Configuration du client SSH pour Cisco ThreatGrid Appliance

Contenu

Introduction
<u>Problème</u>
Solution
<u>Putty</u>
SecureCRT

Introduction

Ce document décrit comment configurer différents clients SSH pour qu'ils fonctionnent correctement avec Cisco ThreatGrid Appliance via SSH.

Problème

Le client SSH affiche des pseudographiques incorrects lors de la connexion à Cisco ThreatGrid Appliance.



Solution

Putty

Étape 1. Sélectionnez **DEC-MCS** comme **jeu de caractères distant** sous **Configuration PuTTY -> Fenêtre -> Traduction**, comme indiqué dans l'image.



Étape 2. Entrez **putty** comme **chaîne de type Terminal** sous **Configuration PuTTY -> Connexion -> Données**, comme indiqué dans l'image.

Session Data to send to the server Logging Login details Keyboard Auto-login username Bell When username is not specified: Features Prompt Window Appearance Behaviour Terminal details Selection Image details Selection Selection Colours Terminal speeds Data to send to the server
- Data - Proxy - Telnet - Rlogin ● SSH - Serial

Étape 3. Ouvrez la session configurée.



SecureCRT

Étape 1. Sélectionnez **Linux** comme terminal sous Options de session -> Terminal -> Emulation, comme illustré dans l'image.

* Connection	- Ferriting	
Connection Logon Actions SSH2 SFTP Session Advanced	Terminal: Linux	ANSI Color Use color scheme ation
Port Forwarding Remote/X11 Tormical	Linux 0	
* Finulation	Size	On resize
Modes Emacs Mapped Keys Advanced V Appearance Window Log File Printing X/Y/Zmodem	Logical rows: 24 Logical columns: 256 Scrolback	Scale the font Retain size and font
	Scrollback buffer: 2000	
		Carcel OK

Étape 2. Ouvrez la session configurée.

