CHAPTER 31

ネットワーク アドミッション コントロール

ネットワーク アドミッション コントロール（NAC）は、クライアント ワークステーションの健全性を検証し、使用可能な最新の更新済みウィルス シグニチャがデータ ネットワークで受信されるようにし、データ ネットワークからネットワークへのアクセスを制御することによって、データ ネットワークをコンピュータ ウィルスから保護します。

NAC は、アンチウィルス ソフトウェアとともに動作し、クライアントの状態（クライアントの*ポスチャ*と呼ばれる）を検証してから、クライアントがネットワークにアクセスするのを許可します。NAC では、ネットワーク クライアントがウィルスに感染していない最新のウィルス シグニチャセットを保持していることが確認されます。クライアントのシグニチャを更新する必要がある場合は、NAC からクライアントに対して更新を完了するように指示されます。クライアントが危険にさらされているか、ネットワーク上でウィルスが発生している場合は、ウィルスの削除が完了するまで、クライアントは隔離されたネットワーク セグメントに置かれます。

NAC の詳細については、次のリンクをクリックしてください。

- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

NAC の作成タブ

［NAC の作成］タブと NAC ウィザードを使用して NAC ポリシーを作成し、そのポリシーをインターフェイスと関連付けます。NAC ポリシーの作成後は、［NAC の編集］をクリックし、ポリシー リストからその NAC ポリシーを選択して編集できます。

ルータ上の NAC 設定は、完全な NAC 実装の一部分にすぎません。NAC を実装するには、「NAC 実装のその他の作業」（クリックすると、この項に移動します）で、他のデバイスで行う必要がある作業について確認してください。

AAA の有効化ボタン

認証、許可、アカウンティング（AAA）をルータ上で有効にしなければ、NAC を設定できません。AAA が無効の場合は、［AAA の有効化］ボタンをクリックします。AAA がすでにルータ上で設定されている場合は、このボタンは表示されません。

NAC ウィザードの起動ボタン

このボタンをクリックして、NAC ウィザードを起動します。ウィザードでは、NAC 設定が一連の画面に分割され、それぞれで単一の設定作業を完了します。

実行方法リスト

このウィザードを使用して行うことのできない設定作業が必要な場合は、このリストの隣にあるボタンをクリックします。このリストには、行うことのできるその他のタイプの設定作業が表示されています。一覧表示されている設定作業の方法について確認する場合は、その設定作業を選択し［移動］をクリックします。

NAC 実装のその他の作業

完全な NAC 実装の設定手順は、次のとおりです。

ステップ 1　ネットワーク ホストに Cisco Trust Agent（CTA）をインストールし、設定します。これによって、ルータからの EAPoUDP クエリに応答可能なポスチャ エージェントがホストに設定されます。この手順の後のリンクを参照して CTA ソフトウェアを取得し、インストールと設定方法を確認してください。

ステップ 2　AAA 認証 EAPoUDP サーバをインストールし設定します。このサーバは、RADIUS プロトコルを使用する Cisco Secure Access Control Server（ACS）でなければなりません。Cisco Secure Access Control Server ソフトウェア バージョン 3.3 が必要です。ACS のインストールと設定の詳細については、この手順の後のリンクを参照してください。

ステップ 3　ポスチャの検証および修復用サーバをインストールし、設定します。

登録済みの Cisco.com ユーザである場合は、次のリンクから Cisco Trust Agent（CTA）ソフトウェアをダウンロードできます。

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

次のリンクのドキュメントには、ホストへの CTA ソフトウェアのインストールと、その設定方法が説明されています。

http://www.cisco.com/en/US/products/ps5923/tsd_products_support_series_home.html

次のリンクのドキュメントには、設定プロセスの概要が記載されています。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

次のリンクのドキュメントでは、Windows Servers バージョン 3.3 用の Cisco Secure ACS のインストールと設定の方法が説明されています。

