EAP-TLS de 802.1x avec la comparaison binaire de certificat exemple de configuration d'AD et NAM de profils

Contenu

Introduction

Ce document décrit la configuration de 802.1x avec le Protocol-transport Layer Security (EAP-TLS) d'authentification extensible et le système de contrôle d'accès (ACS) comme ils exécutent une comparaison binaire de certificat entre un certificat client fourni par le suppliant et le même certificat maintenu dans la Microsoft Active Directory (AD). Le profil du gestionnaire d'accès au réseau d'AnyConnect (NAM) est utilisé pour la personnalisation. La configuration pour tous les composants est présentée dans ce document, avec des scénarios pour dépanner la configuration.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Configurez

Topologie

- suppliant de 802.1x - Windows 7 avec la version de Client à mobilité sécurisé Cisco AnyConnect 3.1.01065 (module NAM)
- authentificateur de 802.1x - commutateur 2960
- serveur d'authentification de 802.1x - Version 5.4 ACS
- ACS intégrés avec l'AD de Microsoft - Contrôleur de domaine - Serveur de Windows 2008

Détails de topologie

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (e0/0 - suppliant connecté)
- C.C - 192.168.10.101
- Windows 7 - DHCP

Écoulement

La station de Windows 7 a AnyConnect NAM installé, qui est utilisé en tant que suppliant pour authentifier au serveur ACS avec la méthode d'EAP-TLS. Le commutateur avec le 802.1x agit en tant qu'authentificateur. Le certificat utilisateur est vérifié par l'ACS et l'autorisation de stratégie applique des stratégies basées sur le nom commun (NC) à partir du certificat. Supplémentaire, l'ACS cherche le certificat utilisateur de l'AD et exécute une comparaison binaire avec le certificat fourni par le suppliant.

Configuration du commutateur

Le commutateur a une configuration de base. Par défaut, le port est dans la quarantaine VLAN 666. Ce VLAN a un accès restreint. Après que l'utilisateur soit autorisé, le port VLAN est modifié.

```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco
```

Préparation de certificat

Pour l'EAP-TLS, un certificat est exigé pour le suppliant et le serveur d'authentification. Cet exemple est basé sur OpenSSL a généré des Certificats. Microsoft Certificate Authority (CA) peut être utilisé pour simplifier le déploiement dans les réseaux d'entreprise.

1. Afin de générer le CA, sélectionnez ces commandes :`openssl genrsa -des3 -out ca.key 1024`
   `openssl req -new -key ca.key -out ca.csr`
   `cp ca.key ca.key.org`
   `openssl rsa -in ca.key.org -out ca.key`
   `openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt`Le certificat de CA est maintenu dans le fichier ca.crt et la clé privée (et non protégée) dans le fichier ca.key.
2. Générez trois certificats utilisateurs et un certificat pour ACS, tout signé par ce CA : CN=test1CN=test2CN=test3CN=acs54Le script pour générer un certificat simple signé par le CA de Cisco est :`openssl genrsa -des3 -out server.key 1024`
   `openssl req -new -key server.key -out server.csr`

   `cp server.key server.key.org`
   `openssl rsa -in server.key.org -out server.key`

   `openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial`
   `-out server.crt -days 365`
   `openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt`
   `-certfile ca.crt`La clé privée est dans le fichier server.key et le certificat est dans le fichier server.crt. La version pkcs12 est dans le fichier server.pfx.
3. Double-cliquer chaque certificat (fichier .pfx) pour l'importer au contrôleur de domaine. Dans le contrôleur de domaine, chacun des trois Certificats est de confiance.

Le même processus peut être suivi dans le Windows 7 (suppliant) ou le Répertoire actif d'utilisation pour pousser les certificats utilisateurs.

Configuration de contrôleur de domaine

Il est nécessaire de tracer le certificat spécifique à l'utilisateur spécifique dans l'AD.

1. Àpartir des utilisateurs et des ordinateurs de Répertoire actif, naviguez vers le répertoire d'**utilisateurs**.
2. Du menu Affichage, choisissez la **fonctionnalité avancée**.
3. Ajoutez ces utilisateurs : test1test2test3Remarque: Le mot de passe n'est pas important.
4. De la fenêtre de Properties, choisissez les **Certificats édités que** tableau choisissent le certificat spécifique pour le test. Par exemple, parce que test1 la NC d'utilisateur est test1.Remarque: N'utilisez pas le mappage de noms (clic droit sur le nom d'utilisateur). Il est utilisé pour différents services.

