション]タブ」を参照してください。

タグ・ベースの VLAN を作成または編集するには:

VLAN を新規作成するには、既存ネットワーク（スイッチまたはブリッジ）の一部でない物理インタフェースが1つ以上必要です。

タブのフィールドを設定します。

【設定】タブ

- 【VLAN ID】- 仮想識別子となる番号を入力します。
- 【割当先】- 仮想ネットワークを新規作成する物理インタフェースを選択します。
- IP アドレス
- サブネット・マスク
- 【ホットスポットを使用】- このインタフェースからのアクセスを許可する前に、ユーザをホットスポット・ポータルにリダイレクトするには、このチェック・ボックスをオンにします。ホットスポットの設定は、[デバイス]→[ホットスポット]ページで行います。
- DHCP サーバー

いずれかのオプションを選択します。

- 【有効】- IP アドレス範囲を入力し、必要な場合は IP アドレスの除外範囲を入力します。アプライアンス自体の IP アドレスは自動的にこの範囲から除外されます。[デバイス]→[ネットワーク・オブジェクト]ページでネットワーク・オブジェクトを定義して、特定の IP アドレスを除外または予約することも可能です。特定の IP アドレスを予約するには、デバイスの MAC アドレスが必要です。
- リレー - DHCP サーバーの IP アドレスを入力します。
- 【無効】

【DHCP サーバ・オプション】タブ

後述する「[DHCP サーバ・オプション]タブ」を参照してください。

VPN トンネル（VTI）を作成または編集するには

仮想トンネル・インタフェース（VTI）は、既存のルート・ベースの VPN トンネルに関連付けられた、セキュリティ・ゲートウェイ上の仮想インタフェースです。ルート・ベースの VPN トンネルは、VPN コミュニティに含まれる2台のピア・セキュリティ・ゲートウェイ間のポイントツーポイント接続として機能します。各ピア・セキュリティ・ゲートウェイは、トンネルに接続する VTI を1つ保持します。

VPN トンネルとそのプロパティは、2台のゲートウェイが含まれる VPN コミュニティで定義します。VTI を作成するには、VPN コミュニティとそのメンバとなるセキュリティ・ゲートウェイを事前に定義しておく必要があります。

タブのフィールドを設定します。

【設定】タブ

- 【VPN トンネル ID】- VTI を識別するための番号。
- 【ピア】- VPN サイトの名前。「VPN サイトの設定」を参照してください。
VPNトンネル・インタフェースは、番号を付けることも付けないこともできます。該当するオプションを選択します。

- [番号付き VTI] - 番号付き VTIのローカルおよびリモート IP アドレスを設定します。
  - [ローカル IP アドレス] - ローカルのポイントツーポイント仮想インタフェースで使用する IP アドレス。
  - [リモート IP アドレス] - ピア・ゲートウェイのポイントツーポイント仮想インタフェースで使用する IP アドレス。
- [番号が付いていない VTI] - VTIが番号なしの場合、ローカルおよびリモート IP アドレスは設定する必要はありません。ローカル・インタフェースを定義して外部へのトラフィックの発信元 IP アドレスとして使用します。
- [ローカル・インタフェース] - リストからローカル・インタフェースを選択します。

ブリッジを作成または編集するには

タブのフィールドを設定します。

[設定]タブ
- [ブリッジ設定] で、ブリッジの一部とするネットワークを選択します。
- [STP を有効にする] - Spanning Tree Protocol (STP - IEEE 802.1d) が有効である場合、各ブリッジは、隣接するブリッジまたはスイッチと通信して相互接続の方法を判断します。この情報は、ループを防止し、パケットのルーティングを最適化するために使用されます。また、ブリッジやネットワークのリンクに障害が発生した場合にトポロジを再計算し、耐障害性を高めるためにも使用されます。
- [ブリッジ・インタフェースの名前を入力します。名前の形式は「brN」とする必要があります。N は、0 から 9 までの数字です。たとえば「br2」のようにします。]
- [スイッチが使用する IP アドレスとサブネット・マスクを選択します。]
- [ホットスポットを使用] - このインタフェースからのアクセスを許可する前に、ユーザをホットスポット・ポータルにリダイレクトするには、このチェック・ボックスをオンにします。ホットスポットの設定は、[デバイス]→[ホットスポット]ページで行います。
- [DHCP サーバ] いずれかのオプションを選択します。
  - [有効] - IP アドレス範囲を入力し、必要な場合は IP アドレスの除外範囲を入力します。アプライアンス自体の IP アドレスは自動的にこの範囲から除外されます。[デバイス]→[オブジェクト]→[ネットワーク・オブジェクト]ページでネットワーク・オブジェクトを定義して、特定の IP アドレスを除外または予約することも可能です。特定の IP アドレスを予約するには、デバイスの MAC アドレスが必要です。
  - リレー - DHCP サーバの IP アドレスを入力します。
  - [無効]

[詳細]タブ
- [MTU サイズ] - インタフェースの最大転送単位のサイズを設定します。

[DHCP サーバ・オプション]タブ
後述する「[DHCP サーバ・オプション]タブ」を参照してください。

仮想アクセス・ポイント (VAP) を作成または編集するには

[デバイス]→[ワイヤレス・ネットワーク]のヘルプ・ページを参照してください。

[DHCP サーバ・オプション]タブ
このタブで設定される DHCP オプションの値は、DHCP サーバから DHCP クライアントへ配布されます。
このタブは、ワイヤレス・ネットワークが別にあり、そこに DHCP サーバが設定されている場合のみ利用できます。

**DNS サーバ**
いずれかのオプションを選択します。
- 自動 - [デバイス]→[DNS とデバイス]→[インターネット]のページで設定されたアプライアンスの DNS 設定を使います。
- 次の IP アドレスを使用 - 最初の DNS サーバ、2 番目の DNS サーバ、3 番目の DNS サーバの IP アドレスを入力します。

**デフォルト・ゲートウェイ**
いずれかのオプションを選択します。
- このゲートウェイの IP アドレスをデフォルトゲートウェイとして使用
- 次の IP アドレスを使用 - デフォルト・ゲートウェイとして使う IP アドレスを入力します。

**WINS**
いずれかのオプションを選択します。
- インターネット接続に設定された WINS サーバを使用
- 次の WINS サーバを使用 - 1 番目と2番目の WINS サーバの IP アドレスを入力します。

**リース**
- リース時間 - 1 台のデバイスで、動的に取得する IP アドレスを保持する際のタイムアウトを設定します（時間）。

**その他の設定**
次の追加パラメータを設定して、DHCP クライアントへ配布することができます（オプション）。
- Time サーバ
- Call マネージャ
- TFTP サーバ
- TFTP ブート・ファイル
- X-Windows ディスプレイ・マネージャ
- Avaya IP phone
- Nortel IP phone
- Thomson IP phone

**カスタム・オプション**
上記以外のカスタム・オプションを追加することができます。各オプションには、名前、タグ、タイプ、データ・フィールドを設定する必要があります。

**ホットスポットの設定**
[デバイス]→[ホットスポット]ページでは、次の設定ができます。
ゲストのアクセス - ユーザが利用規約に同意またはホットスポットのポータルで認証すると、IP アドレスにセッションが作成されます。セッションは、設定したタイムアウト（デフォルトでは 240 分）の時間が過ぎると切れます。

ホットスポットの例外 - 特定の IP アドレス、IP 範囲、ネットワークをホットスポットから除外するように定義できます。

ホットスポットは、システムで自動的に有効になります。無効にするには、[デバイス]→[詳細設定]に移動します。ホットスポットを検索し、該当のエントリをダブルクリックして[無効]を選択し、[適用]をクリックします。

インターフェースのホットスポットを設定するには
1. [ローカル・ネットワークで設定]をクリックします。
   [ローカル・ネットワーク]ウィンドウが開きます。
2. インタフェースを選択して、[編集]をクリックします。
   [<interface>の編集]ウィンドウが表示されます。
3. [ホットスポットを使用]をオンにします。
4. [適用]をクリックします。

設定したインターフェースからアクセスするユーザは、Check Point のホットスポット・ポータルへリダイレクトされます。

ホットスポットの例外を設定するには
1. [例外の管理]をクリックします。
   [ホットスポット・ネットワーク・オブジェクトの例外管理]ウィンドウが開きます。
2. 例外として追加するオブジェクトを選択します。
   [選択したネットワーク・オブジェクト]ウィンドウに、選択したオブジェクトが表示されます。オブジェクトをリストから削除するには、横にある「x」をクリックします。
3. オブジェクトのリストを絞り込むには、絞り込む値を入力します。絞り込む値に一致するオブジェクトがリストに表示されます。
4. 必要に応じて、[新規]をクリックして新しいオブジェクトをリストに追加します。新しいオブジェクトの作成に関する情報は、[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]ページを参照してください。
5. [適用]をクリックします。

追加したオブジェクトがホットスポットから除外されます。

ユーザ認証を要求するには
1. [認証を求める]チェックボックスをオンにします。
2. アクセスをすべてのユーザまたは特定のユーザ・グループに対して許可できます。
3. 特定のユーザ・グループを選ぶ場合は、グループ名をテキスト・ボックスに入力します。
4. [適用]をクリックします。

設定したインターフェースからアクセスするユーザ/ユーザ・グループは、Check Point のホットスポット・ポータルへリダイレクトされ、認証情報を入力するよう求められます。
セッション・タイムアウトを設定するには
1. [セッション・タイムアウト]に数字（分）を入力します。この設定値はセッションが切れるまでユーザがログインできる時間を定義します。
2. [適用]をクリックします。

ポータルの外観をカスタマイズするには
1. [ホットスポット・ポータルのカスタマイズ]をクリックします。
2. 以下のフィールドを設定します。
   - [ポータル・タイトル] - デフォルトのままにするか、新しくタイトルを入力します。
   - [ポータル・メッセージ] - デフォルトのままにするか、新しくメッセージを入力します。
   - [利用規約] - 「この利用条件に同意します」というチェックボックスをホットスポットのポータル・ページに追加するには、このチェック・ボックスをオンにします。利用条件のテキストをテキスト・ボックスに入力します。ユーザが[利用条件]リンクをクリックすると、ここで入力したテキストが表示されます。
4. [適用]をクリックします。

ホットスポット・ポータルへの同時ログインをブロックするには
1. [デバイス]→[詳細設定]へ移動します。
2. [ホットスポット]を選択します。
3. [編集]をクリックします。
   - [ホットスポット]ウィンドウが開きます。
4. [同時ログインのブロック]チェックボックスをオンにします。
5. [適用]をクリックします。
   同じユーザが複数のコンピュータから同時にホットスポット・ポータルにログインできなくなります。

ルーティング・テーブルの設定
[デバイス]→[ルーティング]ページには、アプライアンスに追加されたルートを示すルーティング・テーブルが表示されます。このページで新しいルートを追加できます。
デフォルトルートの設定はこのページではなく[デバイス]→[インターネット]ページで行いますが、参照することはできます。このページには、すべてのルーティング・ルール、つまりこのページで手動設定したルールとシステムによって自動定義されたルールが表示されます。システム定義のルートを編集することはできません。
ここでは、宛先ベースの新しいカスタム・ルールや、発信元またはサービスに基づくポリシー・ベースのルーティング・ルールを作成できます。

新しいルートを追加するには
1. [新規]をクリックします。
   - [新しいルーティング・ルール]ウィンドウが開きます。
2. ルール・サマリまたは表のセル中のリンクをクリックして、ルーティング・ルールの値を選択します。詳細については、以下の表を参照してください。サービスについては、新しいサービスやサービス・グループを作成することもできます。
3. オプション: コメントを入力します。
4. メトリックを0～100で入力します。デフォルトは0です。
5. [適用]をクリックします。

<table>
<thead>
<tr>
<th>表のカラム</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>宛先</td>
<td>ルート・ルールは、トラフィックの宛先が、ここで指定された宛先IPアドレス/ネットワークに合致する場合のみ適用されます。</td>
</tr>
<tr>
<td>ソース</td>
<td>ルート・ルールは、トラフィックの発信元が、ここで指定された発信元IPアドレス/ネットワークに合致する場合のみ適用されます。</td>
</tr>
<tr>
<td>サービス</td>
<td>ルート・ルールは、トラフィックのサービスが、ここで指定されたサービスのIPプロトコルおよびポート、またはサービス・グループに合致する場合のみ適用されます。</td>
</tr>
<tr>
<td>ネクスト・ホップ</td>
<td>このルートのネクスト・ホップ・ゲートウェイです。次段のゲートウェイのIPアドレスか、アプライアンスに設定された接続のうち特定のインターネット接続を指定できます。</td>
</tr>
<tr>
<td>メトリック</td>
<td>ルートの優先度を指定します。同じ宛先に到達するルートが複数ある場合、メトリックの最も小さいルートが選択されます。</td>
</tr>
</tbody>
</table>

編集、削除、有効化/無効化は、このページで作成された手動設定のルーティング・ルールに対してのみ行うことができます。直接接続されたネットワーク用にOSが作成したルーティング・ルールや、ダイナミック・ルーティング・プロトコルが定義したルールを編集、削除、有効化/無効化することはできません。

既存のルートを編集するには
ルートを選択して[編集]をクリックします。

既存のルートを削除するには
ルートを選択して[削除]をクリックします。

既存のルートを有効/無効にするには
ルートを選択して[有効]または[無効]をクリックします。

重要な情報
- このページでデフォルト・ルートを追加することはできません。システムのデフォルト・ルートは、インターネット接続設定から引き継がれます。デフォルト・ルートを変更するには、インターネット接続を編集してから、そのデフォルト・ゲートウェイ（ネクスト・ホップ）のIPアドレスを変更します。
- インターネット接続をハイ・アベイラビリティ構成にしている場合、デフォルト・ルートは、アクティブなインターネット接続に合わせ、フェイルオーバー時に自動的に変更されます。
- ネットワーク・インタフェースが無効にされている場合、そのインタフェースに到達するルートはすべて「非アクティブ」となります。この場合、トラフィックはアクティブなルーティング・ルール（通常はデフォルト・ルート）に従ってルーティングされます。このようなルートは、ルーティング・ページで[無効]と表示されます。インタフェースが有効になると、非アクティブなルートは自動的にアクティブとなります。

インターネット接続が存在しないなど、アクティブなデフォルト・ルートがない場合「デフォルトのルートが未設定です。インターネット接続がダウンしているか未設定の可能性があります」というメッセージが表示されます。
DNS サーバの設定

[デバイス]→[DNS] ページでは、DNS サーバの設定とドメイン名の定義を行うことができます。

DNS を設定するには

1. 最大 3 つの DNS サーバを定義してすべてのインターネット接続に適用するか、アクティブなインターネット接続（プライマリ）で提供されている DNS 設定を使用するかを選択します。

2. DNS を設定するには、次の手順に従います。

   DNS サーバの設定を選択する場合は、必ず有効な IP アドレスを入力してください。

   組織の DNS サーバが本社環境に設置されている場合は、DNS サーバの設定とドメイン名の定義を行うことができます。

   DNS サーバを設定するには、次の手順に従います。

   1. DNS サーバを設定するには、次の手順に従います。

   2. DNS サーバを選択する場合は、必ず有効な IP アドレスを入力してください。

   3. DNS サーバが本社環境に設置されている場合、DNS サーバの設定とドメイン名の定義を行うことができます。

   4. DNS サーバを設定するには、次の手順に従います。

   DNS サーバの設定を選択する場合は、必ず有効な IP アドレスを入力してください。

   組織の DNS サーバが本社環境に設置されている場合は、DNS サーバの設定とドメイン名の定義を行うことができます。

   DNS サーバを設定するには、次の手順に従います。

   1. DNS サーバの設定を選択する場合は、必ず有効な IP アドレスを入力してください。

   2. DNS サーバを選択する場合は、必ず有効な IP アドレスを入力してください。

プロキシ・サーバの設定

[デバイス]→[プロキシ] ページでは、プロキシクセシクスとインターネット間のプロキシ・サーバがある場合に必要な設定を行います。このプロキシ・サーバは、プロキシクセシクスの内部プロセスから Check Point サーバにアクセスする必要があるときに使用します。たとえば、アップデートライセンス・サーバからアップデートを取得する場合、URL フィルタリング・サービスにアクセスする場合などです。

通常は、プロキシ・サーバを組織の内部ネットワークに導入するため、このようなケースは多くありません。

プロキシ・サーバを設定するには

1. [プロキシ・サーバを使用する] を選択します。

2. ホスト名または IP アドレスを入力します。
3. ポートを入力します。
4. [適用]ボタンをクリックします。

バックアップ、復元、アップグレード、およびその他のシステム操作
[デバイス]→[システム操作]ページでは、次の操作を行うことができます。
- 再起動
- 工場出荷時のデフォルト設定に復元
- 工場出荷時のデフォルト・イメージと設定に復元
- アプライアンス・ファームウェアの最新バージョンへのアップグレード（自動または手動）
- 前のファームウェア・イメージに戻す
- アプライアンス設定のデスクトップ・コンピュータ上のファイルへのバックアップ
- バックアップした設定の復元

アプライアンスを再起動するには
1. [再起動]をクリックします。
2. 確認メッセージで[OK]をクリックします。
アプライアンスが再起動します。

工場出荷時のデフォルト設定に復元するには
1. [デフォルト設定]をクリックします。
2. 確認メッセージで[OK]をクリックします。
工場出荷時のデフォルト設定に復元されます。アプライアンスが再起動し、操作が完了します。

注 - この操作では、ソフトウェア・イメージは変更されません。設定のみがデフォルト値に復元されます（IP アドレス: 192.168.1.1:4434、ユーザ名: admin、パスワード: admin）。

工場出荷時のデフォルト・イメージに戻すには
1. Click Factory Defaults。
2. 確認メッセージで[OK]をクリックします。
工場出荷時のデフォルト設定に復元されます。アプライアンスが再起動し、操作が完了します。

注 - この操作では、ソフトウェア・イメージがアプライアンス出荷時のデフォルト・イメージに、設定がデフォルト値に復元されます（IP アドレス: 192.168.1.1:4434、ユーザ名: admin、パスワード: admin）。

ファームウェアのバージョンが最新かどうか確認するには
[今すぐチェック]をクリックします。

アプライアンス・ファームウェアを自動アップグレードするには（クラウド・サービスが設定されていない場合）
1. [自動アップグレードの設定]をクリックします。
   [ファームウェアの自動アップグレード]ウィンドウが開きます。
2. [ファームウェアを自動的にアップグレード]をオンにします。
アプライアンスの設定

3. 新しいファームウェアが見つかった場合に使用するアップグレード・オプションを選択します。
   • [すぐにアップグレード]
     または
   • [次の頻度でアップグレード]
4. [次の頻度でアップグレード]を選択した場合は、次のオプションを選択します。
   • [毎日] - 時刻を指定します。
   • [毎週] - 曜日と時刻を指定します。
   • [毎月] - 日日にちと時刻を指定します。
5. [適用]をクリックします。
   注 - 新しいファームウェアにアップグレードできる場合、そのファームウェアのバージョン番号が表示されます。すぐにアップグレードする場合は[今すぐアップグレード]をクリックし、新しいファームウェアの新機能を確認する場合は[詳細情報]をクリックします。
   注 - ゲートウェイがクラウド・サービスで設定されている場合は、ファームウェアの自動アップグレードはロックされています。この設定はクラウド・サービスでのみ変更できます。

アプライアンス・ファームウェアを手動アップグレードするには
1. [手動アップグレード]をクリックします。
   ソフトウェアのアップグレード・ウィザードが開きます。
2. ウィザードの手順に従います。
   注 - ファイアウォールは、アップグレード実行中も動作を継続します。ただし、次の場合に限りトラフィックの中断が発生することがあります。
     • アップグレード前にローカル・イメージを保存する際（このとき、ファイアウォール・デーモンがシャットダウンします）。これにより、VPN接続が中断する場合があります。
     • アップグレード・プロセスでアプライアンスが自動的に再起動します。

前のファームウェア・イメージに戻すには
1. [前のイメージに戻す]をクリックします。
2. 確認メッセージで[OK]をクリックします。
   アプライアンスが再起動し、操作が完了します。

アプライアンスの設定をバックアップするには
1. [バックアップ]をクリックします。
   [バックアップの設定]ページが開きます。
2. バックアップ・ファイルを暗号化するには、[ファイルの暗号化]チェック・ボックスをオンにします。パスワードを入力し、確認のためもう一度同じパスワードを入力します。
3. アプライアンスにインストールしたセキュリティ・ポリシーをバックアップするには、[セキュリティ・ポリシーのバックアップ]チェック・ボックスをオンにします。作成するバックアップ・ファイルについてのコメントを追加できます。
4. [バックアップの保存]をクリックします。[ファイルのダウンロード]ダイアログ・ポックスが表示されます。ファイル名は、<ソフトウェアの現在のバージョン>-<YY-Month-day>-<HH_MM_Seconds>.zip という形式になります。
5. [保存]をクリックし、保存場所を指定します。
バックアップした設定を復元するには
1. [復元]をクリックします。[復元の設定]ページが開きます。
2. バックアップ・ファイルの保存場所を参照します。
3. [ファイルのアップロード]をクリックします。

重要な情報
- ハードウェア障害の発生時などにアプライアンスを交換する場合は、[デバイス]→[ライセンス]から、元のアプライアンスで保存した設定を復元し、ライセンスを再度有効にできます。
- 既存のアプライアンスを複製する場合は、そのアプライアンスの設定を新しいアプライアンスに復元します。
- バージョンが異なるアプライアンスの設定をリストアすることもできますが、バージョンによっては自動的にリストアできない場合もあります。リストアがサポートされないバージョン同士の場合、設定のリストアは受け付けられません。

ソフトウェア・アップグレード・ウィザードの使用
ソフトウェア・アップグレード・ウィザードの各ページの手順に従います。
ウィザードを途中で終了するには、[キャンセル]をクリックします。

ようこそ
Check Point Download Center リンクをクリックして、指示に従ってアップグレード・パッケージをダウンロードします。ファイルをすでにダウンロードしてある場合は、この手順をスキップできます。

ソフトウェアのアップロード
[参照]をクリックし、ダウンロードしたアップグレード・パッケージのファイルを選択します。
[アップロード]をクリックします。この処理には数分かかる場合があります。アップロードが完了すると、自動的にイメージの検証が行われます。ページの下部に表示されるインジケータで、処理の進捗状況を確認できます。イメージの検証が正常に終了すると、[アップロードが完了しました]というメッセージが表示されます。

アップグレード設定
アップグレードは、独立したフラッシュ・パーティションで実行されるため、現在実行中のパーティションが影響を受けることはありません。このため、アップグレード・プロセス中に障害が発生した場合には、いつでも現在のイメージに切り替えることができます。アプライアンスが正常に起動しないなど予期せぬ事態が発生した場合は、電源ケーブルを差し込み直してください。アプライアンスは、自動的に元のイメージに回復します。
[システム操作]ページで[前のイメージに戻す]ボタンをクリックすると、以前のイメージに回復することができます。バックアップには、ファームウェア、すべてのシステム設定、最新のセキュリティ・ポリシーなどイメージ全体が含まれています。
[次へ]をクリックすると、アップグレード・プロセスが開始されます。

アップグレード中
アップグレード中のページにはアップグレードの進捗状況を示すインジケータが表示され、終了したステップを確認できます。
- アップグレード・プロセスの初期化
- 新しいイメージのインストール
システムのバックアップ
[デバイス]→[システム操作]ページでは、次の操作を行うことができます。

バックアップ・ファイルを作成するには
1. [バックアップ・ファイルの作成]をクリックします。
   [バックアップの設定]ウィンドウが開きます。
2. ファイルを暗号化する場合は[ファイルの暗号化]をチェックします。
   このオプションを選択した場合、パスワードを入力し、確認用に再度入力する必要があります。
3. バックアップ・ファイルのコメントを入力します（オプション）。
4. [バックアップの作成]をクリックします。
   システム設定がバックアップされます。

バックアップ・ファイルには、ネットワーク設定や DNS 設定など、すべてのシステム設定が記録されます。SIC（Secure Internal Communication）証明書とライセンスもバックアップの対象となります。

アプライアンスを交換する必要がある場合、[ライセンス]ページ→[ライセンスの有効化]から、元のアプライアンスで保存した設定を復元し、ライセンスを再度有効にできます。

既存のアプライアンスを複製する場合は、そのアプライアンスの設定を新しいアプライアンスに復元します。この場合は、新しいアプライアンスの IP アドレスを[デバイス]→[インターネット]ページで変更し、新しいライセンスを生成してください。

定期的なバックアップを FTP サーバに保存するには
1. [デバイス]→[システム操作]→[システム設定のバックアップと復元]に移動します。
2. [設定]をクリックします。
   [定期バックアップの設定]ウィンドウが開きます。
3. [バックアップ・スケジュールを有効にする]をクリックします。
4. ファイル・ストレージの場所を指定します（以下を参照）。
5. オプション：[ファイルの暗号化]を選択します。
   このオプションを選択した場合、パスワードを入力し、確認用に再度入力する必要があります。
6. [定期的バックアップのスケジュール]で頻度を指定します。
   • [毎日] - 時刻を指定します。
   • [毎週] - 曜日と時刻を指定します。
   • [毎月] - 日にちと時刻を指定します。31 日など、ここで指定した日にちがない月は、最後の日にバックアップが行われます。
1. [適用]をクリックします。

ファイル・ストレージの場所を設定するには
1. [デバイス]→[システム操作]→[システム設定のバックアップと復元]にある[設定]をクリックします。
   [定期バックアップの設定]ウィンドウが開きます。
2. [バックアップ・スケジュールを有効にする]をクリックします。
3. [Backup server path]を入力します。
4. ユーザ名とパスワードを入力します。
ローカルとリモート・システム管理者の設定

[デバイス]→[管理者]ページには、Check Point 730/750 Appliance の管理者のリストが表示されます。また、新しいローカル管理者の作成と、セッション・タイムアウト、ログインの失敗回数の設定を行うこともできます。管理者は、リモートの RADIUS サーバで定義することもできます。この場合は、RADIUS サーバで定義した管理者によるアクセスを許可するようアプライアンスを設定します。リモートの RADIUS サーバで定義した管理者の認証は、同じ RADIUS サーバで行います。

読み取り専用の管理者を作成できます。読み取り専用管理者は、アプライアンス設定を更新することはできませんが、それ以外の一部の操作を実行できます。例えば、新しい読み取り専用ユーザを作成したり、[ツール] ページからトラフィックのモニタリング・レポートを実行することが可能です。

Check Point 730/750 Appliance のローカル管理者を作成するには

1. [新規] をクリックします。 [管理者の追加] ページが表示されます。
2. 名前やパスワード、確認用のパスワードなど、ページに表示されているパラメータを設定します。管理者の名前にはハイフン（-）を入れることができます。パスワードや共有キーを入力する際は、{ } [ ] ` ~ | ' " # + の文字は使用できません。
3. 読み取り専用権限を持つ管理者を設定する場合は、[読み取り専用管理者] を選択します。
4. [適用] をクリックします。

管理者の名前と権限情報が、表に追加されます。WebUI ヘログインする際、管理者名と、読み取り/書き込み権限を示すアイコンがページの上部に表示されます。

ローカル定義した管理者の詳細を変更するには

1. 表から管理者を選択し、[編集] をクリックします。
2. 必要な変更を行います。
3. [適用] をクリックします。

ローカルで定義した管理者を削除するには

1. リストから目的の管理者を選択します。
2. [削除] をクリックします。
3. 確認メッセージで [はい] をクリックします。

注 - ログイン中の管理者を削除することはできません。

リモートの RADIUS サーバで定義した管理者によるアクセスを許可するには

1. リモートの RADIUS サーバで管理者を定義します。
2. アプライアンスで RADIUS サーバを定義します。RADIUS サーバが定義されていない場合は、ページ上部の RADIUS サーバの設定リンクをクリックします。 RADIUS サーバが使用している IP アドレスと共有キー情報を設定するよう求められます。
3. 設定済みの RADIUS サーバがある場合は、[権限の編集] をクリックします。
4. [RADIUS 認証を管理者に有効にする] チェック・ボックスをオンにします。
5. 管理者権限を付与する RADIUS サーバ上のユーザ・グループを選択します。
   a) [RADIUS サーバで定義されたすべてのユーザ] を選択するか（お勧めしません）、[特定の RADIUS グループのみ] を選択して必要な RADIUS グループをカンマ区切りで入力します。
   b) 読み取り専用管理者の RADIUS 認証を有効にするには、[読み取り専用管理者] チェックボックスをオンにします。
6. [適用] をクリックします。
ローカル定義とリモート定義の管理者にセッション・タイムアウト値を設定するには
1. [セキュリティ設定]をクリックします。[管理者セキュリティ設定]ウィンドウが開きます。
2. セッション・タイムアウト値（操作しない状態の再長時間）を分単位で設定します。最大値は999分です。
3. ログインの失敗回数を制限するには[管理者ログインの失敗回数を制限]を選択します。
4. [連続したログイン失敗の最大回数]に、ユーザがロックアウトされるまで試行できるログイン回数を入力します。
5. [ロックする時間]に、ロックアウトしてから管理者が再度ログインできるようになるまで待機する時間（秒）を入力します。
6. 管理者パスワードの条件に複雑さを設定する場合はチェックボックスを選択して、パスワードの期限日数を指定します。
7. [適用]をクリックします。

注 - このページには、[デバイス]タブと[ユーザ＆オブジェクト]タブからアクセスできます。

Check Point 730/750 Appliance の非ローカル・ユーザに対する RADIUS サーバの設定
非ローカル・ユーザは、Check Point 730/750 Appliance ではなくRADIUS サーバで定義できます。非ローカル・ユーザがCheck Point 730/750 Appliance にログインすると、RADIUS サーバでユーザが認証されて該当する権限が割り当てられます。非ローカル・ユーザを適切に認証して承認するように、RADIUS サーバを設定する必要があります。

注 - パスワードを空にして RADIUS ユーザを定義すると（RADIUS サーバで）、そのユーザはCheck Point 730/750 Appliance で認証できなくなります。

Check Point 730/750 Appliance の非ローカル・ユーザに Steel-Belted RADIUS サーバを設定するには
1. ディクショナリ・ファイル checkpoint.dct を RADIUS サーバのデフォルトのディクショナリ・ディレクトリ（radius.dct が入っている場所）に作成します。以下の行をファイルに追加します。

```
@radius.dct

MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2 data=%s%]

ATTRIBUTE CP-Gaia-User-Role CheckPoint-VSA(229, string) r
ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-VSA(230, integer) r
```
2. 以下の行を RADIUS サーバの vendor.ini ファイルに追加します（他社製品もあるためファイル内ではアルファベット順にします）。

```
vendor-product = Check Point Check Point 730/750 Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```
3. dictiona.dcm ファイルに次の行を追加します。
```
"@checkpoint.dct"
```
4. この Check Point ベンダー指定の属性を、RADIUS サーバのユーザ設定ファイルのユーザに追加します。
```
CP-Gaia-User-Role = <group_name>
```
<group_name>は、Check Point 730/750 Appliance の WebUI で定義した RADIUS グループの名前です。

Check Point 730/750 Appliance の非ローカル・ユーザに FreeRADIUS サーバを設定するには
1. ディクショナリ・ファイル dictionary.checkpoint を RADIUS サーバの/etc/freeradius/ に作成します。

```
# Check Point dictionary file for freeradius AAA server
# VENDOR CheckPoint 2620
ATTRIBUTE CP-Gaia-User-Role 229 string
# CheckPoint
ATTRIBUTE CP-Gaia-SuperUser-Access 230 integer

2. /etc/freeradius/dictionary に以下の行を追加します。
   "$INCLUDE dictionary.checkpoint"
3. この Check Point ベンダー指定の属性を、RADIUS サーバのユーザ設定ファイルのユーザに追加します。
   CP-Gaia-User-Role = <group_name>
   <group_name>は、Check Point 730/750 Appliance の WebUI で定義した RADIUS グループの名前です。

Check Point 730/750 Appliance の非ローカル・ユーザに OpenRADIUS サーバを設定するには
1. ディクショナリ・ファイル dict.checkpoint を RADIUS サーバの
   /etc/openradius/subdicts/
   に作成します。

```
$add vendor 2620 CheckPoint
$set default vendor=CheckPoint
   space=RAD-VSA-STD
   len_ofs=1 len_size=1 len_adj=0
   val_ofs=2 val_size=-2 val_type=String
   nodec=0 noenc=0
$add attribute 229 CP-Gaia-User-Role
$add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
   val_size=4
```
2. 次の行
   "$include subdicts/dict.checkpoint"
   を以下に追加します。
   /etc/openradius/dictionaries
dict.ascend の直後に追加してください。
3. この Check Point ベンダー指定の属性を、RADIUS サーバのユーザ設定ファイルのユーザに追加します。
アプライアンスの設定

Superuser（スーパーユーザ）としてログインするには
スーパーユーザは、ファイル・システムで Check Point 730/750 Appliance シェルを使い、システムレベルの操作が行える権限を持ちます。
1. SSH クライアントまたはシリアル・コンソール・クライアントを使って Check Point 730/750 Appliance プラットフォームに接続します。
2. ユーザ名とパスワードを使って clish シェルにログインします。
3. Expert を実行します。
エキスパートのパスワードを入力します。

管理者アクセスの設定
[デバイス]→[管理者アクセス]ページでは、管理者が Check Point 730/750 Appliance へのアクセスに使用する IP アドレスとインタフェースの設定を行います。ここでは、Web と SSH ポートの設定も行います。
初めにインタフェースを設定し、そのソースから許可された IP アドレスがアプライアンスにアクセスできるようになります。

管理者アクセスを許可するインタフェース・ソースを設定するには
次の 1 つ以上のオプションを選択します。
- [LAN] - すべての内部物理ポート。
- [トラスト・ワイヤレス] - デフォルトで LAN にアクセス許可されているワイヤレス・ネットワーク（ワイヤレス・ネットワーク・モデルのみ）。
- [VPN] - VPN トンネルを使用して、リモート・サイトまたはリモート・アクセス・クライアントからのトラフィックを暗号化します。
- [インターネット] - インターネットからのトラフィックをクリアします（すべての IP アドレスからのアクセス許可はお勧めしません）。

任意の IP アドレスから管理者アクセスを許可するには
1. [任意の IP アドレス]を選択します。このオプションは安全性を考えるとお勧めできません。インターネットから特定の IP アドレスだけを許可することをお勧めします。
2. 必要に応じて、[Web ポート（HTTPS）]と[SSH ポート]のいずれかまたは両方を変更します。
3. [適用]をクリックします。管理者は、許可されたインタフェース・ソースの任意の IP アドレスを使って Check Point 730/750 Appliance にアクセスできるようになります。

特定の IP アドレスから管理者アクセスを許可するには
1. [特定の IP アドレスのみ]を選択します。
2. [新規]をクリックします。
3. [IPv4 アドレス設定]が表示されます。
3. IPv4 アドレスを以下のいずれかに定義します。
   - IP アドレス - 手動で IP アドレスを入力する、または[コンピュータから IP を取得]をクリックします。
   - 特定のネットワーク - 手動で[ネットワーク IP]と[IP マスク]を入力します。
4. [適用]をクリックします。
アプライアンスの設定

IP アドレスがテーブルに追加されます。
5. 必要に応じて、[Web ポート（HTTPS）]と[SSH ポート]のいずれかまたは両方を変更します。
6. [適用]をクリックします。管理者は、許可されたインタフェース・ソースの指定 IP アドレスを使って Check Point 730/750 Appliance にアクセスできるようになります。

インターネットから特定の IP アドレス/任意の IP アドレスからその他のソースに管理者アクセスを許可するには
インターネットから管理者アクセスを許可するにはこのオプションを選択します（特定の IP アドレスを定義する必要があります）。他のソースが任意の IP アドレスから管理者アクセスをできるようになります。
1. [インターネット]をオンにします。
2. [インターネットからの指定 IP アドレスとインターネット以外からの任意の IP アドレス]オプションを選択します。
3. [新規]をクリックします。
   [IP アドレス設定]が表示されます。
4. IPv4 アドレスを以下のいずれかに定義します。
   - IP アドレス - 手動で IP アドレスを入力する、または [コンピュータから IP を取得]をクリックします。
   - 特定のネットワーク - 手動で [ネットワーク IP]と [IP マスク]を入力します。
5. [適用]をクリックします。
   IP アドレスがテーブルに追加されます。
6. 必要に応じて、[Web ポート（HTTPS）]と[SSH ポート]のいずれかまたは両方を変更します。
7. [適用]をクリックします。管理者は、許可されたインタフェース・ソースの指定 IP アドレスを使って Check Point 730/750 Appliance にアクセスできるようになります。

特定の IP アドレスから管理者アクセスを削除するには
1. IPv4 アドレス・テーブルから削除する IPv4 アドレスを選択します。
2. [削除]をクリックします。

重要な情報:
- インターネット接続がブリッジ・モード（[次からの管理アクセスを許可]オプションでインターネットまたは LAN が表示されない）で設定されている場合、LAN およびインターネットの異なるアクセス権限の設定はサポートされません。
- 自動暗黙ルールは、ここで指定したアクセスを許可するために定義されます。[アクセス・ポリシー]ページで、このアクセスを許可するための明示的なルールを追加する必要はありません。
- 接続中の IP アドレスやインタフェース・グループをブロックする場合には、操作の便宜上、すぐに切断されることはありません。アクセス・ポリシーはすぐに反映されますが、現行セッションはログアウトするまでアクティブな状態になります。

デバイス詳細情報の管理
[デバイス]→ [デバイスの詳細]ページでは、アプライアンスの名前を設定できます。
- この Check Point 730/750 Appliance を識別するための名前を [アプライアンス名]に入力します。
  - アプライアンス名に使用できるのは、英数字とハイフンのみです。
  - ハイフンは、アプライアンス名の先頭と末尾には使用できません。
ワイヤレス・ネットワーク・モデルでは、このページの[国]で国を設定できます。使用できるワイヤレス・ラジオ設定は、各国の規制によって異なります。

**DDNS およびアクセス・サービスの設定**

[デバイス]→[DDNS & デバイス・アクセス]ページでは、次の操作を行うことができます。

- DDNS アカウントの詳細をサポートされているプロバイダで設定する
- NAT で隠れている、ファイアウォールがある、動的 IP アドレスが割り当てられている場合でも、リモートでアプライアンスに接続できるサービスを設定する

**DDNS**

DDNS を設定すると、アプライアンスでプロバイダと IP アドレスがアップデートされます。その後、IP アドレスの代わりにプロバイダから指定されるホスト名を使ってデバイスに接続できるようになります。

