ロギングの設定

ロギング機能で、ロギングをイネーブルにしてログ情報の処理方法を指定できます。ログ表示機能では、リアルタイムでシステム ログ メッセージを表示できます。ログ表示機能の詳細については、第 37 章「システム ログ メッセージのモニタリング」を参照してください。

ロギングの概要

セキュリティ アプライアンスは、アクティビティ（許可または拒否されたネットワーク トラフィックの種類など）を説明するシステム ログ メッセージの監査証跡の生成をサポートし、システム ロギングの設定を可能にします。

すべてのシステム ログ メッセージには、デフォルトの重大度レベルが設定されています。メッセージには、必要に応じて新しい重大度レベルを再割り当てできます。重大度レベルを選択するとき、そのレベルから下位のレベルへのロギング メッセージが生成されます。上位レベルからのメッセージは含まれません。重大度レベルが高いほど、含まれるメッセージは多くなります。ロギングおよびシステム ログ メッセージの詳細については、『*Cisco Security Appliance Logging Configuration and System Log Messages*』を参照してください。

ロギングのセキュリティ コンテキスト

各セキュリティ コンテキストは、ロギング コンフィギュレーションがあり、メッセージを生成します。システム コンテキストまたは管理コンテキストにログインし、他のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージだけです。

システム実行スペースで生成されたシステム ログ メッセージにはフェールオーバー メッセージが含まれており、管理コンテキストで生成されたメッセージとともに管理コンテキストで表示されます。システム実行スペースで、ロギングを設定したり、ロギング情報を表示したりすることはできません。

各メッセージにコンテキスト名を表示するようにセキュリティ アプライアンスを設定できます。単一の syslog サーバに送信されるコンテキスト メッセージを区別するのに役立ちます。この機能を使用すると、管理コンテキストで生成されたメッセージとシステムで生成されたメッセージを判別できます。システム実行スペースから送信されたメッセージはデバイス ID **system** を使用し、管理コンテキストから送信されたメッセージはデバイス ID として管理コンテキスト名を使用します。デバイス ID を使用するには、P.13-8 の「Advanced Syslog Configuration」を参照してください。

ロギングの使用

ロギングをイネーブルにしたら、次の作業を実行します。

ステップ 1　Logging Setup ペインで、ロギング パラメータを設定します。詳細については、P.13-3 の「Logging Setup」を参照してください。

ステップ 2　Syslog Setup ペインでは、syslog サーバに送信されるシステム ログ メッセージにファシリティのコードを含めるように設定したり、各メッセージにタイムスタンプを含めるように指定したり、メッセージの重大度レベルを表示または変更したり、メッセージを抑止したりします。詳細については、P.13-6 の「Syslog Setup」を参照してください。

ステップ 3　E-Mail Setup ペインで、通知を目的として電子メールで送信されるシステム ログ メッセージを指定します。詳細については、P.13-6 の「Syslog Setup」を参照してください。

ステップ 4　Event Lists ペインで、記録するメッセージを指定するイベントのカスタム リストを作成します。ここで作成したリストは、ログ フィルタのセットアップ時に使用されます。詳細については、P.13-11 の「Event Lists」を参照してください。

ステップ 5　Logging Filters ペインで、各ログの宛先に送信されるメッセージのフィルタリングに使用する基準を指定します。フィルタの作成に使用する基準とは、重大度レベル、メッセージ クラス、メッセージ ID、またはイベント リストです。詳細については、P.13-15 の「Logging Filters」を参照してください。

ステップ 6　Rate Limit ペインで、指定した時間間隔に生成可能なメッセージ数を制限します。詳細については、P.13-19 の「Rate Limit」を参照してください。

ステップ 7　Syslog Server ペインで、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを 1 つ以上指定します。詳細については、P.13-22 の「Syslog Servers」を参照してください。

