Importando Certificados SSL ao perfilador NAC

Índice

Introdução

O sistema UI com base na Web do perfilador pode usar Certificados digitais de modo que a autenticidade do servidor de Web encaixado no server do Cisco NAC Profiler possa ser verificada pelo navegador enquanto conecta para o acesso à interface do utilizador do perfilador servida pelo HTTPS. O sistema leverages um da maioria de aplicativos comuns do PKI e dos Certificados digitais onde o navegador da Web valida que um servidor de Web SSL é autêntico de modo que o usuário sinta seguro que sua interação com o servidor de Web, está confiada de fato e suas comunicações com ela segura. Este é o mesmo mecanismo que é usado hoje para fixar o comércio eletrônico e as outras comunicações seguras com os sites de muitos tipos que usam o SSL.

O sistema do perfilador envia com um certificado digital “auto-assinado” que permita o acesso ao UI mas sem verificação do servidor de Web a bordo SSL como confiado. Até que o certificado do padrão esteja substituído com o um criado com os atributos ambiente-específicos, tais como o nome do servidor, e assinado por um Certificate Authority (CA), os navegadores da Web que alcançam o indicador do perfilador UI um aviso similar a este exemplo, que indicam que o navegador não reconhece CA que emitiu o certificado e é incapaz verificam-no como uma site confiável.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Server NAC

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Tarefas principal: Instale o certificado

A maioria de navegadores exigem o usuário fornecer a entrada adicional para continuar a conexão, que pode ser incômodo.

A fim utilizar inteiramente a segurança aumentada tida recursos para pelo uso dos Certificados digitais para a Segurança SSL da relação do perfilador, as mudanças à configuração de subsistema SSL dos NP devem ser feitas. Aquelas mudanças exigem a substituição da chave privada e do certificado digital que são usadas pelo sistema à revelia com as aquelas emitidas por um Certificate Authority confiado e que são específicas à instalação. Após este procedimento, o navegador inicia uma sessão HTTPS com o server e toma o usuário imediatamente ao processo de login UI para contornear os avisos do certificado.

Duas opções

Há duas alternativas para esta nos sistemas NP:

1. Utilize o residente do conjunto de ferramentas do OpenSSL no dispositivo para gerar um certificado assinado que possa ser instalado no sistema de servidor NP e nos PC usados para controlar o sistema com a Web UI.

Esta opção pode ser usada nos ambientes que atualmente não têm CA interno e o escolhem não confiar nos fornecedores comerciais de CA que carregam uma taxa para fornecer um certificado digital assinado que seja reconhecido pela maioria de navegadores comerciais automaticamente.

2. Use o conjunto de ferramentas do OpenSSL para gerar uma solicitação de assinatura de certificado para o sistema NP que é submetido a um serviço comercial interno ou externo de CA, que retorne um certificado digital pronto para uso, assinado para o uso no sistema.

Étipicamente uma matéria da política de segurança interna da organização em que o sistema do perfilador é instalado para fazer a determinação de que opção para se usar em um ambiente específico. As instruções detalhadas para ambas as opções são fornecidas no restante deste documento.

Opção 1: Use o conjunto de ferramentas do OpenSSL em Beacon/NPS para gerar o sinal

Antes de começar o procedimento esboçado, é importante verificar que o sistema do perfilador está configurado corretamente para utilizar o serviço de nome do empreendimento, e que uma

entrada de DNS está feita a tais que o sistema tem um nome de domínio totalmente qualificado (FQDN). A fim verificar que este é o caso, assegure-se de que você possa abrir uma sessão UI com o sistema do perfilador com o FQDN do sistema (isto é, https://beacon.bspruce.com/beacon) em vez do endereço IP de Um ou Mais Servidores Cisco ICM NT (ou do VIP no caso dos sistemas HA) na URL quando você consulta ao UI.

Este procedimento está usado nos casos quando não se deseja submeter o CSR a um fora-dispositivo CA para assinar. Este procedimento permite a criação de um certificado assinado com o conjunto de ferramentas do OpenSSL no dispositivo exclusivamente - nada precisa de ser submetido a um outro sistema ou anúncio publicitário CA para gerar um certificado assinado para o sistema do perfilador.

