Importation de certificats SSL dans NAC Profiler

Contenu

Introduction

Le système UI basé sur le WEB de profileur peut utiliser des Certificats numériques de sorte que l'authenticité du web server inclus sur le serveur de Cisco NAC Profiler puisse être vérifiée par le navigateur pendant qu'elle se connecte pour l'accès à l'interface utilisateur de profileur servie par HTTPS. Le système accroît une des la plupart des applications courantes du PKI et des Certificats numériques où le navigateur Web valide qu'un web server SSL est authentique de sorte que les impressions d'utilisateur sécurisent que leur interaction avec le web server est en fait faite confiance et leurs transmissions avec elle sécurisée. C'est le même mécanisme qui est utilisé aujourd'hui pour sécuriser le commerce électronique et d'autres communications protégées avec des sites Web de beaucoup de types qui utilisent le SSL.

Le système de profileur se transporte avec un certificat numérique « auto-signé » qui permet l'accès à l'UI mais sans vérification du web server à bord SSL comme fait confiance. Jusqu'à ce que le certificat par défaut soit remplacé par un créé avec des attributs d'environnement-particularité, tels que le nom du serveur, et soit signé par un Autorité de certification (CA), les navigateurs Web qui accèdent à l'affichage du profileur UI un avertissement semblable à cet exemple, qui indiquent que le navigateur n'identifie pas le CA qui a délivré le certificat et ne peut pas le vérifient comme un site de confiance.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur NAC

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Tâche principale : Installez le certificat

La plupart des navigateurs exigent de l'utilisateur de fournir les données supplémentaires pour continuer la connexion, qui peut être gênante.

Afin d'utiliser entièrement la Sécurité accrue accordée en employant des Certificats numériques pour la sécurité ssl de l'interface de profileur, des modifications à la configuration de sous-système SSL du NPS doivent être apportées. Ces modifications exigent le remplacement de la clé privée et du certificat numérique qui sont utilisées par le système par défaut avec ceux émis par une autorité de certification de confiance et qui sont spécifiques à l'installation. Après cette procédure, le navigateur initie une session HTTPS avec le serveur et prend l'utilisateur immédiatement au processus de procédure de connexion UI pour sauter les avertissements de certificat.

Deux options

Il y a deux solutions de rechange pour ceci sur les systèmes NPS :

1. Utilisez le résident de boîte à outils d'OpenSSL sur l'appliance pour générer un certificat signé qui peut être installé sur le système serveur NPS et les PC utilisés pour gérer le système par le Web UI.

Cette option peut être utilisée dans les environnements qui actuellement n'ont pas un CA interne et choisissent de ne pas compter sur les fournisseurs commerciaux CA qui chargent des frais pour fournir un certificat numérique signé qui est identifié par la plupart des navigateurs commerciaux automatiquement.

2. Employez la boîte à outils d'OpenSSL pour générer une demande de signature de certificat du système NPS qui est soumis à un service interne ou externe du message publicitaire CA, qui renvoie un certificat numérique prêt à employer et signé pour l'usage sur le système.

C'est typiquement une question de la stratégie de sécurité intérieure de l'organisation dans laquelle le système de profileur est installé pour faire la détermination dont option de utiliser dans un environnement spécifique. Le mode d'emploi détaillé pour les deux options est fourni dans le reste de ce document.

Option 1 : Boîte à outils d'OpenSSL d'utilisation sur Beacon/NPS pour générer le signe

Avant de commencer la procédure tracée les grandes lignes, il est important de vérifier que le système de profileur est correctement configuré pour utiliser le service de nom d'entreprise, et qu'une entrée DNS est faite à tels que le système a un nom de domaine complet (FQDN). Afin de vérifier que c'est le cas, assurez-vous que vous pouvez ouvrir une session UI avec le système de profileur avec le FQDN du système (c'est-à-dire, https://beacon.bspruce.com/beacon) au lieu de l'adresse IP (ou du VIP dans le cas des systèmes ha) dans l'URL quand vous parcourez à l'UI.