Logging Setup

SupportedUserRoles

Configuration > Properties > Logging > Logging Setup

Logging Setup ペインでは、セキュリティ アプライアンスでのシステム ロギングをイネーブルにして、スタンバイ装置がロギングを引き継ぐかどうか、デバッグ メッセージを送信するかどうか、EMBLEM 形式を使用するかどうかなど、一般ロギング パラメータを指定できます。また、内部ログ バッファやセキュリティ アプライアンスのロギング キューのデフォルト設定も変更できます。

フィールド

- Enable logging：メイン セキュリティ アプライアンスのロギングをオンにします。
- Enable logging on the failover standby unit：使用可能な場合は、スタンバイ セキュリティ アプライアンスのロギングをオンにします。
- Send debug messages as syslogs：すべてのデバッグ トレース出力をシステム ログにリダイレクトします。このオプションがイネーブルになっている場合、システム ログ メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでロギングをイネーブルにし、デバッグ システム ログ メッセージ番号および重大度レベルの宛先として設定する必要があります。使用されるシステム ログ メッセージ番号は、711001 です。このシステム ログ メッセージのデフォルトの重大度レベルは debug です。
- Send syslogs in EMBLEM format：syslog サーバ以外のすべてのログの宛先に使用するため、EMBLEM 形式をイネーブルにします。
- Buffer Size：ロギング バッファがイネーブルになっている場合に、システム ログ メッセージが保存される内部ログ バッファのサイズを指定します。FTP サーバまたは内部フラッシュ メモリへのログの保存をイネーブルにしていない限り、バッファがいっぱいになったときは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。指定できる範囲は、4096 ～ 1048576 バイトです。
- Save Buffer To FTP Server：上書きされる前にバッファの内容を FTP サーバに保存するには、このチェックボックスをオンにします。FTP コンフィギュレーションを削除するには、チェックボックスをオフにします。
- Configure FTP Settings：FTP サーバを示し、バッファの内容の保存に使用する FTP パラメータを設定します。
- Save Buffer To Flash：上書きされる前にバッファの内容を内部フラッシュ メモリに保存するには、このチェックボックスをオンにします。

（注） このオプションは、ルーテッドまたは透過シングルモードでのみ使用できます。

- Configure Flash Usage：ロギングのために内部フラッシュ メモリで使用される最大容量および維持する最小空き容量を、KB で指定します。このオプションをオンにすると、「syslog」という名前のディレクトリが、メッセージの格納先のデバイス ディスクに作成されます。

（注） このオプションは、ルーテッドまたは透過シングルモードでのみ使用できます。

- Security Appliance Logging Queue Size：セキュリティ アプライアンスで表示されるシステム ログのキュー サイズを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-4 の「Configure FTP Settings」を参照してください。
- P.13-5 の「Configure Logging Flash Usage」を参照してください。

Configure FTP Settings

Configuration > Features > Properties > Logging > Logging Setup > Configure FTP Settings

Configure FTP Settings ダイアログボックスでは、バッファの内容の保存に使用する FTP サーバのコンフィギュレーションを指定します。

フィールド

- Enable FTP client：FTP クライアントのコンフィギュレーションをイネーブルにします。
- Server IP Address：FTP サーバの IP アドレスです。
- Path：保存されたファイルを格納する FTP サーバ上のディレクトリ パスです。
- Username：FTP サーバにログインするためのユーザ名です。
- Password：FTP サーバにログインするためのユーザ名に関連付けられたパスワードです。
- Confirm Password：パスワードを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Configure Logging Flash Usage

Configuration > Properties > Logging > Logging Setup > Configure Logging Flash Usage

Configure Logging Flash Usage ダイアログボックスでは、バッファの内容を内部フラッシュ メモリに保存するときの制限を指定します。

フィールド

- Maximum Flash to Be Used by Logging : ロギングに使用できる内部フラッシュ メモリの最大容量を、KB で指定します。
- Minimum Free Space to Be Preserved : 保持する内部フラッシュ メモリの容量を、KB で指定します。内部フラッシュメモリが制限値に近づくと、新しいログが保存されなくなります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Syslog Setup