O sucesso deste procedimento é dependente de segui-lo como especificado. A sintaxe de comando é erros longos e inclinados. Assegure-se de que você esteja no diretório correto como especificado nas instruções antes que você execute os comandos. A informação para os DN gerados para o certificado de CA e a solicitação de assinatura de certificado, tal como o país, o estado, a cidade, o nome do servidor, etc., deve ser incorporada identicamente (diferenciando maiúsculas e minúsculas), assim que seja certo fazer anotações como você terminar as etapas para assegurar-se de que o processo vá lisamente.

1. Inicie um SSH ou uma sessão de console ao dispositivo NP e eleve-os ao acesso raiz. Para sistemas HA, assegure-se de que você esteja no sistema preliminar iniciando um SSH ao VIP.Antes de usar o OpenSSL pela primeira vez, alguma estrutura de arquivo utilizada pelo OpenSSL deve ser inicializada. Termine estas etapas para inicializar o OpenSSL:
2. Mude o diretório a /etc/pki/CA com este comando:
   ```
   cd /etc/pki/CA/
   ```
   Crie um diretório novo chamado **newcerts**, e emita estes comandos:
   ```
   mkdir newcerts touch index.txt
   ```
3. O uso vi criar um arquivo novo nomeou a **série**; a inserção **01 no** arquivo, e compromete as mudanças. (: wq!)Mude este diretório:CD /etc/pki/tls/certs
4. Gerencia uma chave privada nova para o sistema com este comando:
   ```
   openssl genrsa -out profilerFQDN.key 1024
   ```
   (onde o “profilerFQDN” for substituído com o nome de domínio totalmente qualificado do dispositivo NP quando autônomo distribuído. Para sistemas HA, o FQDN do VIP deve ser usado).Se o sistema do perfilador não está no DNS, o endereço IP de Um ou Mais Servidores Cisco ICM NT do server (VIP) pode ser usado em vez do FQDN, mas do certificado está amarrado a este endereço IP de Um ou Mais Servidores Cisco ICM NT, que exige o uso do IP na URL (isto é, https://10.10.0.1/profiler) para evitar os avisos do certificado.
5. Gerencia um certificado de CA para usar-se para gerar o certificado de servidor com este comando, que cria um certificado de CA de 3 anos, e a chave gerada na etapa #4:
   ```
   openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem
   ```
   Você é alertado para diversos atributos que são incorporados no pedido do certificado e na formação de um nome destacado (DN) para o certificado de CA. Para algum do este estes artigos, um valor padrão são sugeridos (no []). Incorpore o valor desejado para cada parâmetro do DN ou “.” A fim saltar o artigo, seja certo fazer uma anotação dos parâmetros DN usados nesta etapa. Devem ser idênticos àqueles especificados na geração da solicitação de assinatura de certificado para o certificado de servidor na etapa #7.Mova o certificado de CA criado na última etapa para o diretório exigido:
   ```
   mv cacert.pem /etc/pki/CA
   ```

Gerencia uma solicitação de assinatura de certificado para o sistema do perfilador com a chave privada nova:

```
openssl req -new -key profilerFQDN.key -out profilerFQDN.csr
```

6. Apenas como na etapa #5, você é alertado terminar um DN para o sistema para o server CSR. Assegure-se de que você use os mesmos valores para o server CSR que foram usados para o certificado de CA na etapa #5. Se há alguma variação nos parâmetros, o CSR não está criado com sucesso. Além, você é alertado criar uma frase de passagem para o certificado. Seja certo fazer uma anotação da frase de passagem.
7. Gerencia o certificado de servidor com o CSR e a chave privada gerados nas etapas precedentes. A saída desta etapa é o certificado assinado que é instalado no server do perfilador (ou em server, no caso dos pares HA).

