فهم تبادل حزم Secure Shell

المحتويات

المقدمة

يصف هذا المستند تبادل مستوى الحزمة أثناء تفاوض طبقة الأمان (SSH).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بمفاهيم الأمان الأساسية:

- المصادقة
- السرية
- نزاهة
- أساليب تبادل المفاتيح

المكونات المستخدمة

لا يقيد هذا وثيقة إلى خاص جهاز صيغة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي).

بروتوكول SSH

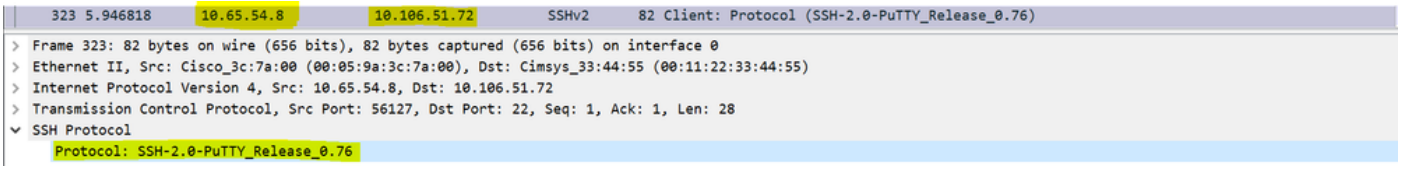
بروتوكول SSH هو طريقة لتأمين تسجيل الدخول عن بعد من جهاز كمبيوتر إلى آخر. تستند تطبيقات SSH إلى بنية خادم عميل، لتوصيل مثيل عميل SSH بخادم SSH.

تبادل SSH

1. تسمى الخطوة الأولى من بروتوكول طبقة الأمان (SSH) Identification String Exchange.

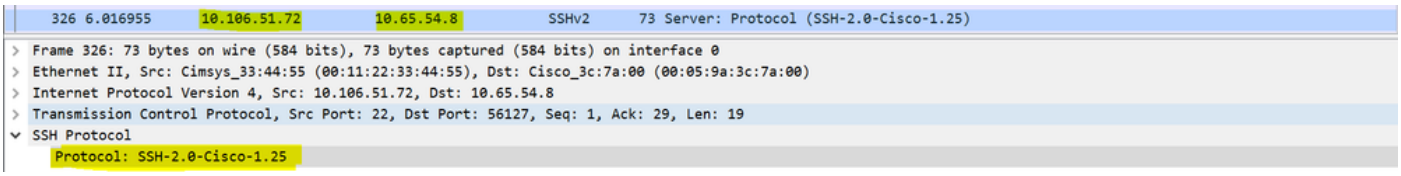
أ. يقوم العميل بإنشاء حزمة وإرسالها إلى الخادم الذي يحتوي على:

- إصدار بروتوكول SSH
- إصدار البرامج



إصدار بروتوكول العميل هو SSH2.0 وإصدار البرنامج هو PuTTY_0.76.

ب. يستجيب الخادم باستخدام سلسلة التعريف الخاصة به، بما في ذلك إصدار بروتوكول SSH وإصدار البرنامج.

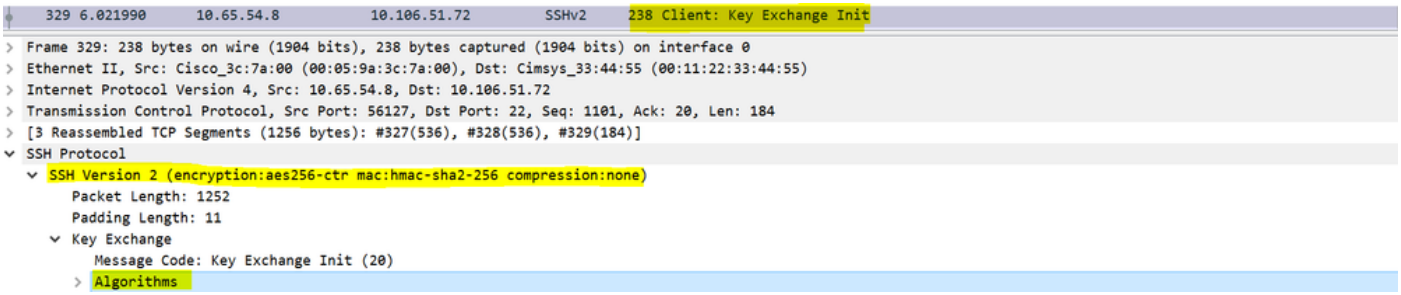


إصدار بروتوكول الخادم هو SSH2.0 وإصدار البرنامج هو Cisco1.25

2. الخطوة التالية هي **Algorithm Negotiation**. في هذه الخطوة، حيث يقوم كل من العميل والخادم بالتفاوض حول هذه الخوارزميات:

- تبادل المفاتيح
- تشفير
- HMAC (رمز مصادقة الرسائل المستندة إلى التجزئة)
- ضغط

1. يرسل العميل رسالة Key Exchange Init إلى الخادم، ويحدد الخوارزميات التي يدعمها. يتم سرد الخوارزميات حسب الأفضلية.



