CHAPTER 33

ネットワーク アドミッション コントロールの設定

この章は、次の項で構成されています。

使用方法、要件、および制限

ネットワーク アドミッション コントロール（NAC）は、実働状態でのネットワーク アクセスの条件として、エンドポイントにおける準拠性チェックと脆弱性チェックを実行することで、ワーム、ウイルス、および危険なアプリケーションの侵入や感染から企業ネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。IPSec セッションを確立しているホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防御ソフトウェアが最新であることを保障するためにポスチャ検証を設定できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、IPSec および他のアクセス方式が提供するアイデンティティ ベースの検証を補足するものです。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）から企業ネットワークを保護する場合は特に有用です。

（注） NAC をサポートするように設定すると、セキュリティ アプライアンスは、Cisco Secure Access Control Server のクライアントとして機能します。そのため、NAC 認証サービスを提供するために、ネットワーク上に少なくとも 1 台の Access Control Server をインストールする必要があります。

ネットワークに 1 つまたは複数の Access Control Server を設定した後で、**aaa-server** コマンドを使用して Access Control Server グループに名前を付ける必要があります。その後、「基本設定」（P.33-2）の手順に従って NAC を設定します。

NAC に対する ASA サポートは、リモート アクセス IPSec セッションおよび L2TP over IPSec セッションに限定されます。ASA 上の NAC は、WebVPN、VPN 以外のトラフィック、IPv6 およびマルチモードをサポートしません。

基本設定

次の各項の手順では、セキュリティ アプライアンスの NAC のサポートを設定する最小限のコマンド セットの入力方法に関して説明します。

（注）　次の手順に進む前に「使用方法、要件、および制限」（P.33-1）を参照してください。

Access Control Server グループの指定

NAC をサポートするためには、少なくとも 1 つの Cisco Access Control Server を設定する必要があります。次に、グループにサーバが 1 台だけ含まれている場合でも、**aaa-server host** コマンドを使用して Access Control Server グループに名前を付けます。その後、NAC ポスチャ検証で使用されるグループと同じグループを指定するには、トンネル グループ一般属性コンフィギュレーション モードで次のコマンドを入力します。

nac-authentication-server-group *server-group*

server-group は、**aaa-server host** コマンドで指定した server-tag 変数と一致する必要があります。

たとえば、acs-group1 を NAS ポスチャ検証に使用される認証サーバ グループとして指定するには、次のコマンドを入力します。

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

デフォルトのリモート アクセス グループから認証サーバ グループを継承するには、継承元となる代替のグループ ポリシーにアクセスし、次のコマンドを入力します。

no nac-authentication-server-group

次に例を示します。

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

NAC のイネーブル化

グループ ポリシーの NAC をイネーブルまたはディセーブルにするには、グループ ポリシー コンフィギュレーション モードで次のコマンドを入力します。

nac {**enable** | **disable**}

次の例では、グループ ポリシーに対して NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)
```

デフォルト グループ ポリシーから NAC の設定を継承するには、継承元の代替グループ ポリシーにアクセスして、次のコマンドを発行します。

no nac

次に例を示します。

```
hostname(config-group-policy)# no nac
hostname(config-group-policy)#
```

NAC 用デフォルト ACL の設定

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。セキュリティ アプライアンスは、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、セキュリティ アプライアンスはデフォルト ACL をリモート ホストのアクセス コントロール サーバから取得した ACL に置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。

また、セキュリティ アプライアンスは、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

（注）　NAC はデフォルトでディセーブルになっているため、セキュリティ アプライアンスを通過する VPN トラフィックは、NAC がイネーブルになるまで、NAC デフォルトの ACL の影響は受けません。

NAC セッションのデフォルト ACL として使用される ACL を指定するには、グループ ポリシー コンフィギュレーション モードで次のコマンドを入力します。

nac-default-acl value *acl-name*

acl-name は、**aaa-server host** コマンドを使用してセキュリティ アプライアンスに設定されている、ポスチャを検証するサーバ グループの名前を指定します。この名前は、そのコマンドに指定された server-tag 変数に一致する必要があります。

たとえば、NAC デフォルト ACL として acl-1 を指定するには、次のコマンドを入力します。

