CHAPTER 7

ネットワーク アドミッション コントロールの設定

この章の内容は、次のとおりです。

ネットワーク アドミッション コントロールに関する情報

ネットワーク アドミッション コントロールは、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。ポスチャ検証を設定して、イントラネット上の脆弱なホストへのアクセスを提供する前に、IPsec セッションまたは WebVPN セッションを行っ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、または侵入予防ソフトウェアが最新の状態であることを確認できます。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、ユーザ認証およびトンネルの設定の完了後に行われます。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）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。

エンドポイントと ASA 間でトンネルを確立すると、ポスチャ検証がトリガーされます。

クライアントがポスチャ検証の要求に応答しない場合は、ASA を設定して、そのクライアントの IP アドレスをオプションの監査サーバに渡すことができます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

ポスチャ検証が成功する、またはリモート ホストが正常であることを示すトークンを受信すると、ポスチャ検証サーバは、トンネル上のトラフィックに対するアプリケーション用のネットワーク アクセス ポリシーを ASA に送信します。

ASA を含む *NAC Framework* のコンフィギュレーションには、クライアントで実行されている Cisco Trust Agent だけがポスチャ エージェントの役割を果たすことができ、Cisco Access Control Server（ACS）だけがポスチャ検証サーバの役割を果たすことができます。ACS はダイナミック ACL を使用して、各クライアントのアクセス ポリシーを決定します。

RADIUS サーバである ACS は、ポスチャ検証サーバとしての役割を果たすことに加え、トンネルの確立に必要なログイン クレデンシャルを認証できます。

（注） ASA に設定されている NAC Framework ポリシーだけが、監査サーバの使用をサポートしています。

ACS はそのポスチャ検証サーバとしての役割において、アクセス コントロール リストを使用します。ポスチャ検証が成功し、ACS によって、ASA に送信するアクセス ポリシーの一部としてリダイレクト URL が指定されると、ASA は、リモート ホストからのすべての HTTP 要求と HTTPS 要求をリダイレクト URL にリダイレクトします。ポスチャ検証サーバによってアクセス ポリシーが ASA にアップロードされると、関連するすべてのトラフィックはその宛先に到達するためにセキュリティ アプライアンスと ACS（またはその逆も同じ）の両方を通過する必要があります。

IPsec または WebVPN クライアントと ASA 間のトンネルが確立されると、NAC Framework ポリシーがグループ ポリシーに割り当てられている場合、ポスチャ検証がトリガーされます。ただし、NAC Framework ポリシーでは、ポスチャ検証を免除されているオペレーティング システムを特定し、そのようなトラフィックをフィルタリングするためにオプションの ACL を指定できます。

ライセンス要件

次の表に、この機能のライセンス要件を示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1,2]
ASA 5505	AnyConnect Premium ライセンス： • 基本ライセンスまたは Security Plus ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* • *共有ライセンスはサポートされていません。*[3]
ASA 5510	AnyConnect Premium ライセンス： • 基本ライセンスと Security Plus ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス*[3] *：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件[1,2]
ASA 5520	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5540	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5550	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5580	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5512-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5515-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5525-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件[1,2]
ASA 5545-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5555-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-10）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-20、-40、および -60）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASASM	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

1. クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。
2. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。
3. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

NAC の前提条件

NAC をサポートするように設定すると、ASA 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。

注意事項と制限事項

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。次に、「NAC ポリシーの設定」（P.7-8）の手順の説明に従ってください。

NAC Framework 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 WebVPN クライアント セッションに限定されます。NAC Framework コンフィギュレーションは、シングル モードだけをサポートしています。

ASA 上の NAC は、レイヤ 3（非 VPN）トラフィックと IPv6 トラフィックはサポートしていません。

セキュリティ アプライアンスの NAC ポリシーの表示

グループ ポリシーに割り当てる NAC ポリシーを設定する前に、ASA にすでに設定されている可能性があるポリシーを確認することをお勧めします。デフォルト コンフィギュレーションには NAC ポリシーは含まれていませんが、このコマンドを入力すると、他のユーザによってすでにポリシーが追加されているかどうかを手軽に判断できます。設定済みのポリシーがある場合に、そのポリシーが適切であると判断できる場合は、NAC ポリシーの設定に関する項を無視してもかまいません。

