CHAPTER 9

ローカル トラフィック制御ポリシー

この章では、Clean Access Server（CAS）のトラフィック フィルタリング規則の設定方法について説明します。この章の内容は、次のとおりです。

概要

トラフィック制御ポリシーを使用すると、アクセス可能なネットワーク リソース、およびそれらにアクセス可能なユーザを制御できます。トラフィック制御ポリシーはユーザ ロールによって設定され、Clean Access Agent（CAA）の Temporary ロールおよび Quarantine ロールに対して設定する必要があります。

Cisco NAC アプライアンスには、次の 3 種類のトラフィック ポリシーが用意されています。

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、おもに CAA 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 Clean Access Layer 2 Ethernet 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 CAS にのみ適用されます。

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 ポリシーおよびレイヤー 2 イーサネット トラック 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することができます。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。

非信頼ネットワークから送信されたすべてのトラフィックは最初にブロックされるため、通常は、ロール作成後に、ロールに適合するトラフィックを許可するポリシーを作成する必要があります。

また、トラフィック制御ポリシーによって、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（電子メールの使用や Web ブラウジングなど）に制限することができます。次に、ポリシーの例を示します。

deny access to the computer at 191.111.11.1 または
allow www communication from computers on subnet 191.111.5/24

最終的に、トラフィック制御ポリシーは階層的であり、トラフィックのフィルタリング方法は、ポリシー リスト内の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。信頼できない側から信頼できる側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：

- プライオリティ 1：Deny Telnet
- プライオリティ 2：Allow All

結果：Telnet トラフィックだけがブロックされ、ほか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）：

- プライオリティ 1：Allow All
- プライオリティ 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 番め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 SNA レイヤ 2 トラフィックのみが許可され、それ以外のレイヤ 2 トラフィックは拒否されます。

ローカルおよびグローバルなトラフィック ポリシー

ほとんどのトラフィック制御ポリシーは、Clean Access Manager（CAM）グローバル フォームを使用してすべての CAS にグローバルに設定できます。各 CAS にローカル トラフィック ポリシーを追加すると、グローバルに定義されたポリシーを拡張して、目的の CAS で管理されるネットワークのフィルタリングを限定的に設定できます。

この章では、**Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles** で CAS に設定されるローカル トラフィック制御ポリシーについて説明します。

ローカルなトラフィック ポリシー リストでは、グローバル ポリシーはイエローの背景で、ローカル ポリシーはホワイトの背景で表示されます。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。

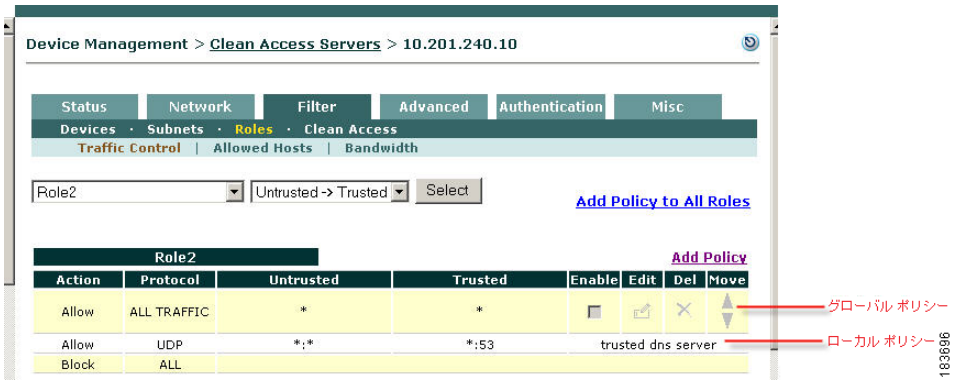
グローバル ポリシーにアクセスしたり、変更したりするには、**User Management > User Roles > Traffic Control** グローバル フォームを使用します。詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

（注） 特定の 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、すべての CAS を対象としたグローバル ポリシーよりもプライオリティが高い場合は、ローカル ポリシーが優先されます。

ローカル トラフィック制御ポリシーの表示

ローカル トラフィック制御ロール ポリシーを表示および設定するには、**Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles** の順番に進みます。**Traffic Control** フォームにポリシーがロール別に表示されます（図 9-1 を参照）。