```
hostname(config-group-policy)# nac-default-acl value acl-1
hostname(config-group-policy)
```

デフォルト グループ ポリシーから ACL の設定を継承するには、継承元の代替グループ ポリシーにアクセスして、次のコマンドを入力します。

no nac-default-acl

次に例を示します。

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

デフォルト グループ ポリシーから ACL を継承しないようにして、NAC デフォルト ACL を指定しないというオプションもあります。そのためには、次のコマンドを入力します。

nac-default-acl none

次に例を示します。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)
```

NAC 免除の設定

セキュリティ アプライアンスのコンフィギュレーションには、NAC ポスチャ検証免除のリストが保存されます。免除されるオペレーティング システムを指定できます。ACL を指定すると、指定したオペレーティング システムを実行しているクライアントは、ポスチャ検証が免除され、クライアントのトラフィックは ACL の対象になります。

NAC ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、グループ ポリシー コンフィギュレーション モードで次のコマンドを入力します。

vpn-nac-exempt os "*os name*" [**filter** *acl-name*] [**disable**]

（注） このコマンドは、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

os name は、オペレーティング システムの名前です。引用符は、名前にスペースが含まれている場合に使用します（たとえば "Windows XP"）。

たとえば、ポスチャ検証から免除されるコンピュータのリストに Windows XP を実行しているすべてのホストを追加するには、次のコマンドを入力します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

残りのキーワードと引数は任意です。

- **filter** は、コンピュータの OS の名前が一致したときにトラフィックをフィルタリングするために ACL に適用するフィルタです。
- *acl-name* は、セキュリティ アプライアンス コンフィギュレーションにある ACL の名前です。
- **disable** は、免除リストのエントリを削除せずにディセーブルにします。このキーワードを入力しないと、エントリがイネーブルにされます。

たとえば、Windows 98 を実行するすべてのホストを免除し、acl-1 という ACL をこれらのホストからのトラフィックに適用するには、次のコマンドを入力します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次に、免除リストに同じエントリを追加して、それをディセーブルにする例を示します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

継承をディセーブルにし、すべてのホストをポスチャ検証の対象にするには、次のコマンドを入力します。

vpn-nac-exempt none

次に例を示します。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

免除リストのエントリを削除するには、免除リストから削除するオペレーティング システム（および ACL）の名前を指定して、次のコマンドを入力します。

no vpn-nac-exempt [os "*os name*"] [**filter** *acl-name*]

たとえば、免除リストから Windows 98 および acl-1 のエントリをディセーブルかどうかに関係なく削除するには、次のコマンドを入力します。

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

このグループ ポリシーに関連付けられている免除リストにある全エントリを削除し、デフォルト グループ ポリシーの免除リストを継承するには、キーワードを指定せずに次のコマンドを入力します。

no vpn-nac-exempt

次に例を示します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

詳細設定の変更

セキュリティ アプライアンスには、NAC のデフォルト設定があります。この項の手順に従って、ネットワークの強制ポリシーを順守するようにこれらの設定を調整します。

クライアントレス認証設定の変更

クライアントレス認証に対する NAC のサポートは設定可能です。これは、ポスチャ エージェントがない Cisco Trust Agent などのホストに適用されます。セキュリティ アプライアンスは、デフォルト アクセス ポリシーを適用し、ポスチャ検証用に Extensible Authentication Protocol（EAP）over User Datagram Protocol（UDP）要求を送信して、その要求がタイムアウトします。セキュリティ アプライアンスが、Access Control Server からのクライアントレス ホストに対するポリシーを要求するように設定されていない場合、クライアントレス ホストにすでに使用されているデフォルト アクセス ポリシーを保持します。セキュリティ アプライアンスが、Access Control Server からのクライアントレス ホストに対するポリシーを要求するように設定されている場合、そのように要求して、Access Control Server はセキュリティ アプライアンスが実施するアクセス ポリシーをダウンロードします。