手順の詳細

	コマンド	目的
ステップ 1	**show running-config nac-policy** **例：** hostname# **show running-config nac-policy** nac-policy nacframework1 nac-framework default-acl acl-1 reval-period 36000 sq-period 300 exempt-list os "Windows XP" filter acl-2 hostname#	ASA 上ですでに設定されている NAC ポリシーを表示します。 nac-framework1 という名前の NAC ポリシーのコンフィギュレーションを表示します。
ステップ 2	• default-acl：NAC デフォルト ACL がポスチャ検証の前に適用されます。セキュリティ アプライアンスは、ポスチャ検証の後、リモート ホストの Access Control Server から取得した ACL でデフォルト ACL を置き換えます。ポスチャ検証が失敗した場合、ASA にはデフォルト ACL が残ります。 • reval-period：NAC フレームワーク セッション内でのポスチャ検証が正常に完了してから次回の検証までの間隔（秒）。 • sq-period：NAC フレームワーク セッション内でのポスチャ検証が正常に完了してから、ホスト ポスチャの変化を調べる次回のクエリーまでの間隔（秒）。 • exempt-list：ポスチャ検証を免除されるオペレーティング システム名。リモート コンピュータのオペレーティング システムがこの名前に一致する場合は、トラフィックをフィルタリングするオプションの ACL も表示されます。 • authentication-server-group：NAC ポスチャ検証に使用される認証サーバ グループの名前。	nac-framework の属性を表示します。

	コマンド	目的

ステップ 3	`show nac-policy`
	
	例：
	`asa2(config)# show nac-policy`
	`nac-policy framework1 nac-framework`
	`  applied session count = 0`
	`  applied group-policy count = 2`
	`  group-policy list:  GroupPolicy2  GroupPolicy1`
	`nac-policy framework2 nac-framework is not in use.`
	`asa2(config)#`
		グループ ポリシーへの NAC ポリシーの割り当てを表示します。
		
		どの NAC ポリシーが未割り当てであるかと、各 NAC ポリシーの使用回数を表示します。

ステップ 4	• applied session count：この ASA が NAC ポリシーを適用した VPN セッションの累積数。 • applied group-policy count：この ASA が NAC ポリシーを適用したグループ ポリシーの累積数。 • group-policy list：この NAC ポリシーが割り当てられているグループ ポリシーのリスト。この場合、グループ ポリシーの使用状況によってこのリストに表示されるかどうかは決まりません。NAC ポリシーが実行コンフィギュレーションのグループ ポリシーに割り当てられている場合は、このリストにグループ ポリシーが表示されます。	show nac-policy コマンドのフィールドの説明です。 **（注）** どのグループ ポリシーにも割り当てられていないポリシーについては、「is not in use」がポリシー タイプの隣に表示されます。

