

Foire aux questions de sécurité du contenu : Comment accédez à-vous le CLI sur une appliance de sécurité du contenu ?

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Comment accédez à-vous le CLI sur une appliance de sécurité du contenu ?](#)

Introduction

Ce document décrit comment accéder au CLI par un client de telnet ou de Protocole Secure Shell (SSH) sur une appliance de sécurité du contenu de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Appliance de sécurité Web de Cisco (WSA)
- Appliance de Gestion de sécurité Cisco (SMA)
- AsyncOS

[Composants utilisés](#)

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

- Cisco ESA AsyncOS, toutes les versions
- Cisco WSA AsyncOS, toutes les versions
- Versions AsyncOS de Cisco SMA, toutes les versions

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.

Note: Ce document met en référence le logiciel qui n'est pas mis à jour ou est pris en charge par Cisco. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.

Comment accédez à-vous le CLI sur une appliance de sécurité du contenu ?

Vous pouvez accéder au CLI de votre appliance avec un client Telnet ou un client SSH. Cependant, le protocole Telnet est décrypté, ainsi quand vous vous connectez dans votre appliance par le telnet, vos qualifications mettent en boîte plus facilement soit dérobé.

Cisco recommande que tous les ordinateurs de production utilisent un client SSH. Supplémentaire, il est difficile l'utiliser le client Telnet de Microsoft Windows de norme. Par défaut d'usine, le telnet est configuré sur le port de gestion.

Terminez-vous ces étapes afin de désactiver le telnet :

1. Connectez-vous dans le GUI de Web.
2. Naviguez vers le **réseau > les interfaces IP**.
3. Cliquez sur le nom de l'interface que vous voulez éditer.
4. Décochez la case de **telnet** dans le domaine de services.

Terminez-vous ces étapes afin d'accéder à votre appliance par le SSH (port 22) :

1. Installez un client SSH dans Microsoft Windows, tel que le [mastic](#).

2. Lancez le client SSH :

Ajoutez les informations d'hôte pour votre appliance (telle que **c650.example.com**).

Chargement de clic.

Écrivez votre nom d'utilisateur.

Entrez votre mot de passe.

3. Ouvrez une invite de commande avec le ***nix**.
4. Sélectionnez la commande d'**exampleC650.com de ssh \$**.
5. Si vous devez spécifier un utilisateur différent, sélectionnez la commande du **ssh**

`<user>@exampleC650.com $`. Si le nom d'utilisateur est **admin**, sélectionnez la commande `d'admin@C650.example.com de ssh $`.

Terminez-vous ces étapes afin d'accéder à votre appliance par le telnet :

Note: Cisco recommande que vous utilisiez un client SSH pour l'accès ; l'utilisation du telnet n'est pas recommandée.

1. Ouvrez une invite de commande.
2. Sélectionnez la commande de `c650.example.com de telnet`.
3. Écrivez votre nom d'utilisateur.
4. Entrez votre mot de passe.