Authentification Anyconnect ASA 8.x avec la carte eID belge

Contenu

Introduction

Ce document décrit comment installer l'authentification ASA 8.x Anyconnect pour utiliser la carte belge d'eID.

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 :

- ASA 5505 avec le logiciel approprié ASA 8.0
- Client d'AnyConnect
- ASDM 6.0

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.

Informations générales

L'eID est une carte de PKI (infrastructure de clé publique) émise par le gouvernement belge que les utilisateurs doivent utiliser afin d'authentifier sur un PC Windows distant. Le client logiciel d'AnyConnect est installé sur l'ordinateur local et prend des qualifications d'authentification de l'ordinateur distant. Une fois que l'authentification est complète, l'utilisateur distant accède aux ressources centrales par un plein tunnel SSL. L'utilisateur distant provisioned avec une adresse IP obtenue d'un groupe géré par l'ASA.

Installation d'ordinateur local

Système d'exploitation

Le système d'exploitation (Windows, MaOS, Unix, ou Linux) sur votre ordinateur local doit être en cours avec tous les correctifs exigés installés.

Lecteur de cartes

Un lecteur de cartes électronique doit être installé sur votre ordinateur local afin d'utiliser la carte d'eID. Le lecteur de cartes électronique est un périphérique matériel que les establishs un canal de transmission entre les programmes sur l'ordinateur et la puce sur l'ID cardent.

Pour une liste de lecteurs de cartes approuvés, référez-vous à cet URL : http://www.cardreaders.be/en/default.htm

Note: Afin d'utiliser le lecteur de cartes, vous devez installer les gestionnaires recommandés du

constructeur de matériel.

logiciel de délai d'exécution d'eID

Vous devez installer le logiciel d'exécution d'eID fourni par le gouvernement belge. Ce logiciel permet à l'utilisateur distant pour lire, valider, et imprimer le contenu de la carte d'eID. Le logiciel est disponible en français et Néerlandais pour Windows, le MAC OS X, et le Linux.

Le pour en savoir plus, se rapportent à cet URL :

- http://www.belgium.be/zip/eid_datacapture_nl.html

Certificat d'authentification

Vous devez importer le certificat d'authentification dans la mémoire de Microsoft Windows sur l'ordinateur local. Si vous n'importez pas le certificat dans la mémoire, le client d'AnyConnect ne pourra pas établir une connexion SSL à l'ASA.

Procédure

Afin d'importer le certificat d'authentification dans la mémoire de Windows, terminez-vous ces étapes :

1. Insérez votre eID dans le lecteur de cartes, et lancez le middleware afin d'accéder au contenu de la carte d'eID.Le contenu de la carte d'eID apparaît.
2. Cliquez sur l'onglet de **Certificats** (franc).La hiérarchie de Certificats est affichée.
3. Développez la **racine CA de la Belgique**, et puis développez le **citoyen CA.**
4. Choisissez la version d'**authentification de** votre certificat Désigné.
5. Cliquez sur le bouton d'**Enregistrer** (franc).Le certificat est copié dans la mémoire de Windows.

Note: Quand vous cliquez sur les **détails** se boutonnent, une fenêtre est évident que des détails d'affichages au sujet du certificat. Dans les détails tabulez, sélectionnez le **champ Subject** afin de visualiser le gisement de numéro de série. Le gisement de numéro de série contient une seule valeur qui est utilisée pour l'autorisation d'utilisateur. Par exemple, le numéro de série « 56100307215" représente un utilisateur dont la date de naissance est le 3 octobre, 1956 avec un numéro de séquence de 072 et une clef de contrôle de 15. *Vous devez soumettre une demande pour approbation des autorités fédérales afin d'enregistrer ces nombres. Il est de votre responsabilité de faire les déclarations officielles appropriées liées à la maintenance d'une base de données des citoyens belges dans votre pays*.