   ```
   openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key
   ```

   Você é alertado assinar e comprometer o certificado. Incorpore **y** para confirmar a assinatura e comprometer do certificado para terminar a geração do certificado de servidor.
8. Mova o arquivo certificado para o lugar especificado pela política de segurança interna (se aplicável) ou use os locais padrões:Os Certificados devem ser colocados em /etc/pki/tls/certs/ se nenhum lugar é especificado pela política de segurança interna.

   ```
   mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
   ```
9. Mova o arquivo-chave privado para o lugar especificado pela política de segurança interna (se aplicável) ou use os locais padrões:A chave privada deve ser colocada em /etc/pki/tls/private/ se nenhum lugar é especificado pela política de segurança interna. Use o comando:

   ```
   mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
   ```
10. Edite o **arquivo ssl.conf** com um editor como vi para fazer alterações necessárias para forçar o servidor de Web do perfilador para usar a chave privada e o certificado novos (ssl.conf é encontrado em /etc/httpd/conf.d/).**Em ssl.conf, a** parcela do certificado de servidor começa na linha 107. Mude o item de configuração de SSLCertificateFile do padrão de fábrica (/etc/pki/tls/certs/localhost.cert) para apontar ao arquivo certificado novo que foi criado no sistema na etapa #8.**Em ssl.conf, a** parcela da chave privada do server começa na linha 114. Mude o item de configuração da chave privada do server do padrão de fábrica (etc./pki/tls/privado/localhost.key) para apontar ao arquivo-chave privado novo colocado no sistema na etapa #9.
11. Reinicie o servidor da Web Apache no dispositivo com este comando:

    ```
    apachectl -k restart
    ```

    Note: Se o sistema é autônomo distribuído, salte para pisar #13.
12. Para sistemas HA NP somente, termine estas etapas para instalar a chave privada e o CRT no outro membro (secundário atual) dos pares HA. Isto assegura-se de que, apesar de que o dispositivo é preliminar nos pares, os mecanismos de segurança SSL para o UI se operem identicamente.a. Copie a chave privada gerada no dispositivo preliminar na etapa #3 ao dispositivo secundário. A chave privada deve ser colocada em /etc/pki/tls/private/ se nenhum lugar é especificado pela política de segurança interna. Use este comando (do diretório de /etc/pki/tls/private em preliminar):

    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```

    Copie o CRT assinado que foi retornado de CA do preliminar ao dispositivo secundário. Os Certificados devem ser colocados em /etc/pki/tls/certs/ se nenhum lugar é especificado pela política de segurança interna.

    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```

    O SSH ao dispositivo secundário e edita seu **arquivo ssl.conf** com um editor como vi para fazer alterações necessárias para forçar o servidor de Web no secundário para usar a

chave privada e o certificado novos (ssl.conf é encontrado em /etc/httpd/conf.d/)**Em ssl.conf, a** parcela do certificado de servidor começa na linha 107. Mude o item de configuração de SSLCertificateFile do padrão de fábrica (/etc/pki/tls/certs/localhost.cert) para apontar ao arquivo certificado novo colocado no sistema na etapa #11b.**Em ssl.conf, a** parcela da chave privada do server começa na linha 114. Mude o item de configuração da chave privada do server do padrão de fábrica (etc./pki/tls/privado/localhost.key) para apontar ao arquivo-chave privado novo colocado no sistema na etapa #11a.Reinicie o servidor da Web Apache no dispositivo secundário com este comando:
`apachectl -k restart`
Porque o certificado de servidor que foi criado com estas etapas utilizou CA privado, os navegadores que alcançam o perfilador UI têm que ser configurados para instalar o certificado no repositório do Certificate Authority do root confiável em Windows PC com IE 7.0. Siga estes passos:Copie o certificado de servidor criado ao diretório de /home/beacon do dispositivo:
`cp profilerFQDN.crt /home/beacon`
Use WinSCP ou um software comparável ao SCP o arquivo .crt do dispositivo ao PC.Fazer duplo clique o **arquivo .crt** para começar o gerenciador certificado de Windows, e o clique **instala o certificado**, que começa o assistente da importação do certificado.Escolha o **botão de rádio**. Coloque todos os Certificados nesta loja para ativar o **botão Browse**.Escolha **consultam**, e clicam a loja do certificado das **Autoridades de certificação de raiz confiável**.Clique a **APROVAÇÃO** para aceitar este certificado.Repita este processo nos outros PC que são usados para controlar o sistema do perfilador.