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

ようこそ

NAC ウィザードでは、次のことが可能です。

- NAC が有効となるインターフェイスの選択 — このインターフェイスを介してネットワークにアクセスするホストは、NAC 検証プロセスを経る必要があります。
- NAC ポリシー サーバの設定 — アドミッション コントロール ポリシーがこれらのサーバに設定され、ネットワーク ホストがネットワークにアクセスする際に、ルータがそれらのサーバに接続します。複数のサーバに対して情報を指定できます。NAC ポリシー サーバでは、RADIUS プロトコルが使用されます。
- NAC 例外リストの設定 — プリンタや IP 電話などのホスト、および NAC ポスチャ エージェントがインストールされていないホストでは、NAC プロセスを回避する必要がある場合があります。スタティック IP アドレスを持つホストや他のデバイスは、例外リストで識別でき、関連付けられた例外ポリシーを使用して制御できます。また、ホストはその MAC アドレスやデバイス タイプによっても識別できます。
- エージェントレス ホスト ポリシーの設定 — Cisco Secure ACS サーバに存在するポリシーを使用して、ポスチャ エージェントがインストールされていないホストが制御されるようにすることもできます。Cisco Secure ACS サーバは、エージェントレス ホストからのパケットを受信すると、エージェントレス ホスト ポリシーを送信して応答します。エージェントレス ホスト ポリシーの設定は、DHCP クライアントなど、動的アドレス設定を行うエージェントレス ホストがある場合に有用です。
- リモート アクセス用の NAC の設定 — Cisco CP を使用してルータを管理しているホストでは、アクセスが許可されている必要があります。ウィザードでリモート管理用の IP アドレスを指定すると、Cisco CP で、それらの IP アドレスを持つホストからルータへのアクセスを許可するように NAC ACL を変更できるようになります。

ルータ上での NAC の設定が、NAC 設定での最後の手順になります。ルータにこの機能を設定する前に、「NAC 実装のその他の作業」で説明されている手順を完了してください。

NAC ポリシー サーバ

NAC アドミッション コントロール ポリシーが設定されると、Cisco Secure ACS バージョン 3.3 が実行されている RADIUS サーバ上にあるポリシー データベースに格納されます。ルータでは、RADIUS サーバと通信してネットワーク ホストのクレデンシャルを検証する必要があります。このウィンドウでは、ルータから RADIUS サーバへの接続に必要な情報を設定します。指定する各 RADIUS サーバでは、Cisco Secure Cisco Access Control Server（ACS）ソフトウェア バージョン 3.3 がインストールおよび設定されている必要があります。

RADIUS クライアント ソースの選択

RADIUS のソースを設定すると、RADIUS サーバにバインドされた RADIUS パケットで送信されるように、送信元 IP アドレスを指定できます。インターフェイスの詳細については、インターフェイスを選択し、［詳細］ボタンをクリックして確認してください。

Cisco ACS バージョン 3.3 以降では、ルータ から送信される RADIUS パケットの送信元 IP アドレスを NAD IP アドレスとして設定する必要があります。

［ルータが送信元を選択します］を選択すると、RADIUS パケットの送信元 IP アドレスは、RADIUS パケットがルータから送り出されるときに通過するインターフェイスのアドレスになります。

インターフェイスを選択すると、RADIUS パケットの送信元 IP アドレスは、RADIUS クライアント ソースとして選択したインターフェイスのアドレスになります。

（注） Cisco IOS ソフトウェアを使用すると、単一 RADIUS ソースのインターフェイスをルータ上で設定できます。ルータにある設定済み RADIUS ソースとは別のソースを選択する場合、RADIUS サーバに送信されるパケットの送信元 IP アドレスは、新しいソースの IP アドレスに変わり、Cisco ACS で設定された NAD IP アドレスと一致しなくなる場合があります。

詳細ボタン

インターフェイスを選択する前に、インターフェイスに関する情報のクイック スナップショットが必要な場合は、［詳細］をクリックします。画面には、IP アドレスとサブネット マスク、インターフェイスに適用されるアクセス ルールとインスペクション ルール、適用された IPSec ポリシーと QoS ポリシー、およびインターフェイス上に Easy VPN 設定があるかどうかが表示されます。

サーバ IP/ タイムアウト / パラメータ カラム

［サーバ IP］、［タイムアウト］、および［パラメータ］カラムには、ルータから RADIUS サーバへの接続に使用される情報が含まれています。RADIUS サーバの情報が、選択されたインターフェイスに関連しない場合は、これらのカラムには何も表示されません。

NAC の使用チェック ボックス

一覧表示された RADIUS サーバを NAC に使用する場合は、このチェック ボックスを選択します。サーバを NAC に使用するには、必要なアドミッション コントロール ポリシーがそのサーバに設定されている必要があります。

