CHAPTER 8

ユーザ管理：トラフィック制御、帯域幅、スケジュール

この章では、ロールベースのトラフィック制御ポリシー、帯域幅管理、セッションおよびハートビート タイマーの設定方法について説明します。次の内容について説明します。

ユーザ ロールおよびローカル ユーザの設定の詳細については、第 6 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」を参照してください。

認証サービスの設定に関する詳細は、第 7 章「ユーザ管理：認証サーバの設定」を参照してください。

Web ユーザ ログイン ページの作成および設定の詳細については、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。

概要

さまざまなメカニズムを使用して Clean Access Server（CAS）を通過するインバンド ユーザ トラフィックを制御できます。ここでは、ユーザ ロールごとに設定するトラフィック制御、帯域幅、スケジューリングのポリシーについて説明します。

Cisco NAC アプライアンスを新たに導入した場合、デフォルト システム ロール（Unauthenticated、Temporary、Quarantine）であろうと、作成した新しいユーザ ロールであろうと、デフォルトのままでは信頼ネットワークから非信頼ネットワークへのトラフィックはすべて許可され、非信頼ネットワークから信頼ネットワークへのトラフィックはブロックされます。ただし、非信頼ネットワークからのトラフィックの必要性に応じて、アクセス権を拡大することはできます。

Cisco NAC アプライアンスには、次の 3 種類のトラフィック ポリシーがあります。

IP ベースのポリシー：IP ベースのポリシーは、細かく柔軟な設定が可能であり、さまざまな方法でトラフィックを停止できます。IP ベースのポリシーは、あらゆるロールに適用でき、送信元および宛先のポート番号に加え、IP プロトコル番号も指定できます。たとえば、特定のホストへの IPSec トラフィックを通し、その他のトラフィックは拒否するといった IP ベースポリシーを作成できます。

ホストベースのポリシー：ホストベースのポリシーは、IP ベースのポリシーほど柔軟性はありませんが、ホストに複数の IP アドレスまたはダイナミック IP アドレスがある場合にホスト名またはドメイン名でトラフィック ポリシーを指定できるという利点があります。ホストベースのポリシーは、主に Agent Temporary ロールと Quarantine ロール用のトラフィック ポリシーの設定の簡易化を目的としたものです。このポリシーは、ホストの IP アドレスが常に変化する場合や、ホスト名が複数の IP に解決される可能性がある場合に使用してください。

レイヤ 2 イーサネット トラフィックのポリシー：レイヤ 2 レベルで発生するデータ転送などの処理をサポートするため、Cisco NAC アプライアンス レイヤ 2 イーサネット トラフィック制御ポリシーにより、トラフィックのタイプに基づいて CAS を通るレイヤ 2 イーサネット トラフィックを許可したり拒否したりすることができます。IP、ARP、RARP フレーム以外のネットワーク フレームが、標準のレイヤ 2 トラフィックを構成します。

（注） レイヤ 2 イーサネット トラフィック制御は､バーチャル ゲートウェイ モードで動作する Clean Access Server にだけ適用されます。

トラフィック制御ポリシーはトラフィックの方向別に指定します。IP ベース ポリシーとレイヤ 2 イーサネット トラフィック ポリシーでは、非信頼（管理対象）ネットワークから信頼ネットワークへのトラフィック、または信頼ネットワークから非信頼ネットワークへのトラフィックを許可したり拒否したりできます。ホストベースのポリシーでは、非信頼ネットワークから特定のホストおよび特定の信頼できる DNS サーバへのトラフィックを許可できます。

新しいユーザのロールの作成時、デフォルトでは次のようになります。

- 非信頼ネットワークから信頼ネットワークへのトラフィックはすべてブロックされます。
- 信頼ネットワークから非信頼ネットワークへのトラフィックはすべて許可されます。

ロールに応じて適切なトラフィックを許可するようなポリシーを作成する必要があります。あるいは、特定のマシンへのトラフィックをブロックしたり、ユーザを特定の活動（E メールの使用や Web ブラウジングなど）に制限するようなトラフィック制御ポリシーを設定することもできます。たとえば、次のようなトラフィック ポリシーを作成できます。

`deny access to the computer at 191.111.11.1` や
`allow www communication from computers on subnet 191.111.5/24` など

トラフィック ポリシーのプライオリティ

最終的にトラフィックがどのようにフィルタリングされるかは、ポリシー リスト内のトラフィック ポリシーの順序によって決まります。リストの一番上にある第 1 ポリシーが最も優先されます。非信頼から信頼への方向のトラフィック制御ポリシーがどのように機能するかを、いくつかの例で示します。

例 1:

1. Deny Telnet
2. Allow All

結果：Telnet トラフィックだけがブロックされ、他のトラフィックはすべて許可されます。

例 2（逆のプライオリティ）：

1. Allow All

2. Deny Telnet

結果：すべてのトラフィックが許可され、Telnet トラフィックをブロックするという 2 番目のポリシーは無視されます。

例 3：

1. Allow TCP *.* 10.10.10.1/255.255.255.255
2. Block TCP *.* 10.10.10.0/255.255.255.0

結果：10.10.10.1 への TCP アクセスは許可され、サブネット（10.10.10.*）のその他の場所への TCP アクセスはブロックされます。

例 4（レイヤ 2 イーサネット - バーチャル ゲートウェイ モードのみ）：

1. IBM Systems Network Architecture（SNA; システム ネットワーク アーキテクチャ）を許可
2. すべてのトラフィックを拒否

結果：IBM System Network Architecture（SNA; システム ネットワーク アーキテクチャ）レイヤ 2 トラフィックだけが許可され、その他のレイヤ 2 トラフィックは拒否されます。

グローバルおよび ローカル範囲

この章では、[User Management] > [User Roles] > [Traffic Control] で設定するグローバル トラフィック制御ポリシーについて説明します。[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Roles] で設定するローカル トラフィック制御ポリシーの詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

（注） 特定の Clean Access Server（CAS）を対象としたローカル トラフィック制御ポリシーの方が、プライオリティが高い場合は、グローバル ポリシーよりもローカル ポリシーが優先されます。

[User Management] > [User Roles] > [Traffic Control] のグローバル フォームを使用して追加したトラフィック ポリシーは、Clean Access Manager（CAM）のドメイン内のすべての CAS に適用され、グローバル ページには、白いバックグラウンドで表示されます。

グローバル トラフィック ポリシーは、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Roles] のローカル CAS 用のフォームにも表示されますが、ローカル リストでは、バックグラウンドが黄色になります。

トラフィック制御ポリシーを削除するには、そのポリシーの作成に使用したグローバルまたはローカルのフォームを使用します。

あらかじめ設定されているデフォルトのホストベース ポリシーは、グローバル設定としてすべての CAS に適用され、グローバルとローカルの両方のホストベース ポリシー リストに、黄色のバックグラウンドで表示されます。これらのデフォルト ポリシーは、イネーブルにもディセーブルにもできますが、削除することはできません。詳細については、「デフォルト許可ホストのイネーブル設定」（P.8-10）を参照してください。

グローバル トラフィック制御ポリシーの表示

[User Management] > [User Roles] > [Traffic Control] > [IP] で IP ベースのトラフィック ポリシーを設定するには、[IP] サブタブ リンクをクリックします（図 8-2）。

[User Management] > [User Roles] > [Traffic Control] >[Host] でホストベースのトラフィック ポリシーを設定するには、[Host] サブタブ リンクをクリックします（図 8-7）。

[User Management] > [User Roles] > [Traffic Control] > [Ethernet] でレイヤ 2 イーサネット トラフィックの制御ポリシーを設定するには、[Ethernet] サブタブ リンクをクリックします（図 8-9）。

デフォルトでは、ロール用の IP ベースのトラフィック ポリシーは、トラフィックの送信元として非信頼ネットワーク、宛先として信頼ネットワークが表示されます。反対方向のトラフィックのポリシーを設定するには、送信元から宛先への方向フィールドで [Trusted->Untrusted] を選択し、[Select] をクリックします。

ロールのドロップダウン メニューから選択して、[Select] ボタンをクリックすることにより、すべてのロールの（ALL Roles）または特定のロールの IP、ホストベース、またはレイヤ 2 イーサネットのトラフィック ポリシーを表示できます（図 8-1）。

図 8-1　[Trusted -> Untrusted] 方向フィールド

IP ベースのグローバル トラフィック ポリシー

システム内にすでに存在しているすべてのデフォルト ロール（Unauthenticated、Temporary、Quarantine）のトラフィック ポリシーを設定することができます。通常のログイン ユーザ ロールを作成してから、トラフィック ポリシーを設定する必要があります（第 6 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」を参照）。

ここでは、次の内容について説明します。

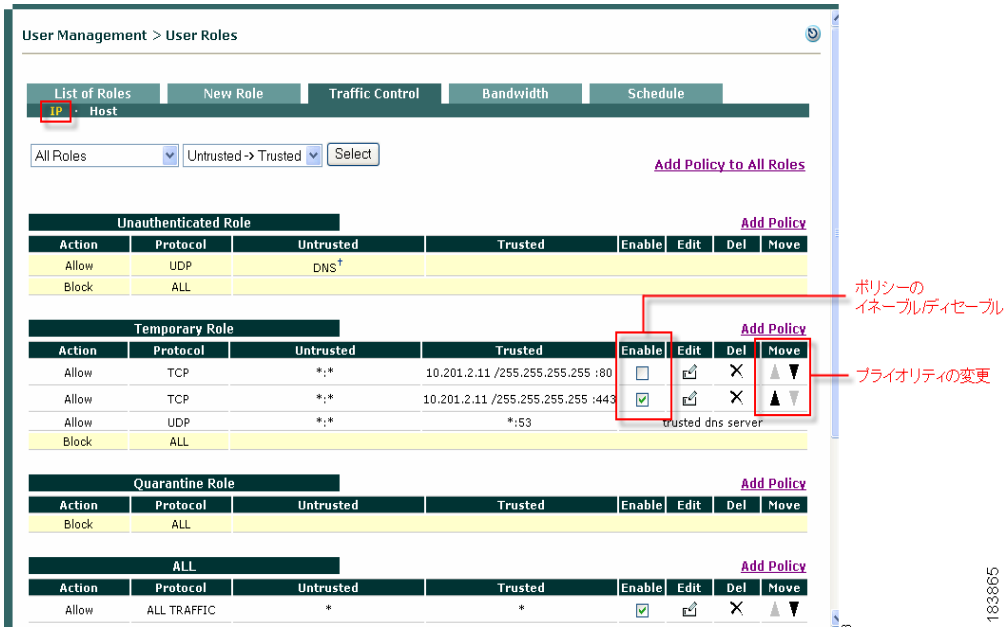
- 「IP ベースのポリシーの追加」（P.8-4）
- 「IP ベースのポリシーの編集」（P.8-8）

IP ベースのポリシーの追加

IP ベースのトラフィック ポリシーを設定する際、個々のポート、ポート範囲、ポートとポート範囲の組み合わせ、またはワイルドカードを指定できます。

1. [User Management] > [User Roles] > [Traffic Control] > [IP] に進みます。すべてのロールの IP ベース ポリシーのリストが表示されます（図 8-2）。

