NAC Profiler への SSL 証明書のインポート

目次

概要

Profiler システム Web ベースの UI はデジタル証明書を使用できるため、Cisco NAC Profiler Server の組み込み Web サーバの信頼性は、HTTPS によって提供される Profiler ユーザ インターフェイスにアクセスするために接続する際にブラウザによって検証できます。 システムは、PKI の最も一般的なアプリケーションの 1 つおよびデジタル証明書を利用し、Web ブラウザは SSL Web サーバが本物であることを検証します。そのため、ユーザは Web サーバとのやりとりが事実上信頼されていて、Web サーバとの通信が安全であると感じることができます。 これは、SSL を使用している多くのタイプの Web サイトとの e- コマースやその他のセキュアな通信を保護するために今日使用されているメカニズムと同じです。

Profiler システムには、オンボードの SSL Web サーバを信頼済みとして検証することなく、UI へのアクセスが可能な「自己署名」のデジタル証明書が付属しています。 デフォルトの証明書が、サーバ名などの環境固有の属性を指定して作成され、認証局（CA）によって署名された証明書と交換されるまで、Profiler UI にアクセスする Web ブラウザには、この例と同様の、ブラウザがサイトの証明書を発行した CA を認識せず、信頼済みサイトとして検証することができないことを示す警告が表示されます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- NAC サーバ

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

主なタスク： 証明書のインストール

ほとんどのブラウザでは、接続を続行するため、煩わしい追加入力が要求されます。

Profiler インターフェイス の SSL セキュリティに関するデジタル証明書を使用することで、セキュリティ強化をフル活用するには、NPS の SSL サブシステム設定を変更する必要があります。これらの変更では、システムがデフォルトで使用する秘密キーおよびデジタル証明書を、インストールに固有の信頼できる認証局によって発行されたものに変更することが必要です。 この手順の後、ブラウザはサーバと HTTPS セッションを開始し、UI ログイン プロセスがすぐに表示され、証明書の警告を回避します。

2 つのオプション

NPS システムでは、この手順の代わりに 2 つの選択肢があります。

1. アプライアンスに常駐する OpenSSL ツールキットを使用して、NPS サーバ システムと、Web UI を通じたシステム管理に使用される PC にインストールできる署名付き証明書を生成します。

このオプションは、現在内部 CA が存在せず、商用 CA プロバイダー（ほとんどの商用ブラウザが自動的に認識する署名入りのデジタル証明書を有償で提供する）に依存しないことを選択する環境で使用できます。

2. OpenSSL ツールキットを使用して、NPS システムに証明書署名要求を生成します。これを社内または社外の商用 CA サービスに提出すると、システムですぐに使用できる署名入りのデジタル証明書が返されます。

通常、これは特定の環境でどのオプションを使用するか決定するために Profiler システムがインストールされている、組織の内部セキュリティ ポリシーの問題です。 これらのオプションの詳細については、このマニュアルの後半で説明します。

オプション 1： ビーコン/NPS で OpenSSL ツールキットを使用して署名を生成する

概説した手順を開始する前に、エンタープライズ名サービスを利用するために Profiler システムが正しく設定されていること、および DNS エントリはシステムが完全修飾ドメイン名（FQDN）を持つように作成されていることを検証することが重要です。 これを検証するには、UI を参照するときの URL に書かれた IP アドレス（HA システムの場合は VIP)ではなく、システムの FQDN （つまり、https://beacon.bspruce.com/beacon）を持つ Profiler システムにより UI セッションが開けることを確認します。

この手順は、署名のために CSR をオフアプライアンス CA に送信することを望まない場合に使

用されます。 この手順では、アプライアンスの OpenSSL ツールキットだけを使用して署名付き証明書を作成することができ、Profiler システムの署名付き証明書を生成するために、別のシステムまたは商用 CA に何かを提出する必要がありません。