Cette procédure est utilisée dans des cas quand on ne le désire pas pour soumettre le CSR à une hors fonction-appliance CA pour la signature. Cette procédure tient compte de la création d'un certificat signé avec la boîte à outils d'OpenSSL sur l'appliance exclusivement - rien ne doit être soumise à un système ou à un CA commercial différent pour générer un certificat signé pour le système de profileur.

Le succès de cette procédure dépend de le suivre comme spécifié. La syntaxe de commande est longues et enclines à erreurs. Assurez-vous que vous êtes dans le répertoire correct comme spécifié dans les instructions avant que vous exécutiez les commandes. Les informations pour les dn générés pour le certificat de CA et la demande de signature de certificat, telle que le pays, l'état, ville, le nom du serveur, etc., doivent être écrites identiquement (distinguant majuscules et minuscules), ainsi soient sûres de faire des notes pendant que vous vous terminez les étapes pour s'assurer que le processus va sans à-coup.

1. Initiez un SSH ou une session de console à l'appliance NPS et les élevez pour enraciner l'accès. Pour des systèmes ha, assurez-vous que vous êtes sur le système primaire en initiant un SSH au VIP.Avant d'utiliser OpenSSL pour la première fois, une certaine structure de fichier utilisée par OpenSSL doit être initialisée. Terminez-vous ces étapes pour initialiser OpenSSL :
2. Changez le répertoire à /etc/pki/CA avec cette commande : `cd /etc/pki/CA/`Créez un nouveau répertoire appelé les **newcerts**, et émettez ces commandes :`mkdir newcerts touch index.txt`
3. L'utilisation vi de créer un nouveau fichier a nommé l'**interface série** ; l'insertion **01** dans le fichier, et commettent les modifications. (: wq !)Changez ce répertoire :cd /etc/pki/tls/certs
4. Générez une nouvelle clé privée pour le système avec cette commande :`openssl genrsa -out profilerFQDN.key 1024`(où le « profilerFQDN » est remplacé par le nom de domaine complet de l'appliance NPS quand autonome déployé. Pour des systèmes ha, le FQDN du VIP doit être utilisé).Si le système de profileur n'est pas dans des DN, l'adresse IP du serveur (VIP) peut être utilisée au lieu du FQDN, mais du certificat est attachée à cette adresse IP, qui exige l'utilisation de l'IP dans l'URL (c'est-à-dire, https://10.10.0.1/profiler) pour éviter les avertissements de certificat.
5. Générez un certificat de CA pour l'utiliser pour générer le certificat de serveur avec cette commande, qui crée des 3 certificats de CA d'an, et la clé générée dans l'étape #4 :`openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem`Vous êtes incité pour plusieurs attributs qui sont incorporés à la demande de certificat et à la formation d'un nom unique (DN) pour le certificat de CA. Pour une partie de ce ces éléments, une valeur par défaut est suggérés (dedans []). Écrivez la valeur désirée pour chaque paramètre du DN ou « . » Afin d'ignorer l'élément, soyez sûr de noter les paramètres de DN utilisés dans cette étape. Ils doivent être identiques à ceux spécifiés dans la génération de la demande de signature de certificat du certificat de serveur dans l'étape #7.Déplacez le certificat de CA créé dans la dernière étape au répertoire requis :`mv cacert.pem /etc/pki/CA`Générez une demande de signature de certificat du système de profileur avec la nouvelle clé privée :`openssl req -new -key profilerFQDN.key -out profilerFQDN.csr`