これは、VPN でデバイスに接続して内部ネットワークにアクセスするリモート・アクセス・ユーザにとって特に重要です。

**DDNS を設定するには**

1. [インターネットから名前でアプライアンスに接続（DDNS）] を選択します。
2. ページでアカウントの詳細を入力します。
   - プロバイダ - アカウントで設定した DDNS プロバイダを選択します。
   - ユーザ名 - アカウントのユーザ名を入力します。
   - パスワード - アカウントのパスワードを入力します。パスワードや共有キーを入力する際は、{ } [ ] ` ~ | の文字は使用できません。
   - ホスト名 - DDNS アカウントで定義した、ルーティング可能なホスト名を入力します。
   - これらの詳細については、使用しているプロバイダの Web サイトを参照してください。
3. [証明書の再初期化] がオンになっていることを確認します。この機能を有効にするまたは設定を変更した場合は、内部証明書の再初期化を行って新しい DNS に対して有効にする必要があります。

**デバイス・アクセス**

デバイス・アクセスは、インターネット経由でアプライアンスに接続し、必要に応じて WebUI や CLI を使用することができる機能です。これは、Check Point Cloud Service を使って管理 UI や CLI 接続を通じてトンネリングすることで実現します。アプライアンスが NAT で隠れている、ファイアウォールがある、直接接続できない場合などに便利な設定です。また、動的 IP アドレスが割り当てられているアプライアンスへのアクセスしやすいという点でも有効です。
# アプライアンスの設定

## 機能の仕組み

<table>
<thead>
<tr>
<th>番号</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check Point 730/750 Appliance を Check Point クラウド・サービスに登録 - [デバイス]→ [DDNS &amp; デバイス・アクセス]ページに初回アクセスすると、アプライアンスを登録するリンクが表示されます。以下の手順でアプライアンスをサービスに登録します。</td>
</tr>
</tbody>
</table>
| 2 | 登録完了後、使用中の Check Point クラウド・サービスへのトンネルがアプライアンスの IP アドレスで確立されます。WebUI の[デバイス]→[DDNS & デバイス・アクセス]ページで、以下が表示されます。- 検証トークン - ホスト名が有効かどうかを確認するために入力するトークン。このトークンは既存の名前がアプライアンスの所有者に属しているかどうかを検証するために使われます。
- Web リンク - ブラウザからこのリンク先にアクセスしてアプライアンスに接続します。
  例: https://mygateway-web.smbrelay.checkpoint.com
  ログイン・ページが表示されたら、アプライアンスのユーザ名とパスワードを入力します。
- シェル・リンク - CLI コマンドを使うために、ブラウザからこのリンク先にアクセスしてアプライアンスへの SSH 接続を開きます。
  例: https://mygateway-shell.smbrelay.checkpoint.com
  管理者の認証情報を入力します。 |
| 3 | 管理者が WebUI や CLI にアクセスすると、URL をブラウザに入力し、クラウドの Web Service を経由します。 |
| 4 | 管理者は確立されたパイプを経由し、Check Point クラウド・サービスからアプライアンスの WebUI や CLI へアクセスできるようになります。 |
インターネットからアプライアンスへ接続できない状況で、接続するために登録するには

1. ［登録］をクリックします。
   ［デバイス・アクセス］ウィンドウが開きます。
2. ［ホスト名］で、このCheck Point 730/750 Applianceの名前を入力、またはデフォルトのホスト名を使用してリモート・アクセスを有効にします。
3. ホスト名がすでに定義されている場合は、［既存のホスト名で登録］を選択してゲートウェイの検証トークンを入力します。
4. ［適用］をクリックします。
   検証トーク、Web リンク、シェル・リンクが［DDNS &アプライアンス・アクセス］ページに表示されます。
5. ［デバイス］→［管理者アクセス］ページで、インターネットを管理者アクセスの発信元に設定して、特定の IP アドレスを指定してください。

日付と時刻の設定の管理

［デバイス］→［日付と時刻］ページには、現在のシステム時刻が表示され、Check Point 730/750 Appliance の日付と時刻を設定できます。オプションで NTP を使用することもできます。

手動で日付と時刻を設定するには

1. ［日付と時刻を手動で設定］オプションを選択します。
2. 現在の日付と時刻を入力します。日付を入力するにはカレンダーのアイコンをクリックします。時刻は午前か午後かを指定します。
3. ［適用］をクリックします。

NTP (Network Time Protocol) を使用してネットワーク上のコンピュータの時刻を同期化するには

1. ［Network Time Protocol（NTP）サーバを使って日付と時刻を設定］オプションを選択します。
2. ［プライマリ NTP サーバとセカンダリ NTP サーバ］に各 NTP サーバのホスト名または IP アドレスを入力します。プライマリ NTP サーバが応答しない場合、セカンダリ NTP サーバに対して照会が行われます。
3. ［アップデート間隔（分）］フィールドを設定します。
4. 共有の秘密キーと共有秘密キーの識別子を指定する場合は、［NTP 認証］チェック・ボックスをオンにします（オプション）。パスワードや共有キーを入力する際は、{ } ] ` ~ | ' " # + の文字は使用できません。
5. ［適用］をクリックします。

タイムゾーン

1. ［ローカル・タイムゾーン］リストから適切なタイムゾーン・オプションを選択します。
2. 自動的に夏時間の調整を行う場合は、［システム クロックを自動調整して夏時間の変更に合わせる］チェック・ボックスをオンにします。
3. ［適用］ボタンをクリックします。

システム・ツールの使用

「システム・ツールの使用」（28ページ）を参照してください。
ハイ・アベイラビリティの設定

[デバイス]→[ハイ・アベイラビリティ]ページでは、高可用性向けに2台のCheck Point 730/750 Applianceのクラスタを作成できます。

注 - 製品のネットワーク設定でスイッチ/ブリッジが定義されている場合は、クラスタを作成することができません。必要であれば、[デバイス]→[ローカル・ネットワーク]ページでネットワーク設定を変更してください。

クラスタを定義した後、クラスタを有効または無効にすることができます。

ページでは、表にモニタリング設定のインタフェースやハイ・アベイラビリティが有効になったインタフェースが表示され、編集することができます。

クラスタ・メンバの設定の詳細を変更する場合は、[トラストの再初期化]をクリックしてメンバ間の信頼を再度確立させます。

[クラスタ設定のリセット] - それまでの設定をすべて削除します。クラスタを有効にするには、ウィザードを再度実行する必要があります。

[メンバのダウンを強制] - もう一方のメンバにフェイルオーバーさせる必要がある場合はこのオプションを使用します。たとえば、もう一方のメンバの機能性をテストする場合などがあげられます。

トラブルシューティングの場合は、[診断]ボタンをクリックして、クラスタの現状に関する詳細情報を確認できます。

クラスタを作成するには

1. [クラスタの設定]をクリックします。
   新規クラスタウィザードが開きます。
2. 手順1: [ゲートウェイ優先度]で、次のオプションのいずれかを選択します。
   • [プライマリ・メンバとして設定] - このアプライアンスを最初に設定したい場合。
   • [セカンダリ・メンバとして設定] - プライマリ・メンバがすでに設定されていて、このアプライアンスをそのプライマリに接続する場合。
3. [次へ]をクリックします。
4. プライマリ・メンバの場合:
   a) 手順2: [SIC設定]でパスワードを入力し、確認のためもう一度同じパスワードを入力します。このパスワードは、メンバ間の信頼性を確立するために使われます。パスワードや共有キーを入力する際は、{ } ~ | " # + の文字は使用できません。
      注 - ここで変更した設定が、もう一方のクラスタ・メンバにも反映されていることを確認してください。
   c) [次へ]をクリックします。
   d) 手順3: [ゲートウェイ・インタフェース（1/N）]では、目的のインタフェースにクラスタIPを定義できます。必要な詳細情報を入力します。
      デフォルトでは、インタフェースでハイ・アベイラビリティが有効かどうかの状態をアプライアンスでモニタリングし、障害が起きた場合に2つ目のクラスタ・メンバに自動的にフェイル・オーバーします。インタフェースでハイ・アベイラビリティが無効になっている場合は、モニタリングするかどうかを選択することができます。
e) [次へ]をクリックします。ネットワーク上の該当するすべてのインタフェースに対して、「手順 d.」を繰り返します。

注 - インターネット接続については、静的 IP インターネット接続にのみハイ・アベイラビリティを有効にできます。それ以外のインターネット接続は、モニタリングのみ可能です。

5. セカンダリ・メンバの場合:
   a) 手順 2: SIC 設定で、Secure Internal Communication のパスワードを入力します。
   b) [トラスト接続の確立]をクリックします。

6. [完了]をクリックします。
   クラスタが正しく設定されると、メンバのステータスがこのページに表示されます。
   クラスタを設定した後、クラスタ IP アドレスにアクセスすると、自動的にアクティブなクラスタ・メンバにリダイレクトされるようになります。特定のメンバにログインする場合は、そのメンバの IP アドレスにログインする必要があります。
   セカンダリ・メンバ（スタンバイ・メンバ）の WebUI には、微調整が可能なオプションのみがあります。これは、すべてのクラスタ管理がアクティブ・メンバから行われるためです。

詳細設定の設定

[デバイス]→[詳細設定]ページは、上級管理者またはチェック・ポイント・サポートが使用します。さまざまな Software Blade に対して複数の詳細設定の値を指定できます。

重要 - 正しい知識を持たずに詳細設定を変更すると、この製品の安定性やセキュリティの安全性、パフォーマンスに悪影響を及ぼす恐れがあります。必要な変更について正しい理解がある場合のみ、操作を行うようにしてください。

属性に関する詳細については、必要に応じて Check Point サポートにお問い合わせください。
属性のリストを絞り込むには
1. [入力して絞り込み]フィールドにテキストを入力します。
   入力していくと動的に検索結果が表示されていきます。
2. 絞り込みをキャンセルするには、検索文字列の横にある「X」をクリックします。

アプライアンス属性を設定するには
1. 属性を選択します。
2. [編集]をクリックします。
   [属性]ウィンドウが表示されます。
3. 各種設定を行うか、[デフォルトに戻す]をクリックして属性をデフォルト設定に戻します。属性の詳細については、次節のセクションを参照してください。
4. [適用]ボタンをクリックします。
   アプライアンスの属性が設定されます。

アプライアンスの属性をすべてデフォルトの設定にリセットするには
1. [詳細設定]ウィンドウから、[デフォルトに戻す]をクリックします。
   [確認]ウィンドウが開きます。
2. [はい]をクリックします。
   すべてのアプライアンス属性がデフォルトの設定にリセットされます。

アグレッシブ・エージング

<table>
<thead>
<tr>
<th>アグレッシブ・エージング属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>複数のパラメータ</td>
<td>アグレッシブ・エージングにより、ファイアウォールの接続テーブル容量およびメモリ消費を管理し耐久性と安定性を高めることができます。</td>
</tr>
<tr>
<td></td>
<td>アグレッシブ・エージングにより、アグレッシブ・タイムアウトと呼ばれる一連の新しいショート・タイムアウトが導入されます。接続がアグレッシブ・タイムアウトを超えてアイドリングすると、&quot;eligible for deletion（削除対象）&quot;とマークされます。接続テーブルまたはメモリ消費がユーザ定義のしきい値に達すると、メモリ消費または接続容量が望ましいレベルに戻るまでアグレッシブ・エージングによって&quot;削除対象&quot;接続が削除されます。</td>
</tr>
<tr>
<td></td>
<td>アグレッシブ・エージングによりゲートウェイ・マシンは、特にサービス拒否攻撃による大量の予期しないトラフィックを処理できるようになります。</td>
</tr>
<tr>
<td></td>
<td>定義したしきい値を超えると、外部から接続があるたびに、削除対象リストから接続が10件ずつ削除されます。メモリ消費または接続容量が設定した制限を下回るまで、新たな接続があることに10件の接続が削除されています。削除対象&quot;接続がない場合、その時点では接続は削除されませんが、その後しきい値を超える接続がある度にリストがチェックされます。</td>
</tr>
<tr>
<td></td>
<td>タイムアウト設定はメモリ消費の重要な設定項目です。タイムアウト値を低くすると、接続がテーブルから削除されるタイミングが早まり、ファイアウォールがより多くの接続を同時に処理できるようになります。メモリ消費がしきい値を超えているときは、大量のトラフィックの接続性を維持できるようにタイムアウトを短くするのが最善の方法です。</td>
</tr>
<tr>
<td></td>
<td>マシンに利用可能なメモリがまだあり接続テーブルが満杯になっていない段階で作業を開始する点がアグレッシブ・エージングの大きな利点です。これにより、リソースが乏しい状況で発生しがちな接続性の問題の可能性を低く抑えることが可能です。</td>
</tr>
</tbody>
</table>
アプライアンスの設定

### アグレッシブ・エージング属性

<table>
<thead>
<tr>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>アグレッシブ・エージングを設定するには</td>
</tr>
<tr>
<td>1. [アプライアンスの負荷時は接続のアグレッシブエージングを有効] を選択します。</td>
</tr>
<tr>
<td>2. アグレッシブ・エージング・イベントを記録するには、[アグレッシブ・エージング・イベントのログ記録] を選択します。IPS Blade の [ログ＆モニタリング] → [セキュリティログ] にログが表示されます。</td>
</tr>
<tr>
<td>3. 実行する [アグレッシブ・エージング・タイムアウト] の各チェックボックスを選択してアグレッシブ・エージング・タイムアウトを入力します。アグレッシブ・タイムアウトがデフォルトのタイムアウトより短いことを確認します。デフォルトのタイムアウトは、[デバイス] → [詳細設定] → [ステートフル・インスペクション] の属性で確認および設定できます。</td>
</tr>
<tr>
<td>アグレッシブ・エージング・タイムアウトを実行するタイミングを設定するには</td>
</tr>
<tr>
<td>1. [Aggressive Aging Timeout are enforced when] (アグレッシブ・タイムアウトを実行する条件) セクションで、接続テーブルが制限を超えるか、メモリが制限を超えるか、またはその両方が制限を超えたときに実行するのを選択します。</td>
</tr>
<tr>
<td>2. 接続テーブルまたはメモリ消費の限界を定義するパーセンテージを入力します。両方を選択した場合は、その他オプションのパーセンテージ・フィールドの値が適用されます。デフォルト値は 80% で、接続テーブルまたはメモリ消費がこの制限を超えると &quot;削除対象&quot; リストから接続が削除されます。</td>
</tr>
</tbody>
</table>

### アンチスパムポリシー

<table>
<thead>
<tr>
<th>アンチスパムポリシーの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>すべてのメールを追跡</td>
<td>スパムまたはスパムの疑いがあると見なされていない E メールを追跡するオプションです。このような電子メールを追跡するとパフォーマンスに影響することがあります。</td>
</tr>
<tr>
<td>許可されたメールを追跡</td>
<td>[警戒対策] → [アンチスパム例外] ページで手動で許可された電子メールを追跡するオプションです。</td>
</tr>
<tr>
<td>コンテンツ・ベースのアンチスパムタイムアウト</td>
<td>コンテンツ・ベースのアンチスパムインスペクション中にクラウドからの応答を待つタイムアウト（秒）を表示します。</td>
</tr>
<tr>
<td>E メール・サイズ・スキャン</td>
<td>スキャンする E メールのコンテンツの最大サイズ（KB）を表示します。</td>
</tr>
<tr>
<td>IP レビュテーション・フェイル・オープン</td>
<td>アンチスパム IP レビュテーション・テスト中に内部エラーが発生したときに行うアクションを表示します。</td>
</tr>
<tr>
<td>IP レビュテーション・タイムアウト</td>
<td>IP レビュテーション・テストの結果を待つタイムアウト（秒）時間を表示します。</td>
</tr>
<tr>
<td>透過型プロキシ</td>
<td>検査済みの E メール接続に透過型プロキシを使用します。無効にすると、クライアント・マシンでのプロキシ・アドレスおよびポートの設定が必要になります。</td>
</tr>
</tbody>
</table>

Check Point 730/750 Appliance Locally Managed Administration Guide R77.20.15 | 61
アンチスプーフィング

<table>
<thead>
<tr>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>グローバル・アンチスプーフィングを有効にする</td>
</tr>
</tbody>
</table>

アプリケーション・コントロール & URL フィルタリング

<table>
<thead>
<tr>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>サービスが利用できない場合はブロック</td>
</tr>
<tr>
<td>キャッシュおよび変換されたページを分類</td>
</tr>
<tr>
<td>セーフ・サーチの強制</td>
</tr>
<tr>
<td>フェイル・モード</td>
</tr>
<tr>
<td>参照時間の追跡</td>
</tr>
<tr>
<td>HTTP 参照元ヘッダの使用</td>
</tr>
<tr>
<td>Web サイト分類モード</td>
</tr>
</tbody>
</table>

容量の最適化

<table>
<thead>
<tr>
<th>容量の最適化の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>接続ハッシュ・テーブル・サイズ</td>
<td>接続ハッシュ・テーブルのサイズをバイト単位で表示します。この値は整数かつ 2 のべき乗の指数で最大同時接続数の約 4 倍になります。</td>
</tr>
<tr>
<td>容量の最適化の属性</td>
<td>説明</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>最大同時接続数</td>
<td>全体的な同時接続の最大数を表示します。</td>
</tr>
</tbody>
</table>

### クラウド・サービス・ファームウェアのアップグレード

<table>
<thead>
<tr>
<th>クラウド・サービス・ファームウェアのアップグレードの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>サービスアクセスの最大リトライ回数</td>
<td>サービスを使用したアップグレードに失敗した場合の最大リトライ回数を表示します。</td>
</tr>
<tr>
<td>リトライまでのサービスアクセスタイムアウト</td>
<td>サービスへの接続に失敗したときのリトライまでの待ち時間（秒）を入力します。</td>
</tr>
</tbody>
</table>

### クラスタ

<table>
<thead>
<tr>
<th>クラスタの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>仮想MACの使用</td>
<td>ネットワークの切り替えによるすばやいフェイルオーバーを可能にするためすべてのメンバが仮想MACアドレスを使用するかどうかを表示します。 仮想MACアドレスを使用することにより  • フェイルオーバー中にトラフィックが途絶する可能性を最小化します。 • NATed IPアドレスにG-ARPを使用する必要がなくなる</td>
</tr>
</tbody>
</table>

### DHCP リレー

<table>
<thead>
<tr>
<th>DHCP リレーの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>内部IPアドレスをソースとして使用する</td>
<td>アプライアンスからのDHCPリレー・パケットが内部IPアドレス由来の場合は、[内部IPアドレスをソースとして使用する]を選択します。これはDHCPサーバがリモートVPNサイトの背後にある場合に必要となることがあります</td>
</tr>
</tbody>
</table>

### 一般テンポラリ・ディレクトリ・サイズ

<table>
<thead>
<tr>
<th>一般テンポラリ・ディレクトリ・サイズの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般テンポラリ・ディレクトリ・サイズ</td>
<td>一般テンポラリ・ディレクトリのサイズ（MB）を制御します。</td>
</tr>
<tr>
<td>システム・テンポラリ・ディレクトリ・サイズ</td>
<td>システムが使用するテンポラリ・ディレクトリのサイズ（MB）を制御します。</td>
</tr>
</tbody>
</table>
### ハードウェア・オプション

<table>
<thead>
<tr>
<th>ハードウェア・オプションの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>工場出荷時のタイムアウトに戻す</td>
<td>工場出荷時のデフォルトのイメージを復元するには、アプライアンスのバック・パネルの工場出荷時設定ボタンをこの時間（秒）だけ押し続ける必要があります。</td>
</tr>
</tbody>
</table>

### ホットスポット

<table>
<thead>
<tr>
<th>ホットスポットの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ポータルを有効にする</td>
<td>[無効]を選択するとホットスポット機能が完全に無効になります。</td>
</tr>
</tbody>
</table>

### IP フラグメント・パラメータ

<table>
<thead>
<tr>
<th>IP フラグメント・パラメータの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>複数のパラメータ</td>
<td>これらのパラメータでアプライアンスがIPフラグメントを処理する方法を設定できます。フラグメント化IPパケットをブロックするか、または設定した閾値に達したときフラグメントをドロップすることができます。以下のいずれかのオプションを選択します。</td>
</tr>
<tr>
<td>• IPフラグメントを禁止する</td>
<td>フラグメント化IPパケットをドロップします。</td>
</tr>
<tr>
<td>• IPフラグメントを許可する</td>
<td>設定した閾値を超えていなければフラグメント化IPパケットを許可します。このオプションを選択した場合、容認する不完全パケットの最大数を設定できます。また、整合していないフラグメント化パッケージをドロップする前に保持するタイムアウト（秒）も設定できます。</td>
</tr>
</tbody>
</table>

### IPS 追加パラメータ

<table>
<thead>
<tr>
<th>IPS 追加パラメータの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>最大 ping</td>
<td>&quot;最大Pingサイズ&quot;保護が有効になったときに許可される最大Pingパケット・サイズを表示します。</td>
</tr>
<tr>
<td>IPS エンジン設定の属性</td>
<td>説明</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>サポートされる Web 保護のエラー・ページ・オプションを設定する - 複数のパラメータ</td>
<td>一部の Web ベースの保護は検出に関するエラー・ページを表示します。このエラー・ページは設定可能です。次のエラー・ページがサポートされます。</td>
</tr>
<tr>
<td></td>
<td>• マルシャス・コード・ブロック</td>
</tr>
<tr>
<td></td>
<td>• クロスサイト・スクリプティング</td>
</tr>
<tr>
<td></td>
<td>• LDAP インジェクション</td>
</tr>
<tr>
<td></td>
<td>• SQL インジェクション</td>
</tr>
<tr>
<td></td>
<td>• コマンド・インジェクション</td>
</tr>
<tr>
<td></td>
<td>• ディレクトリ・トラバーサル</td>
</tr>
<tr>
<td></td>
<td>• ディレクトリ・リスティング</td>
</tr>
<tr>
<td></td>
<td>• エラー・コンシールメント</td>
</tr>
<tr>
<td></td>
<td>• HTTP フォーマット・サイズ</td>
</tr>
<tr>
<td></td>
<td>• ASCII オンリー・リクエスト</td>
</tr>
<tr>
<td></td>
<td>• ASCII オンリー・レスポンス・ヘッダ</td>
</tr>
<tr>
<td></td>
<td>• HTTP メソッド</td>
</tr>
<tr>
<td></td>
<td>これらのオプションからすべての保護に適用するオプションをひとつ選択します。</td>
</tr>
<tr>
<td></td>
<td>• 表示しない</td>
</tr>
<tr>
<td></td>
<td>• [事前定義済み HTML エラー・ページを表示する] - 攻撃を検出したときに開く HTML ページを設定できます。ページを設定するには、[詳細設定]→[IPS エンジン設定]→[HTML エラー・ページ設定]に移動します。</td>
</tr>
<tr>
<td></td>
<td>• [別の URL にリダイレクトする] - 攻撃を検出したときにユーザをリダイレクトする URL を入力します。検出した攻撃の詳細な情報を提供するエラー・コードを追加することもできます。ただし、情報が攻撃者によって悪用される可能性があるため推奨されません。</td>
</tr>
<tr>
<td>HTML エラー・ページ設定 - 複数のパラメータ</td>
<td>これらの設定により、エラー・ページ詳細設定が[事前定義済み HTML エラー・ページを表示する]に設定されたとき表示される事前定義済み HTML エラー・ページを設定することができます。以下のいずれかのオプションを選択します。</td>
</tr>
<tr>
<td></td>
<td>• ロゴ URL - 必要に応じて会社のロゴがある URL を入力します。</td>
</tr>
<tr>
<td></td>
<td>• HTML エラー・ページ設定 - 検出した攻撃に関する詳細情報を提供するエラー・コードを表示します。ただし、情報が攻撃者によって悪用される可能性があるため推奨されません。</td>
</tr>
<tr>
<td></td>
<td>• 詳細なエラー・コードを送信する - HTML ページに表示する手動で定義したテキストを入力します。テキストを説明ボックスに入力します。たとえば、IPS ポリシー違反によるアクセス拒否などと入力します。</td>
</tr>
</tbody>
</table>
### 管理されたサービス

<table>
<thead>
<tr>
<th>管理されたサービスの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理者のリモート管理サーバからのシームレスなアクセスを許可します。</td>
<td>管理者が管理者ユーザ名とパスワードを入力せずにリモート Security Management サーバからアプライアンスにアクセスできるかどうかを表示します。</td>
</tr>
<tr>
<td>ログイン時にデバイス詳細を表示する</td>
<td>管理者がアプライアンスにアクセスしたときアプライアンスの詳細を表示するかどうかを表示します。</td>
</tr>
</tbody>
</table>

### NAT

<table>
<thead>
<tr>
<th>NAT の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP 手動ファイル・マージ</td>
<td>自動 ARP 検出を有効にしたとき、より高い優先度でローカル・ファイル内の ARP 定義を使用するかどうかを表示します。手動設定の NATルールには手動ブロック ARP設定が必要です。手動設定されたNAT設定が有効である場合は、両方の定義を管理します。これらの定義が競合する（両方に同じ NAT IPアドレスが使用される）場合は、手動設定が優先されます。</td>
</tr>
<tr>
<td>複数のパラメータ - IPプール NAT</td>
<td>IPプールは、ゲートウェイがルーティングできるIPアドレス（アドレス範囲、それらのオブジェクトのひとつつのネットワークまたはグループ）の範囲です。サーバへの接続が開かれると、ゲートウェイはソースIPアドレスの代わりにIPプールからIPアドレスを使用します。サーバからのリプライ・パケットがゲートウェイに返されるときは、元のソースIPアドレスが復元されてからパケットがソースに転送されます。IPプールを使用する場合は、既存のIPアドレス範囲オブジェクトを選択します。ただし、[ユーザ&amp;オブジェクト]→[ネットワーク・オブジェクト]ページで事前に定義する必要があります。IPプール NATメカニズムにより、この範囲からIPアドレスの割り当てが行われます。</td>
</tr>
</tbody>
</table>

VPNクライアント接続にIPプール NATを使用 - VPNリモート・アクセス・クライアントからゲートウェイへの接続に適用します。

IPプール NATをゲートウェイ間の接続に使用 - サイト間のVPN接続に適用します。

Hide NATよりIPプール NATを優先 - 両者が同じ接続をマッチしたときIPプール NATがHide NATより優先するように指定します。IPプールが使い尽くされている場合は、Hide NATのみが適用されます。

プールのIPアドレスを別のが宛先に再利用 - 異なる宛先にはプールからIPアドレスを再利用するには、このオプションを選択します。

未使用アドレスの間隔 - 使用されていないアドレスをIPアドレス・プールに戻すまでの間隔を分単位で指定します。

アドレス枯渇の追跡 - IPプールの尽きたときに発行するログのタイプを指定します。

アドレスの割り当てと解放の追跡 - IPプールからのIPアドレスの各割り当ておよび解放を記録するかどうかを指定します。
### NAT の属性

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>自動 ARP 検出</td>
<td>ローカル・ネットワーク内の内部デバイスが静的 NAT を使用して定義されている場合、アプライアンスは静的 NAT IP アドレス宛のパケットをそれぞれのデバイスに渡す必要があります。このオプションにより、アプライアンスはそれらの IP アドレスの ARP リクエストに自動的に応答するようになります。</td>
</tr>
<tr>
<td>Hide NAT の容量を増やす</td>
<td>Hide NAT 容量に追加容量を加えるかどうかを表示します。</td>
</tr>
<tr>
<td>NAT 有効</td>
<td>デバイスの NAT 機能が有効かどうかを表示します。</td>
</tr>
<tr>
<td>NAT のキャッシュの期限</td>
<td>NAT キャッシュ・エントリの有効期限を分単位で表示します。</td>
</tr>
<tr>
<td>NAT キャッシュのエントリ数</td>
<td>NAT キャッシュ・エントリの最大数を表示します。</td>
</tr>
<tr>
<td>NAT ハッシュ・サイズ</td>
<td>NAT テーブルのハッシュ・バケット・サイズを表示します。</td>
</tr>
<tr>
<td>NAT 制限</td>
<td>NAT による接続の最大数を表示します。</td>
</tr>
<tr>
<td>クラスタ非表示フォールドを実行</td>
<td>該当する場合、ローカル IP アドレスをクラスタ IP アドレスで隠すか、または逆に各クラスタ・メンバの物理 IP アドレスを隠すのかを表示します。</td>
</tr>
<tr>
<td>クライアント側の宛先を変換</td>
<td>宛先 IP アドレスをクライアント側で変換します（NAT ルールを自動生成する場合）。</td>
</tr>
<tr>
<td>クライアント側で宛先を変換（手動ルール）</td>
<td>宛先 IP アドレスをクライアント側で変換します（NAT ルールを手動で設定している場合）。</td>
</tr>
</tbody>
</table>

### QoS Blade

<table>
<thead>
<tr>
<th>QoS Blade の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ログ記録</td>
<td>QoS Blade が有効なとき、アプライアンスが QoS イベントを記録するかどうかを表示します。</td>
</tr>
</tbody>
</table>

### デバイス・アクセス

<table>
<thead>
<tr>
<th>デバイス・アクセスの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL 証明書を無視する</td>
<td>アクセス・サービスの実行中は SSL 証明書を無視するかどうかを表示します。</td>
</tr>
<tr>
<td>サーバ・アドレス</td>
<td>NAT に隠れている場合でもインターネットからアプライアンスへの管理者アクセスを許可するリモート・サーバのアドレスを表示します。</td>
</tr>
</tbody>
</table>
シリアル・ポート

<table>
<thead>
<tr>
<th>シリアル・ポートの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>複数のパラメータ</td>
<td>シリアル・ポートのパラメータで、アプライアンスの背面パネルのコンソール・ポートを設定できます。必要な場合は完全に無効にでき(シリアル・ポートを有効にする]チェックボックスをオフ)、ポート・スピードと[フロー制御]を設定します。これらの設定は、コンソール・ポートに接続されているデバイスの設定と一致している必要があります。このポートのモードは3 種類あります。</td>
</tr>
</tbody>
</table>

- コンソール - デフォルトで設定されているモードです。ポートはアプリアンスのコンソールへアクセスするために使用されます。
- アクティブ - ポートからアプリアンスのコンソールに接続するのではなく、データは指定されたTelnetサーバをリレーします。Telnetサーバはこのポートから確認できます。TelnetサーバのIP アドレスを入力します。2つの異なるIP サーバのIP アドレスを設定できます（プライマリ・サーバとセカンダリ・サーバ）。
- パッシブ - このモードでは、データのフローが予約されてアプリアンスはシリアル・ポートを経由して接続デバイスのコンソールにアクセスします。このコンソールは、Telnet接続からアプリアンスの設定したポートを経由してアクセスできます。[Listen on TPC port]にポート番号を入力します。

任意の発信元からこのポートへのトラフィックを許可する暗黙ルールを設定するには、[Implicitly allow traffic to this port]がオンになっていることを確認します。暗黙ルールを作成しない場合は、ファイアウォール・ルールベースで手動で定義する必要があります。

2つのアプリアンスのうち、1台がアクティブ・モードでもう1台がパッシブ・モードの場合、クライアントは、Telnet接続を使ったインターネットで、リモートからアプリアンスに接続されたコンソールにアクセスできます。

ステートフル・インスペクション

<table>
<thead>
<tr>
<th>ステートフル・インスペクションの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ステータスから外れたTCPパケットを許可する</td>
<td>TCP接続の現在のステータスと一致しないTCPパケットをドロップするか(0に設定されている場合)、許可するか(0以外の値に設定されている場合)を表示します。</td>
</tr>
<tr>
<td>ステートフルICMPエラーを許可する</td>
<td>ルールベースによって許可された非ICMP接続(継続中のTCPまたはUDP接続など)を参照するICMPエラー・パケットを許可します。</td>
</tr>
<tr>
<td>ステートフルICMPリプライを許可する</td>
<td>ルールベースによって許可されたICMPリクエストに対するICMPリプライ・パケットを許可します。</td>
</tr>
<tr>
<td>不明なサービスに対するステートフルUDPリプライを許可する</td>
<td>不明なサービスに対するステートフルUDPリプライを許可するかどうかを指定します。各UDPサービス・オブジェクトに対して、サービスがトラフィックを許可するルールに合致する場合、それに対するUDPリプライを許可するかどうかを設定できます。このパラメータはサービス・オブジェクトが対象としないすべての接続を参照します。</td>
</tr>
<tr>
<td>アプライアンスの設定</td>
<td>説明</td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>不明なサービスに対するその他のステートフルIPプロトコルを許可する</td>
<td>不明なサービスに対するその他のステートフルIPプロトコルを許可します。各サービス・オブジェクトについて、サービスがトラフィックを許可するルールに合致する場合に、それに対するリプレイを許可するかどうかを設定できます。このパラメータはサービス・オブジェクトが対象としないすべての非UDP/TCP接続を参照します。</td>
</tr>
<tr>
<td>LAN-DMZ DPIを許可する</td>
<td>内部ネットワークとDMZネットワーク間のトラフィックでのディープ・パケット・インスペクションを許可します。</td>
</tr>
<tr>
<td>LAN-LAN DPIを許可する</td>
<td>内部ネットワーク間のトラフィックでのディープ・パケット・インスペクションを許可します。</td>
</tr>
<tr>
<td>ステータスから外れたICMPパケットをドロップする</td>
<td>&quot;バーチャル・セッション&quot;に関連しないICMPパケットをドロップします。</td>
</tr>
<tr>
<td>ICMPパーサーチャル・セッションのタイムアウト</td>
<td>この時間（秒）を過ぎたICMP仮想セッションはタイムアウトしたとみなされます。</td>
</tr>
<tr>
<td>ステータスから外れたICMPパケットを記録する</td>
<td>ステータスから外れたICMPパケットを記録するかどうかを表示します。&quot;ステータスから外れたICMPパケットをドロップする&quot;パラメータを参照してください。</td>
</tr>
<tr>
<td>ステータスから外れたTCPパケットを記録する</td>
<td>ステータスから外れたTCPパケットを記録するかどうかを表示します。&quot;ステータスから外れたTCPパケットをドロップする&quot;パラメータを参照してください。</td>
</tr>
<tr>
<td>他のIPプロトコルのバーチャル・セッションのタイムアウト</td>
<td>この時間（秒）を過ぎたTCP、UDPまたはICMP以外の仮想セッションはタイムアウトしたと見なされます。</td>
</tr>
<tr>
<td>TCPエンド・タイムアウト</td>
<td>TCPセッション終了のタイムアウト（秒）時間を表示します。2個または各方向に1つのFINパケットまたはRSTパケットの後、TCPセッションは「終了」したものと見なされます。</td>
</tr>
<tr>
<td>TCPセッション・タイムアウト</td>
<td>TCPセッションのタイムアウト（秒）時間のを表示します。この時間（秒）以上にアイドリングが続いたTCPセッションはタイムアウトします。</td>
</tr>
<tr>
<td>TCPスタート・タイムアウト</td>
<td>TCPセッション開始のタイムアウト（秒）時間を表示します。最初のパケットの到着から接続（TCP 3方向ハンドシェイク）が確立されるまでの間隔がこの時間（秒）を超えると、TCP接続はタイムアウトします。</td>
</tr>
<tr>
<td>UDP仮想セッションのタイムアウト</td>
<td>この時間（秒）を過ぎたUDP仮想セッションはタイムアウトしたと見なされます。</td>
</tr>
</tbody>
</table>
ストリーミング・エンジン設定

### ストリーミング・エンジン設定の属性

<table>
<thead>
<tr>
<th>複数のパラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>これらの設定では、様々な詳細インスペクションのブレード（IPS、アプリケーション・コントロール、アンチウイルスなど）で使用する TCP ストリーミング・エンジンがストリーミング・エンジンによるインスペクションを妨げるプロトコル違反やイベントをどのように処理するかを決定します。</td>
<td></td>
</tr>
<tr>
<td>これらの設定は常にブロック・モードにしておくことを強く推奨します。これらの設定を検出モードで使用すると、イベントまたは違反が発生するとインスペクションが停止し、セキュリティが大幅に低下することがあります。</td>
<td></td>
</tr>
<tr>
<td>この設定がこのようなイベントを記録するように設定されている場合、IPS Blade の[ログ &amp; モニタリング]→[セキュリティ・ログ]にログが表示されます。</td>
<td></td>
</tr>
<tr>
<td>各違反またはイベントについては、アクションおよび追跡モードで設定します。</td>
<td></td>
</tr>
</tbody>
</table>

| TCP セグメント制限実施 | ゲートウェイを通す TCP セグメントについて、ゲートウェイはセグメント受信通知を受けるまでセグメントのコピーを保持します。これによりバッファされたデータはゲートウェイのメモリを占有します。このパラメータはバッファするセグメントの数とサイズを接続ごとに制限します。接続がこれらの制限のいずれかに達すると、ゲートウェイはバッファされたセグメントが認知されるまでその接続の新たなセグメントを受け付けなくなります。 |

| TCP シーケンス外 | TCP セグメントの受信ホストはセグメントをバッファリングし、指定のウィンドウ内でそれらのセグメントのみを保持します。このウィンドウの外のセグメントは受信ホストによる処理を受けません。TCP 受信ウィンドウの外にある TCP セグメントはゲートウェイ上で処理すべきではありません。ウィンドウの外にある TCP セグメントのすべてのデータはドロップまたは削除されます。セグメントがウィンドウに近い場合、データは取り除かれます。セグメントがウィンドウから離れれている場合は、データはドロップされます。 |

| TCP 無効な再送 | ゲートウェイを通す TCP セグメントについて、ゲートウェイはセグメント受信通知を受けるまでセグメントのコピーを保持します。通知の受信がない場合、ソース・マシンはセグメントを再送信し、ゲートウェイがコピーと比較して新しいパケットが元のパケットと一致しているか確認します。元のセグメントと一致しない再送信を通すことにより、未検査データを目的のアプリケーションに届けることができます。これにより、元のセグメントと異なるセグメントの再送信がブロックされ、ゲートウェイが受信側アプリケーションで処理されるすべてのデータを検査できるようになります。検出するに至った場合、このような再送信によってトラフィックが Blade の詳細な検査をバイパスします。 |

