CHAPTER 9

ゲスト アクティビティ ロギング

ゲスト アクティビティ ロギングを使用すると、Cisco NAC ゲスト サーバでネットワーク デバイス（ファイアウォール、プロキシ サーバ、ルータなど）から syslog 情報を受信できます。syslog 情報には、ゲストが行ったすべての接続に関する詳細情報に加えて、ネットワーク デバイスによっては、アクセスした URL などのレイヤ 7 情報も含まれます。

ゲスト アクティビティ ロギングでは、各ゲストがネットワーク認証を行ったときの IP アドレスが必要です。Cisco NAC ゲスト サーバは RADIUS アカウンティングから IP アドレスの情報を受信するため、ユーザが認証に使用するネットワーク デバイスがこの情報を送信するように設定する必要があります。このネットワーク デバイスは、通常、Wireless LAN Controller または Cisco NAC アプライアンスです。これらのデバイスを RADIUS クライアントとして追加する方法の詳細については、第 8 章「RADIUS クライアントの設定」を参照してください。

（注） ゲスト アクティビティ ロギングでは、syslog 情報を RADIUS アカウンティングから受信した IP アドレスに関連付ける必要があります。これは、認証後にゲストの IP アドレスが変更されても追加の RADIUS アカウンティング メッセージが送信されないような構成方法を使用している場合、ゲスト アクティビティ ロギングが機能しなくなることを意味しています。

Cisco NAC ゲスト サーバは、各ゲストの IP アドレスを受信した後に、ネットワーク デバイスから syslog 情報を受信する必要があります。ゲスト サーバの UDP ポート 514 に syslog を送信するように、各ネットワーク デバイスを設定してください。ゲスト サーバでは、syslog 情報を受信すると、その syslog 情報を各ゲストに対して関連付ける処理が行われます。この関連付けにより、「ゲスト ユーザに関するレポート」（P.17-20）に示すように、各ゲストのゲスト アクティビティ ログ詳細ページでゲストのアクティビティを参照できるようになります。

ゲスト アクティビティは、アプライアンスのディスクに格納されている個別のファイルに関連付けられます。アプライアンスでは、残りのディスク スペースが 30% 未満になるまでログ ファイルを格納できます。その後、最も古いログ ファイルが削除されるか、「Syslog モニタリングの設定」（P.9-1）に示すように、外部の FTP サーバにログ ファイルがアーカイブされます。

（注） ゲスト ユーザがアクセスした URL のリストを表示するレポートに関して、NAD に対する HTTP トラフィックの検査をイネーブルにする必要があります。これは WLC には該当しません。

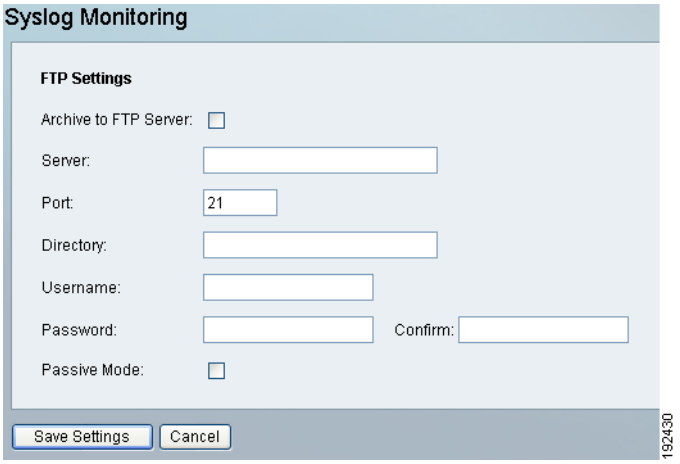
Syslog モニタリングの設定

ログを FTP サーバにアーカイブすると、ログを長期間保存でき、ログのバックアップにもなります。

スポンサー インターフェイスを使用してログを参照すると、NAC ゲスト サーバでアーカイブ サーバ上のログが自動的に検索され、レポート形式でログが表示されます。

ステップ 1　管理インターフェイスを使用して、左側のメニューから [Devices] > [Syslog Monitoring] を選択します（図 9-1 を参照）。

図 9-1　Syslog Monitoring



ステップ 2　ゲスト ログをアーカイブするように NAC ゲスト サーバを設定する場合は、[Archive to FTP Server] チェックボックスをオンにします。

ステップ 3　[Server] フィールドに、FTP サーバの名前または IP アドレスを入力します。

ステップ 4　[Port] に、FTP サーバのポートを入力します。

ステップ 5　[Directory] で、アーカイブ ファイルを格納する FTP サーバのディレクトリを指定します。

ステップ 6　[Username] と [Password] に、FTP サーバにログイン可能な、指定したディレクトリに対する書き込み権限があるアカウントのユーザ名とパスワードをそれぞれ入力します。

ステップ 7　デフォルトで使用される FTP モードはアクティブ FTP です。パッシブ モードを使用する場合は、[Passive Mode] チェックボックスをオンにします。

レプリケーションがイネーブルな場合のゲスト アクティビティ ロギング

復元用データベース情報のレプリケーションを実行する NAC ゲスト サーバが 2 つある場合、各レプリケーション ボックス間でのゲスト アクティビティ ログのレプリケーションは実行されません。

ただし、スポンサー インターフェイスでレポートを参照する場合には、NAC ゲスト サーバはレプリケーション ボックスに接続して、そこからログを取得します。これにより、すべてのログが統合ビューに表示されます。

スポンサー インターフェイスを使用すると、syslog をどちらの NAC ゲスト サーバに送信するかをネットワーク デバイスごとに設定できますが、すべての結果は単一のインターフェイスによって参照されます。

各 NAC ゲスト サーバは、HTTPS を介してレプリケーション ペアのもう一方のゲスト サーバからログを安全に取得します。各 NAC ゲスト サーバは、検索が正常に実行できるように、もう一方の NAC ゲスト サーバの証明書を信頼する必要があります。これをイネーブルにするには、もう一方の NAC ゲスト サーバのルート CA 証明書がアップロードされるようにします（「証明書ファイルのアップロード」（P.3-14）を参照）。