図 9-1　ローカル トラフィック制御ポリシー



デフォルトでは、非信頼ネットワーク（送信元）から、信頼ネットワーク（宛先）に送信されるトラフィックのポリシーが表示されます。逆方向、つまり信頼ネットワーク（送信元）から非信頼ネットワーク（宛先）方向のポリシーを表示するには、方向フィールドで **Trusted->Untrusted** を選択し、**Select** をクリックします。

図 9-2　Trusted -> Untrusted 方向フィールド

同様に、単一ロールに対応するポリシーを表示するには、ロール ドロップダウン メニューでロールを選択し、**Select** をクリックします。

ポリシーのプライオリティは、リスト内の順番に対応します。最初の項目のプライオリティが最も高くなります。ポリシーのプライオリティを変更するには、**Move** カラムで対応する上下の矢印をクリックします。

IP ベースのローカル トラフィック制御ポリシーの追加

トラフィック制御ポリシーはロール単位で作成され、ネットワーク上のリソースへのトラフィックを許可またはブロックします。トラフィック制御ポリシーを作成する前に、そのポリシーを割り当てるロールがあるかどうかを確認してください。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。

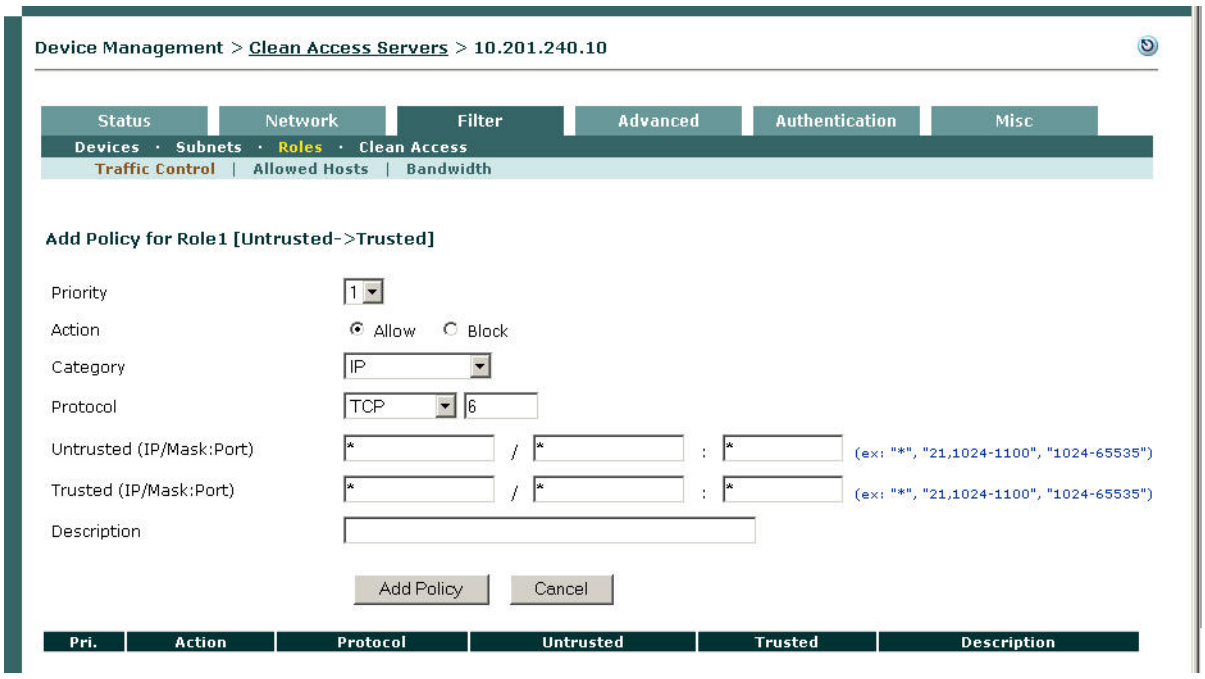
IP ベースのローカル トラフィック ポリシーの追加 / 編集

1. **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles** の順番に進みます。
2. **Traffic Control** フォームで、そのポリシーを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. 新しいポリシーの場合：
   - ポリシーを作成するロールの横にある **Add Policy** リンクをクリックします。または、
   - **Add Policy to All Roles** をクリックして、すべてのロール（Unauthenticated ロール以外）に新しいポリシーを一度に追加します。