Configuration > Properties > Logging > Syslog Setup

Syslog Setup ペインでは、syslog サーバを宛先とするメッセージにファシリティ コードを含めるように設定し、システム ログ メッセージにタイムスタンプを含める必要があるかどうかを決定します。また、メッセージの重大度レベルを変更したり、記録しないメッセージを抑止したりもできます。

フィールド

- Facility code to include in syslogs：syslog サーバのシステム ログ ファシリティを、ファイル メッセージの基本として使用するように指定します。デフォルトは LOCAL(4)20 で、ほとんどの UNIX システムで想定されているコードです。ただし、ネットワーク デバイスでは使用可能な 8 つのファシリティを共有しているため、システム ログのこの値を変更しなければならない場合があります。
- Include timestamp in syslogs：送信されるすべてのシステム ログ メッセージに日付と時刻を含めます。
- Syslog ID Setup：Syslog ID テーブルに表示される情報を選択します。オプションは次のように定義されています。
  - Show all syslog IDs：syslog ID テーブルで、システム ログ メッセージ ID のリスト全体を表示するように指定します。
  - Show suppressed syslog IDs：syslog ID テーブルで、明示的に抑止されたシステム ログ メッセージ ID のみを表示するように指定します。
  - Show syslog IDs with changed logging：syslog ID テーブルで、デフォルト値から変更された重大度レベルを持つシステム ログ メッセージ ID のみを表示するように指定します。
  - Show syslog IDs that are suppressed or with a changed logging level：syslog ID テーブルで、重大度レベルが変更されたシステム ログ メッセージ ID と、明示的に抑止されたシステム ログ メッセージ ID のみを表示するように指定します。
- Syslog ID Table：表示のみ。Syslog ID Table View にある設定に基づいてシステム ログ メッセージのリストを表示します。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID の抑止またはその重大度レベルの変更のいずれかを行えます。リスト内の複数のメッセージ ID を選択するには、範囲の最初の ID を選択し、Shift キーを押した状態で範囲の最後の ID をクリックします。
- Advanced：システム ログ メッセージにデバイス ID を含めるように設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-7 の「Edit Syslog ID Settings」を参照してください。
- P.13-8 の「Advanced Syslog Configuration」を参照してください。

Edit Syslog ID Settings

Configuration > Properties > Logging > Syslog Setup > Edit Syslog ID Settings

Edit Syslog ID Settings ダイアログボックスでは、選択したシステム ログ メッセージの重大度レベルを変更したり、選択したシステム ログ メッセージの抑止を指定したりできます。

フィールド

- Syslog ID(s)：このテキスト領域は読み取り専用です。この領域に表示される値は、Syslog Setup ペインにある Syslog ID テーブルで選択されたエントリで決まります。
- Suppress Message(s)：Syslog ID リストに表示されるシステム ログ メッセージ ID のメッセージを抑止するには、このチェックボックスをオンにします。
- Logging Level：Syslog ID リストに表示されるシステム ログ メッセージ ID に送信されるメッセージの重大度レベルを選択します。レベルは次のように定義されています。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Advanced Syslog Configuration

Configuration > Properties > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration

セキュリティ アプライアンスが非 EMBLEM 形式のシステム ログ メッセージにデバイス ID を含めるように設定できます。システム ログ メッセージに、1 つのタイプだけのデバイス ID を表示できます。デバイス ID は、FWSM のホスト名、インターフェイス IP アドレス、コンテキスト、またはテキスト文字列で指定できます。

Advanced Syslog Configuration ダイアログボックスでは、システム ログ メッセージにデバイス ID を含めるかどうかを決定できます。この機能がイネーブルになっている場合、デバイス ID がすべての非 EMBLEM 形式のシステム ログ メッセージに含まれます。