<p>| TCP 無効なチェックサム | 無効な TCP チェックサムを持ったパケットは受信ホストの TCP スタックでドロップされるため、ゲートウェイはそのようなパケットを検査する必要がありません。これにより無効なチェックサムを持った TCP パケットがブロックされます。ネットワークの不調により、ネットワーク上に誤ったチェックサムを持つパケットが現れることが普通のことです。これは攻撃の試みを示すものではないため、デフォルトではこうしたイベントは記録されません。 |</p>
<table>
<thead>
<tr>
<th>ストリーミング・エンジン設定の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP SYN 变更された再送の追跡</td>
<td>IPS が検査していない接続を開始しようと、変更されたシーケンス番号で TCP SYN パケットが再送信されることがあります。このため、シーケンス番号が変更された SYN の再送信をブロックします。検出するように設定した場合、このような再送信によってトラフィックが Blade の詳細な検査をバイパスします。</td>
</tr>
<tr>
<td>TCP 緊急データ実施</td>
<td>Telnet のような一部の TCP プロトコルでは、プロトコル構文の一部として TCP URG ビットを使用して帯域外データを送信しますが、ほとんどのプロトコルでは TCP の帯域外データ処理機能を使用しません。URG ビットを含むパケットを許可すると、受信しているアプリケーションによってどのデータが処理されているかゲートウェイが判断できなくなることがあります。このため、ゲートウェイによって検査したデータが受信しているアプリケーションが処理するデータと異なるという状態になることがあります。この場合には IPS 保護がバイパスされることになります。帯域外データ処理機能をサポートしていないプロトコルで URG ビットを含むパケットを受信した場合、ゲートウェイは受信しているアプリケーションがそのデータを処理するかどうか判断できません。そこで、TCP の帯域外データ処理機能をサポートしていないプロトコルで URG ビットを含むパケットを送信したい場合は、検出するように設定した場合、URG ビットを使用すると、トラフィックが Blade の詳細な検査をバイパスします。</td>
</tr>
</tbody>
</table>

| ストリーム・インスペクション・タイムアウト | 特定の処理によって接続を検査した場合、検査完了までに遅れが発生することがあります。検査が制限時間内に完了しない場合、リソースを開放したままでにしないように接続は切断されます。このようにして、検査制限時間を超過した接続をブロックします。検出するように設定した場合、検査制限時間を過ぎると、トラフィックが Blade の詳細な検査をバイパスします。 |

<table>
<thead>
<tr>
<th>脅威対策アンチボットポリシーの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>リソース分類モード</td>
<td>アンチボットエンジンによるリソースの分類に使用するモードを示します。</td>
</tr>
<tr>
<td>• [ホールド] - 分類が完了するまで、接続はブロックされます。</td>
<td>接続がキャッシュされた情報で分類できない場合、チェック・ポイントのオンライン Web サービスによる分類が完了するまで接続はブロックされます。</td>
</tr>
<tr>
<td>• [バックグラウンド] - 分類が完了するまで、接続は許可されます。</td>
<td>接続がキャッシュされた情報で分類できない場合、接続を許可していない応答を受信します。</td>
</tr>
</tbody>
</table>

| スキャンするファイル・サイズの制限 | アンチウイルスエンジンでスキャンするファイル・サイズの制限値（キロバイト）を示します。制限なしを指定する場合は、0 に設定します。 |
| MIME 最大ネスト・レベル | ネストされた MIME コンテンツを含むメールに対して、ThreatSpect エンジンがどのネスト・レベルのメールまでスキャンするかを示す最大ネスト・レベル数を設定します。 |
### 説明

#### MIME ネスト・レベル超過時のアクション
MIME コンテンツのネスト・レベルが設定されたレベルより大きい場合、ファイルを「ブロック」または「許可」するよう設定できます。

#### 優先度付けスキャン
スキャンを最適化するために、セキュリティとパフォーマンスの優先度に従ってスキャンします。

#### リソース分類モード
アンチウイルスエンジンによってリソース分類に使用されるモードを示します。
- **ホールド** - 分類が完了するまで、接続はブロックされます。接続がキャッシュされた情報で分類できない場合、チェック・ポイントのオンライン Web サービスによる分類が完了するまで接続はブロックされます。
- **バックグラウンド** - 分類が完了するまで、接続は許可されます。接続がキャッシュされた情報で分類できない場合、分類されていない応答を受信します。接続は許可されます。バックグラウンドではチェック・ポイントのオンライン Web サービスにより分類が続行されます。このとき、応答は今後の要求に備えてローカルにキャッシュされます。このオプションにより分類プロセスの待ち時間が短縮されます。

#### 説明

サービスが利用できない場合はブロック
Check Point ThreatCloud のオンライン Web サービスを利用できない場合、Web の要求トラフィックはブロックされます。

フェイル・モード
内部システムエラーまたはオーバーロードが起きた場合、トラフィックに対して実行するアクション（「すべての要求を許可」または「すべての要求をブロック」）を示します。

検査するファイル・サイズの制限
注 - 制限値が小さすぎるとアプリケーション・コントロール Blade の機能に影響することがあります。制限なしを指定する場合は、0 に設定します。

HTTP 検査のスキップ方法
警告: [フル]に設定変更すると、セキュリティに重大な影響を与えます。

HTTP 接続はさまざまなセッションで構成されていることがあります。1 つの HTTP 接続の一部のファイルは HTTP セッションを通過します。

【検査するファイル・サイズの制限】の設定が 0 でない場合、【HTTP 検査のスキップ方法】を[デフォルト]に設定すると、ファイルの検査がそのセッションの終わりまでスキップされ、次の HTTP セッションから再開されます。

【検査するファイル・サイズの制限】の設定が 0 でない場合に【HTTP 検査のスキップ方法】の設定を[フル]に変更すると、ファイルの検査がその接続の終わりまでスキップされ、次の接続から再開されます。これによってその接続の残りの検査が速まり、パフォーマンスが改善されます。しかし、[フル]への設定変更はセキュリティに重大な影響を与えるためお勧めしません。その接続の残りのセッションは検査されないままになります。
## アプライアンスの設定

### USB モデム・ウォッチドッグ

<table>
<thead>
<tr>
<th>USB モデム・ウォッチドッグの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>間隔</td>
<td>USB モデム・ウォッチドッグがインターネットをプローブする頻度（分）を示します。</td>
</tr>
<tr>
<td>モード</td>
<td>インターネットをプローブしてもインターネット・アクセスがない場合、USB モデム・ウォッチドッグを有効にするために、次のリセット・オプションのいずれかを選択します。</td>
</tr>
<tr>
<td></td>
<td>- [ハード・リセット] - USB モデムの電源をオフにしてから再投入します。</td>
</tr>
<tr>
<td></td>
<td>- [ゲートウェイ・リセット] - アプライアンスを再起動します。</td>
</tr>
</tbody>
</table>

### アップデート・サービスのスケジュール

<table>
<thead>
<tr>
<th>アップデート・サービスのスケジュールの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>再試行の最大数</td>
<td>クラウドを利用できない時、単一のアップデートに対する再試行の最大数を示します。</td>
</tr>
<tr>
<td>再試行するまでのタイムアウト値</td>
<td>アップデートを再試行するまでのタイムアウト値（秒）を示します。</td>
</tr>
</tbody>
</table>

### ユーザ認識

<table>
<thead>
<tr>
<th>ユーザ認識の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory 関連付けのタイムアウト値</td>
<td>ユーザとIPアドレスとの関連付けをキャッシュするまでのタイムアウト値（分）を示します。</td>
</tr>
<tr>
<td>認識していないユーザに対するDNSトラフィックの許可</td>
<td>[ユーザ&amp;オブジェクト]→[User Awareness]→[ブラウザ・ベース認証]→[認識]タブで[Captive Portalが利用できない場合は認識できないユーザをブロック]が選択されているとき、認証されないユーザからのDNSトラフィックはブロックされることを示します。DNSトラフィックを許可しないと、エンドユーザのブラウザでCaptive Portalを表示できないことがあるためです。</td>
</tr>
<tr>
<td>IP アドレスごとにシングル・ユーザを想定</td>
<td>[ユーザ&amp;オブジェクト]→[User Awareness]でActive Directoryクエリを有効にすると、1台のデバイスに対して1人のユーザのみが認識されるようになることがパラメータで示されます。2人以上のユーザが1台のデバイスから接続した場合、最後にログオンしたユーザのみが認識されます。</td>
</tr>
<tr>
<td>ブロックした認識していないユーザをログ記録</td>
<td>[ユーザ&amp;オブジェクト]→[User Awareness]→[ブラウザ・ベースの認証]→[認識]タブで[Captive Portalが利用できない場合は認識できないユーザをブロック]が選択されているとき、ブロックした認証されないユーザをログ記録するかどうかを示します。</td>
</tr>
</tbody>
</table>
### VPN リモート・アクセス

<table>
<thead>
<tr>
<th>VPN リモート・アクセスの属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>オフライン時のトラフィックのクリアを許可</td>
<td>サイトに接続されていないリモート・アクセス VPN クライアントが暗号化していない（クリア）トラフィックを送信された場合、もしくは切断されている場合、VPN ドメインへのトラフィックを許可するかどうかを示します。</td>
</tr>
<tr>
<td>同時ログインを許可</td>
<td>複数のセッションへのログインを許可するかどうかを示します。このオプションが無効の場合、ユーザが同じ認証情報で 2 度目にログインすると、前のセッションは切断されます。</td>
</tr>
<tr>
<td>認証タイムアウト</td>
<td>タイムアウトが有効な場合、リモート・クライアントのパスワードの有効性が維持される時間（分）を示します。</td>
</tr>
<tr>
<td>認証タイムアウト - 有効</td>
<td>リモート・クライアントのパスワードの有効性が維持されるのは設定した時間のみかどうかを示します（認証タイムアウトの属性）。</td>
</tr>
<tr>
<td>VPN ドメインで自動切断</td>
<td>クライアントが安全な内部ネットワーク内（ローカル暗号化ドメイン）から接続している場合、リソース消費削減のためにクライアントが自動的に切断されるかどうかを示します。</td>
</tr>
<tr>
<td>バック接続 - 有効</td>
<td>ゲートウェイで隠れている暗号化ドメインからクライアントへの逆向き接続を有効にします。</td>
</tr>
<tr>
<td>バック接続キープアライブの間隔</td>
<td>ゲートウェイへのキープアライブ・パケットと逆向き接続のクライアントへのキープアライブ・パケットとのサイクル間隔（秒）を示します。</td>
</tr>
<tr>
<td>すべてのインタフェースでビジター・モードを有効にする</td>
<td>このダイアログ・ボックスを使用して、ビジター・モードの特定のインタフェースを設定できます。ビジター・モードでは、リモート・アクセス・クライアントからの IKE 接続のバックアップとして、アプライアンスにより指定されたポート（デフォルトはポート 443）で TCPT トラフィックの待ち受けをすることできます。一般に、このモードの使用によって、ホテルなど制約のある環境での VPN リモート・アクセスを可能にします。特定のインタフェースについてのみ有効になるようにビジター・モードを変更することをお勧めしません。</td>
</tr>
<tr>
<td>DNS トラフィックの暗号化</td>
<td>リモート・クライアントによって暗号化ドメインにある DNS サーバに送られた DNS クエリが VPN トンネルを通じていかからかを示します。</td>
</tr>
<tr>
<td>暗号化メソッド</td>
<td>IKE フェーズの 1 および 2 に、どの IKE 暗号化メソッド（バージョン）が使用されるかを示します。</td>
</tr>
<tr>
<td>Endpoint Connect の再認証タイムアウト</td>
<td>Endpoint Connect のユーザ認証情報が、認証確認のためにゲートウェイに再送されるまでの時間（分）を示します。</td>
</tr>
<tr>
<td>IKE IP 圧縮のサポート</td>
<td>リモート・アクセス・クライアントの IPSec パケットが圧縮されるかどうかを示します。</td>
</tr>
<tr>
<td>IKE over TCP</td>
<td>IKE over TCP のサポートを有効にします。</td>
</tr>
<tr>
<td>アプライアンスの設定</td>
<td>説明</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>IKE 再起動リカバリ</td>
<td>リモート・アクセス・クライアントを扱う場合、クライアントのアドレスが不明なため、アプライアンスでは IKE フェーズ 1 ネゴシエーションを開始できません。アプライアンスにおいてリモート・アクセス・クライアントを含むアクティブな SA がある状態で再起動した場合、SA が失われるためアプライアンスでは IKE フェーズ 1 ネゴシエーションを開始できません。しかし、再起動オプションが選択されている場合はトンネルの詳細情報が 1 分ごとにアプライアンスに保存されます。アプライアンスの再起動後に最初の暗号化パケットが届くと、アプライアンスによって SA 削除メッセージが送信されます。これによりリモート・クライアントは古い SA を破棄し、さらに IKE フェーズ 1 を開始してトンネルを再構築します。</td>
</tr>
<tr>
<td>レガシー NAT トラバーサル</td>
<td>チェック・ポイント独自の NAT トラバーサル・メカニズム（UDP カプセル化）が SecureClient に対して有効かどうかを示します。</td>
</tr>
<tr>
<td>複数インタフェースでオフライン・モードを有効にする</td>
<td>複数の外部インタフェースによってリモート・アクセス・クライアントとアプライアンスとの接続性を改善するパフォーマンスインパクトのあるメカニズムが有効かどうかを示します。</td>
</tr>
<tr>
<td>オフィス・モードでアンチスプーフィングを実行</td>
<td>[オフィス・モードでアンチスプーフィングを実行] - このオプションを選択した場合、カプセル化されたパケットの IP アドレスがオフィス・モード IP アドレスになっているが、オフィス・モードで作業中のクライアントのアドレスから確かに送信されたものをを VPN によって確認します。IP アドレスが DHCP サーバで割り当てられる場合、アンチスプーフィング実行のために、VPN は DHCP スコープから割り当てられたアドレスの範囲を知る必要があります。DHCP スコープを表すネットワーク・オブジェクトを定義し、それを選択します。</td>
</tr>
<tr>
<td>各サイトにシングル・オフィス・モード</td>
<td>[各サイトにシングル・オフィス・モード] - リモート・ユーザが接続して、ゲートウェイからオフィス・モード IP アドレスを受け取った後は、このゲートウェイ暗号化ドメインに対するすべての接続では、オフィス・モード IP が内部の送信元 IP として使用されます。オフィス・モード IP は、暗号化ドメインのホストがリモート・ユーザの IP アドレスとして認識するアドレスです。特定のゲートウェイが割り当てるオフィス・モード IP アドレスは、それに自体の暗号化ドメインと共に、隣接する暗号化ドメインでも使用できます。隣接する暗号化ドメインは、アドレスを割り当てたゲートウェイと同じ VPN コミュニティに属すゲートウェイの背後にある必要があります。リモート・ホスト接続は、受け取ったオフィス・モード IP アドレスに依存しているため、IP を発行したゲートウェイが使用不能になると、このサイトに対するすべての接続が終了します。</td>
</tr>
<tr>
<td>オフィス・モードに RADIUS から割り当て</td>
<td>オフィス・モード IP アドレスが、ユーザの認証に使用される RADIUS サーバで割り当てられているかどうかを示します。</td>
</tr>
<tr>
<td>オフライン・モード - 無効</td>
<td>オフライン・モード - 無効オフライン・モード IP アドレスをリモート・アクセス・クライアントに割り当てが無効になっているかどうかを示します。このオプションは選択しないことをお勧めします。</td>
</tr>
<tr>
<td>クライアントでパスワードのキャッシュ</td>
<td>パスワードのキャッシュを使用するかどうかを示します。キャッシュを使用する場合、クライアントが複数のゲートウェイにアクセスしても再認証する必要はありません。</td>
</tr>
</tbody>
</table>
### VPN リモート・アクセスの属性

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP プール NAT の不使用</td>
<td>IP プール NAT 設定をオフィス・モードのユーザに適用されないようにします。SecureClient やその他の VPN クライアントを使用する場合、この措置が必要です（sk20251 h_121870 を参照）。</td>
</tr>
<tr>
<td>リモート・アクセス・ポート</td>
<td>デフォルトのリモート・アクセス・ポートはポート 443 番です。このポート番号を使用している別のサーバと競合が生じる場合、別のリモート・アクセス・ポートに設定します。Check Point VPN クライアント、Mobile クライアント、SSL VPN リモート・アクセス・メソッドのいずれかが有効で、ポート 443 番をデフォルトで使用している場合、デフォルトのリモート・アクセス・ポートを変更する必要があります。デフォルトのポート番号 443 を変更する場合、必ず [ポート 443 番をポート転送に予約] を選択してください。</td>
</tr>
<tr>
<td>SNX キープアライブ間隔</td>
<td>SSL Network Extender キープアライブ・パケット間の時間（秒）を示します。</td>
</tr>
<tr>
<td>SNX 再認証タイムアウト</td>
<td>SSL Network Extender リモート・アクセス・ユーザの再認証までの時間（分）を示します。</td>
</tr>
<tr>
<td>SNX の RC4 サポート</td>
<td>SSL クライアントで、RC4 暗号化方式とデフォルトのアルゴリズムの両方をサポートするかどうかを示します。</td>
</tr>
<tr>
<td>SNX アンインストール</td>
<td>このパラメータを使用して、SSL Network Extender クライアントをアンインストールする条件を設定できます。選択肢は以下のとおりです。自動的にアンインストールはしません（推奨設定、デフォルト）。ユーザが接続を切断すると常にアンインストールします。ユーザが接続を切断すると、アンインストールするかどうか尋ねます。</td>
</tr>
<tr>
<td>SNX アップグレード</td>
<td>このパラメータを使用して、SSL Network Extender クライアントをインストールする条件を設定できます。選択肢は以下のとおりです。自動的にアップグレードはしません。常にアップグレードします。アップグレードするかどうか尋ねます（デフォルト）。</td>
</tr>
<tr>
<td>トポロジ・アップデート手動間隔</td>
<td>クライアントにダウンロードされたトポロジの更新頻度（時間）（手動設定）を示します。上書き設定が「true」に設定されている場合だけ適用されます。</td>
</tr>
<tr>
<td>トポロジ・アップデートの上書き</td>
<td>トポロジ更新の設定変更によってデフォルトのポリシー「週 1 回」を変更するかどうかを示します。</td>
</tr>
<tr>
<td>再起動時のみトポロジ・アップデート</td>
<td>トポロジ更新がクライアントの起動時のみに実行されるかどうかを示します。上書き設定が「true」に設定されている場合だけ適用されます。</td>
</tr>
<tr>
<td>デバイス証明書の検証</td>
<td>リモート・アクセス・クライアントにより、証明書失効リストでデバイス証明書の確認をします。</td>
</tr>
<tr>
<td>ポリシの項目</td>
<td>説明</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| NAT トランスバーサル許可 | 業界標準 NAT トランスバーサル（UDP カプセル化）が有効かどうかを示します。これにより、リモート・サイトが NAT デバイスで隠れている場合でも VPN トンネルの確立が可能になります。
| 管理通知 | 管理イベント（たとえば、証明書の有効期限が間もなく切れる場合）を記録する方法を示します。
| IPSec 応答パケットの妥当性チェック | IPSec 応答パケットの妥当性チェックを行うかどうかを示します。
| クラスタ SA 同期パケットのしきい値 | パケット数がこのしきい値に達する場合、他のクラスタ・メンバを含む同期 SA。
| 暗号化/復号 IPSec パケットからの DiffServ マークをコピー | 暗号化/復号された IPSec パケットから DiffServ マークをコピーします。
| DiffServ マークを暗号化/復号 IPSec パケットへコピー | 暗号化/復号 IPSec パケットへ DiffServ マークをコピーします。
| 暗号化パケットの再ルーティングを有効にする | ピアの IP アドレスまたはプロービングに従って、暗号化パケットが最適なインタフェースを使用するルート変更されるかどうかを示します。この値を「false」に変更することをお勧めしません。
| CRL が無効になるまでの時間 | CRL の無効期間は、アプライアンスとリモート CAとのシステム時刻のずれの問題を解決するために必要です。
| | 無効期間によって CRL 有効期間を拡げることができます。
| | リモート・サイトの失办性の証明書が失効後も有効とみなされる時間（秒）を示します。
| CRL が有効になるまでの時間 | CRL の有効期間は、アプライアンスとリモート CAとのシステム時刻のずれの問題を解決するために必要です。
| | 有効期間によって CRL 有効期間を拡げることができます。
| | CAによって証明書が有効と設定される時に先立って有効とみなされる時間（秒）を示します。
| 既知サイトからの IKE DoS 保護 | 認識している IP アドレスからの IKE DoS に対する保護がアクティブになっています。潜在的な攻撃者を検出できる方法を有するかどうかを示します。
| 未知サイトからの IKE DoS 保護 | 認識していない IP アドレスからの IKE DoS に対する保護がアクティブになっており、潜在的な攻撃者を検出できる方法を有するかどうかを示します。
| 同じ IP からの IKE 応答 | IKE セッションで使用される発信元 IP アドレスが、着信接続に対する応答時の宛先に基づいているか、または一般的な発信元 IP アドレスのリンク選択の設定に基づいているかを示します。
# アプライアンスの設定

<table>
<thead>
<tr>
<th>VPN サイト間のグローバル設定の属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE クイック・モードの連続するサブネットをまとめる</td>
<td>IKE クイック・モードにおいて、隣接するサブネットを結合するかどうかを示します。</td>
</tr>
<tr>
<td>DF フラグをパケットに設定</td>
<td>暗号化/復号処理中、パケットの DF フラグ（「断片化しない」）が保持されるかどうかを示します。</td>
</tr>
<tr>
<td>キー交換エラーの追跡</td>
<td>VPN 設定エラーまたは鍵交換エラーのログ記録の方法を示します。</td>
</tr>
<tr>
<td>最大同時 IKE ネゴシエーション数</td>
<td>同時実行 VPN IKE ネゴシエーションの最大数を示します。</td>
</tr>
<tr>
<td>最大同時トンネル数</td>
<td>トンネル同時使用の最大数を示します。</td>
</tr>
<tr>
<td>オープン SA 制限</td>
<td>VPN ピアごとの有効な SA の最大数を示します。</td>
</tr>
<tr>
<td>外部へのリンクの追跡</td>
<td>発信 VPN リンクのログ記録の方法を示します（ログ記録、ログ記録しない、警告）。</td>
</tr>
<tr>
<td>管理者のデバイスへのアクセスのための設定「すべてのトラフィックをリモート VPN サイトへルーティング」を無効にします。</td>
<td>このオプションを選択して、「すべてのトラフィックをリモート VPN サイトにルーティング」が設定されている場合でも、管理者がリモート・サイトへのルートでこのアプライアンスへアクセスしないようにします。</td>
</tr>
<tr>
<td>パケット処理エラーの追跡</td>
<td>VPN パケット処理エラーのログ記録の方法を示します（ログ記録、ログ記録しない、警告）。</td>
</tr>
</tbody>
</table>
| 内部 IP アドレスでトンネル・テストを実行 | トンネル・テストによって、ピア VPN ゲートウェイ間の VPN トンネルがアップ状態であることを確認します。デフォルトでは、テストによりピア VPN ゲートウェイのすべての外部 IP アドレス間が接続されていることを確認します。このオプションを変更して、ゲートウェイの内部 IP アドレスを使用してトンネル・テストをすることができます。この場合、ローカル暗号化ドメインの一部を使用することになります。
[ログ&モニタリング] タブで VPN トンネルのステータスを確認できます。 |
| 永続的なトンネル・ダウンの追跡 | トンネルがダウンした場合のログ記録の方法を示します（ログ記録、ログ記録しない、警告）。 |
| 永続的なトンネル・アップの追跡 | トンネルがアップ状態の場合のログ記録の方法を示します（ログ記録、ログ記録しない、警告）。 |
| RDP パケット応答タイムアウト | RDP パケット応答のタイムアウト（秒）。 |
| 外部からのインタフェースからの応答 | トンネルがリモート・サイトから開始された場合、同じ着信インタフェースから応答します（IKE および RDP セッションのみ該当）。 |
### VPN サイト間のグローバル設定の属性

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>完了したキー交換の追跡</td>
<td>キー交換が正常に行われた場合のログ記録の方法を示します（ログ記録、ログ記録しない、警告）。</td>
</tr>
<tr>
<td>IKE にクラスタ IP アドレスを使用</td>
<td>IKE がクラスタ IP アドレス（使用できる場合）を使用して行われるかどうかを示します。</td>
</tr>
<tr>
<td>VPN トンネル共有</td>
<td>新規トンネルの作成の条件には以下の種類があることを示します。ホストのペアごとに 1 つの VPN トンネル、サブネット（業界標準）のペアごとに 1 つの VPN トンネル、リモート・サイト/ゲートウェイのペアごとに 1 つの VPN トンネル。これにより、作成されるトンネルの数を抑制します。</td>
</tr>
</tbody>
</table>

### VoIP

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>登録したポートに MGCP 接続を許可</td>
<td>MGCP トラフィック全体にわたる検査によって登録されたポートへの MGCP 接続を自動的に許可するかどうかを示します。</td>
</tr>
<tr>
<td>登録したポートに SIP 接続を許可</td>
<td>SIP トラフィック全体にわたる検査によって登録されたポートへの SIP 接続を自動的に許可するかどうかを示します。</td>
</tr>
</tbody>
</table>

### Web インタフェース設定とカスタマイズ

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
</table>
アクセス・ポリシーの管理

このセクションでは、Check Point 730/750 Appliance アクセス・ポリシーのセットアップおよび管理の方法について説明します。

ファイアウォール・アクセス・ポリシーとブレードの設定

[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページでは、デフォルトのアクセス・ポリシー・コントロールのレベルを設定する、デフォルトのアプリケーション& URLを指定して安全なブラウジングのブロック/許可を設定する、User Awareness を設定するといったことを実行できます。

アクセス・ポリシーは、Check Point 730/750 Appliance の着信、内部、発信トラフィックに関するセキュリティ要件を定義するルールの集合です。

アクセス・ポリシーには以下のものが含まれます。

- ファイアウォール・ポリシー - パケットのインスペクション方法を定義します。
- アプリケーション& URL フィルタリング - インターネット・ブラウジングとアプリケーションの使用の制御方法を定義します。

[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページでは、組織のデフォルト・ポリシーを簡単に定義できます。また、ルール・ベースのポリシーを[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページで定義および表示できます。[ファイアウォール・ブレード・コントロール]ページの設定は、自動生成のシステム・ルールとしてルール・ベースの下に表示されます。[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページでは、このページで定義されたデフォルト・ポリシーの例外となるルールを手動で定義することをお勧めします。

[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページでは、組織を対象にした着信、内部、発信トラフィックのデフォルト・ポリシーを定義します。また、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページでは、組織内の特定サーバのデフォルト・アクセス・ポリシーを簡単に定義できます。自動的に生成されるシステム・ルールも定義されます。

ファイアウォール・ポリシー

デフォルトのアクセス・ポリシーを設定するオプションのいずれかを選択します。

- 厳格
  - デフォルトで、方向にかかわらずすべてのトラフィックをブロックします。このモードでは、ポリシーは[サーバ]ページでのみ定義することができ、また[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページでアクセス・ポリシー・ルールを手動で定義することができます。

- 標準
  - 設定したサービスでインターネットへの発信トラフィックを許可します。サービスリンクをクリックして、すべてのサービスまたは特定のサービスを許可するよう設定できます。
  - 内部ネットワークとトラスト・ワイヤレス・ネットワーク間のトラフィックを許可します（該当するデバイス）。
  - インターネットからの暗号化されていない着信トラフィックをブロックします（組織外部からのトラフィック）。

標準ポリシーのオプションはデフォルトで、多くの場合、推奨される設定です。セキュリティ・レベルを上げる/下げる特別な必要性がない限り、この設定を維持しておくことをお勧めします。

- オフ
  - すべてのトラフィックが許可されます。ファイアウォールが無効になると、ネットワークは危険にさらされます。手動で定義したルールは適用されません。
注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。

特定の外部へのサービスを標準ファイアウォール・ポリシーに設定するには
1. アクセス・ポリシーのコントロール・レベルが標準の場合、すべてのサービスリンクをクリックします。
2. [以下で指定したサービスを除くすべてをブロック]をオンにします。
3. 許可するサービスのチェックボックスをオンにします。
4. すべてのサービスを許可するには、[すべての外部へのサービスを許可]をオンにします。
5. [適用]をクリックします。

アクセス・ポリシー・ルールを手動で設定するには
[アクセス・ポリシー]→[ポリシー]ページへ移動します。

[アクセス・ポリシー]→[ブレード・コントロール]ページで、以下を実行します。

- 手動のルールが設定されていない場合は、ファイアウォール・ポリシーのリンクをクリックして、ファイアウォール・ポリシーに手動ルールを追加できます。
- 手動ルールを設定すると、追加されたルールの数が表示されます。 手動ルールのリンクをクリックすると、[アクセス・ポリシー]で確認できます。

ここでは、サーバのリンクをクリックして、アプライアンスで定義されたサーバの数を確認することもできます。サーバが未定の場合、サーバの追加リンクをクリックして簡単に追加できます。サーバ・オブジェクトは定義されたIPアドレスで、必要に応じて、特定のアクセス・ポリシーや外部からのNATルールを定義することも可能です。例えば、ポート転送NATを定義できます。自動的に生成されたサーバへのアクセス・ルールは、デフォルトのポリシー・ルールの上に作成され、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページで確認できます。サーバへの例外ルールも、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページで作成できます。

アプリケーション& URLフィルタリング
アプリケーション& URLフィルタリングのセクションでは、組織からインターネットへのトラフィックにおけるアプリケーションとURLカテゴリの処理方法を定義します。

アプリケーション& URLフィルタリングはサービス・ベースの機能です。 新しいアプリケーションの最新シグネチャ・パッケージをダウンロードしたり、URLカテゴリをダウンロードするためにCheck Pointクラウドに通信するためには、インターネット接続が必要です。 このページでは、アプリケーション& URLフィルタリングを制御するデフォルトのポリシーを定義できます。 セキュリティリスクとなるカテゴリとアプリケーションのブラウジングは、デフォルトでブロックすることをお勧めします。 企業のポリシーに基づいて、アプリケーションやカテゴリをデフォルトでブロックするように追加で追加することもあります。また、帯域幅を消費するアプリケーションを制限するよう選択して、帯域幅をコントロールしやすく設定することもできます。

オン/オフのボタンのほか、URLフィルタリング・モードを選択することができます。これはURLとカスタム・アプリケーションのみをブロックするオプションです。 コミュータに初期インストールされており、自動アップデートで追加された定義済みアプリケーションはブロックされません。

URLフィルタリング・モードを選択すると、以下のような動作になります。

- URLを含むルールが実施されます。ルール内のアプリケーションは実施されません。
- カスタムのURLやアプリケーションを含むルールが実施されます。
カスタムの URL やアプリケーションを含むルールが実施されます。定義済みのアプリケーションには実施されません。

アプリケーションは自動アップデートではアップデートされません。ここで定義されるデフォルトのポリシーは、自動的に生成されたルールとして、[アクセス・ポリシー]→[ポリシー]ページの外部へのトラフィック・ルール・ベースの下に表示されます。

次の1つ以上のオプションを選択します。

- [セキュリティ・リスク・カテゴリをブロック] - セキュリティのリスクとなりうるアプリケーションと URL をブロックし、スパイウェア、フィッシング、ボットネット、スパム、アンチマイザ、ハッキングといったカテゴリに分類します。このオプションはデフォルトで有効になっています。
- [不適切なコンテンツをブロック] - コンテンツ制御を行い、好ましくないコンテンツの Web サイト（アダルト、暴力、兵器、ギャンブル、アルコールなど）へのインターネット・アクセスをブロックします。
- [ファイル共有アプリケーションをブロック] - TorrentやP2Pアプリケーションを利用した違法なソースからのファイル共有をブロックします。
- [その他の好ましくないアプリケーションをブロック] - 好ましくないアプリケーションのグループに、アプリケーションやURLカテゴリを手動で追加してブロックします。URLやアプリケーションがデータベースにない場合は、新しく作成することもできます。このオプションをクリックして、基本的なアプリケーションとURLフィルタリング・ポリシーでブロックする項目を管理します。さらに詳細なポリシーの設定については、[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページに移動してください。
- [帯域幅を大量消費するアプリケーションを制限] - 帯域幅を大幅に消費するアプリケーションは、大切な業務に必要なアプリケーションのパフォーマンスを低下させる可能性があります。このオプションで、アプリケーションのQoS強化（帯域幅コントロール）が可能です。このオプションを選択すると、P2Pファイル共有、メディア共有、メディアストリーミングやダウンロードをブロックします。グループを編集して、帯域幅の消費量を制限すべきアプリケーションやカテゴリを追加することができます。実際のインターネット接続のアップロードおよびダウンロード帯域幅に基づいて、帯域幅の上限を設定することが重要です。この情報については、ISPに問い合わせてください。制限を有効に設定するには、ISPが提供する帯域幅の上限値である必要があります。アップデートとダウンロードの帯域幅は、通常異なる値が設定されています。

アップデート

サービス・ベースの機能として、このページにはアップデートのステータスも表示されます。

- 最新
  アップデート・サービスにアクセスできません - インターネットに接続されていない場合などに表示されます。インターネット接続を確認します。[デバイス]→[インターネット]ページから確認し、問題が続く場合はISPに連絡してください。
  最新ではありません - ダウンロード可能な新しいアップデート・パッケージがある状態で、アップデートのスケジュール時間になっていない場合などに表示されます。アップデートは、通常ピーク時を避けた時間帯に予定されています（週末や夜間など）。

アップデートをスケジュールするには

1. アップデート・ステータスの横にあるアイコン上でアップデートのスケジュールリンクを選択します。
2. アップデートのスケジュールを設定するブレードを選択します。それ以外のブレードについては、新しいアップデート・パッケージが利用可能になり、『最新ではありません』というメッセージがステータス・バー（WebUIアプリケーションの下部）に表示されていたら、手動でアップデートする必要があります。
3. 『繰り返し』の間隔を選択します。
   - 『毎日』 - 時刻を指定します。
   - 『毎週』 - 曜日と時刻を指定します。
アプライアンスの設定

・ [毎月] - 日にちと時刻を指定します。
4. [適用]をクリックします。

ユーザ認識

ユーザ認識では、個別のユーザとグループのアクセス制御を実施する Check Point 730/750 Applianceを設定し、IP アドレスに基づくログではなく、ユーザ・ベースのログを確認することができます。

初めて設定する場合は、[設定]をクリックしてユーザ認識でユーザの認識する方法をセットアップします。設定が完了したら、ログでユーザを確認することができます。ユーザのベースのアクセス・ポリシー・ルールも設定可能になります。ユーザ認識は、組織の AD サーバを使用してアプライアンスでシームレスに行われます。ユーザ・データベースと認証は、すべて AD サーバを通じて行われます。ユーザが AD サーバにログインすると、アプライアンスに通知が送られます。AD サーバからのユーザはアクセス・ポリシー・ルールのソースとして使用できます。

ユーザ認識を設定すると、[ユーザ認識を有効にする]チェックボックスが表示されます。ユーザ認識を無効にするには、チェックボックスをオフにします。設定を変更するには、[設定の編集]をクリックします。

また、[ユーザ&オブジェクト]→[ユーザ]ページで、パスワードを使ってローカルでユーザを定義することも可能です。これからのソフトウェアのトラフィックをアプライアンスで認識させるためには、ブラウザベース認証を設定して、アクセスする前に認識する必要がある特定の宛先を設定します。通常、ブラウザベース認証はすべてのトラフィックに使用されるのではなく、特定の宛先のみが対象になります。これは、エンド・ユーザが専用のポータルで、手動でログインする必要があるためです。

ユーザ認証を設定すると、[ユーザ認識を有効にする]チェックボックスが表示されます。ユーザ認識を無効にするには、チェックボックスをオフにします。設定を変更するには、[設定の編集]をクリックします。

また、[Active Directory サーバ]をクリックして、ゲートウェイと連動させる AD サーバをいつでも定義できます。AD サーバの作成は、設定の編集ウィザードで行うことができます。

トラッキング

ブロックするトラフィックと許可するトラフィックをログに記録できます。デフォルトでは、ブロックするトラフィックがログ記録されます。必要であれば、この設定をオフにできます。設定は、デフォルトのファイアウォール・ポリシーとアプリケーション&URL サイレント・ポリシーでブロック/許可するすべてのトラフィックに適用されます。

関連情報

Check Point アプリケーション・データベースには、4,500 個以上のアプリケーションと 9600 万以上のカテゴリ分類された URL が登録されています。

各アプリケーションでは、説明、カテゴリ、追加カテゴリ、リスク・レベルが確認できます。アプリケーション・コントロール & URL Filtering ルールに、アプリケーションとカテゴリを追加できます。アプライアンスに Application Control & URL Filtering Software Blade のライセンスがある場合、データベースは定期的にアップデートされ、新しいアプリケーション、カテゴリ、ソーシャル・ネットワーキング・ウィジェットが追加されます。このため、常に最新のポリシーを簡単に作成することが可能です。

アプリケーション・データベースは、以下から確認できます。

・ その他の好ましくないアプリケーションをブロックするリンクから。
・ アプリケーション & URL リンク - [アクセス・ポリシー] → [アプリケーション & URL] ページが開きます。
アプライアンスの設定

- Check Point AppWiki リンク - AppWiki は、アプリケーション & URL フィルタリングのデータベースを検索して絞り込む、便利なツールです。

ファイアウォール・アクセス・ポリシー

[アクセス・ポリシー] → [ファイアウォール・ポリシー] ページでは、ファイアウォール・アクセス・ポリシー・ルール・ベースを管理できます。ここでは、ルールを作成、編集、削除したり、有効/無効にすることが可能です。[アクセス・ポリシー] → [ファイアウォール・ブレード・コントロール] ページでは、基本的なファイアウォール・ポリシーのモードを決定します。

標準モードの場合、デフォルトのポリシー設定に基づいて自動生成されたルールと、このデフォルト・ポリシーの例外として手動で定義したルールが両方表示されます。

厳格モードの場合、デフォルトですべてのアクセスがブロックされ、このページでのみ組織のアクセス・ルールを設定することができます。

ルール・ベースは、以下の 2 つのセクションに分割されます。各セクションには異なるセキュリティ・ポリシーが表示されます。組織からインターネットへのブラウジング方法（組織の外部）と、組織のリソースにアクセスする際のセキュリティ・ポリシー（組織の内部からと外部からの両方）です。ページの上部には 3 つのリンクがあり、両方を表示する、またはどちらか一方のセクションのみを表示するよう変更できます。

- [インターネットへの外部アクセス] - 外部へのすべてのトラフィック・ルール。このルール・ベースでは、組織の外部であるインターネットへアクセスする際のポリシーを決定します。通常、ここでのポリシーは、基本的なトラフィックは許可し、企業が判断したアプリケーションと URL をブロックします。[アクセス・ポリシー] → [ファイアウォール・ブレード・コントロール] ページでは、ブロックするアプリケーションと URL のデフォルト・ポリシーを設定できます。このページでは、デフォルト・ポリシーの例外となるルールを手動で追加できます。また、ルール・ベースでブロック/許可されたとき、特定の Web サイトに対してユーザーに表示するメッセージのカスタマイズを行うことも可能です（以下を参照）。さらに、アプリケーションと URL のデフォルト・ポリシーを設定できます。
ケーションまたは URL の確認アクションを使用して、アクセスが業務関連の目的かどうかをエンド・ユーザに確認することもできます。たとえば、カテゴリに分類されていない URL へアクセスするユーザに確認するルールを追加することは、推奨される設定です。このようなルールを設定すれば、潜在的なポット攻撃を防ぐことが可能です。