   既存のポリシーを変更する手順は、次のとおりです。
   - 変更するポリシーの横にある **Edit** をクリックします。

   図 9-3 に、Add Policy フォームを示します。

図 9-3　新しいローカル IP ポリシーの追加



（注）　**Add Policy to All Roles** オプションを使用すると、すべてのロール（Unauthenticated ロール以外）にポリシーを追加できます。追加したトラフィック ポリシーは、個別の修正や、ロール単位のみで削除が可能です。

4. **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。

5. **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。
6. **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、信頼できる側および信頼できない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、CAS 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。
7. **IP** カテゴリを選択した場合は、以下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 の設定には、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。
   - **ESP（50）** — 主として 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、Encapsulated Security Payload（ESP）を設定する場合に選択します。
   - **AH（51）** — IP ヘッダ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、Authentication Header（AH）を設定する場合に選択します。
8. **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。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。

9. **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。
10. （任意）**Description** フィールドにそのポリシーの説明を入力します。
11. 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。

（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 番めの IP/Mask/Port エントリは宛先です。

ホストベースのローカル トラフィック制御ポリシーの追加

ローカル ホストベースのポリシーでは、ロール内のユーザまたは特定の CAS に対して、ホスト サイトへのユーザ トラフィックを制御できます。

CAM から CAA 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。

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。

Device Management > Clean Access > Updates で CAM にダウンロードされる自動**アップデート**の内容の詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「Clean Access Agent」を参照してください。

プロキシ トラフィックのイネーブル化

特定のプロキシ サーバをユーザ トラフィックが通過するとき、ホスト ポリシーを解析するための個々の CAS をイネーブル化することができます。

ある CAS の「**Parse Proxy Traffic for Roles other than Unauthenticated Role**」オプションにチェックが入っていて CAS **Proxy** ページでプロキシ サーバが指定されている場合、プロキシ サーバへトラフィックを許可する前に、ホストがホスト ポリシー リストに記述されていることを確認するため、CAS によって GET、POST、CONNECT HTTP/HTTPS/FTP 要求のペイロードがチェックされます。これにより、指定のプロキシ サーバを使用する際に、ユーザはロール（要件を満たす必要のある Temporary または Quarantine ユーザ）のためにイネーブル化されたホスト サイトのみにアクセス可能になります。「parse proxy traffic」機能は、CAS ごとにイネーブル化されます。この機能を有効にするには、CAS **Proxy** ページでプロキシ サーバ IP とポート指定し、「**Parse Proxy Traffic for Roles other than Unauthenticated Role**」をイネーブル化する必要があります。

（注）

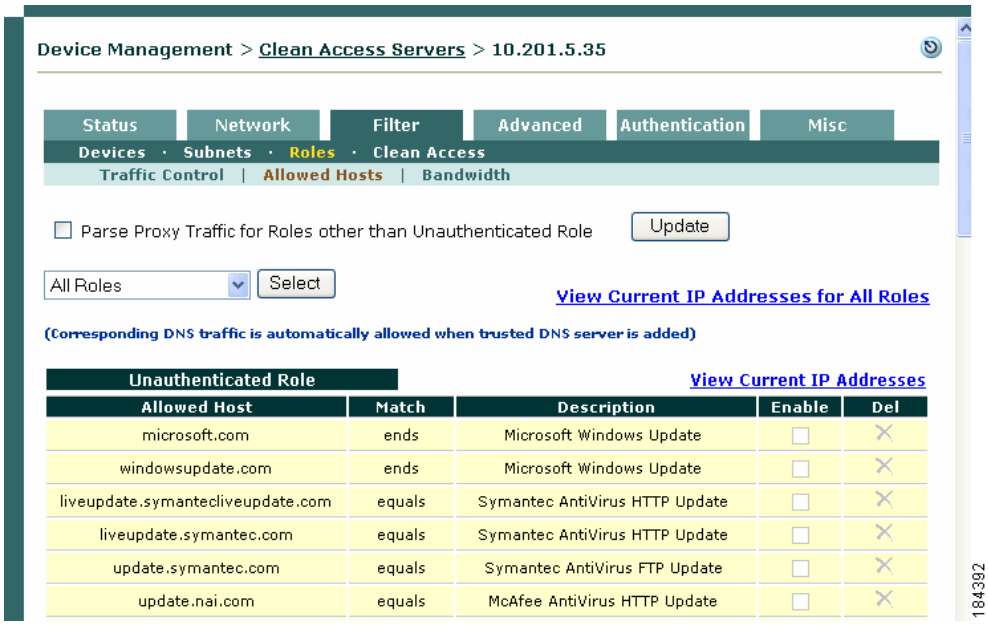
Unauthenticated ロールについては、プロキシ サーバを指定した場合、ホスト ポリシーは機能せず、ユーザは常にログインページにリダイレクトされます。