Vérifiez

Afin de vérifier que le certificat importé avec succès, se terminent ces étapes :

1. Sur un ordinateur Windows XP, ouvrez une fenêtre DOS, et introduisez la commande **MMC**.L'application de console apparaît.
2. Choisissez le **fichier > l'ajout/suppression SNAP-dans** (ou la presse Ctrl+M).L'ajout/suppression SNAP-dans la boîte de dialogue apparaît.
3. Cliquez sur le bouton **Add**.L'ajouter autonome SNAP-dans la boîte de dialogue apparaît.
4. Dans la liste SNAP-Institut central des statistiques autonome disponible, choisissez les

Certificats, et cliquez sur Add.

5. Cliquez sur la **ma** case d'option de **compte utilisateur**, et cliquez sur Finish.Le certificat SNAP-dans apparaît dans l'ajout/suppression SNAP-dans la boîte de dialogue.
6. Cliquez sur **étroitement** afin de clôturer l'ajouter autonome SNAP-dans la boîte de dialogue, et cliquez sur OK alors dans l'ajout/suppression SNAP-dans la boîte de dialogue afin de sauvegarder vos modifications et retourner à l'application de console.
7. Sous le répertoire racine de la console, développez les **Certificats - Utilisateur courant**.
8. Développez **personnel**, et puis développez les **Certificats**.Le certificat importé doit apparaître dans la mémoire de Windows suivant les indications de cette image :

Installation d'AnyConnect

Vous devez installer le client d'AnyConnect sur l'ordinateur distant. Le logiciel d'AnyConnect utilise un fichier de configuration XML qui peut être édité afin de pré-établir une liste de passerelles disponibles. Le fichier XML est enregistré dans ce chemin sur l'ordinateur distant :

C:\Documents and Settings\ *%USERNAME%* \ données des applications \ Cisco \ Cisco AnyConnect VPN Client

là où *%USERNAME%* est le nom d'utilisateur sur l'ordinateur distant.

Le nom du fichier XML est *preferences.xml.* Voici un exemple du contenu du fichier :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

là où *192.168.0.1* est l'adresse IP de la passerelle ASA.

Conditions requises ASA

Assurez-vous que l'ASA répond à ces exigences :

- AnyConnect et ASDM doivent fonctionner dans l'éclair.Afin de remplir les procédures dans ce document, utilisez une ASA 5505 avec le logiciel approprié ASA 8.0 installé. Les applications d'AnyConnect et ASDM doivent être préchargées dans l'éclair. Employez la commande de **show flash** afin de visualiser le contenu de l'éclair :
  ```
  ciscoasa#show flash:
  --#--  --length--  -----date/time------  path
     66  14524416    Jun 26 2007 10:24:02  asa802-k8.bin
     67  6889764     Jun 26 2007 10:25:28  asdm-602.bin
     68  2635734     Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg
  ```
- L'ASA doit fonctionner avec des par défaut d'usine.Vous pouvez ignorer cette condition requise si vous utilisez un nouveau châssis ASA afin de remplir les procédures dans ce document. Autrement, terminez-vous ces étapes afin de remettre à l'état initial l'ASA aux par défaut d'usine :Dans l'application ASDM, connectez au châssis ASA, et choisissez le **fichier > périphérique remis à l'état initial à la configuration d'usine**.Laissez les valeurs par défaut dans le modèle.Connectez votre PC sur les Ethernets 0/1 interface interne, et renouvelez votre adresse IP qui provisioned par le serveur DHCP de l'ASA.**Note**: Afin de remettre à l'état initial l'ASA aux par défaut d'usine de la ligne de commande, utilisez ces commandes :

```
ciscoasa#conf t
ciscoasa#config factory-default 192.168.0.1 255.255.255.0
```

Configuration ASA

Une fois que vous remettez à l'état initial les par défaut d'usine ASA, vous pouvez commencer l'ASDM à 192.168.0.1 afin de connecter à l'ASA sur les Ethernets 0/1 interface interne.