13. Alcance o perfilador UI e note que a sessão HTTPS começa sem os avisos do certificado gerados pelo navegador.

Opção 2: Gerencia/submeta o CSR a CA interno/externo

Antes que você comece o procedimento esboçado em seguida, é importante verificar que o sistema do perfilador está configurado corretamente para utilizar o serviço de nome do empreendimento, e que uma entrada de DNS está feita a tais que o sistema tem um nome de domínio totalmente qualificado (FQDN). A fim verificar que este é o caso, assegure-se de que você possa abrir uma sessão UI com o sistema do perfilador com o FQDN do sistema (isto é, https://beacon.bspruce.com/beacon) em vez do endereço IP de Um ou Mais Servidores Cisco ICM NT ou do VIP no caso dos sistemas HA.

Termine estas etapas para gerar uma chave privada nova para o sistema, gerencia um CSR para apresentação a CA interno ou externo, e coloque então o certificado assinado válido no NP:

1. Inicie um SSH ou uma sessão de console ao dispositivo NP, e eleve-a ao acesso raiz. Para sistemas HA, inicie o SSH ao VIP para assegurar-se de que você esteja no sistema preliminar.
2. Vá ao diretório do padrão PKI para NP:
   `cd /etc/pki/tls`
3. Use este comando gerar um arquivo-chave privado novo para o sistema:
   `openssl genrsa ?des3 ?out profilerFQDN.key 1024`
   Onde o “profilerFQDN” for substituído com o nome de domínio totalmente qualificado do dispositivo NP quando autônomo distribuído. Para sistemas HA, o FQDN do VIP deve ser usado). Você é alertado entrar e confirmar em uma frase de passagem para terminar a geração da chave privada. Esta frase de passagem é exigida para as operações futuras usando a chave privada. Seja certo fazer a anotação da frase de passagem usada para a

geração de chave privada.

4. Com a chave privada gerada na última etapa, gerencia uma solicitação de assinatura de certificado (CSR) que está enviado ao Certificate Authority (CA) para a geração do certificado (CRT) para este sistema.

   Use este comando gerar o CSR
   ```
   openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr
   ```
   (Substitua o nome de domínio totalmente qualificado do sistema para o "profilerFQDN".)Você está alertado para a frase de passagem para a chave privada quando você cria o CSR para o sistema; entre n para continuar.Você é alertado então para diversos atributos que são incorporados no pedido do certificado e na formação de um nome destacado (DN). Para algum do este estes artigos, um valor padrão são sugeridos (no []). Incorpore o valor desejado para cada parâmetro do DN ou "." para saltar o artigo.
5. Verifique os índices do CSR com este comando:
   ```
   openssl req -noout -text -in profilerFQDN.csr
   ```
   (Substitua o nome de domínio totalmente qualificado do sistema para o "profilerFQDN".) Isto retornam a informação sobre o CSR e o DN que foram incorporados à última etapa. Se alguma informação no CSR precisa de ser mudada, repita a etapa #4 em sua totalidade
6. Submeta o CSR ao Certificate Authority (CA) escolhido de acordo com as políticas internas. Se o pedido é bem sucedido, CA envia para trás um certificado de identidade que seja assinado digitalmente com a chave privada de CA. Quando este CRT novo assinado por seu CA escolhido é usado para substituir o padrão de fábrica CRT no sistema do perfilador, todo o navegador que alcançar o perfilador UI pode verificar a identidade do local, e os mensagens de advertência no navegador considerado em cima da conexão ao servidor de Web nos NP que o server está indicado já não antes da autenticação de usuário para enquanto o CRT permanece válido. (Isto supõe que o navegador teve CA adicionado a suas autoridades de certificação do root confiável.)
7. O dependente em cima de CA que é usado, da informação adicional as necessidades possivelmente de ser submetido junto com o CSR, tal como outras credenciais ou provas de identidade exigidas pelo Certificate Authority, e pelo Certificate Authority podem contactar o candidato para mais informações.Uma vez que o CRT digitalmente assinado volta de CA, continue com próxima etapa substituir a chave privada e o certificado da fábrica com os aqueles criados nas etapas acima. Para sistemas HA, o mesmo procedimento é usado para instalar a chave privada e o certificado no dispositivo secundário nos pares, também.
8. Mova o certificado e o arquivo-chave privado para o lugar especificado pela política de segurança interna, se aplicável, ou use os locais padrões:A chave privada deve ser colocada em /etc/pki/tls/private/ se nenhum lugar é especificado pela política de segurança interna. Use este comando:
   ```
   mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
   ```
   Os Certificados devem ser colocados em /etc/pki/tls/certs/ se nenhum lugar é especificado pela política de segurança interna.
   ```
   mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
   ```
9. Edite o **arquivo ssl.conf** com um editor tal como Vito fazem alterações necessárias para forçar o servidor de Web para usar a chave privada e o certificado novos (ssl.conf é encontrado em /etc/httpd/conf.d/).**Em ssl.conf, a** parcela do certificado de servidor começa na linha 107. Mude o item de configuração de SSLCertificateFile do padrão de fábrica (/etc/pki/tls/certs/localhost.cert) para apontar ao arquivo certificado novo colocado no sistema na etapa #8.b.**Em ssl.conf, a** parcela da chave privada do server começa na linha 114. Mude o item de configuração da chave privada do server do padrão de fábrica