CAS で指定されたプロキシ サーバをトラフィックが通過する際にホスト ポリシーをイネーブル化するには、次の手順を実行します。

1. **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Proxy** の順番に進みます。
2. 「CAS でのプロキシ サーバ設定を指定する」（p.5-44）の説明に従って、プロキシ IP/ ポートを指定します。

3. **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**（図 9-4）の順番に進みます。

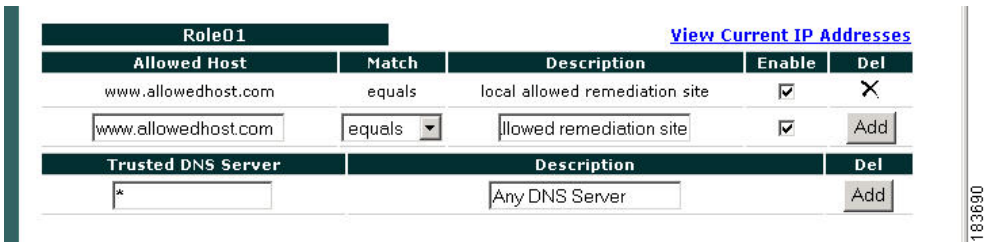
図 9-4　CAS — 許可ホスト



4. 「**Proxy Traffic for Roles other than Unauthenticated Role**」のチェックボックスをクリックします。このオプションは、（Temporary/Quarantine ロールだけでなく）Unauthenticated ロール以外のすべてのロールに適用されます。
5. **Update** ボタンをクリックします。

ローカル許可ホストの追加

1. **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** の順番に進んで、DNS ホストを追加するロールを選択します。



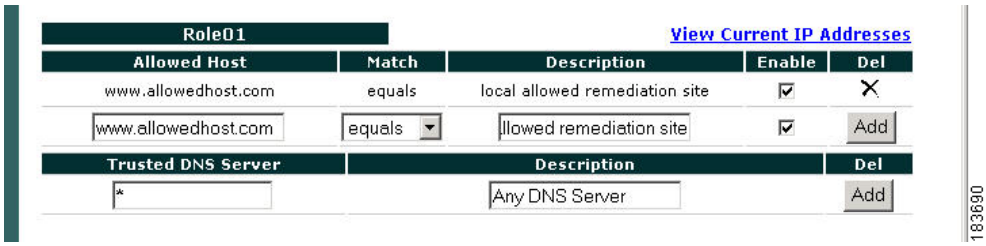
2. **Allowed Host** フィールドにホスト名を入力します（「allowedhost.com」など）。
3. **Match** ドロップダウン メニューで、ホスト名の照合に使用する演算子を選択します（equals、ends、begins、または contains）。
4. **Description** フィールドに、そのホストの説明を入力します（「Allowed Host Update」など）。
5. **Enable** をクリックします。
6. **Add** をクリックします。

（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。

ローカルな信頼できる DNS サーバの追加

ローカルな信頼できる DNS サーバを追加する手順は、次のとおりです。

1. **Trusted DNS Server** フィールドに IP アドレスを入力します。あるいは、あらゆる DNS サーバを指定する場合は、アスタリスク 「*」を入力します。