Note: Votre mot de passe précédent est préservé (ou il peut être vide par défaut).

Par défaut, l'ASA reçoit une session entrante de Gestion avec une adresse IP source dans le sous-réseau 192.168.0.0/24. Le serveur DHCP par défaut qui est activé sur l'interface interne de l'ASA fournit des adresses IP dans la plage 192.168.0.2-129/24, valide pour se connecter à l'interface interne avec l'ASDM.

Terminez-vous ces étapes afin de configurer l'ASA :

1. Activez l'interface extérieure
2. Configurez le nom de domaine, le mot de passe, et l'heure système
3. Activez un serveur DHCP sur l'interface extérieure
4. Configurez le pool d'adresses de l'eID VPN
5. Importez le certificat de CA de racine de la Belgique
6. Configurez Secure Sockets Layer
7. Définissez la stratégie de groupe par défaut
8. Définissez le mappage de certificat
9. Ajoutez un utilisateur local
10. Redémarrez l'ASA

Étape 1. Activez l'interface extérieure

Cette étape décrit comment activer l'interface extérieure.

1. Dans l'application ASDM, la **configuration de** clic, et cliquent sur alors l'**installation de périphérique**.
2. Dans la région d'installation de périphérique, choisissez les **interfaces**, et puis cliquez sur l'onglet d'**interfaces**.
3. Sélectionnez l'interface extérieure, et cliquez sur Edit.
4. Dans la section d'adresse IP de l'onglet Général, choisissez l'**option IP de charge statique d'utilisation**.
5. Entrez dans **197.0.100.1** pour l'adresse IP et **255.255.255.0** pour le masque de sous-réseau.
6. Cliquez sur **Apply**.

Étape 2. Configurez le nom de domaine, le mot de passe, et l'heure système

Cette étape décrit comment configurer le nom de domaine, le mot de passe, et l'heure système.

1. Dans la région d'installation de périphérique, choisissez le **nom du périphérique/mot de passe**.
2. Écrivez **cisco.be pour le** nom de domaine, et écrivez cisco123for la valeur du mot de passe

d'enable.**Note**: Par défaut, le mot de passe est vide.
3. Cliquez sur **Apply**.
4. Dans la région d'installation de périphérique, choisissez l'**heure système**, et changez la valeur d'horloge (s'il y a lieu).
5. Cliquez sur **Apply**.

Étape 3. Activez un serveur DHCP sur l'interface extérieure.

Cette étape décrit comment permettre à un serveur DHCP sur l'interface extérieure afin de faciliter le test.

1. Cliquez sur **Configuration**, puis sur **Device Management**.
2. Dans le secteur de Gestion de périphériques, développez le **DHCP**, et choisissez le **serveur DHCP**.
3. Sélectionnez l'interface extérieure de la liste interface, et cliquez sur Edit.La boîte de dialogue de serveur DHCP d'éditer apparaît.
4. Cochez la case de **serveur DHCP d'enable**.
5. Dans le pool d'adresses DHCP, écrivez une adresse IP de 197.0.100.20 à 197.0.100.30.
6. Dans la région globale d'options DHCP, décochez la **configuration automatique d'enable de la** case d'**interface**.
7. Cliquez sur **Apply**.

Étape 4. Configurez le pool d'adresses de l'eID VPN

Cette étape décrit comment définir un groupe d'adresses IP qui sont utilisées pour provision les clients distants d'AnyConnect.

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Dans la région de VPN d'accès de retirer, développez le **réseau (client) Access**, et puis développez l'**affectation d'adresses**.
3. Choisissez les **pools d'adresses**, et puis cliquez sur le bouton d'**ajouter** situé dans Configure nommé zone de groupes d'adresse IP.La boîte de dialogue Add IP Pool apparaît.
4. Dans la zone d'identification, écrivez l'**eID-VPNPOOL**.
5. L'adresse IP commençante et en finissant des champs d'adresse IP, écrivez une plage d'adresse IP de 192.168.10.100 à 192.168.10.110.
6. Choisissez **255.255.255.0 de la** liste déroulante de masque de sous-réseau, cliquez sur OK, et puis cliquez sur Apply.

