Cisco Secure Firewall 移行ツールの FAQ

Cisco Secure Firewall 移行ツールのよく寄せられる質問

Q. リリース 3.0.1 の Cisco Secure Firewall 移行ツールでサポートされる新機能は何ですか。

A. Cisco Secure Firewall 移行ツール 3.0.1 では、Cisco Secure Firewall 3100 シリーズを Check Point からの移行先デバイスとしてのみサポートするようになりました。

Q. リリース 3.0 の Cisco Secure Firewall 移行ツールでサポートされる新機能は何ですか。

A. クラウド提供型 Firewall Management Center への移行。

Q. リリース 2.5.2 の Cisco Secure Firewall 移行ツールでサポートされる新機能は何ですか。

A. Check Point の ACL 最適化。

Q. Check Point から Threat Defense への変換におけるハードウェア制限は何ですか。

A. 構成ファイルが Check Point Web Visualization Tool および FMT-CP-Config-Extractor_v4.0.1-8248 ツールと互換性がある場合は、送信元 Check Point を移行できます。

Q. Check Point r76SP からエクスポートされた構成を使用して、それを 4100 および 6100 Firepower プラットフォームに移行できますか。

A. はい。r75 ～ r77.30 は、すべてのプラットフォームでサポートされます。

プラットフォームは、Check Point Web Visualization Tool が利用可能であればサポートされます。

Q. Check Point 上のルールで否定されたオブジェクトを処理する方法を教えてください。

A. オブジェクトが除外タイプのオブジェクト/グループである場合、ACL 変換は「許可」と「ブロック」の組み合わせに従います。この変換は ACL でサポートされていますが、除外タイプのネットワークオブジェクト/グループはサポートされていません。たとえば、Check Point ACE ルールが、参照される除外タイプのオブジェクトグループを持つ場合です。

- Check Point ルールアクションが「許可」の場合は、次のようになります。

- ACE には、**<exception></exception>** XML タグで参照されている Object-Group を「拒否」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。
- ACE には、*<base></base>* XML タグで参照されている Object-Group を「許可」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。

- Check Point ルールアクションが「拒否/リセット」の場合は、次のようになります。
  - ACE には、**<exception></exception>** XML タグで参照されている Object-Group を「許可」するアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。
  - ACE には、**<base></base>** XML タグで参照されている Object-Group についての「リセット（拒否）」をともなう「ブロック（拒否）/ブロック」のアクションが必要です。ルールに「Rule for Exception Object-Group」コメントを追加してください。

Q. Cisco Secure Firewall 移行ツールは、否定セルをともなう ACE をサポートしていますか。サポートしていない場合、それらのルールは Cisco Secure Firewall 移行ツールによってどのように処理されますか。

A. 否定セルをともなう ACE は、Cisco Secure Firewall 移行ツールでサポートされておらず、その ACE を通常の ACE として扱うことによって変換されます。これらの問題は今後のリリースで解決される予定です。

Q. 「Failed to bind to the DB. Access denied error.」というメッセージが表示されます。どうすればいいですか。

A. 次の手順を実行します。

- Check Point Gaia Console for Management Server を開きます。
- Gaia Console 上のユーザーおよびロールの設定に移動します。
- 管理者ロールを持つ Check Point Management Server Gaia Console で、ホームディレクトリの `/home` パラメータとシェルの `/etc/cli.sh` パラメータを使用して、新しいユーザー名ログイン情報を作成します。

Q. Cisco Secure Firewall 移行ツールを使用して Check Point 構成を解析すると、解析カウントが 0 と表示されます。どうすればいいですか。

A. 次のいずれかの手順を実行します。

FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用して *networking.txt* ファイルを取得します。手動で作成した *networking.txt* ファイルは使用しないでください。

または

何らかの理由で、*networking.txt* ファイルの出力がエクスポートされた Check Point Security Gateway でロギングが有効になっている可能性があります。ロギングが有効になっている