2. **Description** フィールドに、DNS サーバの説明を入力します。
3. **Add** をクリックします。

（注）　信頼できる DNS サーバが追加されると、そのサーバを許可する IP ベース トラフィック ポリシーがロールに自動的に追加されます。

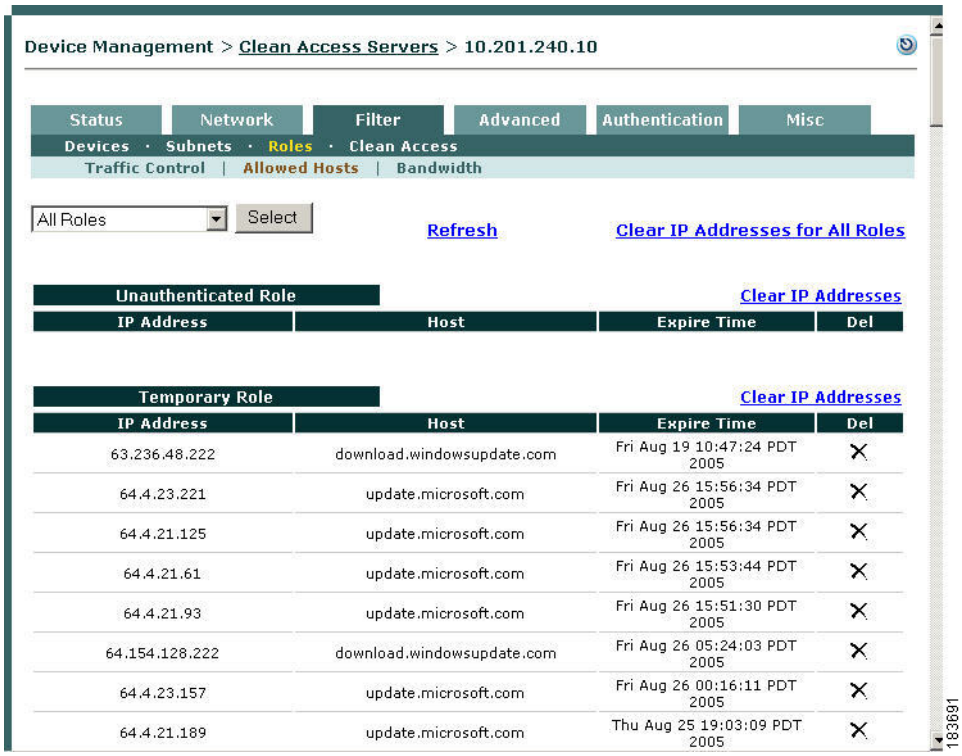
（注）　特定の DNS サーバを追加してから、このフォームを使用して任意の（「*」）DNS サーバを追加すると、前に追加したサーバはすべての DNS サーバを許可する全体ポリシーのサブセットになるので、表示されなくなります。その後、あらゆる（「*」）DNS サーバのポリシーを削除すると、以前に許可した特定の信頼できる DNS サーバが再度表示されるようになります。

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。

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 IP アドレス全体を表示するには、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。

図 9-5　すべてのロールの現行 IP アドレスの表示



（注）　このリストは、CAS 管理ページから表示できますが、リストを変更するには、CAM グローバル フィルタ フォームを使用します。詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

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. アクセスする IP アドレスごとに、IP アドレス、ホスト名、および有効期限が表示されます。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。

レイヤ 2 イーサネット トラフィック制御ポリシーの追加

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

レイヤ 2 イーサネット トラフィック制御ポリシーを使用すると、CAS を通過するレイヤ 2 トラフィックのタイプに基づいてレイヤ 2 トラフィックを許可または拒否することができます。

CAM から CAA 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 トラフィック制御ポリシーが自動的に取得され、更新されます。

（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 レイヤ 2 イーサネット トラフィック制御ポリシーはディセーブルになりますが、既存のイーサネット トラフィック制御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、既存のすべてのレイヤ 2 イーサネット トラフィック制御ポリシーが削除され、新しい デフォルト イーサネット トラフィック制御ポリシーがデフォルト設定のディセーブルのまま追加されます。

Device Management > Clean Access > Updates で CAM にダウンロードされる自動更新内容の詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「Clean Access Agent」を参照してください。