この手順の成功は、指定通りに実施することにかかっています。 コマンド構文は長く、エラーが起こりやすいです。 コマンドを実行する前に、この手順で指定された正しいディレクトリか確認します。 CA 証明書および証明書署名要求に対して生成された DN の情報、たとえば国、州、都市、サーバ名などは、同じものを（大文字と小文字を区別）入力する必要があります。そのため、プロセスが円滑に進むように、ステップを行うごとにメモしておいてください。

1. NPS アプライアンスで SSH セッションまたはコンソール セッションを開始し、root アクセスに昇格させます。 HA システムでは、SSH を VIP に開始して、プライマリ システムであることを確認します。OpenSSL を初めて使用する前に、OpenSSL で使用されるファイル構造の一部を初期化する必要があります。 OpenSSL を初期化するには、次の手順を実行します。
2. 次のコマンドを使用して、ディレクトリを /etc/pki/CA に変更します。 `cd /etc/pki/CA/`**newcerts** という名前の新しいディレクトリを作成し、次のコマンドを発行します。`mkdir newcerts touch index.txt`
3. vi を使用して、**serial** という名前の新しいファイルを作成します。 ファイルに **01** を挿入し、変更を確定します。 （: wq!）このディレクトリを変更します。cd /etc/pki/tls/certs
4. 次のコマンドを使用して、システムの新しい秘密キーを生成します`openssl genrsa -out profilerFQDN.key 1024`（スタンドアロンで導入された場合、「profilerFQDN」は NPS アプライアンスの完全修飾ドメイン名に置き換えられます。 HA システムの場合、VIP の FQDN が使用されます）。Profiler システムが DNS に存在しない場合、サーバの IP アドレス（VIP）を FQDN の代わりに使用することができますが、証明書はこの IP アドレスに結び付けられているため、証明書の警告を回避するには URL の IP（https://10.10.0.1/profiler）を使用することが必要です。
5. このコマンドを使用して、サーバ証明書の生成に使用する CA 証明書を生成します。すると、3 年間の CA 証明書と、ステップ 4 で生成したキーが作成されます。`openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem`CA 証明書の識別名（DN）の証明書要求と構成に組み込まれた複数の属性の入力が求められます。 これらの項目のいくつかは、デフォルト値が推奨されます（[]）。 DN の各パラメータに目的とする値、または「.」を入力して 項目をスキップします。この手順で使用される DN パラメータの値をメモしてください。 これらはステップ 7 のサーバ証明書の証明書署名要求の生成で指定したものと同一である必要があります。最後のステップで作成した CA 証明書を必要なディレクトリに移動します。`mv cacert.pem /etc/pki/CA`新しい秘密キーで Profiler システムの証明書署名要求を生成します。`openssl req -new -key profilerFQDN.key -out profilerFQDN.csr`
6. ステップ 5 と同様に、サーバ CSR に対してシステムの DN を入力するように要求されます。 サーバ CSR には、ステップ 5 で CA 証明書に使用したものと同じ値を使用してください。 パラメータが異なっている場合、CSR が作成されません。 また、証明書のパスフレーズを作成するように求められます。 必ず、このパスフレーズを書き留めてください。
7. 前の手順で生成した CSR と秘密キーを使用してサーバ証明書を生成します。 この手順により、Profiler サーバ（または HA ペアの場合は複数サーバ上で）にインストールされた署名付き証明書が出力されます。`openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key`証明書に署名し、確定するよう求められます。 **y** を入力して署名を確認し、証明書がサーバ証明書の生成を実行するように確定します。
8. 証明書ファイルを内部セキュリティ ポリシーで指定された場所に移動するか（該当する場合）、デフォルトの場所を使用します。内部セキュリティ ポリシーで指定されていない場合、証明書は /etc/pki/tls/certs/ に配置する必要があります。`mv profilerFQDN.crt`