6. Juste comme dans l'étape #5, vous êtes incité à se terminer un DN pour le système pour le CSR de serveur. Assurez-vous que vous utilisez les mêmes valeurs pour le CSR de serveur qui ont été utilisées pour le certificat de CA dans l'étape #5. S'il y a des variations des paramètres, le CSR n'est pas créé avec succès. En outre, vous êtes incité à créer un mot de passe pour le certificat. Soyez sûr de noter le mot de passe.
7. Générez le certificat de serveur avec le CSR et la clé privée générés dans les étapes précédentes. La sortie de cette étape est le certificat signé qui est installé sur le serveur de profileur (ou des serveurs, dans le cas des paires ha).`openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key`Vous êtes incité à signer et commettre le certificat. Écrivez **y** pour confirmer signer et commettre le certificat pour se terminer la génération de certificat de serveur.
8. Déplacez le fichier du certificat à l'emplacement spécifié par la stratégie de sécurité intérieure (si c'est approprié) ou utilisez les emplacements par défaut :Les Certificats doivent être placés dans /etc/pki/tls/certs/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure.`mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. Déplacez le fichier principal privé à l'emplacement spécifié par la stratégie de sécurité intérieure (si c'est approprié) ou utilisez les emplacements par défaut :La clé privée doit être placée dans /etc/pki/tls/private/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure. Utilisez la commande :`mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`
10. Éditez le **fichier ssl.conf** avec un éditeur comme vi pour apporter des modifications nécessaires pour forcer le web server de profileur pour utiliser la nouveaux clé privée et certificat (ssl.conf est trouvé dans /etc/httpd/conf.d/).Dans **ssl.conf, la** partie de certificat de serveur commence sur la ligne 107. Changez l'élément de configuration de SSLCertificateFile du par défaut d'usine (/etc/pki/tls/certs/localhost.cert) pour indiquer le nouveau fichier du certificat qui a été créé sur le système dans l'étape #8.Dans **ssl.conf, la** partie de clé privée de serveur commence sur la ligne 114. Changez l'élément de configuration de clé privée de serveur du par défaut d'usine (etc./PKI/tls/privé/localhost.key) pour indiquer le nouveau fichier principal privé placé sur le système dans l'étape #9.
11. Redémarrez l'Apache Web Server sur l'appliance avec cette commande : `apachectl -k restart` **Remarque:** Si le système est autonome déployé, ignorez pour faire un pas #13.
12. Pour des systèmes ha NPS seulement, terminez-vous ces étapes pour installer la clé privée et le tube cathodique sur l'autre membre (secondaire en cours) des paires ha. Ceci s'assure dont que, indépendamment l'appliance est primaire dans les paires, les mécanismes de sécurité ssl pour l'UI fonctionnent identiquement.a. Copiez la clé privée générée sur l'appliance primaire dans l'étape #3 sur l'appliance secondaire. La clé privée doit être placée dans /etc/pki/tls/private/ si aucun emplacement n'est spécifié par la stratégie de sécurité intérieure. Utilisez cette commande (à partir du répertoire de /etc/pki/tls/private sur primaire) :`scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/`Copiez le tube cathodique signé qui a été retourné du CA du primaire à l'appliance secondaire. Les Certificats doivent être placés dans /etc/pki/tls/certs/ si aucun emplacement n'est spécifié par la stratégie de sécurité intérieure.`scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs` Le SSH à l'appliance secondaire et éditent son **fichier ssl.conf** avec un éditeur comme vi pour apporter des modifications nécessaires pour forcer le web server sur le secondaire pour utiliser la nouveaux clé privée et certificat (ssl.conf est trouvé dans /etc/httpd/conf.d/)Dans **ssl.conf, la** partie de certificat de serveur commence sur la ligne 107. Changez l'élément de configuration de SSLCertificateFile du par défaut d'usine (/etc/pki/tls/certs/localhost.cert) pour indiquer le nouveau fichier du certificat placé sur le système dans l'étape #11b.Dans **ssl.conf, la** partie de clé privée de serveur commence sur

la ligne 114. Changez l'élément de configuration de clé privée de serveur du par défaut d'usine (etc./PKI/tls/privé/localhost.key) pour indiquer le nouveau fichier principal privé placé sur le système dans l'étape #11a.Redémarrez l'Apache Web Server sur l'appliance secondaire avec cette commande :`apachectl -k restart`Puisque le certificat de serveur qui a été créé avec ces étapes a utilisé un CA privé, les navigateurs qui accèdent au profileur UI doivent être configurés pour installer le certificat dans le référentiel de confiance d'autorité de certification de racine sur des PC de Windows avec IE 7.0. Suivez ces étapes :Copiez le certificat de serveur créé sur le répertoire de /home/beacon de l'appliance :`cp profilerFQDN.crt /home/beacon`Utilisez WinSCP ou un logiciel comparable au SCP le fichier .crt de l'appliance au PC.Double-cliquer le **fichier .crt** pour commencer le gestionnaire de certificat de Windows, et le clic **installent le certificat**, qui commence l'assistant d'importation de certificat.Choisissez la **case d'option**. Placez tous les Certificats dans cette mémoire pour actionner le **bouton Parcourir**.Choisissez **parcourent**, et cliquent sur la mémoire de certificat d'**Autorités de certification racine approuvée**.Cliquez sur OK pour recevoir ce certificat.Répétez ce processus sur les autres PC qui sont utilisés pour gérer le système de profileur.

