瞭解安全殼層資料包交換

目錄

簡介

本檔案介紹安全殼層(SSH)交涉期間之封包層級交換。

必要條件

需求

思科建議您瞭解基本的安全概念：

- 驗證
- 機密性
- 完整性
- 金鑰交換方法

採用元件

本檔案所述內容不限於特定硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。

SSH協定

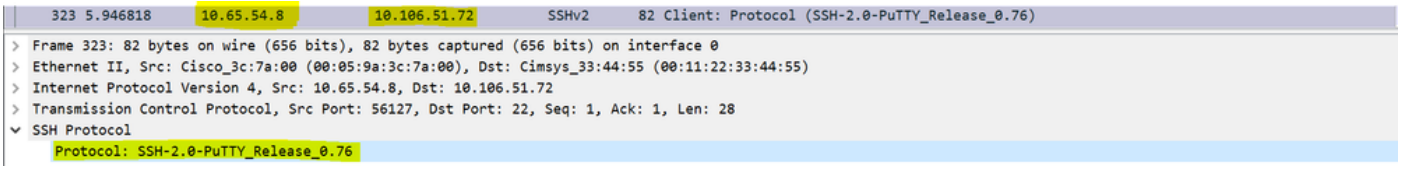
SSH協定是一種從一台電腦到另一台電腦進行安全遠端登入的方法。SSH應用基於客戶端-伺服器架構，連線SSH客戶端例項與SSH伺服器。