レイヤ 2 イーサネット トラフィック制御のイネーブル化

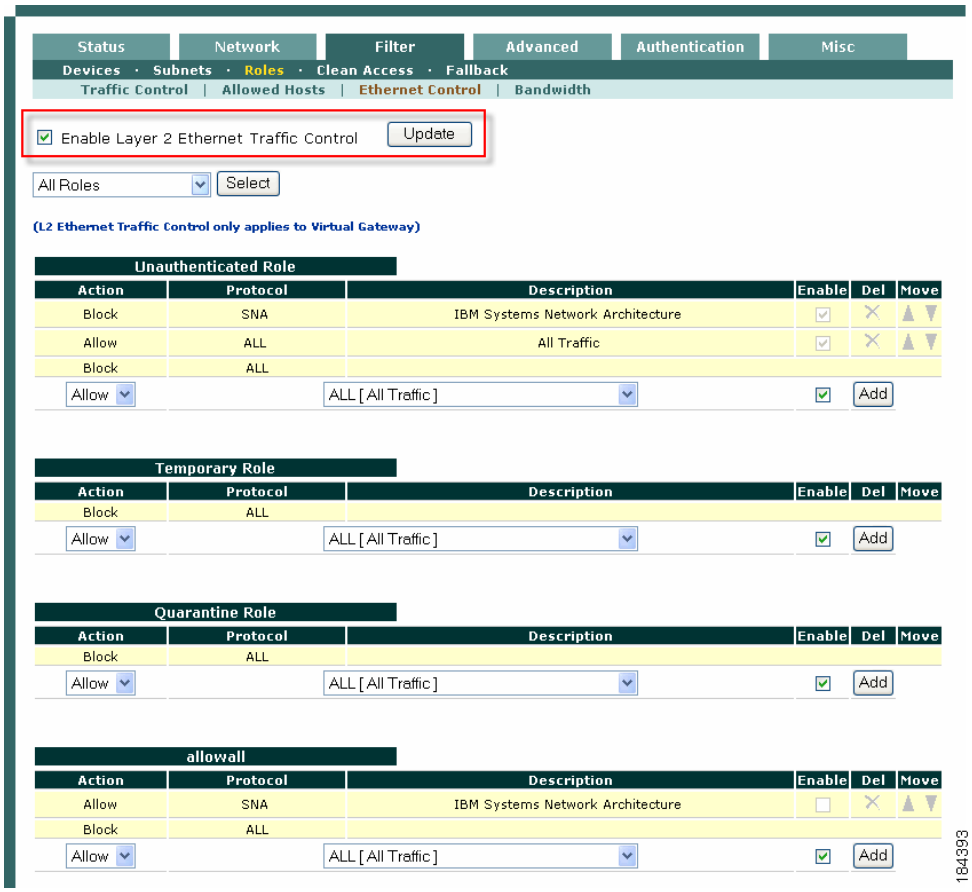
個々の CAS を、制御ポリシーに基づいて指定のレイヤ 2 イーサネット トラフィックを許可または拒否するよう設定することができます。

ある CAS に対して「**Enable Layer 2 Ethernet Traffic Control**」オプションにチェックを付けた場合、CAS を通過するトラフィックに、関連するレイヤ 2 イーサネット トラフィック制御ポリシーが適用され、CAS を通過するレイヤ 2 トラフィックのタイプに基づいてパケットが許可または拒否されます。

CAS でレイヤ 2 イーサネット トラフィック制御をイネーブルにする手順は、次のとおりです。

1. **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control**（図 9-4）の順番に進みます。