- [着信、内部および VPN トRAフィック] - すべての着信、内部、VPN トRAフィックのルール。このルール・ベースでは、組織のソースがアクセスする際のポリシーを決定します。すべての内部ネットワーク、ワイヤレス・ネットワーク、そして外部 VPN サイトは、企業の一部としてみなされ、これらに送られるトRAフィックはこのルール・ベースで検査されます。通常、ここでのポリシーは、組織の外部から中に送られるトRAフィックはブロックし、組織の中のトRAフィックは許可します。

標準モードでは、複数のページにわたってさらに詳細なデフォルト・ポリシーを設定できます。
- 特定のソースから組織へのトRAフィックは、デフォルトでブロックまたは許可することができます。この設定は各ソースの編集モードで確認できます。
  - 外部の VPN サイト - [VPN]→[サイト・ツー・サイト・ブレード・コントロール]ページで、VPN サイトへのデフォルト・アクセスを設定します。
  - リモート・アクセス VPN ユーザ - デフォルト・アクセスを[VPN]→[リモート・アクセス・ブレード・コントロール]ページから設定します。
  - ワイヤレス・ネットワーク - 各ワイヤレス・ネットワークの編集ウィンドウ（[デバイス]→[ワイヤレス・ネットワーク]ページ）の[アクセス]タブから、各ワイヤレス・ネットワークのデフォルト・アクセスを設定します。
  - DMZ ネットワーク - DMZ オブジェクトの編集ウィンドウ（[デバイス]→[ローカル・ネットワーク]ページ）からデフォルト・アクセスを設定します。
- 各サーバーの編集ウィンドウ（[アクセス・ポリシー]→[ファイアウォール・サーバ]ページ）で設定した定義したサーバ・オブジェクトへのトラフィック。

このページでは、デフォルト・ポリシーの例外となるルールを手動で追加できます。厳格モードでは、デフォルト・ポリシーですべてのトラフィックがブロックされ、アクセスは手動のルールで設定します。

各セクションには、以下があります。
- 手動ルール - 手動で作成するルール。
- 自動生成ルール - 上記で説明した初期のファイアウォール・ポリシー・モード（厳格または標準）に基づき、システムで判断したルール。このルールは、システムのそれ以外の要素も考慮されています。たとえば、サーバを追加した場合、対応するルールが[着信、内部および VPN トRAフィック]セクションに追加されます。

以下は、ファイアウォール・アクセス・ポリシーのルールを管理するフィールドです。

<table>
<thead>
<tr>
<th>フィールド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO.</td>
<td>ファイアウォール・ルール・ベースのルール番号。</td>
</tr>
<tr>
<td>ソース</td>
<td>接続を開始する IP アドレス、ネットワーク・オブジェクト、ユーザ・グループ。</td>
</tr>
<tr>
<td>宛先</td>
<td>接続の送信先となる IP アドレスまたはネットワーク・オブジェクト。</td>
</tr>
<tr>
<td>アプリケーション</td>
<td>許可/ブロックするアプリケーションまたは Web サイト。一般的なアプリケーション、カテゴリ、カスタム定義のアプリケーション、URL、グループなどでリストを絞り込むことができます。詳細については、[アプリケーション&amp; URL]を参照してください。</td>
</tr>
<tr>
<td></td>
<td>このフィールドは、インターネットへの外部へのアクセス・セクションのみに表示されます。</td>
</tr>
<tr>
<td>サービス</td>
<td>許可/ブロックするネットワーク・サービスのタイプ。</td>
</tr>
</tbody>
</table>
フィールド | 説明
--- | ---
アクション | トラフィックがルールに一致した場合に実行するファイアウォールのアクション。
外部へのトラフィック・ルールの場合、通常のブロック/許可アクションのほかに、メッセージのカスタマイズ・オプションを使用して"確認"、「通知」アクションを設定することができます。
メッセージは、「許可して通知」、「ブロックして通知」、「確認」の各アクション・タイプの場合に表示されます。メッセージは、「許可して通知」、「ブロックして通知」、「確認」の各アクション・タイプの場合に表示されます。「確認」アクションは、トラフィックが業務目的かプライバシー目的かをエンド・ユーザに確認させるアクションです。以下のメッセージのカスタマイズのセクションを参照してください。ユーザはポータルにリダイレクトされ、そこでメッセージまたは質問が表示されます。
ルールに時間の範囲が設定されている場合、時計アイコンが表示されます。
ログ | トラフィックがルールに一致した場合に実行する追跡とログ記録のアクション。
コメント / 自動生成ルール | 上記フィールドのすぐ下に表示される各詳細。
ルールの作成時に入力したコメント。
システムで自動的に生成されるルール。コメントのオブジェクト名のリンクをクリックすると、設定タブが開きます。
"確認"アクション
外部へのルール・ベースでは、許可/ブロックの単純な処理ではなく、ブラウザ・ベースのアプリケーションに「確認」アクションを設定できます。この設定は、次のような状況において役立ちます。
組織において通常はブロックし、業務関連の目的でアクセスする場合には許可したいトラフィックに使用します。エンド・ユーザは、業務に関連するための必要なアクセスであることを確認し、このイベントのために管理者がアクセス・ポリシーを変更することなく、続行できます。たとえば、Facebookへのトラフィックは通常はブロックしますが、人事の担当者が業務関連でアクセスする場合は許可したい場合があります。
カテゴリ分類されていないURLへのトラフィックに対してこのアクションを使うことで、組織の内部にインストールされる可能性のあるマルウェアの防御対策にもなります。カテゴリ分類されていないURLへのアクセス時に"確認"アクションを実施することで、このようなマルウェアをブロックできます。
新しく手動で定義したアクセス・ルールを作成するには
1. ［新規］の横にある矢印をクリックします。ルール・ベースが両方表示されたら、該当するテーブルで［新規］をクリックします。
2. ルールに指定可能な位置をいずれか１つクリックします。[一番上]、[一番下]、[選択したルールの上]、[選択したルールの下]から選んでクリックします。
3. ［ルールの追加］ウィンドウが開きます。次の２種類のルール・フィールドが表示されます。
   - ルールの概要文とデフォルト値。
   - テーブル形式のルール・ベース・フィールド。
4. ルール・サマリのリンク、またはテーブルのセルをクリックして、ネットワーク・オブジェクトを選択するか、ルール・ベースのフィールド・オプションを選択します。上述の説明を参照してください。

注 - アプリケーション]フィールドは、外部へのトラフィックのルールのみに該当します。
アプライアンスの設定

[ソース]フィールドでは、オプションで手動で IP アドレス（ネットワーク）、ネットワーク・オブジェクト、ユーザ・グループ（ユーザ・ベースのポリシーを設定するには User Awareness Blade がアクティブになっている必要があります）を入力できます。ユーザはアプライアンスでローカルに定義することも、Active Directory で外部に定義することも可能です。詳細については、[アクセス・ポリシー]→[ユーザ認識プレード・コントロール]ページを参照してください。

5. [コメントの入力]フィールドでは、ルールを説明するテキストを入力します（オプション）。このテキストは[アクセス・ポリシー]のルールの下にコメントとして表示されます。

6. ルールを特定の時間に制限する場合は、[時間の設定]を選択して、開始時間と終了時間を指定します。

7. 発信ルールでダウンロード・トラフィック・レートを制限する場合は、[アプリケーション・トラフィックのダウンロード制限]を選択して、レート（Kbps）を入力します。

8. 発信ルールでアップロード・トラフィック・レートを制限する場合は、[アプリケーション・トラフィックのアップロード制限]を選択して、レート（Kbps）を入力します。

9. 受信ルールで、暗号化された VPN トラフィックのみを一致させるには、[暗号化トラフィックだけを一致]を選択します。

10. [適用]をクリックします。ルールは[アクセス・ポリシー]の発信/着信のセクションに追加されます。

ルールを複製するには
既存のルールとほとんど同じ内容のルールを作成する場合、ルールを複製して追加できます。

1. ルールを選択して[複製]をクリックします。
2. 必要に応じてフィールドを編集します。
3. [適用]をクリックします。

ルールを編集するには
アクセス・ポリシー・ルールでは、自動生成されたルールの追跡オプションのみ編集できます。

1. ルールを選択して、[編集]をクリックします。
2. 必要に応じてフィールドを編集します。
3. [適用]をクリックします。

ルールを削除するには

1. ルールを選択して、[削除]をクリックします。
2. 認証メッセージで[はい]をクリックします。

ルールを有効/無効にするには
- ルール・ベースに追加した、手動で定義したルールを無効にするには、ルールを選択して[無効]をクリックします。
- 一度無効にした、手動で定義したルールを有効にするには、ルールを選択して[有効]をクリックします。

ルールの順番を変更するには

1. 移動するルールを選択します。
2. 移動する場所へドラッグ・アンド・ドロップします。
3. 注 - 変更できるのは、手動で定義したルールの順番のみです。

メッセージのカスタマイズ
メッセージをカスタマイズして、セキュリティ・ゲートウェイからユーザへコミュニケーションさせることができます。これにより、一部のWeb サイトへのアクセスが企業のセキュリティ・ポリシーに違反することをとユーザに
アプライアンスの設定

教えることができます。また、Web サイトやアプリケーションのインターネット・ポリシーの変更についても伝えることが可能です。メッセージを設定すると、メッセージが関連するアクションを指定したルールにトラフィックが一致した際、ユーザのインターネット・ブラウザで新しいウィンドウにメッセージが表示されます。

アクションのオプションと関連する通知は以下のとおりです。

<table>
<thead>
<tr>
<th>ルール・ベース・アクション</th>
<th>通知</th>
</tr>
</thead>
<tbody>
<tr>
<td>許可して通知</td>
<td>ユーザにメッセージを表示します。ユーザはアプリケーションを使い続けるか、リクエストをキャンセルできます。</td>
</tr>
<tr>
<td>ブロックして通知</td>
<td>ユーザにメッセージが表示され、アプリケーションのリクエストはブロックします。</td>
</tr>
</tbody>
</table>
| 確認                    | ユーザにメッセージが表示され、リクエストを続行するかどうかを確認します。
詳細については、上述を参照してください。 |

メッセージをカスタマイズするには

1. [インターネットへの外部アクセス] セクションで [メッセージのカスタマイズ] をクリックします。
2. 次のタブでオプションを設定します。
   - 許可して通知
   - ブロックして通知
   - 確認
3. 各通知のフィールドを設定します。
   - タイトル - デフォルトのままにするか、新しくタイトルを入力します。
   - サブジェクト - デフォルトのままにするか、新しくサブジェクトを入力します。
   - 本文 - デフォルトのままにするか、新しく本文を入力します。 [オプション・キーワード] をクリックして、ユーザへの情報の本文に使用できるキーワードのリストを表示できます。
   - 無視する場合（確認の場合のみ）- ユーザへの確認メッセージになります。デフォルトのままにするか、新しくテキストを入力します。
   - ユーザは必ず理由を入力（確認の場合のみ）- ユーザがアクティビティ的理由を入力する必要があるときにこのチェックボックスを選択します。ユーザ・メッセージには理由を入力するテキストボックスがあります。
   - フォールバック - 通知がブラウザまたはアプリケーションに表示されない場合に、代わりのアクション（ブロック/許可）を選択します。通知がブラウザまたはアプリケーションで表示されない場合、動作は次のようになります。
     - フォールバックが「許可」の場合 - ユーザは Web サイトまたはアプリケーションにアクセスできます。
     - フォールバックが「ブロック」の場合 - セキュリティ・ゲートウェイで通知をアプリケーション（通知を発生させたもの）に表示させようと試みます。出来ない場合、Web サイトまたはアプリケーションはブロックされ、ユーザに通知は表示されません。
   - 頻度 - ユーザに通知を表示する回数、またはポリシーで許可されていないアプリケーションにアクセスできる回数を設定できます。選択肢は以下のとおりです。
     - 毎日
     - 毎週
     - 毎月
   とえば、アプリケーション - ソーシャル・ネットワーキングのカテゴリを含むルールの場合、頻度に毎日を選択すると、Facebook に何度もアクセスするユーザには一度だけ通知が表示されます。
アプライアンスの設定

- ユーザを URL にリダイレクト - ユーザを外部のポータル（ゲートウェイ以外）にリダイレクトできます。[URL]フィールドに、外部ポータルの URL を入力します。URL には外部システムを指定できます。ユーザから認証情報（ユーザ名/パスワードなど）を受け取り、この情報をゲートウェイに送ります。「ブロック」と[通知]だけに該当します。


5. [適用]をクリックします。

サーバ・オブジェクトの定義

[サーバ]ページでは、システムで定義されているサーバのリストを確認できます。ここでは、サーバ・オブジェクトを作成、編集、削除、検索することができます。サーバ・オブジェクトとは、アクセス・ポリシーと NAT ポリシー（該当する場合）が定義されたネットワーク・オブジェクトのことです。

新しいサーバ・オブジェクトは、ウィザードから作成します。
- ステップ 1 - サーバ・タイプを選択します。
- ステップ 2 - サーバの詳細を定義します。
- ステップ 3 - サーバのアクセス・ポリシーのプロパティを設定します。
- ステップ 4 - NAT の設定を行います（該当する場合）。

サーバを作成すると、1 つ以上の対応するルールが自動的に生成されてアクセス・ポリシーに追加されます。追加されたルールは[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページに表示されます。ルールのコメントにはオブジェクト名が表示されます。コメントのオブジェクト名のリンクをクリックすると、[サーバのプロパティ]の[アクセス]タブが開きます。
サーバ・オブジェクトを定義する簡単な方法は、[ホーム]→[アクティブ・コンピュータ]ページで検出し、サーバとして保存する方法です。この方法では自動的にサーバのMACアドレスを検出するため、設定が簡単になります。

ウィザード:
- [キャンセル]をクリックしてウィザードを終了します。
- [次へ]をクリックしてウィザードの次のページに進みます。
- [戻る]をクリックしてウィザードの前のページに進みます。
- [完了]をクリックしてウィザードを完了します。

新しいオブジェクトを作成するには
[新規]をクリックします。[新しいサーバ]ウィザードが開き、ステップ1：サーバ・タイプが表示されます。

ステップ1：サーバ・タイプ
1. サーバ・タイプを選択します。一般サーバ向けの組み込みタイプがあります。設定したポートを待機するサーバを手動で定義することができます。また、一般的なサーバ・タイプのポートを変更することも可能です。
2. 組み込みタイプを選択する場合は、[編集]をクリックして、プロトコルのポートを変更することも可能です。
3. [その他のサーバ]を選択する場合:
   - プロトコル（TCP、UDP、両方）を選択します。
   - TCP/UDPポートを入力します（ポート番号、ポート範囲をカンマで区切って入力。例：1,3,5-8,15）。

ステップ2：サーバの定義
1. [名前]、[IPアドレス]、[コメント]（オプション）に入力します。
2. サーバに該当するオプションを選択します。詳細は、[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]を参照してください。
   - DNSサーバをこのオブジェクト名に解決 - ゲートウェイが内部ネットワークのDNSサーバである場合、このオプションがオンになっていると、サーバ/ネットワーク・オブジェクトの名前がIPアドレスに変換されます。
   - DHCPサービス除去 - 内部DHCPサービスは、このサーバ/ネットワーク・オブジェクトの設定されたIPアドレスを誰にも配布しません。
     - DHCPサービスでMACのIPアドレスを予約 - 内部DHCPサービスで、MACアドレスに基づき、設定されたIPアドレスをこのサーバ/ネットワーク・オブジェクトのみに配布します。
     - MACアドレスを入力 - IP予約が必要です。[アクティブなコンピュータ]ページからオブジェクトを作成するとき、MACアドレスは自動的に検出されます。

ステップ3：アクセス
1. サーバからアクセス可能なゾーンを選択します。
   - [すべてのゾーン（インターネットも含む）] - 組織の外部から誰でもアクセスできるサーバを作成する場合はこのオプションを選択します。このオプションでは、NAT経由でサーバにアクセスする方法も設定する必要があります（次のステップで）。
   - [トラスト・ゾーンのみ（My Organization）] - 該当するチェックボックスを選択します。手動でアクセス・ルールを追加することで、これらの設定をオーバーライドできます。
     - LAN - 物理内部ネットワーク。
     - リモート・アクセス VPN ユーザ - 自宅やモバイル・デバイスからオフィスへ接続するユーザ。
     - トラスト・ワイヤレス・ネットワーク - バスワードで保護されたネットワーク（ゲスト・ネットワークは除く）。
アプライアンスの設定

- DMZ - セカンダリインターネット接続に使われていないとき、DMZポートに物理的に接続したネットワーク。
- リモートVPNサイト - ゲートウェイの背後で定義されたリモートVPNサイトへのネットワーク。
- [このサーバにアクセス・ポリシーを手動で設定] - 手動のアクセスルールだけを使ってアクセスポリシーを定義する場合はこのオプションを選択します。

2. サーバからPingにアクセスしない場合は、[pingを許可]チェックボックスをオフにします。
3. サーバトラフィックのログ記録のポリシーを選択します。
   - [ブロックされる接続をログ記録]
   - [許可される接続をログ記録]

ステップ4: NAT（サーバがインターネットからアクセス可能な場合）

1. 該当するオプションを選択します。
   - [ゲートウェイの後に隠す（ネット転送）] - ポート転送によるアクセスを定義します。アプライアンスには、インターネット接続で設定する、外部のルーティング可能なIPアドレスがあります（デバイス）→[インターネットページ]。アプライアンスへのトラフィックのうち、ウィザードのステップ1でサーバオブジェクトに設定されたポートへのトラフィックは、サーバに転送されます。これにより、外部のルーティング可能なIPアドレスを使わながら、インターネットから組織（パブリックサーバ）へのトラフィックを許可します。
   - [このIPアドレスでサーバから外部へのトラフィックを隠す] - このチェックボックスをオンにして外部へのNATルールを作成します。オリジナルの発信元がサーバ（内部IPアドレス）となり変換されたIPアドレスがサーバの静的IPアドレスになります。
   - [NATなし] - このオプションは、[アクセス・ポリシー]→[NATコントロールページの[ゲートウェイの外部IPアドレスで内部ネットワークを隠す]チェックボックスをオフになっている場合のみ、該当します（詳細は上記参照）。つまり、サーバにNATルールがない状態です。

2. 同じポートを使う内部サーバが複数存在する場合、[リダイレクト元ポート]を選択して、インターネットからこのサーバにアクセスする際に使う別のポート番号を入力します。ここで入力するポート上のサーバに送られるトラフィックは、サーバのポートに転送されます。
3. [アドレス変換したトラフィックをゲートウェイに戻す]はデフォルトでオンになっています。これにより、ローカルネットワークを経由して内部ネットワークからサーバの外部IPアドレスへのアクセスを許可します。発信元は「このゲートウェイ」に変換されます。チェックボックスをオフの場合、発信元は[Any]となり、スイッチを経由した内部ネットワークから外部IPアドレスへのアクセスはなくなります。
   このオプションは、内部ソースからのトラフィックに重要ですが、現時点ではサーバへ送れるすべてのトラフィックソースが変換されて、ゲートウェイのIPアドレスで隠されます。

ウィザードを完了すると、ページのサーバリストに追加されて、自动生成されたアクセスルールが[アクセス・ポリシー]→[ファイアウォール・ルール・ページ]に追加されます。NATがサーバに定義されている場合、生成される転送ルールは[アクセス・ポリシー]→[ファイアウォール]のNATページに自動的に追加されます。

リモート・アクセスマポート設定を変更するには

デフォルトのリモート・アクセス・ポート（ポート443番）と、同じポートを使用するサーバ間で競合が生じる場合、メッセージが表示されます。サーバでポート443番を使用する場合は、デフォルトのリモート・アクセス・ポートを変更する必要があります。
1. リモート・アクセス・ポートの変更リンクをクリックします。
アプライアンスの設定

[リモート・アクセス・ポートの設定]ウィンドウが開きます。
2. [リモート・アクセス・ポート]に、新しいポート番号を入力します。
3. [ポート 443 番をポート転送に予約]がオンになっていることを確認します。
4. [適用]をクリックします。

注 - このページは、[アクセス・ポリシー]タブの[ファイアウォール]と[NAT]セクションからアクセスできます。

ユーザ認識

[ユーザ認識]ページでは、プレードをオン/オフに切り替えたり、設定ウィザードを使い、ユーザ認識の取得、ログ記録、設定目的のソースを設定することが出来ます。

Check Point 730/750 Appliance のユーザ認識では、IP アドレス・ベースのログではなく、ユーザ・ベースのログを確認でき、さらに個々のユーザやグループに対するアクセス制御を実施できます。

ユーザ認識を使用するためには、ユーザとユーザ・グループの情報を取得する認識メソッドを設定する必要があります。ゲートウェイでユーザのアイデンティティを取得したら、ユーザ・ベースのルールは[アクセス・ポリシー]のネットワークトラフィックで実施できます。

ユーザ認識では、認識するソースとして以下を使用できます。
- Active Directory クエリ - AD サーバに対するシームレスなクエリでユーザ情報を取り扱います。
- ブラウザベース認証 - ローカル定義のユーザの認証、または別の認識メソッドのバックアップとして、ポータルを使って認証可能。

AD クエリ

セキュリティ・ポリシーをインストールする際、Check Point 730/750 Appliance は、AD ドメイン・コントローラからセキュリティ・イベント・ログを受信するための登録を行います。これには、AD サーバの管理者権限が必要です。AD 認証情報を使ってユーザが認証を行うと、イベント・ログが生成されてセキュリティ・ゲートウェイに送られます。その後 Check Point 730/750 Appliance で、AD のセキュリティ・イベント・ログに基づいてユーザを認識します。

ブラウザベース認証

ブラウザベース認証では、ネットワーク・リソースやインターネットにアクセスするユーザの認証が Web インタフェースを使用します。保護されたリソースにアクセスするユーザは、まず Web ページにログインする必要があります。この方法は、ローカルで定義されたユーザや他の方法で識別できなかったユーザを識別するために使用します。すべてのトラフィックでブラウザベース認証を使用するように設定することもできますが、この場合、エンドユーザは認証をスムーズに受けることができなくなるため、一般的には、エンドユーザが特定のネットワーク・リソースやインターネットにアクセスする場合にのみこの方法を使用します。これにより、認証時のエンドユーザの手間を軽減することができます。HTTP ベースでないトラフィックについても、ブラウザベース認証で認証されていないユーザによる特定のリソースやインターネットへのアクセスをブロックするよう設定できます。

ユーザ認識のオン/オフを切り替えるには
[オン]または[オフ]オプションを選択します。
アプライアンスの設定

注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。


ウィザードを使用してユーザ認識を設定するには
1. [設定ウィザード] リンクをクリックします。
   （ユーザ認識ウィザード）が開きます。
2. 上で説明したユーザ識別方法を 1 つ以上選択し、[次へ] をクリックします。

Active Directory クエリを使用する場合:
Active Directory サーバが定義済みである場合は、[既存の Active Directory サーバを使用] をクリックします。

新しい Active Directory サーバを定義する場合、
1. [新しい Active Directory サーバの定義] をクリックします。
2. [ドメイン]、[IP アドレス]、[ユーザ名]、[パスワード]、[ユーザ DN] に入力します。[ユーザ DN] で[検索] をクリックして該当のユーザを表すオブジェクトの DN を自動検出するか、そのユーザの DN を入力します。
3. Active Directory に定義された一部のユーザ・データベースだけを使う場合は、[特定のブランチからのユーザ・グループのみ使用] をオンにします。[ブラウザ] にブランチ名を入力します。
4. [次へ] をクリックします。

ブラウザベース認証を使用する場合:
1. ポータルが使用できない場合に、認証されていないユーザによるアクセスをブロックするには、[Captive Portal が利用できない場合は認識できないユーザをブロック] をオンにします。この設定オプションを選択した場合、HTTP 以外の通信でアクセスしているユーザは、先にブラウザベース認証でログインするよう要求されます。
4. [完了] をクリックします。

ブラウザベース認証の設定を編集しポータルをカスタマイズするには
2. 必要に応じて、[認識] タブでウィザードでの設定内容を編集します。
3. [カスタム] タブで以下の該当するオプションを設定します。
   • [次の条件に対するユーザの承諾を求める] - ユーザが規約条件に必ず同意するように設定します。テキストボックスに、ユーザに表示する条件を入力します。
アプライアンスの設定

Check Point 730/750 Appliance Locally Managed Administration Guide R77.20.15 | 94

4. [詳細] タブで以下の設定を行います。

- [デフォルト使用] - デフォルトのロゴを使用します。

5. [適用]をクリックします。

注 - このページには、[アクセス・ポリシー]→[ユーザ認識ブレード・コントロール]または[ユーザ&オブジェクト]→[ユーザ認識]からアクセスできます。

QoS の設定 - 帯域幅の制御

[アクセス・ポリシー]→[QoS ブレード・コントロール]ページでは、QoS のアクティブ化、QoS のデフォルト・ポリシーの定義、手動ルールの追加を実行できます。

QoS（帯域幅・コントロール）ポリシーは、帯域幅のパラメータを設定して、ネットワーク通信のフローを制御するためのルール・セットです。これらのルールを使用して、ネットワークの通信が混雑したとき、重要なトラフィックを優先させることで業務への支障を最小限に抑えます。

QoSはインターネット接続でアクティブに設定できます。少なくとも2つのインターネット接続が、ISPが提供するダウンロード/アップロードの最高速度と共に設定されている必要があります。ダウンロード/アップロードの速度に関する詳細情報は、契約しているローカルISPに問い合わせてください。

このページでは、デフォルトの簡易QoSポリシーを設定できます。詳細のポリシーは[アクセス・ポリシー]→[QoSポリシー]ページで設定できます。

QoSポリシーは外部インターネットのトラフィックのみに適用されます。

QoS

いずれかのオプションを選択してアクセス・ポリシーのコントロール・レベルを設定します。

- オン - デフォルトのQoSポリシーを実施します。
- オフ - デフォルトのQoSポリシーは実施されません。

注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。
アプライアンスの設定

QoS デフォルト・ポリシー
デフォルトのQoSポリシーのオプションを選択します。また、[アクセス・ポリシー]→[QoS デフォルト・ポリシーページ]ですべてのチェックボックスをオフにすることで、QoSポリシーをすべて設定することも可能です。

- [遅延に影響されるサービスを対象に優先的に通信(VoIPなど)] - このオプションを選択して、遅延が起こると大きな支障が出るトラフィックを優先させます。たとえば、IPテレフォニー、ビデオカンファレンス、インタラクティブ・プロトコルなどは、Teinetのような短時間の応答時間が要求されます。
  [遅延に影響されるサービス]リンクをクリックして、含まれているデフォルトのサービスを確認し、必要に応じて新しく追加したり既存を削除したりします。QoSではこれらのパケットを他のパケットより先に送信します。このオプションにより、QoSポリシー・ルール・ベースにルールが追加されます。
- [X%の帯域幅を必ずすべてのサービスのVPN/すべてのトラフィックに保持] - このオプションを選択して、特定のトラフィックまたは選択したサービスに対して最低限の帯域幅を保証します。
  帯域幅率を入力し、必要に応じてトラフィックのタイプを変更します。必要であれば、[すべてのサービス]リンクをクリックして保証する選択したサービスのリストを編集します。このオプションにより、QoSポリシー・ルール・ベースにルールが追加されます。
- [帯域幅を大量消費するアプリケーションを制限] - 帯域幅を大幅に消費するアプリケーションは、大切な業務に必要なアプリケーションのパフォーマンスを低下させる可能性があります。
  [帯域幅を消費するアプリケーション]リンクをクリックして、含まれているデフォルトのアプリケーション/カテゴリを確認し、必要に応じて新しく追加したり既存を削除したりします。
  [帯域幅を大量消費するアプリケーションを制限]チェックボックスをオンにして、[ダウンロード]または[アップロード]のどちらかまたは両方を選択し、各選択オプションの制限と最大帯域幅を決定します。アプリケーション・コントロールを消費する帯域幅は、[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]と[ポリシー]ページでも設定できます。

保証するサービスをデフォルト・ポリシーに追加するには
1. [X%の帯域幅を必ずすべてのサービスのVPN/すべてのトラフィックに保持]を選択し、[サービス]リンクをクリックします。
  [保証するサービスの編集]ウィンドウが開きます。
2. [選択したサービス]を選択します。
3. [選択]をクリックして、選択できるサービスの一覧を表示します。該当するチェックボックスを選択します。
4. 必要なサービスが既存のリストにない場合は、[新規]をクリックします。新しいサービスの作成に関する情報は、[ユーザ&オブジェクト]→[サービス]ページを参照してください。
5. [適用]ボタンをクリックします。

QoSの使用
[アクセス・ポリシー]→[QoSポリシー]ページでは、QoSのデフォルト・ポリシーの管理、手動ルールの追加を実行できます。

ページのトップには、以下の制限に関する情報が表示されます。
- [帯域を消費するアプリケーション]ダウロードおよびアップロード・レートを[アクセス・ポリシー]→[QoSブレード・コントロール]ページまたは[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページで設定している場合、無効(disabled)リンクがある場合、クリックしてレートを設定します。
- 低遅延トラフィック - 遅延でないトラフィックのために保持できる最大帯域率が表示されます。最大率を設定しないと、それ以外のトラフィックの帯域が大幅に減る（場合によっては処理されない）可能性があります。値を変更するにはパーセンテージのリンクをクリックします。
アプライアンスの設定

QoS ポリシー・ルール・ベースはこのページで確認できます。各ルールには以下のフィールドが含まれます。

<table>
<thead>
<tr>
<th>フィールド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO.</td>
<td>QoS ポリシーのルール番号。</td>
</tr>
<tr>
<td>ソース</td>
<td>接続を開始するネットワーク・オブジェクト。</td>
</tr>
<tr>
<td>宛先</td>
<td>接続を完了するネットワーク・オブジェクト。</td>
</tr>
<tr>
<td>サービス</td>
<td>重み付け、制限、保証に応じて調整される帯域のネットワーク・サービス・タイプ。</td>
</tr>
<tr>
<td>保証/制限</td>
<td>トラフィックの帯域幅レートを制限するパーセンテージ、トラフィックの帯域幅を保証するパーセンテージを設定。トラフィックを低遅延として設定するオプションもあります。こうすることで優先的に処理されます。</td>
</tr>
<tr>
<td>重み付け</td>
<td>インターネット接続に設定された最大帯域トラフィックが超過した場合に利用可能な帯域を分けるための単位。以下を参照してください。</td>
</tr>
<tr>
<td>追跡</td>
<td>トラフィックがルールに一致した場合に実行する追跡とログ記録のアクション。</td>
</tr>
<tr>
<td>コメント</td>
<td>コメントを入力すると表示されるオプション・フィールド。デフォルト・ポリシーのシステム生成ルールの場合はメモが表示されます。</td>
</tr>
</tbody>
</table>

重み付け

重み付けに基づいて利用可能な帯域をQoSポリシーで分けます。パーセンテージでなく重み付けを使用するのは、特定のトラフィックに従って最大帯域幅が超過したとき、QoSエンジンで帯域を割り当てる柔軟な方法です。これにより、帯域を最大限に利用できます。

たとえば、ある組織でWebトラフィックの重要性はFTPトラフィックの重要性に比べて3倍だと考えます。このサービスのルールには重み付け30と10が割り当てられます。ラインが混雑する場合、QoSでWebトラフィックとFTPトラフィックに割り当てた帯域率(3と1)を維持します。

デフォルト・ポリシーにオプションを設定する、またはQoSポリシーに手動でルールを定義することができます。ルールですべての帯域幅を使わない場合、未使用の帯域幅は重み付けに従って残りのルールに分けられます。上記の例の場合、WebとFTPそれぞれ1つずつ接続がアクティブで競合しているとき、残りの帯域のうちWeb接続が75%(30/40)、FTPが25%(10/40)を受け取ることになります。Web接続が閉じると、FTP接続が100%受け取るようにになります。

[重み付け]フィールドで、他の定義されたサービスと比較したサービスの重要度を示す値を入力します。たとえば、あるサービスに重み付け100を指定し、別のサービスに50を指定した場合、ラインが混雑した際に最初のサービスには2つのサービスの2倍の帯域が割り当てられることになります。

QoSルールを作成するには

1. ［新規］の横にある矢印をクリックします。
2. ルールに指定可能な位置をいずれか1つクリックします。［一番上］、［一番下］、［選択したルールの上］、［選択したルールの下］から選んでクリックします。
   ［ルールの追加］ウィンドウが開きます。次の2種類のルール・フィールドが表示されます。
   - ルールの概要文とデフォルト値。
   - テーブル形式のルール・ベース・フィールド。
3. ルール・サマリのリンク、またはテーブルのセルをクリックして、ネットワーク・オブジェクトを選択するか、ルール・ベースのフィールド・オプションを選択します。上述の説明を参照してください。
注 - 特定のルールに特定の保証/制限を指定する、または低遅延トラフィックとしてマークすることができます。後者の場合、すべての低遅延トラフィックに対して最大制限バーセンテージをグローバルで設定します。上記を参照してください。
4. 着信ルールで、暗号化された VPNトラフィックのみを一致させるには、[暗号化トラフィックだけを一致]を選択します。[サービス]カラムには「暗号化」が表示されます（選択した場合）。
5. ルールを特定の時間に制限する場合は、[次の指定した期間だけ適用]を選択して、開始時間と終了時間を指定します。指定した期間中の接続だけが検査されます。
6. DiffServ Markは、サービス・パーティが処理するよう接続をマークする方法です。DSCPに従ってパブリック・ネットワークで優先度を指定するようパケットをマークするには、[DiffServマーク(1-63)]を選択して値を指定します。このオプションを使用するには、ISPまたはプライベートWANでDiffServがサポートされている必要があります。DSCPの値は、ISPまたはプライベートWAN管理者から取得できます。
7. [コメントの入力]フィールドでは、ルールを説明するテキストを入力します（オプション）。このテキストはルールの下にコメントとして表示されます。
8. [適用]をクリックします。
注 - QoSルール・ベースのルールの順序は、ドラッグ&ドロップで変更できます。

ルールを編集するには
アクセス・ポリシー・ルールでは、自動生成されたルールの追跡オプションのみ編集できます。
1. ルールを選択して、[編集]をクリックします。
2. 必要に応じてフィールドを編集します。
3. [適用]をクリックします。

ルールを削除するには
1. ルールを選択して、[削除]をクリックします。
2. 確認メッセージで[はい]をクリックします。

ルールを有効/無効にするには
- ルール・ベースに追加した、手動で定義したルールを無効にするには、ルールを選択して[無効]をクリックします。
- 一度無効にした、手動で定義したルールを有効にするには、ルールを選択して[有効]をクリックします。

ルールの順番を変更するには
1. 移動するルールを選択します。
2. 移動する場所ヘドラッグ・アンド・ドロップします。
3. 注 - 変更できるのは、手動で定義したルールの順番のみです。

NATの定義
[アクセス・ポリシー]→[ファイアウォール NAT]ページでは、外部へのトラフィックのNATを設定できます。またシステムで定義されているサーバーの数を確認できます。サーバーは[アクセス・ポリシー]→[サーバー]ページで定義され、アクセスとNAT設定を指定したネットワーク・オブジェクトとなります。これを、ルーティングするIPアドレスがなくても、インターネットからアクセス可能なサーバーを設定できます。このページで、NAT設定のサーバーを設定することもできます。
外部へのトラフィックの NAT を無効にするには（Hide NAT）

デフォルトでは、NAT は外部へのトラフィックに設定されます。NAT を無効にする必要がある場合、[ゲートウェイの外部 IP アドレスで内部ネットワークを隠す]がオフになっていますことを確認してください。

重要 - Hide NAT 機能をオフにすると、インターネット接続に問題が多く発生します。アプライアンスがインターネットにつながるオフィスのゲートウェイである場合は、ネットワーク担当者に必ず相談してからこのチェックボックスをオフにしてください。

インターネットからルーティング可能なサーバを設定するには（NAT のサーバ）

1. [新しいサーバ（転送ルール）] をクリックします。
2. サーバウィザードの使い方については、[アクセス・ポリシー]→[サーバ] ページを参照してください。
3. サーバウィザードの「アクセス」のステップで、このサーバにアクセス可能な場所を求められた場合、いずれかのオプションを選択します。
4. サーバウィザードの NAT のステップで、該当するオプションを選択します。
   - [ポート転送] - ポート転送によるアクセスを定義します。アプライアンスには、インターネット接続で設定する、外部のルーティング可能な IP アドレスがあります（[デバイス] →[インターネット] ページ）。アプライアンスへのトラフィックのうち、ウィザードのステップ 1 でサーバオブジェクトに設定したポートへのトラフィックは、サーバに転送されます。これにより、外部のルーティング可能な IP アドレスを使いながら、インターネットから組織（パブリック・サーバ）へのトラフィックを許可します。
   - [静的 NAT] - 静的 NAT によるアクセスを定義します。ルーティング可能な IP アドレスをサーバ用に購入した場合は、アドレスのフーパールドに入力します。残りの内部ネットワークがゲートウェイの外部 IP アドレスで隠れている場合、この特定サーバは自身のアクセス可能な IP アドレスを使用します。ウィザードのステップ 1 で設定したとおり、該当するポートの特定の IP アドレスへのトラフィックは、このサーバに転送されます。
     - [この IP アドレスでサーバから外部へのトラフィックを隠す] - このチェックボックスをオンにした場合、外部への NAT ルールを作成します。オリジナルの発信元がサーバ（内部 IP アドレス）になり変換ルールがサーバの静的 IP アドレスになります。
   - [NAT なし] - このオプションは、[アクセス・ポリシー] →[NAT コントロール] ページの[ゲートウェイの外部 IP アドレスで内部ネットワークを隠す]チェックボックスがオフになっている場合のみ、該当します（詳細は上記参照）。つまり、サーバに NAT ルールがない状態です。
5. 同じポートを使用する内部サーバが複数存在する場合、[リダイレクト元ポート] を選択して、インターネットからこのサーバにアクセスする際に使う別のポート番号を入力します。ここで入力するポート上のサーバに送られるトラフィックは、サーバのポートに転送されます。
6. [アドレス変換したトラフィックをゲートウェイに戻す] はデフォルトでオンになっています。これにより、ローカル・スイッチを経由して内部ネットワークからサーバの外部 IP アドレスへのアクセスを許可します。発信元は「このゲートウェイ」に変換されます。チェックボックスがオフの場合、発信元は [Any] となり、スイッチを経由した内部ネットワークから外部 IP アドレスへのアクセスはなくなります。
7. [完了] をクリックします。