SSH交換

1. SSH的第一步稱為 Identification String Exchange.

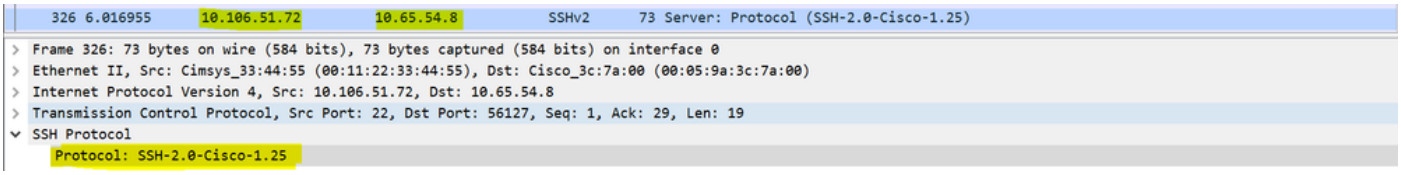
a.客戶端構建資料包並將其傳送到包含以下內容的伺服器：

- SSH協定版本
- 軟體版本



客戶端協定版本為SSH2.0，軟體版本為Putty_0.76。

b.伺服器使用其自己的標識字串交換進行響應，包括其SSH協定版本和軟體版本。

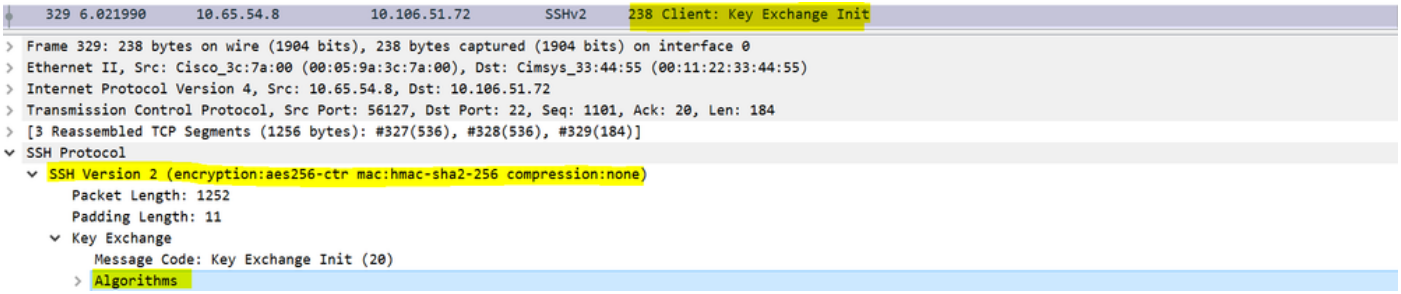


伺服器的協定版本為SSH2.0，軟體版本為Cisco1.25

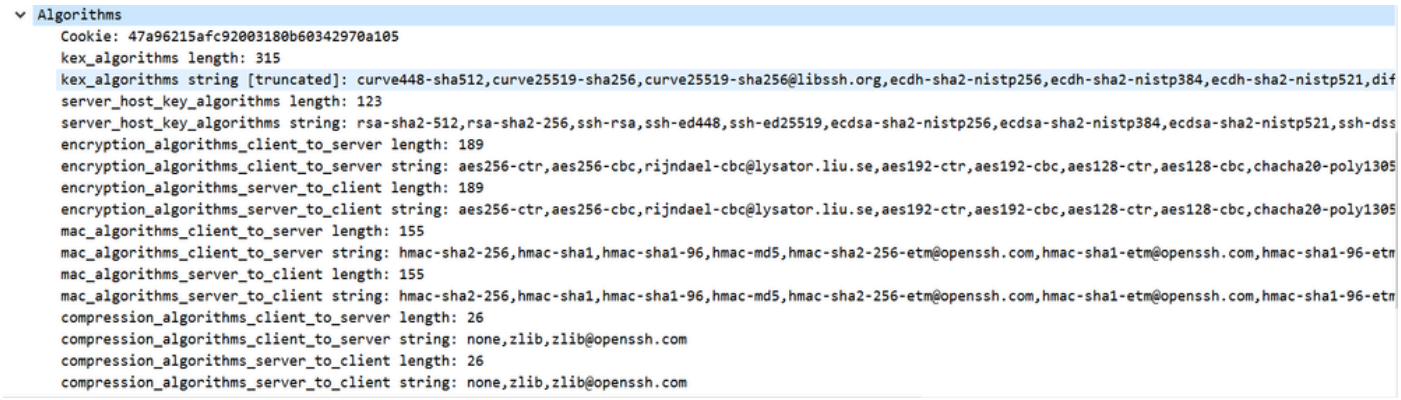
2. 下一步是**Algorithm Negotiation**.在此步驟中，客戶端和伺服器都會協商以下演算法：

- 金鑰交換
- 加密
- HMAC（雜湊型訊息驗證碼）
- 壓縮

1. 客戶端向伺服器傳送Key Exchange Init消息，指定其支援的演算法。這些演演算法會依偏好順序列出。



金鑰交換初始化

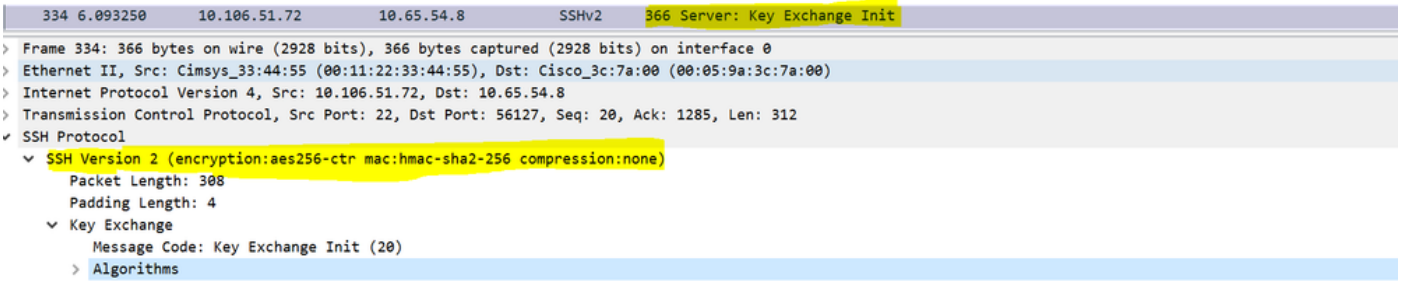


客戶端支援的演算法

b.伺服器以自己的金鑰交換初始化消息作出響應，列出其支援的演算法。

c.由於這些消息同時交換，雙方會比較其演算法清單。如果兩端所支援的演算法中存在匹配項，則繼續執行下一步。如果沒有完全相符的專案，伺服器會從使用者端清單中選取它同樣支援的第一個演演算法。