追加 / 編集 /Ping ボタン

RADIUS サーバの情報を入力するには、［追加］ボタンをクリックして、表示された画面に情報を入力します。RADIUS サーバの情報を変更するには、行を選択して［編集］をクリックします。ルータと RADIUS サーバ間の接続をテストするには、行を選択して［Ping］をクリックします。

（注） Ping テストを実行するときは、［Ping］ダイアログ ボックスの［送信元］フィールドに、RADIUS ソース インターフェイスの IP アドレスを入力します。［ルータが送信元を選択します］を選択した場合は、［Ping］ダイアログ ボックスの［送信元］フィールドに値を入力する必要はありません。

選択されたインターフェイスで RADIUS サーバ情報を使用できない場合、［編集］ボタンと［Ping］ボタンは無効です。

インターフェイスの選択

このウィンドウでは、NAC を有効にするインターフェイスを選択します。ネットワーク ホストがネットワークに接続する際に使用されるインターフェイスを選択します。

［詳細］ボタンをクリックして、選択したインターフェイスに関連するポリシーとルールを表示します。ウィンドウには、このインターフェイスのインバウンド / アウトバウンド トラフィックに適用される ACL の名前が表示されます。

インバウンド ACL がインターフェイスに存在する場合、Cisco CP では、EAPoUDP トラフィック用の適切な許可のステートメントを追加することによって、その ACL を NAC に使用します。NAC が適用されるインターフェイスの IP アドレスが 192.55.22.33 の場合、許可のステートメント例は次のとおりです。

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

Cisco CP で追加される許可のステートメントでは、EAPoUDP プロトコル用にポート番号 21862 が使用されます。ネットワーク ホストが、カスタム ポート番号で EAPoUDP を実行している場合は、ホストが使用するポート番号を使用するように、この ACL エントリを修正する必要があります。

指定したインターフェイスでインバウンド ACL が設定されていない場合は、Cisco CP によって ACL がインターフェイスに適用されるようにできます。推奨ポリシーか、レポートされた NAC ポスチャを単に監視するポリシーを選択できます。

- **完全検証（推奨）—** Cisco CP によって、すべてのトラフィックを拒否する ACL が適用されます（**deny ip any any**）。ネットワークに対するアドミッションは、NAC 検証プロセスによって決定されます。デフォルトでは、すべてのトラフィックが拒否されます。ただし、NAC ポリシー サーバに設定されているポリシーに基づいて有効と見なされたトラフィックは除きます。
- **NAC ポスチャの監視 —** Cisco CP によって、すべてのトラフィックを許可する ACL が適用されます（**permit ip any any**）。NAC 検証プロセス後、ルータでは、特定のホストへのアクセスを拒否するポリシーを NAC サーバから受信する可能性があります。［NAC ポスチャの監視］設定を使用して、ネットワーク上の NAC 設定の影響を判断できます。その後、NAC ポリシー サーバ上のポリシーを変更できます。さらに、Cisco CP Firewall Policy 機能を使用して、インターフェイスに適用される ACL を **deny ip any any** に変更することによって、ルータ上の NAC を、**完全検証**を使用するように再設定できます。

NAC 例外リスト

NAC 検証プロセスの省略を許可する必要があるホストを識別できます。一般的に、プリンタや IP 電話などのホスト、および NAC ポスチャ エージェント ソフトウェアがインストールされていないホストは、例外リストに追加されます。

ネットワーク上にスタティック アドレスがないホストがある場合は、そのホストを NAC 例外リストではなくエージェントレス ホスト ポリシーに入力することをお勧めします。ホスト IP アドレスが変更されると、NAC 例外ポリシーは適切に機能しない場合があります。

NAC ウィザードを使用しており、NAC 例外リストを設定する必要がない場合は、このウィンドウに情報を入力せずに［次へ］をクリックできます。ウィザードでは、NAC 例外リストの代替あるいは補完として、別のウィンドウでエージェントレス ホスト ポリシーを設定できます。

IP アドレス /MAC アドレス / デバイス タイプ、アドレス / デバイス、ポリシー カラム

これらのカラムには、例外リストにあるホストに関する情報が表示されます。ホストは、IP アドレス、MAC アドレス、そのデバイスのタイプによって識別できます。アドレスによって識別される場合は、ネットワークへのホスト アクセスを制御するポリシーの名前とともに、IP アドレスまたは MAC アドレスが行に表示されます。