NAC ポリシーを作成する、またはすでに存在するポリシーを変更するには、次の項を参照してください。

NAC ポリシーの追加、アクセス、または削除

NAC ポリシーを追加または変更するには、次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**global**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**nac-policy** *nac-policy-name* **nac-framework** **例：** hostname(config)# **nac-policy nac-framework1 nac-framework** hostname(config-nac-policy-nac-framework)	NAC ポリシーを追加または変更します。 *nac-policy-name* は、新しい NAC ポリシーまたはすでに存在するポリシーの名前です。名前は最大 64 文字の文字列です。 **nac-framework** は、NAC Framework コンフィギュレーションで、リモート ホスト用のネットワーク アクセス ポリシーを提供することを指定します。ASA の NAC フレームワーク サービスを提供するには、シスコ アクセス コントロール サーバがネットワークに存在している必要があります。このタイプを指定すると、プロンプトは nac-policy-nac-framework コンフィギュレーション モードにいることを示します。このモードでは、NAC フレームワーク ポリシーを設定できます。 **（注）** NAC Framework ポリシーは複数作成できますが、1 つのグループ ポリシーに 1 つしか割り当てることはできません。 NAC フレームワーク ポリシーを nac-framework1 という名前で作成し、アクセスします。
ステップ 3	（任意） [**no**] **nac-policy** *nac-policy-name* **nac-framework**	NAC ポリシーをコンフィギュレーションから削除します。ポリシーの名前とタイプの両方を指定する必要があります。
ステップ 4	（任意） **clear configure nac-policy**	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーをコンフィギュレーションから削除します。
ステップ 5	**show running-config nac-policy**	セキュリティ アプライアンスにすでに存在する各 NAC ポリシーの名前およびコンフィギュレーションを表示します。

NAC ポリシーの設定

nac-policy コマンドを使用して NAC Framework ポリシーに名前を付けたら、そのポリシーをグループ ポリシーに割り当てる前に、次の項の手順に従ってポリシーの属性に値を割り当てます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**aaa-server host**	Access Control Server グループに名前を付けます（グループに含まれているサーバが 1 つだけであっても）。
ステップ 2	（任意） **show running-config aaa-server** **例：** hostname(config)# **show running-config aaa-server** aaa-server acs-group1 protocol radius aaa-server acs-group1 (outside) host 192.168.22.44 key secret radius-common-pw secret hostname(config)#	AAA サーバの設定を表示します。
ステップ 3	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 4	**authentication-server-group** *server-group* **例：** hostname(config-nac-policy-nac-framework)# **authentication-server-group acs-group1** hostname(config-nac-policy-nac-framework)	NAC ポスチャ検証に使用されるグループを指定します。 *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。このコマンドの **no** バージョンを使用している場合は、一致していなくてもかまいません。 NAC ポスチャ検証に使用される認証サーバ グループとして acs-group1 を指定します。
ステップ 5	（任意） [**no**] **authentication-server-group** *server-group*	コマンドを NAC ポリシーから削除します。

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、ASA 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。ASA 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。ステータス クエリーの間隔を変更するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 2	**sq-period seconds** **例：** hostname(config-group-policy)# **sq-period 1800** hostname(config-group-policy)	ステータス クエリーの間隔を変更します。 *seconds* は、30 ～ 1800 秒（5 ～ 30 分）の範囲で指定する必要があります。 クエリー タイマーを 1800 秒に変更します。
ステップ 3	（任意） [**no**] **sq-period** *seconds*	ステータス クエリー タイマーをオフにします。
ステップ 4	**show running-config nac-policy**	sq-period 属性の隣に 0 が表示されます。これは、タイマーがオフであることを意味します。

再検証タイマーの設定

ポスチャ検証が成功するたびに、ASA 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。ASA 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。この間隔を変更するには、nac-policy-nac-framework 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。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework に切り替えます。
ステップ 2	**reval-period** ***seconds*** **例：** hostname(config-nac-policy-nac-framework)# **reval-period 86400** hostname(config-nac-policy-nac-framework)	ポスチャ検証が正常に完了してから次回の検証までの間隔を変更します。 *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。
ステップ 3	（任意） [**no**] **reval-period** *seconds*	ステータス クエリー タイマーをオフにします。
ステップ 4	**show running-config nac-policy**	sq-period 属性の隣に 0 が表示されます。これは、タイマーがオフであることを意味します。

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。ASA 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、ASA 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。ポスチャ検証が失敗した場合、ASA にはデフォルト ACL が残ります。

また、ASA 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。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 2	**default-acl** *acl-name* **例：** hostname(config-nac-policy-nac-framework)# **default-acl acl-2** hostname(config-nac-policy-nac-framework)	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。 *acl-name* は、セッションに適用されるアクセス コントロール リストの名前です。 ポスチャ検証成功の前に適用される ACL として ac1-2 を指定します。
ステップ 3	（任意） [**no**] **default-acl** *acl-name*	コマンドを NAC フレームワーク ポリシーから削除します。*acl-name* の指定は任意です。