مفتاح Init

```
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
```

الخوارزميات المدعومة من قبل العميل

ب. يستجيب الخادم برسالة Key Exchange Init الخاصة به، ويسرد الخوارزميات التي يدعمها.

ج - بما أن هاتين الرسالتين تتبادلان في آن واحد، فإن كل الطرفين يقارن قوائمهما الخوارزمية. إذا كان هناك تطابق في الخوارزميات التي يدعمها كل الجانبين، فانها تتقدم إلى الخطوة التالية. وفي حالة عدم وجود تطابق تام، يحدد الخادم الخوارزمية الأولى من قائمة العميل التي يدعمها أيضا.

د. إذا تعذر على العميل والخادم الموافقة على خوارزمية مشتركة، فسيفشل تبادل المفاتيح.

```
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
SSH Protocol
  SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 308
    Padding Length: 4
  Key Exchange
    Message Code: Key Exchange Init (20)
    Algorithms
```

Server Key Exchange Init

3. بعد ذلك، يدخل كل الجانبين **Key Exchange**المرحلة لإنشاء سر مشترك باستخدام تبادل مفاتح DH ومصادقة الخادم:

أ. يقوم العميل بإنشاء زوج مفاتيح،Public and Privateوإرسال المفتاح العام DH في حزمة Init لتبادل مجموعة DH. يستخدم زوج المفاتيح هذا لحساب المفتاح السري.

```
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
SSH Protocol
  SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 268
    Padding Length: 6
  Key Exchange
    Message Code: Diffie-Hellman Group Exchange Init (32)
    Multi Precision Integer Length: 256
    DH client e: 1405ab00ff368031363467ad6653967d5a64eac4734e5dc6…
    Padding String: 5c81f2cffc95
```

مفتاح DH العام العميل ومدخل تبادل مجموعة Diffie-hellman

ب. يقوم الخادم بإنشاء زوج مفاتيح خاص بهPublic and Private. وهو يستخدم المفتاح العام

للعميل وزوج مفتاحه الخاص به لحساب السر المشترك.

ج. يقوم الخادم أيضا بحساب تجزئة Exchange باستخدام هذه المدخلات:

- سلسلة تعريف العملاء
- سلسلة تعريف الخادم
- حمولة Kexinit العميل
- حمولة Server KEXINIT
- الخوادم عامة المفتاح من مفاتيح المضيف (زوج مفاتيح RSA)
- مفتاح DH العام للعملاء
- المفتاح العام للخوادم DH
- مفتاح سري مشترك

د. بعد حساب التجزئة، يقوم الخادم بتوقيعه باستخدام مفتاح RSA الخاص به.

ه. يقوم الخادم بإنشاء رسالة DH_EXCHANGE_REPLY تتضمن:

