Configurando o cliente SSH para o Cisco ThreatGrid Appliance

Contents

Introduction
<u>Problema</u>
<u>Solução</u>
<u>Putty</u>
SecureCRT

Introduction

Este documento descreve como configurar diferentes clientes SSH para um trabalho apropriado com o Cisco ThreatGrid Appliance via SSH.

Problema

O cliente SSH exibe pseudográficos incorretos quando se conecta ao Cisco ThreatGrid Appliance.



Solução

Putty

Etapa 1. Selecione **DEC-MCS** como o **conjunto de caracteres remotos** em **PuTTY Configuration -** > **Window -> Translation**, como mostrado na imagem.



Etapa 2. Digite **putty** como **Terminal-type string** em **PuTTY Configuration -> Connection -> Data**, como mostrado na imagem.

Session Logging Terminal Keyboard Bell Features Window	Data to send to the server
 Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial) Use system username (1) ng putty 38400,38400 bles Add Remov

Etapa 3. Abra a sessão configurada.



SecureCRT

Etapa 1. Selecione **Linux** como Terminal em Session Options -> Terminal -> Emulation, como mostrado na imagem.

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

Etapa 2. Abra a sessão configurada.