追加 / 編集 / 削除ボタン

ホストに関する情報を入力して、例外リストを構築するには、［追加］をクリックします。必要に応じて何度でも、［追加］ボタンを使用できます。

ホストに関する情報を変更するには、行を選択して［編集］をクリックします。このウィンドウからホストに関する情報を削除するには、［削除］をクリックします。［編集］と［削除］ボタンは、このリストに情報がない場合は無効になります。

例外リスト エントリの追加、編集

このウィンドウでは、例外リスト エントリの情報を追加または編集します。

タイプ リスト

ホストは、識別される方法に応じて選択されます。このリストには、次の選択肢が含まれています。

- IP アドレス — IP アドレスでホストを識別する場合に選択します。
- MAC アドレス — MAC アドレスでホストを識別する場合に選択します。
- Cisco IP Phone — 例外リストにネット上の Cisco IP Phone を追加する場合に選択します。

アドレスの指定フィールド

ホスト タイプとして IP アドレスまたは MAC アドレスを選択する場合は、このフィールドにアドレスを入力します。デバイス タイプを選択すると、このフィールドは無効になります。

ポリシー フィールド

例外ポリシーの名前がわかっている場合は、このフィールドにその名前を入力します。［ポリシー］フィールドの右にある 3 つのドットがついたボタンをクリックして、既存ポリシーを選択するか、新しいポリシーを作成するためのダイアログ ボックスを表示します。

例外ポリシーの選択

ホストに適用するポリシーを選択します。ポリシーを選択すると、ポリシーに指定したリダイレクト URL が読み取り専用フィールドに表示され、ポリシーのアクセス ルール エントリが表示されます。

使用可能なポリシーがリストにない場合は、［キャンセル］をクリックして、ウィザードの画面に戻ります。その後、ポリシーを追加できるオプションを選択します。

リストから除外されたホストに適用するポリシーを選択します。リストにポリシーがない場合は、［キャンセル］をクリックして、ウィザードに戻ります。その後、［新しいポリシーを作成］を選択して、［例外リストへの追加］ウィンドウでポリシーを選択します。

リダイレクト URL：URL フィールド

この読み取り専用フィールドには、選択したポリシーに関連するリダイレクト URL が表示されます。このポリシーが適用されるホストは、ネットワークにアクセスする際に、この URL にリダイレクトされます。

アクセス ルールのプレビュー

［アクション］、［送信元］、［宛先］、および［サービス］カラムには、ポリシーに関連付けられているアクセス ルールの ACL エントリが表示されます。このポリシーに対して ACL が設定されていない場合は、これらのカラムには何も表示されません。

例外ポリシーの追加

このウィンドウでは、新しい例外ポリシーを作成します。

新しい例外ポリシーを作成するには、ポリシーの名前を入力し、例外リスト内のホストがアクセス可能な IP アドレスを定義するアクセス ルールを指定するか、リダイレクト URL を入力します。リダイレクト URL には、修復情報が含まれている必要があります。修復情報を使用して、ユーザはウィルス定義ファイルを更新できます。アクセス ルール名かリダイレクト URL のいずれかを指定する必要があります。両方を指定することもできます。

名前フィールド

このフィールドには、ポリシーの名前を入力します。ポリシー名には、クエスチョン マーク（?）や空白文字は使用できません。ポリシー名は、256 文字以内にしてください。

アクセス ルール フィールド

使用するアクセス ルール名を入力するか、このフィールドの右側にあるボタンをクリックして、アクセス ルールを参照します。あるいは、新しいアクセス ルールを作成します。アクセス ルールには、例外リストにあるホストが接続できる IP アドレスを指定する許可エントリが含まれている必要があります。アクセス ルールは名前付きの ACL で、番号付き ACL はサポートされていません。

リダイレクト URL フィールド

ネットワークの修復情報が含まれる URL を入力します。この情報には、ウィルス定義ファイルをダウンロードするための指示が含まれている場合があります。

修復 URL は、次のような形式です。

```
http://172.23.44.9/update
```

リダイレクト URL は、通常 `http://URL` または `https://URL` という形式になります。

エージェントレス ホスト ポリシー

エージェントレス ホストのポリシーが Cisco Secure ACS サーバに存在する場合、ルータでは、そのポリシーを使用して、ポスチャ エージェントがインストールされていないホストを制御できます。エージェントレス ホストの制御方法は、NAC 例外リストの代替あるいは補完として使用できます。NAC ウィザードを使用しており、エージェントレス ホスト ポリシーを設定する必要がない場合は、このウィンドウに情報を入力せずに［次へ］をクリックできます。