詳細 - 手動 NAT ルール

注 - ほとんどの場合、手動 NAT ルールは必要ありません。経験豊富なネットワーク管理者でない場合は、このオプションを使用する必要はありません。

アドレス変換をより高度に設定するには、手動 NAT ルールを定義します。NAT のサーバが設定されている場合、手動の NAT ルールは適用されません。ただし、Hide NAT がアクティブになっても、これらのルールは有効になります。

NAT ルールのフィールドには以下が含まれます。

<table>
<thead>
<tr>
<th>フィールド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>元のソース</td>
<td>変換する接続のオリジナルのソースであるネットワーク・オブジェクト（特定 IP アドレス）またはネットワーク・グループ・オブジェクト（特定 IP アドレス範囲）。</td>
</tr>
<tr>
<td>元の宛先</td>
<td>変換する接続のオリジナルの宛先であるネットワーク・オブジェクト（特定 IP アドレス）またはネットワーク・グループ・オブジェクト（特定 IP アドレス範囲）。</td>
</tr>
<tr>
<td>元のサービス</td>
<td>変換する接続で使われるオリジナルのサービス。</td>
</tr>
<tr>
<td>変換後のソース</td>
<td>オリジナルのソース変換後となる、新しいソースであるネットワーク・オブジェクトまたはネットワーク・グループ・オブジェクト。</td>
</tr>
<tr>
<td>変換後の宛先</td>
<td>オリジナルの宛先変換後となる、新しい宛先であるネットワーク・オブジェクトまたはネットワーク・グループ・オブジェクト。</td>
</tr>
<tr>
<td>変換後のサービス</td>
<td>オリジナルのサービス変換後となる新しいサービス。</td>
</tr>
</tbody>
</table>

新しい NAT ルールを作成するには
1. [NAT ルール]の表がページに表示されない場合は、[NAT ルールの表示]リンクをクリックします。
2. [新規]の横にある矢印をクリックします。
3. ルールに指定可能な位置をいずれか 1 つクリックします。一番上、一番下、選択したルールの上、選択したルールの下があります。
   [手動 NAT ルールの追加]ウィンドウが開きます。次の 2 種類のルール・フィールドが表示されます。
   - ルールの概要文とデフォルト値。
   - テーブル形式のルール・ベース・フィールド。
4. ルール・サマリのリンク、またはテーブルのセルをクリックして、ネットワーク・オブジェクトを選択するか、ルール・ベースのフィールド・オプションを選択します。上述の説明を参照してください。
5. [コメントの入力]フィールドでは、ルールを説明するテキストを入力します（オプション）。このテキストは[NAT 手動ルール]のルールの下にコメントとして表示されます。
6. オリジナルのソースに複数の IP アドレス、IP 範囲、ネットワークなどを含め、さらに変換したソースを 1 つの IP アドレスにする場合は、[変換ソース アドレスの背後にある複数ソースを隠す]を選択します。
   このオプションが選択されていない場合、[元のソース]に IP 範囲を使用して、[変換ソース]に同じサイズの異なる IP 範囲を使用できます。このルールにより、IP アドレスの変換が 1 つの範囲から順番に行われます（最初の範囲の最初の IP は 2 番目の範囲の最初の IP、ということになります）。
7. [元の宛先 IP アドレスの ARP プロキシとして動作]を選択して、元の宛先の IP アドレスに送られた ARP リクエストに対してゲートウェイが応答するように設定します。これは、IP 範囲またはネットワークには適用されません。
8. ［適用］をクリックします。
手動ルールを作成すると、手動 NAT ルールのセクションの NAT ルール表に追加されます。

ルールを編集するには
アクセス・ポリシー・ルールでは、自動生成されたルールの追跡オプションのみ編集できます。
1. ルールを選択して、［編集］をクリックします。
2. 必要に応じてフィールドを編集します。
3. ［適用］をクリックします。

ルールを削除するには
1. ルールを選択して、［削除］をクリックします。
2. 確認メッセージで［はい］をクリックします。

ルールを有効/無効にするには
1. ルール・ベースに追加した、手動で定義したルールを無効にするには、ルールを選択して［無効］をクリックします。
2. 一度無効にした、手動で定義したルールを有効にするには、ルールを選択して［有効］をクリックします。

ルールの順番を変更するには
Note - you can only change the order of manually defined rules.
1. 移動するルールを選択します。
2. 移動する場所へドラッグ・アンド・ドロップします。

NAT サーバ・オブジェクトの定義
「サーバ・オブジェクトの定義」 (89ページ) を参照してください。

詳細 - NAT ルールの作成と編集

注 - ほとんどの場合、手動 NAT ルールは必要ありません。経験豊富なネットワーク管理者でない場合は、このオプションを使用する必要はありません。よく使用するオプションについては、[アクセス・ポリシー] → [NAT コントロール] ページを参照してください。

[アクセス・ポリシー] → [NAT 手動ルール] ページでは、カスタムの NAT ルールの作成や編集が可能です。NAT を使用するサーバが設定されている場合、手動の NAT ルールは適用されません。ただし、Hide NAT がアクティブになっても、これらのルールは有効になります。

NAT ルールのフィールドには以下が含まれます。

<table>
<thead>
<tr>
<th>フィールド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>元のソース</td>
<td>変換する接続のオリジナルのソースであるネットワーク・オブジェクト（特定 IP アドレス）またはネットワーク・グループ・オブジェクト（特定 IP アドレス範囲）。</td>
</tr>
<tr>
<td>元の宛先</td>
<td>変換する接続のオリジナルの宛先であるネットワーク・オブジェクト（特定 IP アドレス）またはネットワーク・グループ・オブジェクト（特定 IP アドレス範囲）。</td>
</tr>
</tbody>
</table>
新しい NAT ルールを作成するには

1. [新規]の横にある矢印をクリックします。
2. ルールに指定可能な位置をいずれか 1 つクリックします。[一番上]、[一番下]、[選択したルールの上]、[選択したルールの下]から選んでクリックします。
   [ルールの追加]ウィンドウが開きます。次の 2 種類のルール・フィールドが表示されます。
   - ルールの概要文とデフォルト値。
   - テーブル形式のルール・ベース・フィールド。
3. ルール・サマリのリンク、またはテーブルのセルをクリックして、ネットワーク・オブジェクトを選択します。上述の説明を参照してください。
4. [コメントの入力]フィールドでは、ルールを説明するテキストを入力します（オプション）。このテキストは[NAT 手動ルール]のルールの下にコメントとして表示されます。
5. オリジナルのソースに複数の IP アドレス、IP 範囲、ネットワークなどを含め、さらに変換したソースを 1 つの IP アドレスにする場合は、[変換ソース アドレスの後ろにある複数ソースを隠す]を選択します。
   このオプションが選択されていない場合、[元のソース]に IP 範囲を使用して、[変換ソース]に同じサイズの異なる IP 範囲を使用できます。このルールにより、IP アドレスの変換が 1 つの範囲から順番に行われます（最初の範囲の最初の IP は 2 番目の範囲の最初の IP、というように）。
6. [適用]をクリックします。

ルールを編集するには

アクセス・ポリシー・ルールでは、自動生成されたルールの追跡オプションのみ編集できます。

1. ルールを選択して、[編集]をクリックします。
2. 必要に応じてフィールドを編集します。
3. [適用]をクリックします。

ルールを削除するには

1. ルールを選択して、[削除]をクリックします。
2. 確認メッセージで[はい]をクリックします。

ルールを有効/無効にするには

- ルール・ベースに追加した、手動で定義したルールを無効にするには、ルールを選択して[無効]をクリックします。
- 一度無効にした、手動で定義したルールを有効にするには、ルールを選択して[有効]をクリックします。
ルールの順番を変更するには
1. 移動するルールを選択します。
2. 移動する場所へドラッグ・アンド・ドロップします。
3. 注 - 変更できるのは、手動で定義したルールの順番のみです。
脅威対策の管理

このセクションでは、侵入脅威対策システム（IPS）、アンチウイルス、アンチボット、およびアンチスパムBladeのセットアップおよび管理の方法について説明します。

脅威対策 Bladeの設定

【脅威対策】→【脅威対策ブレード・コントロール】ページでは、以下を有効にできます。

- 侵入防御システム（IPS） - ファイルやネットワーク・プロトコルの既知の脆弱性を悪用する不正な試みをブロックします。
- アンチウイルス - ウイルスに感染した危険なファイルをブロックします。
- アンチボット - ポットの検出、ポットとC&Cセンター間の通信のブロック、脅威の可視化を行います。ポットとは、悪意のあるソフトウェアで、ユーザのコンピュータをマルウェアに感染させる脅威があるものです。コンピュータがポットに感染すると、C&Cサーバによって悪用され、別の攻撃（スパム・メッセージを送信したりDoS攻撃をWebサイトに仕掛けるなど）を実行される可能性があります。感染には様々な経路があります。ファイル添付を開くことで脆弱性を悪用したり、Webサイトにアクセスすることで悪質なファイルをダウンロードしたり、というのが代表的な例です。

注 - アンチボットとアンチウイルスは同じ場所で設定します。

このページでは、攻撃や感染を防ぐようブレードの機能を有効することも、検出すのみの設定にすることもできます。ページの上部には、感染したホストの数が表示されます。詳細情報については、【詳細】をクリックしてください。アンチウイルスとアンチウイルスのマルウェア数とIPS攻撃の数は、各ブレードの【オン】/【オフ】スイッチの横に表示されます。また、ログを利用して、システムに攻撃が発生しているかどうかを見ることもできます。【ログモニタリング】→【セキュリティ・ログ】ページを参照してください。

Check Pointでは、シグネチャに基づく保護機能の大規模なデータベースを使用しており、このページではデフォルトの推奨ポリシーが設定されています。ポリシーを編集して、組織環境の接続性とセキュリティを最適にするIPSポリシー、アンチウイルスおよびアンチボット・ポリシーを設定することができます。各ポリシーは、その重大度、パフォーマンスへの影響、信頼性レベルに応じて、異なる性質の保護機能を提供します。

IPS/アンチウイルス/アンチボット・ブレードを有効/無効にするには

1. 【オン】または【オフ】を選択します。
2. 【適用】をクリックします。

注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。

IPS

IPSポリシーを設定するには

1. 【IPS】セクションで【編集】をクリックします。
2. いずれかのオプションを選択します。
   - 【厳格】 - セキュリティを重視した保護プロファイル。
   - 【標準】 - セキュリティ/パフォーマンスのバランスが最適化された、小中規模環境に最適な保護プロファイル。これはデフォルト・オプションです。
カスム IPS ポリシーを設定するには

各保護機能には、Check Point IPS サービスでレベルが定義される次の 3 つの定義パラメータがあります。「重大度」（対象となる脅威の深刻さ）、「コンフィデンス・レベル」（信頼性レベルの低い保護機能は幅広い攻撃に対する防御を提供するため、誤検出が多くなる可能性があります）、「パフォーマンスへの影響」（保護機能を有効にすることによるアプリアンスのパフォーマンスへの影響）です。

また保護機能は、サーバを保護するものとクライアントを保護するものに分類されます。

1. 有効にする保護機能のタイプを以下の中から選択します。
   - [クライアント保護]
   - [サーバ保護] - インターネットからアクセス可能なサーバが組織のネットワーク環境に存在しない場合は、このオプションをオフにできます。

2. 以下の各保護パラメータの 1 つ以上のレベルに従って、どの保護機能を無効にするかを選択します。
   - [重大度が次を下回る保護を無効] - 保護機能を無効にする重大度を指定できます。
   - [コンフィデンスレベルが次を下回る保護を無効] - 保護機能を無効にする信頼性レベルを指定できます。
   - [パフォーマンスへの影響が次を上回る保護を無効] - 保護機能を無効にするパフォーマンスへの影響レベルを指定できます。

3. プロトコル・アノーマリに対して保護機能を無効にする場合は、[プロトコル・アノーマリを無効にする]を選択します。
   - ほとんどの IPS 保護機能は、脆弱性を悪用する不正な試みを防御するためのものですが、保護機能にはこのほかにも以下の 2 つのタイプがあります。
   - プロトコル・アノーマリ - このタイプの保護機能は、プロトコル違反を検出してブロックします。
   - プロトコル制御 - このタイプの保護機能は、特定のプロトコルまたはファイルの使用を検出してブロックします。このタイプの保護機能を使用すると、組織のポリシーに従って特定のプロトコルやファイルをブロックできます。これは、IPS Software Blade が提供するアクセス制御の一機能です。プロトコル制御の保護機能は、IPS ポリシーによって自動的には有効化されません。[脅威対策] → [IPS 保護機能] ページから、企業のポリシーに従ってそれぞれを確認して手動で有効にすることができます。

4. また、すべてのポリシーパラメータを [高] または [標準] の保護プロファイルと同じ設定にした後、前述の手順に従って手動で調整を加えることもできます。そのためには、[デフォルト設定の読み込み] と使用するプロファイルを選択します。

5. [適用] をクリックします。

アンチボット

アンチボット・ポリシーは、有効に設定された保護機能のセットと、それに一致するトラフィックの検査処理方法に基づくポリシーです。保護機能によりネットワークに対する脅威を防御および管理することができます。保護の詳細については、「Check Point ThreatWiki」を参照してください。[脅威対策] → [エンジン設定] ページのリンクからアクセスできます。

以下の基準に従って保護を有効にしてください。

- コンフィデンス・レベル - コンフィデンス・レベルは、Software Blade で認識された攻撃が本当にボットトラフィックかどうかの信頼レベルです。一部の攻撃タイプは見分けがつくにくく、通常のトラフィックが脅威だと誤認識される場合もあります。コンフィデンス・レベルの値、保護機能によって特定の攻撃を正しく認識できる正確度を表します。保護機能のコンフィデンス・レベルが高いと、チェック・ポイン
トで攻撃だと認識されたものが実際に攻撃であるという確信が高いことになります。コンフィデンス・レベルが低いと、正規のトラフィックが攻撃だと誤認識される可能性があることを意味します。

- **保護アクション - 一致するトラフィックで実施するアクション。アクションの通知は、追跡オプションにしたがって設定されます（なし、ログ記録、アラートとログ記録）。**
  - ブロック - ボットだと認識されたトラフィックがゲートウェイを通過するのを防ぎます。
  - 検出 - ボットだと認識されたトラフィックはゲートウェイを通じますが、検出とログ記録が行われます。
  - 確認 - ユーザが確認して許可するまでトラフィックはブロックされます。アンチボットのユーザ・メッセージ設定は、「脅威対策」→「エンジン設定」ページを参照してください。
  - 非アクティブ - 保護機能が無効であることを示しています。

- **パフォーマンスへの影響 - セキュリティ・ゲートウェイのパフォーマンスに対する影響レベルを示します。**

アンチウイルス
アンチウイルス・ポリシーは、有効に設定された保護機能のセットと、それに一致するトラフィックの検査処理方法に基づくポリシーです。

以下の基準に従って保護を有効にしてください。

- **コンフィデンス・レベル - コンフィデンス・レベルは、Software Blade で認識された攻撃が本当にウイルスかどうかの信頼レベルです。一部の攻撃タイプは見分けがつきにくく、通常のトラフィックが脅威だと誤認識される場合もあります。コンフィデンス・レベルの値は、保護機能によって特定の攻撃を正しく認識できる確率を表します。保護機能のコンフィデンス・レベルが高いと、チェック・ポイントで攻撃だと認識されたものが実際に攻撃であるという確信が高いことになります。コンフィデンス・レベルが低いと、正規のトラフィックが攻撃だと誤認識される可能性があることを意味します。**

- **保護アクション - 一致するトラフィックで実施するアクション。アクションの通知は、追跡オプションにしたがって設定されます（なし、ログ記録、アラートとログ記録）。**
  - ブロック - ヴィルスだと認識されたトラフィックがゲートウェイを通過するのを防ぎます。
  - 検出 - ヴィルスだと認識されたトラフィックはゲートウェイを通じますが、検出とログ記録が行われます。
  - 確認 - ユーザが確認して許可するまでトラフィックはブロックされます。アンチウイルスのユーザ・メッセージをカスタマイズするには、「脅威対策」→「エンジン設定」ページを参照してください。
  - 非アクティブ - 保護機能が無効であることを示しています。

- **パフォーマンスへの影響 - セキュリティ・ゲートウェイのパフォーマンスに対する影響レベルを示します。**

アンチボット/アンチウイルスのポリシーを設定するには
1. 「アンチボット」または「アンチウイルス」セクションで「編集」をクリックします。
2. 各コンフィデンス・レベル（高、中、低）に対し、リストから該当するアクション（ブロック、検出、確認、非アクティブ）を選択します。
3. 「パフォーマンスの影響度」で、許可する影響レベルを選択します（低、中-低、高-中）。
4. 「追跡オプション」で、いずれかのオプションを選択します。
  - なし - ログ記録しない。
  - ログ - ログを作成する。
  - アラート - アラートとログ記録。
5. ポリシーのデフォルト値を復元する必要がある場合は、「デフォルトに戻す」をクリックします。「適用」をクリックします。
アップデート
サービス・ブレードとして、アップデートをダウンロードする間隔を設定する必要があります。

アップデートをスケジュールするには
1. ページの下にあるアップデートのスケジュール・リンクをクリックしてください。アップデート・ステータスの横にあるアイコン上でリンクを選択することもできます。
2. アップデートのスケジュールを設定するブレードを選択します。それ以外のブレードについては、新しいアップデート・パッケージが利用可能になり、「最新ではありません」というメッセージがステータス・バー（WebUI アプリケーションの下部）に表示されていたり、手動でアップデートする必要があります。
3. [繰り返し]の間隔を選択します。
   • [毎日] - 時刻を指定します。
   • [毎週] - 曜日と時刻を指定します。
   • [毎月] - 日にちと時刻を指定します。
4. [適用]ボタンをクリックします。

ブロック・モードと検出のみモードを切り替えるには
1. 該当するチェックボックスをオンまたはオフにします。
   • IPS - 検出のみ (IDS)
   • アンチボット/アンチウイルス - 検出のみ
2. [適用]をクリックします。

検出のみのモードでは、ログ記録だけ行い、ブレードによってトラフィックはブロックされません。

IPS アップデートをオフラインでインポートするには
一部の組織では、インターネットに接続しないゲートウェイで IPS が必要になる場合があります。このような場合にオフラインの IPS アップデート・パッケージを入手するには、Check Point のサポートまでお問い合わせください。
1. ページの下部にある[手動でインポート]をクリックします。
2. Check Point のサポートから入手したオフライン・パッケージ・ファイルの場所を参照します。
3. [インポート]をクリックします。

IPS 例外の設定
[脅威対策]→[例外]ページでは、アンチウイルスおよびアンチボットの IPS エンジンおよびマルウェア・エンジンで検査されないトラフィックに例外ルールを設定できます。

IPS の例外
新しい IPS 例外ルールを追加するには
1. [IPS の例外]セクションで[編集]をクリックします。
2. ルール・サマリまたは表のセル中のリンクをクリックして、例外ルールの各フィールドに挿入するネットワーク・オブジェクトまたはオプションを選択します。
   • [保護] - すべての IPS 保護機能を選択するか、リストから特定の IPS 保護機能を選択します。
   • [ソース] - 接続を開始するネットワーク・オブジェクト。
   • [宛先] - 接続先となるネットワーク・オブジェクト。
アプライアンスの設定

- 『サービス/ポート』 - ネットワーク・サービスの種類。特定のサービス/ポートに対する特定の保護機能に例外を設定すると、その保護機能の効果が失われる可能性があります。

3. 『コメントの記入』フィールドにコメントを入力します（オプション）。

4. 『適用』をクリックします。

マルウェアの例外

脅威対策では、『スコープ』で指定したすべてのオブジェクトに対するトラフィックを検査します。指定したオブジェクトの接続が確立していない場合でも、検査は行われます。ファイアウォール・ルールのソース/ターゲットは、接続が確立したオブジェクトを定義しているため、相違点として重要です。

脅威対策では、MyWebServer に送られるすべてのファイルに対してマルウェア脅威のインスペクションを実行します。MyWebServer で接続が確立されていなくても、インスペクションが行われます。

スコープには、以下のタイプがあります。
- Security Gateway、クラスタ、サーバ、ネットワークなどのネットワーク・オブジェクト
- ネットワーク・オブジェクト・グループ
- IP アドレスの範囲
- ローカル・ユーザ

新しいマルウェア例外ルールを追加するには

1. 『マルウェアの例外』セクションで、『新規』をクリックします。

2. ルール・サマリまたは表のセル中のリンクをクリックして、例外ルールの各フィールドに挿入するネットワーク・オブジェクトまたはオプションを選択します。
- スコープ - 任意を選択するか、リストから特定のスコープを選択します。
- 保護 - 『すべてのマルウェア』、『すべてのアンチボット』、『すべてのアンチウイルス』のいずれかを選択します。特定の保護は設定できません。特定の保護に対して例外を設定する場合は、『脅威対策』→『感染したホスト』ページを参照してください。
- アクション - 一致するトラフィックで実施するアクションを、『確認』『ブロック』『検出』『非アクティブ』から選びます。アクション・タイプの説明は、『脅威対策』→『脅威対策ブレード・コントロール』ページを参照してください。
- ログ記録 - 追跡オプションとして『なし』『ログ』『アラート』から選びます。ログのテーマの説明は、『脅威対策』→『脅威対策ブレード・コントロール』ページを参照してください。

3. オプション: 『コメントの記入』フィールドにコメントを入力します（オプション）。

4. 『適用』ボタンをクリックします。

ファイルと URL のホワイトリスト

ファイルや URL を指定し、アンチボットとアンチウイルスでスキャンや分析を行わないよう設定できます。たとえば、安全だとわかっているファイルが分析時に誤検知される可能性がある場合は、ファイルのホワイトリストに追加します。

ファイルまたは URL をホワイトリストに追加するには

1. 『ファイルのホワイトリスト』または『URL ホワイトリスト』を選択します。

2. 『新規』をクリックします。
  『ファイルの追加』または『URL の追加』ウィンドウが開きます。

3. ファイルの場合は、指定ファイルのデジタル署名を作成する MD5 チェックサムを入力します。
アプライアンスの設定

4. URL の場合は、URL を入力します。
5. ［適用］をクリックします。

例外ルールを編集または削除するには
1. 該当するルールを選択します。
2. ［編集］または［削除］をクリックします。

感染ホストの表示

［感染ホスト］ページでは、内部ネットワークで感染したホストとサーバの情報を確認することができます。また、感染または感染の疑いがあるホスト/サーバに関連する特定の保護に対して、例外ルールを直接作成することもできます。

感染ホストテーブルには、各エントリの次の情報が表示されます。

• アイコン - 感染ホストやサーバの異なる分類を示すアイコン

<table>
<thead>
<tr>
<th>説明</th>
<th>ホストアイコン</th>
<th>サーバアイコン</th>
</tr>
</thead>
<tbody>
<tr>
<td>感染ホスト/サーバ - 特定の保護により、アンチボットでホストまたはサーバと外部の C&amp;C センター間での疑わしい通信が検出されたとき</td>
<td><img src="https://example.com" alt="アイコン" /></td>
<td><img src="https://example.com" alt="アイコン" /></td>
</tr>
<tr>
<td>感染の疑いがあるホスト/サーバ - 特定の保護により、アンチウイルスでホストやサーバの感染につながる可能性があるアクティビティが検出されたとき</td>
<td><img src="https://example.com" alt="アイコン" /></td>
<td><img src="https://example.com" alt="アイコン" /></td>
</tr>
<tr>
<td>感染したインターネット・サイトや安全でないインターネット・サイトにアクセスすると、マルウェアインストールしてしまう可能性があります。</td>
<td><img src="https://example.com" alt="アイコン" /></td>
<td><img src="https://example.com" alt="アイコン" /></td>
</tr>
<tr>
<td>感染したファイルをダウンロードすると、そのファイルを開く際にホストやサーバを感染させてしまう可能性があります。</td>
<td><img src="https://example.com" alt="アイコン" /></td>
<td><img src="https://example.com" alt="アイコン" /></td>
</tr>
</tbody>
</table>

• オブジェクト名 - ホストまたはサーバがネットワーク・オブジェクトとして設定された場合オブジェクト名が表示されます。

• IP/MAC アドレス

• デバイス/ユーザ名 - DHCP またはユーザ認証により Check Point 730/750 Appliance が情報を確認できた場合、デバイス/ユーザ名が表示されます。

• インシデント・タイプ - 検出されたインシデントのタイプ:
  • ボットのアクティビティ
  • マルウェアのダウンロード
  • マルウェアを持つサイトへのアクセス

• 深刻度 - マルウェアの深刻度レベル:
  • 低
  • 中
  • 高
  • クリティカル

• 保護名 - アンチボット/アンチウイルスの保護機能名が表示されます。

• 最終インシデント - 最後のインシデントの日付。
インシデント - 先月のホストまたはサーバのインシデントの合計件数。大量にある場合は期間が短くなる場合があります。

感染ホストリストを絞り込むには
1. [絞り込み]をクリックします。
2. いずれかの絞り込みオプションを選択します。
   - サーバのみ - サーバとして識別されるマシンのみが表示されます（任意のマシン/デバイスではない）。サーバは[アクセス・ポリシー]→[サーバ]ページで定義され、システムのサーバ・オブジェクトとして定義されます。
   - 感染の疑いがあるホストのみ - 感染の疑いがあるホストまたはサーバのみが表示されます。
   - 感染したホストのみ - 感染したホストまたはサーバのみが表示されます。
   - 深刻度が「高」以上のホスト - マルウェアに感染または感染の疑いがあり、深刻度が「高」「クリティカル」なホストおよびサーバが表示されます。

特定の保護にマルウェア例外ルールを追加するには
1. 例外を作成する保護を含むリストのエントリを選択します。
2. [保護機能の例が義の追加]をクリックします。
3. ルール・サマリまたは表のセル中のリンクをクリックして、例外ルールの各フィールドに挿入するネットワーク・オブジェクトまたはオプションを選択します。
   - スコープ - 任意を選択するか、リストから特定のスコープを選択します。
   - アクション - 一致するトラフィックで実施するアクションを、[確認][ブロック][検出][非アクティブ]から選びます。アクション・タイプの説明は、[脅威対策]→IPSの[インスタンス管理]→[セキュリティ・ログ]ページにログが表示されます。アラートはログのフラグです。フラグを使ってログを絞り込むことができます。
4. [コメントの記入]フィールドにコメントを入力します（オプション）。
5. [適用]をクリックします。
   ルールは[脅威対策]→[例外]ページのマルウェアの例外に追加されます。

特定エントリのログを表示するには
1. 表示するログのリストのエントリを選択します。
2. [ログ]をクリックします。
   [ログ]→[セキュリティ・ログ]ページが開いてIP/MACアドレスに該当するログが表示されます。

注 - このページには、[ホーム]および[ログ・モニタリング]タブからアクセスできます。

保護リストの表示
[脅威対策]→[IPS保護リスト]ページでは、IPSのサービス・ブレードとしてアプライアンスでダウンロードしたシグネチャ・ベースの保護機能が表示されます。保護機能は、[脅威対策]→IPSの[ブレード・コントロール]ページで設定したポリシーに基づいて、アクティブになっているかどうかがわかります。
各保護の詳細を確認でき、さらに各保護のアクションや追跡オプションを手動でオーバーライドするよう設定することもできます。

絞り込みボックスに名前を入力して特定の保護を検索したり、[次へ]と[前へ]のページ・ボタンを使い、ページをスクロールして探すこともできます。

IPS の例外を管理するフィールドは以下のとおりです。

- [保護(Protection)] - IPS 保護の名前
- [保護タイプ(Protection Type)] - 保護がサーバ、クライアント、または両方に適用されるかどうか
- [カテゴリ(Category)] - 保護のカテゴリ
- [アクション(Action)] - この保護に対するファイアウォールの処理。「上書き」は手動オーバーライド
- [深刻度(Severity)] - 攻撃を受けた場合の深刻さレベル
- [コンフィデンス(Confidence)] - 認識した攻撃が実際に望ましくないトラフィックであるかどうかを示す IPS での信頼レベル
- [パフォーマンス(Performance)] - 保護機能とリソースがゲートウェイ/サーバのパフォーマンスに及ぼす影響

特定の保護設定を手動で上書きするには

1. リストから保護を選択します。
2. [編集]をクリックします。
   [保護設定]ウィンドウが開きます。
3. [IPS ポリシー・アクションの上書き]チェックボックスをオンにして、該当するオプションを選択します。
   - Prevent (ブロック)
   - Detect (検出)
   - Inactive (非アクティブ)

   保護のアクションは、IPS ポリシー設定の影響は受けなくなります。
4. 保護の[追跡]オプションを選択します。
5. [適用]をクリックします。

脅威対策のエンジン設定

[脅威対策]→[脅威対策エンジン設定]ページでは、アンチウイルス、アンチボット、IPS エンジンの詳細設定を行うことができます。

注 - 以下の設定の多くは高度な内容となっているため、熟練の管理者以外の方は使用しないようにしてください。

アンチウイルス

アンチウイルスを設定するには

1. いずれかの保護スコープ・オプションを選択します。
   - ["X"インタフェースからの外部からのファイルをスキャン - [X]を指定します。
     - 外部および DMZ - 外部および DMZ インタフェースから送られるファイルをインスペクトします。
     - 外部 - 外部インタフェースから送られるファイルをインスペクトします。
     - すべての - すべてのインタフェース間で転送されるファイルをインスペクトします。
アプライアンスの設定

2. 指定したスコープでスキャンするプロトコルを選択します。
   - HTTP（任意のポート）
   - メール（SMTPとPOP3）
   - FTP

3. いずれかのファイル・タイプ・ポリシーを選択します。
   - 既知のマルウェアが含まれるファイル・タイプを処理
   - すべてのファイル・タイプを処理
   - 特定のファイル・タイプを処理

設定可能なアクションは以下のとおりです。
   - スキャン - アンチウイルスエンジンでこのタイプのファイルをスキャンします。
   - ブロック - アンチウイルスエンジンでこのタイプのファイルがブロックされ、ファイルは通過しません。
   - 通過 - アンチウイルスエンジンでこのタイプのファイルはスキャンされず、そのまま通過します。

システム定義のファイル・タイプは削除できません。システム定義のファイル・タイプは、変更できないビルトイン・シグネチャによって識別されます。手動で定義したファイル・タイプは拡張子で識別され、Webおよびメール・プロトコルでサポートされます。

4. [ポリシー上書き]を設定して、脅威対策の [ブレード・コントロール] ページで定義される一般的なポリシー設定を上書きできます。以下の各保護タイプ・オプションに対し、確認、ブロック、検出、非アクティブ、ポリシーに基づく、のいずれかのアクションを設定できます。アクション・タイプの説明は、[脅威対策] → [ブレード・コントロール] ページを参照してください。

アンチボット

[ポリシー上書き]を設定して、脅威対策の [ブレード・コントロール] ページで定義される一般的なポリシー設定を上書きできます。以下の各保護タイプ・オプションに対し、確認、ブロック、検出、非アクティブ、ポリシーに基づく、のいずれかのアクションを設定できます。アクション・タイプの説明は、[脅威対策] → [ブレード・コントロール] ページを参照してください。

- 不正なアクティビティ - ポットネットやマルウェアの特定ファミリのユニーサルな通信に関する保護。
- [レピュテーション・ドメイン] - C&Cサーバに関連する保護。各ホストはチェック・ポイントのThreatCloudレピュテーション・データベースでチェックされます。
- [レピュテーション・IP] - C&Cサーバに関連する保護。各IPはチェック・ポイントのThreatCloudレピュテーション・データベースでチェックされます。
- [レピュテーション・URL] - C&Cサーバに関連する保護。各URLはチェック・ポイントのThreatCloudレピュテーション・データベースでチェックされます。
- [通常とは異なるアクティビティ] - ポットネットやマルウェアのアクティビティとして知られる振る舞いパターンに関連する保護。
アンチウイルスおよびアンチボットのユーザ・メッセージ

確認アクションでは、保護タイプに応じてメッセージをカスタマイズできます。確認アクションが設定されている保護タイプとトラフィックが一致すると、ユーザのインターネット・ブラウザで新しいウィンドウにメッセージが表示されます。

確認アクションのオプションと関連する通知は以下のとおりです。

<table>
<thead>
<tr>
<th>オプション</th>
<th>アンチウイルス通知</th>
<th>アンチボット通知</th>
</tr>
</thead>
<tbody>
<tr>
<td>確認</td>
<td>ユーザにメッセージが表示され、悪質だと分類されているサイトへのアクセスまたはファイルのダウンロードを続行するかどうかを確認します。</td>
<td>ユーザにメッセージが表示され、ユーザのコンピュータが悪質なサーバへアクセスしようとしていることを通知します。</td>
</tr>
<tr>
<td>ブロック</td>
<td>ユーザにメッセージが表示され、サイトはブロックします。</td>
<td>アンチボットでバックグラウンドのプロセスはブロックされます。ブラウザから悪質なサーバへの特定操作がブロックされると、ユーザにメッセージが表示されます。</td>
</tr>
</tbody>
</table>

メッセージをカスタマイズするには

1. [アンチウイルス・ユーザ・メッセージのカスタマイズ]または[アンチボット・ユーザ・メッセージのカスタマイズ]をクリックします。
2. 次のタブでオプションを設定します。
   - 確認
   - ブロック
3. 各通知のフィールドを設定します。
   - タイトル - デフォルトのままにするか、新しくタイトルを入力します。
   - サブジェクト - デフォルトのままにするか、新しくサブジェクトを入力します。
   - 本文 - デフォルトのままにするか、新しく本文を入力します。[オプション・キーワード]をクリックして、ユーザへの情報の本文に使用できるキーワードのリストを表示できます。
   - 無視する場合（確認のみ） - ユーザがメッセージを無視する場合、このテキストとチェックボックスが表示されます。デフォルトのままにするか、新しくテキストを入力します。
   - ユーザは必ず理由を入力（確認の場合のみ） - ユーザがアクティビティの理由を入力する必要があるときにこのチェックボックスを選択します。ユーザ・メッセージには理由を入力するテキストボックスがあります。
   - フォールバック（確認のみ） - 通知がブラウザまたはアプリケーションに表示されず、その通知が表示される場合（主にWebアプリケーション以外）、代わりのアクション（ブロック/許可）を選択します。
     - フォールバックが許可の場合 - ユーザはWebサイトまたはアプリケーションにアクセスできます。
     - フォールバックがブロックの場合 - Webサイトまたはアプリケーションはブロックされ、ユーザに通知は表示されません。
   - 頻度 - アンチウイルスまたはアンチボットの確認メッセージがユーザに表示される回数を設定できます。
     - 毎日
     - 毎週
     - 毎月
   - ユーザをURLにリダイレクト（ブロックのみ） - ユーザを外部のポータル（ゲートウェイ以外）にリダイレクトできます。[URL]フィールドに、外部ポータルのURLを入力します。URLには外部システム
アプライアンスの設定

ムを指定できます。ユーザから認証情報（ユーザ名/パスワードなど）を受け取り、この情報をゲートウェイに送ります。


5. [適用]をクリックします。

IPS

IPS エンジンによる保護の範囲を変更するには

いずれかのオプションを選択します。

- [内部ホストのみ保護] - IPS エンジンは、組織内のクライアントおよびサーバを対象とした攻撃に対してのみ保護を行います。この場合、ネットワーク外のホストを保護するためにリソースを消費することがなくなります。

- [すべてのトラフィックに IPS インスペクションを実行] - リソースの消費量が多くなるため、なるべく使用しないことをお勧めします。

アプライアンスの負荷増大時に IPS エンジンをバイパスするよう設定するには

1. [負荷時のバイパス]チェックボックスをオンにします。

2. [設定]をクリックして、IPS エンジンのバイパス・モードとインスペクション・モードを切り替えるしきい値を選択します。表示されるウィンドウの手順に従い、[適用]をクリックします。

3. [負荷時のバイパスの追跡]で発行するログのタイプを選択し、この機能の追跡オプションを設定します。

追跡設定を変更するには

イベント追跡オプションとして、[ログ]または[アラート]（特に重要なログとして表示）を選択します。

このページで行ったすべての変更を適用するには

[適用]をクリックします。

アンチスパム Blade の設定

[脅威対策]→[アンチスパム・ブレード・コントロール]ページでは、アンチスパム・エンジンを有効にして、スパムの疑いがある E メールをブロックする、またはフラグを立てることができます。

このページでは、ブレードを有効にして該当のメールを識別する、ブロックする、フラグを付ける、または検出モードに設定してログ記録を利用し、システムがスパム攻撃を受けていないかどうかを調べたりすることができます。

チェック・ポイントでは、発信元アドレスからほとんどのスパム・メールを識別することができます。また、メールの内容で識別も行います。スパム・メールをブロックして内部のメール・サーバで処理方法を決定するためにフラグを使う設定にする、という方法ではなく、スパムの疑いがあるメールにシステムでフラグを付けるよう設定し、簡潔にできます。フラグは、スパムの疑いがあるメールを削除したくない場合によく使用されます。メールの内容はクラウドで検査され、その後メールの処理方法についてアプライアンスに通知が送られます。
アプライアンスの設定

スパムの疑いがあるメールは、既知のスパムと同じように処理することも、チェックボックスをオンにして疑わしいスパムとして別に処理することもできます（下記参照）。

アンチスパム Software Blade を有効/無効にするには
1. [オン]または[オフ]を選択します。
2. [適用]をクリックします。

アンチスパム・エンジンを検出のみに設定するには
1. [検出のみ]チェックボックスをオンにします。
2. [適用]をクリックします。

アンチスパム・ポリシーを設定するには
スパムのフィルタリングでは、常に送信者の発信元アドレスを基に検査を行います。この検査方法で、多くのスパム・メールをすばやく処理することができます。これに加え、メールの内容を検査することで残りのスパム・メールをフィルタリングすることができます。これを行うためには、[メールの内容]チェックボックスがオンになっていることを確認します。スパムの内容が含まれているメールに実行するアクションを選択します。

・ スパム・メールをブロック
・ フラグを付けて件名に次を追加 - 手動で定義したテキストをスパム・メールの件名に追加します。
・ メールのヘッダにフラグを付ける - このオプションにより、メールのメッセージのヘッダでスパム・メールを識別します。

必要な場合は追跡オプションとして、[ログ記録]または[アラート]のどちらか選択をします（重要なログとして表示）。

スパムの疑いがあるメールを既知のスパムとは別に処理するには
1. スパムの疑いがあるメールを既知のスパムとは別に処理するには
2. オプション（ブロック、件名にフラグを付ける、ヘッダにフラグを付ける）を選択します。

