

Exemple de configuration d'un accès sans client ASA avec l'utilisation de Citrix Receiver sur des appareils mobiles

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Périphériques mobiles pris en charge](#)

[Démonstration](#)

[Informations générales](#)

[Limites](#)

[Configuration](#)

[Commandes CLI](#)

[Exemple de configuration](#)

[Configuration d'Adaptive Security Device Manager \(ASDM\)](#)

[Certificats d'identité ASA et autorités de certification \(CA\)](#)

[Interface utilisateur/expérience utilisateur](#)

[Ajouter un nouveau compte](#)

[Déconnexion de la session WebVPN](#)

[Vérification](#)

[Dépannage](#)

[Débogages](#)

[Foire aux questions \(FAQ\)](#)

Introduction

Ce document décrit comment configurer l'appareil de sécurité adaptatif (ASA) de Cisco comme proxy pour Citrix Receiver sur les appareils mobiles. Cette fonctionnalité fournit un accès à distance sécurisé pour l'application Citrix Receiver qui s'exécute sur des appareils mobiles vers des serveurs XenApp/XenDesktop Virtual Desktop Infrastructure (VDI) via ASA, ce qui élimine le besoin de la passerelle d'accès Citrix.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Receveur Citrix
- WebVPN sans client

Exigences d'infrastructure :

- L'ASA doit disposer d'un certificat d'identité valide approuvé par les appareils mobiles.
- L'interface XML doit être activée et configurée sur le serveur Citrix XenApp/XenDesktop/Storefront.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Périphériques mobiles pris en charge

Voici une liste des périphériques mobiles pris en charge :

- iPad - Citrix Receiver Version 4.x ou ultérieure
- iPhone/iTouch - Citrix Receiver Version 4.x ou ultérieure
- Téléphone Android 2.x - Citrix Receiver Version 2.x ou ultérieure
- Tablette Android 3.x - Citrix Receiver Version 2.x ou ultérieure
- Téléphone/Tablette Android 4.0/4.1 - Récepteur Citrix version 2.x ou ultérieure

Démonstration

Pour voir une démonstration de ce processus, visitez la page Web suivante :

[Démonstration du proxy du récepteur mobile Cisco ASA 9.0 Citrix](#)

Informations générales

La passerelle d'accès Citrix (CAG) était traditionnellement le seul moyen de fournir un accès à distance sécurisé aux ressources Citrix virtualisées (postes de travail et applications). Dans un déploiement classique, un tel périphérique se trouve derrière le pare-feu dans une zone démilitarisée (DMZ). Cette fonctionnalité ajoute une fonctionnalité ASA afin de prendre en charge les connexions distantes sécurisées aux ressources virtuelles à partir des périphériques mobiles.

Les déploiements traditionnels nécessitent la présence d'un CAG, généralement situé derrière le pare-feu :



Avec ASA, les connexions aux ressources Citrix internes sont possibles sans CAG :



Pour que l'ASA puisse établir des connexions proxy entre un récepteur Citrix et un serveur Citrix, l'ASA emprunte l'identité Citrix Access.

Passerelle :

1. Lorsque vous essayez de vous connecter à une ressource virtualisée Citrix, vous n'avez pas besoin de fournir l'adresse/les informations d'identification du serveur Citrix ; à la place, saisissez l'adresse IP et les informations d'identification VPN SSL (Secure Sockets Layer) de l'ASA.
2. Un nouveau gestionnaire ASA est créé afin de traiter les demandes, qui inclut les demandes d'authentification des récepteurs Citrix (demandes HTTPS avec une chaîne d'agent qui s'identifie comme le récepteur Citrix).
3. Une fois que l'ASA a vérifié les informations d'identification, le client du récepteur commence à récupérer les applications autorisées via l'ASA. L'ASA réécrit et proxie l'interface de service XML de XenApp ou XenDesktop Server (le service XML est un service qui s'exécute sur un serveur Citrix et qui répond aux demandes de ressources de virtualisation).

4. L'ASA se connecte et s'authentifie au serveur VDI avec des informations d'identification préconfigurées (voir la section Configurer). Lorsque vous envoyez des informations d'identification au serveur XenApp/XenDesktop principal, l'ASA brouille toujours le mot de passe de l'utilisateur avec le codage Citrix CTX1.

Voici une liste des méthodes d'authentification ASA prises en charge avec le récepteur Citrix :

- Municipal
- Domaine
- RSA SecurID utilisant le protocole natif SDI.
ASA prend également en charge les modes de confirmation, notamment le jeton suivant, le nouveau code PIN et le code PIN expiré.
- Authentification à deux facteurs (RSA et LDAP (Lightweight Directory Access Protocol))

Limites

- Limitations de certificat :
L'authentification par certificat/carte à puce n'est pas prise en charge en tant que méthode de connexion automatique, car ces formes d'authentification ne permettent pas l'ASA au milieu.

La signature Md5 des certificats ne fonctionne pas en raison d'un problème de sécurité et pose un problème sur les plates-formes iOS. Pour plus d'informations, consultez [l'erreur Receiver for iOS : Erreur de connexion. Citrix Receiver n'a pas pu établir de connexion avec la discussion d'hôte distant](#).

Si le nom du sujet ne correspond pas entièrement au nom de domaine complet (FQDN) ASA, même si le certificat d'identité ASA contient des noms de domaine alternatifs (SAN), la session ICA (Independent Computing Architecture) ne démarre pas (en fonction de la version, l'erreur de certificat peut être affichée). Ce problème a été corrigé par l'ID de bogue Cisco [CSCuj23632](#).

- Le client Citrix Receiver accède à un seul serveur XenApp/XenDesktop à la fois. Par conséquent, l'ASA envoie également des requêtes proxy à une session XenApp/XenDesktop par session VPN. L'ASA choisit le premier XenApp/XenDesktop configuré lorsqu'un client Citrix Receiver se connecte.
- La redirection HTTP n'est pas prise en charge, car la version actuelle de l'application Citrix Receiver ne fonctionne pas avec les redirections.
- Les vérifications des certificats clients, la notification d'expiration de mot de passe, Cisco Secure Desktop (CSD) et tout ce qui se trouve dans CSD (pas seulement Secure Vault) ne sont pas pris en charge lorsque des clients autonomes/mobiles sont utilisés, car les clients d'infrastructure de virtualisation autonome/mobile ne comprennent pas ces concepts.

Configuration

Note: Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\) pour obtenir plus d'informations sur les commandes utilisées dans cette section.](#)

Commandes CLI

Lorsque vous utilisez le client mobile Citrix Receiver pour vous connecter à l'ASA, l'ASA doit le connecter à un serveur Citrix XenApp prédéfini ou à un serveur XenDesktop. Pour ce faire, l'administrateur configure l'adresse et les informations d'identification de connexion du serveur Citrix sous la stratégie de groupe ou le nom d'utilisateur. Dans le cas où le nom d'utilisateur et l'interface de ligne de commande de stratégie de groupe sont configurés, les paramètres de nom d'utilisateur priment sur la stratégie de groupe.

```
configure terminal
group-policy DfltGrpPolicy attributes
webvpn
[no] vdi { none | type <vdi_type>url domain username
password <password>}
```

```
configure terminal
username <username> attributes
webvpn
[no] vdi { none | type <vdi_type>url domain username
password <password>}
```

Note:

type - type de VDI. Pour le récepteur Citrix, le type doit être **citrix**.

url : URL complète du serveur XenApp ou XenDesktop, qui inclut HTTP ou HTTPS, nom d'hôte, numéro de port, ainsi que le chemin d'accès au service XML. Le nom d'hôte et le chemin d'accès du service XML peuvent contenir une macro sans client. Si le chemin du service XML n'est pas fourni, le chemin par défaut de **/Citrix/pnagent/** est utilisé.

username - nom d'utilisateur utilisé pour se connecter au serveur d'infrastructure de virtualisation. Il peut s'agir d'une macro sans client.

password : mot de passe utilisé pour se connecter au serveur d'infrastructure de virtualisation. Il peut s'agir d'une macro sans client.

domaine - domaine utilisé pour se connecter au serveur d'infrastructure de virtualisation. Il peut s'agir d'une macro sans client.

Note: Les serveurs XenAPP sont généralement configurés pour écouter le port 80, de sorte que le VDI doit être configuré avec **HTTP** au lieu de **HTTPS**.

Les utilisateurs de Citrix Mobile Receiver peuvent sélectionner le groupe de tunnels pendant leur authentification avec l'ASA. La sélection de groupe de tunnels permet la prise en charge de différents protocoles d'authentification et de serveurs XenApp/XenDesktop pour l'accès VDI. Les administrateurs peuvent configurer un groupe de tunnels comme groupe par défaut pour l'accès VDI. Ce groupe de tunnels configuré est utilisé lorsque les utilisateurs ne sélectionnent pas de groupe de tunnels :

```
configure terminal
webvpn
[no] application-type default tunnel-group
```

- *nom_application* - nom de l'application. La seule application actuellement prise en charge est **citrix-récepteur**.
- *tunnel-group-name* - nom du groupe de tunnels actif à utiliser comme valeur par défaut pour l'accès VDI de type spécifié.

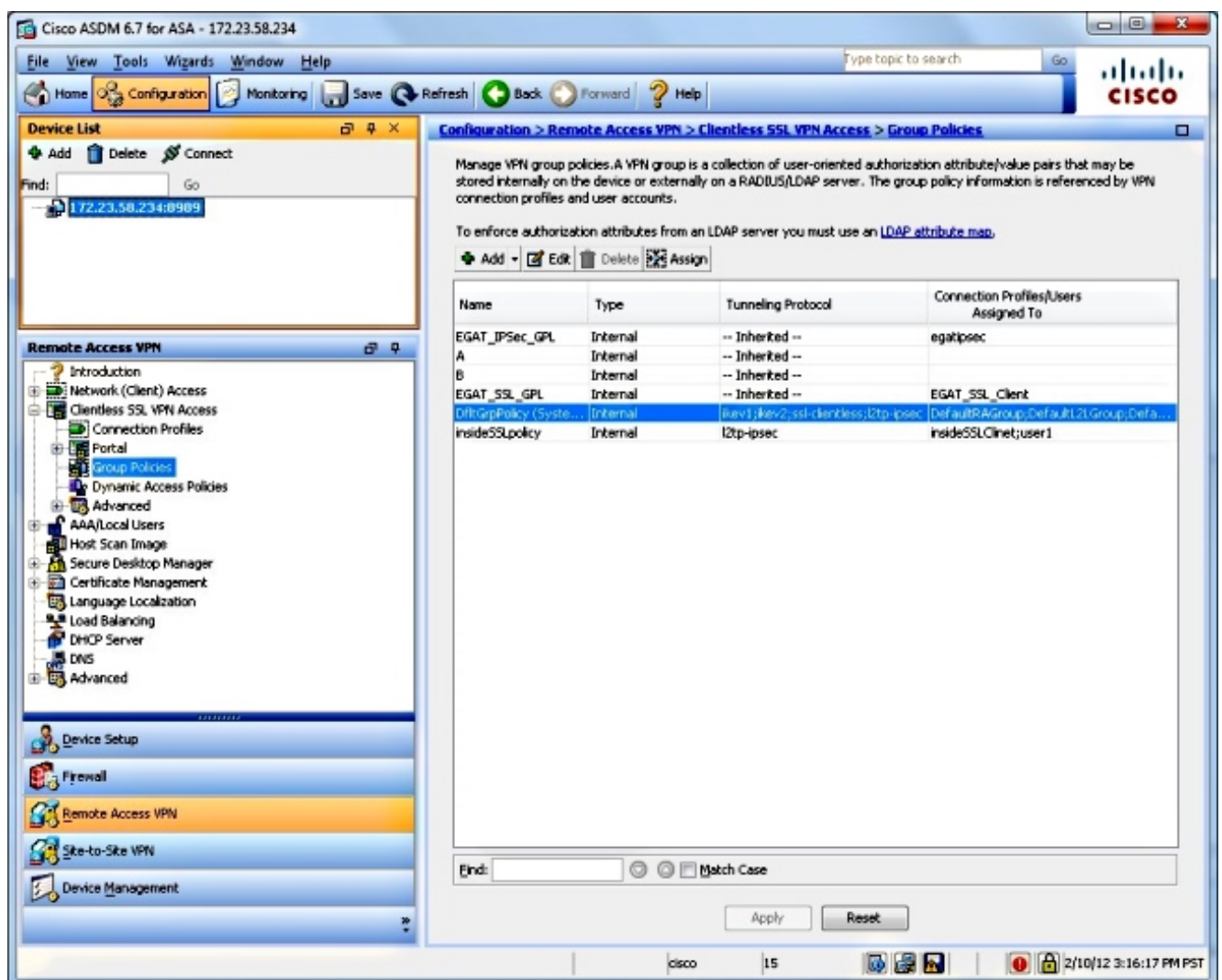
Exemple de configuration

Voici des exemples de configuration VDI valides :