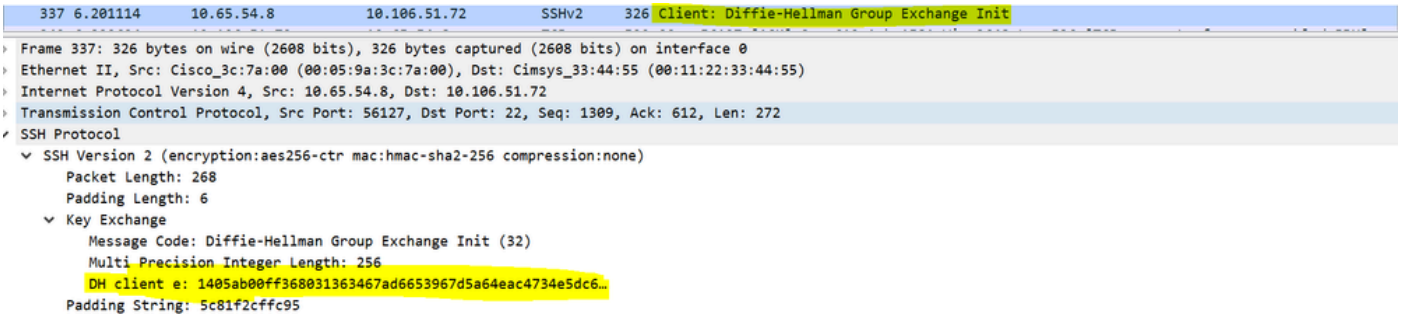
d.如果客戶端和伺服器無法就通用演算法達成一致，金鑰交換將失敗。



伺服器金鑰交換初始化

3. 在此之後，兩端進入**Key Exchange**階段，使用DH金鑰交換生成共用金鑰，並對伺服器進行身份驗證：

a.客戶端生成金鑰對，Public and Private並在DH組交換初始化資料包中傳送DH公鑰。此金鑰對用於金鑰計算。



客戶端DH公鑰和Diffie-Hellman組交換初始化

b.伺服器生成自己的Public and Private「金鑰對」。 它使用客戶端的公鑰和自己的金鑰對來計算共用金鑰。

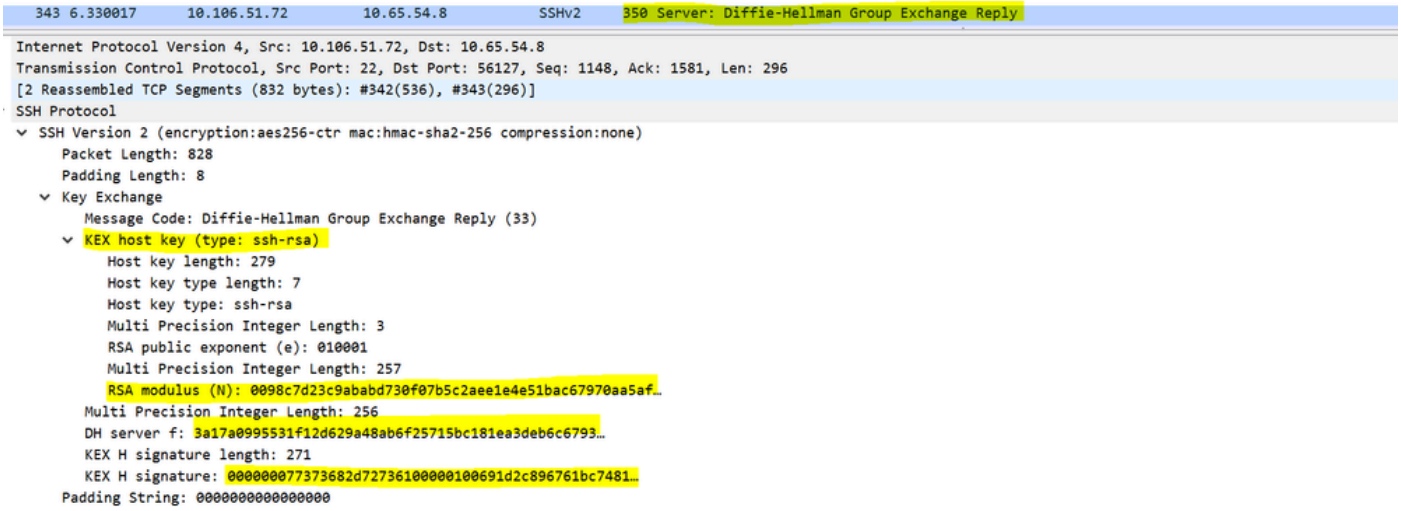