Àce stade, le certificat binded à un utilisateur spécifique dans l'AD. Ceci peut être vérifié avec l'utilisation du ldapsearch :

```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

Les résultats d'exemple pour test2 sont comme suit :

```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF
oxCzAJBgNVBAYTAlBMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN
jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA
QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n
PulwF4nkcnu1xO/B7x+LpcjxjhQ==
```

Configuration de suppliant

1. Installez cet éditeur de profil, anyconnect-profileeditor-win-3.1.00495-k9.exe.
2. Ouvrez l'éditeur de profil de gestionnaire d'accès au réseau et configurez le profil spécifique.
3. Créez un réseau câblé spécifique.

   Àce stade il est très important est de donner à l'utilisateur le choix pour utiliser le certificat à chaque authentification. Ne cachez pas ce choix. En outre, utilisez le « nom d'utilisateur » car il est importante se souvenir l'identification non protégée il que ce n'est pas le même id qui est utilisé par ACS pour questionner l'AD pour le certificat. Cet id sera configuré dans ACS.
4. Sauvegardez le fichier .xml comme utilisateurs de c:\Users\All \ Cisco \ Client à mobilité sécurisé Cisco AnyConnect \ gestionnaire d'accès au réseau \ système \ configuration.xml.
5. Redémarrez le service du Cisco AnyConnect NAM.

Cet exemple a affiché un déploiement manuel de profil. L'AD a pu être utilisé pour déployer ce

fichier pour tous les utilisateurs. En outre, l'ASA a pu être utilisée pour provision le profil une fois intégrée avec des VPN.

Configuration ACS

1. Joignez le domaine d'AD.Noms d'utilisateur d'AD de correspondances ACS avec l'utilisation du champ NC du certificat reçu du suppliant (dans ce cas c'est test1, test2, ou test3). La comparaison binaire est également activée. Ceci force ACS pour obtenir le certificat utilisateur de l'AD et pour le comparer au même certificat reçu par le suppliant. S'il ne s'assortit pas, l'authentification échoue.
2. Configurez les ordres de mémoire d'identité, qui utilise l'AD pour l'authentification basée sur certificat avec le profil de certificat.

   Ceci est utilisé comme source in d'identité la stratégie d'identité de RAYON.
3. Configurez deux stratégies d'autorisation. La première stratégie est utilisée pour test1 et elle refuse l'accès à cet utilisateur. La deuxième stratégie est utilisée pour le test 2 et elle permet l'accès avec le profil VLAN2.VLAN2 est le profil d'autorisation qui renvoie les attributs RADIUS qui lient l'utilisateur à VLAN2 sur le commutateur.
4. Installez le certificat de CA sur ACS.
5. Générez et installez le certificat (pour l'utilisation d'Extensible Authentication Protocol) signé par le CA de Cisco pour ACS.

Vérifiez

Il est dans bonne pratique de désactiver le service indigène de 802.1x sur le suppliant de Windows 7 puisqu'AnyConnect NAM est utilisé. Avec le profil configuré, on permet au le client pour sélectionner un certificat spécifique.

Quand le certificat test2 est utilisé, le commutateur reçoit une réponse de succès avec les attributs RADIUS.

```
00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client
(0800.277f.5f64) on Interface Et0/0
00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0800.277f.5f64) on Interface Et0/0
switch#
00:02:51: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64|
       AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X|
       EVENT=APPLY

switch#show authentication sessions interface e0/0
           Interface:  Ethernet0/0
          MAC Address:  0800.277f.5f64
           IP Address:  Unknown
           User-Name:  test2
           Status:  Authz Success
           Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  2
      Session timeout:  N/A
```

```
         Idle timeout:  N/A
   Common Session ID:  C0A80A0A00000001000215F0
      Acct Session ID:  0x00000005
           Handle:  0xE8000002

Runnable methods list:
      Method   State
      dot1x    Authc Succes
```

Notez que le VLAN 2 a été assigné. Il est possible d'ajouter d'autres attributs RADIUS à ce profil d'autorisation sur ACS (tel que les temporisateurs avancés de liste de contrôle d'accès ou de réautorisation).

Les logins ACS sont comme suit :

Dépannez

Configurations heure non valide sur ACS

Erreur possible - erreur interne dans le Répertoire actif ACS

Aucun certificat configuré et Binded sur le C.C d'AD

Erreur possible - pour récupérer le certificat utilisateur à partir du Répertoire actif

Personnalisation de profil NAM

Dans les réseaux d'entreprise, est il a informé pour authentifier avec l'utilisation de l'ordinateur et des certificats utilisateurs. Dans un tel scénario, on lui informe utiliser le mode ouvert de 802.1x sur le commutateur avec le VLAN restreint. Sur la réinitialisation d'ordinateur pour le 802.1x, la première session d'authentification est initiée et authentifiée avec l'utilisation du certificat d'ordinateur d'AD. Puis, après que l'utilisateur fournisse des qualifications et des logins au domaine, la deuxième session d'authentification est initiée avec le certificat utilisateur. L'utilisateur est mis dans le VLAN (de confiance) correct avec le plein accès au réseau. Il est intégré bien sur le Cisco Identity Services Engine (ISE).

Puis, il est possible de configurer des authentifications distinctes des onglets d'authentification de machine et d'authentification de l'utilisateur.

Si le mode ouvert de 802.1x n'est pas acceptable sur le commutateur, il est possible d'utiliser le mode de 802.1x avant que la caractéristique de login soit configurée dans la stratégie de client.

Informations connexes

- Guide utilisateur pour le Système de contrôle d'accès sécurisé Cisco 5.3
- Guide de l'administrateur de Client à mobilité sécurisé Cisco AnyConnect, version 3.0
- Client sécurisé 3.0 de mobilité d'AnyConnect : Gestionnaire d'accès au réseau et éditeur de

profil sur Windows

- Support et documentation techniques - Cisco Systems