Alerts - Untraceable SSL Sessions - Unsupported Cipher

Rate This Knowledgebase	(Average Rating: 3)	Show Properties

Information

Introduction

In case the connection between the client and the webserver is encrypted, On-Premises (SecureSphere) will require the certificate and the private key in order to decrypt monitor the traffic. During the key exchange between the client and the webserver, a Cipher suite was selected by the client The decryption failed because the Cipher suite selected for the connection is not supported by On-Premises (SecureSphere). The alert may be observed at the following locations: * On the Gateway which failed to decrypt the traffic under: Setup->Gateways->Specific Gateway-> Server group: Error * An alert of "SSL Untraceable Connection - Connection using unsupported Cipher" - In the alert, you may see the specific unsupported Cipher which caused the violation.

To

Steps

The article below clarifies Untraceable SSL Sessions: Unsupported Cipher, for more information regarding additional Untraceable SSL Session alerts. refer here.

For On-Premises (SecureSphere) supported Ciphers, please refer to User Guide "**SSL Ciphers**"

Untraceable SSL Sessions: Unsupported Cipher - The Cipher suite selected for the connection is not supported by On-Premises (SecureSphere) (example: DH). The Cipher suite indicated in the violation details.

The solution to the issue is one of the following options:

1. Disable the unsupported Ciphers on the Web server

Verify which Ciphers are enabled on your Web server and compare them to the Ciphers supported by **On-Premises (SecureSphere)**. Refer for the list of supported Ciphers described in user guide "**SSL Ciphers**"
Verify what Cipher was used to trigger the alert by referring to the **Main**-> **Monitor** -> **Alerts** screen and search for "Untraceable SSL session: Unsupported Ciphers" alert. In event details of the alert, you can find the Cipher name.

Example:

User-added image

2. Change mode of the **On-Premises (SecureSphere)** to Reverse Proxy (**TRP/KRP/NGRP**) which supports DHE and ECDHE Cipher suites. Please refer user guide "**Reverse Proxies**"

Conclusion

Share This Link with a Friend

https://www.imperva.com/sign_in.asp?retURL=/articles/Procedure/SSL-How-to-handle-Unsupported-Ciphers-Alert0

Attachments

Attachment1

Attachment2

Attachment3