図 8-2　IP ベースのポリシーのリスト

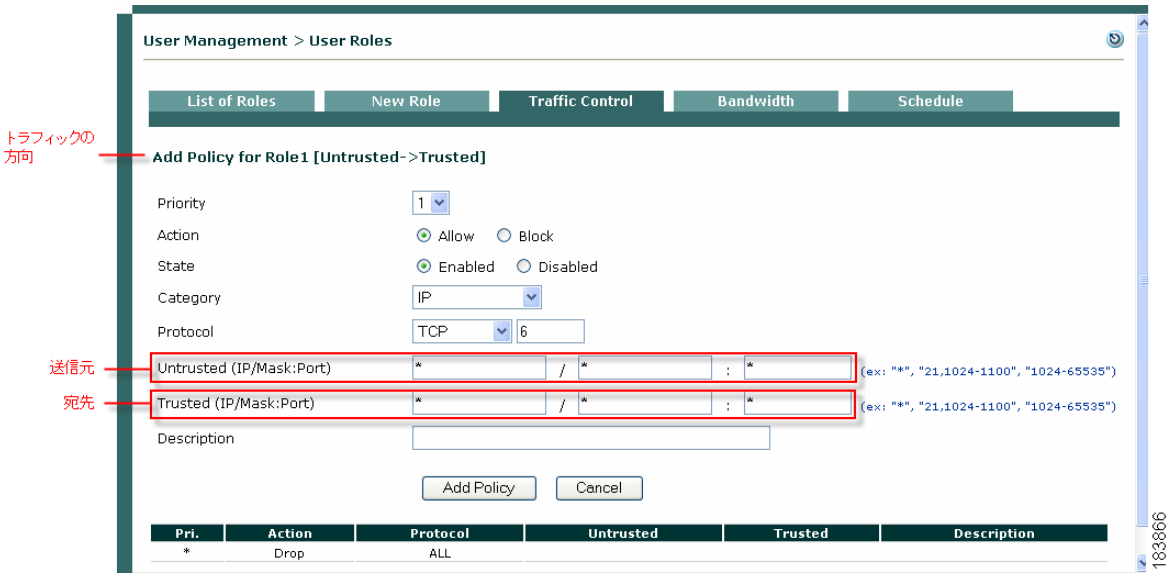


2. そのポリシーに適用する送信元から宛先の方向を選択します。[Trusted->Untrusted] または [Untrusted->Trusted] を選択して、[Select] をクリックします。
3. 特定のロールに新しいポリシーを作成する場合は、該当するユーザ ロールの横にある [Add Policy] リンクをクリックします。また、一度にすべてのロールに新しいポリシーを追加する場合は、[Add Policy to All Roles] をクリックします（Unauthenticated ロールを除く）。

（注）　[Add Policy to All Roles] オプションは、Unauthenticated ロールを除くすべてのロールにポリシーを追加します。追加したトラフィック ポリシーは、ロール単位でだけ、個別の修正や削除が可能です。

4. そのロールの [Add Policy] フォームが表示されます（図 8-3）。

図 8-3　IP ベースのポリシーの追加



5. [Priority] ドロップダウン メニューで、そのポリシーの**プライオリティ**を設定します。実行時には、リストの一番上にある IP ポリシーが最も優先されます。デフォルトでは、最後に作成されたポリシーよりも低いポリシーが表示されます（第 1 ポリシーは 1、第 2 ポリシーは 2 のように表示されます）。リスト内のプライオリティの数は、そのロール用に作成されたポリシーの数に応じて決まります。組み込まれている [Block All] ポリシーは、デフォルトでは、すべてのポリシーの中で最も低いプライオリティに設定されます。

（注） ポリシーの [Priority] をあとで変更する場合は、IP ポリシー リスト ページの [Move] カラムで、そのポリシーの上または下の矢印をクリックします（図 8-2）。

6. [Action] で、そのトラフィック ポリシーの動作を設定します。
   - [Allow]（デフォルト）：トラフィックを許可します。
   - [Block]：トラフィックをドロップします。
7. [State] で、そのトラフィック ポリシーのステートを設定します。
   - [Enabled]（デフォルト）：ロールの新規トラフィックに対してこのトラフィック ポリシーをただちにイネーブルにします。
   - [Disabled]：ロールに対するこのトラフィック ポリシーをディセーブルにしますが、今後使用する場合に備えてこのポリシーの設定を保持します。

（注） ロール レベルでトラフィック ポリシーをイネーブルまたはディセーブルにするには、IP ポリシー リスト ページの [Enable] カラムにある対応するチェックボックスをオンにします（図 8-2）。

8. [Category] で、そのトラフィックのカテゴリを設定します。
   - [ALL TRAFFIC]（デフォルト）：このポリシーは、すべてのプロトコルの、信頼側および非信頼側のすべての送信元および宛先アドレスに適用されます。
   - [IP]：これを選択すると、[Protocol] フィールドが表示されます（後述の説明を参照）。

- [IP FRAGMENT]：デフォルトでは、Clean Access Manager は IP 断片化パケットをブロックします。このようなパケットは DoS 攻撃に使用される可能性があるからです。断片化されたパケットを許可する場合は、このオプションを使用して、そのようなパケットを許可するロール ポリシーを定義してください。

9. [IP] カテゴリを選択した場合は、次のオプションとともに [Protocol] フィールドが表示されます。
   - [CUSTOM] : [Protocol] ドロップダウン メニューに表示されているプロトコル以外のプロトコル番号を指定する場合は、このオプションを選択します。
   - [TCP (6)] : TCP の場合に選択します。TCP アプリケーションには、HTTP、HTTPS、Telnet が含まれます。
   - [UDP (17)] : 通常、ブロードキャスト メッセージに使用される UDP を設定する場合に選択します。
   - [ICMP (1)] : Internet Control Message Protocol（ICMP）の場合に選択します。ICMP を選択する場合は、ドロップダウン メニューから [Type] も選択してください。
   - [ESP (50)] : 主に VPN トンネルを構築する目的で IP パケット データの暗号化に使用される IPSec サブプロトコルである Encapsulated Security Payload（ESP）を設定する場合に選択します。
   - [AH (51)] : IP ヘッダーおよびパケットの認証を保証するために暗号チェックサムの計算に使用される IPSec サブプロトコルである Authentication Header（AH）を設定する場合に選択します。
10. [Untrusted (IP/Mask:Port)] フィールドで、そのポリシーを適用する非信頼ネットワークの IP アドレスとサブネット マスクを指定します。[IP/Mask:Port] フィールドのアスタリスクは、そのポリシーがあらゆるアドレス/アプリケーションに適用されることを意味しています。
    [Protocol] で [TCP] または [UDP] を選択した場合は、[Port] テキスト フィールドに、そのアプリケーションの TCP/UDP ポート番号も入力してください。

（注）　TCP/UDP ポートの設定に、個々のポート、ポート範囲、ポートとポート範囲の組み、またはワイルドカードを指定できます。たとえば、ポート値を、「*****」、「**21, 1024-1100**」、または「**1024-65535**」のように指定して、1 つのポリシーで複数のポートに対応させることができます。TCP/UDP ポート番号に関する詳細は、http://www.iana.org/assignments/port-numbers を参照してください。

11. [Trusted (IP/Mask:Port)] フィールドで、そのポリシーを適用する信頼ネットワークの IP アドレスとサブネット マスクを指定します。[IP/Mask:Port] フィールドのアスタリスクは、そのポリシーがあらゆるアドレス/アプリケーションに適用されることを意味しています。[Protocol] で [TCP] または [UDP] を選択した場合は、[Port] テキスト フィールドに、そのアプリケーションの TCP/UDP ポート番号も入力してください。

（注）　ポリシー リストを表示する際に選択したトラフィックの方向（[Untrusted -> Trusted] または [Trusted -> Untrusted]）によって、[Add Policy] フォームを開いたときの送信元と宛先が設定されます。

- 表示される最初の IP/Mask/Port エントリは送信元です。
- 表示される 2 番目の IP/Mask/Port エントリは宛先です。

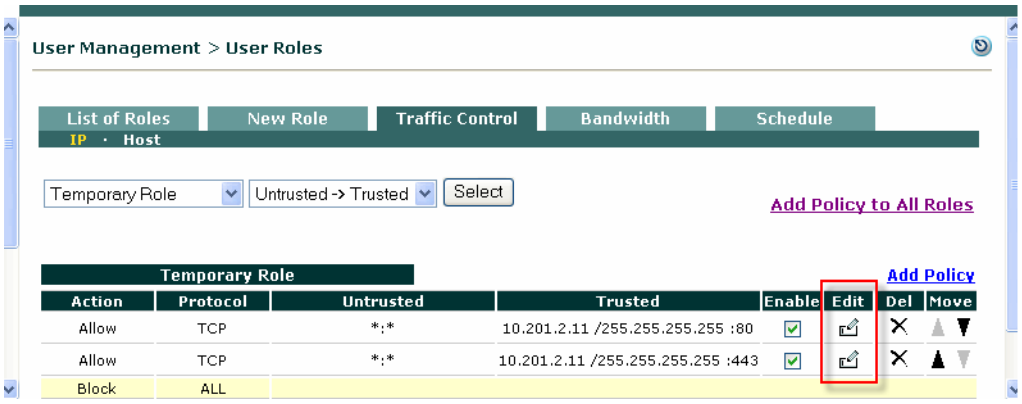
12.（任意）[Description] フィールドにそのポリシーの説明を入力します。

13. 完了したら、[Add Policy] をクリックします。ポリシーを変更した場合は、[Update Policy] ボタンをクリックします。

IP ベースのポリシーの編集

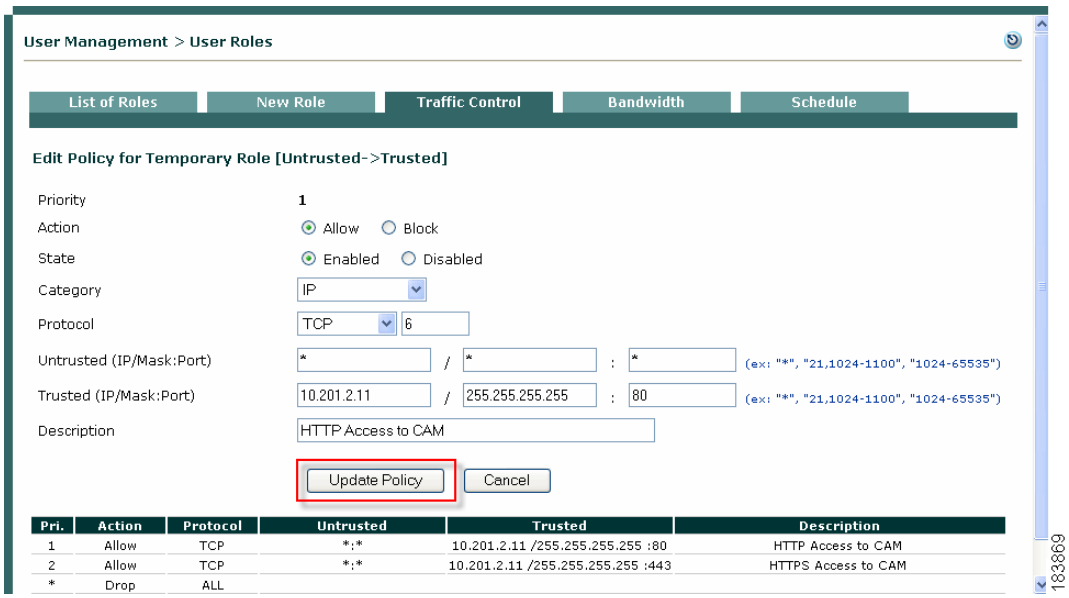
1. [User Management] > [User Roles] > [Traffic Control] > [IP] に進みます。
2. 変更するロール ポリシーの [Edit] ボタンをクリックします（図 8-4）。

図 8-4　　IP ポリシーの編集



3. そのロール ポリシーの [Edit Policy] フォームが表示されます（図 8-5）。

図 8-5　　IP ポリシー編集用のフォーム



4. 目的に応じてプロパティを変更します。

（注） TCP/UDP ポート用に「*****」、「**21, 1024-1100**」、または「**1024-65535**」のように、個々のポート、ポート範囲、ポートとポート範囲の組み合わせ、またはワイルドカードを指定できます。TCP/UDP ポートに関する詳細は、http://www.iana.org/assignments/port-numbers を参照してください。