フラグオプションを選択すると、疑わしいスパム・メールにフラグを付ける際に使用するテキストを編集できます。デフォルトは"[SUSPECTED SPAM]"です。フラグのオプションはスパムと疑わしいスパムに設定できます。フラグを付けるアクションに別の文字列を指定してオプションを使うことができます。
3. トラッキング・オプションを選択します。
4. [適用]をクリックします。

アンチスパムの例外の設定
[脅威対策]→[アンチスパムの例外]ページでは、
・ メールを検査する必要のない安全な送信者（メール・アドレス）/ドメイン、または IP アドレスを設定できます。
・ 分類に関係なく、アンチスパム・エンジンでブロックする特定の送信者、ドメイン、IP アドレス。
送信者別にブロック/許可するためには、アンチスパム・エンジンがメールの内容に基づいてフィルタリングするよう設定する必要があります。これは、【脅威対策】→【アンチスパム・ブレード・コントロール】ページで行います。

注 - IP アドレスの例外については、POP3 トラフィックでは無視されます。

新しい送信者/ドメイン/IP アドレスを許可またはブロック・リストに追加するには
1. 許可またはブロックのリストから【追加】または【新規】をクリックします。
2. IP アドレスまたは送信者/ドメインを入力します。
3. 【適用】をクリックします。

許可/ブロック・リストの送信者/ドメイン/IP アドレスを編集または削除するには
1. 許可/ブロック・リストの該当する行を選択します。
2. 【編集】または【削除】をクリックします。オプションが表示されていない場合は、絞り込みボックスの横にある矢印をクリックします。
VPN の管理

このセクションでは、リモート・アクセス VPN およびサイト間 VPN の設定および管理の方法について説明します。

リモート・アクセス・ブレードの設定

[VPN]→[リモート・アクセス・ブレード・コントロール]ページでは、安全かつ暗号化されたインターネット接続を、自宅のコンピュータと組織の間に確立させるための機能を有効にできます。

リモート・アクセス機能を利用するためには、認証情報を持つシステムのユーザの定義と、特定ユーザに設定する権限が必要です。また、アプライアンスをインターネットからアクセスできる状態にしておく必要があります。

リモート・アクセス接続は以下の方法がサポートされています。

- 自宅のコンピュータに VPN クライアントをインストールする。
- 自宅のデバイスからアプライアンスにブラウジングし（安全な HTTPS を使用）、必要に応じてシンクライアントをダウンロードする。これは「SSL Network Extender」として知られています。

アプライアンスに DDNS または静的 IP インターネット接続を設定した後は、リモート・アクセスで作業することを強くお勧めします。静的 IP を使わない場合、お使いのインターネット・サービス・プロバイダによってアプライアンスの IP アドレスが異なります。DDNS では、変わる可能性のある IP アドレスではなく、名前によってリモート・ユーザを組織に接続させます。詳細については、[デバイス]→[DDNS]を参照してください。

DDNS を設定するには、DDNS リンク、または静的 IP のインターネットリンクをクリックしてください。

VPN リモート・アクセスを有効/無効にするには

1. [オン]または[オフ]を選択します。
2. [適用]をクリックします。

注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになりま。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。

組織に対するデフォルトのアクセス・ポリシーをリモート・アクセスで設定するには

1. [リモート・アクセス・ユーザからのトラフィックを許可（デフォルト）]チェックボックスをオンまたはオフにします。オフにした場合、リモート・アクセス・ユーザが組織のリソースにアクセスするには、[アクセス・ポリシー]→[サーバ]ページで各リソースに定義するか、[アクセス・ポリシー]→[ファイアウォール・ポリシー]ページで手動でアクセス・ルールを定義する必要があります。
2. [リモート・アクセス・ユーザからのトラフィックをログ記録（デフォルト）]チェックボックスをオンまたはオフにします。
3. [適用]をクリックします。

VPN リモート・アクセス・メソッドを設定するには

デフォルトでは、[Check Point VPN クライアント]は有効になっています。

1. Check Point Mobile VPN クライアントで接続する場合は（スマートフォンまたはタブレット）、[モバイル・クライアント]チェックボックスをオンにします。
2. SSL VPN で接続する場合は、チェックボックスをオンにします。
アプライアンスの設定

3. **Windows VPN クライアント**で接続する場合は、チェックボックスをオンにします。L2TP 事前共有キーのリンクをクリックして、事前共有キーを入力し、[OK]をクリックします。

**SSL VPN ブックマークを管理するには**

1. [SSL VPN]チェック・ボックスをオンにします。
2. [適用]をクリックします。
3. [SSL VPN ブックマークの管理]をクリックします。
   [VPN]→[詳細設定]ページが開きます。
4. [SSL VPN ブックマーク]で、[新規]をクリックして新しくブックマークを作成します。
   新しいウィンドウが開きます。
5. 次の詳細を入力します。
   - **URL**
     注 - [グローバル・ブックマーク]を選択すると、すべてのユーザに表示されます。
   - **タイプ** - リンクまたは RDP（リモート・デスクトップ・プロトコル）
   - **ラベル** - ブックマークの名前
   - **ツールチップ** - 説明
6. [適用]をクリックします。
   ブックマークのタイプで「RDP」を選択する場合、[RDP 詳細設定]でユーザ名とパスワードを指定する必要があります。この情報はエンドユーザに送られます。
   注 - [文字の表示]をオンにすると、パスワードの文字が表示されます。
   リモート・デスクトップのスクリーン・サイズを指定することもできます。デフォルトのモードは「フル・スクリーン」です。

**ブックマークを管理するには**

1. ブックマークをクリックします。
2. [編集]または [削除]をクリックします。
3. [適用]をクリックします。

**ユーザにリモート・アクセスの使用方法について送信するには**

1. 該当のリモート・アクセス・メソッドの横にある [接続方法]リンクをクリックします。
2. [詳細方法をメールで送信]をクリックします。方法を説明した内容が記載されたメールが自動的に開きます。
3. [閉じる]をクリックします。

**リモート・アクセスのポート設定を変更するには**

デフォルトのリモート・アクセス・ポート（ポート 443 番）と、同じポートを使用するサーバ間で競合が生じる場合、メッセージが表示されます。Check Point VPN クライアント、Mobile クライアント、SSL VPN リモート・アクセス・メソッドのいずれかが有効で、ポート 443 番をデフォルトで使用している場合、デフォルトのリモート・アクセス・ポートを変更する必要があります。

1. Change port リンクをクリックします。
   [リモート・アクセス・ポートの設定]ウィンドウが開きます。
2. [リモート・アクセス・ポート]に、新しいポート番号を入力します。
3. [ポート 443 番をポート転送に予約]がオンになっていることを確認します。
4. [適用]ボタンをクリックします。

リモート・アクセス・ユーザの設定

[VPN]→[リモート・アクセス・ユーザ]ページでは、ユーザやグループにリモート・アクセスの権限を設定できます。

ユーザやユーザ・グループは、別のページでも設定できます（[ユーザ&オブジェクト]→[ユーザ]）。ここでは、リモート・アクセス権限を持つユーザ/グループに焦点をあてています。リモート・アクセス権限は、次を対象に追加できます。

- 新しいローカル・ユーザ
- 新しいユーザ・グループ
- Active Directory グループ
- Active Directory 権限
- RADIUS グループ

SSL VPN ブックマークは、ユーザ、ユーザ・グループ、Active Directory グループで設定することもできます。

認証サーバが定義されていない場合は、Active Directory / RADIUS リンクをクリックして定義してください。

User Awareness がオフの場合、ブラウザベース認証とActive Directory クエリに基づくユーザ識別は行われません。

リモート・アクセス権限を持つ新しいローカル・ユーザを追加するには

1. [追加]→[新しいローカル・ユーザ]をクリックします。
2. [リモート・アクセス]タブで、必要な詳細情報を入力します。
3. テンポラリ・ユーザやゲストの場合は[テンポラリ・ユーザ]をクリックします。
   有効期限と時間を入力します。
4. [リモート・アクセス権限]チェックボックスはオンのままにしておきます。
5. [SSL VPN ブックマーク]タブで、SSL VPN ブックマークを設定します（下記参照）。
6. [適用]をクリックします。
作成したユーザがページの表に追加されます。

リモート・アクセス権限を持つ新しいローカル・ユーザ・グループを追加するには
1. [追加] → [新しいユーザ・グループ]をクリックします。
2. [リモート・アクセス]タブで、グループ名を入力します。
3. [リモート・アクセス権限]チェックボックスはオフのままでしておきます。
4. ユーザのリストから該当のチェックボックスを選択し、グループに追加する初期ユーザを選択します。または、[新規]をクリックして新しいユーザを作成します。
   ユーザ・リストの上に表示される、グループ・メンバの概要を確認することができます。メンバを削除するには、そのユーザ名の隣にある[X]をクリックします。
5. [SSL VPN ブックマーク]タブで、SSL VPN ブックマークを設定します（下記参照）。
6. [適用]をクリックします。
   作成したグループがページの表に追加されます。

既存の Active Directory グループにリモート・アクセス権限を追加するには
1. [追加] → [Active Directory グループ]をクリックします。
2. Active Directory が定義されていない場合は、設定するようメッセージが表示されます。Active Directory の設定方法については、[VPN] → [認証サーバ]を参照してください。
3. Active Directory を定義し終われば、サーバに定義されているユーザ・グループのリストが表示されます。
4. ユーザ・グループを選択します。
5. [適用]をクリックします。
   Active Directory グループがテーブルに追加されます。

リモート・アクセス権限を Active Directory で定義されたすべてのユーザに追加するには
1. [権限の編集]をクリックするか、[追加] → [Active Directory 権限]をクリックします。
2. Active Directory のすべてのユーザを選択します。このオプションを使えば、[VPN] → [リモート・アクセス・ユーザ]ページで特定のユーザをずわざわ選択する必要がありません。
   Active Directory には、たいてい多数のユーザが含まれています。組織へのリモート・アクセス権限をすべてのユーザに付与することは、お勧めできません。通常は、指定した Active Directory ユーザ・グループのみにします。
3. [適用]をクリックします。
   Active Directory がテーブルに追加されます。

RADIUS グループに定義されたユーザにリモート・アクセス権限を追加するには
1. [追加] → [RADIUS グループ]をクリックします。
2. RADIUS グループが定義されていない場合は、設定するようメッセージが表示されます。
3. [RADIUS 認証をリモート・アクセス・ユーザに有効にする]チェックボックスをオンまたはオフにします。
4. オフにした場合は、リモート・アクセス権限を付与するユーザを選択します。
   - RADIUS サーバに定義されているすべてのユーザの認証を許可するには、[RADIUS サーバで定義されたすべてのユーザ]を選択します。
   - RADIUS サーバに定義されている特定のユーザ・グループの認証を許可するには、[特定 RADIUS グループのみ]を選択し、ユーザ・グループの名前をカンマ区切りでテキスト・フィールドに入力します。
   - 管理者に認証目的で読み取り専用権限を付与するには - 読み取り専用管理者を選択
5. [適用]をクリックします。
   RADIUS サーバまたは RADIUS サーバの特定ユーザがテーブルに追加されます。
SSL VPN ブックマークを設定するには
1. [追加]→[新しいローカル・ユーザ/ユーザ・グループ/Active Directory グループ]→[SSL VPN ブックマーク]タブをクリックします。
   新しいウィンドウが開きます。
2. 新しいブックマークを入力するか、既存を選択します。
   注 - [グローバル・ブックマーク]を選択すると、常に表示されるようになります。
3. [適用]をクリックします。

ユーザ/グループを編集するには
1. リストからユーザまたはグループを選択します。
2. [編集]をクリックします。
3. 必要な変更を行ってから[適用]をクリックします。

ユーザまたはグループを削除するには
1. リストからユーザまたはグループを選択します。
2. [削除]をクリックします。
3. 確認メッセージで[OK]をクリックします。
   ユーザ/グループが削除されます。

リモート・アクセス認証サーバの設定
[認証サーバ]ページでは、複数の認証サーバを定義、参照できます。外部ユーザ・データベースと、そのデータベースに定義されているユーザの認証方法を定義できます。

定義できる認証サーバの種類は以下のとおりです。
- RADIUS サーバ - プライマリとセカンダリの RADIUS サーバの詳細を定義できます。Check Point 730/750 Appliance は RADIUS サーバに接続し、これらのサーバで定義、認証されているユーザを認識できます。
- Active Directory ドメイン - 組織に属するユーザの情報が登録された Active Directory ドメインの詳細を定義できます。ユーザ認証機能では、これらの詳細情報を使用してシームレスにユーザを認識し、その識別情報をログ記録やユーザ・ベースのポリシー設定に活用することができます。この機能は、VPN リモート・アクセスのユーザ認証にも使用できます。この場合は、[VPN]→[リモート・アクセス・ユーザ]ページで追加設定を行う必要があります。

RADIUS サーバを追加するには
1. [設定]をクリックします。
2. [プライマリ]タブで以下の情報を入力します。
   - [IP アドレス] - RADIUS サーバの IP アドレス。
   - [ポート] - RADIUS サーバとクライアントとの通信に使用するポート番号。デフォルトは 1812 です。
   - [共有秘密キー] - RADIUS サーバとCheck Point 730/750 Appliance の間で使用される秘密情報（メッセージの暗号化に使用される事前共有情報）。パスワードや共有キーを入力する際は、{ } [ ] ` ~ | ' " # + の文字は使用できません。
   - [表示] - 共有秘密情報を表示します。
   - [タイムアウト] - RADIUS サーバとの通信に適用するタイムアウト値（秒単位）。デフォルトのタイムアウトは 3 秒です。
3. セカンダリ RADIUS サーバを使用する場合は、[セカンダリ]タブで手順 2 を繰り返します。
注 - IP アドレスや共有キーに入力した情報を削除する場合は、[クリア]をクリックします。

4. [適用]をクリックします。
プライマリとセカンダリ（定義した場合）のサーバがページの [RADIUS] セクションに追加されます。

RADIUS サーバは以下の用途に使用できます。
- リモート・アクセス権限のあるユーザのデータベースを定義する。このようなユーザの定義と認証は RADIUS サーバで行います。
- 管理者を定義する。詳細については、[ユーザ&オブジェクト] → [管理者] ページを参照してください。

RADIUS サーバを編集するには
1. 編集する RADIUS サーバの IP アドレス・リンクをクリックします。
2. 必要な変更を行います。
3. [適用]をクリックします。
変更内容が RADIUS サーバに適用されます。

RADIUS サーバを削除するには
削除する RADIUS サーバの横にある削除のリンクをクリックします。
RADIUS サーバが削除されます。

RADIUS サーバに定義されているユーザのリモート・アクセス権限を設定するには
1. [RADIUS ユーザの権限]をクリックします。
2. [RADIUS 認証をリモート・アクセス・ユーザに有効にする] チェック・ボックスをオンまたはオフにします。
3. オンにした場合は、リモート・アクセス権限を付与するユーザを選択します。
   - RADIUS サーバに定義されているすべてのユーザの認証を許可するには、[RADIUS サーバで定義されたすべてのユーザ] を選択します。
   - RADIUS サーバに定義されている特定のユーザ・グループの認証を許可するには、[特定 RADIUS グループのみ] を選択し、ユーザ・グループの名前をカンマ区切りでテキスト・フィールドに入力します。
   - 管理者に認証目的で読み取り専用権限を付与するには - [読み取り専用管理者] を選択します。
4. [適用]をクリックします。

Active Directory ドメインを追加するには
   [新しいドメインの追加] ウィンドウが開きます。
2. 以下の情報を入力します。
   - [ドメイン] - ドメイン名。
   - [IP アドレス] - ドメインのいずれかのドメイン・コントローラの IP アドレス。
   - [ユーザ名] - 設定を効率化し、Active Directory に定義されているユーザを使用してユーザ・ベースのポリシーを作成するには、管理者権限のあるユーザを指定する必要があります。
   - [パスワード] - ユーザのパスワード。パスワードや共有キーを入力する際は、{ } [] ` ~ | ' " # + の文字は使用できません。
   - [ユーザ DN] - [検索] をクリックして該当のユーザを表すオブジェクトの DN を自動検出するか、そのユーザの DN を入力します。例えば、次のように入力します。CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com
3. Active Directory に定義されたユーザ・データベースの一部のみを使用する場合は、[特定のブランチからのユーザグループのみ使用]を選択します。[ブランチ]のテキスト・フィールドにそのブランチ名（フル DN）を入力します。

4. [適用]をクリックします。

定義した Active Directory が表に表示されます。この Active Directory を選択して、編集や削除を行うことができます。

編集を行う場合、ドメイン情報は読み取り専用となり変更することはできません。

新しい Active Directory を追加する際、既存のドメインを使用して別のオブジェクトを作成することはできません。

Active Directory に定義されているすべてのユーザにリモート・アクセス権限を設定するには

Active Directory に定義されているユーザには、デフォルトではリモート・アクセス権限は付与されません。

[VPN] → [リモート・アクセス・ユーザ] ページから、ローカルまたは Active Directory で定義されているユーザを個別に選択してリモート・アクセス権限を付与できます。

1. [Active Directory ユーザの権限] をクリックします。
2. [Active Directory のすべてのユーザ] を選択します。このオプションを使用する場合、[VPN] → [リモート・アクセス・ユーザ] ページに移動して特定のユーザを選択する必要はありません。

Active Directory には、たいてい多数のユーザが含まれています。組織へのリモート・アクセス権限をすべてのユーザに付与することは、お勧めできません。[選択した Active Directory ユーザ・グループ]オプションを選択し、[VPN] → [リモート・アクセス・ユーザ] ページでリモート・アクセス権限を設定します。

3. [適用]ボタンをクリックします。

定義した Active Directory との同期化モードを変更するには


3. [適用]をクリックします。

Active Directory を編集するには

1. リストから Active Directory を選択します。
2. [編集]をクリックします。
3. 必要な変更を行ってから[適用]をクリックします。

Active Directory を削除するには

1. リストから Active Directory を選択します。
2. [削除]をクリックします。
3. 確認メッセージで[OK]をクリックします。

選択した Active Directory が削除されます。

注 - このページには、[VPN]タブと[ユーザ&オブジェクト]タブからアクセスできます。
詳細リモート・アクセス・オプションの設定

[VPN]→[リモート・アクセス詳細]ページでは、VPN リモート・アクセス・ユーザに関してさらに詳細な設定を決定できます。

このページでは、SSL VPN 経由で接続する際の特定の URL やコンピュータを対象にした、ブックマーク（HTMLやRDPリンク）を追加できます。次回ログインすると、ブックマークが表示されます。

オフィス・モードとは

リモート・アクセス VPN クライアントを利用することで、ユーザの自宅から VPN トンネルを経由してアプライアンスに接続し、そこから組織のリソースにアクセスできるようになります。

アプライアンスで、各リモート・アクセス・ユーザに特定のネットワークからの IP アドレスを割り当て、リモート・アクセス・ユーザのトラフィックが組織内部に入ると、組織外部からのトラフィックだと認識されないようにします。

この技術を「オフィス・モード」といいます。IP アドレスのネットワークは設定することができます。

オフィス・モード・ネットワークを設定するには

1. [オフィス・ネットワーク・アドレス]と[オフィス・サブネット・マスク]を入力します。
2. [適用]をクリックします。デフォルトのオフィス・モードは「172.16.10.0/24」に設定されています。

VPN リモート・アクセス・クライアントのすべてのトラフィックをゲートウェイ経由でルーティングするには

1. [接続先クライアントからのインターネットトラフィックをこのゲートウェイにルーティング]チェックボックスをオンにします。
2. [適用]をクリックします。通常は、VPN クライアントから組織の暗号化ドメインへのトラフィックだけが暗号化され、VPN トンネルを経由してゲートウェイに送られます。上記のチェックボックスをオンにすると、VPN クライアントからのトラフィックがすべて暗号化され、ゲートウェイに送られるようになります。組織外部の場所へ送られるトラフィックには、外部へのアクセス・ポリシーが適用されます。詳細については、[アクセス・ポリシー]の[ファイアウォール・ブレード・コントロール]ページを参照してください。

注 - この設定は、SSL Network Extender クライアントからのトラフィックには適用されません。

リモート・アクセス・ユーザのみにローカル暗号化ドメインを手動で設定するには

ローカル暗号化ドメインは、リモート・アクセス VPN ユーザからの暗号化トラフィックがアクセスできる内部ネットワークです。デフォルトでは、ローカル暗号化ドメインはアプライアンスで自動的に決定されます。LAN インタフェースの背後、そしてトラスト・ワイヤレスのネットワークは、ローカル暗号化ドメインの一部です。

それ以外に、リモート・アクセス・ユーザだけが使用するローカル暗号化ドメインを、手動で作成することもできます。また、別のローカル暗号化ドメインを VPN リモート・アクセスと VPN サイト間に手動で設定することも可能です。[VPN]→[サイトツーサイト・ブレード・コントロール]のページを参照してください。

1. ローカル暗号化ドメインのリンクをクリックします。トポロジに従って自動または手動のどちらかを選択します。表示されるリンクには、現在設定されているものが反映されます。
2. [ローカル・ネットワーク・トポロジーを手動で定義]を選択します。
3. [選択]をクリックして、選択できるネットワークの一覧を表示します。該当するチェックボックスを選択します。
4. 必要なネットワークが既存のリストにない場合は、[新規]をクリックします。新しいネットワーク・オブジェクトを作成する方法については、[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]ページを参照してください。
5. [適用]をクリックします。
リモート・アクセス・ユーザの DNS サービス

リモート・アクセス・クライアントの DNS サーバとして、3 つまで定義できます。デフォルトでは、[オフィスモードの 1 番目のクライアント用 DNS]がこのゲートウェイに設定されます。

別の DNS プライマリ・サーバを使用するには

1. [手動で設定]をクリックします。
2. [オフィスモードの 1 番目のクライアント用 DNS]に、DNS サーバとして使用するサーバの IP アドレスを入力します。
3. [適用]をクリックします。

DNS ドメイン名

リモート・アクセス・クライアントのデバイスで、非 FQDN ドメインを解決するために自動的に使われる DNS ドメイン名を設定できます。デフォルトでは、サフィックスは[DNS]ページで設定された DNS ドメイン名が自動的に使われます。

DNS ドメイン名を手動で設定するには

1. [手動で設定]をクリックします。
2. [DNS ドメイン名]に、使用する DNS ドメイン名サフィックスを入力します。
3. [適用]をクリックします。

DNS ドメイン名を定義した DNS ドメイン名同じ名前に設定するには

1. [手動で設定]をクリックします。
2. [適用]をクリックします。
   DNS ドメイン名に「Same as DNS domain name（DNS ドメイン名と同じ）」と表示されます。

SSL VPN ブックマークを設定するには

1. [SSL VPN ブックマーク]で、[新規]をクリックして新しくブックマークを作成します。
   新しいウィンドウが開きます。
2. 次の詳細を入力します。
   • URL
     注 - [グローバル・ブックマーク]を選択すると、すべてのユーザに表示されます。
   • タイプ - リンクまたは RDP（リモート・デスクトップ・プロトコル）
   • ラベル - ブックマークの名前
   • ツールチップ - 説明
3. [適用]をクリックします。

ブックマークのタイプで「RDP」を選択する場合、[RDP 詳細設定]でユーザ名とパスワードを指定する必要があります。この情報はエンドユーザに送られます。

注 - [文字の表示]をオンにすると、パスワードの文字が表示されます。

リモート・デスクトップのスクリーン・サイズを指定することもできます。デフォルトのモードは「フル・スクリーン」です。

ブックマークを管理するには

1. ブックマークをクリックします。
2. [編集]または[削除]をクリックします。
[適用]をクリックします。

サイト間 VPN ブレードの設定

[VPN]→[サイト間 VPN ブレード・コントロール]ページでは、リモート・サイトの VPN トンネルを作成することができます。サイト間 VPN は、インターネットで離れた 2 つのネットワークを、安全な暗号化した VPN トンネルを使って接続します。これにより、物理的に離れていても、シームレスかつ安全な通信が同じ組織内の 2 つのネットワーク間でできるようになります。

このページでは、ブレードの機能を有効にしてサイト間の接続を許可します。すでに定義されているサイトの数を確認し、また、リモート・サイトからこのゲートウェイでアクセス可能、特定のネットワークへの基本的なアクセス・ポリシーを設定できます。

リモート・サイトには、別の Check Point Appliance（推奨）を利用する、またはサード・パーティ製 VPN を利用してアクセスすることができます。

定義した後は、リモート・サイトへのアクセスは着信/内部 VPN トンネル→[ファーイウォール・ポリシー]ページで決定します。これにより、実際にはインターネットへの発信トラフィックでも、VPN ポリシーであるため、リモート・サイトの暗号化ドメインが組織の一部であるとみなされるためです。

サイト間 VPN ブレードを有効/無効にするには
1. [オン]または[オフ]を選択します。
2. [適用]をクリックします。

注 - ブレードがクラウド・サービスで管理されていると、アイコンがロックされて表示されます。オン/オフの切り替えはできません。ポリシー設定を変更した場合、その変更は一時的なものになります。ローカルで行ったこれらの変更は、次回ゲートウェイとクラウド・サービスで同期する際に上書きされます。

ブレードがアクティブな状態で VPN サイトが未定義の場合は、警告アイコンが表示されます。[VPN サイト]をクリックして、VPN サイトを追加する、または定義されている VPN サイトの数を確認します。サイトの完全なリストは、[VPN]→[サイト間 VPN サイト]にあります。

リモート VPN サイトからのデフォルトのアクセス・ポリシーを設定するには
1. [リモート・サイトからのトラフィックを許可（デフォルト）]チェックボックスをオン/オフにします。通常、リモート・サイトは組織の一部であるため、このチェックボックスをオフにすることはお勧めしません。
2. [遠隔地からのトラフィックをログ記録（デフォルト）]チェックボックスをオンまたはオフにします。
3. [適用]をクリックします。
ローカル暗号化ドメイン

ローカル暗号化ドメインは、リモート・サイトとネットワークからの暗号化トラフィックがアクセスできる内部ネットワークを定義します。このドメインからリモート・サイトへのトラフィックは暗号化されます。デフォルトでは、ローカル暗号化ドメインはアプライアンスで自動的に決定されます。LAN インタフェースの背後、そしてトラスト・ワイヤレスのネットワークは、ローカル暗号化ドメインの一部です。オプションで、ローカル暗号化ドメインを手動で作成することができます。[VPN]→[サイト間 VPN]→[詳細]ページを参照してください。

VPN サイトの設定

[VPN]→[サイト間 VPN]→[VPN サイト]ページでは、リモート VPN サイトを設定できます。サイト間 VPN の一般的な設定情報は、[VPN]→[サイト間 VPN ブレード・コントロール]のページを参照してください。

設定した新しいサイトを追加する場合：

- リモート・サイトの詳細 - 名前、接続タイプ、認証方式（事前共有キーまたは証明書）、リモート・サイト暗号化ドメイン
- 暗号化設定
  暗号化メソッドと証明書のマッチングに関する詳細設定も行うことができます。

新しい VPN サイトを追加するには

1. [新規]をクリックします。
[新規 VPN サイト]ウィンドウが開きます。
2. [リモート・サイト]タブの各フィールドに入力します。
   - サイト名
   - 接続タイプ - 該当するタイプを選択します。
     - [ホスト名または IP アドレス] - 該当する IP アドレスまたはホスト名オプションを選択し、情報を入力します。IP アドレスを選択し、リモート・サイトが変換される静的 NAT IP アドレスを設定する必要がある場合は、[静的 NAT で隠す]を選択して IP アドレスを入力します。
     - [ハイ・アベイラビリティ/負荷共有] - IP アドレスのリストを作成して、ファイアル時（ハイ・アベイラビリティ）やデータ分散（負荷分散）の場合に、バックアップするための冗長性を設定します。アプライアンスでは、リモート・サイトの IP アドレスをモニタリングするためにプロービングを行います。HA（ハイ・アベイラビリティ）の場合、いずれかの IP アドレスをプライマリ IP アドレスとして設定できます。このオプションを選択する場合は[詳細]タブでプロービングのメソッドを設定する必要があります。プロービング・メソッドにより、複数の IP アドレスの中で VPN に使用されるアドレスをモニタリングします。[新規]をクリックして IP アドレスを追加し、プライマリ IP アドレスを設定します（HA に必要な場合）。
     - [リモート・サイトだけが VPN を開始] - リモート・サイトからこのアプライアンスに対してのみ接続を実行できます。たとえば、リモート・サイトが NAT デバイスで隠されている場合を考えられます。この場合、ア
ブライアンスはトンネル開始のリクエストのみに応答します。これには、リモート・サイトの認証および識別の安全なメソッドが必要です。

いずれかの認証方式を選択します。このブライアンスが他のゲートウェイのリモート・サイトで設定されているときの認証設定と同様設定してください。

- プライシェアード・シークレット - このオプションを選択した場合は、リモートのゲートウェイで設定したパスワードを[パスワード]に入力し、[確認]に確認のため再入力します。パスワードや共有キーを入力する際は、『 ` ~ | ^ # ` + の文字は使用できません。

- 証明書 - ゲートウェイが持つ証明書を使って認証を行います。詳細については、[VPN]→[内部証明書]を参照してください。

リモート・サイト暗号化ドメインを選択します。ここで、一致したトラフィックの暗号化やリモート・サイトへ送られるタイミングを設定します。

- [リモート・ネットワーク・トポロジを手動で定義] - 宛先が下のリストに含まれている場合は、トラフィックは暗号化されます。選択をクリックして、リモート・サイトの内部ネットワークとなるネットワークを、下のリストで選択します。該当するネットワーク・オブジェクトをまだ作成していない場合は、[新規]をクリックします。

- [すべてのトラフィックをこのサイト経由でルーティング] - すべてのトラフィックは暗号化されてこのリモート・サイトに送られます。このオプションで設定できるリモート・サイトは1つだけです。

- [ルーティング・テーブルに従って暗号化] - ダイナミック・ルーティングを使用する場合、発信元のサーバと宛先に基づいてトラフィックが暗号化されます。VTI(バーチャル・トンネル・インタフェース)を作成して(【デバイス】→【ローカル・ネットワーク】ページ)、このリモート・サイトに関連付ける必要があります。その後、VTIを利用しルーティング・ルールを作成できます。これらのルーティング・ルールに一致するトラフィックは暗号化され、リモート・サイトにルーティングされます。

- [リモート・ゲートウェイの外部IPで隠す] - リモート・サイトがNATで隠れている場合、トラフィックは暗号化されます。インターネットに向かう場合、このオプションを選択します。このオプションを選択する場合は、暗号化ドメインを定義する必要はありません。

3. デフォルト設定は[暗号化]タブで変更できます(オプション)。使用できるビルドインの暗号化設定グループがあります。この設定とリモート・サイトの両方でのみ一致する必要があります。

- Default（最も互換性あり）
- VPN A - RFC4308に準ずる。
- VPN B - RFC4308に準ずる。
- Suite-B GCM-128/256 - RFC6379に準ずる。
- Custom - このオプションを選択して、使用する暗号化メソッドを手動で決定できます(オプション)。

4. デフォルト設定は[詳細]タブのセクションで変更できます(オプション)。

設定

- リモート・サイトがCheck Pointゲートウェイかどうかを設定します。また、この設定で永続的トンネルの設定も有効になります。

- このサイトのNATを無効にすることができます。これは、内部ネットワークにサーバがある場合に便利です。

- IKEネゴシエーションには2種類のモードがあります。メイン・モードとアグレッシブ・モードです。IKEネゴシエーションでは、メイン・モードの場合は6パケット、アグレッシブ・モードでは3パケットを使用します。安全性が高い理由から、メイン・モードの使用をお勧めします。デフォルトでは、[アグレッシブ・モードを有効にする]はオフになっていて、メイン・モードが使われます。アグレッシブ・モードは、VPNトンネルの一方でメイン・モードがサポートされていないなど、必要な場合のみに有効にしてください。
アプライアンスの設定

- [Diffie-Hellman グループを使用] - IKE フェーズ 1 で IKE フェーズ 2 のキーに交換するため
  に使われる共有 DH キーの強度を決定します。ビット数が大きいグループはより強いキーとなります
  が、パフォーマンスは低下します。
- [このゲートウェイの識別子で VPN トンネルを開始] - このゲートウェイの IP アドレスが動的で、認証メ
  ソッドが事前共有キーである場合、ゲートウェイ自身で認識する必要があります。マッチングに使う
  [ゲートウェイ ID] を入力して、[タイプ] でドメイン名またはユーザ名を選択します。
- [ピア識別子ごとの VPN アクセスを有効にする] - 接続タイプを使用し、認証メソッドが事前共有キー
  の場合はピア識別子を設定することが重要です。[ピア ID] に識別子を入力し、[タイプ] でドメイン名
  またはユーザ名を選択します。

暗号化メソッド
アプライアンスでサポートする IKE のバージョンを選択します。

証明書マッチング
- 事前共有キーを使用する場合は、このセクションは関係ありません。[リモート・サイト]タブで認証
  に証明書を選んだ場合、まず CA を追加する必要があります。この CA は、[VPN] → [証明書トラ
  スト CA] ページで、リモート・サイトの証明書を署名している必要があります。[詳細]タブで、既知
  のトラスト CA または特定の CA に証明書をマッチングさせるよう、選択できます。また、証明書に
  関する追加のマッチング基準を設定することもできます。

プローブング・メソッド
このセクションは、接続タイプに HA または負荷共有が指定されている場合に表示されます。リモート・サイトで
VPN トрафックに対し複数の IP アドレスがある場合、VPN の正しいアドレスは以下のいずれかのプローブン
・メソッドで決定されます。
- 継続的なプローブ - セッションを開始すると、使用可能なすべての送信 IP アドレスが継続して
  RDP パケットを受信し、いずれかが応答するまで続きます。接続は、最初に応答した IP（またはプ
  ライマリ IP が設定されて HA でアクティブになっている場合はプライマリ IP）を使用し、応答を停止
  するまでこの IP を使用し続けます。接続が開かれて、バックグラウンド・プロセスとして続行されて
  いる間は、RDP プローブがアクティブになります。
- ワンタイム・プローブ - セッションを開始すると、すべての送信先 IP アドレスは、ルートをテストするために
  RDP セッションを受信します。応答した最初の IP が選択され、VPN 設定が変わるまでこれが使用されま
  す。

5. [適用]をクリックします。
初期のトンネル・テストがリモート・サイトで開始します。設定をしていない場合は、[スキップ]をクリックし
ます。VPN サイトがテーブルに追加されます。

リモート・サイトでトンネル・テストを実行するには
チェック・ポイントでは、VPN トンネルがアクティブかどうかをテストする、独自のプロトコルを使用します。
このプロトコルは、サイト間 VPN 設定をサポートしています。トンネル・テストを行うためには、2 つのセ
キュリティ・ゲートウェイと UDP ポート番号 18234 が必要です。Check Point のトンネル・テスティング・プ
ロトコルでは、サード・パーティ製のセキュリティ・ゲートウェイはサポートしていません。
1. リストから既存のサイトを選択します。
2. [テスト]をクリックします。

VPN サイトを編集するには
1. リストから VPN サイトを選択します。
2. [編集]をクリックします。
3. 必要な変更を行ってから[適用]をクリックします。
VPN サイトを削除するには
1. リストから VPN サイトを選択します。
2. [削除] をクリックします。
3. 確認メッセージで [OK] をクリックします。
   VPN サイトが削除されます。

VPN サイトを有効または無効にするには
1. リストから VPN サイトを選択します。
2. [有効/無効] をクリックします
   VPN サイトが設定に基づいて無効/有効になります。

VPN トンネルの表示
[VPN トンネル] ページでは、このゲートウェイとリモート・サイト間で利用可能な現在の VPN トンネルを確認できます。サイトによって、必要なものだけトンネルを確立するサイト、永続的なトンネルが設定されたサイトがあります。クラウド・サービスで管理する場合、この表にはコミュニティのゲートウェイのトンネルも表示されます。

このページは、主に永続的トンネルを確認するために使われます。アクティブな VPN トンネルがあると、テーブルに各トンネルの詳細が表示されます。

<table>
<thead>
<tr>
<th>フィールド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>送信元</td>
<td>トンネルの発信元ゲートウェイのホスト名または IP アドレス。</td>
</tr>
<tr>
<td>サイト名</td>
<td>VPN サイト名の名前。</td>
</tr>
<tr>
<td>ピア・アドレス</td>
<td>トンネルの宛先ゲートウェイのホスト名または IP アドレス。</td>
</tr>
<tr>
<td>コミュニティ名</td>
<td>ゲートウェイがクラウド・サービスで設定されているコミュニティの一部である場合、このカラムにはコミュニティ名と関連するトンネルが表示されます。</td>
</tr>
<tr>
<td>ステータス</td>
<td>VPN トンネルのステータス情報。</td>
</tr>
</tbody>
</table>

リストを絞り込むには
[入力して絞り込み] ボックスに絞り込みの条件を入力します。
入力内容に従ってリストが絞り込まれます。

リストを更新するには
[更新] をクリックすると、手動でこのページを更新して最新のトンネル情報を確認できます。

注 - このページには、[VPN] および[ログ＆モニタリング] タブからアクセスできます。

サイト間の詳細設定
[VVPN] → [サイト間 VPN 詳細設定] ページでは、アプライアンスからリモート・サイトに接続する方法を定義するグローバルな詳細オプションを設定できます。
このページでは、たとえば以下のような設定を具体的に指定できます。

- リモート・サイトの接続を実行する - 「ローカル暗号化ドメインの設定」を参照。リモート・サイトの暗号化ドメインはサイトごとに設定します。[VPN]→[サイト間 VPN]→[VPN サイト]ページを参照してください。
- アプライアンスからリモート・サイトに接続する方法 - VPN に使用するアプライアンスの外部へのインタフェースの設定は、後述を参照してください。

ローカル暗号化ドメインの設定
ドメインベースの VPN では、1 つの暗号化ドメインのトラフィックは暗号化され、別のドメインに送信されます。
ローカル暗号化ドメインでは、以下が定義されます。
- リモート・サイトとネットワークからの暗号化トラフィックがアクセスできる内部ネットワーク。
- 暗号化ドメインからリモート・サイトへのトラフィックは暗号化される。
デフォルトでは、ローカル暗号化ドメインはアプライアンスで自動的に決定されます。LAN ネットワークの背後、そしてトラスト・ワイヤレスのネットワークは、ローカル暗号化ドメインの一部です。オプションで、ローカル暗号化ドメインを手動で作成することができます。