ために *networking.txt* ファイルに無関係な情報が追加されており、そのような問題が発生しています。その場合は、次の手順を実行します。

- *networking.txt* ファイルを確認します。
- 追加された余分なログ行を削除してファイルを修正します。
- 新しい zip を Cisco Secure Firewall 移行ツールにアップロードします。

Q. VSX を使用して Check Point から構成を移行できますか。

A. 仮想システムに関連する特定のポリシーパッケージをエクスポートできます（一度に 1 つの仮想システム）。たとえば、Web Visualization Tool（r75 ～ r77.30）を使用して構成をエクスポートすると、すべての仮想システムのポリシー要素がエクスポートされます。そのため、*index.xml*、*communities.xml*、*network_objects.xml*、および *networking.txt*（移行されるポリシーの Security Gateway から）とともに移行する仮想システムの NAT ファイルとポリシーファイルのみを保持して、それを完全な構成にします。

r80 の場合、Check Point ポリシーパッケージを選択して構成を取得する際、手順 5 で、移行する Live Connect を介して Check Point Security Manager に接続するときに、特定の仮想システムのポリシーパッケージを選択します。

Check Point Security Gateway にも接続する場合は、Check Point ポリシー パッケージに対応する適切な Check Point Virtual System Check Point Firewall Package の正しい詳細情報を提供してください。

それでも問題が解決しない場合は、Cisco TAC に連絡して、これらの障害の TAC ケースを作成してください。

Q. Check Point（r80）構成を手動で取得できますか。

A. いいえ。Check Point（r80）構成を手動で取得することはできません。完全な r80 構成を取得するには、Cisco Secure Firewall 移行ツールで Live Connect を使用します。手動の回避策を使用するか Cisco Secure Firewall 移行ツールで構成されていない Check Point（r80）構成を使用して構成を抽出すると、構成が不完全になるだけでなく、サポートされていないものとして移行されるか、部分的に移行されるか、場合によっては移行が失敗します。

詳細については、「r80 の Check Point 構成ファイルのエクスポート」を参照してください。

Q. さまざまな Check Point（r80）展開タイプのログイン情報を事前設定する方法を教えてください。

A. 次のいずれかの方法により、移行前に Check Point（r80）デバイスでログイン情報を構成できます。

- 分散 Check Point 展開からのエクスポート
- スタンドアロン Check Point 展開からのエクスポート

- マルチドメイン展開の Check Point（r80）のエクスポート

Q. Check Point Security Manager 用に Check Point r80 でカスタム API ポートを使用しています。構成を完全に取得する方法を教えてください。

A. Check Point API を使用するために Check Point Smart Manager でカスタム API ポートを使用している場合は、次の手順を実行します。

- [Check Point Security Manager] ページの [Check Point マルチドメイン展開（Check Point Multi-domain Deployment）] チェックボックスをオンにします。
- マルチドメイン展開を使用している場合は、Check Point CMA のIP アドレスと API ポートの詳細を追加します。
- 一般的な展開の Check Point Security Manager の場合、Check Point Security Manager の IP アドレスを保持し、カスタム API ポートの詳細を入力します。

Q. バージョン r80.40 の Check Point Gateway を使用しており、Live Connect を介した取得は問題なく実行できます。ただし、解析時に「Blocked VSX Feature is UNSUPPORTED in FTD」というエラーが表示されます。どうすればいいですか。

A. このエラーは、Check Point r80.40 以降で **fw vsx stat** コマンドが廃止されたために発生します。*networking.txt* ファイルを解析するときに **fw vsx stat** コマンドを実行すると、Cisco Secure Firewall 移行ツールは値を解析できません。

回避策として、次の手順を実行します。

1. *config.zip* ファイルを解凍します。
2. *networking.txt* ファイルを開きます。

   次に、出力例を示します。

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   これを次のように手動で置き換えます。

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. すべてのファイルを選択し、.zip 拡張子に圧縮します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。