CHAPTER 33

ネットワーク アドミッション コントロールの設定

次の事項について説明します。

使用、要件、および制限

Network Admission Control（NAC; ネットワーク アドミッション コントロール）は、製品がネットワークにアクセスする条件として、エンドポイントの適合性と脆弱性チェックを実施することにより、ワーム、ウイルスの侵入と感染、不正アプリケーションから企業を保護します。こうしたチェックを*ポスチャ確認と呼びます*。ポスチャ確認を設定して、アンチウイルス ファイル、パーソナル ファイアウォール規則、または IPSec セッションを確立しているホスト上の侵入防御ソフトウェアが最新のバージョンであることを確認します。ポスチャ確認では、リモート ホスト上で動作しているアプリケーションが最新のパッチが組み込まれた最新バージョンであることを確認します。NAC は IPSec などのアクセス方式が提供するアイデンティティベースの確認を補完します。ホーム PC などの自動ネットワーク ポリシー実施の影響を受けないホストから企業ネットワークを保護するのに特に有用です。

（注） NAC をサポートするように設定した場合、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、NAC 認証サービスを提供するため、少なくともネットワークに 1 台の Access Control Server をインストールすることを要求します。

ネットワークに 1 つ以上の Access Control Server を設定した後に、**aaa-server** コマンドを使用して Access Control Server グループを指定します。次に、P.33-2 の「基本の設定」の手順に従って NAC を設定します。

NAC をサポートする ASA は、リモート アクセス IPSec と L2TP over IPSec セッションに制限されます。ASA 上の NAC は WebVPN、非 VPN トラフィック、IPv6、マルチモードをサポートしません。

基本の設定

次の項の手順は、セキュリティ アプライアンス上の NAC をサポートする最少のコマンドセットを入力する方法について説明します。

（注）　P.33-1 の「使用、要件、および制限」を参照してから、これらの手順に従ってください。

Access Control Server グループの指定

NAC をサポートする Cisco Access Control Server を少なくとも 1 つ設定します。次に、グループにサーバが 1 台のみ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 グループを指定します。最後にトンネルグループの一般アトリビュート 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、NAC ポスチャ確認に使用されるグループと同一のグループを指定します。

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、次のコマンドを入力して、acs-group1 を NAC ポスチャ確認に使用される認証サーバ グループとして指定します。

```
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、継承元の別のグループポリシーにアクセスしてから、次のコマンドを入力します。

no nac-authentication-server-group

次の例を参考にしてください。

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

NAC のイネーブル化

グループポリシーに対して 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)
```

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

no nac

次の例を参考にしてください。

```
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 の対象となるホストに適用されるデフォルト ACL をポイントします。セキュリティ アプライアンスは NAC デフォルト ACL を適用してからポスチャ確認を実行します。ポスチャ確認の後は、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 Access Control Server から入手したものに置換します。ポスチャ確認に失敗した場合、デフォルトの ACL を保持します。

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（デフォルト設定）の場合、NAC デフォルト ACL も適用します。

（注）　NAC はデフォルトでディセーブルになっているので、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。

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て、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 アプライアンス上に設定されるポスチャ確認サーバ グループの名前です。名前は、このコマンドで指定された server-tag 変数と一致している必要があります。

たとえば、次のコマンドを入力して acl-1 を NAC デフォルト ACL として指定します。

```
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 を継承するには、継承元の別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-default-acl

次の例を参考にしてください。

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

ACL をデフォルトのグループポリシーから継承せず、no NAC default ACL を指定するオプションもあります。これを行うには、次のコマンドを入力します。

nac-default-acl none

次の例を参考にしてください。

```
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 ポスチャ確認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、ポスチャ確認が免除され、クライアントのトラフィックは ACL の対象になります。

NAC ポスチャ確認が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）　このコマンドは免除リストにすでに追加されているエントリを上書きしません。各オペレーティング システムと免除する ACL に対してコマンドを一度だけ入力します。

os name は、オペレーティング システムの名前です。名前にスペース（「Windows XP」など）が含まれる場合、引用符を使用します。

たとえば、次のコマンドを入力して、Windows XP を実行しているすべてのホストをポスチャ確認が免除されるコンピュータのリストに追加します。

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

次に示す残りのキーワードと引数はオプションです。

- **filter**：コンピュータが os name に一致する場合、トラフィックをフィルタリングするために ACL に適用します。
- *acl-name* は、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存在する ACL の名前です。
- **disable**：免除リストのエントリをリストから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なります。

たとえば、次のコマンドを入力して Windows 98 を実行しているすべてのホストを免除し、それらのホストのトラフィックに ACL acl-1 を適用します。

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

次の例は、同一エントリを免除リストに追加し、これをディセーブルにする方法を示します。

```
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、すべてのホストがポスチャ確認の対象になることを指定するには、次のコマンドを入力します。

vpn-nac-exempt none

次の例を参考にしてください。

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

エントリを免除リストから削除するには、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）を指定する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、次のコマンドを入力して Windows 98 と acl-1 に伴うエントリを、ディセーブルであるかどうかにかかわらず、免除リストから削除します。

```
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する免除リストからすべてのエントリを削除し、リストをデフォルトのグループポリシーから継承するには、別の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

次の例を参考にしてください。

```
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 アプライアンスでは、NAC がデフォルトで設定されています。この項の手順に従って、ネットワークの強制ポリシーを遵守するよう設定を調整します。

