ネットワーク運用の保護

ネットワーク運用の保護は重要なトピックです。このドキュメントのほとんどは、FXOS を実行する Firepower 4100/9300 デバイスの安全な設定に焦点を当てていますが、設定だけではネットワークを完全に保護することはできません。ネットワークで使用されている操作手順、およびネットワークを管理する人は、基礎となるデバイスの設定と同じくらいセキュリティに貢献します。

次のセクションには、FXOS 管理者が実施することをお勧めする運用上の推奨事項が含まれています。これらのセクションは、ネットワーク運用の特定の重要な領域を強調しており、包括的なものではありません。

- Cisco セキュリティアドバイザリの監視 （1 ページ）
- FXOS の最新バージョンへの更新 （2 ページ）
- ログイン前バナーのカスタマイズ （2 ページ）
- コモンクライテリアまたは FIPS モードの有効化 （2 ページ）
- ネットワーク タイム プロトコル（NTP）の保護 （3 ページ）
- ドメイン ネーム システム（DNS）の保護 （3 ページ）
- 認証、認可、アカウンティングの活用 （4 ページ）
- セキュアなプロトコルの使用 （4 ページ）
- 構成管理 （4 ページ）

Cisco セキュリティアドバイザリの監視

Cisco Product Security Incident Response Team（PSIRT）は、シスコ製品のセキュリティ関連問題に関して、シスコ セキュリティ アドバイザリと呼ばれる通知を作成し、維持しています。セキュリティアドバイザリは、http://www.cisco.com/go/psirt で入手できます。

Cisco PSIRT 脆弱性レポートについては、「Cisco Security Vulnerability Policy 」を参照してください。

安全なシステムを維持するために、Cisco FXOS 管理者は、シスコ セキュリティ アドバイザリで伝達される情報に注意する必要があります。脆弱性がネットワークにもたらす可能性のある脅威を評価する前に、脆弱性に関する詳細な知識が必要です。この評価プロセスのサポートについては、「Risk Triage for Security Vulnerability Announcements」を参照してください。

FXOS の最新バージョンへの更新

重要なセキュリティの更新は、FXOS の新しいプラットフォーム バンドル リリースごとに含まれています。できるだけ早くFXOSシステムを利用可能な最新バージョンに更新することをお勧めします。

さまざまな構成でのFXOSのサポートされている互換性とアップグレードパスの詳細については、Cisco.com の『*Cisco Firepower 4100/9300 FXOS Compatibility*』ガイドおよび『*Cisco Firepower 4100/9300 Upgrade Guide*』を参照してください。

ログイン前バナーのカスタマイズ

ユーザーが Firepower Chassis Manager または FXOS CLI にログインする前に、FXOS がユーザーに表示するメッセージを指定できます。強化の観点から、このメッセージは不正アクセスを防止するために使用する必要があります。

次の CLI の例では、FXOS Chassis Manager および FXOS CLI のログイン前バナーを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
 You must have explicit, authorized permission to access or configure this device.
 Unauthorized attempts and actions to access or use this system may result in civil
and/or
criminal penalties.
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

コモンクライテリアまたは FIPS モードの有効化

組織が、米国国防総省や他の政府/自治体認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合、コモンクライテリアまたはFIPSモードを有効化して、1 つの設定で複数の強化変更を適用することができます。組織がセキュリティ認定コンプライアンス標準に準拠する必要がない場合でも、FXOS の FIPS またはコモンクライテリアモードを有効にすることができますが、これによりデバイスで互換性の問題が発生する可能性があることに注意してください。

コモンクライテリアまたは FIPS モードを有効にするオプションは、Firepower Chassis Manager Web インターフェイスの **[プラットフォーム設定（Platform Settings）]** > **[FIPS/コモンクライテリア（FIPS/Common Criteria）]**モードの下に表示されます。

（注）

- セキュリティ認定準拠を有効にしても、選択したセキュリティモードのすべての要件への厳密な準拠が保証されるわけではありません。このドキュメントでは、コモンクライテリアまたは FIPS モードで提供されるものを超えて展開を強化するために推奨されるその他の設定について説明します。完全準拠に必要な強化手順の詳細については、認定機関から提供される本製品に関するガイドラインを参照してください。
- FIPS、コモンクライテリア、またはその両方が有効になっている場合は、デバイスアクセスに FIPS 準拠ツールを使用します。

