グラフィカル ユーザ インターフェイス (GUI)で使用されている暗号方式を変更するに はどうしますか。 GUI で SSL v2 を無効にでき

ますか。

目次

<u>はじめに</u>

<u>グラフィカル ユーザ インターフェイス(GUI)で使用されている暗号方式を変更するにはどうし</u> <u>ますか。 GUI で SSL v2 を無効にできますか。</u> 関連情報

概要

この資料に表示しどんな暗号が Cisco E メール セキュリティ アプライアンス(ESA)のグラフィ カル ユーザ インターフェイス (GUI)と共に使用されるか変更する方法を記述されています。

グラフィカル ユーザ インターフェイス(GUI)で使用されてい る暗号方式を変更するにはどうしますか。 GUI で SSL v2 を無 効にできますか。

着信 GUI 接続のためにアドバタイズされる SSL プロトコルおよび暗号は sslconfig コマンドで設 定することができます。 ssl 方式が GUI SSL 通信のために特に使用される規定できます。

例:

myesa.local> sslconfig

sslconfig settings: GUI HTTPS method: sslv3tlsv1 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL Inbound SMTP method: sslv3tlsv1 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
GUI - Edit GUI HTTPS ssl settings.
INBOUND - Edit Inbound SMTP ssl settings.
OUTBOUND - Edit Outbound SMTP ssl settings.
VERIFY - Verify and show ssl cipher list.
[]> GUI

Enter the GUI HTTPS ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 2
Extend the GUI WEEDE and window want to use.

Enter the GUI HTTPS ssl cipher you want to use. [RC4-SHA:RC4-MD5:ALL]> 主要な CLI に戻り、すべての変更を保存して下さい。

関連情報

- <u>Cisco</u> 電子メール セキュリティ アプライアンス エンド ユーザ ガイド
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>