Windows Ciphers Cause TLS Issue между TMS и OpenSSL базирующиеся устройства

Содержание

Введение

Этот документ описывает проблему, которая вызвана, когда Комплект системы управления telepresence (TMS) Cisco неспособен соединиться с его управляемыми устройствами и нет "никакой ошибки" ответа https, сообщил в TMS Cisco. TMS Cisco не в состоянии начинать/управлять/контролировать совещания.

Общие сведения

Подключение устранения неполадок между TMS и самим управляемым устройством должно быть сделано перед попыткой этого решения.

Эти шаги должны включать:

1. Используйте программное обеспечение перехвата на Сервере TMS (напр. Wireshark) для обеспечения сетевого подключения между TMS и управляемым устройством.

2. Придерживайтесь этих Технических Примечаний:

- https://www. cisco . com/c/en/us/support/docs/conferencing/telepresence-management-server/118387-technote-tms-00.html
- https://www. cisco . com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/211279-How-to-Troubleshoot-No-HTTPS-response.html

Проблема

Анализ захвата пакета указывает, что существует проблема с согласованиями Набора шифров и использованиями между Windows Server, которые размещают TMS и управляемые устройства TMS Cisco , которые включают мосты конференц-связи и оконечные точки.

Решение

Когда некоторые Шифры использовали для соединения Transport Layer Security (TLS) от Windows Server, что TMS хостов был отключен, он решил некоторые вопросы о TMS Cisco,

который не сообщает "ни о какой ошибке" ответа https для управляемых устройств. Это могло позволить совещаниям быть запущенными и проверенными правильно. При использовании подробных данных, на которые обращают внимание в https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014 при отключении этих Шифров, согласно рекомендации Microsoft, он мог бы облегчить проблему:

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
```

```
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

```
TLS_RSA_WITH_AES_256_GCM_SHA384
```

```
TLS_RSA_WITH_AES_128_GCM_SHA256
```

Было также найдено, что могли бы быть другие Шифры, которые могли вызвать проблемы, когда TLS подключение выполняет согласование от Windows - клиента. Для получения дополнительной информации обратитесь к проблемам KB3172605 и его решению от этого узла: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution? forum=w7itprosecurity. Когда эти Шифры отключены, которые использовались для TLS подключение от Windows Server, который размещает TMS, он может решить некоторые вопросы о "никаких ошибках" ответа https с управляемыми устройствами TMS:

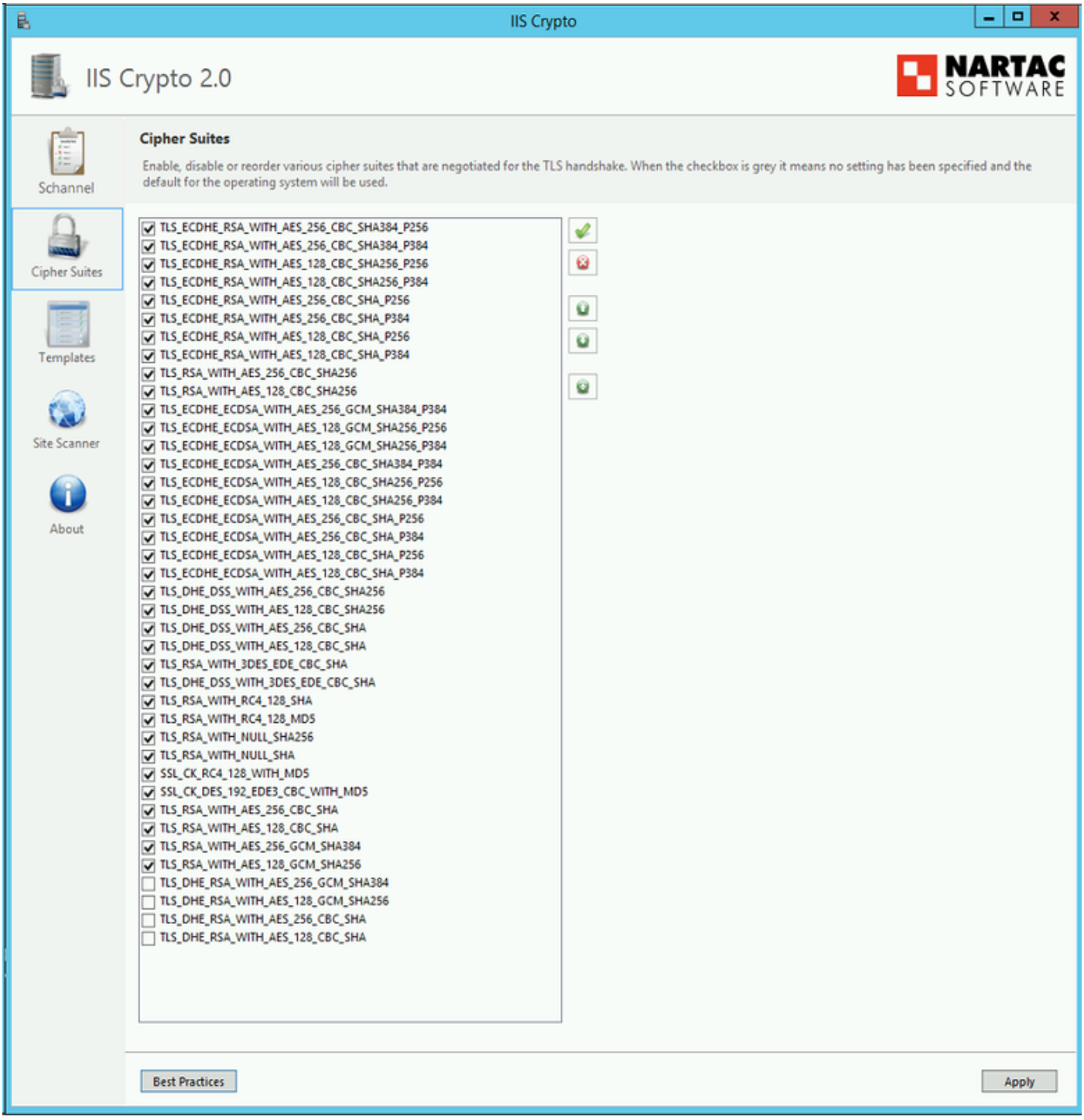
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
```

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Как удалить Шифры?

Самый простой способ удалить Шифры из Сервера TMS состоит в том, чтобы использовать программное средство третьей стороны, названное Крипто-информационными сервисами интернета (IIS). Удалите эти Шифры из списка, и затем необходимо будет перезагрузить Сервер TMS для изменений для взятия влияния. Рекомендуется, чтобы это было сделано в от часов пик во время периода технического обслуживания, чтобы гарантировать, что на пользователей не влияет это изменение.

https://www.nartac.com/Products/IISCrypto


IIS Crypto
IIS Crypto 2.0
NARTAC SOFTWARE
Schannel
Cipher Suites
Templates
Site Scanner
About
Cipher Suites
Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Best Practices
Apply