ネットワーク タイム プロトコル（NTP）の保護

信頼された Network Time Protocol（NTP）サーバーを使用して、Firepower 4100/9300 FXOS デバイスとその関連サーバーのシステム時刻を同期させることを強く推奨します。

FXOS の NTP を有効にするには、最初に NTP キー ID とキー値を生成してから、FXOS Chassis Manager で次のワークフローを使用して NTP サーバーを FXOS シャーシに追加する必要があります。**Platform Settings > Set Time Source > Use NTP Server**。NTP をさらに強化するには、NTP サーバー認証を構成します。

FXOS の NTP サーバーおよび NTP サーバー認証を設定する方法の詳細については、『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「Platform Settings」の章の「Setting the Date and Time Using NTP」トピックを参照してください。

（注）

- 有効にすると、NTP認証機能はFXOSに関連付けられた設定済みのすべてのサーバーでグローバルに機能します。
- NTP サーバー認証では SHA1 のみがサポートされます。
- サーバを認証するには、キー ID とキー値が必要です。キー ID は、メッセージ ダイジェストのコンピューティング時に、使用するキー値をクライアントとサーバーの両方に指示するために使用されます。キー値は、nip-keygen を使用して導出される固定値です。

ドメイン ネーム システム（DNS）の保護

ネットワーク環境で相互に通信しているコンピュータは、DNS プロトコルを利用して、IP アドレスとホスト名の間のマッピングを提供します。

DNS は、セキュリティを考慮して設定されていない DNS サーバーの弱点を利用するようにカスタマイズされた、特定のタイプの攻撃の影響を受ける可能性があります。業界で推奨されているセキュリティのベストプラクティスに従って、ローカル DNS サーバーを設定してくださ

い。シスコでは次のドキュメントでガイドラインを提供しています。https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html。

認証、認可、アカウンティングの活用

認証、認可、アカウンティング（AAA）フレームワークは、ネットワークデバイスへのインタラクティブアクセスを保護するのに重要です。AAA フレームワークは、ネットワークのニーズに基づいて調整できる高度に設定可能な環境を提供します。

RADIUS と TACACS+ は両方とも FXOS システムでサポートされています。TACACS+ は、ユーザー名とパスワードの両方を含む TCP ペイロード全体を暗号化します。RADIUS はパスワードのみを暗号化します。さらに、TACACS+ はコマンド認可を提供しますが、RADIUS は認証とアカウンティングのみを提供します。したがって、認証セキュリティを最大化するために TACACS+ を使用することをお勧めします。

さらに、ユーザー認証に LDAP を使用できます。LDAP 認証交換を暗号化するには、CLI オプションを使用して SSL を使用します。

```
Firepower /security/ldap/server # set ssl yes
```

AAA の設定方法の詳細と完全な手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configuring AAA」セクションを参照してください。

セキュアなプロトコルの使用

Cisco FXOS は、機密性の高いネットワーク管理データを伝送するために多くのプロトコルを使用します。可能な限り、安全なプロトコルを使用する必要があります。安全なプロトコルの選択には、認証データと管理情報の両方が暗号化されるように、Telnet の代わりに SSH を使用することが含まれます。さらに、構成データをコピーするときは、安全なファイル転送プロトコルを使用する必要があります。たとえば、FTP または TFTP の代わりに Secure Copy Protocol（SCP）を使用します。安全なプロトコルの使用方法の詳細については、このドキュメントの「管理プレーン」セクションを参照してください。

構成管理

構成管理は、構成の変更が提案、レビュー、承認、および展開されるプロセスです。

Cisco FXOS デバイスの設定には、ユーザー名、パスワード、アクセスコントロールリスト（ACL）の内容など、機密性の高い多くの詳細が含まれています。Cisco FXOS デバイス設定のアーカイブに使用されるリポジトリは保護する必要があり、アクセスはアクセスを必要とするロールと機能のみに制限する必要があります。この情報への安全でないアクセスは、ネットワーク全体のセキュリティを損なう可能性があります。

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。