クライアントレス認証のイネーブル化とディセーブル化

クライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

eou allow clientless

次に例を示します。

```
hostname(config)# eou allow clientless
hostname(config)#
```

eou clientless コマンドは、NAC がイネーブルの場合にだけ有効です。

（注） クライアントレス認証は、デフォルトでイネーブルになっています。

クライアントレス認証をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

no eou allow clientless

次に例を示します。

```
hostname(config)# no eou allow clientless
hostname(config)#
```

クライアントレス認証に使用するログイン クレデンシャルの変更

クライアントレス認証がイネーブルで、セキュリティ アプライアンスがリモート ホストからの検証要求に対する応答の受信できなかった場合、リモート ホストの代わりに、セキュリティ アプライアンスはクライアントレス認証要求を Access Control Server に送信します。この要求には、Access Control Server でのクライアントレス認証用に設定されたクレデンシャルに一致するログイン クレデンシャルが含まれます。セキュリティ アプライアンスのクライアントレス認証用のデフォルト ユーザ名とパスワードは、Access Control Server のデフォルト ユーザ名とパスワードと一致します。デフォルト ユーザ名とパスワードはいずれも「clientless」です。Access Control Server でこれらの値を変更する場合は、セキュリティ アプライアンスでも変更する必要があります。

クライアントレス認証に使用するユーザ名を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

eou clientless username *username*

username は、クライアントレス ホストをサポートする Access Control Server に設定されているユーザ名に一致する必要があります。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。

クライアントレス認証に使用するパスワードを変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

eou clientless password *password*

password は、クライアントレス ホストをサポートする Access Control Server に設定されているパスワードに一致する必要があります。4 ～ 32 文字の ASCII 文字を入力します。

ユーザ名だけ、パスワードだけ、または両方を指定できます。たとえば、sherlock と 221B-baker それぞれに対するクライアントレス認証のユーザ名とパスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# eou clientless username sherlock
hostname(config)# eou clientless password 221B-baker
hostname(config)#
```

ユーザ名をそのデフォルト値に変更するには、次のコマンドを入力します。

no eou clientless username

次に例を示します。

```
hostname(config)# no eou clientless username
hostname(config)#
```

パスワードをそのデフォルト値に変更するには、次のコマンドを入力します。

no eou clientless password

次に例を示します。

```
hostname(config)# no eou clientless password
hostname(config)#
```

NAC セッション属性の設定

ASA には、セキュリティ アプライアンスとリモート ホスト間の通信を指定する属性のデフォルト設定があります。これらの属性で、リモート ホストのポスチャ エージェントと通信するポート番号、およびポスチャ エージェントとの通信を制限する有効制限カウンタを指定します。これらの属性、デフォルト設定、およびそれらを変更するために入力できるコマンドは次のとおりです。

- ポスチャ エージェントの EAP over UDP の通信に使用するクライアント エンドポイントのポート番号。

  デフォルトのポート番号は 21862 です。変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

  eou port *port_number*

  port_number は、CTA で設定されているポート番号に一致する必要があります。値は 1024 ～ 65535 の範囲で入力します。

  たとえば、EAP over UDP 通信のポート番号を 62445 に変更するには次のコマンドを入力します。

  ```
  hostname(config)# eou port 62445
  hostname(config)#
  ```

  ポート番号をそのデフォルト値に変更するには、このコマンドの **no** 形式を次のように使用します。

  no eou port

  次に例を示します。

  ```
  hostname(config)# no eou port
  hostname(config)#
  ```

- 再送信リトライ タイマー

  セキュリティ アプライアンスは EAP over UDP メッセージをリモート ホストに送信する場合、応答を待ちます。*n* 秒以内に応答を受信できない場合、EAP over UDP メッセージを再送信します。デフォルトでは、再送信タイマーは 3 秒です。この値を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

  eou timeout retransmit *seconds*

  seconds は、1 ～ 60 の範囲の値です。

  次に、再送信タイマーを 6 秒に変更する例を示します。

