CHAPTER 5

SNMP の設定

この章では、Cisco Virtual Security Gateway（VSG）に簡易ネットワーク管理プロトコル（SNMP）を設定する例について説明します。

この章の内容は、次のとおりです。

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション層プロトコルです。SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。ここでは、次の内容について説明します。

SNMP の機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- SNMP エージェント：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。仮想ファイア ウォールはエージェントと MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。

- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。
- SNMP は、RFC 3411 ～ 3418 で規定されています。

（注）　SNMP Role Based Access Control（RBAC）はサポートされていません。

SNMPv1、SNMPv2c、および SNMPv3 です。SNMPv1 および SNMPv2c の両方により、コミュニティ ベースのセキュリティ形式の使用がサポートされています。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知によって、不正なユーザ認証、再起動、接続の終了、隣接ルータとの接続切断、またはその他の重要イベントを示すことができます。

SNMP 通知は、トラップまたは応答要求として生成されます。トラップは、エージェントからホスト レシーバ テーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment（ACK; 確認応答）を送信しないからです。仮想ファイアウォールではトラップが受信されたかどうかを判別することはできません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージの受信を確認します。仮想ファイアウォールが応答を受信しない場合、インフォーム要求を再度送信できます。仮想ファイアウォールを複数のホスト レシーバに通知を送信するように設定できます。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

この項は、次の内容で構成されています。

「SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル」（P.5-3）
「User-Based Security Model」（P.5-3）
「コマンドライン インターフェイス（CLI）および SNMP ユーザの同期」（P.5-4）
「グループベースの SNMP アクセス」（P.5-4）

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。

セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル
- authPriv：認証と暗号化両方を実行するセキュリティ レベル

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。表 5-1 では、セキュリティ モデルとレベルの組み合わせの意味について説明します。

表 5-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	No	コミュニティ ストリングの照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）標準に基づいた認証を提供します。

User-Based Security Model

SNMPv3 User-Based Security Model（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

仮想ファイアウォールでは、SNMPv3 に対して次の 2 種類の認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

仮想ファイアウォールは SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、Request For Comments（RFC）3826 に準拠しています。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注）　外部 AAA（認証、許可、アカウンティング）サーバを使用する SNMPv3 動作の場合は、外部 AAA サーバ上のユーザ コンフィギュレーションで、プライバシー プロトコルとして AES を使用する必要があります。

コマンドライン インターフェイス（CLI）および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、仮想ファイアウォールの SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

仮想ファイアウォールはユーザ設定を次の方法で同期します。

- **snmp-server user** コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります。
- **username** コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシー パスフレーズになります。
- SNMP または CLI を使用してユーザを削除すると、SNMP と CLI の両方でユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。

（注）　パスフレーズ/パスワードをローカライズド キー/暗号化形式で設定すると、仮想ファイアウォールはパスワードを同期化しません。

Cisco NXOS はデフォルトで、同期したユーザ設定を 60 分間維持します。

グループベースの SNMP アクセス

*グループ*は業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは読み取りアクセス権または読み取りと書き込みアクセス権を指定して定義します。ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

ハイ アベイラビリティ

SNMP ではステートレス リスタートがサポートされています。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

ガイドラインと制限事項

SNMP には、次の注意事項および制限事項があります。

- 一部の SNMP MIB に対する読み取り専用アクセスがサポートされています。詳細については、次の URL で示すサイトにある Cisco NXOS の MIB サポート リストを参照してください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- SNMP Role Based Access Control（RBAC）はサポートされていません。
- SNMP 設定コマンドは、次の Cisco MIB でサポートされています。
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB

SNMP の設定

SNMP の設定については、『*Cisco Virtual Network Management Center GUI Configuration Guide*』（http://www.cisco.com/en/US/docs/unified_computing/vnmc/sw/1.3/VNMC_GUI_Configuration/b_VNMC_GUI_Configuration_Guide_1_3.pdf ）を参照してください。

SNMP の設定確認

SNMP 設定を表示するには、次のコマンドを使用します。

表 5-2　SNMP の設定

コマンド	目的
show running-config snmp [all]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp session	SNMP セッションを表示します。
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。

その他の参考資料

SNMP の実装に関するその他の情報については、次の項を参照してください。

- 「関連資料」（P.5-7）
- 「標準」（P.5-7）
- 「MIB」（P.5-8）

関連資料

関連項目	マニュアル タイトル
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	*『Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(4)』*
MIB	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

標準

標準	タイトル
この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。	—

MIB

MIB	MIB のリンク
• CISCO-TC • SNMPv2-MIB • SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • IF-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • ISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB • CISCO-UNIFIED-FIREWALL-MIB	

SNMP の機能履歴

表 5-3

機能名	リリース	機能情報
SNMP	4.0(4)SV1(1)	この機能が導入されました。