

# 瞭解安全殼層資料包交換

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[SSH協定](#)

[SSH交換](#)

[相關資訊](#)

---

## 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

```
323 5.946818 10.65.54.8 10.106.51.72 SSHv2 82 Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
> Frame 323: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
> Internet Protocol Version 4, Src: 10.65.54.8, Dst: 10.106.51.72
> Transmission Control Protocol, Src Port: 56127, Dst Port: 22, Seq: 1, Ack: 1, Len: 28
SSH Protocol
  Protocol: SSH-2.0-PuTTY_Release_0.76
```

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。

```
326 6.016955 10.106.51.72 10.65.54.8 SSHv2 73 Server: Protocol (SSH-2.0-Cisco-1.25)
> Frame 326: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: Cisco_3c:7a:00 (00:05:9a:3c:7a:00)
> Internet Protocol Version 4, Src: 10.106.51.72, Dst: 10.65.54.8
> Transmission Control Protocol, Src Port: 22, Dst Port: 56127, Seq: 1, Ack: 29, Len: 19
SSH Protocol
  Protocol: SSH-2.0-Cisco-1.25
```

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。

```
329 6.021990 10.65.54.8 10.106.51.72 SSHv2 238 Client: Key Exchange Init
> Frame 329: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface 0
> Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
> Internet Protocol Version 4, Src: 10.65.54.8, Dst: 10.106.51.72
> Transmission Control Protocol, Src Port: 56127, Dst Port: 22, Seq: 1101, Ack: 20, Len: 184
> [3 Reassembled TCP Segments (1256 bytes): #327(536), #328(536), #329(184)]
SSH Protocol
  SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 1252
    Padding Length: 11
    Key Exchange
      Message Code: Key Exchange Init (20)
      Algorithms
```

金鑰交換初始化

```

v Algorithms
  Cookie: 47a96215afc92003180b60342970a105
  kex_algorithms length: 315
  kex_algorithms string [truncated]: curve448-sha512,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,dif
  server_host_key_algorithms length: 123
  server_host_key_algorithms string: rsa-sha2-512,rsa-sha2-256,ssh-rsa,ssh-ed448,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-dss
  encryption_algorithms_client_to_server length: 189
  encryption_algorithms_client_to_server string: aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305
  encryption_algorithms_server_to_client length: 189
  encryption_algorithms_server_to_client string: aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305
  mac_algorithms_client_to_server length: 155
  mac_algorithms_client_to_server string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm
  mac_algorithms_server_to_client length: 155
  mac_algorithms_server_to_client string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm
  compression_algorithms_client_to_server length: 26
  compression_algorithms_client_to_server string: none,zlib,zlib@openssh.com
  compression_algorithms_server_to_client length: 26
  compression_algorithms_server_to_client string: none,zlib,zlib@openssh.com

```

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。

```

334 6.093250 10.106.51.72 10.65.54.8 SSHv2 366 Server: Key Exchange Init
> Frame 334: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface 0
> Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: Cisco_3c:7a:00 (00:05:9a:3c:7a:00)
> Internet Protocol Version 4, Src: 10.106.51.72, Dst: 10.65.54.8
> Transmission Control Protocol, Src Port: 22, Dst Port: 56127, Seq: 20, Ack: 1285, Len: 312
v SSH Protocol
  v SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 308
    Padding Length: 4
    v Key Exchange
      Message Code: Key Exchange Init (20)
      > Algorithms

```

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。

```

337 6.201114 10.65.54.8 10.106.51.72 SSHv2 326 Client: Diffie-Hellman Group Exchange Init
> Frame 337: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface 0
> Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
> Internet Protocol Version 4, Src: 10.65.54.8, Dst: 10.106.51.72
> Transmission Control Protocol, Src Port: 56127, Dst Port: 22, Seq: 1309, Ack: 612, Len: 272
v SSH Protocol
  v SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 268
    Padding Length: 6
    v Key Exchange
      Message Code: Diffie-Hellman Group Exchange Init (32)
      Multi Precision Integer Length: 256
      DH client e: 1405ab00ff368031363467ad6653967d5a64eac4734e5dc6
      Padding String: 5c81f2cffc95