フィールド

- Enable Syslog Device ID：デバイス ID をすべての非 EMBLEM 形式のシステム ログ メッセージに含めるように指定します。
- Hostname：デバイス ID としてホスト名を使用するように指定します。
- IP Address：デバイス ID としてインターフェイスの IP アドレスを使用するように指定します。
  - Interface Name：指定した IP アドレスに対応するインターフェイス名を指定します。
- String：デバイス ID としてユーザ定義の文字列を使用するように指定します。
  - User-defined ID：英数字のユーザ定義文字列を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

E-Mail Setup

Configuration > Properties > Logging > E-Mail Setup

E-Mail Setup ペインでは、通知目的の電子メール メッセージとして送信される、指定したシステム ログ メッセージの受信者リストとともに、送信元電子メール アドレスもセットアップします。送信先電子メール アドレスに送信されるシステム ログ メッセージは、重大度レベルでフィルタリングできます。テーブルには、どのエントリのセットアップが完了しているかが表示されます。

送信先電子メール アドレスへのメッセージのフィルタリングに使用されるシステム ログ メッセージの重大度レベルは、Logging Filters ペインですべての電子メール受信者に対して設定されたグローバル フィルタに比べ、ここで選択した方がより高くなっています。

送信先電子メール アドレスに使用されるシステム ログ メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。Logging Filters ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。

フィールド

- Source E-Mail address：電子メール メッセージとして送信されるシステム ログ メッセージの送信元アドレスとなる電子メール アドレスを指定します。
- Destination E-Mail Address：指定したシステム ログ メッセージの受信者の電子メール アドレスを指定します。
- Syslog Severity：この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。指定した重大度またはそれ以上の重大度を持つメッセージが送信されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-10 の「Add/Edit E-Mail Recipients」を参照してください。
- P.13-15 の「Logging Filters」を参照してください。

Add/Edit E-Mail Recipients

Configuration > Properties > Logging > E-Mail Setup > Add/Edit E-Mail Recipient

Add/Edit E-Mail Recipient ダイアログボックスでは、特定の重大度を持つシステム ログ メッセージを電子メール メッセージとして送信する、送信先電子メール アドレスをセットアップします。

送信先電子メール アドレスへのメッセージのフィルタリングに使用される重大度レベルは、Logging Filters ペインですべての電子メール受信者に対して設定されたグローバル フィルタに比べ、ここで選択した方がより高くなっています。

フィールド

- Destination E-Mail Address：選択したシステム ログ メッセージの受信者の電子メール アドレスを指定します。
- Syslog Severity：この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Event Lists

Configuration > Properties > Logging > Event Lists

Event Lists ペインでは、どのシステム ログ メッセージが特定の宛先に送信されるのかを選択するときに使用する、イベントのカスタム リストを作成できます。ロギングをイネーブルにし、Logging Setup ペインを使用してロギング パラメータを設定したら、Event Lists ペインでイベントのリストを 1 つ以上作成します。これらのリストは、イベントの各リストのロギング出力先を指定する場合に Logging Filters ペインで使用します。

イベント リストの定義には、次の 3 つの基準を使用できます。

- メッセージ クラス
- 重大度
- メッセージ ID

メッセージ クラスは、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できるようにする、セキュリティ アプライアンスの機能に関連したシステム ログ メッセージのグループです。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを分類します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

メッセージ ID は、各メッセージを一意に識別する数値です。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

フィールド

- Name：イベント リストの名前を一覧表示します。
- Event Class/Severity：ロギング メッセージのイベント クラスおよびレベルを一覧表示します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - ip：IP スタック
  - np：ネットワーク プロセッサ
  - ospf：OSPF ルーティング
  - rip：RIP ルーティング
  - rm：リソース マネージャ
  - session：ユーザ セッション
  - snmp：SNMP
  - sys：システム

  重大度レベルは次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）

  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- Message IDs：フィルタに含めるシステム ログ メッセージ ID または ID の範囲（101001-101010 など）を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-12 の「Add/Edit Event List」を参照してください。
- P.13-14 の「Add/Edit Syslog Message ID Filter」を参照してください。
- P.13-15 の「Logging Filters」を参照してください。