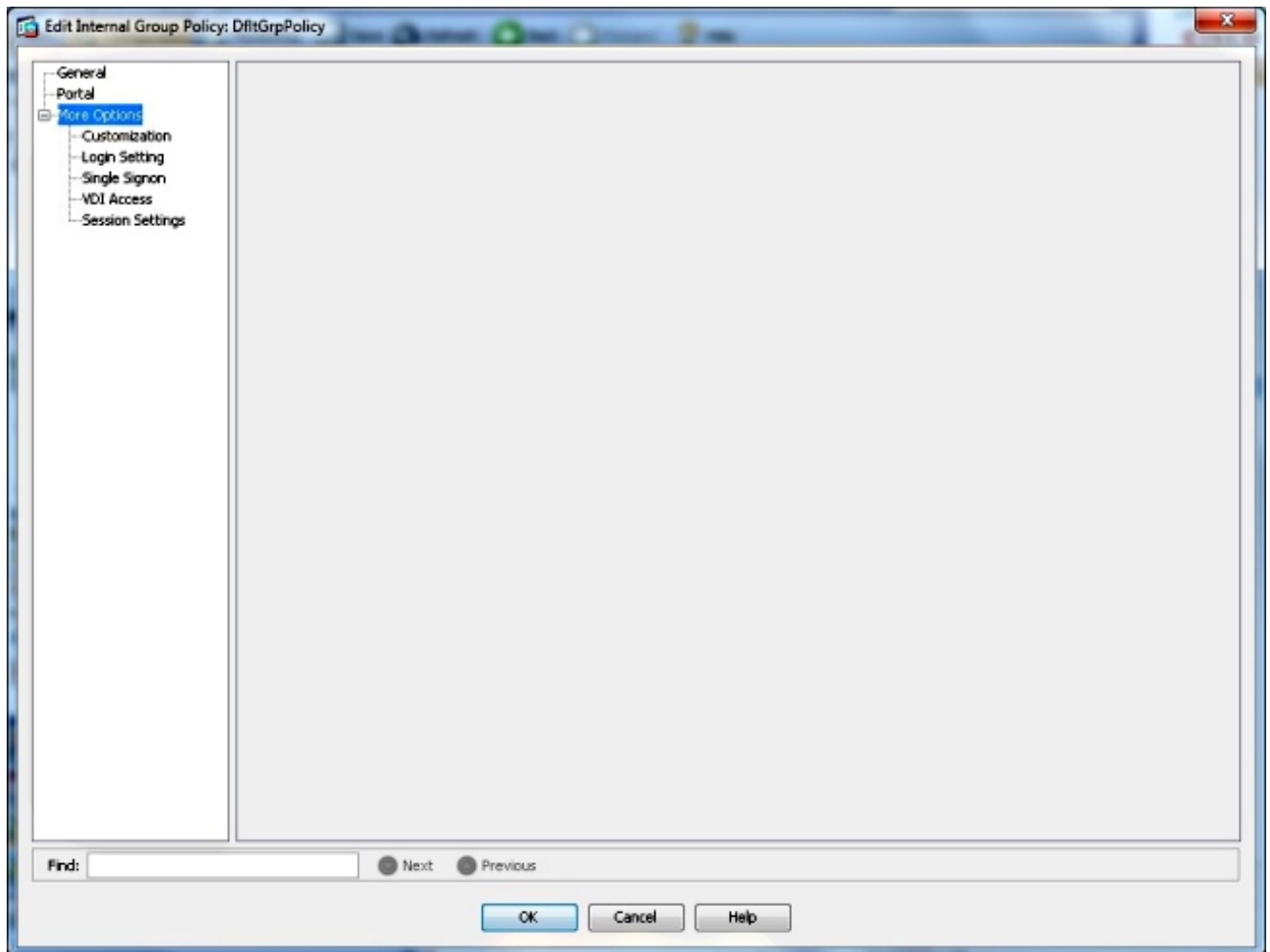
```
vdi type citrix url http://192.168.1.2 domain domain1 username user1 password pass1
vdi type citrix url https://192.168.1.2/Citrix/pnagent1/ domain domain2 username
username2 password password2
vdi type citrix url http://192.168.1.2:8080/Citrix/pnagent3 domain CSCO_WEBVPN_MACRO1
username CSCO_WEBVPN_USERNAME password CSCO_WEBVPN_PASSWORD
```

Configuration d'Adaptive Security Device Manager (ASDM)

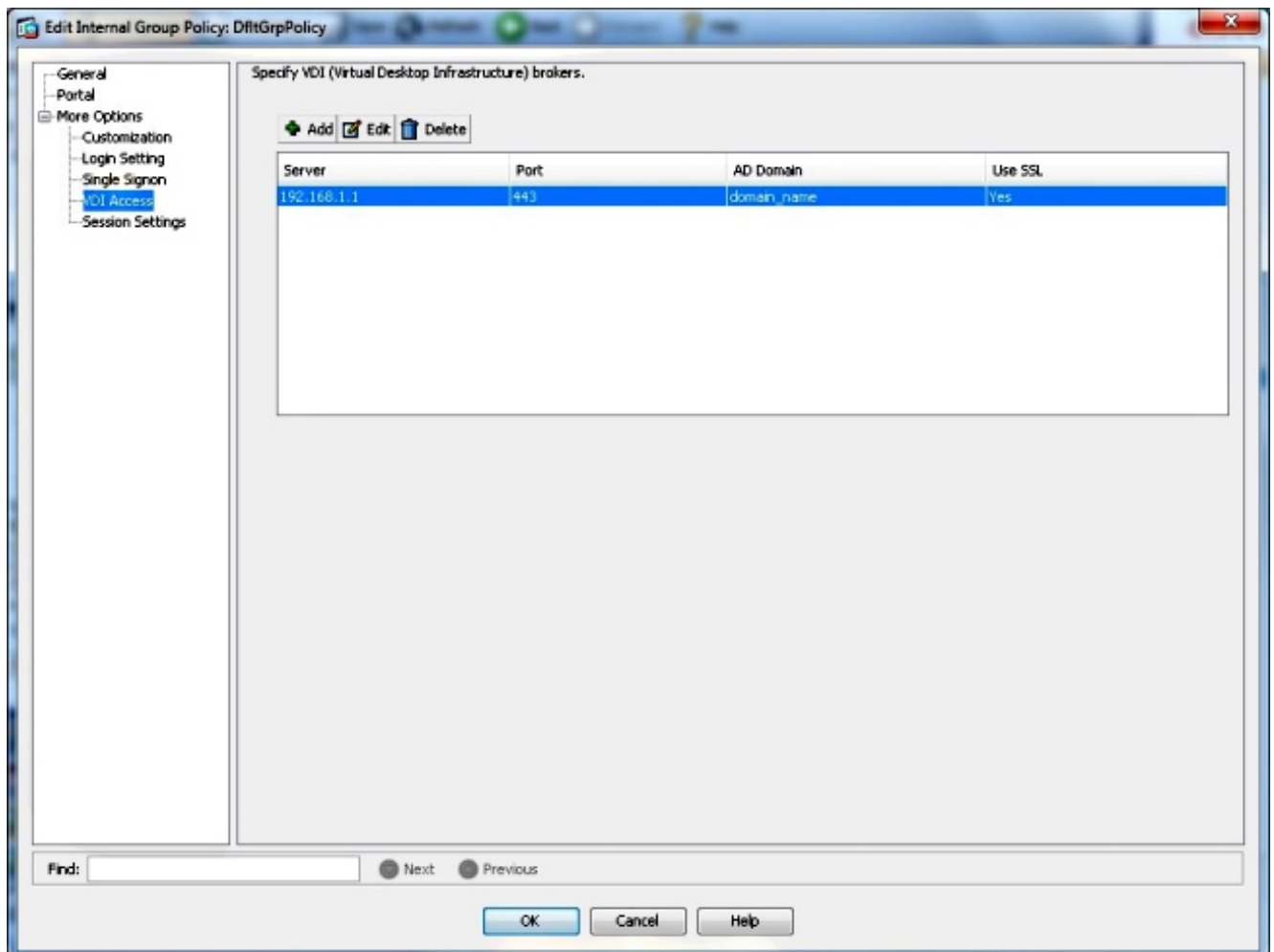
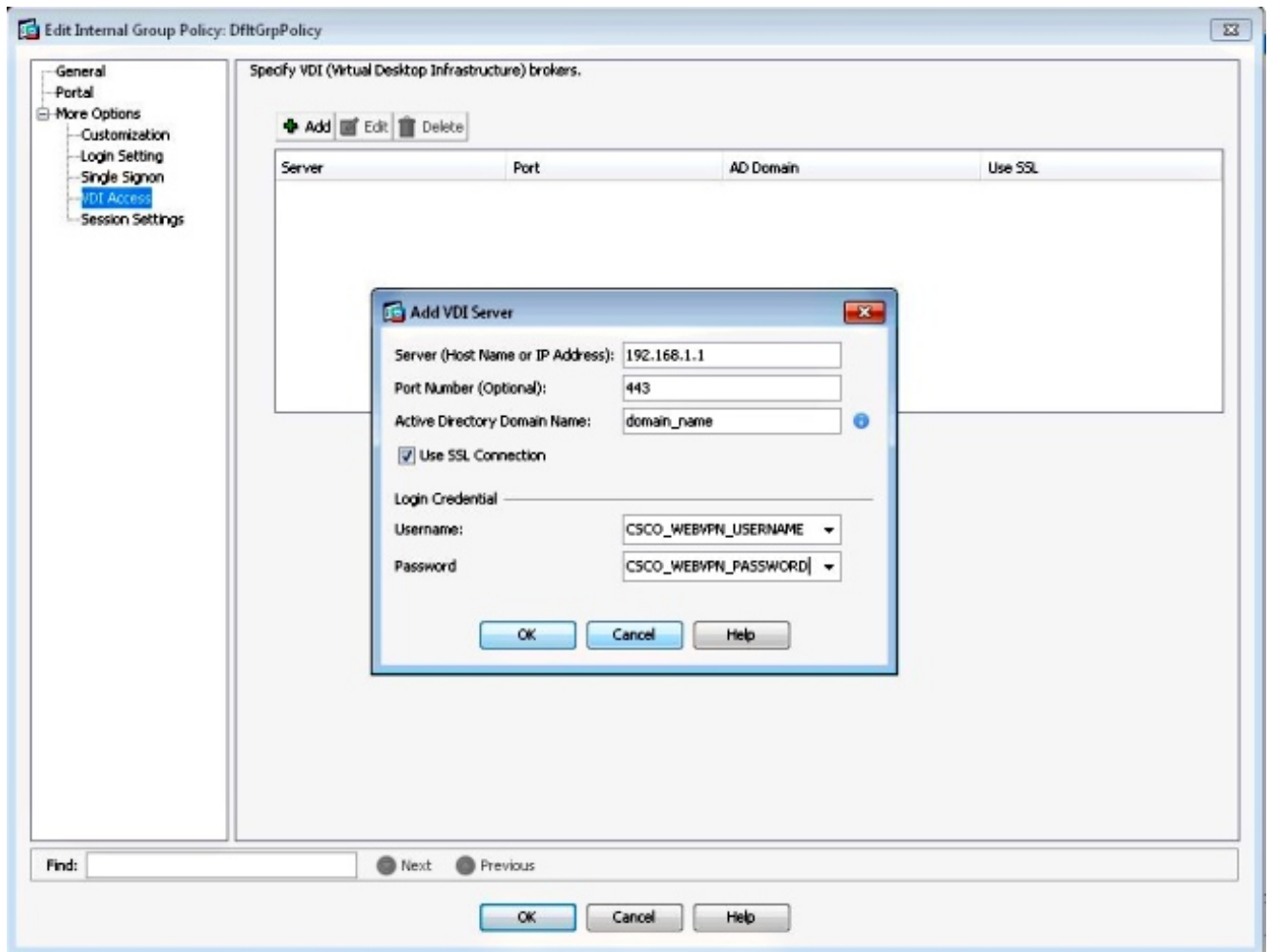
1. Accédez à **Asdm > Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policy** :



2. Accédez à **Edition > Autres options > Accès VDI** :



3. Ajouter le **serveur VDI** :



Note: Le seul mode pris en charge est le mode unique.

Certificats d'identité ASA et autorités de certification (CA)