エージェントレス ホストの認証チェック ボックス

このチェック ボックスを選択して、Cisco Secure ACS サーバ上でエージェントレス ホスト ポリシーを使用することを指定します。

ユーザ名、パスワード フィールド

Cisco IOS ソフトウェア イメージの中には、Cisco Secure ACS サーバへの要求時にユーザ名とパスワードの入力を求めるものがあります。この場合は、Cisco Secure ACS サーバで設定されているユーザ名とパスワードを入力します。Cisco IOS ソフトウェア イメージでこの情報が要求されない場合は、これらのフィールドは表示されません。

リモート アクセスのための NAC の設定

リモート アクセス用に NAC を設定することによって、NAC 設定で作成される ACL を、Cisco CP トラフィックを許可するよう変更できます。Cisco CP を使用してルータにアクセスできるようにしなければならないホストを指定します。

Cisco CP リモート管理を有効化

このチェック ボックスを選択して、名前付きインターフェイスで Cisco CP リモート管理を有効にします。

ホスト / ネットワーク アドレス フィールド

Cisco CP で、単一ホストからの Cisco CP のトラフィックを許可するように ACL が修正されるようにするは、［ホスト アドレス］を選択して、ホストの IP アドレスを入力します。特定のネットワーク上のホストからの Cisco CP のトラフィックが許可されるようにするには、［ネットワーク アドレス］を選択して、そのネットワークとサブネット マスクのアドレスを入力します。ホストやネットワークは、指定したインターフェイスからアクセス可能でなければなりません。指定したインターフェイスに接続されている任意のホストからの Cisco CP のトラフィックが許可されるようにうするには、［任意］を選択します。

ファイアウォールの変更

Cisco CP では、設定された機能が正常に動作するようにするために、この設定で指定されたインターフェイスに適用されている各 ACL がチェックされ、ファイアウォールを通過できる必要のあるいずれかのトラフィックが ACL によってブロックされていないかどうかが確認されます。

各インターフェイスは、現在ブロックされているサービスと、そのサービスをブロックしている ACL とともに一覧表示されます。Cisco CP で、一覧表示されているトラフィックを許可するように ACL が修正されるようにするには、適切な行の［変更］ボックスを選択します。Cisco CP によって ACL に追加されるエントリを確認する場合は、［詳細］ボタンをクリックします。

次の表では、FastEthernet0/0 が NAC に設定されています。このインターフェイスは、［サービス］カラムに表示されているサービスを使用して設定されます。

インターフェイス	サービス	ACL	アクション
FastEthernet0/0	RADIUS サーバ	101 (INBOUND)	[ ]Modify
FastEthernet0/0	DNS	100 (INBOUND)	[ ]Modify
FastEthernet0/0	DHCP	100 (INBOUND)	[ ]Modify
FastEthernet0/0	NTP	101 (INBOUND)	[ ]Modify
FastEthernet0/0	VPN	190 (INBOUND)	[ ]Modify

詳細ウィンドウ

このウィンドウには、設定するサービスに必要なサービスが許可されるようにするため、Cisco CP により ACL に追加されるエントリが表示されます。ウィンドウには、次のようなエントリが含まれます。

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

この場合、ローカル ネットワーク上のホスト 10.77.158.84 からホスト 10.77.158.1 への、ポート番号が 1024 より大きい Web トラフィックが許可されます。

設定の要約

このウィンドウには入力した情報の要約が表示され、単一ウィンドウで確認できます。［戻る］ボタンを使用して任意のウィザード画面に戻り、情報を変更できます。［完了］をクリックすると、ルータに設定が配布されます。

次の例は、NAC 設定の概要です。

```
NAC Interface:  FastEthernet0/1.42
Admission Name::  SDM_EOU_3


AAA Client Source Interface: FastEthernet0/1.40
NAC Policy Server 1:   10.77.158.54

Exception List
-------------------------------------------------------------------------
Address/Device     IP Address       (22.22.22.2) newly added
Policy Details:
Policy Name:          P55
       Redirect URL:  http://www.fix.com
        Access Rule:   test11

-------------------------------------------------------------------------

Enabled agentless host policy
Username:  bill
Password:   ******
```