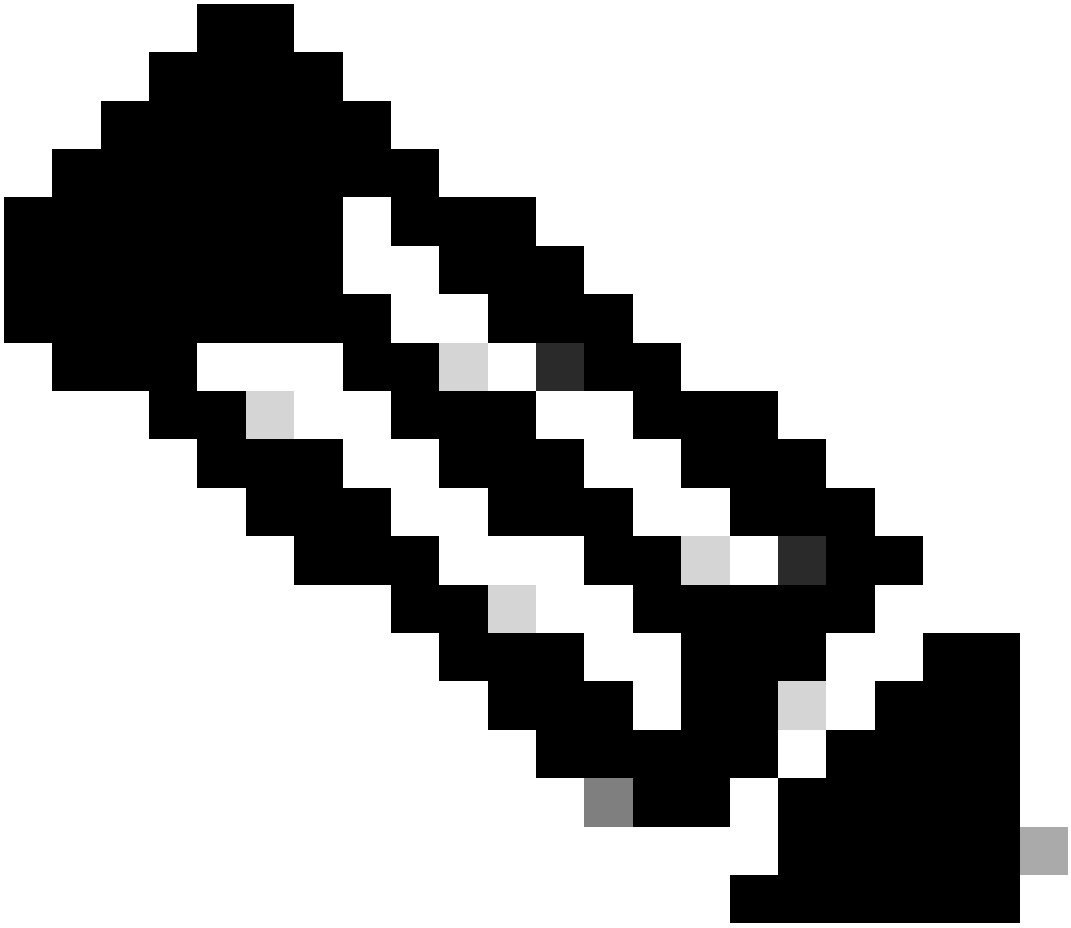
- مفتاح RSA-العام للخادم (لمساعدة العميل على مصادقة الخادم)
- مفتاح DH العام للخادم (لحساب السر المشترك)
- تجزئة (لمصادقة الخادم وإثبات أن الخادم قام بإنشاء السر المشترك، حيث أن المفتاح السري هو جزء من عملية حساب التجزئة)

```
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
```