/etc/pki/tls/certs/profilerFQDN.crt

9. 秘密キー ファイルを内部セキュリティ ポリシーで指定された場所に移動するか（該当する場合）、デフォルトの場所を使用します。内部セキュリティ ポリシーで指定されていない場合、秘密キーは /etc/pki/tls/private/ に配置する必要があります。 コマンドを使用しますmv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
10. vi などの工ディタを使用して **ssl.conf ファイル**を編集し、Profiler Web サーバに新しい秘密キーと証明書を使用させるために必要な変更を行います（ssl.conf は /etc/httpd/conf.d/ にあります）。**ssl.conf** では、サーバ証明書部分はライン 107 から始まります。 ステップ 8 でシステムに作成された新しい証明書ファイルを指定するように、工場出荷時のデフォルト（/etc/pki/tls/certs/localhost.cert）から SSLCertificateFile の設定項目を変更します。**ssl.conf** では、サーバ秘密キー部分はライン 114 から始まります。 ステップ 9 でシステムに作成された新しい秘密キー ファイルを指定するように、工場出荷時のデフォルト（etc/pki/tls/private/localhost.key）からサーバ秘密キーの設定項目を変更します。
11. 次のコマンドを使用して、アプライアンス上で Apache Web サーバを再起動してください。 apachectl -k restart **注:** スタンドアロンで導入した場合、ステップ 13 に進みます。
12. HA NPS システムのみ、次のステップを実施して、HA ペアの他のメンバー（現在のセカンダリ）上で秘密キーと CRT をインストールします。 これにより、ペアのどちらのアプライアンスがプライマリかを問わず、UI の SSL セキュリティ メカニズムが同様に動作するようになります。a. ステップ 3 でプライマリ アプライアンスに生成した秘密キーを、セカンダリ アプライアンスにコピーします。 内部セキュリティ ポリシーで指定されていない場合、秘密キーは /etc/pki/tls/private/ に配置する必要があります。 次のコマンドを使用します（プライマリの /etc/pki/tls/private ディレクトリから）。scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/CA から戻された署名 CRT をプライマリからセカンダリ アプライアンスにコピーします。 内部セキュリティ ポリシーで指定されていない場合、証明書は /etc/pki/tls/certs/ に配置する必要があります。scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs セカンダリ アプライアンスで SSH を実行し、vi などの工ディタを使用して **ssl.conf ファイル**を編集し、セカンダリの Web サーバに新しい秘密キーと証明書を使用させるために必要な変更を行います（ssl.conf は /etc/httpd/conf.d/ にあります）。**ssl.conf** では、サーバ証明書部分はライン 107 から始まります。 ステップ 11b でシステムに配置された新しい証明書ファイルを指定するように、工場出荷時のデフォルト（/etc/pki/tls/certs/localhost.cert）から SSLCertificateFile の設定項目を変更します。**ssl.conf** では、サーバ秘密キー部分はライン 114 から始まります。 ステップ 11a でシステムに作成された新しい秘密キー ファイルを指定するように、工場出荷時のデフォルト（etc/pki/tls/private/localhost.key）からサーバ秘密キーの設定項目を変更します。次のコマンドを使用して、セカンダリ アプライアンス上で Apache Web サーバを再起動してください。apachectl -k restartこれらのステップで作成されたサーバ証明書はプライベートな CA を使用するため、Profiler UI にアクセスするブラウザを、IE 7.0 を搭載した Windows PC 上の Trusted Root Certification Authority レポジトリに証明書をインストールするように設定する必要があります）。 次の手順に従ってください。アプライアンスの /home/beacon ディレクトリに作成されたサーバ証明書をコピーします。cp profilerFQDN.crt /home/beaconWinSCP または同等のソフトウェアを使用して、アプライアンスから PC に .crt ファイルの SCP を行います。Certificate import ウィザードを開始する Windows certificate マネージャを開始し、『install certificate』 をクリック するために **.crt ファイルを**ダブルクリックして下さい。**ラジオ ボタン**を選択します。 このストアにすべての証明書を配置すると、**Browse ボタン**が有効になります。[Browse] を選択し、[Trusted Root Certification Authorities] 証明書ストアをクリックします。[OK] をクリックしてこの証明書を受け入れます。Profiler システムの管理に使用する他の PC でもこのプロセスを繰り返します。

13. Profiler UI にアクセスして、ブラウザで証明書の警告が生成されずに HTTPS セッションが起動することを確認します。

オプション 2： 内部/外部 CA 向けに CSR を生成/提出

次に概説した手順を開始する前に、エンタープライズ名サービスを利用するために Profiler システムが正しく設定されていること、および DNS エントリはシステムが完全修飾ドメイン名（FQDN）を持つように作成されていることを検証することが重要です。 これを検証するには、IP アドレス、または HA システムの場合は VIP ではなく、システムの FQDN（つまり、https://beacon.bspruce.com/beacon）を持つ Profiler システムにより UI セッションを開けることを確認します。

これらのステップを実施して、システムの新しい秘密キーを生成し、内部または外部 CA への提出用の CSR を生成し、有効な署名付き証明書を NPS に配置します。

1. NPS アプライアンスで SSH セッションまたはコンソール セッションを開始し、root アクセスに昇格させます。 HA システムの場合、プライマリ システムであることを確認するため、VIP に SSH を開始します。
2. NPS のデフォルト PKI ディレクトリに移動します。`cd /etc/pki/tls`
3. 次のコマンドを使用して、システムの新しい秘密キーを生成します。`openssl genrsa ?des3 ?out profilerFQDN.key 1024`スタンドアロンで導入された場合、「profilerFQDN」は NPS アプライアンスの完全修飾ドメイン名に置き換えられます。 HA システムの場合、VIP の FQDN が使用されます）。 秘密キーの生成を実行するため、パスフレーズの入力と確認が求められます。 このパスフレーズは、今後秘密キーを使用するときに必要となります。 必ず、秘密キーの生成に使用したパスフレーズを書き留めてください。
4. 最後のステップで生成した秘密キーを使用して証明書署名要求（CSR）を生成します。これが認証局（CA）に送信され、このシステムの証明書（CRT）が生成されます。次のコマンドを入力して、CSR を生成します`openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr`（「profilerFQDN」では、システムの完全修飾ドメイン名に置き換えます）。システムの CSR を作成すると、秘密キーのパスフレーズを入力するように求められます。 入力して続行します。証明書要求と識別名（DN）の生成に組み込まれたいくつかの属性を入力するように求められます。 これらの項目のいくつかは、デフォルト値が推奨されます（[]）。 DN の各パラメータに目的とする値、または「.」を入力して 項目をスキップします。
5. 次のコマンドを使用して、CSR の内容を検証します`openssl req -noout -text -in profilerFQDN.csr`（「profilerFQDN」では、システムの完全修飾ドメイン名に置き換えます）。 このコマンドは、CSR と最後のステップで入力した DN についての情報を返します。CSR の情報を変更する必要がある場合、このエンティティで手順 4 を繰り返します。
6. 内部ポリシーに従って、選択した認証局（CA）に CSR を提出します。 要求が送信されると、CA の秘密キーによってデジタル署名されたアイデンティティ証明書が CA から返されます。 Profiler システムで、任意の CA で署名された新しい CRT を使用して工場出荷時の CRT の置き換えると、その CRT が有効である限り、Profiler UI にアクセスするブラウザがサイトのアイデンティティを検証できるため、NPS サーバで Web サーバへの接続時にブラウザに表示される警告メッセージが、ユーザ認証の前に表示されなくなります。（これは、ブラウザが CA を [Trusted Root Certificate Authorities] に追加していると想定されます)。
7. 使用する CA によっては、認証局が要求するアイデンティティに対する他のクレデンシャルや証明情報などの追加情報の提出が CRS とともに求められる場合があり、証明機関が申請者と連絡を取ってさらに情報を求めることもあります。デジタル署名された CRT が CA か