この例では、RADIUS パケットに FastEthernet 0/1.40 の IP アドレスが含まれます。NAC は FastEthernet 0/1.42 で有効になっており、ウィザードにより適用された NAC ポリシーは SDM_EOU_3 です。例外リストの中に名前の付いたホストが 1 つあり、そのホストからネットワークへのアクセスは、例外ポリシー P55 によって制御されます。

NAC の編集タブ

［NAC の編集］タブでは、ルータに設定されている NAC ポリシーが一覧表示され、他の NAC 設定が可能です。NAC ポリシーは、ポスチャの検証が実行されるインターフェイスごとに設定する必要があります。

NAC タイムアウト ボタン

ルータとクライアントは、Extensible Authentication Protocol over Unformatted Data Protocol（EAPoUDP）を使用してポスチャ情報を交換します。EAPoUDP タイムアウト設定のデフォルト値は事前設定されていますが、変更することもできます。ルータに NAC ポリシーが設定されていない場合は、このボタンは無効になります。

エージェントレス ホスト ポリシー ボタン

エージェントレス ホストのポリシーが Cisco Secure ACS サーバに存在する場合、ルータでは、そのポリシーを使用して、ポスチャ エージェントがインストールされていないホストを制御できます。この方法は、エージェントレス ホストに固有 IP アドレスが割り当てられていない場合に使用できます。ルータに NAC ポリシーが設定されていない場合は、このボタンは無効になります。

追加 / 編集 / 削除ボタン

これらのボタンを使用して、NAC ポリシー リストを管理できます。新しい NAC ポリシーを作成するには［追加］をクリックします。NAC ポリシーを変更または削除するには、［編集］、［削除］ボタンを使用します。ルータに NAC ポリシーが設定されていない場合は、［編集］ボタンや［削除］ボタンが無効になります。

ルータに NAC ポリシーが設定されていない場合は、［追加］ボタンのみが有効です。すべてのルータ インターフェイスが NAC ポリシーを使用して設定されている場合は、［追加］ボタンは無効になります。

NAC ポリシー リスト

このリストには、名前、NAC ポリシーが適用されるインターフェイス、およびポリシーを定義するアクセス ルールが含まれています。NAC の作成ウィザードを使用して、インターフェイス上で NAC を有効にした場合は、デフォルトの NAC ポリシー SDM_EOU_1 がこのリストに表示されます。

NAC コンポーネント

このウィンドウには、Cisco CP を使用して設定できる EAPoUDP コンポーネントの簡単な説明が表示されます。

例外リスト ウィンドウ

この代替トピックは、NAC のヘルプ システムが構築されると削除されます。このヘルプ トピックは、ウィザード モードですでに作成されています。参照する場合は、次のリンクをクリックしてください。

NAC 例外リスト

例外ポリシー ウィンドウ

NAC 例外ポリシーによって、例外リストにあるホストのネットワーク アクセスが制御されます。NAC 例外ポリシーは、名前、アクセス ルール、またはリダイレクト URL から構成されています。アクセス ルールでは、ポリシーによって制御されるホストのアクセス先を指定します。リダイレクト URL がポリシーで指定されている場合は、ポリシーを使用して、利用可能な最新のウィルス保護を入手するための情報が含まれているサイトを Web クライアントに示すことができます。

次の表は、NAC ポリシー エントリの例です。

名前	アクセス ルール	リダイレクト URL
NACLess	nac-rule	http://172.30.10.0/update

NAC ポリシーに関連付けられているアクセス ルールは、拡張 ACL でなければなりません。また名前が付けられている必要があります。次の表は、NAC ポリシーで使用されるアクセス ルールの例です。

アクション	送信元	宛先	サービス	ログ	属性
許可	任意	172.30.2.10	ip		

このルールを使用すると、ポリシーによって制御されるホストは、IP トラフィックを IP アドレス 172.30.2.10 に送信できるようになります。

追加 / 編集 / 削除ボタン

新しい例外ポリシーを作成するには［追加］をクリックします。既存の例外ポリシーを変更するには［編集］ボタンを使用し、例外ポリシーを削除する場合は［削除］ボタンを使用します。リストに例外ポリシーが含まれていない場合は、［編集］、［削除］ボタンは無効になります。