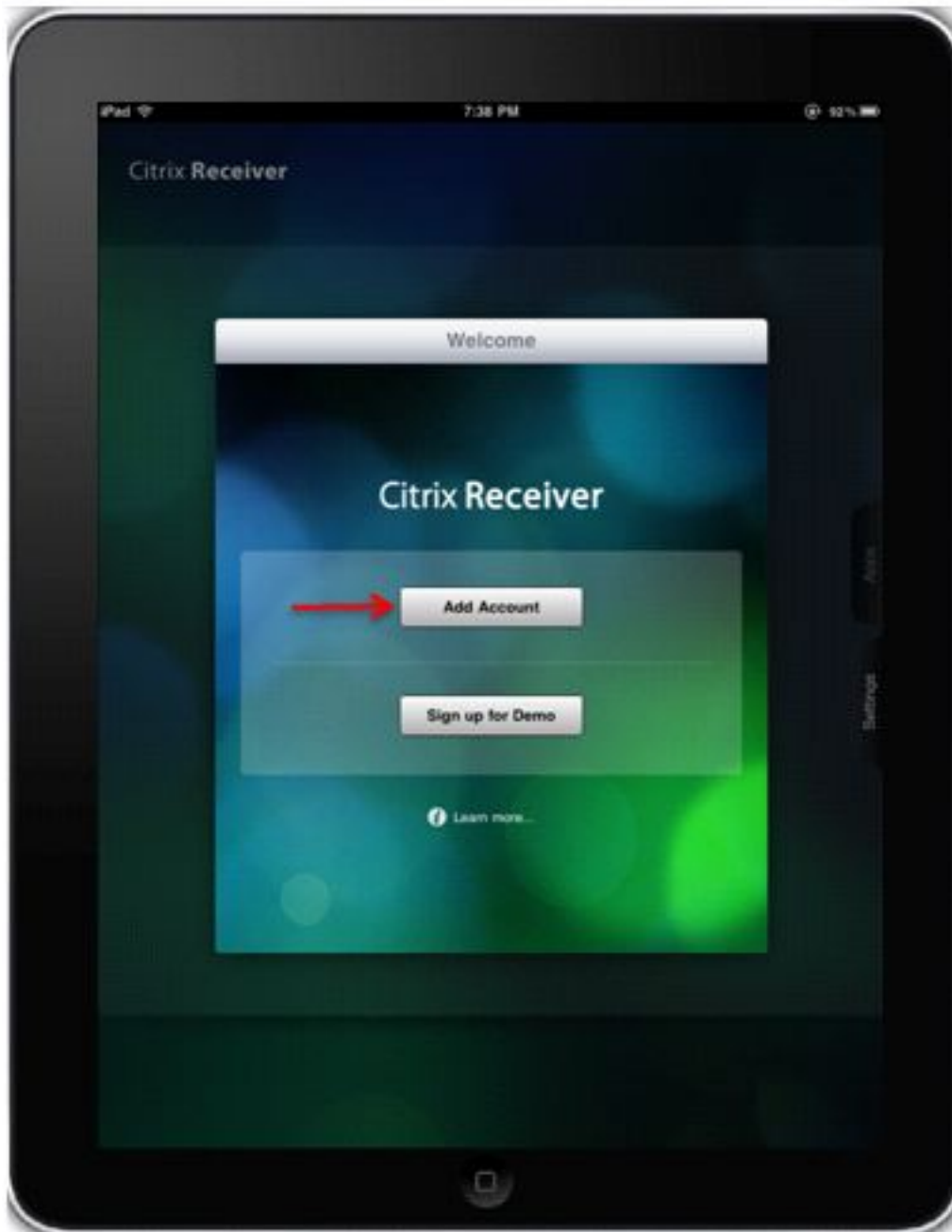
- Pour que Citrix Receiver fonctionne avec l'ASA, **les périphériques mobiles doivent faire confiance à l'autorité de certification qui a délivré le certificat d'identité de l'ASA. Le certificat ASA doit être émis pour un nom de domaine complet** (par exemple, clientlessvdi.cisco.com) et NON pour l'adresse IP de l'ASA. Si le certificat ASA a été émis par une autorité de certification intermédiaire qui n'est pas présente dans le magasin de clés de l'appareil mobile, l'autorité de certification intermédiaire doit également être approuvée.
- Lorsque Citrix Receiver se connecte à l'ASA avec un certificat non approuvé, l'utilisateur est invité à indiquer s'il doit continuer ou non.
- Les périphériques Apple exécutant iOS peuvent prendre en charge les certificats ASA auto-signés, car ils prennent en charge l'importation directe de certificats et d'autorités de certification.
- Sur les appareils mobiles Apple qui exécutent iOS, le récepteur autorise la connexion à l'ASA et la récupération de la liste des applications, si les avertissements de certificat sont ignorés. Cependant, il se peut que l'utilisateur ne puisse démarrer aucune des ressources publiées tant qu'un certificat ASA valide n'est pas installé.
- Certains des anciens appareils mobiles du système d'exploitation Android ne fournissent aucun moyen légitime d'importer des certificats tiers dans le magasin de clés. Par conséquent, pour qu'un récepteur Citrix sur ces périphériques Android fonctionne avec l'ASA/CAG, l'ASA doit avoir un certificat d'identité émis par l'AC qui a été incorporé dans le magasin de clés, par exemple Verisign ou Godaddy.
- Sur les appareils mobiles Android, Citrix Receiver n'autorise pas les connexions à l'ASA si le certificat ASA n'est pas présent dans le magasin de clés de l'appareil.
- Les périphériques Android avec OS version 4.1 et ultérieures prennent en charge l'importation des certificats et des CA et doivent fonctionner comme décrit ci-dessus avec iOS.

Interface utilisateur/expérience utilisateur

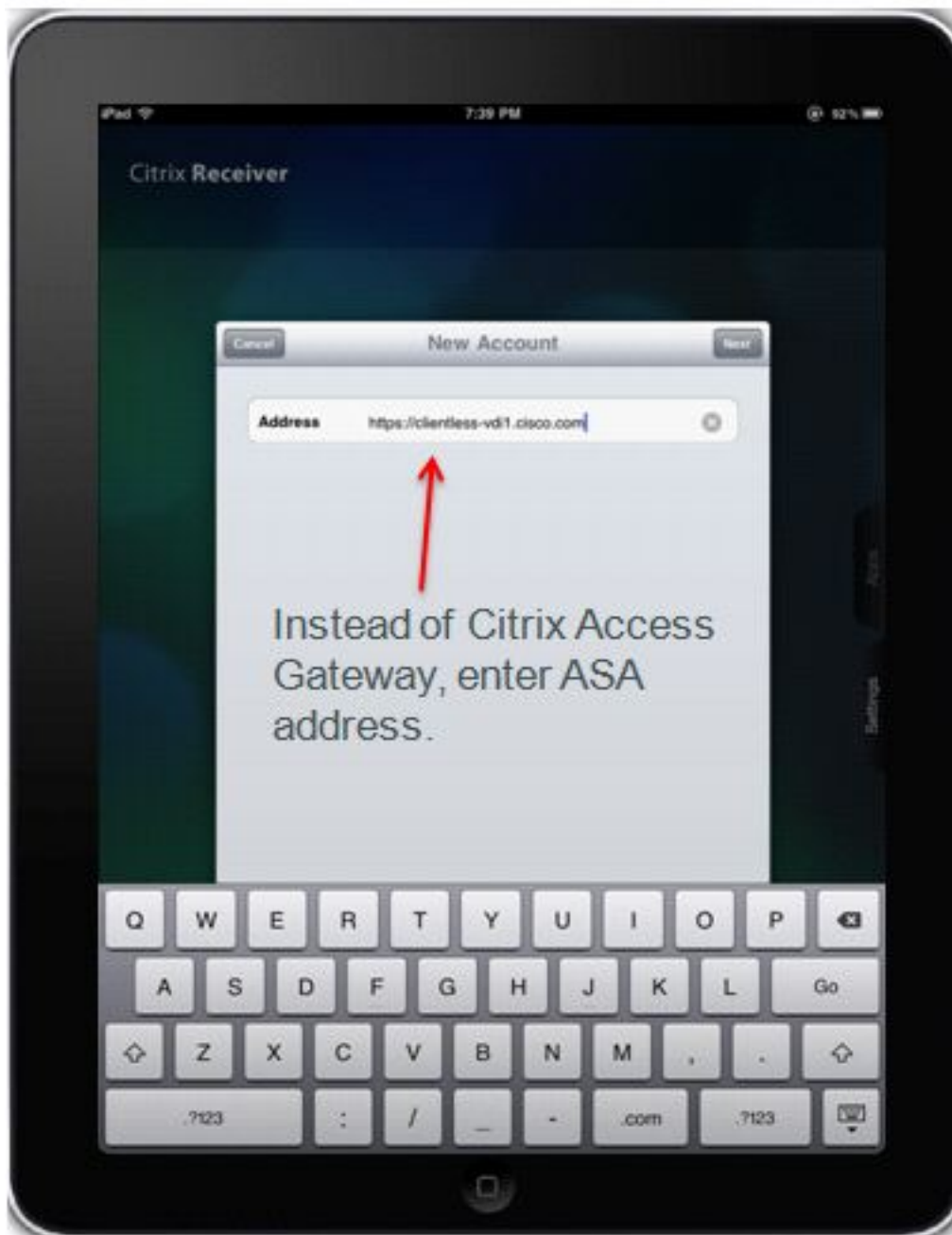
Ajouter un nouveau compte

L'utilisation de Citrix Receiver pour accéder aux ressources virtuelles via l'ASA offre la même expérience utilisateur que lorsqu'une passerelle d'accès Citrix est utilisée.

Si aucun serveur n'est configuré, vous devez configurer une nouvelle ressource virtuelle.



Indiquez l'adresse FQDN/IP de l'ASA :



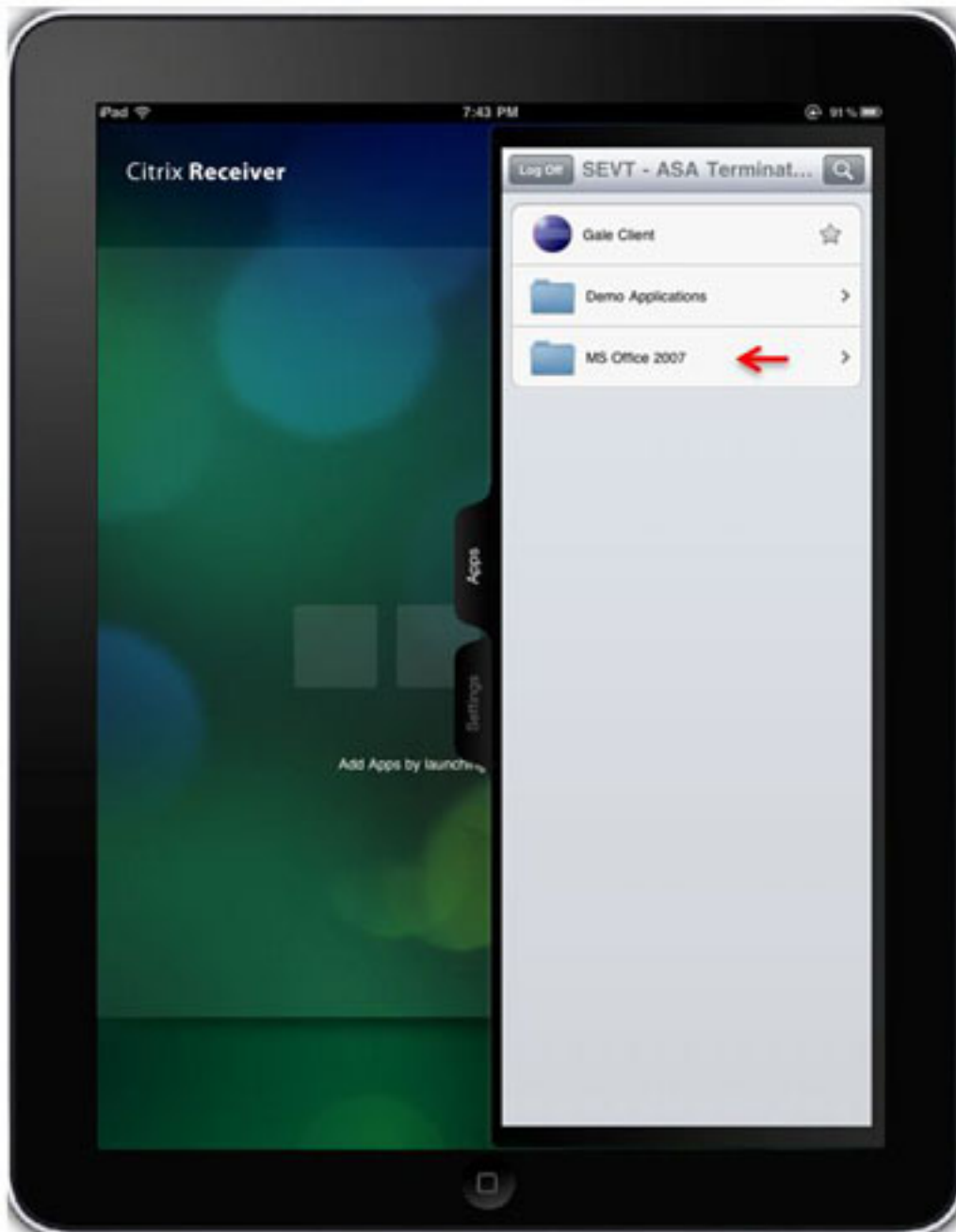
Vérifiez la **passerelle d'accès, Standard Edition**, et entrez les informations d'identification afin de vous connecter à l'ASA.



Lorsque le profil utilisateur est enregistré, l'application demande automatiquement des informations d'identification (ASA) et tente de se connecter.

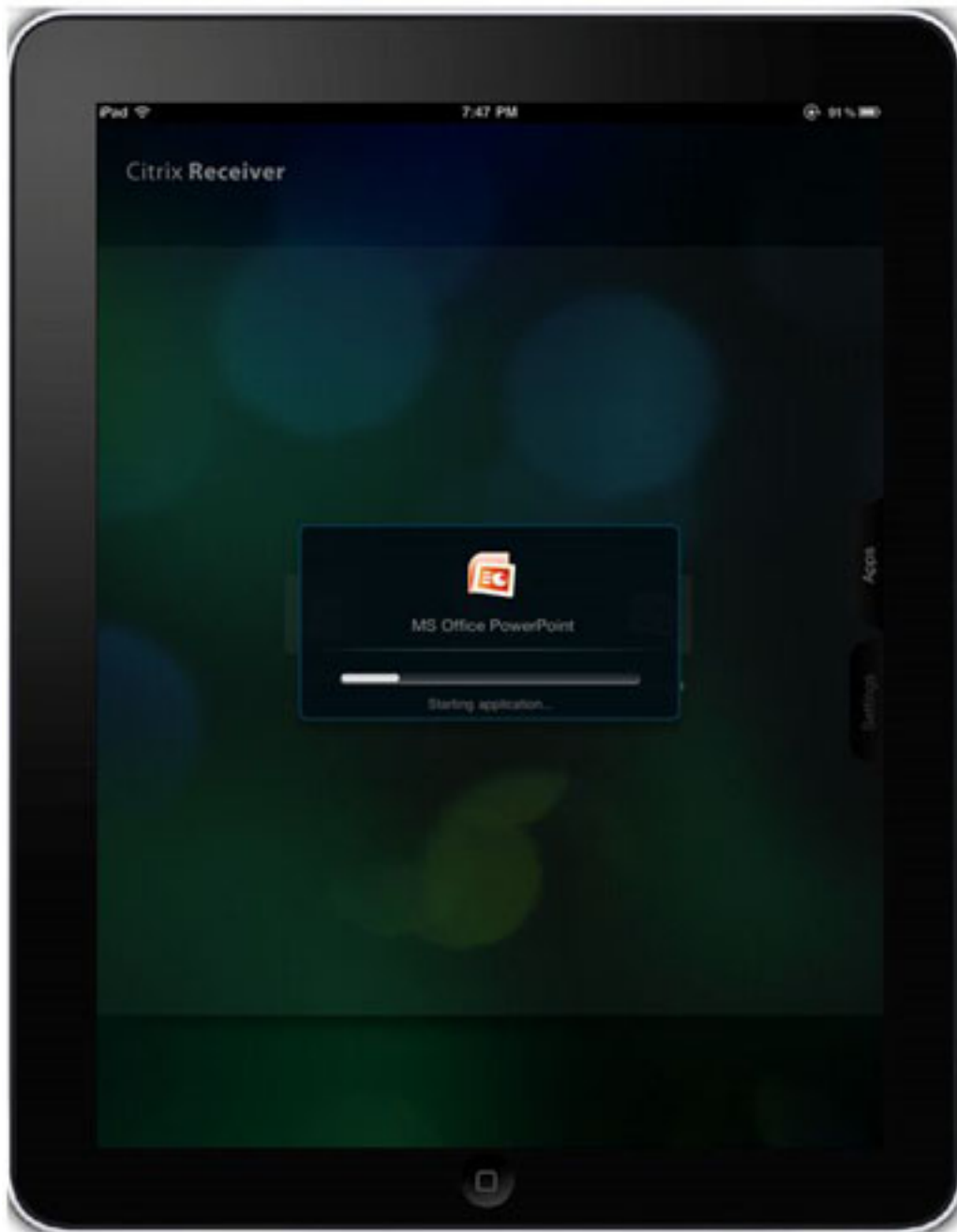


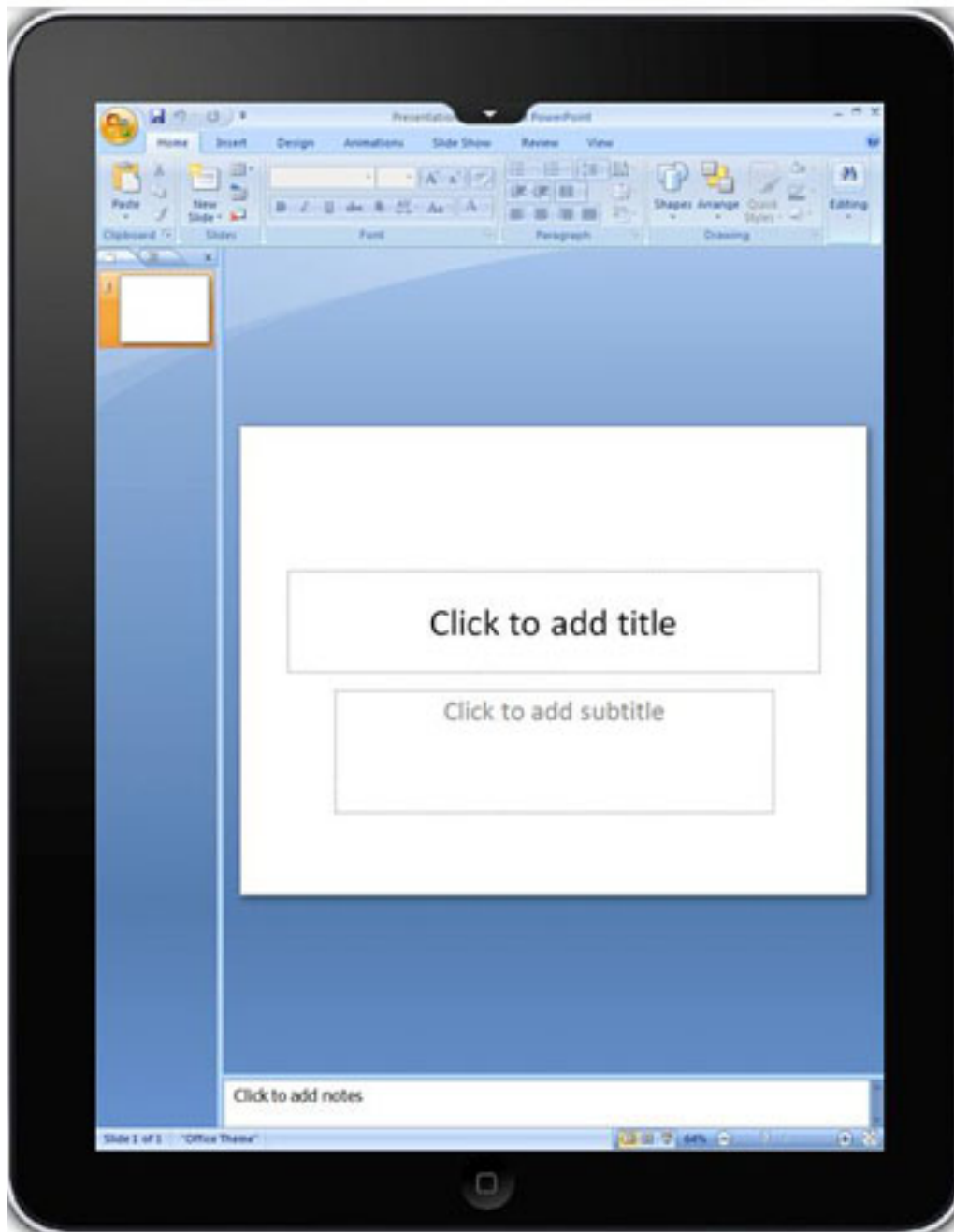
Une fois connecté, l'application affiche la liste des ressources publiées.



Vous pouvez naviguer dans les dossiers et cliquer sur une ressource afin de la lancer.



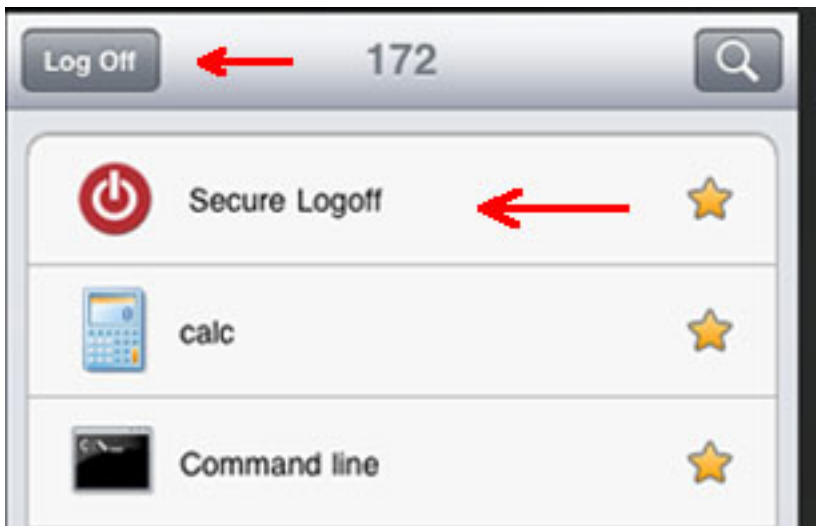




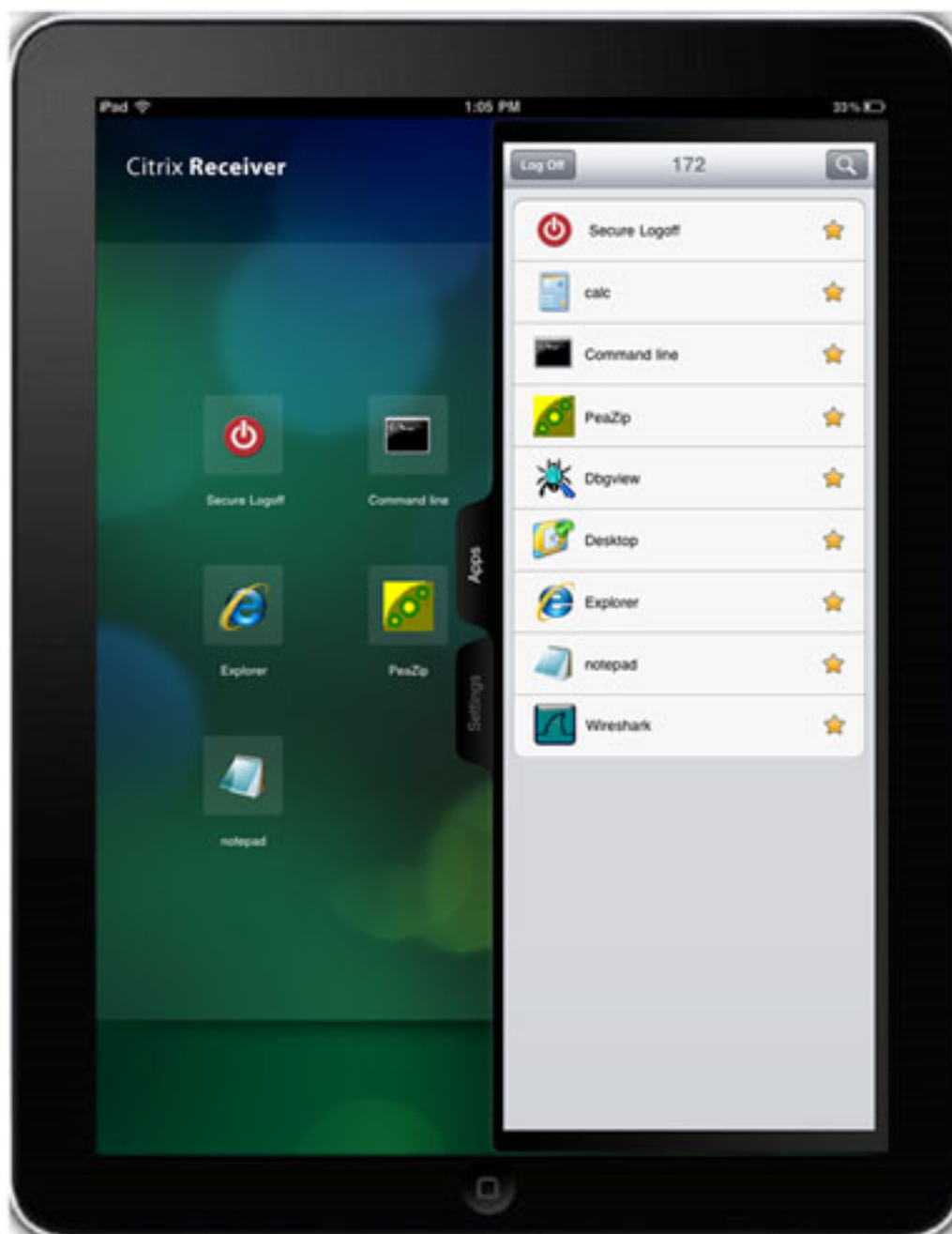
Déconnexion de la session WebVPN

L'application Citrix Receiver ne permet pas de terminer une session WebVPN avec un ASA ou un CAG connecté à volonté. Généralement, une telle session est interrompue lorsque vous atteignez le délai d'attente configuré. Bien que la dernière version de Citrix Receiver dispose d'un nouveau bouton **Déconnexion**, il ne met pas fin à la session en cours avec l'ASA. Il ferme toutes les applications ouvertes et affiche la liste des serveurs configurés. Par conséquent, si l'ASA est configuré pour n'utiliser qu'une seule licence par utilisateur, les clients qui utilisent le bouton **Déconnexion** ne peuvent se reconnecter qu'après la fin de la session.

Afin de permettre aux utilisateurs finaux de mettre fin à la session WebVPN à volonté et, par conséquent, de libérer la licence ASA, de nouvelles fonctionnalités ont été ajoutées pour injecter la ressource **Secure Logoff**.



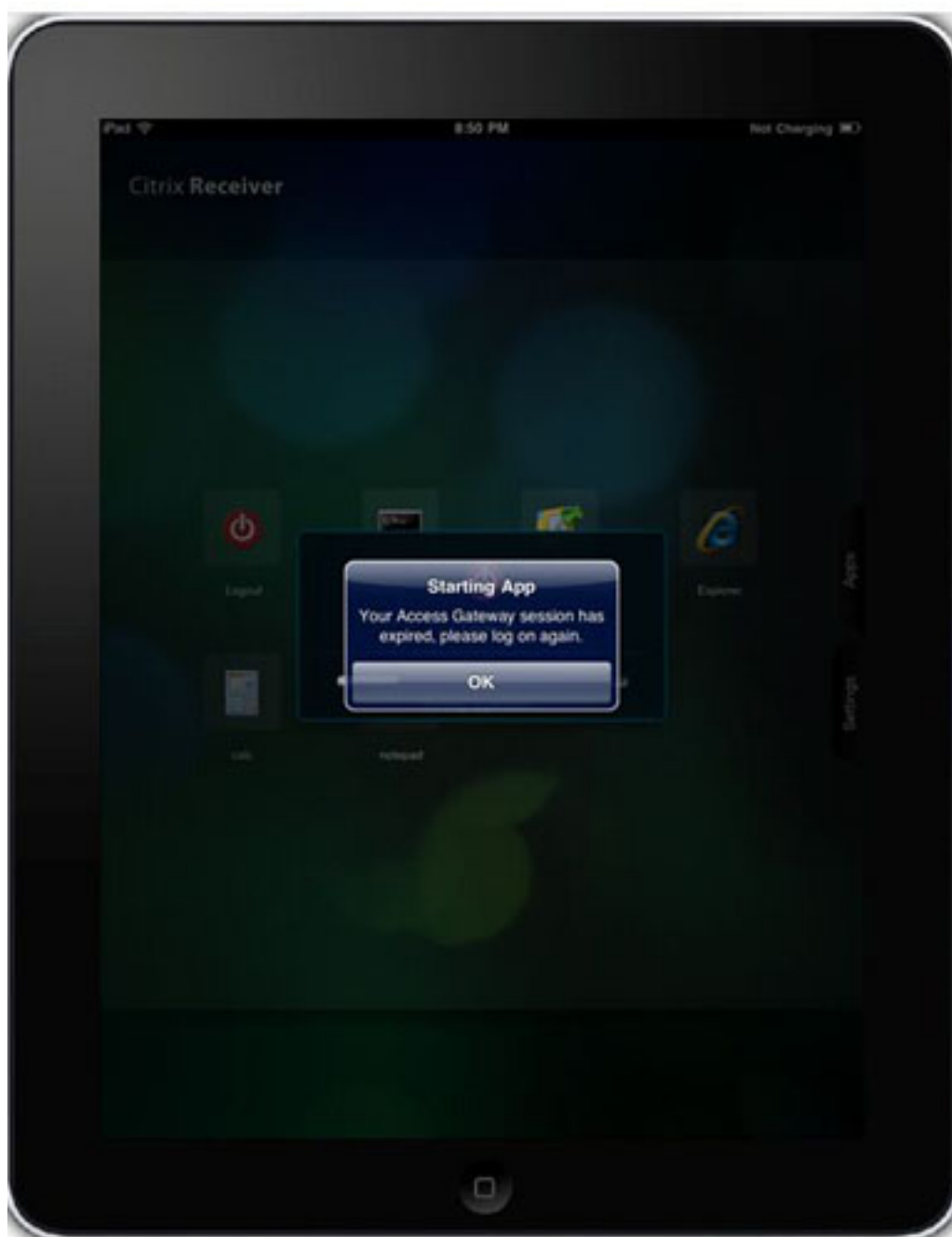
Cette injection se produit chaque fois que le récepteur Citrix récupère la liste des ressources publiées.



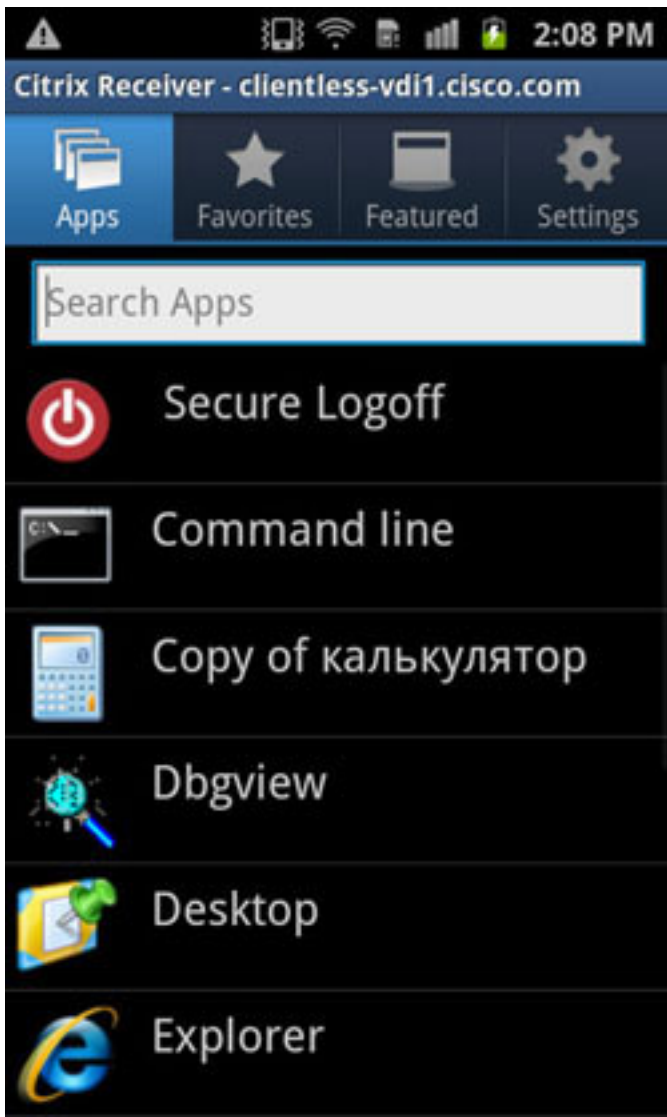
Lorsque vous cliquez sur l'application **Secure Logoff**, la session entre l'ASA et le récepteur Citrix est interrompue. Afin de libérer correctement la licence ASA, la ressource de **fermeture de session sécurisée** doit être utilisée afin de mettre fin à la session WebVPN au lieu du bouton natif Citrix Receiver Log Off.

Différents messages s'affichent à la suite de la fin de session en fonction des périphériques mobiles et de la version de Citrix Receiver. En outre, la différence dans la façon dont l'application Citrix est écrite pour différentes plates-formes mobiles donne une expérience différente lorsque vous déconnectez des appareils Android.

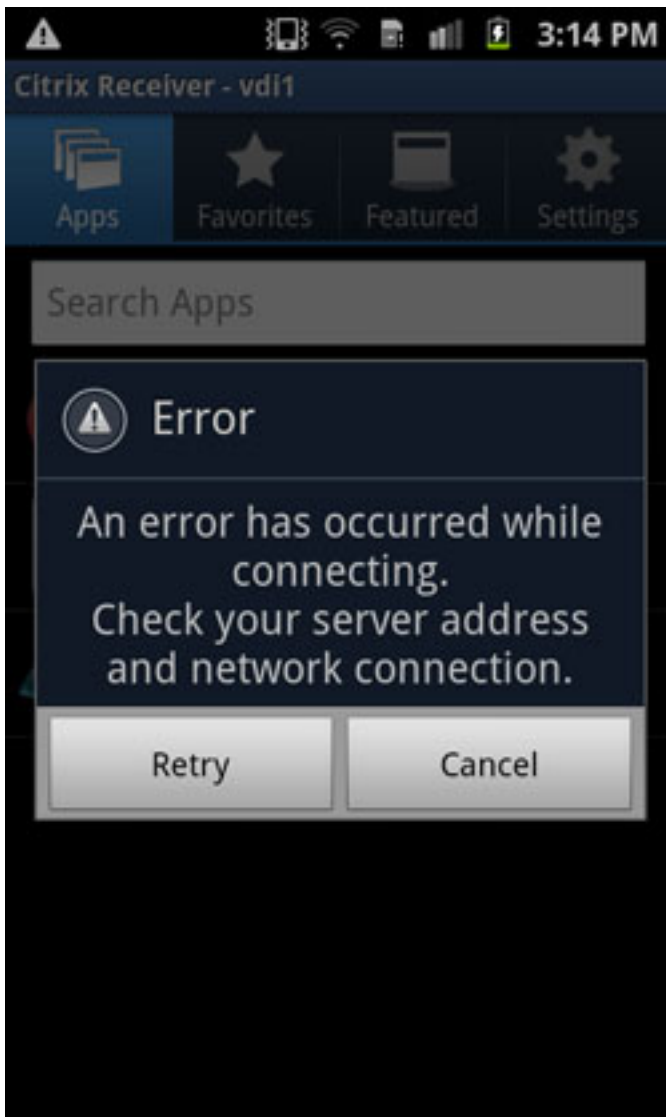
Sur l'iPad et l'iPhone, Citrix Receiver affiche le message **Votre accès à la session Gateway a expiré, veuillez vous reconnecter**. Lorsque vous cliquez sur **OK**, Citrix Receiver affiche l'écran avec les serveurs configurés.



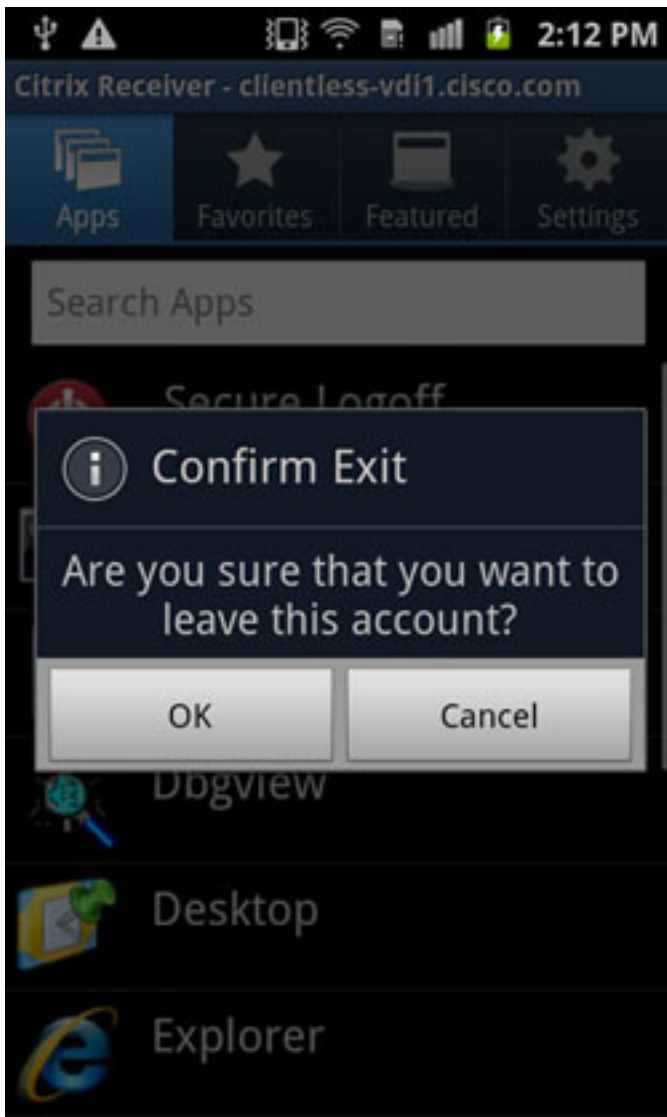
Les périphériques Android affichent également la ressource **Secure Logoff** injectée.



Cependant, lorsque vous cliquez sur l'application **de fermeture de session sécurisée**, une erreur de connexion réseau s'affiche.



Bien que la session WebVPN soit interrompue à ce moment-là, l'application Citrix Receiver ne dispose pas de messages intégrés pour vous informer correctement des actions futures. Ce comportement est attendu. Lorsque ce message d'**erreur** s'affiche à la suite d'une session terminée, il vous attend à cliquer sur le bouton **Annuler**, le bouton **Précédent** du périphérique Android afin de quitter le compte actuel, puis **OK** lorsque vous êtes invité à quitter ce compte.



Après avoir quitté le compte actuel, la liste des serveurs préconfigurés s'affiche.



Vérification

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Débogages

Note: Référez-vous aux [informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage](#).

Vous pouvez afficher les informations de débogage pour Citrix Receiver avec cette commande :

```
debug webvpn citrix <1-255>
```

Note:

Niveau 1 affiche des conditions anormales, des échecs de connexion au serveur XenApp/XenDesktop et des erreurs générales.

Niveau 50 affiche des informations sur les données en cours d'analyse/de réécriture.

Niveau 255 affiche toutes les informations de débogage ajoutées pour les connexions du récepteur Citrix.

Aucune nouvelle commande n'a été ajoutée pour l'authentification Citrix Receiver. Cependant, afin d'afficher les transactions entre le client et l'ASA, vous pouvez utiliser ce débogage :

debug webvpn transformation request

Pour référence. cette sortie montre ces deux débogages provenant d'une connexion qui fonctionne :

```
==== PuTTY log 2013.07.24 14:42:38 =====
Channel NP p=0x00000000 0/0 more bufferedchannel-np.c
TEST-ASA#
TEST-ASA# DBG:89:3178386013:7404365c:0000: netsal_accept returned 0x6d6ce7c0
(unicorn-proxy.c:proxy_thread_asa:1250)
DBG:90:3178386045:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy],
stack(16384) = 0x74136ed0..0x7413aecc (fc=3), sys 0x6d5abea8
(FIBERS/fibers.c:fiber_create:519)
DBG:91:3178386088:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20,
sys 0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:92:3178386111:74100d20:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:93:3178386125:74100d20:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:94:3178386136:74100d20:0009: in process request
(aware.c:aware_dispatch_request:301)
DBG:95:3178386148:74100d20:0009: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:96:3178433565:74100d20:0009: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:97:3178433620:74100d20:0009: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:98:3178433640:74100d20:0009: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)
DBG:99:3178433652:74100d20:0009: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)
DBG:00:3178433694:74100d20:0009: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)
DBG:01:3178433713:74100d20:0009: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)
DBG:02:3178433730:74100d20:0009: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)
DBG:03:3178433742:74100d20:0009: Hook: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)
DBG:04:3178433753:74100d20:0009: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)
DBG:05:3178433810:74100d20:0009: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)
DBG:06:3178433883:74100d20:0009: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)
DBG:07:3178433899:74100d20:0009: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
DBG:08:3178433916:74100d20:0009: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
```

DBG:09:3178433930:74100d20:0009: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:10:3178433942:74100d20:0009: => embedded
(aware.c:aware_dispatch_request:396)
DBG:11:3178433955:74100d20:0009: Serve embedded request [/
(aware.c:aware_serve_request:782)
DBG:12:3178433978:74100d20:0009: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:13:3178434028:74100d20:0009: No session redirect
(aware.c:aware_serve_request:888)
DBG:14:3178434104:74100d20:0009: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:15:3178434149:74100d20:0009: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:16:3178434188:74100d20:0009: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:17:3178434207:74100d20:0009: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:18:3178434226:74100d20:0010: in process request
(aware.c:aware_dispatch_request:301)
DBG:19:3178434239:74100d20:0010: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:20:3179015760:74100d20:0010: -- EOF in iobuf_channel input!!!
(iobuf_channel.c:ucte_input_buf_channel_input_fun:157)
DBG:21:3179015792:74100d20:0010: read_req_headers: first line: Unexpected
character 0x00 (aware_parse_headers.re2c:aware_parse_req_headers:241)
DBG:22:3179015809:74100d20:0010: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:23:3179015821:74100d20:0010: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:24:3179015838:74100d20:0010: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:25:3179015852:74100d20:0010: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:26:3179015865:74100d20:0010: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)
DBG:27:3179015934:74100d20:0010: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:28:3179015965:74100d20:0010: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.c
TEST-ASA#
TEST-ASA#
TEST-ASA#
TEST-ASA# DBG:29:3203022718:7404365c:0000: netsal_accept returned 0x6d6ce7c0
(unicorn-proxy.c:proxy_thread_asa:1250)
DBG:30:3203022750:7404365c:0000: Creating fiber 0x740ff6a0 [unicorn-proxy],
stack(16384) = 0x7413ef10..0x74142f0c (fc=3), sys 0x6d5abea8
(FIBERS/fibers.c:fiber_create:519)
DBG:31:3203022926:740ff6a0:0000: Jumpstarting unicorn-proxy 0x740ff6a0, sys
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:32:3203022959:740ff6a0:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:33:3203022973:740ff6a0:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:34:3203022986:740ff6a0:0011: in process request
(aware.c:aware_dispatch_request:301)
DBG:35:3203022996:740ff6a0:0011: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:36:3203070771:740ff6a0:0011: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:37:3203070845:740ff6a0:0011: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:38:3203070870:740ff6a0:0011: Hook: SharePoint_cb

(aware_webvpn_conf.re2c:SharePoint_cb:1021)
DBG:39:3203070883:740ff6a0:0011: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)
DBG:40:3203070894:740ff6a0:0011: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)
DBG:41:3203070907:740ff6a0:0011: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)
DBG:42:3203070919:740ff6a0:0011: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)
DBG:43:3203070931:740ff6a0:0011: Hook: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)
DBG:44:3203070940:740ff6a0:0011: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)
DBG:45:3203070996:740ff6a0:0011: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)
DBG:46:3203071070:740ff6a0:0011: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)
DBG:47:3203071090:740ff6a0:0011: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
DBG:48:3203071105:740ff6a0:0011: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
DBG:49:3203071122:740ff6a0:0011: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:50:3203071135:740ff6a0:0011: => embedded request
(aware.c:aware_dispatch_request:396)
DBG:51:3203071147:740ff6a0:0011: Serve embedded request [/
(aware.c:aware_serve_request:782)
DBG:52:3203071169:740ff6a0:0011: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:53:3203071218:740ff6a0:0011: No session redirect
(aware.c:aware_serve_request:888)
DBG:54:3203071293:740ff6a0:0011: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:55:3203071338:740ff6a0:0011: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:56:3203071376:740ff6a0:0011: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:57:3203071396:740ff6a0:0011: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:58:3203071414:740ff6a0:0012: in process request
(aware.c:aware_dispatch_request:301)
DBG:59:3203071427:740ff6a0:0012: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:60:3204883539:740ff6a0:0012: -- EOF in iobuf_channel input!!!
(iobuf_channel.c:ucte_input_buf_channel_input_fun:157)
DBG:61:3204883574:740ff6a0:0012: read_req_headers: first line: Unexpected
character 0x00 (aware_parse_headers.re2c:aware_parse_req_headers:241)
DBG:62:3204883591:740ff6a0:0012: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:63:3204883603:740ff6a0:0012: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:64:3204883619:740ff6a0:0012: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:65:3204883632:740ff6a0:0012: Fiber 0x740ff6a0 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:66:3204883645:740ff6a0:0012: Exiting fiber 0x740ff6a0
(FIBERS/fibers.c:fiber__kill:1257)
DBG:67:3204883718:740ff6a0:0012: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:68:3204883750:740ff6a0:0012: Fiber 0x740ff6a0 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.cDBG:69:3212412660:7404365c:0000:
netsal_accept returned 0x6d6ce7c0 (unicorn-proxy.c:proxy_thread_asa:1250)
DBG:70:3212412691:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy],

```
stack(16384) = 0x74136ed0..0x7413aecc (fc=3), sys 0x6d5abea8
(FIBERS/fibers.c:fiber_create:519)
DBG:71:3212413380:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20,
sys 0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:72:3212413415:74100d20:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:73:3212413429:74100d20:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:74:3212413447:74100d20:0013: in process request
(aware.c:aware_dispatch_request:301)
DBG:75:3212413460:74100d20:0013: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:76:3212462785:74100d20:0013: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:77:3212462837:74100d20:0013: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:78:3212462857:74100d20:0013: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)
DBG:79:3212462873:74100d20:0013: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)
DBG:80:3212462884:74100d20:0013: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)
DBG:81:3212462895:74100d20:0013: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)
DBG:82:3212462906:74100d20:0013: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)
DBG:83:3212462918:74100d20:0013: Hook: SCEPPProxy_cb
(aware_webvpn_conf.re2c:SCEPPProxy_cb:2154)
DBG:84:3212462928:74100d20:0013: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)
DBG:85:3212462983:74100d20:0013: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)
DBG:86:3212463058:74100d20:0013: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)
DBG:87:3212463075:74100d20:0013: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
DBG:88:3212463091:74100d20:0013: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
DBG:89:3212463104:74100d20:0013: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:90:3212463118:74100d20:0013: => embedded request
(aware.c:aware_dispatch_request:396)
DBG:91:3212463128:74100d20:0013: Serve embedded request [/]
(aware.c:aware_serve_request:782)
DBG:92:3212463150:74100d20:0013: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:93:3212463202:74100d20:0013: No session redirect
(aware.c:aware_serve_request:888)
DBG:94:3212463305:74100d20:0013: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:95:3212463351:74100d20:0013: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:96:3212463388:74100d20:0013: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:97:3212463407:74100d20:0013: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:98:3212463424:74100d20:0014: in process request
(aware.c:aware_dispatch_request:301)
DBG:99:3212463435:74100d20:0014: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:00:3212610662:74100d20:0014: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:01:3212610716:74100d20:0014: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
```

DBG:02:3212610737:74100d20:0014: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)

DBG:03:3212610750:74100d20:0014: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)

DBG:04:3212610762:74100d20:0014: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)

DBG:05:3212610774:74100d20:0014: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)

DBG:06:3212610787:74100d20:0014: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)

DBG:07:3212610799:74100d20:0014: Hook: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)

DBG:08:3212610810:74100d20:0014: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)

DBG:09:3212610870:74100d20:0014: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)

DBG:10:3212610945:74100d20:0014: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)

DBG:11:3212610964:74100d20:0014: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)

DBG:12:3212610980:74100d20:0014: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)

DBG:13:3212610997:74100d20:0014: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)

DBG:14:3212611011:74100d20:0014: => embedded request
(aware.c:aware_dispatch_request:396)

DBG:15:3212611021:74100d20:0014: Serve embedded request [/
(aware.c:aware_serve_request:782)

DBG:16:3212611042:74100d20:0014: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)

DBG:17:3212611090:74100d20:0014: No session redirect
(aware.c:aware_serve_request:888)

DBG:18:3212611162:74100d20:0014: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)

DBG:19:3212611231:74100d20:0014: HEADERS SENT
(aware.c:aware_send_resp_headers:162)

DBG:20:3212611270:74100d20:0014: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)

DBG:21:3212611289:74100d20:0014: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)

DBG:22:3212611306:74100d20:0015: in process request
(aware.c:aware_dispatch_request:301)

DBG:23:3212611318:74100d20:0015: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)

DBG:24:3212711373:74100d20:0015: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)

DBG:25:3212711428:74100d20:0015: Cookie name:[webvpnlogin]: 11
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:26:3212711458:74100d20:0015: METHOD = 2, POST
(aware_parse_headers.re2c:aware_parse_req_headers:619)

DBG:27:3212711479:74100d20:0015: => handoff (AWARE_HOOK_EXTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:495)

DBG:28:3212711498:74100d20:0015: Channel NP p=0x6d6ce7c0 0/0 more buffered
(SAL/channel-np.c:_sal_np_close:908)

DBG:29:3212711568:74100d20:0015: Finish external handoff for client_ch
0x6d6ce7c0 (aware.c:aware_dispatch_request:497)

DBG:30:3212711589:74100d20:0015: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)

DBG:31:3212711601:74100d20:0015: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)

DBG:32:3212711617:74100d20:0015: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)

DBG:33:3212711630:74100d20:0015: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)

DBG:34:3212711644:74100d20:0015: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)
DBG:35:3212711658:74100d20:0015: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Creating fiber 0x73c63290 [fiber-ldap-class], stack(16384) =
0x73c9eae0..0x73ca2adc (fc=2), sys 0x6d5c1cacfibers.cDBG:36:3212712546:
73c63290:0000: Jumpstarting fiber-ldap-class 0x73c63290, sys 0x73c60ca0
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:37:3212712646:73c63290:0000: Connecting to 00000000:1024239808
(SAL/netsal.c:netsal_connect:319)
DBG:38:3212712677:73c63290:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/192.168.12.61/389/M/VM) (SAL/netsal.c:netsal_connect:443)
DBG:39:3212712923:73c63290:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)
DBG:40:3212723367:73c63290:0000: Exiting fiber 0x73c63290
(FIBERS/fibers.c:fiber__kill:1257)
DBG:41:3212723706:73c63290:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:42:3212723747:73c63290:0000: Fiber 0x73c63290 terminated, 2 more
(FIBERS/fibers.c:fiber__kill:1330)
DBG:36:3212726030:0:0000: Creating fiber 0x740ff6a0 [ak47_attach_class], stack
(256) = 0x741cb870..0x741cb96c (fc=3), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)
DBG:37:3212726072:740ff6a0:0000: Remote storage is not configured
(pstorage.c:pStorage_restore:272)
Terminating fiber 0x740ff6a0fibers.cFiber 0x740ff6a0 terminated, 3 morefibers.
cDBG:38:3212726646:0:0000: Creating fiber 0x74100d20 [ak47_attach_class], stack
(256) = 0x741cb750..0x741cb84c (fc=3), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)
DBG:39:3212726721:74100d20:0000: Creating fiber 0x740ff9a0 [unicorn-proxy], stack
(16384) = 0x74136ed0..0x7413aecc (fc=4), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)
Terminating fiber 0x74100d20fibers.cFiber 0x74100d20 terminated, 4 morefibers.
cDBG:40:3212727006:740ff9a0:0000: Jumpstarting unicorn-proxy 0x740ff9a0, sys
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:41:3212727039:740ff9a0:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:42:3212727052:740ff9a0:0000: new fiber for client_ch 0x6d6cf000
(aware.c:run_aware_fiber:1318)
DBG:43:3212727065:740ff9a0:0016: in process request
(aware.c:aware_dispatch_request:301)
DBG:44:3212727080:740ff9a0:0016: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.cDBG:45:3212821243:740ff9a0:
0016: Hook: UrlSniff_cb (aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:46:3212821289:740ff9a0:0016: Cookie name:[net6_cookie]: 11
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:47:3212821312:740ff9a0:0016: Cookie name:[net6_user_session]: 17
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:48:3212821327:740ff9a0:0016: Cookie name:[webvpn]: 6
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:49:3212821341:740ff9a0:0016: Cookie name:[webvpnaac]: 9
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:50:3212821354:740ff9a0:0016: Cookie name:[webvpnc]: 7
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:51:3212821368:740ff9a0:0016: Cookie name:[webvpnx]: 7
(aware_parse_headers.re2c:aware_parse_cookie:754)
DBG:52:3212821389:740ff9a0:0016: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:53:3212821407:740ff9a0:0016: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:508)
DBG:54:3212821420:740ff9a0:0016: in process request
(proxy.c:process_request:239)
DBG:55:3212821509:740ff9a0:0016: parse_req_headers(client_fd, p_req) ;


```
(proxy.c:process_request:275)
DBG:56:3212821531:740ff9a0:0016: Request: [GET /Citrix/pnagent/config.xml
HTTP/1.1]: 39 (parse_req_headers.re2c:parse_req_headers:1399)
DBG:57:3212821556:740ff9a0:0016: req headers array at 741f3480
(parse_req_headers.re2c:parse_req_headers:1500)
DBG:58:3212821577:740ff9a0:0016: in parse_cookie
(ucte_parse_cookie.re2c:parse_cookie:430)
DBG:59:3212821590:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:60:3212821603:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:61:3212821613:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:62:3212821625:740ff9a0:0016: Cookie name: net6_user_session
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:63:3212821638:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:64:3212821653:740ff9a0:0016: req cookie array at 741f3680
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:144)
DBG:65:3212821665:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:66:3212821675:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:67:3212821685:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:68:3212821695:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:69:3212821705:740ff9a0:0016: Cookie name: webvpnaac
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:70:3212821718:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:71:3212821730:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:72:3212821740:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:73:3212821750:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:74:3212821759:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:75:3212821768:740ff9a0:0016: Cookie name: webvpnx
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:76:3212821778:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:77:3212821788:740ff9a0:0016: in parse Cookie -->
(ucte_parse_cookie.re2c:parse_cookie:777)
DBG:78:3212821844:740ff9a0:0016: User [test.user]
(proxy.c:process_request:418)
DBG:79:3212821870:740ff9a0:0016: Keepalive threshold forced to 4
(ucte_policy.c:ucte_get_ctx_session_settings:798)
DBG:80:3212821888:740ff9a0:0016: => reverse proxy request
(proxy.c:process_request:615)
ERR:81:3212821920:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:82:3212821944:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:83:3212821962:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:84:3212821989:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:85:3212822008:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
```

```
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:86:3212822021:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:87:3212822038:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:88:3212822052:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:89:3212822065:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:90:3212822081:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:91:3212822095:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:92:3212822108:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:93:3212822149:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:94:3212822165:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
DBG:95:3212822203:740ff9a0:0016: + About to dump request body to the file
(proxy.c:process_request:889)
DBG:96:3212822222:740ff9a0:0016: used_at_least_once [0], server_ch [0],
netsal_connection_is_closing [1] (proxy.c:process_request:1204)
DBG:97:3212822236:740ff9a0:0016: no old connection, create a new one
(proxy.c:process_request:1206)
DBG:98:3212822283:740ff9a0:0016: Decoded URL: /Citrix/pnagent/config.xml
(conn.c:establish_connection:626)
DBG:99:3212822326:740ff9a0:0016: Connecting to 00000000:84150794
(SAL/netsal.c:netsal_connect:319)
DBG:00:3212822355:740ff9a0:0016: otherPifNum 3, nexthop4 5080b0a
(SAL/netsal.c:netsal_connect:371)
DBG:01:3212822381:740ff9a0:0016: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/10.10.4.5/80/T/PROXY/2/70.199.131.148/3007)
(SAL/netsal.c:netsal_connect:443)
DBG:02:3212822643:740ff9a0:0016: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)
DBG:03:3212824193:740ff9a0:0016: Back-end connection is READY [6d6ce680]
(proxy.c:process_request:1216)
DBG:04:3212824222:740ff9a0:0016: + sending headers to the server
(proxy.c:process_request:1240)
DBG:05:3212824242:740ff9a0:0016: CONNECT TO http://10.10.4.5/Citrix/pnagent/config.xml
(send_req_headers.c:ucte_send_request_headers:160)
DBG:06:3212824309:740ff9a0:0016: About to open cookie directory:
sessions/2375680/cookie (COOKIE/ucte_cookie.c:send_req_cookie_storage:670)
DBG:07:3212824328:740ff9a0:0016: Could not open cookie directory
(COOKIE/ucte_cookie.c:send_req_cookie_storage:674)
DBG:08:3212824507:740ff9a0:0016: Connection acquired; headers sent
(proxy.c:process_request:1335)
DBG:09:3212824536:740ff9a0:0016: + Request headers and data sent...
(proxy.c:process_request:1438)
DBG:10:3212824550:740ff9a0:0016: + getting headers from the back end server...
(proxy.c:process_request:1449)
DBG:11:3212828428:740ff9a0:0016: resp header array at 741f3500
(parse_resp_headers.re2c:parse_resp_headers:226)
```

DBG:12:3212828485:740ff9a0:0016: => Response headers received (proxy.c:
process_request:1522)
DBG:13:3212828509:740ff9a0:0016: => About to send response headers to
the client (proxy.c:process_request:1693)
DBG:14:3212828527:740ff9a0:0016: ucte_hint = 4, content_type = 4,
resp_code = 200, session_defined = 2 (CACHE/send_resp_headers.c:
ucte_send_response_headers:407)
DBG:15:3212828612:740ff9a0:0016: + Sending response body (6982 bytes) to the client
(proxy.c:process_request:1793)
DBG:16:3212828635:740ff9a0:0016: + sending response body
(proxy.c:process_request:1865)
DBG:17:3212828645:740ff9a0:0016: Response: content-type=4
(proxy.c:process_request:1867)
DBG:18:3212829517:740ff9a0:0016: Session update!!!!!!
(ucte_ctx.c:ucte_session_update:645)
DBG:19:3212829566:740ff9a0:0016: + response body was sent
(proxy.c:process_request:1875)
DBG:20:3212829602:740ff9a0:0016: Backend connection reserved
(proxy.c:process_request:2145)
DBG:21:3212829618:740ff9a0:0016: free req_header, 74058210
(mem_man.c:mem_req_header_free:210)
DBG:22:3212829635:740ff9a0:0016: in req_header_light_destructor: free headers at
741f3480 (http_header.c:req_header_light_destructor:277)
DBG:23:3212829650:740ff9a0:0016: in req_header_light_destructor: free cookie at
741f3680 (http_header.c:req_header_light_destructor:282)
DBG:24:3212829664:740ff9a0:0016: free resp_header: 7406ab20
(mem_man.c:mem_resp_header_free:223)
DBG:25:3212829674:740ff9a0:0016: in resp_header_light_destructor: free headers at
741f3500 (http_header.c:resp_header_light_destructor:307)
DBG:26:3212829687:740ff9a0:0016: free ctx (mem_man.c:mem_ucte_ctx_free:197)
DBG:27:3212829708:740ff9a0:0016: Request finished gracefully
(proxy.c:process_request:2157)
DBG:28:3212829725:740ff9a0:0016: Finish internal handoff for client_ch 0x6d6cf000,
rc=1 (aware.c:aware_dispatch_request:510)
DBG:29:3212829738:740ff9a0:0016: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:30:3212829750:740ff9a0:0016: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:31:3212829766:740ff9a0:0017: in process request
(aware.c:aware_dispatch_request:301)
DBG:32:3212829778:740ff9a0:0017: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:33:3212941045:740ff9a0:0017: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:34:3212941078:740ff9a0:0017: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:508)
DBG:35:3212941117:740ff9a0:0017: in process request (proxy.c:process_request:239)
DBG:36:3212941205:740ff9a0:0017: parse_req_headers(client_fd, p_req) ;
(proxy.c:process_request:275)
DBG:37:3212941240:740ff9a0:0017: Request: [POST /+CSCO+00756767633A2F2F313
02E31302E342E35++/Citrix/pnagent/launch.aspx HTTP/1.1]: 84
(parse_req_headers.re2c:parse_req_headers:1399)
DBG:38:3212941273:740ff9a0:0017: req headers array at 741f33c0
(parse_req_headers.re2c:parse_req_headers:1500)
DBG:39:3212941295:740ff9a0:0017: in parse_cookie
(ucte_parse_cookie.re2c:parse_cookie:430)
DBG:40:3212941308:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:41:3212941332:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:42:3212941342:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:43:3212941353:740ff9a0:0017: Cookie name: net6_user_session
(ucte_parse_cookie.re2c:parse_cookie:605)

DBG:44:3212941366:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:45:3212941383:740ff9a0:0017: req cookie array at 741f3400
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:144)
DBG:46:3212941395:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:47:3212941405:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:48:3212941415:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:49:3212941423:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:50:3212941433:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:51:3212941447:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:52:3212941459:740ff9a0:0017: Cookie name: webvpnaac
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:53:3212941475:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:54:3212941489:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:55:3212941500:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:56:3212941510:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:57:3212941520:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:58:3212941529:740ff9a0:0017: Cookie name: webvpng
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:59:3212941540:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:60:3212941551:740ff9a0:0017: in parse Cookie -->
(ucte_parse_cookie.re2c:parse_cookie:777)
DBG:61:3212941608:740ff9a0:0017: User [test.user]
(proxy.c:process_request:418)
DBG:62:3212941634:740ff9a0:0017: Keepalive threshold forced to 4
(ucte_policy.c:ucte_get_ctx_session_settings:798)
DBG:63:3212941651:740ff9a0:0017: => reverse proxy request
(proxy.c:process_request:615)
DBG:64:3212941677:740ff9a0:0017: + About to dump request body to the file
(proxy.c:process_request:889)
DBG:65:3212941792:740ff9a0:0017: potentially reusing existing backend channel,
old host=10.10.4.5, old port=80 (proxy.c:process_request:1098)
DBG:66:3212941814:740ff9a0:0017: new host=10.10.4.5, new port=80
(proxy.c:process_request:1101)
DBG:67:3212941826:740ff9a0:0017: match, reuse it (0x6d6ce680)
(proxy.c:process_request:1108)
DBG:68:3212941860:740ff9a0:0017: Decoded URL: /Citrix/pnagent/launch.aspx
(proxy.c:process_request:1145)
DBG:69:3212941900:740ff9a0:0017: Back-end connection is READY [6d6ce680]
(proxy.c:process_request:1216)
DBG:70:3212941916:740ff9a0:0017: + sending headers to the server
(proxy.c:process_request:1240)
DBG:71:3212941934:740ff9a0:0017: CONNECT TO
http://10.10.4.5/Citrix/pnagent/launch.aspx (send_req_headers.c:
ucte_send_request_headers:160)
DBG:72:3212941950:740ff9a0:0017: Session update!!!!!!
(ucte_ctx.c:ucte_session_update:645)
DBG:73:3212942027:740ff9a0:0017: About to open cookie directory:
sessions/2375680/cookie (COOKIE/ucte_cookie.c:send_req_cookie_storage:670)
DBG:74:3212942047:740ff9a0:0017: Could not open cookie directory
(COOKIE/ucte_cookie.c:send_req_cookie_storage:674)
DBG:75:3212942220:740ff9a0:0017: Connection acquired; headers sent

(proxy.c:process_request:1335)
DBG:76:3212942307:740ff9a0:0017: + Request headers and data sent...
(proxy.c:process_request:1438)
DBG:77:3212942331:740ff9a0:0017: + getting headers from the back end server...
(proxy.c:process_request:1449)
DBG:78:3213277758:740ff9a0:0017: resp header array at 741f3500
(parse_resp_headers.re2c:parse_resp_headers:226)
DBG:79:3213277835:740ff9a0:0017: => Response headers received
(proxy.c:process_request:1522)
DBG:80:3213277857:740ff9a0:0017: => About to send response headers to the client (proxy.c:process_request:1693)
DBG:81:3213277877:740ff9a0:0017: ucte_hint = 0, content_type = 12, resp_code = 200, session_defined = 2 (CACHE/send_resp_headers.c:ucte_send_response_headers:407)
DBG:82:3213277968:740ff9a0:0017: + Sending response body (1162 bytes) to the client (proxy.c:process_request:1793)
DBG:83:3213277991:740ff9a0:0017: + sending response body (proxy.c:process_request:1865)
DBG:84:3213278030:740ff9a0:0017: Response: content-type=12 (proxy.c:process_request:1867)
DBG:85:3213278100:740ff9a0:0017: Generated SOCKS ticket: [V75E33CBB8657FB03V32333735363830V30V]: 36 (CISOCKS/../../unicorn/aware_apps/api/cisocks.c:cisocks_ticket_create:446)
DBG:86:3213278499:740ff9a0:0017: + response body was sent (proxy.c:process_request:1875)
DBG:87:3213278541:740ff9a0:0017: No front end keepalive (proxy.c:process_request:2153)
DBG:88:3213278621:740ff9a0:0017: SALNP_CLOSENOTIFY: p=0x0 0/0 more buffered (SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:89:3213278651:740ff9a0:0017: free req_header, 74058210 (mem_man.c:mem_req_header_free:210)
DBG:90:3213278669:740ff9a0:0017: in req_header_light_destructor: free headers at 741f33c0 (http_header.c:req_header_light_destructor:277)
DBG:91:3213278684:740ff9a0:0017: in req_header_light_destructor: free cookie at 741f3400 (http_header.c:req_header_light_destructor:282)
DBG:92:3213278697:740ff9a0:0017: free resp_header: 7406ab20 (mem_man.c:mem_resp_header_free:223)
DBG:93:3213278708:740ff9a0:0017: in resp_header_light_destructor: free headers at 741f3500 (http_header.c:resp_header_light_destructor:307)
DBG:94:3213278724:740ff9a0:0017: free ctx (mem_man.c:mem_ucte_ctx_free:197)
DBG:95:3213278756:740ff9a0:0017: Request finished gracefully (proxy.c:process_request:2157)
DBG:96:3213278772:740ff9a0:0017: Finish internal handoff for client_ch 0x6d6cf000, rc=-1 (aware.c:aware_dispatch_request:510)
DBG:97:3213278785:740ff9a0:0017: + freeing ctx (CONN/aware.c:aware_connection_clean_up:251)
DBG:98:3213278796:740ff9a0:0017: free aware ctx (aware_mem.c:mem_aware_ctx_free:64)
DBG:99:3213278809:740ff9a0:0017: Fiber exit - client_ch 0x6d6cf000 (aware.c:run_aware_fiber:1339)
DBG:00:3213278822:740ff9a0:0017: Fiber 0x740ff9a0 finished leaving 4 more (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:01:3213278835:740ff9a0:0017: Exiting fiber 0x740ff9a0 (FIBERS/fibers.c:fiber__kill:1257)
DBG:02:3213278870:740ff9a0:0017: SALNP_CLOSENOTIFY: p=0x0 0/0 more buffered (SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:03:3213278894:740ff9a0:0017: Fiber 0x740ff9a0 terminated, 3 more (FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.cChannel NP p=0x00000000 0/0 more bufferedchannel-np.cDBG:04:3213773777:7404365c:0000: netsal_accept returned 0x6d6ce7c0 (unicorn-proxy.c:proxy_thread_asa:1250)
DBG:05:3213773808:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy], stack(16384) = 0x7413ef10..0x74142f0c (fc=3), sys 0x6d5abea8 (FIBERS/fibers.c:fiber_create:519)
DBG:06:3213773875:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20, sys

```
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:07:3213773902:74100d20:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:08:3213773919:74100d20:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:09:3213773932:74100d20:0018: in process request
(aware.c:aware_dispatch_request:301)
DBG:10:3213773943:74100d20:0018: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:11:3213812394:74100d20:0018: => handoff (AWARE_HOOK_EXTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:495)
DBG:12:3213812426:74100d20:0018: Connection accepted
(CISOCKS/../../unicorn/aware_apps/api/cisocks.c:cisocks_handle:143)
DBG:13:3213860698:74100d20:0018: Connecting to 00000000:-1257461568
(SAL/netsal.c:netsal_connect:319)
DBG:14:3213860731:74100d20:0018: otherPifNum 3, nexthop4 5080b0a
(SAL/netsal.c:netsal_connect:371)
DBG:15:3213860761:74100d20:0018: about to call netsal__safe_encapsulate
for (sal-np/tcp/CONNECT/3/192.168.12.181/1494/T)
(SAL/netsal.c:netsal_connect:443)
DBG:16:3213861036:74100d20:0018: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)
DBG:17:3213861857:74100d20:0018: RELAY notify(0x6d6ce7c0, 2, 0,
socket=0x6218aa8/0x6218aa8) (SAL/channel-np.c:sal_np_relay_cb:1574)
DBG:18:3213861893:74100d20:0018: sal_np_relay_notify: signaling condvar
(SAL/channel-np.c:sal_np_relay_cb:1604)
DBG:19:3213861908:74100d20:0018: Acquired relay_mutex on in 0x6d6e79e8
(SAL/channel-np.c:sal_np_midpath_relay:1775)
DBG:20:3213861920:74100d20:0018: Released relay_mutex on in 0x6d6e79e8
(SAL/channel-np.c:sal_np_midpath_relay:1791)
DBG:21:3213861935:74100d20:0018: RELAY notify(0x6d6ce840, 2, 0,
socket=0x621bb58/0x621bb58) (SAL/channel-np.c:sal_np_relay_cb:1574)
DBG:22:3213861949:74100d20:0018: sal_np_relay_notify: signaling condvar
(SAL/channel-np.c:sal_np_relay_cb:1604)
DBG:23:3213861961:74100d20:0018: Acquired relay_mutex on out 0x764a32f8
(SAL/channel-np.c:sal_np_midpath_relay:1822)
DBG:24:3213861973:74100d20:0018: Released relay_mutex on out 0x764a32f8
(SAL/channel-np.c:sal_np_midpath_relay:1838)
DBG:25:3213861991:74100d20:0018: Succeeded in detaching relay
(SAL/channel-np.c:sal_np_midpath_relay:1907)
DBG:26:3213862012:74100d20:0018: Finish external handoff for client_ch
0x6d6ce7c0 (aware.c:aware_dispatch_request:497)
DBG:27:3213862026:74100d20:0018: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:28:3213862042:74100d20:0018: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:29:3213862058:74100d20:0018: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:30:3213862070:74100d20:0018: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:31:3213862083:74100d20:0018: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)
DBG:32:3213862099:74100d20:0018: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
```