図 9-6　CAS — イーサネット制御



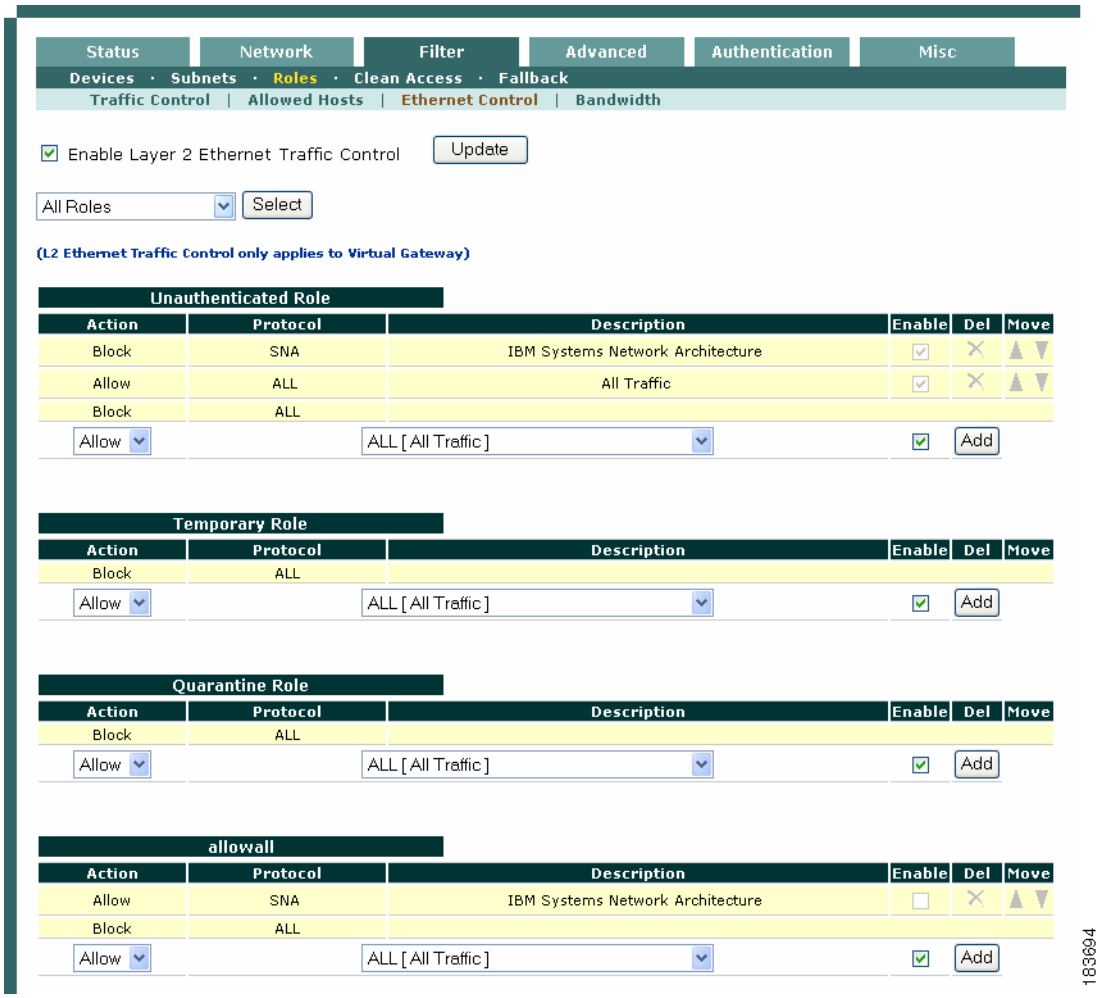
2. **Enable Layer 2 Ethernet Traffic Control** のチェックボックスをクリックします。
3. **Update** ボタンをクリックします。

レイヤ 2 イーサネット トラフィック制御の追加

レイヤ 2 イーサネット トラフィック制御ポリシーを追加する手順は、次のとおりです。

1. **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control** の順番に進んで、レイヤ 2 イーサネット トラフィックを許可または拒否するロールを選択します。

図 9-7　レイヤ 2 イーサネット トラフィック制御の追加



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）　Cisco Clean Access release 4.1(1) では、すべてのレイヤ 2 トラフィックを許可する場合以外は、「IBM Systems Network Architecture（SNA）」プロトコルのみが使用できます。その他の事前設定オプションが、CAM の Cisco Clean Access 更新サービスを通して利用可能になることがあります。

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 が導入されているネットワーク セグメントだけであり、CAS2 が導入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。

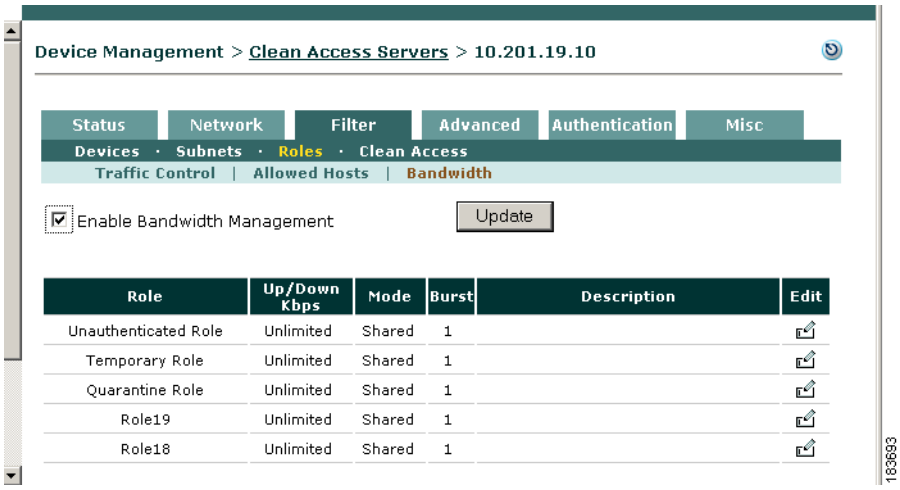
また、バースト時に、帯域幅制限からのわずかな逸脱を許可することもできます。これによって、ユーザによるコンテンツのストリーミングや大きなファイルの転送は帯域制限の対象としながら、断続的に帯域リソースを必要とするユーザ（たとえば、ページのダウンロードや閲覧時）に対応することができます。