Add/Edit Event List

Configuration > Properties > Logging > Event Lists > Add/Edit Event List
（このダイアログボックスへのパスは数種類あります。）

Add/Edit Event List ダイアログボックスでは、ログの宛先に送信するメッセージを指定する場合に使用できるイベント リストを作成または編集できます。メッセージ クラスおよび重大度、またはメッセージ ID に基づいてメッセージをフィルタリングするイベント リストを作成できます。

メッセージ クラスは、セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを定義します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

メッセージ ID は、各メッセージを一意に識別する数値です。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

フィールド

- Name：イベント リストの名前を入力します。
- Event Class：イベント クラスを一覧表示します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局

  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ips：侵入防御サービス
  - ip：IP スタック
  - np：ネットワーク プロセッサ
  - ospf：OSPF ルーティング
  - rip：RIP ルーティング
  - rm：リソース マネージャ
  - session：ユーザ セッション
  - snmp：SNMP
  - sys：システム
- Severity：ロギング メッセージのレベルを一覧表示します。重大度レベルは次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- Message IDs Filters：フィルタに含めるシステム ログ メッセージ ID またはシステム ログ メッセージ ID の範囲（101001-101010 など）を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Syslog Message ID Filter

Configuration > Properties > Logging > Event Lists > Add/Edit Event List > Add/Edit Syslog Message ID Filter

Add/Edit Syslog Message ID Filter ダイアログボックスでは、イベント リストに含める 1 つ以上のシステム ログ メッセージ ID を指定できます。

フィールド

- Message IDs：記録するシステム ログ メッセージ ID または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Logging Filters

Configuration > Properties > Logging > Logging Filters

Logging Filters ペインでは、メッセージ フィルタをログの宛先に適用します。ログの宛先に適用されたフィルタにより、その宛先に送信するメッセージが選択されます。

メッセージ クラスおよび重大度レベルに従ってメッセージをフィルタリングしたり、Event Lists ペインで作成可能なイベント リストを使用したりできます。

フィールド

- Logging Destination：フィルタを適用できるロギングの宛先の名前を一覧表示します。ロギングの宛先は次のとおりです。
  - コンソール
  - セキュリティ アプライアンス
  - Syslog サーバ
  - SNMP トラップ
  - 電子メール
  - 内部バッファ
  - Telnet セッション
- Syslogs From All Event Classes：重大度、またはログの宛先へのメッセージのフィルタリングに使用するイベント リストを一覧表示するか、すべてのイベント クラスに対してロギングをディセーブルにするかどうかを指定します。
- Syslogs From Specific Event Classes：ログの宛先へのメッセージのフィルタリングに使用するイベント クラスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-15 の「Edit Logging Filters」を参照してください。
- P.13-14 の「Add/Edit Syslog Message ID Filter」を参照してください。
- P.13-17 の「Add/Edit Class and Severity Filter」を参照してください。
- P.13-11 の「Event Lists」を参照してください。

Edit Logging Filters

Configuration > Properties > Logging > Logging Filters > Edit Logging Filters

Edit Logging Filters ダイアログボックスでは、各ログの宛先にフィルタを適用したり、すでにログの宛先に適用されたフィルタを編集したり、ログの宛先に対するフィルタをディセーブルにしたりできます。

メッセージ クラスおよび重大度レベルに従ってメッセージをフィルタリングしたり、Event Lists ペインで作成可能なイベント リストを使用したりできます。

フィールド

- Logging Destination：このフィルタに対してロギングの宛先を指定します。
- Filter on severity：重大度レベルに従って、システム ログ メッセージをフィルタリングします。
  - Filter on severity：フィルタリングを行うシステム ログ メッセージのレベルを指定します。
- Use event list：このフィルタへのイベント リストの使用を指定します。
  - Use event：使用するイベント リストを指定します。
- New：新しいイベント リストを追加できます。
- Disable logging from all event classes : 選択した宛先へのすべてのロギングをディセーブルにします。
- Event Class：イベント クラスを指定します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - ip：IP スタック
  - np：ネットワーク プロセッサ
  - ospf：OSPF ルーティング
  - rip：RIP ルーティング
  - rm：リソース マネージャ
  - session：ユーザ セッション
  - snmp：SNMP
  - sys：システム
- Severity：ロギング メッセージのレベルを指定します。重大度レベルは次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Class and Severity Filter