(etc./pki/tls/privado/localhost.key) para apontar ao arquivo-chave privado novo colocado no sistema na etapa #8.a.

10. Reinicie o servidor da Web Apache no dispositivo com este comando:
    ```
    apachectl -k restart
    ```
    Note: Se o sistema é autônomo distribuído, salte para pisar #12.
11. Para sistemas HA NP somente, termine estas etapas para instalar a chave privada e o CRT no outro membro (secundário atual) dos pares HA. Isto assegura-se de que, apesar de que o dispositivo é preliminar nos pares, os mecanismos de segurança SSL para o UI se operem identicamente.Copie a chave privada gerada no dispositivo preliminar na etapa #3 ao dispositivo secundário. A chave privada deve ser colocada em /etc/pki/tls/private/ se nenhum lugar é especificado pela política de segurança interna. Use este comando (do diretório de /etc/pki/tls/private em preliminar):
    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```
    . Copie o CRT assinado retornado de CA do preliminar ao dispositivo secundário. Os Certificados devem ser colocados em /etc/pki/tls/certs/ se nenhum lugar é especificado pela política de segurança interna.
    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```
    O SSH ao dispositivo secundário e edita seu arquivo ssl.conf com um editor como vi para fazer alterações necessárias para forçar o servidor de Web no secundário para usar a chave privada e o certificado novos (ssl.conf é encontrado em /etc/httpd/conf.d/).**Em ssl.conf, a** parcela do certificado de servidor começa na linha 107. Mude o item de configuração de SSLCertificateFile do padrão de fábrica (/etc/pki/tls/certs/localhost.cert) para apontar ao arquivo certificado novo colocado no sistema na etapa #11.b.**Em ssl.conf, a** parcela da chave privada do server começa na linha 114. Mude o item de configuração da chave privada do server do padrão de fábrica (etc./pki/tls/privado/localhost.key) para apontar ao arquivo-chave privado novo colocado no sistema na etapa #11.a.Reinicie o servidor da Web Apache no dispositivo secundário com este comando:
    ```
    apachectl -k restart
    ```
12. Alcance o perfilador UI e note que a sessão HTTPS começa sem os avisos do certificado gerados pelo navegador. Se o aviso persiste, verifique que o navegador usado tem CA de emissão adicionado a suas autoridades de certificação do root confiável.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Página de produto do Dispositivo Cisco NAC (Clean Access)
- Suporte Técnico e Documentação - Cisco Systems