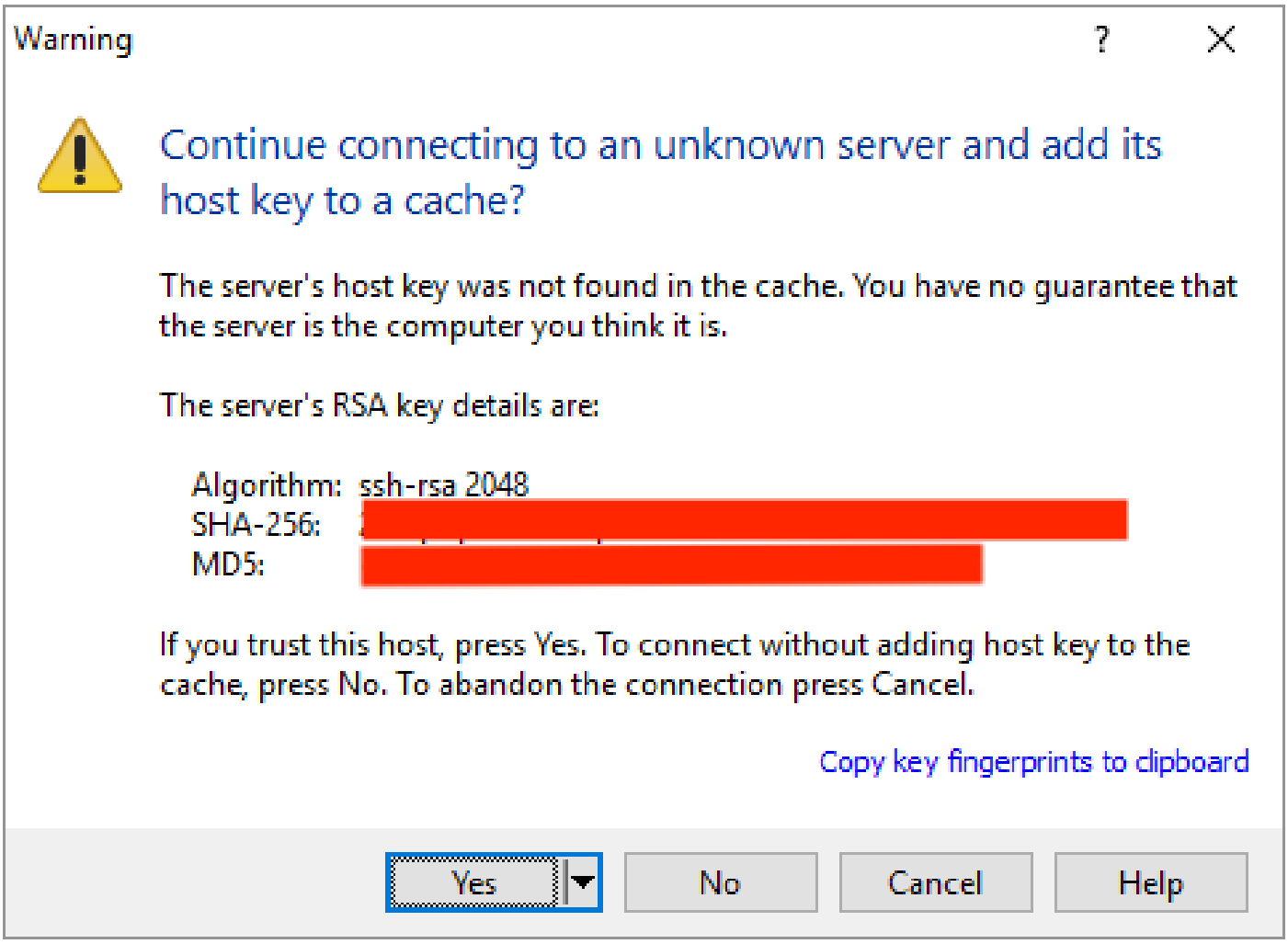
الرد على تبادل مجموعة Diffie-hellman للمفتاح العام للخادم DH

و. بعد تلقي DH_EXCHANGE_REPLY، يقوم العميل بحساب التجزئة بنفس الطريقة ويقارنها بالتجزئة المستلمة، مع فك تشفيرها باستخدام مفتاح RSA العام الخاص بالخادم.

g. قبل فك تشفير التجزئة المستلمة، يجب على العميل التحقق من المفتاح العام للخادم. يتم إجراء هذا التحقق من خلال شهادة رقمية موقعة من قبل مرجع مصدق (CA). في حالة عدم وجود الشهادة، يعود للعميل تقرير قبول المفتاح العام للخادم.



ملاحظة: عند إدخال بروتوكول SSH لأول مرة في جهاز لا يستخدم شهادة رقمية، قد تواجه أحد الإطارات المنبثقة يطلب منك قبول المفتاح العام للخادم يدوياً. لتجنب رؤية هذا الإطار المنبثق في كل مرة تقوم فيها بالاتصال، يمكنك إختيار إضافة مفتاح مضيف الخادم إلى ذاكرة التخزين المؤقت.



مفتاح RSA للخادم

4. بما أن السر المشترك يتم الآن توليده، كلتاهما تستخدمون لاستخلاص هذه المفاتيح :

- مفاتيح التشفير
- IV Keys - هذه أرقام عشوائية تستخدم كمدخلات لخوارزميات متماثلة لتحسين الأمان
- مفاتيح التكامل

يتم الإشارة إلى نهاية تبادل المفاتيح من خلال تبادل NEW KEYS' الرسالة التي تعلم كل طرف بأن جميع الرسائل المستقبلية سيتم تشفيرها وحمايتها باستخدام هذه المفاتيح الجديدة .

```
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
v SSH Protocol
  v SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
      Packet Length: 12
      Padding Length: 10
    v Key Exchange
        Message Code: New Keys (21)
      Padding String: 0000000000000000000
```

العميل والمفاتيح الجديدة للخادم

5. الخطوة الأخيرة هي طلب الخدمة. يرسل العميل حزمة طلب خدمة SSH إلى الخادم لبدء

مصادقة المستخدم. يستجيب الخادم برسالة قبول خدمة SSH، مما يتطلب من العميل تسجيل الدخول. يحدث هذا التبادل عبر القناة الآمنة التي تم إنشاؤها.

معلومات ذات صلة

- https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- https://datatracker.ietf.org/doc/html/rfc4253
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).