5. 完了したら、[Update Policy] をクリックします。

[Edit] フォームから直接、ポリシー プライオリティを変更することはできません。[Priority] の値を変更する場合は、IP ポリシー リスト ページの [Move] カラムで、そのポリシーの上または下の矢印をクリックします。

ホストベースのグローバル トラフィック ポリシーの追加

CAM から Agent の **Update** または **Clean Update** が実行されると、Unauthenticated、Temporary、Quarantine のロールのデフォルト ホスト ポリシーが自動的に取得され、更新されます（更新に関する詳細については、「Cisco NAC アプライアンスのアップデートの取得」（P.9-12）を参照してください）。

ホストに複数の IP アドレスまたはダイナミック IP アドレスがある場合は、ホスト名またはドメイン名でロールのカスタム DNS ホストベース ポリシーを設定することが可能です。ホストベースのポリシーを設定し、すべての IP アドレスを解決すると、すべてのタイプのトラフィックがホスト マシンに対してイネーブルになります。

ユーザ ロールごとに DNS アドレスを設定できるので、クライアントが Clean Access Agent の条件を満たしていない場合やネットワーク スキャンで脆弱性が発見された場合に、システムの修正を目的として Windows やアンチウイルス ソフトの更新サイトへクライアントがアクセスするのを許可できます。ホストベースのポリシーを使用する場合は、まず、そのユーザ ロールに対応する信頼できる DNS サーバを追加しなければなりません。

（注）

- ソフトウェアのアップグレード後、デフォルトの設定では、新しいデフォルト ホストベース ポリシーはディセーブルになりますが、既存のホストベース ポリシーのイネーブル/ディセーブル設定は以前のまま変更されません。
- Clean Update を実行すると、既存のすべてのデフォルト ホストベース ポリシーが削除され、新しいデフォルト ホストベース ポリシーがディセーブルのデフォルト設定のまま追加されます。

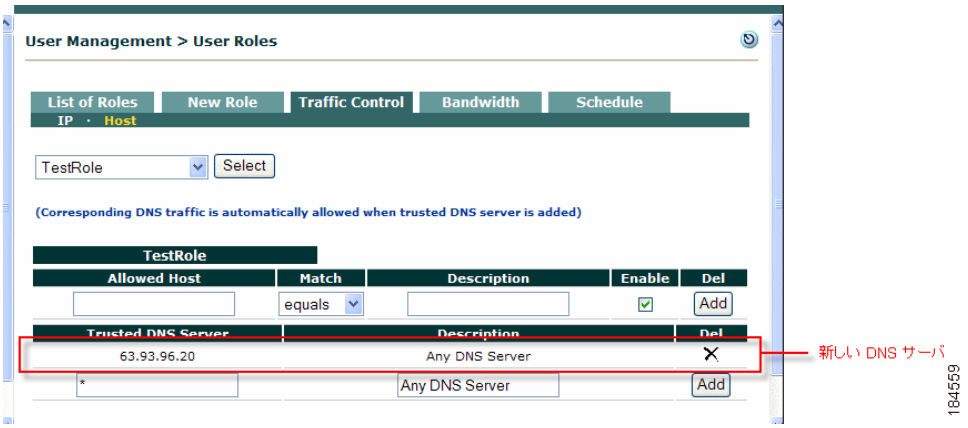
ここでは、次の内容について説明します。

ロール別の信頼 DNS サーバの追加

あるロールのホストベース トラフィック ポリシーをイネーブルにするには、そのロールの信頼 DNS サーバを追加する必要があります。

1. [User Management] > [User Roles] > [Traffic Control] に進み、[Host] リンクをクリックします。
2. 信頼 DNS サーバを追加するロールを選択します。
3. [Trusted DNS Server] フィールドに IP アドレスを入力します。あるいは、すべての DNS サーバを指定する場合は、アスタリスク「*」を入力します。

図 8-6　信頼 DNS サーバの追加



4. （任意）[Description] フィールドに、DNS サーバの説明を入力します。
5. [Enable] チェックボックスはすでに選択されています。
6. [Add] をクリックします。新しいポリシーが [Trusted DNS Server] カラムに表示されます。

（注）
- 信頼 DNS サーバが [Host] フォームに追加されると、そのサーバへの DNS/UDP トラフィックを許可する IP ベースのポリシーが自動的にそのロールに追加されます（[IP] フォーム）。
- 特定の DNS サーバを追加してから、そのロールにあらゆる（「*」）DNS サーバを追加すると、前に追加したサーバはすべての DNS サーバを許可する全体ポリシーのサブセットになり、表示されなくなります。後で、すべての（「*」）DNS サーバのポリシーを削除すると、以前に許可した特定の信頼 DNS サーバが再び表示されるようになります。

デフォルト許可ホストのイネーブル設定

Cisco NAC アプライアンスには、Unauthenticated、Temporary、および Quarantine のロール用のデフォルト ホスト ポリシーがあります。初期状態ではデフォルトのホスト ポリシーがシステムに設定されていますが、Cisco NAC アプライアンスの **Update** または **Clean Update** を実行することにより、動的に更新されます。新たに追加されたデフォルト ホスト ポリシーは、デフォルトではディセーブルに設定されるため、[User Management] > [User Roles] > [Traffic Control] > [Hosts] で、各ロールに対してイネーブルに設定する必要があります。

ユーザ ロール用にデフォルト ホスト ポリシーをイネーブル設定

ステップ 1　[Device Management] > [Clean Access] > [Updates] に移動します。（図 9-6（P.9-16）を参照）。

ステップ 2　[Update] をクリックするか、Cisco NAC アプライアンスのアップデートに伴う最新のデフォルト ホスト ポリシーが取得されます。デフォルト ホスト ポリシーをアップデートしても、既存のデフォルト ホスト ポリシーのユーザ定義設定は上書きされません。

ステップ 3　[User Management] > [User Roles] > [Traffic Control] > [Host] に移動します。（図 8-7（P.8-11）を参照）。

ステップ 4　デフォルト ホスト ポリシーをイネーブルにするロール（Unauthenticated、Temporary、または Quarantine）をドロップダウン メニューから選択し、[Select] を選択します。

ステップ 5　そのロールに許可する各デフォルト ホスト ポリシーの [Enable] チェックボックスをクリックします。

ステップ 6　信頼 DNS サーバが追加されていることを確認します（「ロール別の信頼 DNS サーバの追加」（P.8-9）を参照）。

ステップ 7　その他のカスタム ホストをロールに追加する場合は、「許可ホストの追加」（P.8-11）の手順で行います。

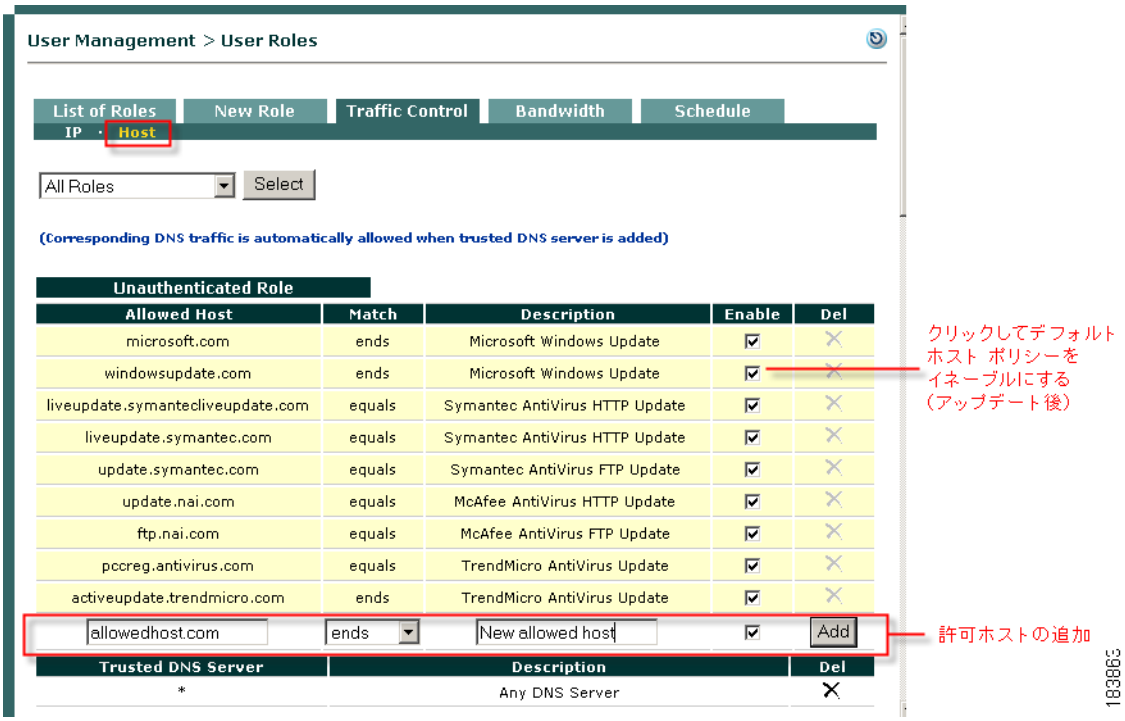
（注）　更新の設定に関する詳細は、「Cisco NAC アプライアンスのアップデートの取得」（P.9-12）を参照してください。

許可ホストの追加

許可ホスト フォームを使用すると、デフォルト ロール用のデフォルト ホスト ポリシーに他の更新サイトを追加したり、任意のユーザ ロール用にカスタム ホストベース トラフィック ポリシーを作成することができます。

1. [User Management] > [User Roles] > [Traffic Control] に進み、[Host] リンクをクリックします。

図 8-7　許可ホストの追加



2. DNS ホストを追加するロールを選択します。
3. [Allowed Host] フィールドにホスト名を入力します（「allowedhost.com」など）。
4. [Match] ドロップダウン メニューで、ホスト名の照合に使用する演算子を選択します（equals、ends、begins、または contains）。
5. [Description] フィールドに、そのホストの説明を入力します（「Allowed Update Host」など）。
6. [Enable] チェックボックスはすでに選択されています。

7. [Add] をクリックします。新しいポリシーが [Add] フィールドの上に表示されます。

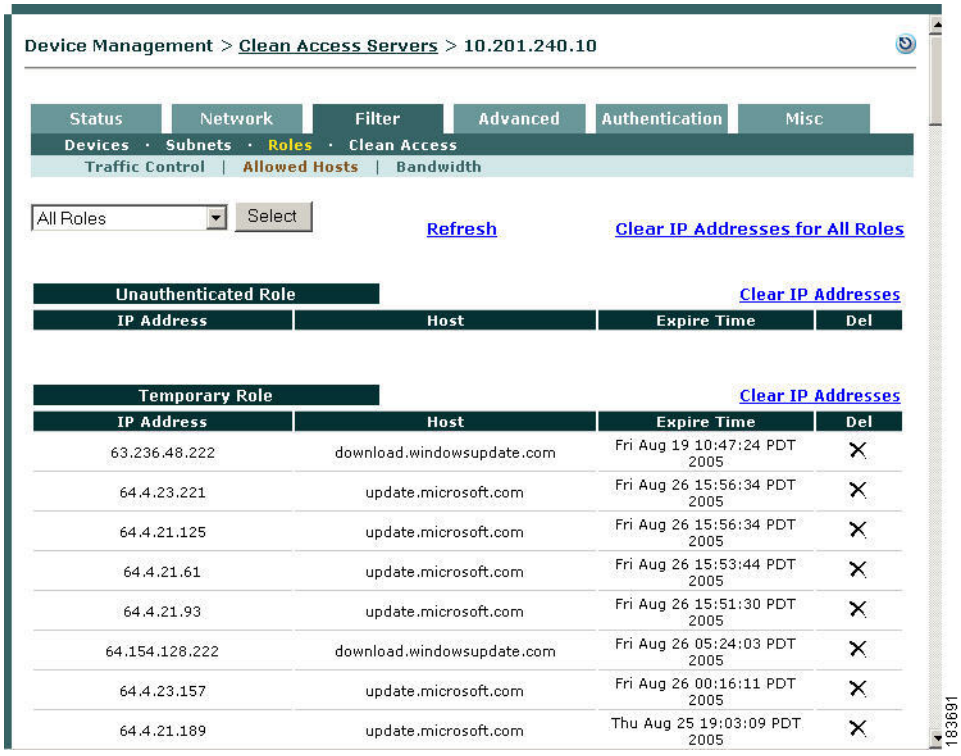
（注）　ロールのホストベース トラフィック ポリシーをイネーブルにするには、そのロールに信頼できる DNS サーバを追加する必要があります。