ローカル暗号化ドメインを手動で設定するには
1. 「トポロジに基づいて自動的に」リンクをクリックします。
2. [ローカル・ネットワーク・トポロジを手動で設定]を選択します。
3. [選択]をクリックして、選択できるネットワークの一覧を表示します。該当するチェックボックスを選択します。
4. 必要なネットワークが既存のリストにない場合は、[新規]をクリックします。新しいネットワーク・オブジェクトを作成する方法については、[ユーザーオブジェクト]→[ネットワーク・オブジェクト]ページを参照してください。
5. [適用]をクリックします。
【サイト間のローカル暗号化ドメイン】ウィンドウが開き、選択したサービスが表示されます。

アプライアンスのインタフェースの設定
リンク選択は以下に使用します。
- 送受信の VPN ドライフックで使用するインタフェースを指定する。
- トラフィックに最適なパスを決定する。
リンク選択メカニズムを使用すると、管理者は、VPN ドライフックにどの発信元 IP アドレスを使用するかを選択できます。
デフォルトでは、送信インタフェースと発信元 IP アドレスの設定はデバイスで自動的に決定されます。必要であれば、デフォルト設定を変更して以下の決定を別な方法で行うこともできます。
- アプライアンスの送信インタフェース
- アプライアンスの発信元 IP アドレス

アプライアンスの VPN の送信インタフェースと発信元 IP アドレスを設定するには
1. [リンク選択]→[外部へのインタフェース選択]で、外部へのインタフェースの方法を選択します。
   - [ルーティング・テーブルに基づく] – OS のルーティング・テーブルで、リモート・サイトの IP アドレスに基づいてトライフィックが送信される、一番低いメトリック（最優先）のインタフェース・リンクを見つけます。
アプライアンスの設定

・ [ルート・ベースのプローブ] - このメソッドも、ルーティング・テーブルを調べて、メトリックが一番低いリンクを判定します。ただし、トラフィックを送信するインタフェース・リンクを選択する前に、すべての可能なルーティンゲが検査されます。これは、リンクがアクティブかどうかを確認するためです。この後、ゲートウェイによって、使用可能なルートの中でメトリックが最も低く（最優先）、最適な（プレフィックスが最も長い）ルートが選択されます。複数の外部インタフェースがある場合に、この方式をお勧めします。

2. [ソース IP アドレス選択] セクションで以下のいずれかのオプションを選択し、VPNトラフィックを開始またはVPNトラフィックに応答する際セキュリティ・ゲートウェイで使用する発信元IPアドレスを設定します。このIPアドレスはリモート・サイトからセキュリティ・ゲートウェイに接続する際に通常使用します。

・ 外部へのインタフェースに従って自動選択
・ 手動で設定 - VPNトンネルの発信元IPアドレスとして常に使われるIPアドレスを入力します。

信頼済み CA の管理

[VPN]→[トラスト CA] ページでは、リモート・サイトで使用するCAを追加して、サイト間VPNをベースにした証明書を有効にできます。リモート・サイトの証明書は、アプライアンスで信頼されている認証局(CA)で署名する必要があります。

ここには、デフォルトでアプライアンスの証明書を作成するビルトインの内部 CA も表示されます。リモート・サイトの証明書の署名に使うこともできます。内部 CA をエクスポートして、リモート・サイトのトラスト CA リストに追加することも可能です。

クラウド・サービスがオンになっていてアプライアンスがクラウド・サービスで設定されている場合、クラウド・サービス・プロバイダの CA がアプライアンスに自動的にダウンロードされます。クラウド・サービス・プロバイダの CA は、クラウド・サービスで設定されたコミュニティ・メンバで使用します。クラウド・サービスをオフにすると、クラウド・サービス・プロバイダ CA は消去されます。

推奨設定

証明書ベースのサイト間 VPN を 1 つのリモート・サイトでのみ使用する場合は、各サイトの内部 CA をエクスポートして、他のサイトのトラスト CA リストに追加することをお勧めします。

証明書ベースのサイト間 VPN を複数のリモート・サイトで使用する場合は（メッシュ設定）、すべてのサイトで同じ CA を使って、アプライアンス上の署名リクエストを作成する内部使用の証明書に署名することをお勧めします。また、同じ CA をすべてのサイトのトラスト CA リストに追加する必要があります。CA は、Verisign などの外部 CA サービス（有料）、またはこのアプライアンスの内部 CA を使うことができます。外部のリクエストを署名する方法は、以下のとおりです。

トラスト CA を追加するには

1. [追加]をクリックします。
2. CA の識別子ファイル（CRT ファイル）を探してアップロードします。
3. CA 名をお勧めしますが、別の名前を付けても構いません。[Preview CA details]をクリックして、CRT ファイルの詳細情報を確認します。
4. [適用]をクリックします。CA がトラスト CA リストに追加されます。

トラスト CA の設定を編集するには

1. リストから CA を選択します。
2. [編集]をクリックします。[編集]ウィンドウが開きます。
3. CRL(Certificate Revocation List)に関する必要なオプションを選択します。
   • HTTP サーバからCRLを取得 - CRLの取得にHTTPを使ってCAにアクセスできます。チェックをオンにすると、リモート・サイトの証明書のCRL検証はアプライアンスでは行われません。
アプライアンスの設定

Security GatewayにCRLキャッシュを格納 - 新しく更新されたCRLを取得する間隔を選択します。

- 期限が切れたら新しいCRLを取得 - CRLの期限が切れたとき。
- 新しいCRLを次の間隔で取得（時間）- CRLの有効期限に関係なく間隔を指定。

4. [詳細]をクリックしてCAの詳細を表示できます。
5. [適用]をクリックします。

トラストCAを削除するには
1. リストからトラストCAを選択して、[削除]をクリックします。
2. 確認メッセージで[OK]をクリックします。

内部CAまたは他のインポートしたCAをエクスポートするには
1. 表から内部CAを選択します。
2. [エクスポート]をクリックします。内部CAの識別子ファイルは、ブラウザからダウンロードされ、リモート・サイトのトラストCAリストにインポートできるようになります。
3. 必要であれば、リストに追加した他のトラストCAを選択して[エクスポート]をクリックし、エクスポートすることも可能です。

内部CAでリモート・サイトの証明書リクエストを署名するには
1. [リクエストの署名]をクリックします。ファイルをアップロードするウィンドウが開きます。
2. [参照]をクリックして、リモート・サイトで作成された署名リクエストのファイルとしてアップロードします。サーバー・パーティ製アプライアンスの場合は、管理ガイドで署名リクエストが作成される場所を確認してください。

ファイルは、アプライアンスからアクセスできるパスに置くことが必要です。[OK]をクリックして、参照ウィンドウでファイルがアップロードされて正しくフォーマットされていれば、内部CAで署名されます。
完了すれば、[ダウンロード]ボタンがクリック可能になります。
3. [ダウンロード]をクリックします。署名された証明書がブラウザからダウンロードされ、リモート・サイトの証明書リストにインポートできるようになります。

インストール済み証明書の管理

[VPN]→[証明書]→[インストール済み証明書]ページでは、アプライアンスの証明書を作成したり、PKCS#12 (.p12, .pfx)ファイルをアップロードしたりできます。

インストールされた証明書はサイト間VPNの認証に使われます。
クラウド・サービスがオンになっていてアプライアンスがクラウド・サービスで設定されている場合、クラウド・サービス・プロバイダ証明書がアプライアンスに自動的にダウンロードされます。クラウド・サービス・プロバイダ証明書は、クラウド・サービスで設定されたコミュニティ・メンバで使用します。クラウド・サービスをオフにすると、クラウド・サービス・プロバイダ証明書は消去されます。
署名済み証明書の作成方法は、次のとおりです。
1. 新しい署名リクエストを作成します。
2. 署名済みリクエストをエクスポートします（署名リクエストをアプライアンスからダウンロード）。
3. 署名リクエストをCAに送信します。
4. 署名済み証明書をCAから受信したら、アプライアンスにアップロードします。

新しい証明書を作成してCAで署名を行うには
1. [新しい署名リクエスト]をクリックします。[新規の証明書リクエスト]ウィンドウが開きます。
2. 証明書の名前を入力します。
アプライアンスの設定

3. [サブジェクト DN]に、識別名を入力します（CN=myGateway など）。
4. 証明書に他の名前を付ける場合は[新規]をクリックします（オプション）。「タイプ」を選択し、[代替名]に入力し[適用]をクリックします。
5. [生成]をクリックします。

新しい署名リクエストが表に追加され、ステータスが[署名済み証明書の待機中]になります。リクエストの作成後に編集することはできません。

署名リクエストをエクスポートするには
[エクスポート]をクリックします。

署名済み証明書を CA から受信後にアップロードするには
1. 表から署名リクエストのエントリを選択します。
2. [署名済み証明書のアップロード]をクリックします。
3. 署名済み証明書ファイルを探します（*.crt）。
4. [完了]をクリックします。

インストールされた証明書のステータス表記が[署名済み証明書の待機中]から[検証済み]に変わります。

PKCS#12(.p12,.pfx)ファイルをアップロードするには
1. [P12 証明書のアップロード]をクリックします。
2. PKCS#12 ファイルを探します（*.p12 または*.pfx）。
3. 必要に応じて証明書名を編集します。
4. 証明書のパスワードを入力します。
5. [適用]をクリックします。

内部証明書の管理

[VPN]→[証明書]の[内部証明書]では、アプライアンスのサイト間 VPN で使われる内部証明書の詳細を確認できます。また、証明書を署名したり外部証明書の署名をする、内部 CA で使われる証明書の確認や再初期化も可能です。

サイト間 VPN に基づく証明書を作成する際、内部 CA で署名された証明書が一度使われると、インターネット接続の IP アドレス変更と共に CA の証明書を再初期化する必要があります。再初期化は、このページで実行できます。

頻繁な再初期化を回避するためにも、DDNS 機能を使う事をお勧めします。[デバイス]→[DDNS]を参照してください。DDNS を設定すれば、証明書を再初期化する必要があるのは一度だけです。DDNS 機能の設定で変更があれば、自動的に証明書が再初期化されます（デフォルト）。

証明書を再初期化するには
1. [証明書の再初期化]をクリックします。[証明書の再初期化]ウィンドウが表示されます。
2. 通常、対象と思われるデバイスのホスト名（DDNS が設定されている場合）または外部 IP アドレスが表示されます。複数のインターネット接続が設定されている場合、負荷共有モードでは、アプライアンスのアクセス可能な IP アドレスを手動で入力することが可能です。これは、リモート・サイトから内部 CA にアクセスして証明書の取り消しを確認する場合に使用します。
3. [適用]をクリックします。
内部 CA 証明書をエクスポートするには
[内部 CA 証明書のエクスポート]をクリックして、内部 CA 証明書をダウンロードします。

内部 CA でリモート・サイトの証明書リクエストを署名するには
1. [リクエストの署名]をクリックします。ファイルをアップロードするウィンドウが開きます。
2. [参照]をクリックして、リモート・サイトで作成された署名リクエストのファイルとしてアップロードします。サード・パーティ製アプライアンスの場合は、管理ガイドで署名リクエストが作成される場所を確認してください。
   ファイルは、アプライアンスからアクセスできるパスに置くことが必要です。[OK]をクリックして、参照ウィンドウでファイルがアップロードされて正しくフォーマットされていれば、内部 CA で署名されます。
   完了すれば、[ダウンロード]ボタンがクリック可能になります。
3. [ダウンロード]をクリックします。署名された証明書がブラウザからダウンロードされ、リモート・サイトの証明書リストにインポートできるようになります。
ユーザおよびオブジェクトの管理

このセクションでは、ユーザ（User Awareness、ユーザ、管理者、および認証サーバ）およびネットワーク・リソースのセットアップおよび管理の方法について説明します。

ユーザ認識

「User Awareness との連携」（92ページ）を参照してください。

ローカル・ユーザとユーザ・グループの設定

ユーザー認識とユーザブジェクトの設定は、ユーザーおよびオブジェクトページでは、ローカルのユーザとユーザ・グループを作成できます。アクセス・ポリシーでこれらのオブジェクトを使用するには、ユーザ認識を有効にする必要があります。

ユーザ・オブジェクトを使用すると、ユーザ・アクセスを制御する複数の条件を定義できます。以下の条件があります。

- ユーザにネットワーク・アクセスを許可する期間。
- ユーザにリモート・アクセスを許可するかどうか。

新しいローカル・ユーザを追加するには

1. [新規]→[ローカル・ユーザ]をクリックします。
2. [ユーザ名]、[パスワード]、[コメント]（オプション）に入力します。パスワードや共有キーを入力する際は、{}[]`~|'"#+ の文字は使用できません。
3. テンポラリ・ユーザやゲストの場合は[テンポラリ・ユーザ]をクリックします。
   有効期限と時間を入力します。
4. このユーザ・グループにリモート・アクセス権限を付与する場合は、[リモート・アクセス権限の付与]を選択します。
5. [適用]をクリックします。
   作成したユーザがページの表に追加されます。

リモート・アクセス権限を持つ新しいローカル・ユーザ・グループを追加するには

1. [新規]→[ユーザ・グループ]をクリックします。
2. グループ名を入力します。
3. このグルーにリモート・アクセス権限を付与する場合は、[リモート・アクセス権限]を選択します。
4. ユーザのリストから該当のチェックボックスを選択し、グループに追加する初期ユーザを選択します。または、[新規]をクリックして新しいユーザを作成します。
   ユーザ・リストの上に表示される、グループ・メンバの概要を確認することができます。メンバを削除するには、そのユーザ名の隣にある[X]をクリックします。
5. [適用]をクリックします。
   作成したグループがページの表に追加されます。

失効したローカル・ユーザを自動的に削除するには

1. [デバイス]→[詳細設定]へ移動します。
2. [ユーザ管理]を選択します。
3. [編集]をクリックします。
アプライアンスの設定

ユーザ管理ウィンドウが開きます。
4. [失効したローカル・ユーザを自動削除] チェックボックスを選択します。
5. [適用] をクリックします。

失効したローカル・ユーザが、24 時間毎に（午前 0 時から）自動削除されます。

ユーザ/グループを編集するには
1. リストからユーザまたはグループを選択します。
2. [編集] をクリックします。
3. 必要な変更を行ってから [適用] をクリックします。

ユーザまたはグループを削除するには
1. リストからユーザまたはグループを選択します。
2. [削除] をクリックします。
3. 確認メッセージで [OK] をクリックします。
4. ユーザ/グループが削除されます。

ローカル・システム管理者の設定
「ローカル・システム管理者の設定」（50ページ）を参照してください。

認証サーバの管理
[認証サーバ] ページでは、複数の認証サーバを定義、参照できます。外部ユーザ・データベースと、そのデータベースに定義されているユーザの認証方法を定義できます。

定義できる認証サーバの種類は以下のとおりです。
- RADIUS サーバ - プライマリとセカンダリの RADIUS サーバの詳細を定義できます。Check Point 730/750 Appliance は RADIUS サーバに接続し、これらのサーバで定義、認証されているユーザを認識できます。
- Active Directory ドメイン - 組織に属するユーザの情報が登録された Active Directory ドメインの詳細を定義できます。ユーザ認証機能では、これらの詳細情報を使用してシームレスにユーザを認識し、その識別情報をログ記録やユーザ・ベースのポリシー設定に活用することができます。この機能は、VPN リモート・アクセスのユーザ認証にも使用できます。この場合は、[VPN] → [リモート・アクセス・ユーザ] ページで追加設定を行う必要があります。

RADIUS サーバを追加するには
1. [設定] をクリックします。
2. [プライマリ] タブで以下の情報を入力します。
   - [IP アドレス] - RADIUS サーバの IP アドレス。
   - [ポート] - RADIUS サーバがクライアントとの通信に使用するポート番号。デフォルトは 1812 です。
   - [共有秘密キー] - RADIUS サーバと Check Point 730/750 Appliance の間で使用される秘密情報（メッセージの暗号化に使用される事前共有情報）。パスワードや共有キーを入力する際は、{ } [ ] ` ~ | ' " # + の文字は使用できません。
   - [表示] - 共有秘密情報を表示します。
   - [タイムアウト] - RADIUS サーバとの通信に適用するタイムアウト値 (秒単位)。デフォルトのタイムアウトは 3 秒です。
アプライアンスの設定

3. セカンダリ RADIUS サーバを使用する場合は、[セカンダリ]タブで手順 2 を繰り返します。
   注 - IP アドレスや共有キーに入力した情報を削除する場合は、[クリア]をクリックします。
4. [適用]をクリックします。
   プライマリとセカンダリ（定義した場合）のサーバがページの [RADIUS] セクションに追加されます。
   RADIUS サーバは以下の用途に使用できます。
   - リモート・アクセス権限のあるユーザのデータベースを定義する。このようなユーザの定義と認証は RADIUS サーバで行います。
   - 管理者を定義する。詳細については、[ユーザ&オブジェクト] → [管理者]ページを参照してください。

RADIUS サーバを編集するには
1. 編集する RADIUS サーバの IP アドレス・リンクをクリックします。
2. 必要な変更を行います。
3. [適用]をクリックします。
   変更内容が RADIUS サーバに適用されます。

RADIUS サーバを削除するには
削除する RADIUS サーバの横にある削除のリンクをクリックします。
RADIUS サーバが削除されます。

RADIUS サーバに定義されているユーザのリモート・アクセス権限を設定するには
1. [RADIUS ユーザの権限] をクリックします。
2. [RADIUS 認証をリモート・アクセス・ユーザに有効にする] チェック・ボックスをオンまたはオフにします。
3. オンにした場合は、リモート・アクセス権限を付与するユーザを選択します。
   - RADIUS サーバに定義されているすべてのユーザの認証を許可するには、[RADIUS サーバで定義されたすべてのユーザ] を選択します。
   - RADIUS サーバに定義されている特定のユーザ・グループの認証を許可するには、[特定 RADIUS グループのみ] を選択し、ユーザ・グループの名前をカンマ区切りでテキスト・フィールドに入力します。
   - 管理者に認証目的で読み取り専用権限を付与するには - [読み取り専用管理者] を選択します。
4. [適用]をクリックします。

Active Directory ドメインを追加するには
   [新しいドメインの追加] ウィンドウが開きます。
2. 以下の情報を入力します。
   - [ドメイン] - ドメイン名。
   - [IP アドレス] - ドメインのいずれかのドメイン・コントローラの IP アドレス。
   - [ユーザ名] - 設定を効率化し、Active Directory に定義されているユーザを使用してユーザベースのポリシーを作成するには、管理者権限のあるユーザを指定する必要があります。
   - [パスワード] - ユーザーのパスワード。パスワードや共有キーを入力する際は、{ } [ ] ` ~ | ' " # + の文字は使用できません。
   - [ユーザ DN] - [検索]をクリックして該当のユーザを表すオブジェクトの DN を自動検出するか、そのユーザの DNS を入力します。例えば、次のように入力します。CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com
3. Active Directoryに定義されたユーザ・データベースの一部のみを使用する場合は、[特定のブランチからのユーザグループのみ使用]を選択します。[ブランチ]のテキスト・フィールドにそのブランチ名（フルDN）を入力します。

4. [適用]をクリックします。

定義したActive Directoryが表に表示されます。このActive Directoryを選択して、編集や削除を行うことができます。

編集を行う場合、ドメイン情報は読み取り専用となり変更することはできません。

新しいActive Directoryドメインを追加する際、既存のドメインを使用して別のオブジェクトを作成することはできません。

Active Directoryに定義されているすべてのユーザにリモート・アクセス権限を設定するには

Active Directoryに定義されているユーザには、デフォルトではリモート・アクセス権限は付与されません。[VPN]→[リモート・アクセス・ユーザ]ページから、ローカルまたはActive Directoryで定義されているユーザを個別に選択してリモート・アクセス権限を付与できます。

1. [Active Directoryユーザの権限]をクリックします。

2. [Active Directoryのすべてのユーザ]を選択します。このオプションを使用する場合、[VPN]→[リモート・アクセス・ユーザ]ページに移動して特定のユーザを選択する必要はありません。

Active Directoryには、たいてい多数のユーザが含まれています。組織へのリモート・アクセス権限をすべてのユーザに付与することは、お勧めできません。[選択したActive Directoryユーザ・グループ]オプションを選択し、[VPN]→[リモート・アクセス・ユーザ]ページでリモート・アクセス権限を設定します。

3. [適用]をクリックします。

定義したActive Directoryとの同期化モードを変更するには


3. [適用]をクリックします。

Active Directoryを編集するには

1. リストからActive Directoryを選択します。

2. [編集]をクリックします。

3. 必要な変更を行ってから[適用]をクリックします。

Active Directoryを削除するには

1. リストからActive Directoryを選択します。

2. [削除]をクリックします。

3. 確認メッセージで[OK]をクリックします。

選択したActive Directoryが削除されます。

注 - このページには、[VPN]タブと[ユーザ&オブジェクト]タブからアクセスできます。
アプリケーションと URL の管理

アプリケーションと URL の管理

アクセス・ポリシーを設定するにはアプリケーションのデフォルト・ポリシーのリンクをクリックするか、アプリケーションの[ブレード・コントロール]ページのリンクをクリックします。

すべてのビルトイン・アプリケーションとカテゴリについての詳細は、ページの上部にあるCheck Point AppWikiリンクをクリックしてください。

注：[アクセス・ポリシー]→[ファイアウォール・ブレード・コントロール]ページでURLフィルタリングが有効になっている場合は、URLとカスタム・アプリケーションが含まれるルールが使われます。

カスタム・アプリケーションとは

多くのアプリケーションはブラウザ・ベースです。カスタム・アプリケーションは、URLで文字列または正規表現の検索で定義できます。

カテゴリとは

各 URL は、Check PointクラウドのURLフィルタリング・ブレードを使って検査され、ビルトイン・カテゴリに一致します（例：フィッシング・サイト、高帯域幅、ギャンブル、ショッピングなど）。

アプリケーション&カテゴリのリスト

アプリケーションとカテゴリの一覧が、リスト上部に表示されるフィルタリングに基づいて表示されます。フィルタリングには4種類あります。

- 共通 - 一般的に使われるアプリケーション、カスタム・アプリケーション、カテゴリ。
- カスタム - カスタム・アプリケーションのみ。
- カテゴリ - カテゴリのみ。
- すべて

タグのアイコンがカテゴリの横に表示され、アプリケーション専用アイコンがアプリケーションの横に表示されます。

アプリケーション・データベースでは、各アプリケーションはその特質に基づいて1つのプライマリ・カテゴリに割り当てられます。また、アプリケーションの特徴として追加のカテゴリがあります。たとえば、「Pinterest」のプライマリ・カテゴリはソーシャル・ネットワーキングで、追加のカテゴリは写真（フォト）の共有とSSLプロトコルです。カテゴリがルールにある場合、ルールでそのカテゴリにマーキングされたすべてのアプリケーションとマッチングを行います。

新しいアプリケーションが、アクセス・ポリシーのルール・ベースにある追加カテゴリに追加されると、データベースの更新とともにルールが自動的にアップデートされます。

カテゴリ/アプリケーションを検索するには

1. リストを絞り込んで必要なアイテムを表示します。
2. 絞り込むフィルタリング・ボックスにアプリケーションのカテゴリを入力します。

入力し始めると、リストが文字ごとにフィルタリングされます。

カスタム URL を作成するには

1. 新規→[URL]を選択します。
2. URL を入力します。
3. ［適用］をクリックします。
   URL はルールに使用できます。

カスタム・アプリケーションを作成するには
1. ［新規］→［アプリケーション］を選択します。
2. カスタム・アプリケーションの名前を入力します。
3. リストからブラウザ・カテゴリーを選択します。
4. 文字列の代わりに正規表現を使用する場合は、［すべての URL は正規表現］を選択します。正規表現では PCRE 構文を使用します（例：www.malicioussite.com を正規表現を使用してブロックするには 「.* ¥.malicioussite ¥.com」 を使用）。
5. ［新規］をクリックして、アプライアンスが URL で検出する文字列の一部または正規表現を追加し、［OK］をクリックします。
6. 関連する文字列/正規表現をさらに追加する場合はステップ 5 を繰り返します。文字列/正規表現の１つが見つかると、カスタム・アプリケーションが一致します。
7. ［追加カテゴリ］タブをクリックして、必要に応じてさらにカテゴリを選択します。
8. ［適用］をクリックします。
   アプリケーションはルールに使用できます。

カスタム・アプリケーション・グループを作成するには
1. ［新規］→［アプリケーション・グループ］を選択します。
2. グループ名を入力します。
3. グループ・メンバとして追加するアプリケーションとカテゴリーを選択します。選択リストを絞り込む場合は、共通、カテゴリー、カスタム、すべての各リンクをクリックします。
   グループ・メンバのウィンドウが開き、選択したアイテムのクイック・ビューが表示されます。選択したアイテムの横にある「×」をクリックして、簡単に削除することができます。
4. 必要であれば、［新規］をクリックしてカスタム・アプリケーションまたは URL をリストに追加できます。
   カスタム・アプリケーションの作成方法については、上記を参照してください。
5. ［適用］をクリックします。
   カスタム・アプリケーション・グループはルールに使用できます。

システム・サービスの管理
[ユーザーオブジェクト] → [サービス] ページには、システムに定義されているシステム・サービスのリストが表示されます。このページでは、新しいサービスの追加や、サービスの編集と削除を行うことができます。
サービス・オブジェクトを使って、異なるネットワーク・プロトコルを簡単に定義できます。通常は IP プロトコルとポート (TCP および UDP IP プロトコルで使用) を使います。
これらのオブジェクトで、セキュリティ・ポリシーがベースのルーティング・ルールを定義できます。サービス・オブジェクトの多くはシステムで事前に定義されており、削除することはできません。事前に定義されている「システムのサービス」は、対象サービスの接続性やセキュリティに関する精密なインスペクションを実行するアプライアンスでの機能性を表わしています。システムのサービスには、追加の設定オプションがある場合があります。

新しいサービスを作成するには
1. ［新規］をクリックします。
2. [サービス]タブで、指定するサービスのタイプに適用するフィールドの情報を入力します。すべてのフィールドが表示されない場合もあります。
   - [名前] - サービス名を入力します。
   - [タイプ] - リストからサービスのタイプを選択します。
     - TCP
     - UDP
     - ICMP - ICMP プロトコルで特定のオプションが必要な場合はこれを選択します。これは高度なオプションです。
     - その他 - TCP または UDP 以外の IP プロトコルの場合はこれを選択します。
   - [ポート] - [タイプ]で TCP または UDP を選択した場合はポートを入力します。ポート番号、または範囲をカンマで区切りて入力できます。
   - [IP プロトコル] - [タイプ]でその他を選択した場合は IP プロトコルを入力します。
   - [ICMP タイプ]と[ICMP コード] - サービス・オブジェクトを RFC 792 でリストされるようにすることは、ICMP タイプとコードを入力します。このオプションは[タイプ]で ICMP を選択した場合のみ該当します。
   - [コメント] - オプションのコメントを入力します。
   - このサービスのインタフェクションを無効にする - このサービスに一致するトラフィックの詳細インタフェクションを無効にする場合はこのチェックボックスをオンにします。このオプションはビルトイン・サービスでのみ選択できます。

3. [詳細]タブで、指定するサービスのタイプに適用するフィールドの情報を入力します。すべてのフィールドが表示されない場合もあります。

一般
- [セッション・タイムアウト(秒) ] - セッションのタイムアウトまでの時間を秒で示します。
- [ソース・ポートの使用] - クライアント側のサービスに対し、このオプションを選んでポート番号を入力します。
- [返答を許可] (TCP サービス以外に該当) - オフの場合、サーバからクライアントのパケットが異なる接続として処理されます。
- [一致] (Check Point サポートが使う高度なオプション)

接続処理
- [ポリシーのインストール後も接続したままにする] - 新しいポリシーで禁止されている場合、このオプションを選択できます。この設定を変更した場合、オープン接続には影響せず、以降の接続のみに反映されます。
- [クラスタでの同期] - クラスタでの HA または負荷共有での状態の同期を有効にします。ルール・ベースで許可されたサービスのうち、クラスタ上の接続同期を行うサービスだけが、クラスタを通過する際に同期されます。デフォルトでは、新規/既存に関わらずすべてのサービスが接続されます。
- [同期開始 X 秒後（接続開始後）] - TCP サービスの場合には、このオプションを使用して Check Point 730/750 Appliance への接続情報の通知を遅らせる、接続開始 x 秒後に接続がまだ存在する場合にのみ接続を同期するように設定できます。一部の TCP サービス（たとえば HTTP）には、継続時間が非常に短いという特徴があります。これらの接続を同期化すると、ゲートウェイ・リソースを消費しフェイルオーバーが発生する時までに接続が終了してしまうため、同期化は意味がありません。

アグレッシブ・エージング
この機能は、[デバイス]→[詳細]ページから設定できます。アプライアンスに負荷がかかっている場合、古い接続が先にメモリから削除され、新しい接続ができるように容量を確保します。
- [アグレッシブ・エージングを有効にする] - このオプションを選択してコネクション・テーブルの容量を管理し、ゲートウェイのメモリ消費を減らして継続時間と安定性を向上させます。
- [アグレッシブ・エージングのタイムアウト(秒) ] - セッションのタイムアウトまでの時間を秒で示します。
4. [適用]をクリックします。

サービスを編集するには
1. リストからサービスを選択します。
2. [編集]をクリックします。
3. 必要な変更を行います。すべてのフィールドが表示されない場合もあります。
4. [適用]をクリックします。

サービスを削除するには
1. リストからサービスを選択します。削除できるのはユーザが定義したサービスのみです。
2. [削除]をクリックします。
3. 確認メッセージで[はい]をクリックします。

特定のサービスを絞り込むには
1. [入力して絞り込み]ボックスにサービス名やその一部を入力します。
2. 入力するとリストが絞り込まれ、入力内容に合致する結果が表示されます。

組み込みのシステム・サービス
組み込みサービスの中には、Check Point の技術をフル活用して特定のプロトコルを深いレベルで検査できるものがあります。これらのシステム・サービスは削除することができません。編集する場合は、いつ深いレベルでの検査が行われるかは設定したポートで決定します。デフォルトのポートは追加/変更できます。一部のシステム・サービスには、深いレベルでの検査の実行方法に影響する追加設定が含まれています。

・ HTTP - [IPS 設定]タブでは、HTTP の深いレベルでの検査を実行する方法とタイミングを設定できます。該当するオプションを選択します。
・ HTTPS - [URL フィルタリング設定]タブでは、証明書の情報ごとに HTTPS サイトを分類できます。
・ FTP - ファイアウォール設定タブで、ファイアウォールでデータ接続を自動的に検出する方法を設定します。以下のいずれかのオプションを選択します。
  ▪ 任意 - ファイアウォールですべてのモードの FTP データ接続を検知および許可します。
  ▪ アクティブ - ファイアウォールでアクティブ・モードの FTP データ接続のみを検知および許可します。
  ▪ パッシブ - ファイアウォールでパッシブ・モードの FTP データ接続のみを検知および許可します。
・ PPTP_TCP - [IPS 設定]タブでは、PPTP の深いレベルでの検査方法を設定できます。
  ▪ Action on malformed connections - 解析が失敗した場合に接続で実行するアクションを選択します。
  ▪ トラックイング - 解析が失敗した場合に発行するログのタイプを選択します。
  ▪ 厳格な PPTP 解析を実施 - プロトコルに対する厳しい実施を行う場合はこれを選択します。
・ SNMP - [ファイアウォール設定]タブで、ファイアウォールで SNMP での読み取り専用モードを実施するよう設定できます。
・ SSH - [ファイアウォール設定]タブで、ファイアウォールで古いバージョンの SSH プロトコル (1.x) をブロックするよう設定できます。
・ Citrix - [ファイアウォール設定]タブで、設定したポートでサポートするプロトコルを設定できます。デフォルトのポート 1494 番は、一般的に 2 つの異なるプロトコル、Winframe または Citrix ICA で使われます。
サービス・グループの管理

[ユーザ＆オブジェクト]→[サービス・グループ]ページには、システムに定義されているサービス・グループのリストが表示されます。このページでは、新しいサービス・グループの追加や、既存のサービス・グループの編集と削除を行うことができます。

サービス・グループを定義すると、セキュリティ・ポリシーの設定が効率化されます。グループを使用してセキュリティ・ポリシーを設定する場合と比較して、継続的なポリシーの管理がはるかに容易になります。新しいサービス・オブジェクトをシステムに追加する場合は、関連するグループにオブジェクトを追加するだけで、自動的にポリシーが適用されます。

システムには、一般的なサービス用の組み込みのサービス・グループがいくつか用意されています。一部のサービス・グループには、特定のプロトコルを検査するための追加設定が含まれています。

新しいサービス・グループを作成するには
1. 新規をクリックします。
2. [新しいサービス・グループ]ウィンドウが開きます。
3. グループの名前とコメント（オプション）を入力します。
4. 必要なサービスがリストにない場合は、新規をクリックします。新しいサービス・オブジェクトを作成する方法については、ユーザ＆オブジェクト→[サービスページ]を参照してください。
5. [適用]をクリックします。
6. [新しいサービス・グループ]ウィンドウが開き、選択したサービスが表示されます。
7. [新しいサービス・グループ]ウィンドウで[新規]をクリックすることもできます。
8. [適用]をクリックします。

サービス・グループを編集するには
1. リストからグループを選択します。
2. [編集]をクリックします。
3. 必要な変更を行います。
4. [適用]をクリックします。

サービス・グループを削除するには
1. リストからグループを選択します。削除できるのは、ユーザ定義のサービス・グループだけです。
2. [削除]をクリックします。
3. 確認メッセージで[はい]をクリックします。

ネットワーク・オブジェクト・グループを絞り込むには
1. [絞り込む語を入力]ボックスに目的のサービス・グループの名前またはその一部を入力します。
2. 入力するにつけでリストが絞り込まれ、入力内容に合致する結果が表示されます。

組み込みのシステム・サービス・グループ
組み込みのサービス・グループの中には、Check Pointの技術をフル活用して特定のプロトコルを深いレベルで検査できるものがあります。これらのシステム・サービス・グループは削除することができません。
組み込みのサービスのリストを保持しているため、グループの内容を編集しても、[リセット]をクリックすれば復元することができます。
一部のシステム・サービス・グループには、深いレベルでの検査の実行方法に影響する追加設定が含まれています。

[DNS]- [ファイアウォール設定] タブでは、DNS を介した NAT サポートを設定できます。このオプションを選択すると、DNS トライフィックのパフォーマンスに影響します。NAT と、インターネットからアクセス可能な内部 DNS サーバの両方を使用している場合を除き、通常はこのオプションを選択する必要はありません。[IPS 設定] タブでは、DNS の深いレベルでの検査を実行する方法とタイミングを設定できます。該当するオプションを選択します。

ネットワーク・オブジェクトの管理

[ユーザ&オブジェクト] → [ネットワーク・オブジェクト] ページには、システムに定義されているネットワークオブジェクトのリストが表示されます。このページでは、新しいネットワーク・オブジェクトの追加や、ネットワーク・オブジェクトの編集と削除を行うことができます。ネットワーク・オブジェクトの最も基本的な用途は、セキュリティポリシーとその例外を定義することです。ネットワーク・オブジェクトは内部 DNS サーバーのホストとして使用でき、その IP アドレスは内部 DHCP サービスに対して固定アドレスとして設定できます。
以下の種類のネットワーク・オブジェクトが用意されています。

• [単一 IP] - 単一の IP アドレスが割り当てられたデバイスを表すネットワーク・オブジェクト。
• [IP 範囲] - IP アドレスの範囲を表すネットワーク・オブジェクト。
• [ネットワーク] - ネットワークを表すネットワーク・オブジェクト。

【単一 IP】ネットワーク・オブジェクトを作成するには
1. [新規]をクリックします。
   [新しいネットワーク・オブジェクト] ウィンドウが開きます。
2. [タイプ] で [単一 IP] を選択します。
3. IP アドレスとオブジェクト名を入力します。
4. 必要に応じて、以下のオプションをオンまたはオフにします。
   • DNS サーバをこのオブジェクト名に解決 - ゲートウェイが内部ネットワークの DNS サーバである場合、このオプションがオンになっていると、サーバ/ネットワーク・オブジェクトの名前が IP アドレスに変換されます。
   • DHCP サービスから除外 - 内部 DHCP サービスは、このサーバ/ネットワーク・オブジェクトの設定された IP アドレスを誰にも配布しません。
     ▪ DHCP サービスで MAC の IP アドレスを予約 - 内部 DHCP サービスで、MAC アドレスに基づき、設定された IP アドレスをこのサーバ/ネットワーク・オブジェクトのみに配布します。
     ▪ MAC アドレスを入力 - IP 予約に必要です。[アクティブなコンピュータ] ページからオブジェクトを作成するとき、MAC アドレスは自動的に検出されます。
5. [適用] をクリックします。

【IP 範囲】ネットワーク・オブジェクトを作成するには
1. [新規]をクリックします。
   [新しいネットワーク・オブジェクト] ウィンドウが開きます。
2. [タイプ] で [IP 範囲] を選択します。
3. [開始 IP] フィールドに IP 範囲の開始 IP アドレス、[終点 IP] フィールドに IP 範囲の終了 IP アドレスを入力します。
4. オブジェクト名を入力します。
5. 必要に応じて、以下のオプションをオンまたはオフにします。
   - [DHCP サービスから除外] - 内部 DHCP サービスは、設定された IP 範囲を割り当てなくなっています。
6. [適用]をクリックします。

ネットワーク・オブジェクトを作成するには

1. [新規]をクリックします。
2. [新しいネットワーク・オブジェクト]ウィンドウが開きます。
3. [タイプ]で[ネットワーク]を選択します。
4. ネットワーク・アドレスとサブネット・マスクを入力します。
5. [適用]をクリックします。

ネットワーク・オブジェクトを編集するには

1. リストからネットワーク・オブジェクトを選択します。
2. [編集]をクリックします。
3. 必要な変更を行います。
4. [適用]をクリックします。

ネットワーク・オブジェクトを削除するには

1. リストからネットワーク・オブジェクトを選択します。
2. [削除]をクリックします。
3. 確認メッセージで[はい]をクリックします。

ネットワーク・オブジェクトを絞り込むには

1. [絞り込む語を入力]ボックスに目的のネットワーク・オブジェクトの名前またはその一部を入力します。
2. 入力するにつれてリストが絞り込まれ、入力内容に合致する結果が表示されます。

ネットワーク・オブジェクト・グループの管理

ユーザ→ネットワーク・オブジェクト→ネットワーク・オブジェクト・グループページには、システムに定義されているネットワーク・オブジェクト・グループのリストが表示されます。このページでは、新しいネットワーク・オブジェクト・グループの追加や、ネットワーク・オブジェクト・グループの編集や削除を行うことができます。