c.伺服器還使用以下輸入計算Exchange雜湊：

- 客戶端標識字串
- 伺服器辨識字串
- 客戶端KEXINIT的負載
- 伺服器KEXINIT的負載
- 來自主機金鑰的伺服器公鑰（RSA金鑰對）
- 客戶端DH公鑰
- 伺服器DH公鑰
- 共用金鑰

d.計算雜湊後，伺服器使用其RSA私鑰對其進行簽名。

e.伺服器建構訊息DH_Exchange_Reply，其中包括：

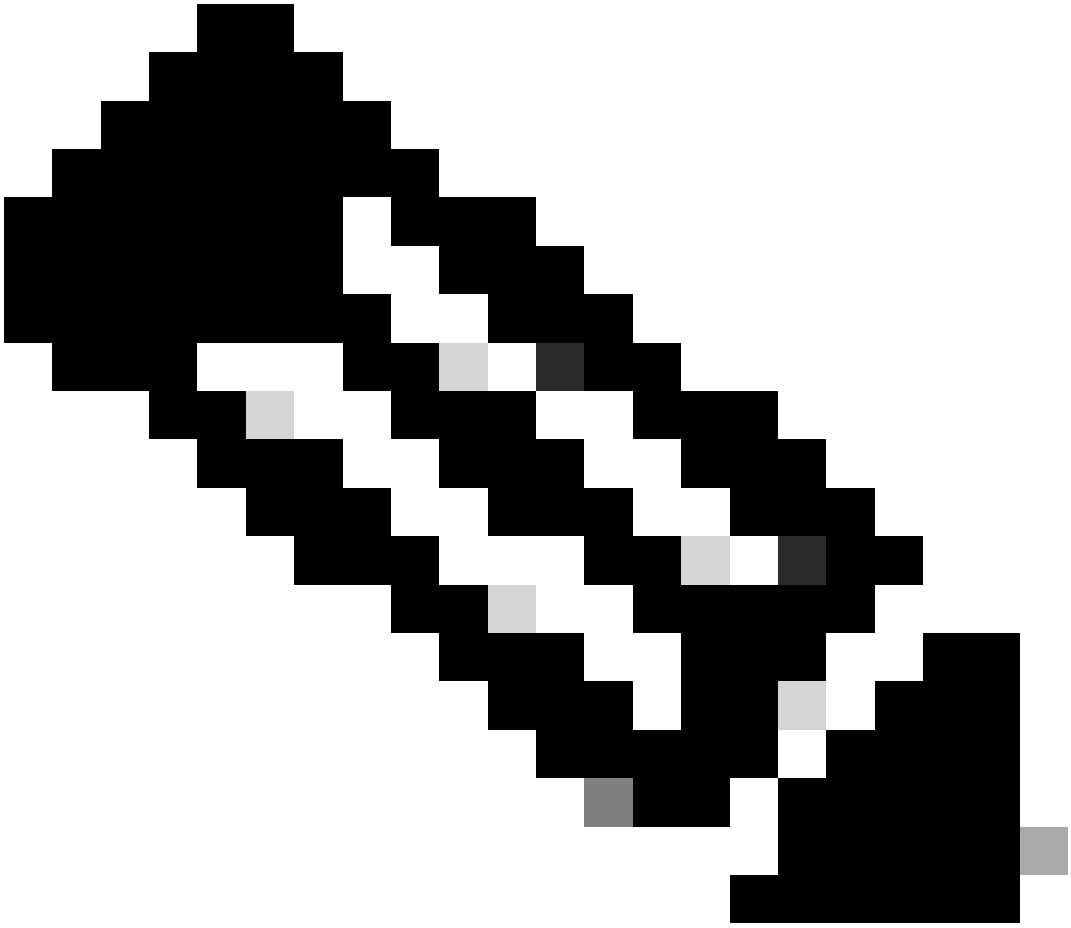
- RSA伺服器公共金鑰（用於幫助客戶端驗證伺服器）
- 伺服器的DH-公鑰（用於計算共用金鑰）
- HASH（驗證伺服器並證明伺服器已生成共用金鑰，因為金鑰是雜湊計算的一部分）