NAC 免除の設定

ASA 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、nac-policy-nac-framework 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。

手順の詳細

	コマンド	目的
ステップ 1	nac-policy-nac-framework	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 2	**exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]	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"）。 • **filter** を指定すると、コンピュータのオペレーティング システムが *os name* と一致する場合、トラフィックをフィルタリングするために ACL が適用されます。**filter**/*acl-name* のペアはオプションです。 • **disable** を指定すると、次の 2 つの機能のいずれかが実行されます。 – "os-name" の後に入力した場合、ASA は、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 – このキーワードを *acl-name* の後に入力すると、ASA はそのオペレーティング システムを免除しますが、関連のトラフィックには ACL を適用しません。 • *acl-name* は、ASA コンフィギュレーションにある ACL の名前です。指定する場合は、**filter** キーワードの後に指定する必要があります。
	例： hostname(config-group-policy)# **exempt-list os "Windows XP"** hostname(config-group-policy)	
	hostname(config-nac-policy-nac-framework)# **exempt-list os "Windows XP" filter acl-2** hostname(config-nac-policy-nac-framework)	ポスチャ検証を免除するコンピュータのリストに、Windows XP を実行するすべてのホストを追加します。
	hostname(config-nac-policy-nac-framework)# **no exempt-list os "Windows XP" filter acl-2** hostname(config-nac-policy-nac-framework)	Windows XP を実行するすべてのホストを免除し、そのホストからのトラフィックに ACL acl-2 を適用します。 同じエントリを免除リストから削除します。
ステップ 3	（任意） [**no**] **exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]	NAC フレームワーク ポリシーからすべての免除を削除します。エントリを指定してこのコマンドの no 形式を発行すると、そのエントリが免除リストから削除されます。
	例： hostname(config-nac-policy-nac-framework)# **no exempt-list** hostname(config-nac-policy-nac-framework)	免除リストからすべてのエントリを削除します。

（注）　コマンドでオペレーティング システムを指定しても、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。

グループ ポリシーへの NAC ポリシーの割り当て

各トンネルのセットアップを完了すると、グループ ポリシーに割り当てられている場合、ASA は NAC ポリシーをセッションに適用します。デフォルトでは、**nac-settings** コマンドは、各グループ ポリシーのコンフィギュレーションには存在しません。ASA は、NAC ポリシーが割り当てられると、グループ ポリシーの NAC を自動的にイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	**group-policy**	グループ ポリシー コンフィギュレーション モードに切り替えます。
ステップ 2	**nac-settings** { **value** *nac-policy-name* | **none** } **例：** hostname(config-group-policy)# **nac-settings value framework1** hostname(config-group-policy)	NAC ポリシーをグループ ポリシーに割り当てます。 • **nac-settings none** は、グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに対する NAC ポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。 • **nac-settings value** は、指定した NAC ポリシーをグループ ポリシーに割り当てます。 framework1 という名前の NAC ポリシーをグループ ポリシーに割り当てます。
ステップ 3	（任意） [**no**] **nac-settings** { **value** *nac-policy-name* | **none** }	nac-policy-name をグループ ポリシーから削除します。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承します。
ステップ 4	（任意） **show running-config nac-policy**	各 NAC ポリシーの名前およびコンフィギュレーションを表示します。

グローバルな NAC Framework 設定の変更

ASA では、NAC Framework コンフィギュレーション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 Framework のサポートは設定可能です。これは、ポスチャ エージェントの役割を果たす Cisco Trust Agent を持たないホストに適用されます。ASA 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。ASA 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。ASA 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 ASA 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は、デフォルトでイネーブルになっています。デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