...Add Event List > Add/Edit Class and Severity Filter（このダイアログボックスへのパスは数種類あります。）

Add/Edit Class and Severity Filter ダイアログボックスでは、メッセージのフィルタリングに使用するメッセージ クラスおよび重大度レベルを指定します。

メッセージ クラスは、セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログを定義します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

フィールド

- Event Class：イベント クラスを指定します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - ip：IP スタック
  - np：ネットワーク プロセッサ
  - ospf：OSPF ルーティング
  - rip：RIP ルーティング
  - rm：リソース マネージャ
  - session：ユーザ セッション
  - snmp：SNMP
  - sys：システム
- Severity：ロギング メッセージのレベルを指定します。重大度レベルは次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Syslog Message ID Filter

Configuration > Properties > Logging > Logging Filters > Edit Logging Filters > Add Event List > Add/Edit Syslog Message ID Filter

Add/Edit Syslog Message ID Filter ダイアログボックスでは、イベント リスト フィルタに含める個々のシステム ログ メッセージ ID または ID の範囲を指定します。

フィールド

- Message IDs：システム ログ メッセージ ID または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Rate Limit

Configuration > Features > Properties > Logging > Rate Limit

Rate Limit ペインでは、ファイアウォールが送信できるシステム ログ メッセージ数を指定します。また、Logging Setup ペインを使用してロギングをイネーブルにする必要もあります。メッセージ ロギング レベルのレート制限を具体的に指定して、特定のメッセージのレートを制限することができます。レート レベルは、重大度レベルまたはメッセージ ID に適用されますが、宛先には適用されません。したがって、レート制限は、すべての設定済み宛先に送信されるメッセージの量に影響を与えます。

フィールド

syslog ロギング レベルのレート制限

- Logging Level：メッセージの重大度レベルを一覧表示します。レベルは次のように定義されています。
  - Disabled（ロギングなし）
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- No of Messages：送信されるメッセージ数を表示します。メッセージ数を制限なしにするには、Number of Messages フィールドと Time Interval フィールドの両方を空白のままにします。
- Interval (Seconds)：このロギング レベルで送信できるメッセージ数を制限するのに使用される間隔を、秒数で表示します。メッセージ数を制限なしにするには、Number of Messages と Time Interval の両方を空白のままにします。
- Edit : Edit Rate Limit ダイアログボックスを開き、選択したロギング レベルのプロパティを編集するには、テーブルからロギング レベルを選択し、このボタンをクリックします。
- **個別にレート制限された syslog メッセージ**
  - Syslog ID：制限されているシステム ログ メッセージの ID を表示します。
  - Logging Level：メッセージの重大度レベルを表示します。重大度レベルのリストについては、P.13-19 の「syslog ロギング レベルのレート制限」を参照してください。
  - No of Messages：指定された時間間隔に送信できるメッセージの最大数を表示します。
  - Interval (Seconds)：システム ログ メッセージの制限に使用される間隔を秒数で表示します。
  - Add：特定のメッセージのレートを制限するには、このボタンをクリックします。
- Apply：変更内容をファイアウォールに送信し、実行中のコンフィギュレーションに適用します。File メニューを使用して、実行中のコンフィギュレーションを内部フラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ ファイアウォール装置に書き込みます。
- Reset：変更内容を破棄し、開いたときに表示された値、または開いている間に最後に Refresh をクリックしたときの値に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-20 の「Edit Rate Limit for Syslog Logging」を参照してください。
- P.13-21 の「Add/Edit Rate Limit for Syslog Message」を参照してください。

Edit Rate Limit for Syslog Logging

Configuration > Features > Properties > Logging > Edit Rate Limit for Syslog Logging Level