Étape 5. Importez le certificat de CA de racine de la Belgique

Cette étape décrit comment importer dans l'ASA le certificat de CA de racine de la Belgique.

1. Téléchargez et installez les Certificats CA de racine de la Belgique (belgiumrca.crt et belgiumrca2.crt) du site Web de gouvernement et enregistrez-les sur votre ordinateur local.Le site Web de gouvernement de la Belgique se trouve à cet URL : http://certs.eid.belgium.be/
2. Dans la région de l'Accès à distance VPN, développez la **Gestion de certificat**, et choisissez les **Certificats CA**.

3. Cliquez sur Add, et puis cliquez sur **installent à partir du fichier**.
4. Parcourez à l'emplacement dans lequel vous avez enregistré le le fichier du certificat de CA de racine de la Belgique (belgiumrca.crt), et cliquez sur InstallCertificate**.**
5. Cliquez sur **Appliquer** afin de sauvegarder vos modifications.

Cette image affiche le certificat installé sur l'ASA :

Étape 6. Configurez Secure Sockets Layer

Cette étape décrit comment donner la priorité à des options de chiffrement sécurisées, définir l'image de client de VPN SSL, et définir le profil de connexion.

1. Donnez la priorité aux la plupart des options de chiffrement sécurisées.Dans la région de l'Accès à distance VPN, développez **avancé**, et choisissez les **configurations SSL**. Dans la section de cryptage, les algorithmes actifs sont empilés, dessus vers le bas, comme suit :AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1
2. Définissez l'image de client de VPN SSL pour le client d'AnyConnect.Dans la région de l'Accès à distance VPN, développez **avancé**, développez le **VPN SSL**, et choisissez les **configurations de client**.Dans la région d'images de client de VPN SSL, cliquez sur Add.Choisissez le module d'AnyConnect qui est enregistré dans l'éclair.Le module d'AnyConnect apparaît dans le client de VPN SSL que les images les répertorient suivant les indications de cette image :
3. Définissez le profil de connexion de DefaultWEBVPNGroup.Dans la région de l'Accès à distance VPN, développez le **réseau (client) Access**, et choisissez les **profils de connexion de VPN SSL**.Dans la région d'interfaces d'Access, cochez la **case de Cisco AnyConnect VPN Client d'enable**.Pour l'interface extérieure, vérifiez l'**autoriser Access**, **exigez le certificat client**, et **activez les** cases **DTLS** suivant les indications de cette image :Dans la région de profils de connexion, choisissez **DefaultWEBVPNGroup**, et cliquez sur Edit.La boîte de dialogue de profil de connexion de VPN SSL d'éditer apparaît.Dans la zone de navigation, choisissez **de base**.Dans la région d'authentification, cliquez sur la case d'option de **certificat**.Dans la région de stratégie de groupe par défaut, cochez la case de **Protocol de client de VPN SSL**.Développez **avancé**, et choisissez l'**authentification**.Cliquez sur Add, et ajoutez l'interface extérieure avec un groupe de serveur local suivant les indications de cette image :Dans la zone de navigation, choisissez l'**autorisation**.Dans la région par défaut de groupe de serveurs d'autorisation, choisissez les **GENS DU PAYS de la** liste déroulante de groupe de serveurs, et cochez les **utilisateurs doit exister dans la base de données d'autorisation pour connecter la** case.Dans le nom d'utilisateur traçant la zone, choisissez **SER (numéro de série) de la** liste déroulante primaire de gisement de DN, n'en choisissez **aucun du** gisement secondaire de DN, et cliquez sur OK.