DNS ホストに使用される IP アドレスの表示

クライアントがシステムを更新するために DNS ホストに接続するときに、その DNS ホストに使用される IP アドレスを表示することができます。このような IP アドレスは、Clean Access Server 管理ページに CAS 別に表示されることに注意してください。

1. [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Roles] > [Allowed Hosts] の順番に進みます。
2. すべてのロールでアクセスされる DNS ホストのすべての IP アドレスを表示するには、このページの上部に表示されている [View Current IP addresses for All Roles] をクリックします。
3. 特定のロールのクライアントがアクセスする DNS ホストの IP アドレスを表示する場合は、該当するロールの横にある [View Current IP addresses] リンクをクリックします。
4. アクセスされる各 IP アドレスの [IP Address]、[Host Name]、および [Expire Time] が表示されます。[Expire Time] には、DNS reply TTL に基づく値が表示されます。その DNS ホストの IP アドレスは、[Expire Time] の値に到達すると無効になります。

図 8-8　すべてのロールの現在の IP アドレスの表示



ヒント　ホストベースのポリシー アクセスに問題が生じた場合は、テスト用のクライアント マシンのコマンド プロンプトから **ipconfig /flushdns** を実行してみてください。Cisco NAC アプライアンスは、該当する IP アドレスを許可リストに入れる前に DNS 応答を必要とします。

プロキシ サーバとホスト ポリシー

CAS で指定されたプロキシ サーバが使用される場合、ユーザ（たとえば、要件を満たす必要のある Temporary ユーザまたは Quarantine ユーザ）がロールでイネーブルにされているホスト サイトにだけアクセスできるようにできます。

プロキシ設定は CAS 管理ページを使用して CAS で設定されたローカル ポリシーであり、この機能をイネーブルにするには次のページを設定する必要があることに注意してください。

- [Device Management] > [Clean Access Servers] > [Manage [CAS_IP]] > [Advanced] > [Proxy]
- [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Roles] > [Allowed Hosts]
  （[Parse Proxy Traffic] オプションがイネーブルに設定されている必要があります）

詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

また、「プロキシの設定」（P.5-3）も参照してください。

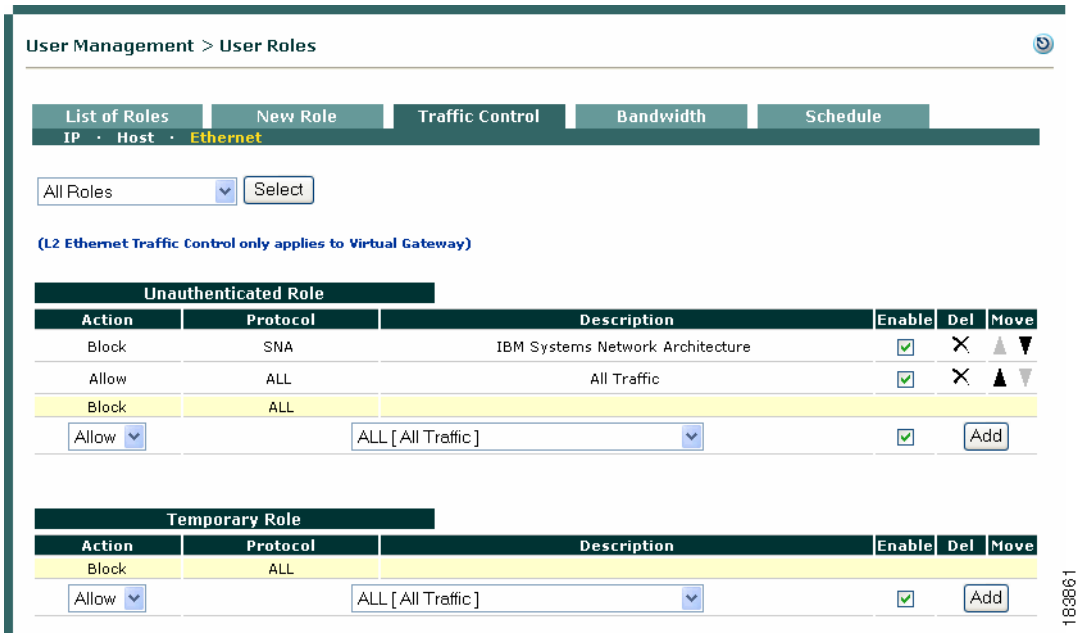
グローバル レイヤ 2 イーサネット トラフィック ポリシーの追加

（注）　レイヤ 2 イーサネット トラフィック制御は、レイヤ 2 イーサネット制御が CAS 設定ページでイネーブルになっているバーチャル ゲートウェイ モードで動作する Clean Access Server にだけ適用されます。

システム内にすでに存在しているすべてのデフォルト ロール（Unauthenticated、Temporary、Quarantine）のトラフィック ポリシーを設定することができます。通常のログイン ユーザ ロールを作成してから、トラフィック ポリシーを設定する必要があります（第 6 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」を参照）。

1. [User Management] > [User Roles] > [Traffic Control] > [Ethernet] の順番に進みます。全ロールのレイヤ 2 イーサネット トラフィック制御ポリシーのリストが表示されます（図 8-2）。

図 8-9　　レイヤ 2 イーサネット トラフィック制御ポリシー



2. [Action] ドロップダウン メニューで、[Allow] または [Block] を選択します。
3. [Protocol] ドロップダウン メニューで、許可または拒否するレイヤ 2 イーサネット トラフィックのタイプを指定します。

（注）　すべてのレイヤ 2 トラフィックを許可する場合を除いて、「IBM Systems Network Architecture（SNA）」プロトコルだけが Cisco NAC アプライアンスで利用できます。追加のプリセット オプションについては、CAM の Cisco NAC アプライアンス アップデート サービスを通じて今後のリリースで利用可能になる予定です。

4. [Enable] をクリックします。
5. [Add] をクリックします。

トラフィック制御ポリシーを追加すると、エントリの [Description] カラムに、[Protocol] ドロップダウン メニューで指定したオプションの説明が自動的に読み込まれます。

帯域利用の制御

Cisco NAC アプライアンスを使用すると、ユーザが使用できるネットワーク帯域幅をロール別に制御できます。CAM のグローバル フォームを使用すれば必要に応じてシステム ユーザ ロールに帯域管理を設定できます。また、ローカル フォームを使用すれば、一部の CAS だけに帯域管理を設定することも可能です。ただし、この機能を使用するためには、まず CAS でこのオプションがイネーブルに設定されている必要があります。さらに、個々のロールまたはロール全体の各ユーザに対する帯域幅制限も指定できます。

たとえば、1 つの CAM で 2 つの CAS を管理している場合、すべてのロールを指定することも、必要に応じて一部のロール（Guest ロール、Quarantine ロール、Temporary ロールなど）に帯域幅管理を設定することもできます。帯域幅が重要なのは CAS1 が配置されているネットワーク セグメントだけで、CAS2 が配置されているネットワーク セグメントでは帯域幅を重要視する必要がないのであれば、CAS1 では帯域管理を有効にし、CAS2 では有効にしないといった設定方法も可能です。

また、バースト時に、帯域幅制限からのわずかな逸脱を許可することもできます。これによって、ユーザによるコンテンツのストリーミングや大きなファイルの転送は帯域制限の対象としながら、断続的に帯域リソースを必要とするユーザ（たとえば、ページのダウンロードや閲覧時）に対応することができます。

デフォルトでは、ロールの帯域ポリシーは無制限になります（アップストリーム トラフィックとダウンストリーム トラフィックでは両方とも -1 に指定）。

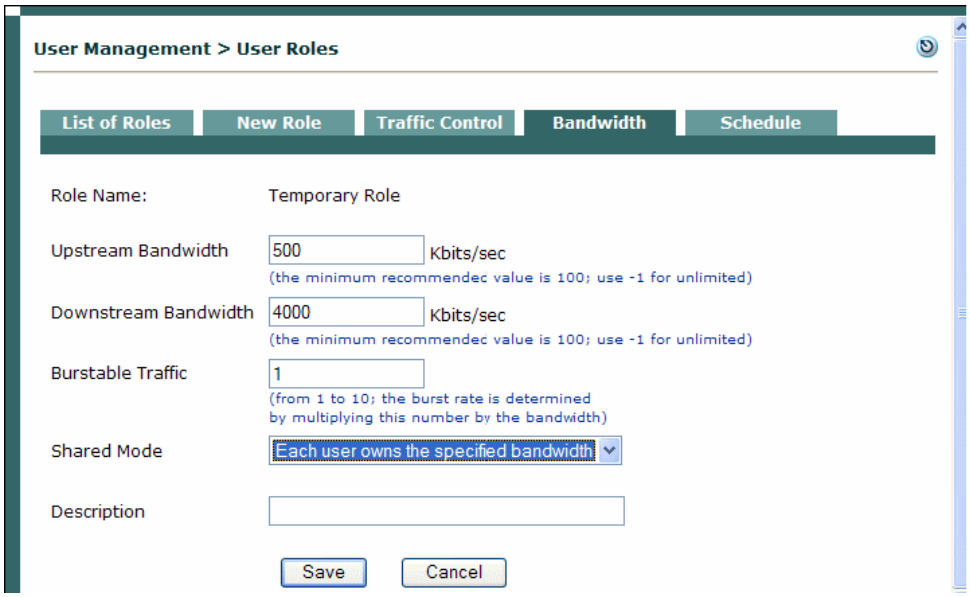
ロールの帯域幅の設定

1. まず、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Roles] > [Bandwidth] に進み、その CAS で帯域幅管理をイネーブルにします。
2. [Enable Bandwidth Management] を選択し、[Update] をクリックします。

（注）　ローカル帯域幅の管理の詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

3. [User Management] > [User Roles] > [Bandwidth] から、帯域幅の制限を設定するロールの横にある [Edit] ボタンをクリックします。次の図のように、[Bandwidth] フォームが表示されます。

図 8-10　User ロール用の [Bandwidth] フォーム



（注）　あるいは、[User Management] > [User Roles] > [List of Roles] に進み、該当ロールの横の [BW] ボタンをクリックする方法でも設定できます。

4. [Upstream Bandwidth] および [Downstream Bandwidth] に、アップストリーム トラフィックとダウンストリーム トラフィックの最大帯域幅をキロビット/秒単位で設定します。アップストリーム トラフィックは、非信頼ネットワークから信頼ネットワークへのトラフィックです。ダウンストリーム トラフィックは、信頼ネットワークから非信頼ネットワークへのトラフィックです。
5. [Burstable Traffic] に、帯域制限からの短時間（1 秒間）の逸脱を許可するレベルとして、2 ～ 10 の値を入力します。[Burstable Traffic] にレベル 1 を設定すると、バースト トラフィックをディセーブルにする効果があります。

   [Burstable Traffic] フィールドは、バケットの「容量」を判断するために使用されるトラフィック バースト係数です。たとえば、帯域幅が 100 Kbps で、[Burstable Traffic] フィールドが 2 の場合、そのバケットの容量は 100Kb*2=200Kb です。あるユーザが一定時間に 1 つもパケットを送信しなかった場合、そのユーザのバケットには最大で 200 Kb のトークンが入ります。そのユーザがパケットを送信する必要が生じた場合、そのユーザはすぐに 200 Kb のパケットを送信できます。その後、そのユーザが追加パケットを送信する場合は、100 Kbps のレートでトークンが来るのを待たなければなりません。これは、平均レートが 100 Kbps で、ピーク レートは約 200 Kbps であると考えることもできます。つまり、これは、Web ブラウズのようなバースト アプリケーションの使用に対応することを目的とした機能なのです。
6. [Shared Mode] フィールドで、次のいずれかを選択します。
   - [All users share the specified bandwidth]：この設定値は、そのロールのすべてのユーザに適用されます。この場合、設定された値が使用可能な総帯域幅になります。つまり、あるユーザが使用可能な帯域幅の 80 %を占有した場合、そのロールの他のユーザは残りの 20 %の帯域幅しか使用できません。
   - [Each user owns the specified bandwidth]：この設定値は、各ユーザに適用されます。使用中の総帯域幅は、そのロールのオンライン ユーザの数の増減によって変化しますが、各ユーザの帯域幅は同じです。
7. （任意）[Description] にその帯域設定値の説明を入力します。
8. 完了したら、[Save] をクリックします。

この帯域設定は、該当ロールに適用され、[Bandwidth] タブに表示されます。

（注）　帯域幅の管理がイネーブルになっている場合、ロールを指定せずにデバイス フィルタを通じて許可されたデバイスには、Unauthenticated ロールの帯域幅が使用されます。詳細については、「デバイスおよびサブネットのグローバル フィルタリング」（P.2-10）を参照してください。

ユーザ セッション タイムアウトおよびハートビート タイムアウトの設定

タイムアウト プロパティは、設定時間経過後にユーザ セッションを終了させることにより、ネットワーク セキュリティを強化します。自動ユーザ タイムアウトの主なメカニズムは次の 3 つです。

- セッション タイマー
- ハートビート タイマー
- 証明済みデバイス タイマー（「証明済みデバイス タイマーの設定」（P.11-14）を参照）

ここでは、セッション タイマーとハートビート タイマーについて説明します。

セッション タイマー

セッション タイマーは、ユーザ ロール固有の絶対的なタイマーです。あるロールにセッション タイマーが設定されると、そのロールに属すユーザのセッションは、セッション タイマーに設定された時間だけしか持続できません。セッション タイマーの値は組み込みで 5 分に設定されています。この値が、ユーザ ロール専用に設定されたセッション タイムアウト値に加えられます。「設定されたセッション タイムアウト値 + 組み込みの 5 分間」が経過すると、ユーザ ロールに対応するユーザ セッションがクリアされます。たとえば、ユーザ A が 1:00pm にログインし、ユーザ B が 1:30pm にログインし、両者ともセッション タイマーが 115 分に設定されている Test ロールに属している場合、ユーザ A は 3:00pm に、ユーザ B は 3:30pm にログアウトされます。セッション タイムアウトが設定されていると、接続状態やアクティビティに関係なく、ユーザはドロップされます。

（注） RADIUS サーバを設定している場合、ユーザ ログインの RADIUS セッション タイムアウトは自動的にイネーブルになります。このため、タイムアウト時間は、RADIUS サーバに設定されているユーザ プロファイルに基づいてユーザ ベースに発生します。Cisco NAC アプライアンスで RADIUS サーバ認証をイネーブルにする場合の詳細については、「RADIUS」（P.7-6）を参照してください。

ハートビート タイマー

ハートビート タイマーでは、Clean Access Server からの ARP クエリに応答しない場合、ユーザが何分後にネットワークからログオフされるかを設定します。この機能によって、CAS は、ネットワークからログオフせずにネットワークから去った（マシンのシャットダウンやサスペンドによって）ユーザを検出し、切断できます。ハートビート タイマーは、ローカル認証か外部認証かに関係なく、すべてのユーザに適用される点に注意してください。

接続の確認は、ping ではなく、ARP クエリで実行されます。これによって、ICMP トラフィックがブロックされていても、ハートビート チェックは機能します。CAS には、その非信頼側の ARP テーブルが維持されており、そのテーブルには、CAS が非信頼側で認識した、またはクエリを送信したすべてのマシンが含まれています。特定のマシンからのパケットが検出されないと、通常の ART キャッシュ タイムアウトを通じて、そのマシンの ARP エントリはタイムアウトになります。パケットが検出されれば、そのマシンのエントリには、fresh のマークが付きます。CAS の ARP キャッシュに完全に解決されたエントリがなく、ハートビート タイマーの設定時間のあいだ ARP に応答しないマシンは、ネットワーク上には存在しないと見なされ、そのマシンのセッションは終了します。

インバンド（L2）セッション

インバンド構成の場合、ユーザ セッションはクライアントの MAC アドレスと IP アドレスに基づいて確立され、次のいずれかが発生するまで持続します。

- Web ユーザ ログアウト ページまたは Agent ログアウト オプションを通じてユーザがネットワークからログアウトした場合
- 管理者がそのユーザを手動でネットワークから削除した場合
- そのユーザ ロールのセッション タイマーの設定に従ってセッション タイムアウトが発生した場合
- CAS がハートビート タイマーを使用して、そのユーザが接続されていないと判断し、CAM がそのセッションを終了した場合
- Certified Device リストが消去され（自動または手動で）、そのユーザがネットワークから削除された場合

OOB（L2）およびマルチホップ（L3）のセッション

セッション タイマーは、マルチホップ L3 インバンド配置の場合も、L2（インバンドまたはアウトオブバンド）配置の場合と同様に機能します。

L3 配置の場合、ユーザ セッションは MAC アドレスではなく、固有の IP アドレスに基づいて確立されます。

ハートビート タイマーは、L2 配置に加えて L3 配置の非アクティブ/アイドル タイマーとして動作します。L3 配置の場合、タイマーでのハートビートは次のケースで説明されているように動作します。

- **ルータがプロキシ ARP を実行しない L3 配置**

  Clean Access Server でハートビート タイマーが設定された期間ユーザからのパケットが検出されない場合、ユーザはログアウトされます。ユーザのマシンがネットワークに接続されていても CAS に到達するネットワーク上で 1 つもパケットを送信していない場合、ログアウトされます。ユーザがアクティブになっていない場合でも、現在のシステムは多くのパケットを送信するので（チャット プログラム、Windows アップデート、AV ソフトウェア、Web ページの広告など）、このようなことは滅多にありません。

- **ルータ /VPN コンセントレータがネットワーク上の IP アドレスのプロキシ ARP を実行している L3 配置**

  このシナリオでは、デバイスがネットワークに接続されている場合、ルータはデバイスの IP アドレスのプロキシ ARP を実行します。そうでない場合、デバイスがネットワークに接続されていないと、ルータはプロキシ ARP を実行しません。一般的に、VPN コンセントレータだけがこのように動作します。この場合、Clean Access Server サーバでパケットが検出されないと、CAM/CAS がユーザの ARP を実行しようとします。プロキシ ARP のためルータが CAS に応答すると、CAM/CAS はユーザをログアウトしません。そうでない場合、デバイスがネットワーク上になくなったためにルータが CAS に応答しないと、CAM/CAS はユーザをログアウトします。

- **ルータ /VPN コンセントレータがサブネット全体のプロキシ ARP を実行している L3 配置**

  このシナリオでは、個別デバイスの接続の有無に関係なくルータ /VPN コンセントレータはプロキシ ARP を実行します。この場合、ハートビート タイマーの動作は変更されず、CAM/CAS はユーザをログアウトしません。

（注）

- ハートビート タイマーはアウトオブバンド ユーザには適用されません。
- マルチホップ L3 VPN コンセントレータ統合構成で SSO（シングルサインオン）機能が設定されている場合、CAS でユーザのセッションがタイムアウトになっても、そのユーザがまだ VPN コンセントレータにログインしたままであれば、SSO によってそのユーザはユーザ名 / パスワードを指定せずに CAS にログバックできます。

セッション タイマーとハートビート タイマーの相互作用

- セッション タイマーがゼロに設定されていて、ハートビート タイマーが設定されていない場合、ユーザは Online Users リストから削除されず、再ログインを要求されません。
- セッション タイマーがゼロに設定されていて、ハートビート タイマーが設定されている場合は、ハートビート タイマーが有効になります。
- セッション タイマーがゼロ以外に設定されていて、ハートビート タイマーが設定されていない場合は、セッション タイマーが有効になります。
- 両方のタイマーが設定されている場合は、到達した最初のタイマーが最初にアクティブになります。

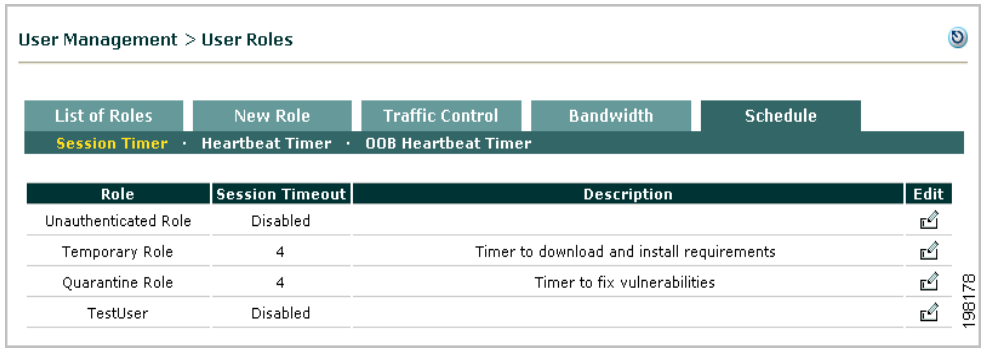
- ユーザがログアウトしてマシンをシャットダウンすると、そのユーザは Online Users リストから削除され、再ログインが必要となります。
- DHCP リース時間がセッション タイムアウトより大幅に長い場合、DHCP リースは効果的に再利用されません。

詳細については、「アクティブ ユーザの意味」（P.11-29）を参照してください。

セッション タイマーの設定（ユーザ ロール単位）

ステップ 1　[User Management] > [User Roles] > [Schedule] > [Session Timer] の順番に進みます。

図 8-11　　セッション タイマー



ステップ 2　タイムアウト値を設定するロールの横にある [Edit] ボタンをクリックします。

ステップ 3　[Session Timeout] チェックボックスをオンにし、分単位で時間を入力します。設定した時間後にユーザ セッションはタイムアウトになります。タイムアウト クロックは、ユーザのアクティビティには関係なく、ユーザのログイン時に開始されます。セッション期限の経過後もネットワークの使用を続けるユーザは、ネットワークに再度ログインしなければなりません。

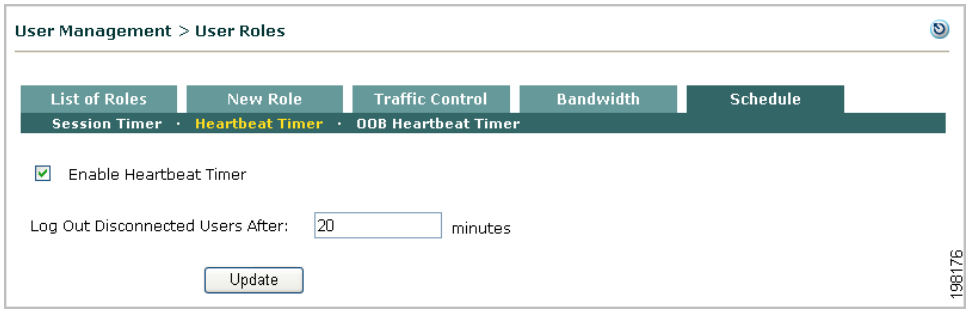
ステップ 4　（任意）[Description] フィールドに、そのセッション時間制限の説明を入力します。

ステップ 5　完了したら、[Update] をクリックします。

ハートビート タイマー（ユーザ非アクティブ タイムアウト）の設定

ステップ 1　[Schedule] タブで、[Heartbeat Timer] フォームを開きます。

図 8-12　　ハートビート タイマー



ステップ 2　[Enable Heartbeat Timer] チェックボックスをクリックします。

ステップ 3　[Log Out Disconnected Users After] フィールドに、分単位で時間を設定します。接続試行によって到達できないユーザは、この時間が経過すると、ネットワークからログオフされます。

ステップ 4　[Update] をクリックして設定値を保存します。

ネットワークからログオフされても、Certified Devices List からそのユーザが削除されるわけではありません。ただし、Certified Devices List から削除されたユーザは、ネットワークからもログオフされます。管理者は、ユーザを個別にネットワークから排除することも、一度にすべてのユーザのセッションを終了させることもできます。詳細については、「証明済みデバイスまたは免除デバイスの手動消去」（P.11-13）および「イベント ログの意味」（P.13-4）を参照してください。

（注）　Cisco NAC アプライアンス セッションベースの接続設定に基づいてクライアント マシンがシャットダウンされた場合、Agent は CAS にログアウト要求を送信しません。

OOB ハートビート タイマーの設定（ユーザ ロール単位）

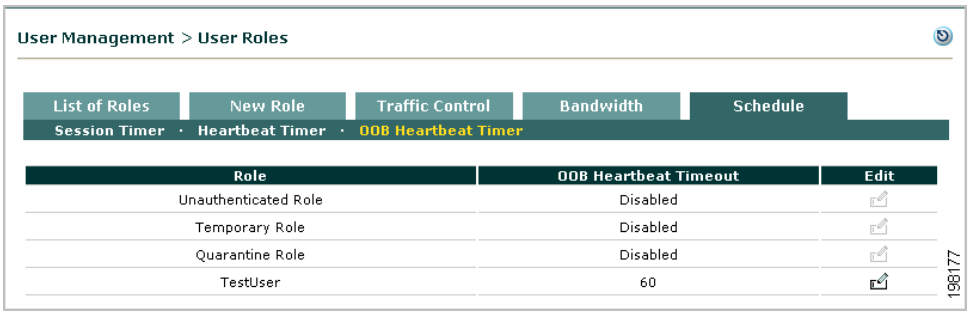
ステップ 1　[User Management] > [User Roles] > [Schedule] > [OOB Heartbeat Timer] の順番に進みます。

（注）　OOB ハートビート タイマーはデフォルトでディセーブルに設定されています。

（注）　OOB ハートビート タイマーを設定するには、アウトオブバンド ログオフをイネーブルにする*必要があります*。「アウトオブバンド ログオフの設定」（P.9-6）を参照してください。

注意　Cisco NAC アプライアンス ネットワークに現在ログインしているユーザの切断を回避するために、ネットワークの停止が計画されている時間中はアウトオブバンド ハートビート タイマーをディセーブルにすることを強くお勧めします。この設定を変更すると、現在のユーザ全員が [Out-of-Band Online Users] リストから除外されます。

図 8-13　OOB ハートビート タイマー



ステップ 2　ハートビート タイムアウト値を設定するロールの横にある [Edit] ボタンをクリックします。

ステップ 3　[OOB Heartbeat Timeout] チェックボックスをオンにし、分単位で時間を入力します。設定した時間後にユーザ セッションはタイムアウトになります。設定可能な最小時間は 2 分です。タイムアウト クロックは、ユーザのアクティビティには関係なく、ユーザのログイン時に開始されます。ハートビート タイマーは、セッションの期限が切れ、クライアントと CAS の間での通信が行われていないときに始動します。セッション期限の経過後もネットワークの使用を続けるユーザは、ネットワークに再度ログインしなければなりません。たとえば、タイマーが 5 分に設定されている場合にユーザが 6 分間ネットワークを使用しないと、ネットワークを使用するにはユーザはもう一度ログインしなければなりません。

ステップ 4　[Update] をクリックして、ハートビート タイムアウトをイネーブルにします。

Agent Temporary および Quarantine ロールのポリシーの設定

ここでは、次の場合に必要な一般的なトラフィック ポリシーおよびセッション タイムアウトの設定について説明します。

- 「Agent Temporary ロールの設定」（P.8-21）
- 「ネットワーク スキャン Quarantine ロールの設定」（P.8-24）

Agent Temporary ロールの設定

システム チェックで不合格となったユーザは、Agent Temporary ロールに指定されます。このロールの目的は、Agent 要件に適合するために必要なリソースだけに、ユーザ アクセスを制限することです。

Quarantine ロールとは異なり、Agent Temporary ロールは Cisco NAC アプライアンス システムに 1 つだけ設定できます。このロールは全面的に変更することが可能であり、必要なインストレーション ファイルへのユーザ アクセスを許可するトラフィック制御ポリシーをすべてこのロールに集めることを目的としています。Temporary ロールが削除された場合、デフォルトの設定では Unauthenticated ロールが使用されます。Temporary ロールに使用されるロール名は（Agent のバージョンとともに）、[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] に表示されます。

Temporary ロールには、セッション タイムアウトとトラフィック ポリシーの両方を設定する必要があります。Temporary ロールのデフォルト セッション タイムアウトは 4 分ですが、この値は、後述の方法で変更できます。Temporary および Quarantine のロールには、非信頼側から信頼側へのすべてのトラフィックをブロックするというトラフィック制御ポリシーがデフォルトで設定されています。重要なのは、ユーザがログインを試行する Normal Login ロールに必要条件（必要なパッケージ）を関連付ける場合、クライアントは Temporary ロールの間にその条件を満たさなければならないという点です。したがって、クライアントがダウンロード サイトで、必要なすべてのソフトウェア インストール ファイルにアクセスできるように、Temporary ロールにトラフィック制御ポリシーを追加する必要があります。

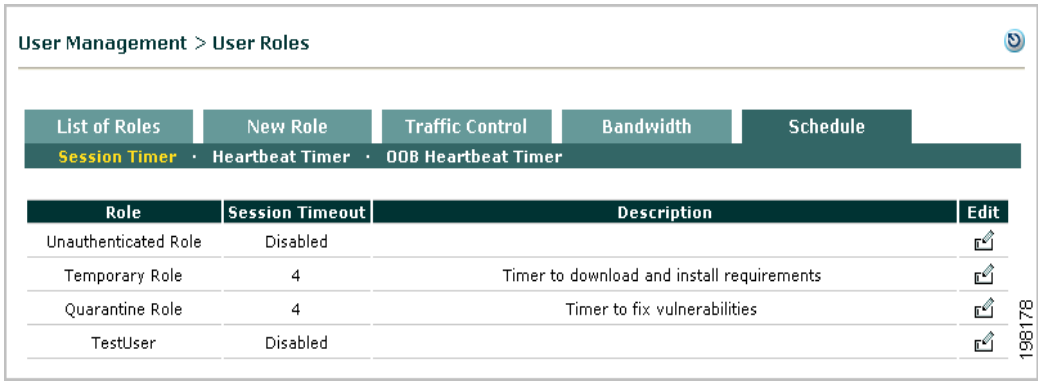
（注）　ユーザが修復ステップの一部としてクライアント マシンを再起動すると（たとえば、必須のアプリケーション インストール プロセスでマシンを再起動する必要がある場合）、CAM の [Device Management] > [Clean Access] > [General Setup] > [Agent Login] Web コンソール ページの [Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs] オプションがオンになっていないと、クライアント マシンはセッション タイマーが切れるまで Temporary ロールのままになり、ユーザには再度ログイン / 修復を実行する機会が与えられます。

「Agent ベースのポスチャ評価の設定」（P.9-41）に、Agent 要件の詳細が説明してあります。また、「ユーザ ロールのタイプ」（P.6-3）も参照してください。

Temporary ロールのセッション タイムアウトの設定

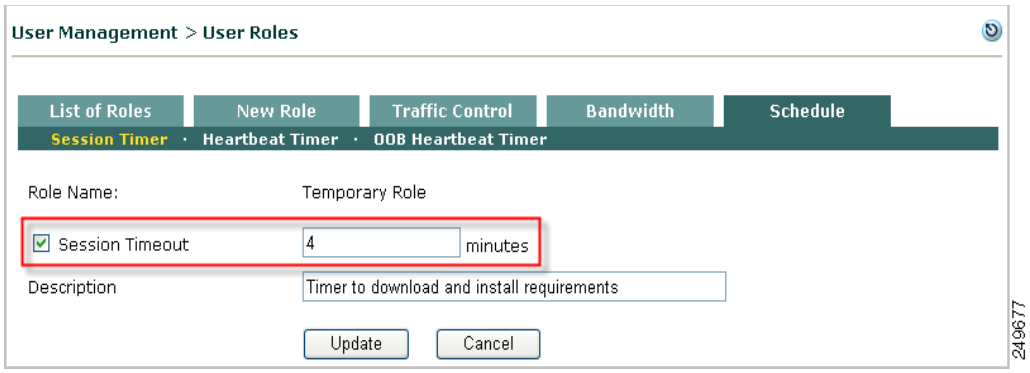
1. [User Management] > [User Roles] > [Schedule] の順番に進みます。
2. [Session Timer] リストが表示されます。

図 8-14　[Schedule] タブ



3. Temporary ロールの [Edit] ボタンをクリックします。
4. Temporary ロールの [Session Timer] フォームが表示されます（図 8-15）。

図 8-15　セッション タイマー - Temporary ロール

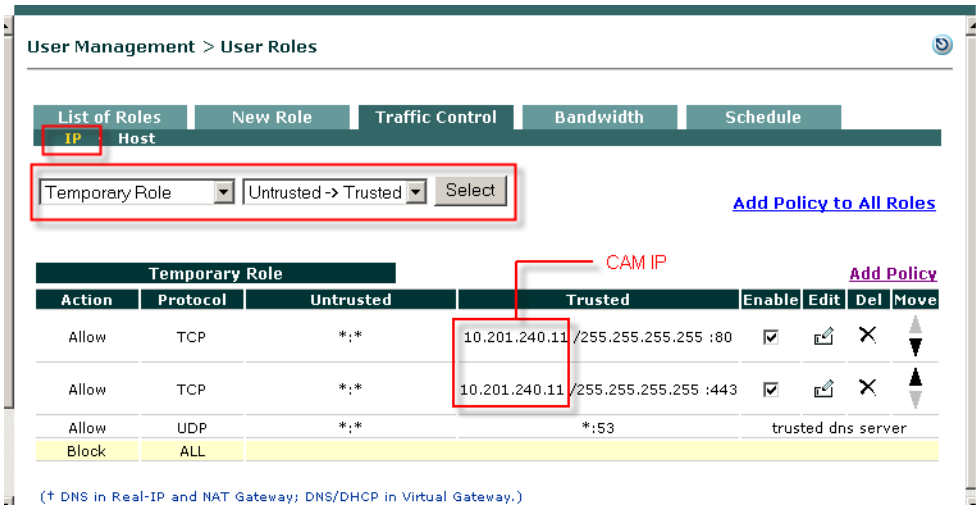


5. [Session Timeout] チェックボックスをクリックします。
6. ユーザ セッションの持続時間を分単位で入力します（デフォルトは 4 分）。システムのパッチや設定のために必要なファイルをユーザがダウンロードできるように適切な値を選択してください。
7. （任意）[Description] に、そのセッション タイムアウト条件の説明を入力します。
8. [Update] をクリックします。[Session Timer] リストに、Temporary ロールの新しい時間が表示されます。