13. Accédez au profileur UI et notez que les sessions starts HTTPS sans les avertissements de certificat générés par le navigateur.

Option 2 : Générez/soumettez le CSR au CA interne et externe

Avant que vous commenciez la procédure tracée les grandes lignes ensuite, il est important de vérifier que le système de profileur est correctement configuré pour utiliser le service de nom d'entreprise, et qu'une entrée DNS est faite à tels que le système a un nom de domaine complet (FQDN). Afin de vérifier que c'est le cas, assurez-vous que vous pouvez ouvrir une session UI avec le système de profileur avec le FQDN du système (c'est-à-dire, https://beacon.bspruce.com/beacon) au lieu de l'adresse IP ou du VIP dans le cas des systèmes ha.

Terminez-vous ces étapes pour générer une nouvelle clé privée pour le système, générez un CSR à soumettre à un CA interne ou externe, et puis placez le certificat signé valide sur un NPS :

1. Initiez un SSH ou une session de console à l'appliance NPS, et élevez-la pour enraciner l'accès. Pour des systèmes ha, SSH initié au VIP pour s'assurer que vous êtes sur le système primaire.
2. Allez au répertoire par défaut de PKI pour NPS :`cd /etc/pki/tls`
3. Utilisez cette commande de générer un nouveau fichier principal privé pour le système :`openssl genrsa ?des3 ?out profilerFQDN.key 1024`Là où le « profilerFQDN » est remplacé par le nom de domaine complet de l'appliance NPS quand autonome déployé. Pour des systèmes ha, le FQDN du VIP doit être utilisé). Vous êtes incité à entrer dans et confirmer un mot de passe pour se terminer la génération de la clé privée. Ce mot de passe est exigé pour de futures exécutions utilisant la clé privée. Soyez sûr de noter le mot de passe utilisé pour la génération de clés privée.
4. La clé privée étant généré dans la dernière étape, générez une demande de signature de certificat (CSR) qui est envoyée à l'Autorité de certification (CA) pour la génération du certificat (tube cathodique) pour ce système.Utilisez cette commande de générer le CSR`openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr`(Substituez le nom de domaine complet du système au « profilerFQDN ».)Vous êtes incité pour le mot de passe pour la clé privée quand vous créez le CSR pour le système ; entrez- dansle pour

poursuivre.Vous êtes alors incité pour plusieurs attributs qui sont incorporés à la demande de certificat et à la formation d'un nom unique (DN). Pour une partie de ce ces éléments, une valeur par défaut est suggérés (dedans []). Écrivez la valeur désirée pour chaque paramètre du DN ou « . » pour ignorer l'élément.