ネットワーク・オブジェクトのグループを定義するとき、セキュリティ・ポリシーの設定が効率化されます。グループを使用してセキュリティ・ポリシーを設定すると、特定のオブジェクトを使用する場合と比較して、継続的なポリシーの管理がはるかに容易になります。新しいネットワーク・オブジェクトをシステムに追加する場合は、関連するグループにオブジェクトを追加するだけで、自動的にポリシーが適用されます。

新しいネットワーク・オブジェクト・グループを作成するには

1. [新規]をクリックします。
2. [新しいネットワーク・オブジェクト・グループ]ウィンドウが開きます。
3. グループの名前とコメント（オプション）を入力します。
3. [選択]をクリックして使用可能なネットワーク・オブジェクトのリストを表示し、該当するチェック・ボックスをオンにします。

4. 必要なネットワーク・オブジェクトがリストにない場合は、[新規]をクリックします。新しいネットワーク・オブジェクトを作成する方法については、[ユーザ&オブジェクト]→[ネットワーク・オブジェクト]ページを参照してください。

5. [適用]をクリックします。
   [新しいネットワーク・オブジェクト・グループ]ウィンドウが開き、選択したネットワーク・オブジェクトが表示されます。

6. [新しいネットワーク・オブジェクト・グループ]ウィンドウで[新規]をクリックすることもできます。

7. グループ・リストからネットワーク・オブジェクトを削除するには、そのオブジェクトを選択して[削除]をクリックします。

8. [適用]をクリックします。
   ネットワーク・オブジェクト・グループがグループのリストに追加されます。

ネットワーク・オブジェクト・グループを編集するには

1. リストからグループを選択します。
2. [編集]をクリックします。
3. 必要な変更を行います。
4. [適用]をクリックします。

ネットワーク・オブジェクト・グループを削除するには

1. リストからグループを選択します。
2. [削除]をクリックします。
3. 確認メッセージで[はい]をクリックします。

ネットワーク・オブジェクト・グループを絞り込むには

1. [絞り込む語を入力]ボックスに目的のネットワーク・オブジェクト・グループの名前またはその一部を入力します。
2. 入力するにつれてリストが絞り込まれ、入力内容に合致する結果が表示されます。
ログとモニタリング

このセクションでは、セキュリティおよびシステム・ログについて説明します。また、様々なモニタリング・ツールについても説明します。

セキュリティ・ログの表示

[ログ&モニタリング]→[セキュリティ・ログ]ページには、最新のログ・レコードが100件表示されます。さらに多くのレコードを読み込むには、ページを下方向にスクロールします。ログの表は自動的に更新されます。

セキュリティ・ログを検索するには

[検索クエリを入力]ボックスにクエリを入力します。同時に検索できるフィールドは1つのみです（AND/OR演算子は使用できません）。

使用する構文：
<IP_address>
または
<column_name>:<value>
例えば、次のように入力します。
または action:drop
または source port:22 source port:22
詳細については、表のヘッダの[クエリ構文]をクリックしてください。

セキュリティ・ログ・レコードを表示するには

1. リストでログ・エントリを選択します。
2. [詳細の表示]をクリックするか、エントリをダブルクリックします。
ログ・レコードが開きます。

セキュリティ・ログ・データを更新するには

[更新]アイコンをクリックします。

ローカルでのログ記録を停止するには

ローカルでのログ記録を停止すると、ログを生成して管理する負荷が排除されるため、パフォーマンスが向上します。ログ記録をいったん停止すると、再開するまで新しいログは記録されません。

1. [オプション]→[ローカル・ログの停止]を選択します。
2. 再開するには、[オプション]→[ローカル・ログの再開]を選択します。

ログの保存

ログは、ローカルの一時メモリや外部のSDカードなどに保存することができます。ログは、外部の管理ログ・サーバに送信することもできます（[ログ・サーバ]ページを参照）。

SDカードを差し込むと、自動的にマウントしてローカルのログが保存されます。SDカードを取り出す前に、必ずアンマウントしてください。[オプション]→[SDカードの安全な取り出し]を選択します。
ログをローカルのログ保存場所から削除するには
1. [ログ&モニタリング]→[ログ]→[セキュリティ・ログ]ページで、[ログのクリア]をクリックします。
   確認ウィンドウが開きます。
2. [はい]をクリックしてログを削除します。
   ログが削除され、保存されたログが自動的に更新されます。
注 - ログは、外部の SD カード（使用している場合）またはローカルのログ・ストレージから削除されます。リモート・ログ・サーバからは削除されません。

システム・ログの表示
[ログ&モニタリング]→[システム・ログ]ページには、アプライアンスで生成された、デバッグ・レベルを除くすべてのレベルのシステム・ログ（Syslog）が最大 500 件表示されます。システム・ログの主な用途はトラブルシューティングですが、アプライアンスで発生したイベントを管理者に通知する目的でも使用できます。
Syslog には、以下の種類があります。
- 情報（Info） - 情報提供を目的としたログ。ポリシーの変更や管理者によるログインの詳細、DHCP 要求などを記録します。
- 通知（Notice） - 通知を目的としたログ。管理者によって行われた変更や日時の変更などを記録します。
- 注意（Warning） - 接続や設定に関する障害を示すログ。クリティカルではないものの注意が必要な問題を記録します。
- エラー（Error） - 特定の機能が動作していないことを警告するシステム・エラー。このエラーは、設定ミスや、インターネット・サービス・プロバイダによる対応が必要な接続障害などが原因で発生します。

完全なログ・ファイルをダウンロードするには
1. [完全ログ・ファイルのダウンロード]をクリックします。
2. [開く]または[保存]をクリックします。

Syslog のスナップショットをフラッシュ・ディスクに保存するには
1. [システム・ログのスナップショットをフラッシュに保存]を選択します。
2. 間隔を分単位で指定します。デフォルトは 180 分（3 時間）です。最小値は 30 分です。
3. [適用]をクリックします。
スナップショットを保存すると、再起動が発生しても Syslog を保持できます。ただし、確実に保持できるとは限りません。
システム・ログのリストを更新するには
[更新]をクリックします。リストが更新されます。

ログ・リストを削除するには
1. [ログのクリア]をクリックします。
2. 確認メッセージで[OK]をクリックします。

外部ログ・サーバの設定
[ログ&モニタリング]→[ログ・サーバ]ページでは、ログを保存する場所が追加で必要になった場合に、セキュリティ・ログとシステム・ログの外部ログ・サーバを設定できます。

注 - クラウド・サービスがオンになっている場合は、外部ログ・サーバは設定できません。

外部セキュリティ・ログ・サーバ
追加のログを保存するために、セキュリティ管理サーバで管理する外部のCheck Pointログ・サーバを利用することができます。

WebUIのこのページで外部のCheck Pointログ・サーバを設定する前に、以下の手順を確認してください。

- ログの送り先となるログ・サーバを識別する
- ログ・サーバを管理するセキュリティ管理サーバを識別する
- 該当のセキュリティ管理サーバでSmartDashboardを開く
- セキュリティ・ゲートウェイウィザードで次の各詳細を指定し、Check Point 730/750 Applianceとなるセキュリティ・ゲートウェイオブジェクトを定義、作成します。
  - [General Properties]で、
    - [Gateway platform] - [Check Point 730/750 Appliance]を選択。
    - [Gateway IP address] - [Dynamic IP address]を選択。
  - [Trusted Communication]で、[Gateway Identifier] - [MAC address]または[First to connect]を選択。

オブジェクトを定義するセキュリティ・ゲートウェイウィザードを使用する際の詳細情報については、『Check Point Check Point 730/750 Appliance集中管理ガイド』を参照してください。
外部セキュリティ・ログ・サーバを設定するには

1. External Security Log Server（外部セキュリティ・ログ・サーバ）の横にある[Configure（設定）]をクリックします。
   [External Security Log Server（外部セキュリティ・ログ・サーバ）]ウィンドウが開きます。

2. [Management Server IP address]を入力します。このIPアドレスは、Check Point 730/750 Applianceとセキュリティ管理サーバ間のトラスト通信を確立するためだけに使用されます。

3. [SIC name]で、SmartDashboardで定義されたログ・サーバ・オブジェクトのSIC名を入力します。この名前は、以下のいずれかの方法で取得できます。
   • セキュリティ管理サーバでGuiDBeditを開く - [Tables]タブで、[Table]→[Network Objects]を展開し、ログ・サーバ・オブジェクトを探して、次にsic_nameを探します。
   • ログ・サーバで次のCLIコマンドを実行する（SSHを使用するか、物理マシンでコマンドを実行）

   ```
   $CPDIR/bin/cpprod_util CPPROD_GetValue SIC MySICname 0
   ```
   SIC名の値をコピーして、このページのSIC名フィールドに貼り付けます。

4. [SIC ワンタイム・パスワードの設定]で、セキュリティ管理サーバで入力したパスワードを入力し、確認のために[SIC ワンタイム・パスワードの確認]フィールドで再入力します。パスワードや共有キーを入力する際は、[]`~|の文字は使用できません。

5. ログ・サーバがセキュリティ管理サーバにない場合は、[ログ・サーバで別のIPアドレスを使用]チェックボックスをオンにします。

6. ログ・サーバIPアドレスを入力します。

7. [接続]をクリックします。通知メッセージが表示されます。

   重要 - 外部ログ・サーバを設定した後に、WebUIのこのページで変更を行うと、SmartDashboardでSICの再初期化が必要になります。SmartDashboardでSICの再初期化を行わないと、ログ・サーバへの接続が失敗する可能性があります。
外部システム・ログ・サーバー（システム・ログ用）

外部システム・ログ・サーバーを設定するには
1. External System Log Server（外部システム・ログ・サーバー）の横にある[Configure（設定）]をクリックします。
   [External System Log Server（外部システム・ログ・サーバー）]ウィンドウが開きます。
2. [システム・ログを外部システム・ログ・サーバへ送信]チェックボックスをオンにします。
3. IP アドレスを入力します。
4. ポートを入力します。
5. [適用]をクリックします。

外部システム・ログ・サーバーを編集するには
1. サーバのIP アドレスをクリックします。
2. 必要な情報を編集します。
3. [適用]をクリックします。

外部システム・ログ・サーバーを削除するには
[削除]をクリックします。
サーバが削除されます。

内部ネットワーク内のアクティブ・コンピュータの管理
「内部ネットワークのアクティブ・コンピュータの管理」(24ページ)を参照してください。

感染ホストの表示

[感染ホスト]ページでは、内部ネットワークで感染したホストとサーバーの情報を確認することができます。
また、感染または感染の疑いがあるホスト/サーバーに関する特定の保護に対して、例外ルールを直接作成することもできます。

感染ホストテーブルには、各エントリの次の情報が表示されます。

- アイコン - 感染ホストやサーバーの異なる分類を示すアイコン

<table>
<thead>
<tr>
<th>説明</th>
<th>ホストアイコン</th>
<th>サーバーアイコン</th>
</tr>
</thead>
<tbody>
<tr>
<td>感染ホスト/サーバー - 特定の保護により、アンチボットでホストまたはサーバーと外部のC&amp;Cセンター間での疑わしい通信が検出されたとき</td>
<td>🌡️</td>
<td>🌡️</td>
</tr>
<tr>
<td>感染の疑いがあるホスト/サーバー - 特定の保護により、アンチウイルスでホストやサーバーの感染につながる可能性があるアクティビティが検出されたとき例えば、次のように入力します。</td>
<td>🚫</td>
<td>🚫</td>
</tr>
<tr>
<td>感染したインターネット・サイトや安全でないインターネット・サイトにアクセスすると、マルウェアをインストールしてしまう可能性があります。</td>
<td></td>
<td></td>
</tr>
<tr>
<td>感染したファイルをダウンロードすると、そのファイルを開く際にホストやサーバーを感染させてしまう可能性があります。</td>
<td></td>
<td></td>
</tr>
<tr>
<td>オブジェクト名 - ホストまたはサーバーがネットワーク・オブジェクトとして設定された場合オブジェクト名が表示されます。</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
アプライアンスの設定

- IP/MAC アドレス
- デバイス/ユーザ名 - DHCP またはユーザ認識により Check Point 730/750 Appliance が情報を確認できた場合、デバイス/ユーザ名が表示されます。
- インシデント・タイプ - 検出されたインシデントのタイプ:
  - ボットのアクティビティ
  - マルウェアのダウンロード
  - マルウェアを持つサイトへのアクセス
- 深刻度 - マルウェアの深刻度レベル:
  - 低
  - 中
  - 高
  - クリティカル
- 保護名 - アンチボット/アンチウイルスの保護機能名が表示されます。
- 最終インシデント - 最後のインシデントの日付。
- インシデント - 先月のホストまたはサーバのインシデントの合計件数。大量にある場合は期間が短くなる場合があります。

感染ホストリストを絞り込むには
1. [絞り込み]をクリックします。
2. いずれかの絞込みオプションを選択します。
   - サーバのみ - サーバとして識別されるマシンのみが表示されます（任意のマシン/デバイスではない）。サーバは[アクセス・ポリシー]→[サーバ]ページで定義され、システムのサーバ・オブジェクトとして定義されます。
   - 感染の疑いがあるホストのみ - 感染の疑いがあるホストまたはサーバのみが表示されます。
   - 感染したホストのみ - 感染したホストまたはサーバのみが表示されます。
   - 深刻度が「高」以上のホスト - マルウェアに感染または感染の疑いがあり、深刻度が「高」「クリティカル」なホストおよびサーバが表示されます。

特定の保護にマルウェア例外ルールを追加するには
1. 例外を作成する保護を含むリストのエントリを選択します。
2. [保護機能の例が挿入]をクリックします。
3. ルール・サマリまたは表のセル中のリンクをクリックして、例外ルールの各フィールドに挿入するネットワーク・オブジェクトまたはオプションを選択します。
   - スコープ - 任意を選択するか、リストから特定のスコープを選択します。
   - アクション - 一致するトラフィックで実施するアクションを、[確認] [ブロック] [検出] [非アクティブ]から選びます。アクション・タイプの説明は、[脅威対策]→[脅威対策ブレード・コントロール]ページを参照してください。
   - ログ記録 - 追跡オプションとして[なし] [ログ] [アラート]から選びます。[ログとモノタリング]→[セキュリティ・ログ]ページにログが表示されます。アラートはログのフラグです。フラグを使ってログを絞り込むことができます。
4. [コメントの記入]フィールドにコメントを入力します（オプション）。
5. [適用]をクリックします。
   ルールは[脅威対策]→[例外]ページのマルウェアの例外に追加されます。
特定エントリのログを表示するには
1. 表示するログのリストのエントリを選択します。
2. [ログ]をクリックします。
   [ログ&モニタリング]→[セキュリティ・ログ]ページが開いてIP/MACアドレスに該当するログが表示されます。

注 - このページには、[ホーム]および[ログ&モニタリング]タブからアクセスできます。

VPNトンネルの表示
「VPNトンネルの表示」（129ページ）を参照してください。

アクティブな接続の表示
[ログ&モニタリング]→[接続]ページには、アクティブな接続のリストが表示されます。
このリストには以下のフィールドがあります。
- [プロトコル]
- [ソース・アドレス]
- [ソース・ポート]
- [宛先アドレス]
- [宛先ポート]

リストを絞り込むには
[入力して絞り込み]ボックスに絞り込みの条件を入力します。
入力内容に従ってリストが絞り込まれます。

リストを更新するには
[更新]リンクをクリックします。

モニタリング・データの表示
[モニタリング]ページには、ネットワーク、セキュリティ、トラブルシューティング情報が表示されます。このページにアクセスすることに、データは更新されます。[更新]をクリックして情報をアップデートできます。
モニタリング・レポートのサンプルを見る場合は[デモ]をクリックします。サンプル・レポートを閉じるには[戻る]をクリックします。
システムの現在の接続数は[VPN トンネル]、[アクティブなコンピュータ]、[接続]に表示されます。リンクをクリックしてWebUIページを開くことができます。
[モニタリング]ページは、次のセクションに分かれています。
- ネットワーク
- セキュリティ
- トラブルシューティング
アプライアンスの設定

各セクションのタイトル・バーにある矢印アイコンをクリックして、セクションを展開したり折り畳んだりすることができます。

ネットワーク

デフォルトでは過去 1 時間のネットワーク統計が表示されます。過去 1 日の統計も確認できます。ネットワーク・セクションのタイトル・バーから[過去 1 時間]または[過去 24 時間]を選択します。

データは指定時間ごとに自動的に更新されます。
過去 1 時間の場合、1 分毎の間隔で処理されます。たとえば、10:15:45 AM にレポートを生成した場合、レポートの内容は9:15から10:15 AM のデータになります。
過去 24 時間の場合、1 時間毎に処理されます。たとえば、10:15 AM にレポートを生成した場合、レポートの内容はその日の 10:00 AM から 24 時間前まで選った 24 時間分のデータになります。

- 帯域幅の使用量 - 円グラフに、指定期間（過去 1 時間/過去 24 時間）で最も帯域を消費したトップ 10 のアプリケーション/ユーザが表示されます。[アプリケーション]または[ユーザ]リンクをクリックして統計を切り替えます。ユーザ情報を確認するには、ユーザ認識ブレードを有効にする必要があります。

- 帯域消費の上位ランク - 帯域消費の上位アプリケーション、カテゴリ、サイト、ユーザのバーセンテージとトラフィック量（MB/GB）の統計が表示されます。

- トラフィック - デフォルトでは、領域グラフで受信および送信したトラフィックの合計量が表示されます。時間軸は、ネットワーク・セクションで選択した期間（過去 1 時間または過去 1 日）を反映します。過去 1 時間の場合グラフには 5 分間隔で表示され、過去 24 時間の場合は 1 時間間隔で表示されます。受信と送信の各リンクをクリックして、受信または送信のトラフィック量だけを確認できます。グラフのオレンジ色の領域は送信トラフィックを表わします。青色の領域は送信トラフィックを表わします。

- 日付と時刻 - 送信または受信トラフィック
- 時間間隔の合計トラフィック

- 合計トラフィック統計 - 領域グラフの隣に過去 1 時間または過去 1 日の合計トラフィックの統計を確認できます。

セキュリティ

- 感染ホスト - 以下の数が表示されます。
  - 感染ホスト
  - 感染サーバ
  - 最近アクティブな感染ホスト
  [すべての感染ホスト]をクリックして、[ログ&モニタリング]→[感染ホスト]ページを開くことができます。

- [高リスク・アプリケーション] - 以下が表示されます。
  - 高リスク・アプリケーションの数
  - 使用頻度が最も高い高リスク・アプリケーション
  - 高リスク・アプリケーションを使用する上位ユーザ
  [アプリケーション・フレード・コントロール]をクリックして、[アクセス・ポリシー]→[ファイアウォール・フレード・コントロール]ページでアプリケーションと URL フィルタリングの設定を確認できます。

- セキュリティ・イベント - 以下の数が表示されます。
  - セキュリティ・ゲートウェイで検出されたアンチボット・マルウェア
  - セキュリティ・ゲートウェイで検出されたアンチウィルスマルウェア
アプライアンスの設定

- IPS の数

リンクをクリックして[脅威対策]→[プレード・コントロール]ページを開くことができます。

トラブルシューティング

- システムのリソース - [CPU、メモリ、ディスク使用量]をクリックして CPU、メモリ、ディスク使用量の情報を確認します。
- デバイス情報 - セキュリティ・ゲートウェイ情報が表示されます。
- モニタリングおよびトラブルシューティングに役立つページへのリンク

注 - このページには、[ホーム]および[ログ&モニタリング]タブからアクセスできます。

レポートの表示

[レポート]ページには、ネットワーク分析、セキュリティ分析、感染ホスト・レポートが指定した期間（毎月、毎週、毎日、毎時間）ごとに表示されます。

レポートには、表示される時間に関係する重要な 2 つの要素があります。

- 時間の丸め処理
- システムの再起動

時間の丸め処理

生成レポートに表示される時間は丸め処理されます。

- レポート（每時）の場合 - 1 分毎の間隔で処理されます。たとえば、10:15:45 AM にレポートを生成した場合、レポートの内容は 9:15 から 10:15 AM のデータになります。
- レポート（毎日）の場合 - 1 時間毎の間隔で処理されます。たとえば、10:15 AM にレポートを生成した場合は、レポートの内容はその日の 10:00 AM から 24 時間前まで遡った 24 時間分のデータになります。
- レポート（毎週）の場合 - 2 時間毎の間隔で、00:00、02:00、04:00、06:00 といった偶数間隔で処理されます。たとえば、9:55 AM にレポートを生成した場合、レポートの内容はその日の 8:00 AM から 1 週間遡った 1 週間分のデータになります。
- レポート（毎月）の場合 - 4 時間毎の間隔で、00:00、04:00、08:00、12:00 といった偶数間隔で処理されます。たとえば、11:15 AM にレポートを生成した場合、レポートの内容はその日の 8:00 AM から 1 か月間遡った 1 か月分のデータになります。

システムの再起動

アプライアンスの起動後（インストール後/アップデート後）最初の 24 時間は、次回のレポート生成までの時間にあたる 1 分間の間隔がシステムで追加されます。

たとえば、対の時間間隔でレポート（毎週）を生成する場合、アプライアンスでは追加の 2 時間と、更に最初の対時間のデルタ（差分）が必要になります。

- 00:00 AM に起動したアプライアンスの場合 - 最初のレポート（毎週）は 04:00 AM に生成されます。合計の 4 時間は、最初の対時間のデルタ時間である 02:00 に、追加の 2 時間を足した時間です。待ち時間は 4 時間です。
- 01:59 AM に起動したアプライアンスの場合 - 最初のレポート（毎週）は 04:00 AM に生成されます。合計の 2 時間は、最初の対時間のデルタ時間である 02:00 に、追加の 2 時間を足した時間です。待ち時間は 2 時間です。
・レポート（毎時間）- 起動した後の 2-3 分後。
・レポート（毎日）- 起動した後の 1-2 時間後。
・レポート（毎週）- 起動した後の 2-4 時間後。
・レポート（毎月）- 起動した後の 4-8 時間後。

注 - 各レポート・タイプで生成したうちの最新レポートのみがアプライアンスに保存されます。新しくレポートを生成すると、最後に保存された該当するタイプのレポートを上書きします。

レポートを生成するには
ページの上部にある該当する期間のリンクをクリックします（「毎月」「毎週」「毎日」「毎時」）。
リンクの下の行には、選択したレポートとその時間間隔が表示されます。表示データを更新するには、「生成」をクリックします。
レポートには以下のセクションがあります。
・サマリ
・目次
・レポート・ページ

サマリ
レポートの最初のページにはサマリと以下が表示されます。
・セキュリティ・ゲートウェイで検出されたアンチボットとアンチウイルスのマルウェア数とIPS攻撃の数。
・カテゴリ、サイト、ユーザ別の帯域幅上位使用率の統計。上位ランク・カテゴリ、上位ランク・サイト、上位ランク・ユーザの各リンクをクリックして該当するレポートのページを表示できます。上位5つのアプリケーション（円グラフ）と、受信および送信トラフィックの合計のアプリケーション別の帯域消費統計も表示されます。
・感染ホスト、サーバ、最近アクティブな感染ホストの数。
・高リスク・アプリケーションの数、使用頻度が最も多い高リスク・アプリケーション、高リスク・アプリケーションを使用する上位ユーザ。
・セキュリティ・ゲートウェイ名、バージョン、MACアドレス。

目次
目次には、ネットワーク分析、セキュリティ分析、感染ホストの各レポートへのリンクがあります。リンクをクリックすると、選択したセクションへ直接移動できます。

レポート・ページ
各レポート・ページには、詳細グラフと表、説明があります。

注 - このページには、「ホーム」および「ログ&モニタリング」タブからアクセスできます。

システム・ツールの使用
「システム・ツールの使用」（28ページ）を参照してください。
**SNMP**

[ログ&モニタリング]→[SNMP]ページで、このゲートウェイのSNMPを設定できます。

以下の操作を行うことができます。

- SNMPエージェントのオン/オフの切り替え
- SNMPの設定（システムの場所、連絡先、SNMP v1とv2認証のコミュニティ文字列）
- SNMP v3ユーザの追加
- SNMPトラップ・レシーバの各種設定
- トラップ・レシーバに送られたSNMPトラップの有効化/無効化

**SNMPのオン/オフを切り替えるには**

1. SNMPのオン/オフのスライダを[オン]または[オフ]の位置に移動し、
2. [適用]をクリックします。

SNMPの各設定（ユーザ、トラップ、トラップ・レシーバ）を行うには、事前にSNMPをオンにしておく必要があります。

**SNMPを設定するには**

[設定]をクリックします。

[SNMP基本設定]ウィンドウが開きます。SNMPトラップを有効にする、システムの場所や連絡先の詳細を設定する、v3以外のSNMPバージョンを有効にするなどを実行できます。

**SNMPv3ユーザ**

- 新しいSNMPv3ユーザを追加するには、[新規]をクリックします。
- 既存のSNMPv3ユーザを編集するには、リストからユーザを選択して[編集]をクリックします。
- SNMPv3ユーザを削除するには、リストからユーザを選択して[削除]をクリックします。

**SNMPトラップ・レシーバ**

SNMPトラップ・レシーバのプロパティを追加、削除、編集できます。

- SNMPトラップ・レシーバを追加するには、[新規]をクリックします。
  
  注：SNMPv3のトラップ・レシーバを新しく追加するには、事前にSNMPv3ユーザを定義しておく必要があります。
- 既存のSNMP トラップ・レシーバを編集するには、リストからユーザを選択して[編集]をクリックします。
- 既存のSNMP トラップ・レシーバを削除するには、リストからユーザを選択して[削除]をクリックします。

**SNMPトラップ**

特定のトラップをリストから選択して有効または無効にしたり、一部のトラップにしきい値を設定することができます。有効になったトラップは受信者に送られます。

**SNMPトラップを編集するには**

1. リストからトラップを選択し、[編集]をクリックします。
2. トラップを有効にするオプションをオンにしてトラップを有効にする、またはオフにしてトラップを無効にします。
3. トラップに値が含まれている場合、必要に応じてしきい値を編集できます。
4. [適用]をクリックします。
詳細設定

このセクションの内容

USBドライブによるアップグレード .................................................. 159
ブート・ローダ ........................................................................ 160
ブート・ローダによるアップグレード .............................................. 160
工場出荷時のデフォルト設定への復元 ........................................... 162
前面パネル .............................................................................. 164
背面パネル .............................................................................. 166

USBドライブによるアップグレード

このセクションでは、アプライアンスへのコンソール接続を行わずにUSBドライブでアプライアンスをアップグレードする方法について説明します。詳細は、「ブート・ローダによるアップグレード」(160ページ)を参照してください。

注 - USBドライブはFAT32でフォーマットする必要があります。

USBドライブから新しいファームウェア・イメージをインストールする

Check Pointから、新しいファームウェア・イメージがリリースされることがあります。このイメージ・ファイルとUSBドライブを使用することで、アプライアンスに再書き込みできます。WebUIを使用してアップグレードすることも可能です。この場合、新しいイメージによってサポートされる場合に限り、以前の設定は維持されます。USBドライブを使って新しいイメージを再書き込みすると、アプライアンスにより以前の設定は削除され、そのアプライアンスに適切な新しい工場出荷時のイメージが作成されます。

USBドライブから新しいファームウェア・イメージをインストールには

1. Check Point 730/750 Applianceを電源から切り離します。
2. USBドライブのファームウェア・イメージ・ファイルを最上位フォルダに置きます。ファームウェア・イメージ・ファイルは名前によって認識されるため、名前を変更しないでください。
3. USBドライブの最上位フォルダに以前のブート・ローダ又はファームウェア・イメージ（u-boot*.binファイルまたはfw1*.imgファイル）が含まれていないことを確認します。
4. USBドライブをCheck Point 730/750 ApplianceのUSBポートに接続します。
5. アプライアンスを電源に接続します。数秒後、システムがブートするまで、通知LEDが点滅します。システムが始動すると、USB LEDが点灯します。システムのブートが完了すると、USB上のイメージのバージョンの確認が行われます。

ファイルが有効であれば、ファイルがアップロードされるまで、LAN LEDが点滅を開始します。数秒後、すべてのLAN LEDが点滅し、システムが再起動します。通知LEDランプが消えたら、インストールが完了し、アプライアンスはユーザーの出力を待機します。
6. USBドライブを抜きます。
7. この操作により以前の設定は削除されるため、「Check Point 730/750 Appliance 導入の手引き」を参照して初期設定ウィザードからアプライアンスを再設定してください。
注 - USBドライブを使用してアップグレードを行う場合は、この方法でアプライアンスに再書き込みしたときに保存されたアプライアンスの工場出荷時のデフォルト・イメージを置き換える必要があります。詳細については、「アップグレード」を参照してください。

**ブート・ローダ**

ブート中にGaia組込のブート・メニューが表示されます。コンソール接続がある場合は、アプライアンスのブート中にCtrl+Cを押すことにより、このメニューを使用できます。このメニューには以下のオプションが含まれています。

1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Restart Boot-Loader
7. Run Hardware diagnostics
8. Upload preset configuration file

Please enter your selection:

ブート・ローダに入るとすべてのインタフェースはダウンし、接続を要求するオプションについてのみインタフェースを有効にできます。この時点では、チェック・ポイントのサービスは有効ではありません。

オプション1〜3でアプライアンスが起動します。

・ 標準モードはアプライアンスのデフォルトのブート・モードです。
・ デバッグ・モード・ブートでは、ブート中に初期化されたプロセスのプリントアウトが提供されます。
・ メンテナンス・モードでマシンをブートすると、ファイル・システムへのアクセスのみが提供されます（ネットワーク・インタフェース、Check Pointプロセスおよびアプライアンスのサービスはダウンします）。

注 - 標準/デバッグ・ブート中にエラーが発生しアプライアンスが適切にブートできない場合は、メンテナンス・モードに戻り、電源LEDが赤色に点灯します。

オプション4〜5については、後のセクションで解説します。

オプション6はアプライアンスを再起動します。

オプション8ではプリセット設定ファイルをアップロードします。

**ブート・ローダによるアップグレード**

U-boot（ブート・ローダ）を使用してCheck Point 730/750 Applianceをアップグレードするには

1. アプライアンスをコンソール接続（アプライアンスのバック・パネルのシリアル・コンソール接続を使用）に接続してアプライアンスをブートし、Ctrl+Cを押します。Gaiaの組込ブート・メニューが表示されます。
2. 5を押して[ネットワークからイメージ/ブート・ローダをインストール/更新]を選択します。
3. TFTPサーバから手動でイメージをロードするか、またはbootpサーバによる自動モードを使用するかの確認メッセージが表示されます。
4. 手動モードを選択した場合は、Check Point 730/750 Appliance の IP、TFTP の IP、およびイメージ名を入力するよう求められます。

5. 自動モードを選択した場合は、bootp サーバを検索する手続きが自動的に開始されます。

6. メニュー・モードで Ctrl+C をもう一度押すとブート・ローダ・メニューに戻ります。
   アップグレード中は、すべての LAN リンク LED およびアクティビティ LED がオレンジ色と緑色に交互に点滅して処理中であることが表されます。この処理には最大で 1 分かかります。
   すべての LAN リンクおよびアクティビティが正常に完了すると、LED が緑色に点灯し、アプライアンスはユーザがいずれかのキーを押すのを待ちます。アップグレード中にエラーが発生すると、すべての LAN リンク LED およびアクティビティ LED が赤色に点滅します。
工場出荷時のデフォルト設定への復元

Check Point 730/750 Appliance には、工場出荷時のデフォルト設定イメージが含まれています。
初めてアプライアンスの電源をオンにすると、このデフォルトのイメージが読み込まれます。
トラブルシューティングの目的など、必要なときに Check Point 730/750 Appliance を工場出荷時の設定に戻すことができます。
工場出荷時のデフォルトイメージに戻す操作は、WebUI やブート・ローダを使う、または背面パネルのボタンを押して実行できます。

重要 - 工場出荷時の設定に復元すると、アプライアンス上のすべての情報が削除されます。また、初期設定ウィザードを再度実行する必要があります。

WebUI から工場出荷時のデフォルト設定に復元するには
1. Check Point 730/750 Appliance の WebUI で、[デバイス]→[システム操作]をクリックします。 [システム操作] が開きます。
2. [Appliance（アプライアンス）] セクションの [工場出荷時のデフォルト] をクリックします。
3. 表示されたポップアップ・ウィンドウで、[OK] をクリックします。
4. 工場出荷時の設定への復元が開始すると、すべての LAN リンクとアクティビティ LED がオレンジと緑に交互に点滅して進行中であることがわかります。
   これには数分かかり、完了するとアプライアンスが自動的に再起動します。

背面パネルのボタンで工場出荷時のデフォルト設定に復元するには
1. ピンなどで工場出荷時の設定への復元ボタンを 12 秒以上押し続けます。
2. 電源 LED と通知 LED が赤色になったら、ボタンを離します。アプライアンスが自動的に再起動し、工場出荷時のデフォルト設定に復元されます。
3. 工場出荷時の設定への復元が開始すると、すべての LAN リンクとアクティビティ LED がオレンジと緑に交互に点滅して進行中であることがわかります。
   これには数分かかり、完了するとアプライアンスが自動的に再起動します。

U-boot（ブート・ローダ）を使って工場出荷時のデフォルト設定に復元するには
1. コンソール接続でアプライアンスを接続します（アプライアンスの背面パネルにあるシリアル・コンソール接続）。
2. アプライアンスを起動して Ctrl+C を押します。
   Gaia に備えられているブート・メニューが表示されます。
   Welcome to Gaia Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Restart Boot-Loader
   7. Run Hardware diagnostics
   8. Upload preset configuration file
Please enter your selection:

3. 4 を入力して[Restore to Factory Defaults (local)]を選択します。

4. プロンプトが表示されたときは、"Are you sure? (y/n)"というプロンプトが表示されたら、y を選びます。プロセスが続行し、アプライアンスが工場出荷時のデフォルト・イメージに復元されます。
   工場出荷時の設定への復元が開始すると、すべての LAN リンクとアクティビティ LED がオレンジと緑に交互に点滅して進行中であることがわかります。これには数分かかり、完了するとアプライアンスが自動的に起動します。

デフォルトへのリセットを無効にするには
次の CLI コマンドを使用します。
> set additional-hw-settings reset-timeout 0

デフォルトへのリセットを有効にするには
次の CLI コマンドを使用します。
> set additional-hw-settings reset-timeout 12
## 前面パネル

### 有線モデル

<table>
<thead>
<tr>
<th>番号</th>
<th>番号</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>アラート LED</td>
<td>• 起動時は緑色に点滅&lt;br&gt;• メモリ不足などのリソース問題が発生している場合は赤色</td>
</tr>
<tr>
<td>2</td>
<td>インターネット LED</td>
<td>• インターネットに接続している場合は緑色&lt;br&gt;• インターネット接続が設定されているが接続できない場合は赤色に点滅</td>
</tr>
<tr>
<td>3</td>
<td>SD LED</td>
<td>SDカードが挿入されている場合は緑色</td>
</tr>
<tr>
<td>4</td>
<td>USB LED</td>
<td>USBデバイスが接続されている場合は緑色</td>
</tr>
<tr>
<td>5</td>
<td>LAN1 - LAN6、DMZ、WAN LED</td>
<td>速度のインジケータ&lt;br&gt;• ポート速度が1000 Mbpsの場合はオレンジ色&lt;br&gt;• ポート速度が100 Mbpsの場合は緑色&lt;br&gt;• ポート速度が10 Mbpsの場合は点灯しない&lt;br&gt;アクティビティのインジケータ&lt;br&gt;• リンクが確立していない場合は点灯しない&lt;br&gt;• リンクが確立していてもトラフィックがない場合は緑色&lt;br&gt;• トラフィックがある場合は緑色に点滅</td>
</tr>
</tbody>
</table>

### WiFi モデル
<table>
<thead>
<tr>
<th>番号</th>
<th>番号</th>
<th>説明</th>
</tr>
</thead>
</table>
| 6    | 電源 LED | • アプライアンスがオンの場合は緑色に点灯  
      |        | • ブート・エラーが発生した場合、またはアプライアンスがメンテナンス・モードの場合は赤色 |
| 7    | USB ポート | 以下の用途の USB ポート:                           
      |        | • セルラー/アナログ・モデム  
      |        | • 新しいファームウェアのアプライアンス再インストール  
      |        | • 初期設定スクリプトの実行 |
| 8    | WiFi LED | （WiFi モデルのみ）                              
      |        | • WiFi アクティビティがある場合は緑色に点滅  
      |        | • WiFi アクティビティがない場合は緑色 |
# 背面パネル

## 有線モデル

<table>
<thead>
<tr>
<th>番号</th>
<th>番号</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>接地（アース）機能接地</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>DMZとWANポートビルトインのイーサネット・ポート</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>コンソール・ポートデフォルトでRJ45またはMini USBシリアル接続は115200 bpsに設定されています。このポートをアナログ・モデム接続に使うことも可能です。注：RJ45とMini USBの両方のケーブルが接続されている場合、Mini USBが優先されます。</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>再起動ボタンアプリアンスを再起動します。ボタンは誤って押すことがないように簡単に押せない構造になっています。ボタンを押すとアプリアンスが再起動します。</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>PWR+DC12V電源ユニット・ケーブルの接続用注：電源ユニット・ケーブルは、アプリアンスに確実にねじ留める必要があります。</td>
</tr>
</tbody>
</table>

## WiFiモデル

<table>
<thead>
<tr>
<th>番号</th>
<th>番号</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>接地（アース）機能接地</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>DMZとWANポートビルトインのイーサネット・ポート</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>コンソール・ポートデフォルトでRJ45またはMini USBシリアル接続は115200 bpsに設定されています。このポートをアナログ・モデム接続に使うことも可能です。注：RJ45とMini USBの両方のケーブルが接続されている場合、Mini USBが優先されます。</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>再起動ボタンアプリアンスを再起動します。ボタンは誤って押すことがないように簡単に押せない構造になっています。ボタンを押すとアプリアンスが再起動します。</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>PWR+DC12V電源ユニット・ケーブルの接続用注：電源ユニット・ケーブルは、アプリアンスに確実にねじ留める必要があります。</td>
</tr>
<tr>
<td>番号</td>
<td>番号</td>
<td>説明</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>6</td>
<td>工場出荷時の設定への復元ボタン</td>
<td>アプライアンスを工場出荷時の設定に復元します。ボタンは誤って押すことができないように簡単に押せない構造になっています。工場出荷時のデフォルト設定への復元（162ページ）を参照してください。</td>
</tr>
<tr>
<td>7</td>
<td>LAN1 - LAN6 ポート</td>
<td>ビルトインのイーサネット・ポート</td>
</tr>
<tr>
<td>8</td>
<td>ANT1、ANT2、ANT3</td>
<td>ワイヤレス・ネットワーク・アンテナ用ポート（WiFiモデルのみ）</td>
</tr>
</tbody>
</table>