Étape 7. Définissez la stratégie de groupe par défaut

Cette étape décrit comment définir la stratégie de groupe par défaut.

1. Dans la région de l'Accès à distance VPN, développez le **réseau (client) Access**, et choisissez les **stratégies de groupe**.
2. Choisissez le **DfltGrpPolicy de la** liste de stratégies de groupe, et cliquez sur Edit.
3. La boîte de dialogue interne de stratégie de groupe d'éditer apparaît.
4. De la zone de navigation, choisissez le **général**.

5. Pour des pools d'adresses, cliquez sur **choisi** afin de choisir un groupe d'adresses, et choisissez l'**eID-VPNPOOL**.
6. Dans plus de région d'options, décochez les cases d'**IPsec** et **L2TP/IPsec**, et cliquez sur OK.

Étape 8. Définissez le mappage de certificat

Cette étape décrit comment définir les critères de mappage de certificat.

1. Dans la région de l'Accès à distance VPN, cliquez sur **avancé**, et choisissez le **certificat aux cartes de profil de connexion de VPN SSL**.
2. Dans le certificat à la région de cartes de profil de connexion, cliquez sur Add, et choisissez **DefaultCertificateMap de la** liste de carte.Cette carte doit apparier *DefaultWEBVPNProfile* dans tracé au champ de profil de connexion.
3. Dans la région de critères de mappage, cliquez sur Add, et ajoutez ces valeurs :Champ : L'émetteur, le pays (c), des égaux, « soit »Champ : Émetteur, nom commun (NC), égaux, « citoyen Ca »Les critères de mappage devraient apparaître suivant les indications de cette image :
4. Cliquez sur **Apply**.

Étape 9. Ajoutez un utilisateur local

Cette étape décrit comment ajouter un utilisateur local.

1. Dans la région de l'Accès à distance VPN, développez l'**installation d'AAA**, et choisissez les **utilisateurs locaux**.
2. Dans la région d'utilisateurs locaux, cliquez sur Add.
3. Dans le domaine de nom d'utilisateur, écrivez le numéro de série du certificat utilisateur. Par exemple, 56100307215 (comme décrit dans la section de certificat d'authentification de ce document).
4. Cliquez sur **Apply**.

Étape 10. Redémarrez l'ASA

Redémarrez l'ASA afin de s'assurer que toutes les modifications sont appliquées aux services système.

Réglez avec précision

Tout en testant, quelques tunnels SSL ne pourraient pas se fermer correctement. Puisque l'ASA suppose que le client d'AnyConnect peut déconnecter et rebrancher, le tunnel n'est pas lâché, qui lui donne une occasion de revenir. Cependant, pendant les essais en laboratoire avec un permis de base (2 tunnels SSL par défaut), vous pourriez épuiser votre permis quand des tunnels SSL ne sont pas fermés correctement. Si cette question se produit, utilisez le **<option > la** commande de **déconnexion de VPN-sessiondb** afin de fermer une session toutes les sessions actives SSL.

Configuration d'one-minute

Afin de créer rapidement une configuration en cours, remettez à l'état initial votre ASA au par défaut d'usine, et collez cette configuration dans le mode de configuration :

ciscoasa

```
ciscoasa#conf t
ciscoasa#clear configure all
ciscoasa#domain-name cisco.be
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
interface Ethernet0/1
 no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
 domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr c eq be
 issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
```

```
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
    6f020301 0001a381 bb3081b8 300e0603 551d0f01
01ff0404 03020106 300f0603
    551d1301 01ff0405 30030101 ff304206 03551d20
043b3039 30370605 60380101
    01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
    72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
    9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
    02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
    148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
    966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
    32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
    4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
    337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
    1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
    83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
    eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
    7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
  quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol svc webvpn
 address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
```

```
 authentication-server-group (outside) LOCAL
 authorization-server-group LOCAL
 authorization-required
 authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
exit
copy run start
```

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems