ASA SSLVPN sans client : Questions de périphérique prêt à brancher RDP

Contenu

Introduction

Ce document apporte des réponses à quelques forums aux questions au sujet du périphérique prêt à brancher de Remote Desktop Protocol (la RDP), disponible aux utilisateurs sans client de Secure Sockets Layer VPN (SSLVPN) de l'appliance de sécurité adaptable Cisco (ASA).

Le périphérique prêt à brancher RDP est seulement un des connexions disponibles aux utilisateurs, avec d'autres tel que le Protocole Secure Shell (SSH), le Virtual Network Computing (VNC), et le Citrix. Le périphérique prêt à brancher RDP est l'une le plus souvent des connexions utilisées dans cette collecte. Ce document fournit plus de détails au sujet du déploiement et dépanne des procédures pour ce périphérique prêt à brancher.

Remarque: Ce document ne fournit pas des informations au sujet de la façon configurer le

périphérique prêt à brancher RDP. Pour des informations supplémentaires, référez-vous au guide de déploiement de VPN SSL de Cisco ASA 5500, version 8.x.

Informations générales

Le périphérique prêt à brancher RDP a évolué d'un périphérique prêt à brancher basé sur Java pur RDP, pour inclure les deux le client RDP d'ActiveX (Internet Explorer), aussi bien que le client java (navigateurs d'explorateur de Non-Internet).

Périphérique prêt à brancher de Javas

Le client RDP de Javas utilise l'applet approprié RDP de Javas. L'applet Java est alors enveloppé dans un périphérique prêt à brancher qui permet l'installation dans le portail sans client ASA.

Périphérique prêt à brancher actif-x

Le périphérique prêt à brancher RDP inclut également le client RDP de Microsoft ActiveX, et le périphérique prêt à brancher détermine si utiliser Javas ou client d'ActiveX basé sur le navigateur. C'est-à-dire :

- Si la tentative d'utilisateurs de l'Internet Explorer (IE) d'utiliser la RDP par un portail sans client SSLVPN, et l'URL de signet ne contient pas l'argument de **ForceJava=true**, alors le client d'ActiveX est utilisé. Si ActiveX n'exécute pas, le périphérique prêt à brancher initie le client java.
- Si la tentative des utilisateurs non-IE de lancer une RDP bookmark ou URL, seulement le client java est lancé.

Pour plus d'informations sur des conditions requises pour la RDP ActiveX et privilèges des utilisateurs, mettez en référence les conditions requises de Microsoft pour l'article de connexion de Web de bureau distant.

La prochaine image illustre les trois liens qui peuvent être sélectionnés dans la fenêtre du navigateur après que le périphérique prêt à brancher soit lancé :

1. **Nouvelle page du portail** - Ce lien ouvre la page du portail dans une nouvelle fenêtre du navigateur.
2. **Plein écran** - Ceci utilise la fenêtre RDP en mode pleine page.
3. **Rebranchez avec Javas** - Ceci force le périphérique prêt à brancher pour rebrancher et utiliser Javas au lieu d'ActiveX.

Périphérique prêt à brancher RDP

Utilisation du périphérique prêt à brancher la RDP et RDP-2

- **Périphérique prêt à brancher RDP :** C'est le périphérique prêt à brancher d'origine créé qui contient Javas et le client d'ActiveX.
- **Périphérique prêt à brancher RDP2 :** En raison des modifications dans le protocole RDP, le client approprié RDP de Javas était mis à jour afin de prendre en charge des serveurs de terminaux de Microsoft Windows 2003 et des serveurs de terminaux de Windows Vista.

  Conseil : Le dernier périphérique prêt à brancher RDP combine les protocoles la RDP et RDP2. En conséquence le périphérique prêt à brancher RDP2 est Désuet(e). Il est recommandé pour utiliser la version plus-récente du périphérique prêt à brancher RDP. Les nomenclatures embrochables RDP suit cette structure : **rdp-plugin.yymmdd.jar, où le yy est un** format **à deux chiffres d'année**, millimètre est un format de **two-digitmonth**, et la densité double est un format **two-digitday**.

Afin de télécharger le périphérique prêt à brancher, visitez la page de téléchargement du logiciel de Cisco.

ActiveX contre le positionnement de client java

RDP-ActiveX

- IE d'utilisations seulement
- Fournit le support pour le bruit expédié

RDP-Javas

- Travaille à tous les navigateurs pris en charge qui Java-sont activés.
- Le client java est lancé dans l'IE seulement si ActiveX ne lance pas, ou l'argument de **ForceJava=true** passe dans le signet RDP.
- L'implémentation de RDP-Javas est basée sur le projet approprié RDP de Javas, une initiative open source ; le support de meilleur effort est donné pour l'application.

Format de signet RDP

Voici un format d'exemple d'un signet RDP :

```
rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

Voici quelques informations importantes au sujet du format :

- **serveur** - C'est le seul attribut exigé. Écrivez le nom de l'ordinateur qui héberge les Microsoft Terminaux Service.

- **port** (facultatif) - C'est l'adresse virtuelle dans l'ordinateur distant qui héberge les Microsoft Terminaux Service. La valeur par défaut, 3389, apparie le nombre de port connu pour des Microsoft Terminaux Service.
- **paramètres** - C'est une chaîne facultative de requête qui se compose des paires de paramètre-valeur. Des demarks d'un point d'interrogation le début de la chaîne d'argument, et chaque paire de paramètre-valeur est séparés par une esperluète.

  Voici une liste de paramètres disponibles :

  la géométrie - C'est la taille de l'écran de client en pixels (W X H).**bpp** - C'est le bit-par-pixel (profondeur de couleurs), 8|16|24|32.**domaine** - C'est le domaine de procédure de connexion.**nom d'utilisateur** - C'est le nom d'utilisateur pour la procédure de connexion.**mot de passe** - C'est le mot de passe de connexion. Utilisez le mot de passe avec soin, parce qu'il est utilisé au côté client et peut être observé.**console** - Ceci est utilisé afin de se connecter à la session de console sur le serveur (oui/non).**ForceJava** - Placez ce paramètre à l'**oui** afin d'utiliser seulement le client java. La valeur par défaut est **non.shell** - Placez ce paramètre au chemin de l'exécutable/d'application qui est commencée automatiquement quand vous vous connectez à la RDP (**rdp://server/?shell=path**, par exemple).

  Voici une liste de à paramètres ActiveX réservés supplémentaires :

  RedirectDrives - Placez ce paramètre **pour rectifier** afin de tracer les lecteurs distants localement.**RedirectPrinters** - Placez ce paramètre **pour rectifier** afin de tracer les imprimantes distantes localement.**Pleine page** - Placez ce paramètre **pour rectifier** afin de lancer en mode pleine page.**ForceJava** - Placez ce paramètre à l'**oui** afin de forcer le client java.**l'audio** ce paramètre est utilisé pour l'expédition sonore au-dessus de la session RDP :

  0 - Réoriente les bruits distants à l'ordinateur client.**1** - Lit des bruits à l'ordinateur distant.**2** - Désactive la redirection saine ; ne lit pas des bruits au serveur distant.

Périphérique prêt à brancher RDP et Équilibrage de charge VPN

l'Équilibrage de charge de Multi-zone géographique est pris en charge avec l'utilisation de l'équilibrage de charge du serveur global basé sur de Domain Name Server (DN). En raison du résultat de DN cachant des différences, les connexions pourraient fonctionner différemment à travers les systèmes d'exploitation divers. Le cache DNS de Windows permet au périphérique prêt à brancher pour résoudre la même adresse IP quand il des lauches l'applet Java. Sur l'OS X de Macintosh (MAC), il est possible que l'applet Java résolve une adresse IP différente. En conséquence, le périphérique prêt à brancher ne lance pas correctement.

Un exemple des DN circulaires est quand vous avez un URL simple (https://www.example.com) où l'entrée DNS pour **www.example.com** peut résoudre 192.0.2.10 (ASA1) ou 198.51.100.50 (ASA2).

Après les journaux de l'utilisateur dans le portail de Sans client-webvpn par l'intermédiaire d'un navigateur sur ASA1, l'initiaition du périphérique prêt à brancher RDP est possible. Pendant l'initiation du client java, les ordinateurs de MAC OS X exécutent une nouvelle demande de résolution de DN. Avec une configuration DNS circulaire, il y a une occasion de 50% que cette deuxième réponse de résolution renvoie le même site qui a été choisi pour la connexion initiale de

webvpn. Si la réponse de serveur DNS est 198.51.100.50 (ASA2) plutôt que 192.0.2.10 (ASA1), le client java initie une connexion à l'ASA fausse (ASA2). Car la session d'utilisateur n'existe pas sur l'ASA2, la demande de connexion est rejetée.

Ceci pourrait avoir comme conséquence des messages d'erreur Java semblables à ceci :

```
java.lang.ClassFormatError: Incompatible magic value 1008813135 in
 class file net/propero/rdp/applet/RdpApplet
```

Foires aux questions

Pourquoi quelques caractères tapés n'apparaissent-ils pas sur la session RDP de distant ?

L'ordinateur distant en session RDP pourrait avoir une configuration différente de région de clavier que l'ordinateur local. En raison de cette différence, l'ordinateur distant ne pourrait pas afficher certains caractères tapés ou caractères incorrects. Ce comportement est vu avec seulement avec le périphérique prêt à brancher de Javas. Afin de résoudre ce problème, employez l'attribut de **keymap** afin de tracer le keymap local dans l'ordinateur distant.

Par exemple, afin de placer un mappage allemand de clavier, utilisation :

```
rdp://<IP Address of the server>/?keymap=de

The following keymaps are available:
----------------------------------------------------------------------
ar    de    en-us fi    fr-be it    lt    mk    pl    pt-br sl    tk
da    en-gb es    fr    hr    ja    lv    no    pt    ru    sv    tr
----------------------------------------------------------------------
```

Problèmes connus avec des mappages de clavier

- ID de bogue Cisco CSCth38454 - **Keymap hongrois de mise en place pour le périphérique prêt à brancher RDP.**
- ID de bogue Cisco CSCsu77600 - **Les clés embrochables de fenêtre RDP de webvpn sont incorrectes. Décalez (clé) .jar**.
- ID de bogue Cisco CSCtt04614 - **Webvpn - Les signes diacritiques de clavier es ont inexactement géré par module d'extension RDP.**
- ID de bogue Cisco CSCtb07767 - **Module d'extension ASA - Configurez les paramètres par défaut**.

  Conseil : Un autre contournement possible est d'utiliser un tunnel intelligent d'application pour **mstsc.exe. Ceci** est configuré sous le mode de sous-titre-configuration de webvpn avec cette commande : **fenêtres de plate-forme RDP mstsc.exe de RDP_List de liste d'intelligent-tunnel.**

Le périphérique prêt à brancher RDP de Javas peut-il prendre en charge des sessions pleine page RDP ?

Actuellement, il n'y a aucune prise en charge native pour des sessions pleine page RDP. La demande d'amélioration CSCto87451 a été classée afin d'implémenter ceci. Si le paramètre de la **géométrie** (la **géométrie =1024x768**, par exemple) est placé à la résolution du moniteur d'utilisateur, il fonctionne en mode pleine page. Car les tailles de l'écran d'utilisateur varient, il pourrait être nécessaire de créer de plusieurs liens de signet. Le client d'ActiveX prend en charge à la façon des indigènes des sessions pleine page RDP.

Le client java peut-il communiquer avec l'utilisation d'AES-256 pour le cryptage ?

Afin de permettre au client java pour négocier le SSL correctement, ajustez la commande du chiffrement-positionnement SSL ASA pour apparier ceci :

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

Le client java pourrait afficher cette erreur si la commande de chiffrement-positionnement est différente :

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

Dépannez les questions RDP

Si vous éprouve d'autres questions avec le périphérique prêt à brancher RDP, il pourrait être utile de collecter ces données afin de dépanner des questions RDP :

- **Le tech d'exposition** sorti de l'ASA
- La sortie **détaillée embrochable de webvpn d'importation d'exposition de l'**ASA
- Le système d'exploitation de l'ordinateur d'utilisateur et niveau du correctif
- Le système d'exploitation de l'ordinateur de destination et niveau du correctif
- Le client qui est utilisé (ActiveX ou Javas) et version de Javas JRE
- Déterminez si l'ASA est dans une batterie d'équilibrer la charge, basée sur dn, ou basée sur ASA

Mises en garde connues

Questions de mise à jour de sécurité de Microsoft

1. KB2695962 - Bulletin de renseignements de Sécurité de Microsoft : Remontée pyramidale de mise à jour pour des bits de mise à mort d'ActiveX : 8 mai, 2012.
2. KB2675157 - MS12-023 : Mise à jour de sécurité cumulative pour l'Internet Explorer : Avril 10, 2012.
3. cisco-sa-20120314-asaclient - Vulnérabilité à distance sans client le 14 d'exécution de code de contrôle de l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 VPN ActiveX mars.
4. ID de bogue Cisco CSCtx68075 - Webvpn ASA se cassant quand le correctif KB2585542 de Windows est appliqué (8.2.5.29/8.4.3.9).
5. KB2585542 - MS12-006 : Description de la mise à jour de sécurité pour Webio, Winhttp, et

schannel dans Windows : Janvier 10, 2012.

Client d'ActiveX

- **Symptômes** : Le client d'ActiveX ne charge pas des versions 6 à 9 IE après une mise à jour à la version 8.4.3 OS ASA.

  Référez-vous à l'ID de bogue Cisco CSCtx58556. La difficulté est disponible pour des versions 8.4.3.4 et plus tard.Contournement : Forcez l'utilisation du client java.

- **Symptômes** : Le client d'ActiveX ne charge pas après que la version OS ASA soit déclassifiée à une version antérieure à 8.4.3. Ceci affecte les utilisateurs qui ont utilisé le client d'ActiveX sur une ASA avec la difficulté pour l'ID de bogue Cisco CSCtx58556, et se connecte à cette ASA à une version antérieure à 8.4.3. C'est dû à une nouvelle connexion RDP d'ActiveX introduite dans la version 8.4.3 ASA, qui n'est pas compatible avec les versions antérieures.

  Référez-vous à l'ID de bogue Cisco CSCtx57453.Retirez tous les exemples de registre de Windows de **b8e73359-3422-4384-8d27-4ea1b4c01232 ?** (vieil ActiveX CLSID).

  Remarque: On lui en suggère d'exécuter une sauvegarde du registre de système informatique avant édite.
- **Symptômes** : Les connexions RDP aux périphériques avec l'authentification de niveau du réseau (NLA) activée échouent.

  Référez-vous à l'ID de bogue Cisco CSCtu63661 pour l'amélioration qui invite NLA pour être incorporée dans le périphérique prêt à brancher RDP d'ActiveX.Bien que le client de Microsoft ActiveX prenne en charge NLA, l'utilisation de cette caractéristique dans le périphérique prêt à brancher ASA n'est pas prise en charge.Contournement : Configurez le périphérique prêt à brancher RDP (**mstsc.exe) intelligent-**à percer un tunnel. Référez-vous au guide de déploiement de VPN SSL de Cisco ASA 5500, version 8.x.

- **Symptômes** : La RDP d'ActiveX ne charge pas, et affiche une page vierge.

  Référez-vous à l'ID de bogue Cisco CSCsx49794.Ceci se produit quand la chaîne de certificat pour le certificat ssl ASA est plus grande que quatre Certificats (CERT de RACINE, SUBCA1, SUBCA2, et ASA, par exemple).Contournement :

  N'installez pas la grande chaîne de certificat sur l'ASA.Le périphérique prêt à brancher RDP de Javas est connu pour fonctionner correctement, par opposition au périphérique prêt à brancher d'ActiveX.La RDP travaille également correctement quand vous configurez Windows indigène **mstsc.exe avec les** tunnels intelligents.

- **Symptômes** : Après que le client RDP d'ActiveX soit utilisé, un utilisateur clique sur le bouton de **déconnexion** et reçoit un **HTTP 404 - paginez l'**erreur **non trouvée**. Référez-vous à l'ID de bogue Cisco CSCtz33266. Cette question a est résolue avec le version du plug-in **rdp-plugin.120424.jar** ou plus tard.