  ```
  hostname(config)# eou timeout retransmit 6
  hostname(config)#
  ```

  再送信リトライ タイマーをそのデフォルト値に変更するには、このコマンドの **no** 形式を次のように使用します。

  no eou timeout **retransmit**

  次に例を示します。

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

- 再送信リトライ

  セキュリティ アプライアンスは EAP over UDP メッセージをリモート ホストに送信する場合、応答を待ちます。応答を受信できない場合、EAP over UDP メッセージを再送信します。デフォルトでは、3 回まで再送信されます。この値を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

  eou max-retry *retries*

  retries は、1 ～ 3 の範囲の値です。

  次に、EAP over UDP の再送信回数を 1 に制限する例を示します。

```
hostname(config)# eou max-retry 1
hostname(config)#
```

  再送信リトライの最大回数をそのデフォルト値に変更するには、このコマンドの **no** 形式を次のように使用します。

  no eou max-retry

  次に例を示します。

```
hostname(config)# no eou max-retry
hostname(config)#
```

- セッション再初期化タイマー

  再送信リトライ カウンタと max-retry 値が一致すると、セキュリティ アプライアンスはリモート ホストとの EAP over UDP セッションを終了し、保持タイマーを起動します。保持タイマーが *n* 秒になると、セキュリティ アプライアンスは、リモート ホストとの新しい EAP over UDP セッションを確立します。デフォルトでは、新規セッションを確立するまでの最大待機秒数は 180 秒です。この値を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

  eou timeout hold-period *seconds*

  seconds は、60 ～ 86400 の範囲の値です。

  たとえば、新しい EAP over UDP アソシエーションを開始するまでの待機期間を 120 秒に変更するには次のコマンドを入力します。

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

  セッションの再初期化をそのデフォルト値に変更するには、このコマンドの **no** 形式を次のように使用します。

  no eou timeout hold-period

  次に例を示します。

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

ポスチャ変更確認のクエリーのタイマーの設定

ポスチャ検証が成功するたびに、セキュリティ アプライアンスはステータス クエリー タイマーを起動します。このタイマーの期限が切れると、直前のポスチャ検証以降のポスチャ変更を確認するクエリーがリモート ホストにトリガーされます。変更がないことを応答が示している場合、ステータス クエリー タイマーがリセットされます。ポスチャに変更があったことを応答が示している場合、無条件のポスチャ再検証がトリガーされます。セキュリティ アプライアンスは、再検証中、現在のアクセス ポリシーを保持します。

デフォルトでは、成功した各ポスチャ検証、ステータス クエリー、および以降の各ステータス クエリーの間隔は 300 秒（5 分）です。グループ ポリシーを変更しない限り、デフォルト グループ ポリシーからステータス クエリー タイマーの値を継承します。ステータス クエリーの間隔を変更するには、グループ ポリシー コンフィギュレーション モードで次のコマンドを入力します。

nac-sq-period *seconds*

seconds は、300 ～ 1800 秒（5 ～ 30 分）の範囲で指定する必要があります。

次の例では、ステータス クエリー タイマーが 1800 秒に変更されます。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承元の代替グループ ポリシーにアクセスして、次のコマンドを入力します。

no nac-sq-period [*seconds***]**

次に例を示します。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)
```

再検証タイマーの設定

ポスチャ検証が成功するたびに、セキュリティ アプライアンスは再検証タイマーを起動します。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスは、再検証中、現在のアクセス ポリシーを保持します。

デフォルトでは、成功した各ポスチャ検証間の間隔は 36000 秒（10 時間）です。グループ ポリシーを変更しない限り、デフォルト グループ ポリシーから再検証タイマーの値を継承します。再検証の間隔を変更するには、グループ ポリシー コンフィギュレーション モードで次のコマンドを入力します。

nac-reval-period *seconds*

seconds は、300 ～ 86400 秒（5 分～ 24 時間）の範囲で指定する必要があります。

たとえば、再検証タイマーを 86400 秒に変更するには次のコマンドを入力します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

デフォルトのグループ ポリシーから再検証タイマーの値を継承するには、継承元の代替グループ ポリシーにアクセスして、次のコマンドを入力します。

no nac-reval-period

次に例を示します。

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)
```