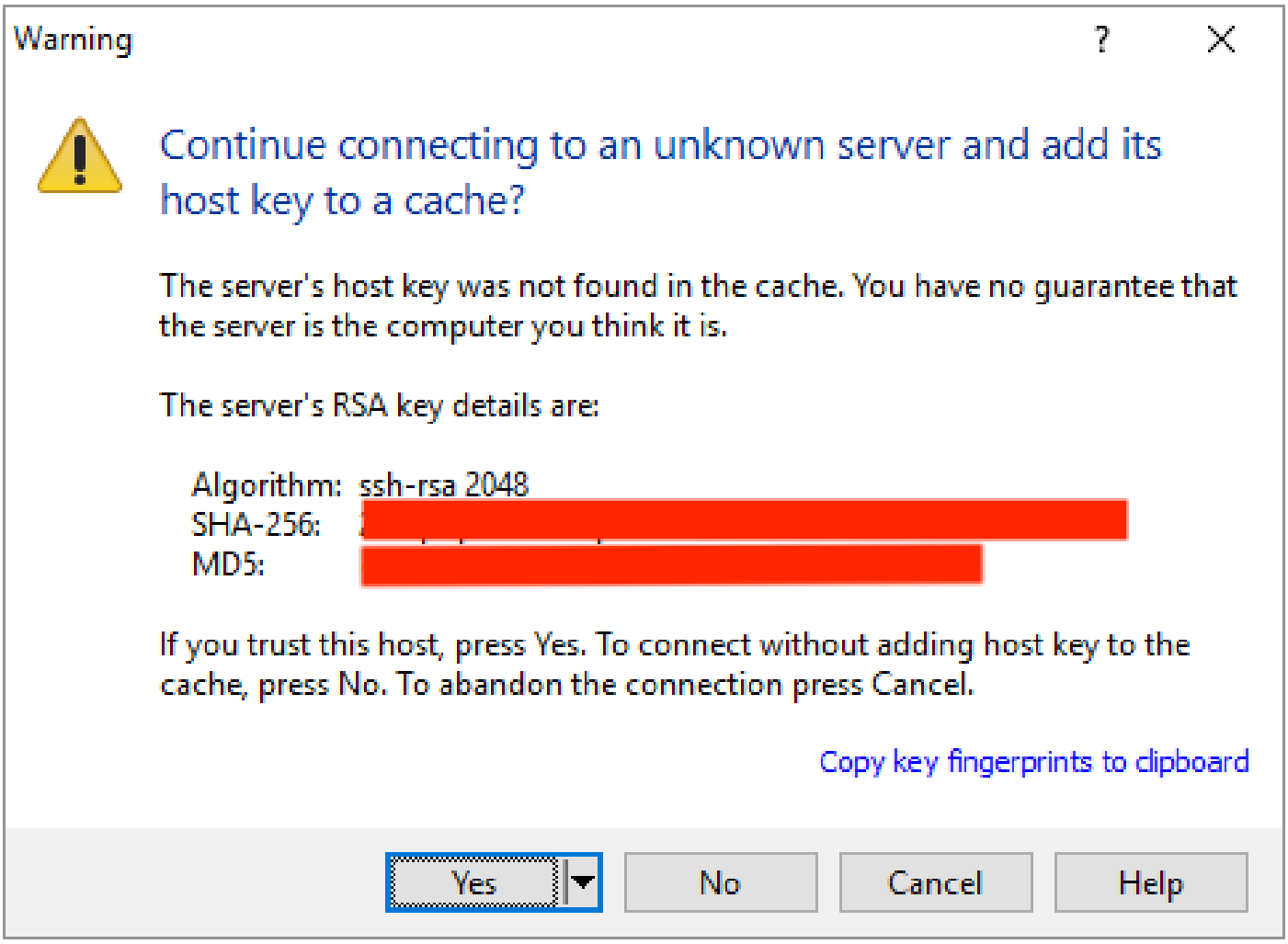
伺服器DH公開金鑰與Diffie-Hellman群組交換回覆

f.收到DH_Exchange_Reply後，客戶端以相同方式計算雜湊並將其與收到的雜湊進行比較，使用伺服器的RSA公鑰對其進行解密。

g.在解密收到的HASH之前，客戶端必須驗證伺服器的公鑰。此驗證透過憑證授權單位(CA)簽署的數位憑證完成。如果憑證不存在，則由使用者端決定是否接受伺服器的公開金鑰。



注意：當您首次以ssh方式進入不使用數位證書的裝置時，您可能會看到一個彈出窗口，要求您手動接受伺服器的公鑰。為避免每次連線時都看到此快顯視窗，您可以選擇將伺服器的主機金鑰新增至快取記憶體。

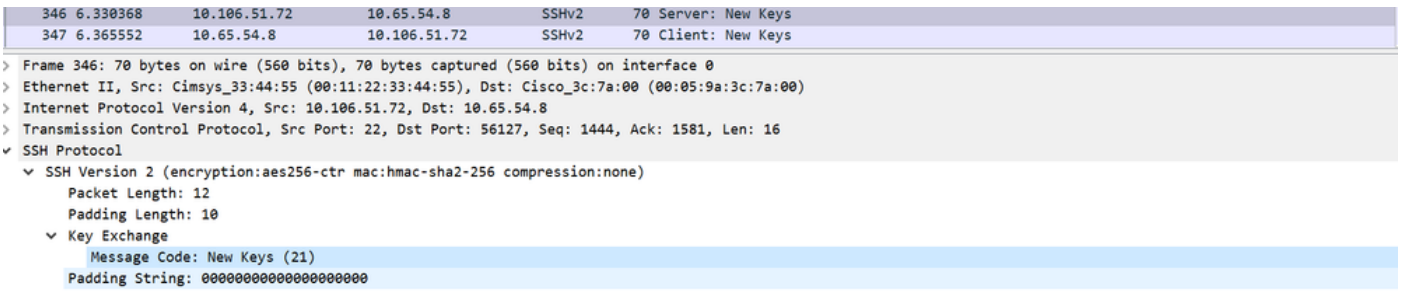


伺服器的RSA金鑰

4. 由於共用金鑰現在已生成，因此兩個終端都使用該金鑰來派生這些金鑰：

- 加密金鑰
- IV金鑰-這些是用作對稱演算法輸入的隨機數，用於增強安全性
- 完整性索引鍵

金鑰交換的結束由NEW KEYS' 消息交換發出訊號，它通知各方未來的所有消息都將使用這些新金鑰加密和保護。



使用者端與伺服器新金鑰

5. 最後一步是服務請求。客戶端向伺服器傳送SSH服務請求資料包以啟動使用者身份驗證。伺服器以SSH服務接受消息作出響應，提示客戶端登入。此交換透過已建立的安全通道進行。

相關資訊

- https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- https://datatracker.ietf.org/doc/html/rfc4253
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。