- **Symptômes** : Un utilisateur a deux onglets ouverts dans l'IE - un pour la session RDP et des autres pour un blanc ou toute autre page Web. L'IE ne fonctionne pas correctement après que la RDP tabulent soit fermée.

  Référez-vous à l'ID de bogue Cisco CSCua69129.Contournement : Utilisez le périphérique prêt à brancher RDP de Javas (placez **ForceJava=true**).

- **Symptômes** : Le périphérique prêt à brancher d'ActiveX entraîne l'utilisation haute-CPU avec l'IE. Référez-vous à l'ID de bogue Cisco CSCua16597.

- **Symptômes** : Après installation de mise à jour KB2695962 de Windows**, la** connexion RDP d'ActiveX ne charge pas. Quand une nouvelle session RDP est ouverte, les tentatives de client d'ActiveX d'installer l'**expéditeur de port de VPN SSL de Cisco** (ceci ne se produit pas toujours) et revient à la page du portail sans client sans se connecter à l'ordinateur distant. C'est dû à la vulnérabilité **CVE-2012-0358,** qui est résolue sur le côté client du bulletin de renseignements de Sécurité de Microsoft (2695962).

  Référez-vous à la vulnérabilité à distance sans client d'exécution de code de contrôle de l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 VPN ActiveX d'avis de sécurité Cisco.Référez-vous à l'ID de bogue Cisco CSCtr00165.

Client java

> Remarque: Cisco ne redistribue des connexions sans aucune modification. En raison de la Licence public général GNU, Cisco ne modifie pas ou étend l'application embrochable. Le périphérique prêt à brancher de **properJavaRDP** est une application open source, et toutes les questions avec le logiciel embrochable doivent être abordées par le propriétaire de projet.

- **Symptômes** : des applications Processeur-intensives sont exécutées sur l'ordinateur distant une fois accédées à par l'intermédiaire du client RDP de Javas, et un crash d'applet Java est expérimenté.

  Ce message d'erreur pourrait afficher : **Net.propero.rdp MORTEL - javax.net.ssl.SSLException : La connexion a été arrêt : .....**Le comportement est triggerd en commutant entre des applications deux ou CPU-plus intensifs rapidement.Cette question est réparée dans les version du plug-in rdp.2012.6.4.jar et plus tard. Contournement :

  Connectez à l'utilisation du client d'ActiveX.Ne commutez pas entre les applications rapidement.

- **Symptômes** : Le client RDP de Javas génère ce message d'erreur : **net.propero.rdp.Rdp - java.net.SocketException : Le socket est java.net.SocketException fermé : Le socket est fermé, et puis se ferme.**

  La question est provoqué par par un groupe de tunnels qui a un groupe-URL configuré avec seulement le FQDN (http://www.example.com, par exemple).Référez-vous à l'ID de bogue

Cisco CSCuh72888.Contournement :

Retirez l'entrée groupe-URL sans « / » au groupe de tunnels.Utilisez le client d'ActiveX.

- **Symptômes** : Le client RDP de Javas échoue quand il est connecté à un ordinateur de Windows 8.

  Le client RDP de Javas n'a pas actuellement le soutien de ceci.Référez-vous à l'ID de bogue Cisco CSCuc79990Contournement :

  Utilisez le client RDP d'ActiveX.Tunnel intelligent le client indigène RDP de Windows (**mstsc.exe).**

- **Symptômes** : Le client RDP de Javas échoue avec ce message d'erreur : **ARSigningException : Fondez l'entrée non signée dans la ressource : https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  Cette question est provoqué par par une bogue dans le rewriter de Javas de webvpn ASA.Référez-vous à l'ID de bogue Cisco CSCuj88114.Contournement : Downgrade à la version 7u40 de Javas.