Temporary ロールのトラフィック制御ポリシーの設定

1. [User Management] > [User Roles] から、[Traffic Control] タブをクリックします。デフォルトでは、[IP] トラフィック ポリシーのリストが表示されます。
2. ロールのドロップダウン メニューから [Temporary Role] を選択し、[Untrusted->Trusted] の方向はそのままにして、[Select] をクリックします。これによって、Temporary ロールのすべての IP ポリシーが表示されます。

図 8-16　IP トラフィック ポリシー - Temporary ロール



3. IP ポリシーを設定する場合は、Temporary ロールの横の [Add Policy] リンクをクリックします。たとえば、必要なソフトウェア インストール ファイルを（CAM にあるファイルのファイル配信要件などを通じて）提供する場合は、非信頼側から信頼側への IP ベースのトラフィック ポリシーと

して、Temporary ロールに、CAM のポート 443（HTTPS）（10.201.240.11/255.255.255.255:443 など）へのアクセスを許可するようなポリシーを設定します。ユーザが他の外部 Web ページやサーバを使用してシステムを修正できるようにする場合は、それらの Web リソースへのアクセスを許可するポリシーを設定します。[Add Policy] ページについての詳細は、「IP ベースのポリシーの追加」（P.8-4）を参照してください。

4. **ホスト**ベースのポリシーを設定する場合は、[Traffic Control] タブの上部にある [Host] リンクをクリックします。次の各項の説明に従って、インストール ファイルが置かれているサーバにアクセスできるように、ホストベースのトラフィック ポリシーを設定してください。
   - 「デフォルト許可ホストのイネーブル設定」（P.8-10）
   - 「許可ホストの追加」（P.8-11）
   - 「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）

ネットワーク スキャン Quarantine ロールの設定

ネットワーク スキャンの設定に関する詳細は、第 12 章「ネットワーク スキャンの設定」を参照してください。

Cisco NAC アプライアンスは、クライアント システムに重大な脆弱性を発見すると、そのユーザを Quarantine ロールに指定します。このロールは、マシンを修正するためにユーザに一時的なネットワーク アクセス権を与えることを目的としたメカニズムです。脆弱なユーザの隔離は、任意設定の機能です。隔離の代わりに、ユーザのアクセスをブロックしたり、ユーザに警告を与える方法もあります。ユーザを隔離しない場合は、次の手順を飛ばして次に進んでください。

Quarantine ロールの追加作成

システムには、あらかじめセッション タイムアウトが 4 分に設定され、トラフィック ポリシーの設定だけを必要とするデフォルト Quarantine ロールが 1 つあります。複数の Quarantine ロールを使用する場合は、次の手順に従って、追加の Quarantine ロールを作成してください。

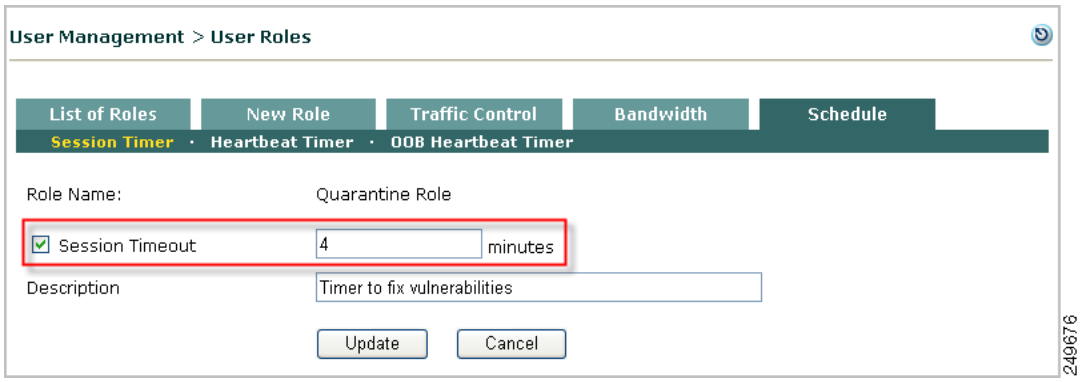
1. [User Management] > [User Roles] > [New Role] の順番に進みます。
2. そのロールの [Role Name] と [Role Description] を入力します。Quarantine ロールを特定のログイン ロールに関連付ける場合は、新しい名前として、そのログイン ロールと隔離タイプを表す名前を付けると判別しやすくなります。たとえば、その Quarantine ロールを「R1」というログイン ロールに関連付ける場合は、「R1-Quarantine」といった名前にします。
3. [Role Type] リストで、[Quarantine Role] を選択します。
4. 必要に応じて、ロールのその他の設定値を入力します。名前、説明、ロール タイプ以外のロール設定値はデフォルトの値のままにしておいてもかまいません（詳細については、「新しいユーザ ロールの追加」（P.6-7）を参照してください）。
5. [Create Role] ボタンをクリックします。[List of Roles] タブにこのロールが表示されます。

Quarantine ロールのセッション タイムアウトの設定

システムにはあらかじめ、セッション タイムアウトが 4 分に設定されたデフォルトの Quarantine ロールが 1 つあります。ロールのセッション タイムアウトは、次の手順で設定します。

1. [User Management] > [User Roles] > [Schedule] > [Session Timer] の順番に進みます。
2. 該当する Quarantine ロールの横にある [Edit] ボタンをクリックします。
3. その Quarantine ロールの [Session Timer] フォームが表示されます。

図 8-17　セッション タイマー - Quaratine ロール



4. [Session Timeout] チェックボックスをオンにします。
5. ユーザ セッションの持続時間を分単位で入力します。ユーザがシステムを修正するために必要なファイルをダウンロードするのに十分な時間を選択します。
6. （任意）[Description] に、そのセッション タイムアウト条件の説明を入力します。
7. [Update] をクリックします。[List of Roles] タブのそのロールの横の [Session Timeout] カラムに新しい値が表示されます。

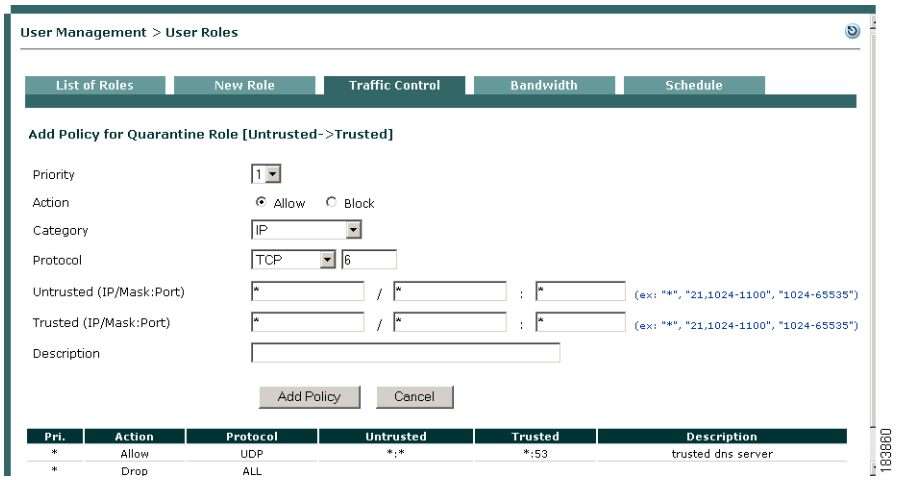
これらのパラメータを比較的小さい値に設定すると、ネットワークをログアウトせずにコンピュータを再起動したユーザを CAS が検出/切断しやすくなります。ここに入力したセッション タイマーの値は、スキャンや必要なソフトウェアのダウンロードをテストしたうえで、さらに適切な値に変更しなければならない場合もあります。

（注）　接続チェックは ARP メッセージで実行されるので、トラフィック制御ポリシーによってクライアントへの ICMP トラフィックがブロックされていても、ハートビート チェックは機能します。

Quarantine ロールのトラフィック制御ポリシーの設定

1. [User Management] > [User Roles] > [List of Roles] から、そのロールの横にある [Policies] ボタンをクリックします（または [Traffic Control] タブをクリックして、ドロップダウン メニューから Quarantine ロールを選択し、[Select] をクリックする方法もあります）。
2. ロールのドロップダウン メニューから [Quarantine Role] を選択し、[Untrusted->Trusted] の方向はそのままにして、[Select] をクリックします。これによって、その Quarantine ロールのすべての IP ポリシーが表示されます。
3. IP ポリシーを設定する場合は、その Quarantine ロールの横の [Add Policy] リンクをクリックします。

図 8-18　Add Policy - Quarantine ロール



4. 「IP ベースのポリシーの追加」（P.8-4）の手順に従って、各フィールドを設定します。
   - 必要なソフトウェア インストール ファイルを CAM から（ネットワーク スキャンの [Vulnerabilities] ページなどを通じて）提供する場合は、非信頼側から信頼側への IP ベースのトラフィック ポリシーとして、その Quarantine ロールに、CAM のポート 80（HTTP）（10.201.240.11 /255.255.255.255:80 など）へのアクセスを許可するようなポリシーを設定します。
   - ユーザが他の外部 Web ページやサーバを使用してシステムを修正できるようにする場合は、それらの Web リソースへのアクセスを許可するポリシーを設定します。「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）も参照してください。
5. ホスト ポリシーを設定する場合は、[Traffic Control] タブの上部にあるその Quarantine ロールの [Host] リンクをクリックします。次の各項の説明に従って、インストール ファイルが置かれているサーバにアクセスできるように、ホストベースのトラフィック ポリシーを設定してください。
   - 「デフォルト許可ホストのイネーブル設定」（P.8-10）
   - 「許可ホストの追加」（P.8-11）
   - 「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）

Quarantine ロールを設定したら、その Quarantine ロールをユーザに適用できます。[General Setup] タブの [Block/Quarantine users with vulnerabilities in role] オプションでユーザの Quarantine ロールとしてそのロールを選択します。詳細については、「クライアント ログインの概要」（P.1-7）を参照してください。

Quarantine ロールの設定が完了したら、「Clean Access Manager のリポジトリへの Nessus プラグインのロード」（P.12-6）の説明に従って、スキャン プラグインをロードします。

トラフィック ポリシーの例

ここでは、次の内容について説明します。

- 「Windows ドメイン認証用の認証サーバ トラフィックの許可」（P.8-27）
- 「ローカル サーバでの企業向け AV 更新用トラフィックの許可」（P.8-27）
- 「ゲーム ポートの許可」（P.8-27）
- 「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）

Windows ドメイン認証用の認証サーバ トラフィックの許可

ネットワーク上のユーザが Cisco NAC アプライアンスで認証を受ける前に、Windows ドメインの認証を受けることができるようにする場合は、次に示す最低限のポリシーによって、Unauthenticated ロールのユーザが AD（NTLM）ログイン サーバにアクセスできるようにします。

Allow　TCP　*:*　Server/255.255.255.255: 88

Allow　UDP　*:*　Server/255.255.255.255: 88

Allow　TCP　*:*　Server/255.255.255.255: 389

Allow　UDP　*:*　Server/255.255.255.255: 389

Allow　TCP　*:*　Server/255.255.255.255: 445

Allow　UDP　*:*　Server/255.255.255.255: 445

Allow　TCP　*:*　Server/255.255.255.255: 135

Allow　UDP　*:*　Server/255.255.255.255: 135

Allow　TCP　*:*　Server/255.255.255.255: 3268

Allow　UDP　*:*　Server/255.255.255.255: 3268

Allow　TCP　*:*　Server/255.255.255.255: 139

Allow　TCP　*:*　Server/255.255.255.255: 1025

ローカル サーバでの企業向け AV 更新用トラフィックの許可

Trend Micro OfficeScan などの企業向けアンチウイルス製品の定義の更新を許可するには、自動 AV 定義更新用のローカル サーバへのアクセスを許可するように Tenporary ロールを設定する必要があります。