```

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：

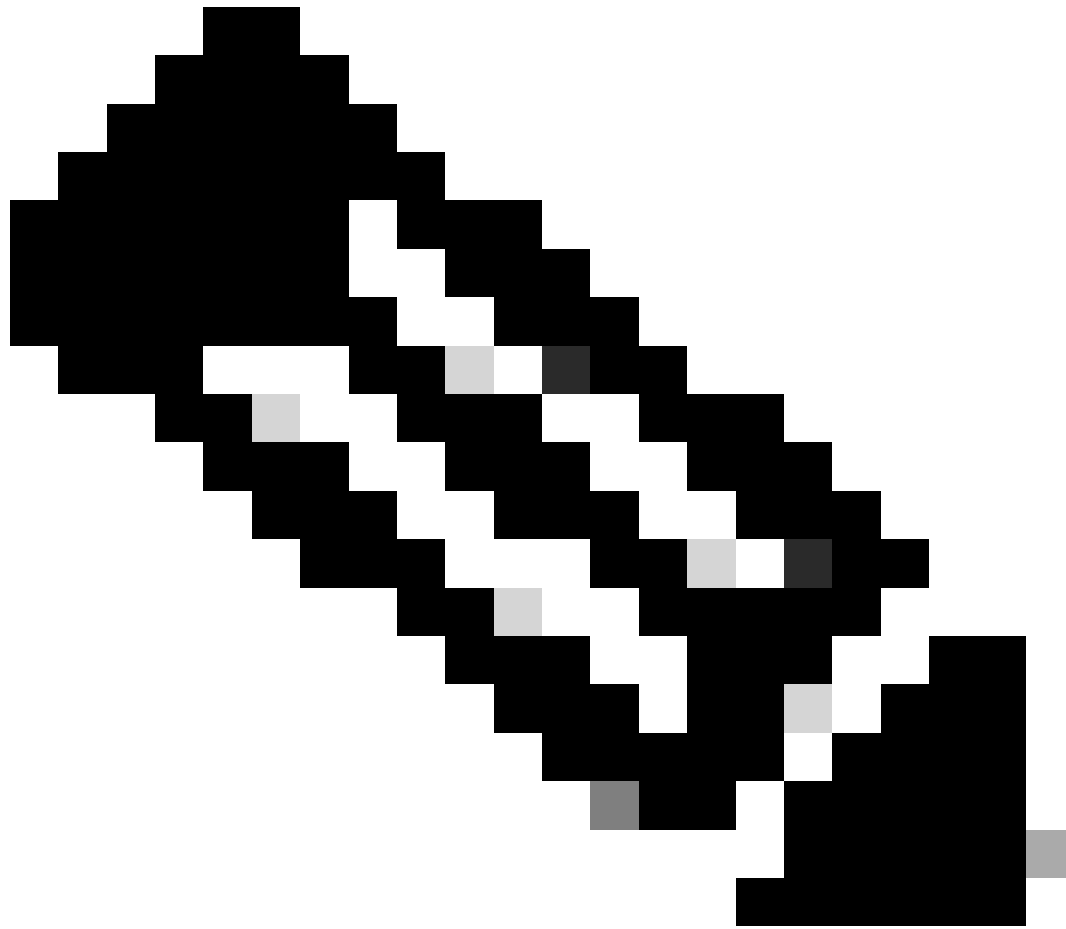
- RSA伺服器公共金鑰 (用於幫助客戶端驗證伺服器)
- 伺服器的DH-公鑰 (用於計算共用金鑰)
- HASH (驗證伺服器並證明伺服器已生成共用金鑰，因為金鑰是雜湊計算的一部分)

```
343 6.330017 10.106.51.72 10.65.54.8 SSHv2 350 Server: Diffie-Hellman Group Exchange Reply
Internet Protocol Version 4, Src: 10.106.51.72, Dst: 10.65.54.8
Transmission Control Protocol, Src Port: 22, Dst Port: 56127, Seq: 1148, Ack: 1581, Len: 296
[2 Reassembled TCP Segments (832 bytes): #342(536), #343(296)]
SSH Protocol
  SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 828
    Padding Length: 8
    Key Exchange
      Message Code: Diffie-Hellman Group Exchange Reply (33)
      KEX host key (type: ssh-rsa)
        Host key length: 279
        Host key type length: 7
        Host key type: ssh-rsa
        Multi Precision Integer Length: 3
        RSA public exponent (e): 010001
        Multi Precision Integer Length: 257
        RSA modulus (N): 0098c7d23c9ababd730f07b5c2aee1e4e51bac67970aa5af...
        Multi Precision Integer Length: 256
        DH server f: 3a17a0995531f12d629a48ab6f25715bc181ea3deb6c6793...
        KEX H signature length: 271
        KEX H signature: 000000077373682d72736100000100691d2c896761bc7481...
        Padding String: 0000000000000000
```