5. Vérifiez le contenu du CSR avec cette commande :`openssl req -noout -text -in profilerFQDN.csr`(Substituez le nom de domaine complet du système au « profilerFQDN ».) Ceci renvoie des informations sur le CSR et le DN qui ont été écrits dans la dernière étape. Si n'importe quelles informations dans le CSR doivent être changées, répétez l'étape #4 en sa totalité
6. Soumettez le CSR à l'Autorité de certification (CA) choisi selon les stratégies internes. Si la demande est réussie, le CA renvoie un certificat d'identité qui a été digitalement signé avec la clé privée du Ca. Quand ce nouveau tube cathodique signé par votre CA choisi est utilisé pour remplacer le tube cathodique de par défaut d'usine sur le système de profileur, n'importe quel navigateur qui accède au profileur UI peut vérifier l'identité du site, et les messages d'avertissement dans le navigateur vu sur la connexion au web server sur le serveur NPS ne sont plus affichés avant l'authentification de l'utilisateur pour tant que le tube cathodique reste valide. (Ceci suppose que le navigateur a eu le CA ajouté à ses autorités de confiance de certificat racine.)
7. La personne à charge sur le CA qui est utilisé, des informations complémentaires les besoins probablement d'être soumis avec le CSR, tel que d'autres qualifications ou preuves d'identité priées par l'autorité de certification, et l'autorité de certification peuvent contacter le candidat pour de plus amples informations.Une fois que le tube cathodique digitalement signé revient du CA, procédez à l'étape suivante pour remplacer la clé privée et le certificat d'usine par ceux créés dans les étapes ci-dessus. Pour des systèmes ha, la même procédure est utilisée pour installer la clé privée et le certificat sur l'appliance secondaire dans les paires, aussi bien.
8. Déplacez le certificat et le fichier principal privé à l'emplacement spécifié par la stratégie de sécurité intérieure, si c'est approprié, ou utilisez les emplacements par défaut :La clé privée doit être placée dans /etc/pki/tls/private/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure. Utilisez cette commande :`mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`Les Certificats doivent être placés dans /etc/pki/tls/certs/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure.`mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. Éditez le **fichier ssl.conf** avec un éditeur tel que Vito apportent des modifications nécessaires pour forcer le web server pour utiliser la nouveaux clé privée et certificat (ssl.conf est trouvé dans /etc/httpd/conf.d/).Dans **ssl.conf, la** partie de certificat de serveur commence sur la ligne 107. Changez l'élément de configuration de SSLCertificateFile du par défaut d'usine (/etc/pki/tls/certs/localhost.cert) pour indiquer le nouveau fichier du certificat placé sur le système dans l'étape #8.b.Dans **ssl.conf, la** partie de clé privée de serveur commence sur la ligne 114. Changez l'élément de configuration de clé privée de serveur du par défaut d'usine (etc./PKI/tls/privé/localhost.key) pour indiquer le nouveau fichier principal privé placé sur le système dans l'étape #8.a.
10. Redémarrez l'Apache Web Server sur l'appliance avec cette commande :`apachectl -k restart` **Remarque:** Si le système est autonome déployé, ignorez pour faire un pas #12.
11. Pour des systèmes ha NPS seulement, terminez-vous ces étapes pour installer la clé privée et le tube cathodique sur l'autre membre (secondaire en cours) des paires ha. Ceci s'assure dont que, indépendamment l'appliance est primaire dans les paires, les mécanismes de sécurité ssl pour l'UI fonctionnent identiquement.Copiez la clé privée générée sur

l'appliance primaire dans l'étape #3 sur l'appliance secondaire. La clé privée doit être placée dans /etc/pki/tls/private/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure. Utilisez cette commande (à partir du répertoire de /etc/pki/tls/private sur primaire) :`scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/.` Copiez le tube cathodique signé retourné du CA du primaire sur l'appliance secondaire. Les Certificats doivent être placés dans /etc/pki/tls/certs/ si aucun emplacement n'est spécifié par stratégie de sécurité intérieure.`scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs` Le SSH à l'appliance secondaire et éditent son fichier ssl.conf avec un éditeur comme vi pour apporter des modifications nécessaires pour forcer le web server sur le secondaire pour utiliser la nouveaux clé privée et certificat (ssl.conf est trouvé dans /etc/httpd/conf.d/).Dans **ssl.conf, la** partie de certificat de serveur commence sur la ligne 107. Changez l'élément de configuration de SSLCertificateFile du par défaut d'usine (/etc/pki/tls/certs/localhost.cert) pour indiquer le nouveau fichier du certificat placé sur le système dans l'étape #11.b.Dans **ssl.conf, la** partie de clé privée de serveur commence sur la ligne 114. Changez l'élément de configuration de clé privée de serveur du par défaut d'usine (etc./PKI/tls/privé/localhost.key) pour indiquer le nouveau fichier principal privé placé sur le système dans l'étape #11.a.Redémarrez l'Apache Web Server sur l'appliance secondaire avec cette commande :`apachectl -k restart`

12. Accédez au profileur UI et notez que les sessions starts HTTPS sans avertissements de certificat générés par le navigateur. Si l'avertissement persiste, vérifiez que le navigateur utilisé a le CA émettant ajouté à ses autorités de confiance de certificat racine.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Page produit de Dispositif Cisco NAC (Clean Access)
- Support et documentation techniques - Cisco Systems