制約事項

eou コマンドは、NAC Framework セッションにだけ適用されます。

手順の詳細

NAC フレームワーク コンフィギュレーションに対してクライアントレス認証をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**global**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**eou allow** {**audit** | **clientless** | **none**} **例：** hostname(config)# **eou allow audit** hostname(config)#	NAC フレームワーク コンフィギュレーションに対してクライアントレス認証をイネーブルにします。 • **audit** を指定すると、クライアントレス認証の実行に監査サーバを使用します。 • **clientless** を指定すると、クライアントレス認証の実行に Cisco Access Control Server を使用します。 • **none** は、クライアントレス認証をディセーブルにします。 監査サーバを使用してクライアントレス認証を実行するように ASA を設定する方法を示します。
ステップ 3	[**no**] **eou allow** {**audit** | **clientless** | **none**} **例：** hostname(config)# **no eou allow audit** hostname(config)#	コマンドをコンフィギュレーションから削除します。 監査サーバの使用をディセーブルにします。

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、ASA 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。ASA 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。

前提条件

Access Control Server でこれらの値を変更する場合は、ASA でも変更する必要があります。

手順の詳細

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、次のとおりに入力します。

	コマンド	目的
ステップ 1	**global**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**eou clientless username** *username* **例：** hostname(config)# **eou clientless username sherlock** hostname(config)# **eou clientless password 221B-baker** hostname(config)#	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。 *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のユーザ名を sherlock に、パスワードを 221B-baker に変更します。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。
ステップ 3	**eou clientless password** *password*	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。 *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。

	コマンド	目的
ステップ 4	(任意) **no eou clientless username** **例：** hostname(config)# **no eou clientless username** hostname(config)#	ユーザ名をデフォルト値に変更します。
ステップ 5	(任意) **no eou clientless password** **例：** hostname(config)# **no eou clientless password** hostname(config)#	パスワードをデフォルト値に変更します。

NAC Framework セッション属性の変更

ASA には、ASA 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。

手順の詳細

	コマンド	目的
ステップ 1	global	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**eou port** *port_number* **例：** hostname(config)# **eou port 62445** hostname(config)#	デフォルト ポート番号は、21862 です。このコマンドは、ポスチャ エージェントとの EAP over UDP 通信に使用されるポート番号（クライアント エンドポイントの）を変更します。 *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。 EAP over UDP 通信用のポート番号を 62445 に変更します。
ステップ 3	(任意) **no** eou port **例：** hostname(config)# **no eou port** hostname(config)#	ポート番号をデフォルト値に変更します。

	コマンド	目的
ステップ 4	**eou timeout retransmit** *seconds* **例：** hostname(config)# **eou timeout retransmit 6** hostname(config)#	再送信リトライ タイマーを変更します。ASA 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。 *seconds* は、1 ～ 60 の範囲の値です。 再送信タイマーを 6 秒に変更します。
ステップ 5	（任意） no eou timeout **retransmit** **例：** hostname(config)# **no eou timeout retransmit** hostname(config)#	再送信リトライ タイマーをデフォルト値に変更します。
ステップ 6	**eou max-retry** *retries* **例：** hostname(config)# **eou max-retry 1** hostname(config)#	再送信リトライ回数を変更します。ASA 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。 *retries* は、1 ～ 3 の範囲の値です。 EAP over UDP 再送回数の上限を 1 に設定します。
ステップ 7	（任意） **no eou max-retry** **例：** hostname(config)# **no eou max-retry** hostname(config)#	再送信リトライの最大回数をデフォルト値に変更します。
ステップ 8	**eou timeout hold-period** *seconds* **例：** hostname(config)# **eou timeout hold-period 120** hostname(config)#	セッション再初期化タイマーを変更します。再送信リトライ カウンタと max-retry 値が一致すると、ASA 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、ASA 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。 *seconds* は、60 ～ 86400 の範囲の値です。 新しい EAP over UDP アソシエーションを開始する前の待機期間を 120 秒に変更します
ステップ 9	（任意） **no** eou timeout hold-period **例：** hostname(config)# **no eou timeout hold-period** hostname(config)#	セッション再初期化をデフォルト値に変更します。