Edit Rate Limit for Syslog Logging Level ボックスでは、指定した時間間隔にファイアウォールが送信できるメッセージ数を制限します。

フィールド

syslog ロギング レベルのレート制限

- Logging Level : 選択したメッセージの重大度レベルを表示します。特定のメッセージ ID のレート制限を変更すると、ロギング レベルを指定できる場合があります。レベルは次のように定義されています。
  - Disabled（ロギングなし）
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- No of Messages：このロギング レベルで送信可能なメッセージの最大数を指定します。
- Time Interval (seconds)：このロギングレベルでメッセージを制限するときに使用される時間を、秒数で指定します。
- OK：変更内容を受け入れて、前のペインに戻ります。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- Help：詳細情報を表示します。
- Reset：変更内容を破棄し、開いたときに表示された値、または開いている間に最後に Refresh をクリックしたときの値に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Rate Limit for Syslog Message

Configuration > Features > Properties > Logging > Rate Limit > Add/Edit Rate Limit for Syslog Message

Add/Edit Rate Limit for Syslog Message ダイアログボックスでは、レート制限を特定のシステム ログ メッセージに割り当てることができます。

フィールド

- Syslog Message ID：制限するシステム ログ メッセージのメッセージ ID を指定します。
- Number of Messages：指定された時間間隔にこのメッセージを送信できる最大回数を指定します。
- Time Interval：指定したメッセージの制限に使用される時間を秒数で指定します。

（注）　メッセージ数を制限なしにするには、Number of Messages と Time Interval の両方を空白のままにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Syslog Servers

Configuration > Properties > Logging > Syslog Servers

Syslog Servers ペインでは、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを指定します。定義した syslog サーバを使用するには、Logging Setup ペインを使用してロギングをイネーブルにし、Logging Filters ペインで適切な宛先をセットアップする必要があります。

（注）　コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

フィールド

- Interface：syslog サーバとの通信に使用するインターフェイスを表示します。
- IP Address：syslog サーバとの通信に使用されるインターフェイスの IP アドレスを表示します。
- Protocol/Port：syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコルおよびポートを表示します。
- EMBLEM：メッセージをシスコ EMBLEM 形式（Protocol/Port で UDP が選択されている場合にのみ使用可能）で記録するかどうかを指定します。
- Queue Size：syslog サーバがビジー状態の場合、セキュリティ アプライアンスでキューに入れることができるメッセージ数を指定します。値がゼロの場合、キューに入れられるメッセージ数に制限がないことを意味します。
- Allow user traffic to pass when TCP syslog server is down：syslog サーバがダウンしている場合に、すべてのトラフィックを制限するかどうかを指定します。
- Deny connection upon queue full：キューがいっぱいのとき（つまり、Queue Size で設定した制限値に達したとき）に、接続を許可するかどうかを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

参考資料

- P.13-23 の「Add/Edit Syslog Server」を参照してください。
- P.13-3 の「Logging Setup」を参照してください。
- P.13-15 の「Logging Filters」を参照してください。

Add/Edit Syslog Server

Configuration > Properties > Logging > Syslog Servers > Add/Edit Syslog Server

Add/Edit Syslog Server ダイアログボックスでは、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを追加または編集できます。定義した syslog サーバを使用するには、Logging Setup ペインでロギングをイネーブルにし、Logging Filters ペインでログの宛先に適切なフィルタをセットアップする必要があります。

（注）　コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

フィールド

- Interface：syslog サーバとの通信に使用するインターフェイスを指定します。
- IP Address：syslog サーバとの通信に使用する IP アドレスを指定します。
- Protocol : syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコル（TCP または UDP）を表示します。
- Port：syslog サーバがセキュリティ アプライアンスとの通信に使用するポートを指定します。
- Log messages in Cisco EMBLEM format (UDP only)：メッセージをシスコ EMBLEM 形式（Protocol で UDP が選択されている場合にのみ使用可能）で記録するかどうかを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—