Trend Micro OfficeScan の場合、Temporary ロール ポリシーは、AutoPccP.exe によるローカル サーバへのアクセスを許可する必要があります。Agent が Trend クライアントをローカルに呼び出し、次に Trend クライアントが（TrendMicro の設定に従って）（\\<trendserverip\ofcscan\Autopccp.exe にある）共有ドライブまたは HTTP を通じて AutoPccP.exe ファイルを実行して AV パッチをダウンロードします。

ゲーム ポートの許可

Microsoft Xbox Live などのゲーム サービスを許可する場合は、ゲーム ユーザ ロールを作成し、そのデバイスの MAC アドレスのフィルタを追加して（[Device Management] > [Filters] > [Devices] > [New]）、作成したゲーム ロールをそのデバイスに割り当てることをお勧めします。このようにすれば、そのゲーム ロールのトラフィック ポリシーを作成し、ゲーム ポートのトラフィックを許可できます。

Microsoft Xbox

次に示すのは、Microsoft Xbox ポートのアクセスを許可するポリシーの推奨例です。

- Kerberos-Sec (UDP); Port 88; UDP; Send Receive
- DNS Query (UDP); Port 53; Send 3074 over UDP/tcp
- Game Server Port（TCP）: 22042

- Voice Chat Port（TCP/UDP）：22043 ～ 22050
- Peer Ping Port（UDP）：
- Peer Query Port（UDP）：

その他のゲーム ポート

表 8-1 に、その他のゲーム ポート（PlayStation など）へのアクセスを許可する推奨ポリシーをまとめます。

表 8-1　その他のゲーム ポート用のトラフィック ポリシー [1]

プロトコル ポート	プロトコル
2300 ～ 2400	UDP
4000	TCP、UDP
4000	TCP、UDP
80	TCP
2300	UDP
6073	UDP
2302 ～ 2400	UDP
33334	UDP
33335	TCP
6667	TCP
3783	TCP
27900	TCP
28900	TCP
29900	TCP
29901	TCP
27015	TCP
各クライアントに 2213 + 1(第 1 コンピュータは 2213、第 2 コンピュータは 2214、第 3 コンピュータは 2215 など)	TCP
6073	TCP
2302 ～ 2400	UDP
27999	TCP
28000	TCP
28805 ～ 28808	TCP
9999	TCP
47624	TCP
2300 ～ 2400	TCP
2300 ～ 2400	UDP
6073	UDP
2302 ～ 2400	UDP
47624	TCP

表 8-1　その他のゲーム ポート用のトラフィック ポリシー [1]（続き）

プロトコル ポート	プロトコル
2300 ～ 2400	TCP
2300 ～ 2400	UDP
5120 ～ 5300	UDP
6500	UDP
27900	UDP
28900	UDP
3782	TCP
3782	UDP
27910	TCP、UDP
6073	UDP
2302 ～ 2400	UDP
47624	TCP
2300 ～ 2400	TCP
2300 ～ 2400	UDP
4000	TCP
7777	TCP、UDP
4000	TCP
27015 ～ 27020	TCP
6667	TCP
28800 ～ 29000	TCP

1. http://www.us.playstation.com/support.aspx?id=installation/networkadaptor/415013907.html で提供されている情報も参照してください。

詳細は、次の項目を参照してください。

- 「デバイス フィルタとゲーム ポート」（P.2-18）
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- 「新しいユーザ ロールの追加」（P.6-7）

デフォルト ロール用のトラフィック ポリシーの追加

次の説明に従って、デフォルト ロール（Unauthenticated、Temporary、Quarantine）に非信頼側から信頼側へのトラフィック ポリシーを作成することにより、任意のリソースへのユーザ アクセスを許可できます。

Unauthenticated ロール

CAM または外部 URL 上のロゴやファイルを参照するように Web ログイン ページをカスタマイズする場合は、Unauthenticated ロールに対して、CAM または外部サーバへの HTTP（ポート 80）アクセスを許可するような IP ポリシーを作成します（「リソース ファイルのアップロード」（P.5-13）および「右フレームのコンテンツの作成」（P.5-12）も参照してください）。

Agent Temporary ロール

- 企業向けアンチウイルス製品の定義アップデートを提供する場合、Agent がライブ アップデートをトリガできるようにローカル アップデート サーバへのアクセスを許可します（「ローカル サーバでの企業向け AV 更新用トラフィックの許可」（P.8-27）を参照）。

（注）　Cisco NAC Web Agent は自動修正をサポートしていないので、これが適用されるのは Cisco NAC アプライアンスだけです。

- CAM から（File Distribution などを通じて）必要なソフトウェア パッケージを提供する場合は、Temporary ロールに対して、CAM のポート 443（HTTPS）へのアクセスを許可するような IP ポリシーを作成します。必ず、CAM へのアクセスだけを許可するような IP アドレス/サブネット マスク（10.201.240.11/255.255.255.255:443 など）を指定してください。
- デフォルトのホスト ポリシーおよび信頼 DNS サーバをイネーブルにするか、または更新サイトへのユーザ アクセスを許可するような新しい許可ホスト ポリシーを作成します（「デフォルト許可ホストのイネーブル設定」（P.8-10）を参照）。
- Temporary ロールのユーザが外部 Web ページまたはサーバにアクセスできるようにするために、任意のトラフィック ポリシーを追加し、設定します（たとえば、「Agent ユーザ用の [Network Policy] ページ（AUP）の設定」（P.9-11）を参照してください）。

Quarantine ロール

- CAM から（ネットワーク スキャンの [Vulnerabilities] ページなどを通じて）必要なソフトウェア パッケージを提供する場合は、Quarantine ロールに対して、CAM のポート 443（HTTPS）へのアクセスを許可するような IP ポリシーを作成します。必ず、CAM へのアクセスだけを許可するような IP アドレス/サブネット マスク（10.201.240.11/255.255.255.255:443 など）を指定してください。
- デフォルトのホスト ポリシーおよび信頼 DNS サーバをイネーブルにするか、または更新サイトへのユーザ アクセスを許可するような新しい許可ホスト ポリシーを作成します（「デフォルト許可ホストのイネーブル設定」（P.8-10）を参照）。
- Quarantine ロールのユーザが修復のために外部 Web ページまたはサーバにアクセスできるようにするために、任意のトラフィック ポリシーを追加し、設定します。

表 8-2 に、リソース、ロール、システム ロールのトラフィック ポリシーの例をまとめて示します。

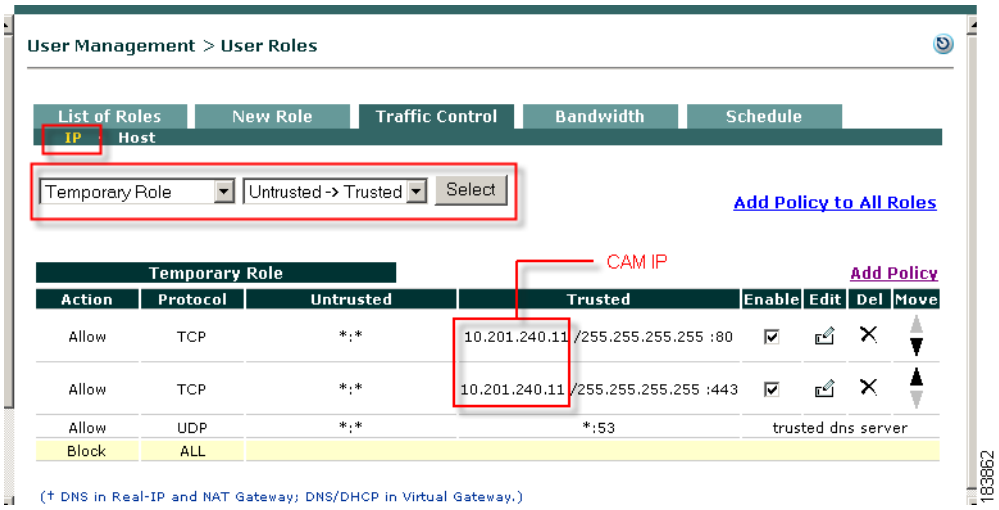
表 8-2　各ロールの一般的なトラフィック ポリシー

リソース	ロール	ポリシーの例（非信頼側から信頼側へ）
IP ベースのトラフィック ポリシー		
ログイン ページのロゴ/右側のフレームのコンテンツ（logo.jpg、file.htm）	Unauthenticated	**IP（CAM または外部サーバ上のファイル）：** TCP *.* <*CAM_IP_address* または *external_server_IP_address*> / 255.255.255.255: http（443）を許可
ユーザ同意ページ（UAP.htm）		
アクセス ブロック後のリダイレクト URL（block.htm）（任意）		
ネットワーク ポリシー ページ（AUP.htm）	Temporary	
ファイル配布条件ファイル（Setup.exe）		
脆弱性レポート ファイル（fixsteps.htm、stinger.exe）	Quarantine	
ホスト ベースのトラフィック ポリシー		
信頼 DNS サーバのイネーブル設定	ホスト ポリシーを使用するすべてのロール	**Trusted DNS Server:**e.g. 63.93.96.20、または *（任意の DNS サーバ）
リンク配布条件（外部 Web サイト）	Temporary	**Default Host：**windowsupdate.com、または **Custom Host:** database.clamav.net（同等）
脆弱性レポート（外部 Web サイトへのリンク）	Quarantine	
その他		
その環境でのプロキシ サーバ	プロキシを通じたアクセスを使用するあらゆるロール	**IP:** <*proxy_IP_address*>/255.255.255.255:https(443) **Host:** proxy-server.com (equals)
フル ネットワーク アクセス	Normal Login ロール	Allow ALL TRAFFIC * /*

詳細は、次の項目を参照してください。

- 「リソース ファイルのアップロード」（P.5-13）
- 「右フレームのコンテンツの作成」（P.5-12）
- 「File Distribution /Link Distribution / Local Check 要件の作成」（P.9-85）
- 「脆弱性の処理の設定」（P.12-14）

図 8-19　ファイル配布条件用のトラフィック ポリシーの例（CAM 内のファイル）



ホストベースのポリシーに関するトラブルシューティング

ホストベースのポリシーの場合、トラフィックを許可するためには、CAS が DNS 応答を認識できなければなりません。ホストベースのポリシーに問題が生じた場合は、次の事項を確認してください。

- 許可ホストがイネーブルに設定されていること。
- 追跡する DNS サーバのリストに DNS サーバが正しく追加されていること（あらゆる DNS サーバを追跡する場合はアスタリスク（「*」）を追加することもできます）。
- DNS サーバが CAS の信頼側インターフェイス上にあること。DNS サーバが CAS の非信頼側にあると、CAS は DNS トラフィックを認識しません。
- DNS 応答トラフィックが CAS を通過すること。たとえば、戻りトラフィック（つまり信頼側から非信頼側へのトラフィック）の代替ルート（トラフィックが CAS を通じて送出されるのに CAS を通じて戻らないようなルート）がないことを確認します。これは、Unauthenticated または Temporary ロールの信頼側から非信頼側への方向に、「Block ALL」ポリシーを追加することによってテストできます。このようなポリシーを追加しても DNS が成功するようなら、代替パスがあると判断できます。
- クライアントに表示されている DNS サーバが正しいこと。
- そのクライアントのプロキシの設定値が正しいこと（プロキシの設定が必要な場合）。
- [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filters] > [Roles] > [Allowed Hosts] > [View Current IP Address List] で、ホストベースのポリシーで追跡されている現行の IP のリストを確認する。このリストが空の場合、ユーザにはセキュリティ メッセージが表示されます。