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 サポートは設定可能です。Cisco Trust Agent といったポスチャ エージェントを持たない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のアクセス ポリシーを適用し、EAP over UDP 要求をポスチャ確認に送信し、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 のクライアントレス ホストにポリシーを要求するよう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のアクセス 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 のクライアントレス ホストにポリシーを要求するよう設定されている場合、そのように要求し Access Control Server はセキュリティ アプライアンスが実行するアクセス 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

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て、クライアントレス認証をイネーブルにします。

eou allow clientless

次の例を参考にしてください。

```
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のみ有効です。

（注）　クライアントレス認証はデフォルトでイネーブルです。

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て、クライアントレス認証をディセーブルにします。

no eou allow clientless

次の例を参考にしてください。

```
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 アプライアンスが確認要求に対する応答をリモート ホストから受信できなかった場合、リモート ホストに代わって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 上のクライアントレス認証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 アプライアンス上のクライアントレス認証に対するデフォルトのユーザ名とパスワードは Access Control Server 上のデフォルトのユーザ名とパスワードに一致します。デフォルトのユーザ名とパスワードはいずれも「クライアントレス」です。Access Control Server のこれらの値を変更する場合、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。

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て、クライアントレス認証に使用するユーザ名を変更します。

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 に設定されたユーザ名に一致する必要があります。1 から 64 までの ASCII 文字を入力します。前後のスペース、ポンド記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< と >）は除外します。

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て、クライアントレス認証に使用するパスワードを変更します。

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 に設定されたパスワードに一致する必要があります。4 ～ 32 文字までの ASCII 文字を入力します。

ユーザ名のみ、パスワードのみ、またはその両方を指定できます。たとえば、次のコマンドを入力して、クライアントレス認証のユーザ名とパスワードを sherlock と 221B-baker にそれぞれ変更します。

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

ユーザ名を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

次の例を参考にしてください。

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

パスワードを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

次の例を参考にしてください。

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

NAC セッション アトリビュートの設定

ASA 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アトリビュートをデフォルト設定します。これらのアトリビュートは、リモート ホスト上のポスチャ エージェントと通信するポート番号とポスチャ エージェントとの通信を制限する制限カウンタを指定します。それらを変更するために入力するアトリビュート、デフォルト設定、コマンドは次の通りです。

- EAP over UDP とポスチャ エージェント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。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て変更します。

  eou port *port_number*

  port_number は CTA で設定されたポート番号に一致する必要があります。1024 から 65535 までの範囲で値を入力します。

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

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

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

  no eou port

  次の例を参考にしてください。

  ```
  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 UDP メッセージを介してリモート ホストに EAP を送信する場合、応答を待ちます。*n* 秒以内に応答の受信に失敗した場合、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 から 60 までの範囲の値です。

  次の例は再送信タイマーを 6 秒に変更します。

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

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

  no eou timeout retransmit

  次の例を参考にしてください。

  ```
  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 UDP メッセージを介してリモート ホストに EAP を送信する場合、応答を待ちます。応答の受信に失敗した場合、EAP over UDP メッセージを再送信します。デフォルトでは、最大 3 回までリトライします。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 から 3 までの範囲の値です。

次の例は EAP over UDP 最転送回数を 1 に制限します。

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

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

no eou max-retry

次の例を参考にしてください。

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

- セッション再初期化タイマー

  再送信リトライ回数が最大リトライ値に一致する場合、セキュリティ アプライアンス リモート ホストにより 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 ホストにより新規 EAP over UDP セッションを確立します。デフォルトでは、新規セッションが確立されるまでの最長待機秒数は、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 から 86400 までの範囲の値です。

  たとえば、次のコマンドを入力して、新規 EAP over UDP アソシエーションが開始されるまでの待機時間を 120 秒に変更します。

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

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

  no eou timeout hold-period

  次の例を参考にしてください。

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

Query-for-Posture-Changes タイマーの設定

ポスチャ確認に成功するたびに、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、直前のポスチャ確認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。変化なしを示す応答は、ステータス クエリー タイマーをリセットします。ポスチャの変化を示す応答は、無条件のポスチャ再確認をトリガーします。セキュリティ アプライアンスは、再確認中に現在のアクセス ポリシーを維持します。

デフォルトでは、成功した各ポスチャ確認とステータス 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。ユーザが変更しない場合、グループポリシーはデフォルト 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。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てステータス クエリー間隔を変更します。

nac-sq-period *seconds*

seconds は、300 秒から 1800 秒（5 分から 30 分）の範囲にする必要があります。

次の例はステータス クエリー タイマーを 1800 秒に変更しています。

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

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

no nac-sq-period [*seconds*]

次の例を参考にしてください。

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

再確認タイマーの設定

ポスチャ確認が成功するたびに、セキュリティ アプライアンスは再確認タイマーを起動します。このタイマーの期限が切れると、次の無条件のポスチャ確認を開始します。セキュリティ アプライアンスは、再確認中に現在のアクセス ポリシーを維持します。

デフォルトでは、成功したポスチャ確認間の間隔は、36000 秒（10 時間）です。ユーザが変更しない場合、グループポリシーは再確認タイマーの値をデフォルト グループポリシーから継承します。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て、再確認の間隔を変更します。

nac-reval-period *seconds*

seconds は、300 秒から 86400 秒（5 分から 24 時間）の範囲にする必要があります。

たとえば、次のコマンドを入力して再確認タイマーを 86400 秒に変更します。

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

再確認タイマーの値をデフォルト グループポリシーから継承するには、継承元の別のグループポリシーにアクセスしてから、次のコマンドを入力します。

no nac-reval-period

次の例を参考にしてください。

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