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）。

ロールのローカル帯域幅を設定する手順は、次のとおりです。

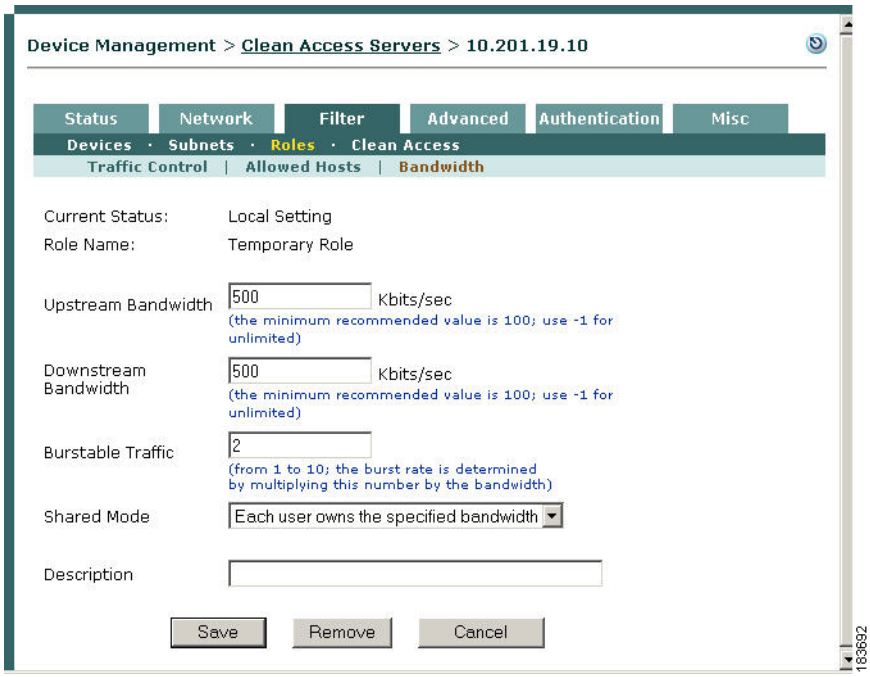
1. まず、**Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Bandwidth** に進み、その CAS で帯域幅管理をイネーブルにします。
2. **Enable Bandwidth Management** を選択し、**Update** をクリックします。

図 9-8　CAS の帯域幅管理のイネーブル化



3. 帯域幅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。**Role Bandwidth** フォームが表示されます。

図 9-9　ユーザ ロール用のローカル Bandwidth フォーム



4. **Current Status** フィールドに、次のいずれかが表示されます。
   - **Default Setting**：ローカル帯域幅管理はディセーブルです（**User Management > User Roles > Bandwidth** の設定値が使用されます）。または、ローカル ポリシーが設定されていません。
   - **Local Setting**：この CAS に設定されたローカル設定が、選択したロールに適用されます。
5. **Role Name** フィールドに、ローカル設定値を設定するユーザ ロールが表示されます。
6. **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、信頼できない（管理対象）側から信頼できる側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、信頼できる側から信頼できない側へのトラフィックです。
7. **Burstable Traffic** に、帯域制限からのわずかな（1 秒）逸脱を許可するレベルとして、2 から 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 100 Kb × 2 = 200 Kb 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としたら、そのユーザのパケットには最大で 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。
8. **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。したがって、あるユーザが使用可能な帯域幅の 80 パーセントを占有した場合、そのロールの他のユーザは残りの 20 パーセント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。

9. （任意）**Description** にその帯域設定値の説明を入力します。
10. 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。

帯域幅管理の詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。