伺服器DH公開金鑰與Diffie-Hellman群組交換回覆

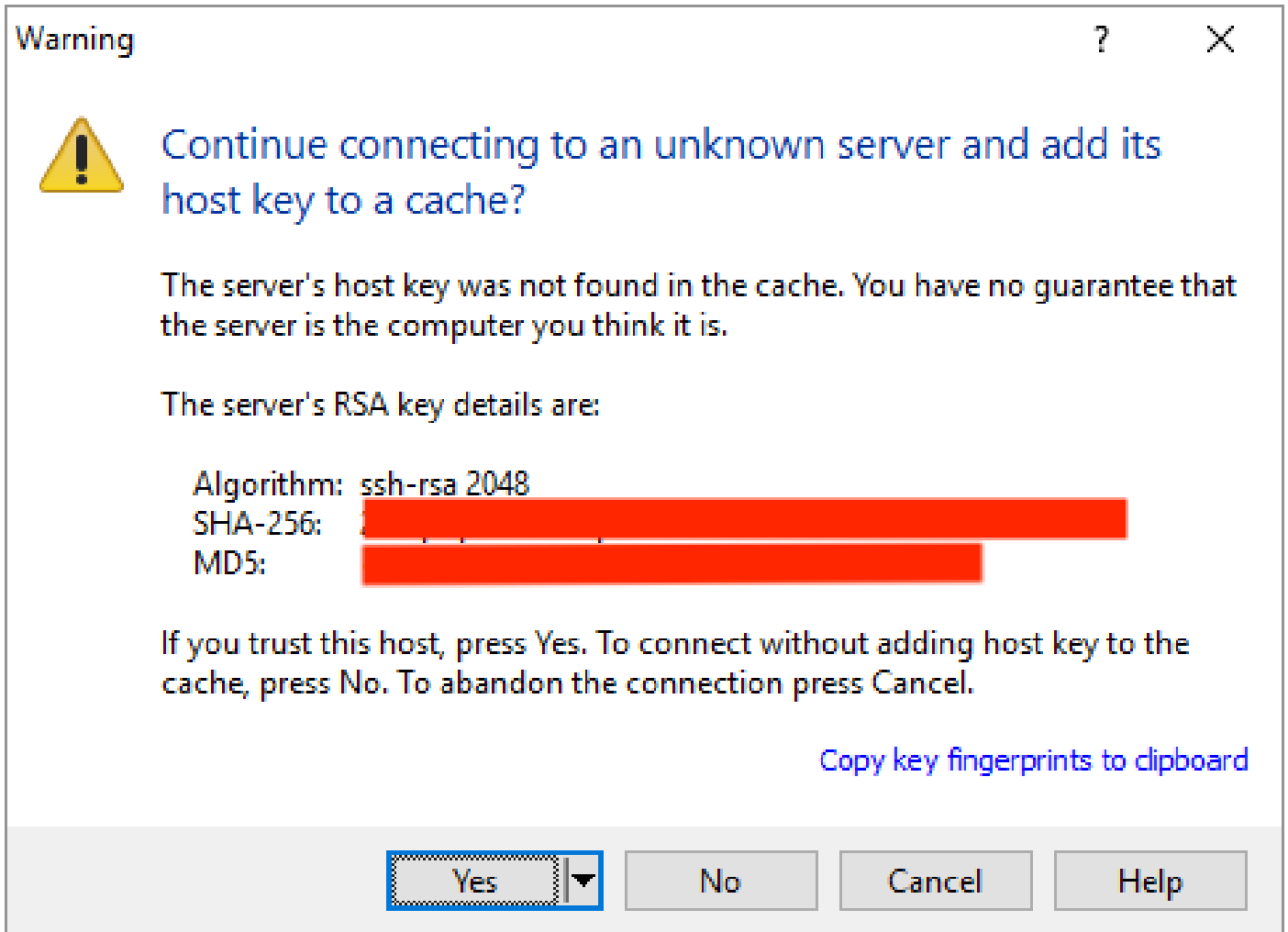
f. 收到DH\_Exchange\_Reply後，客戶端以相同方式計算雜湊並將其與收到的雜湊進行比較，使用伺服器的RSA公鑰對其進行解密。

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。

346	6.330368	10.106.51.72	10.65.54.8	SSHv2	70 Server: New Keys
347	6.365552	10.65.54.8	10.106.51.72	SSHv2	70 Client: New Keys

> Frame 346: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
> Ethernet II, Src: Cimsys\_33:44:55 (00:11:22:33:44:55), Dst: Cisco\_3c:7a:00 (00:05:9a:3c:7a:00)  
> Internet Protocol Version 4, Src: 10.106.51.72, Dst: 10.65.54.8  
> Transmission Control Protocol, Src Port: 22, Dst Port: 56127, Seq: 1444, Ack: 1581, Len: 16  
✓ SSH Protocol  
  ✓ SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)  
    Packet Length: 12  
    Padding Length: 10  
    ✓ Key Exchange  
      Message Code: New Keys (21)  
      Padding String: 00000000000000000000

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）。