NAC タイムアウト

ルータとネットワーク ホストの EAPoUDP 通信に使用されるタイムアウト値を設定します。次の表は、全設定のデフォルト、最小、最大値です。

値	デフォルト	最小	最大
待機期間のタイムアウト	180 秒	60 秒	86,400 秒
再送信のタイムアウト	3 秒	1 秒	60 秒
再検証のタイムアウト	36,000 秒	300 秒	86,400 秒
ステータス クエリのタイムアウト	300 秒	30 秒	1,800 秒

インターフェイスの選択

NAC タイムアウト設定が適用されるインターフェイスを選択します。

待機期間のタイムアウト フィールド

ルータで認証に失敗したクライアントからのパケットが無視されるまでの秒数を入力します。

再送信のタイムアウト フィールド

ルータで EAPoUDP メッセージがクライアントに再送信されるまでの秒数を入力します。

再検証のタイムアウト フィールド

ルータは、クライアントがセキュリティ ポリシーを遵守しているかどうかを確認するために、クライアントのポスチャ エージェントに定期的に問い合わせます。ルータでクエリを待機する間隔を秒数で入力します。

ステータス クエリのタイムアウト フィールド

ルータでホスト上のポスチャ エージェントに対するクエリを待機する間隔を、秒数で入力します。

デフォルトにリセット ボタン

このボタンをクリックすると、すべての NAC タイムアウトがデフォルト値にリセットされます。

これらのタイムアウト値をグローバルに設定しますチェック ボックス

これらの値をすべてのインターフェイスに適用するには、このチェック ボックスを選択します。

NAC ポリシーの設定

NAC ポリシーは、ルータ インターフェイス上のポスチャの検証プロセスを有効にし、アドミッション コントロール プロセスでのポスチャの検証を免除するトラフィックのタイプを指定するために使用できます。

名前フィールド

ポリシーの名前を入力します。

インターフェイス リストの選択

NAC ポリシーを適用するインターフェイスを選択します。ネットワーク クライアントをルータに接続するインターフェイスを選択します。

アドミッション ルール フィールド

アクセス ルールを使用して、特定のトラフィックをアドミッション コントロール プロセスから免除できます。必須ではありません。アドミッション ルールで使用するアクセス ルールの名前または番号を入力します。このフィールドの右にあるボタンをクリックして、アクセス ルールを参照するか、新しいアクセス ルールを作成することもできます。

アクセス ルールには、拒否のステートメントが含まれている必要があります。拒否のステートメントでは、アドミッション コントロール プロセスから免除されるトラフィックを指定します。アクセス ルールに拒否のステートメントしか含まれていない場合は、ポスチャの検証は実行されません。

次は、NAC アドミッション ルールの ACL エントリの例です。

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any
```

最初の拒否のステートメントでは、宛先がポート 53（ドメイン）のトラフィックを免除し、2 番目のステートメントでは、宛先がポート 80（WWW）のトラフィックを免除します。ACL の最後の許可ステートメントで、ポスチャの検証が必ず実行されます。

その他の手順

以降のトピックでは、NAC の作成ウィザードを使用して行うことのできない設定作業の手順について説明しています。

NAC ポリシー サーバを設定する方法

ルータは、Cisco Secure Access Control Server（ACS）ソフトウェア バージョン 3.3 を実行している ACS に接続している必要があります。ACS は、NAC の実装に RADIUS プロトコルを使用するように設定する必要があります。次のリンクのドキュメントには、設定プロセスの概要が記載されています。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

次のリンクのドキュメントでは、Windows Servers バージョン 3.3 用の Cisco Secure ACS のインストールと設定の方法が説明されています。

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

ホストにポスチャ エージェントをインストールし設定する方法

登録済みの Cisco.com ユーザである場合は、次のリンクから Cisco Trust Agent（CTA）ソフトウェアをダウンロードできます。

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

次のリンクのドキュメントには、ホストへの CTA ソフトウェアのインストールと、その設定方法が説明されています。

http://www.cisco.com/en/US/products/ps5923/tsd_products_support_series_home.html

サードパーティ製のポスチャ エージェント ソフトウェアのインストールに必要なインストール手順とオプションの修復サーバは、使用しているソフトウェアによって異なります。完全な詳細については、ベンダーの資料を参照してください。