ら返されたら、次の手順に進み、工場出荷時の秘密キーと証明書を、前述の手順で作成したものと置き換えます。 HA システムでは、ペアのセカンダリ アプライアンスにも同じ手順を使用して秘密キーと証明書をインストールします。

8. 証明書と秘密キー ファイルを内部セキュリティ ポリシーで指定された場所に移動するか（該当する場合）、デフォルトの場所を使用します。内部セキュリティ ポリシーで指定されていない場合、秘密キーは /etc/pki/tls/private/ に配置する必要があります。 コマンド`mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`内部セキュリティ ポリシーで指定されていない場合、証明書は /etc/pki/tls/certs/ に配置する必要があります。`mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. vi などの工ディタを使用して **ssl.conf ファイル**を編集し、Web サーバに新しい秘密キーと証明書を使用させるために必要な変更を行います（ssl.conf は /etc/httpd/conf.d/ にあります）。**ssl.conf** では、サーバ証明書部分はライン 107 から始まります。 ステップ 8.b でシステムに配置された新しい証明書ファイルを指定するように、工場出荷時のデフォルト（/etc/pki/tls/certs/localhost.cert）から SSLCertificateFile の設定項目を変更します。**ssl.conf** では、サーバ秘密キー部分はライン 114 から始まります。 ステップ 8.a でシステムに作成された新しい秘密キー ファイルを指定するように、工場出荷時のデフォルト（etc/pki/tls/private/localhost.key）からサーバ秘密キーの設定項目を変更します。
10. 次のコマンドを使用して、アプライアンス上で Apache Web サーバを再起動してください。`apachectl -k restart` **注:** スタンドアロンで導入した場合、ステップ 12 に進みます。
11. HA NPS システムのみ、次のステップを実施して、HA ペアの他のメンバー（現在のセカンダリ）上で秘密キーと CRT をインストールします。 これにより、ペアのどちらのアプライアンスがプライマリかを問わず、UI の SSL セキュリティ メカニズムが同様に動作するようになります。ステップ 3 でプライマリ アプライアンスに生成した秘密キーを、セカンダリ アプライアンスにコピーします。 内部セキュリティ ポリシーで指定されていない場合、秘密キーは /etc/pki/tls/private/ に配置する必要があります。 次のコマンドを使用します（プライマリの /etc/pki/tls/private ディレクトリから）。`scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/`を探します。 CA から戻された署名 CRT をプライマリからセカンダリ アプライアンスにコピーします。 内部セキュリティ ポリシーで指定されていない場合、証明書は /etc/pki/tls/certs/ に配置する必要があります。`scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs` セカンダリ アプライアンスで SSH を実行し、vi などの工ディタを使用して ssl.conf ファイルを編集し、セカンダリの Web サーバに新しい秘密キーと証明書を使用させるために必要な変更を行います（ssl.conf は /etc/httpd/conf.d/ にあります）。**ssl.conf** では、サーバ証明書部分はライン 107 から始まります。 ステップ 11.b でシステムに配置された新しい証明書ファイルを指定するように、工場出荷時のデフォルト（/etc/pki/tls/certs/localhost.cert）から SSLCertificateFile の設定項目を変更します。**ssl.conf** では、サーバ秘密キー部分はライン 114 から始まります。 ステップ 11.a でシステムに作成された新しい秘密キー ファイルを指定するように、工場出荷時のデフォルト（etc/pki/tls/private/localhost.key）からサーバ秘密キーの設定項目を変更します。次のコマンドを使用して、セカンダリ アプライアンス上で Apache Web サーバを再起動してください。`apachectl -k restart`
12. Profiler UI にアクセスして、ブラウザで証明書の警告が生成されずに HTTPS セッションが起動することを確認します。 警告が続く場合は、使用するブラウザの発行元 CA がその [Trusted Root Certificate Authorities] に追加されていることを確認します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco NAC アプライアンス (Clean Access) に関する製品ページ
- テクニカルサポートとドキュメント - Cisco Systems