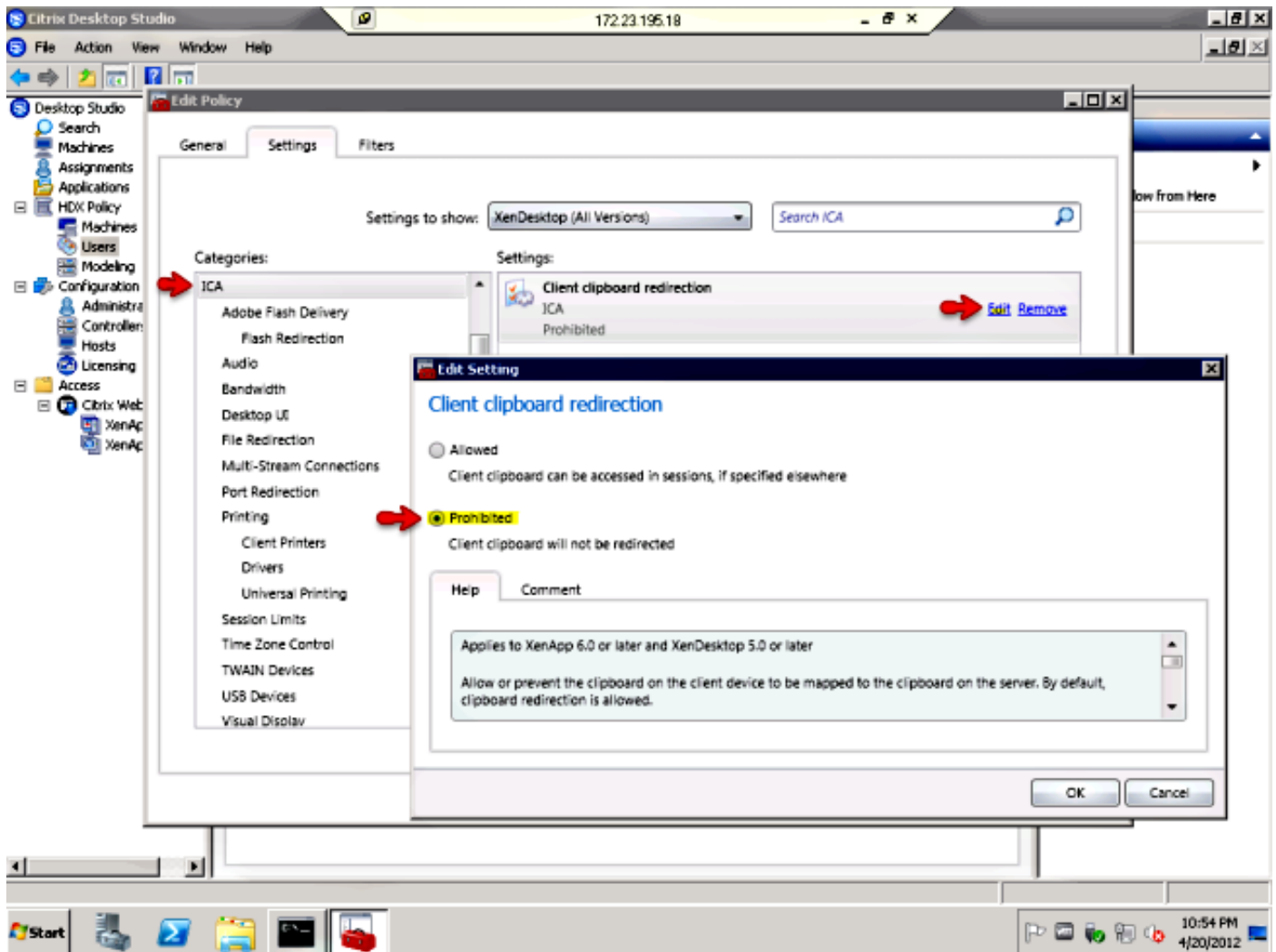
Utilisez les commandes de débogage d'authentification générique afin de déboguer les problèmes d'authentification, tels que :

```
debug aaa commondebug ldapdebug radiusdebug sdi
```

Foire aux questions (FAQ)

Q. Cette nouvelle fonctionnalité conserve-t-elle les contrôles granulaires configurés sur XenServer (par exemple, les contrôles tels que la redirection du lecteur client, la redirection de l'imprimante client, la redirection de la carte clipart client et la redirection des périphériques USB client) ?

A. Ces paramètres sont définis sur XenServer et font partie du fichier ICA. L'ASA ne modifie pas ces paramètres. Par conséquent, le paramètre que vous avez sur XenApp ou XenDesktop est reflété sur le client.



Q. L'ASA dispose-t-il d'un contrôle granulaire de la connexion ICA, par exemple pour empêcher le copier-coller et pour contrôler la redirection de l'imprimante, du lecteur, du presse-papiers ou de l'USB ?

A. L'ASA ne modifie pas ces paramètres. Par conséquent, les paramètres que vous avez sur XenApp ou XenDesktop sont reflétés sur le client du récepteur. Cisco est conscient de l'écart de fonctionnalités, car ses concurrents (Juniper SA et Citrix CAG) sont en mesure d'empêcher le copier-coller, quel que soit le paramètre de XenApp.

Q. Le serveur Citrix de Storefront fonctionne-t-il avec l'ASA en tant que proxy ?

A. Oui, cette fonctionnalité n'est pas prise en charge. La demande d'amélioration [CSCug18734](#) a été déposée afin d'ajouter la prise en charge de ces types de serveurs. La prise en charge SSO de Storefront version 2.0 est ajoutée dans le cadre de la prise en charge XenDesktop. Toutes les fonctionnalités Citrix héritées sont prises en charge dans Storefront Version 2.0 (XenApp et XenDesktop). Les fonctions liées au contrôleur d'applications ne sont pas prises en charge par

l'ASA.

Lorsque vous configurez l'ASA pour Citrix Receiver, assurez-vous de spécifier le chemin d'accès complet au service XML exécuté sur le Storefront, par exemple, <http://storefront.cisco.com/Citrix/storefrontweb/pnagent/>.

Dans les versions qui n'ont pas le correctif pour [CSCug18734](#) et qui ont le **débogage webvpn citrix** activé, si vous essayez d'accéder à un serveur Storefront, vous voyez ceci dans les débogages :

```
-----8<-----  
Received config.xml request  
+++ UNKNOWN EXCEPTION CAUGHT  
Terminating session for user [test]  
-----8<-----
```

Q. Même si le serveur Citrix a activé et configuré le service XML, l'erreur **+++ EXCEPTION INCONNUE CAUGHT** continue à s'afficher. Ça fonctionnait. Qu'est-ce qui pourrait être mal ?

A. Cela peut se produire lorsque AnyConnect Essentials est activé sur l'ASA, comme indiqué ici :

```
webvpn  
  enable outside  
  anyconnect-essentials
```

AnyConnect Essentials est utilisé afin d'activer uniquement la prise en charge complète des clients sur l'ASA, ce qui empêche l'ASA de traiter les tentatives de connexion sans client. Lorsque cela se produit, si la **demande de transformation debug webvpn** et **debug webvpn citrix** sont activées, vous voyez ceci :

Received config.xml request

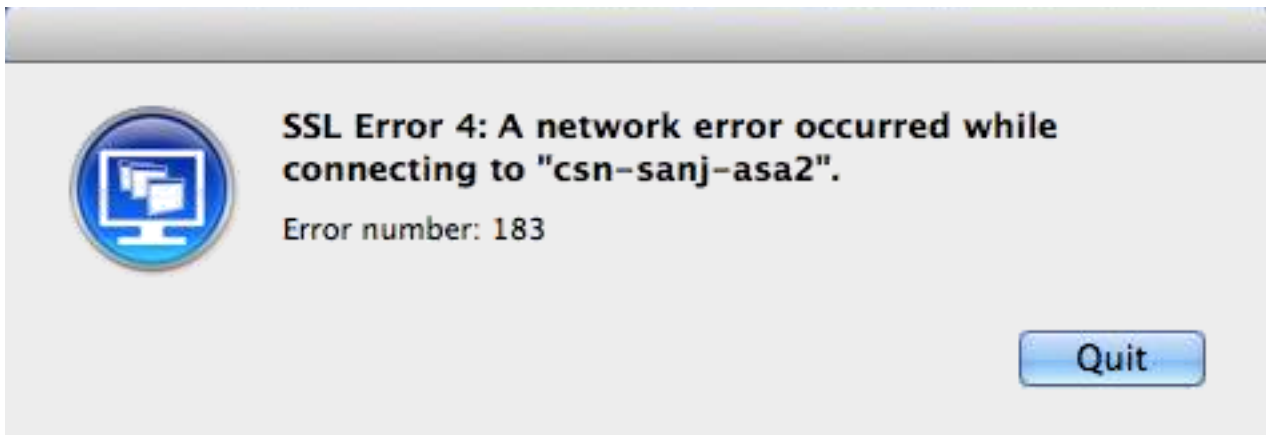
```
DBG:29:4089679874:74100d20:9902: Finished with hooks  
(aware.c:aware_dispatch_request:389)  
DBG:30:4089679886:74100d20:9902: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)  
(aware.c:aware_dispatch_request:508)  
DBG:31:4089679900:74100d20:9902: in process request  
(proxy.c:process_request:239)  
DBG:32:4089679950:74100d20:9902: Load proxy settings  
(ucte_policy.c:ucte_get_ctx_settings:690)  
DBG:33:4089679965:74100d20:9902: Load proxy settings  
(ucte_policy.c:ucte_get_ctx_settings:720)  
DBG:34:4089680019:74100d20:9902: parse_req_headers(client_fd, p_req) ;  
(proxy.c:process_request:275)  
DBG:35:4089680038:74100d20:9902: # req  
(parse_req_headers.re2c:parse_req_headers:1269)  
DBG:36:4089680049:74100d20:9902: # ver: cursor = 0x747e5a9e; lim = 0x747e5d0f  
(parse_req_headers.re2c:parse_req_headers:1383)  
DBG:37:4089680064:74100d20:9902: # ver: cursor = 0x747e5a9f; lim = 0x747e5d0f  
(parse_req_headers.re2c:parse_req_headers:1383)  
DBG:38:4089680077:74100d20:9902: Request: [GET /Citrix/pnagent/config.xml HTTP/1.1]:  
39 (parse_req_headers.re2c:parse_req_headers:1399)  
.  
.  
.  
DBG:96:4089680705:74100d20:9902: Clientless WebVPN is not enabled.  
(proxy.c:process_request:384)  
.  
.  
.
```



```
DBG:31:4089681295:74100d20:9902: fwrite(0 ? ==> 90): [Connection:
close%0d%0aCache-Control: no-store%0d%0aContent-Type: text/html%0d%0aContent-Length:
0%0d%0a%0d%0a]: 90 (SAL/sal-stdio.c:sal_fwrite:92)
+++ UNKNOWN EXCEPTION CAUGHT
Terminating session for user [test.user]
```

Q. Si vous recevez ce message d'erreur **Erreur SSL 4 : Numéro d'erreur : 183**, que devriez-vous faire ?

A. Cette erreur apparaît lorsque la connexion au broker XML (serveur XenDesktop) est autorisée, mais que les ports 1494 et 2598 au pool XenDesktop réel sont bloqués. Vous pouvez déboguer si vous activez tous les ports, puis affiner les ports requis.



Pour que XenDesktop fonctionne sans client, s'il existe des pare-feu intermédiaires entre l'ASA (à l'intérieur) et le serveur XenDesktop, assurez-vous que les ports 443, 1494, 2598 et 80 sont ouverts sur ce pare-feu. Vérifiez également que les ports sont ouverts pour le serveur XenDesktop et le pool de XenDesktop.

Q. L'ASA prend-il en charge les connexions SSL qui proviennent d'un client Citrix Receiver autonome à partir d'une plate-forme OSX Microsoft Windows/Macintosh, tout comme vous utilisez AnyConnect ou le client VPN Cisco ?

A. Actuellement, les récepteurs Citrix autonomes des postes de travail sont pris en charge uniquement via un tunnel intelligent (sans client).

[CSCum85649](#) ENH : Prise en charge des récepteurs Citrix autonomes de bureau vers ASA

Il s'agit d'un bogue d'amélioration pour prendre en charge une connexion Citrix Receiver autonome à l'ASA sans avoir besoin du tunnel intelligent ou de la connexion initiale au portail, comme il y en a pour le récepteur Citrix mobile avec l'ASA comme passerelle d'accès.

Actuellement, l'ASA envoie une réinitialisation après la première connexion à un récepteur Citrix autonome (avec l'utilisation de la dernière version 4.1 pour Windows, et a le même comportement sur d'autres plates-formes également).