Informationen zu Secure Shell Packet Exchange

Inhalt

Einleitung

Dieses Dokument beschreibt den Austausch auf Paketebene während der Secure Shell (SSH)-Aushandlung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse folgender grundlegender Sicherheitskonzepte verfügen:

- Authentifizierung
- Vertraulichkeit
- Integrität
- Wichtige Methoden für den Austausch

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration.

SSH-Protokoll

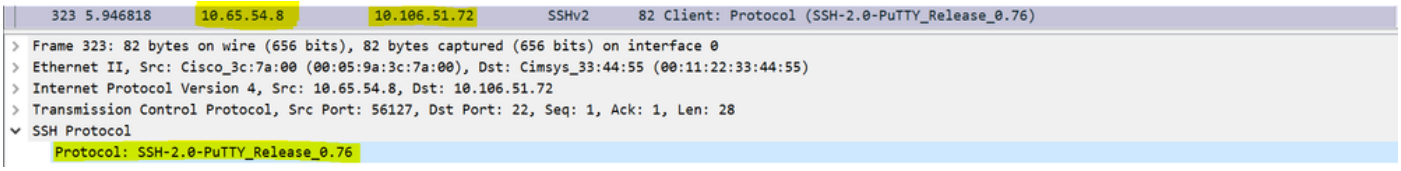
Das SSH-Protokoll ist eine Methode zur sicheren Remote-Anmeldung von einem Computer zum anderen. SSH-Anwendungen basieren auf einer Client-Server-Architektur, die eine SSH-Client-Instanz mit einem SSH-Server verbindet.

SSH-Austausch

1. Der erste Schritt von SSH wird als Identification String Exchange.

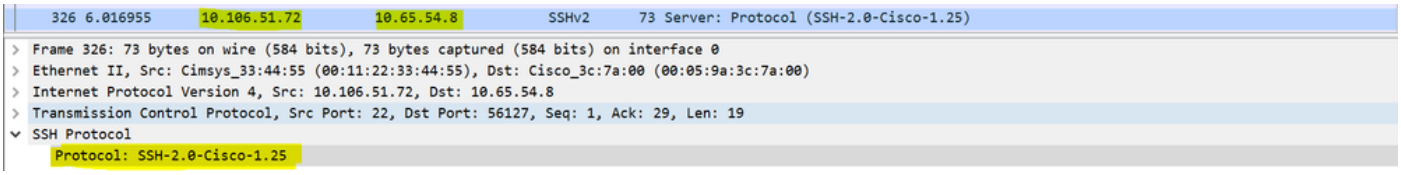
a. Der Client erstellt ein Paket und sendet es an den Server, der Folgendes enthält:

- Version des SSH-Protokolls
- Software-Version



Die Clientprotokollversion ist SSH2.0, und die Softwareversion ist Putty_0.76.

b. Der Server reagiert mit seinem eigenen Identification String Exchange, einschließlich der Version des SSH-Protokolls und der Softwareversion.

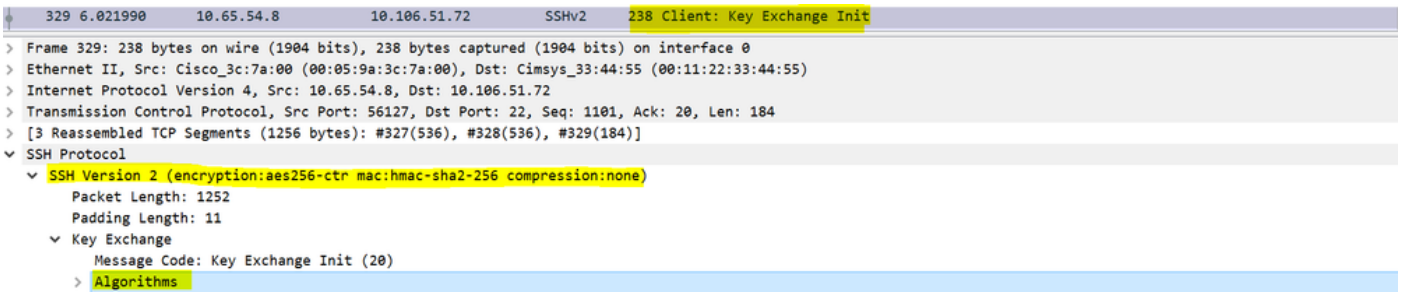


Die Protokollversion des Servers ist SSH2.0, die Softwareversion ist Cisco1.25.

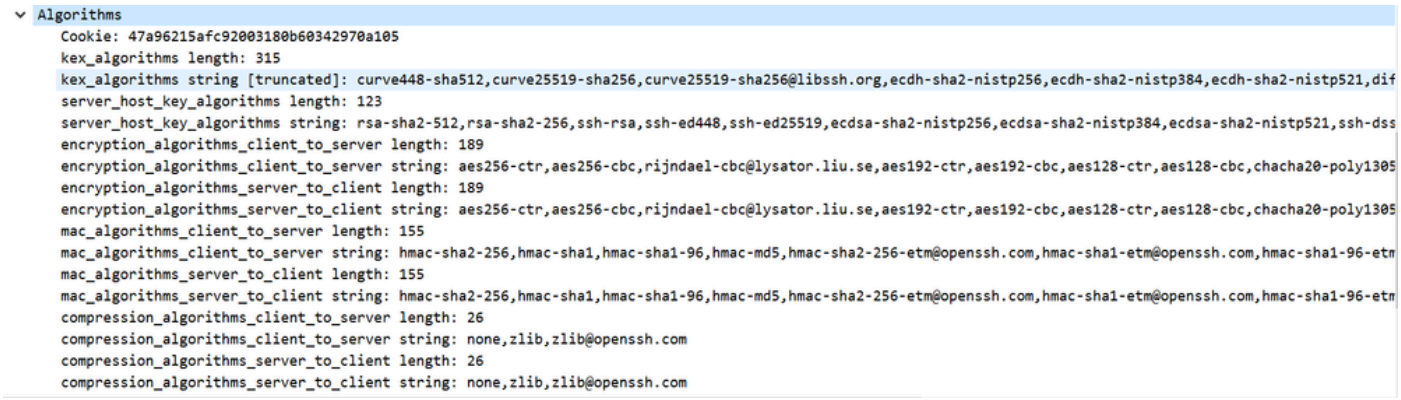
2. Der nächste Schritt ist **Algorithm Negotiation**. In diesem Schritt handeln sowohl Client als auch Server diese Algorithmen aus:

- Schlüsselaustausch
- Verschlüsselung
- HMAC (Hash-based Message Authentication Code)
- Komprimierung

1. Der Client sendet eine Key Exchange Init-Nachricht an den Server, in der er die unterstützten Algorithmen angibt. Die Algorithmen werden nach Präferenz geordnet aufgelistet.



Schlüsselaustausch-Initialisierung

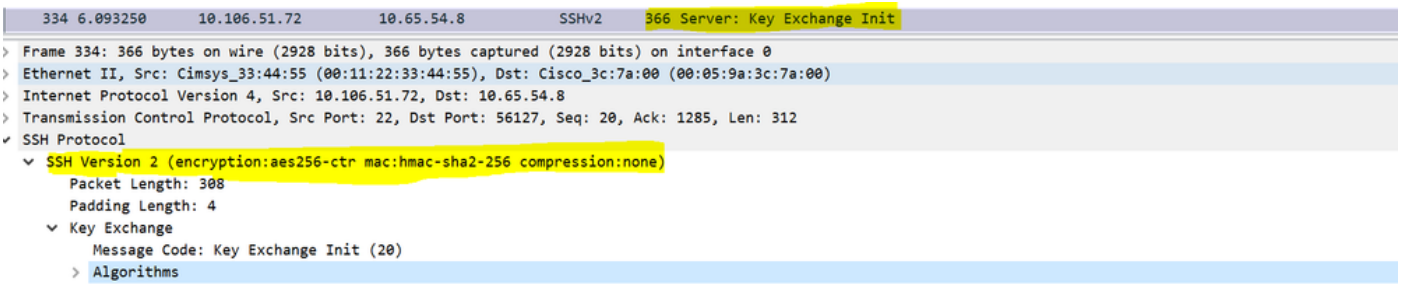


Vom Client unterstützte Algorithmen

b. Der Server antwortet mit einer eigenen Nachricht zur Initialisierung von Schlüsselaustausch, in der die unterstützten Algorithmen aufgeführt sind.

c. Da diese Nachrichten gleichzeitig ausgetauscht werden, vergleichen beide Parteien ihre Algorithmus-Listen. Wenn die von beiden Seiten unterstützten Algorithmen übereinstimmen, fahren sie mit dem nächsten Schritt fort. Wenn keine exakte Übereinstimmung vorliegt, wählt der Server den ersten Algorithmus aus der Liste des Clients aus, den er ebenfalls unterstützt.

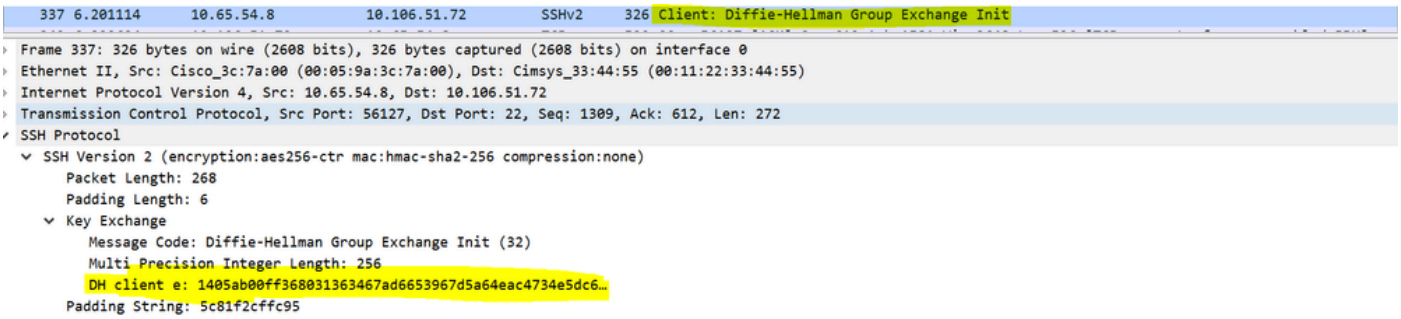
d. Wenn sich Client und Server nicht auf einen gemeinsamen Algorithmus einigen können, schlägt der Schlüsselaustausch fehl.



Serverschlüsselaustausch-Initialisierung

3. Danach gehen beide Seiten in die **Key Exchange**Phase, um mithilfe des DH-Schlüsselaustauschs einen gemeinsamen geheimen Schlüssel zu generieren und den Server zu authentifizieren:

a. Der Client generiert ein Tastenpaar und Public and Privatesendet den öffentlichen DH-Schlüssel im DH Group Exchange-Init-Paket. Dieses Schlüsselpaar wird für die Berechnung des geheimen Schlüssels verwendet.



Client DH Public Key & Diffie-Hellman Group Exchange Init

b. Der Server generiert ein eigenesPublic and PrivateSchlüsselpaar. Er verwendet den öffentlichen Schlüssel des Clients und sein eigenes Schlüsselpaar, um den gemeinsamen geheimen Schlüssel zu berechnen.

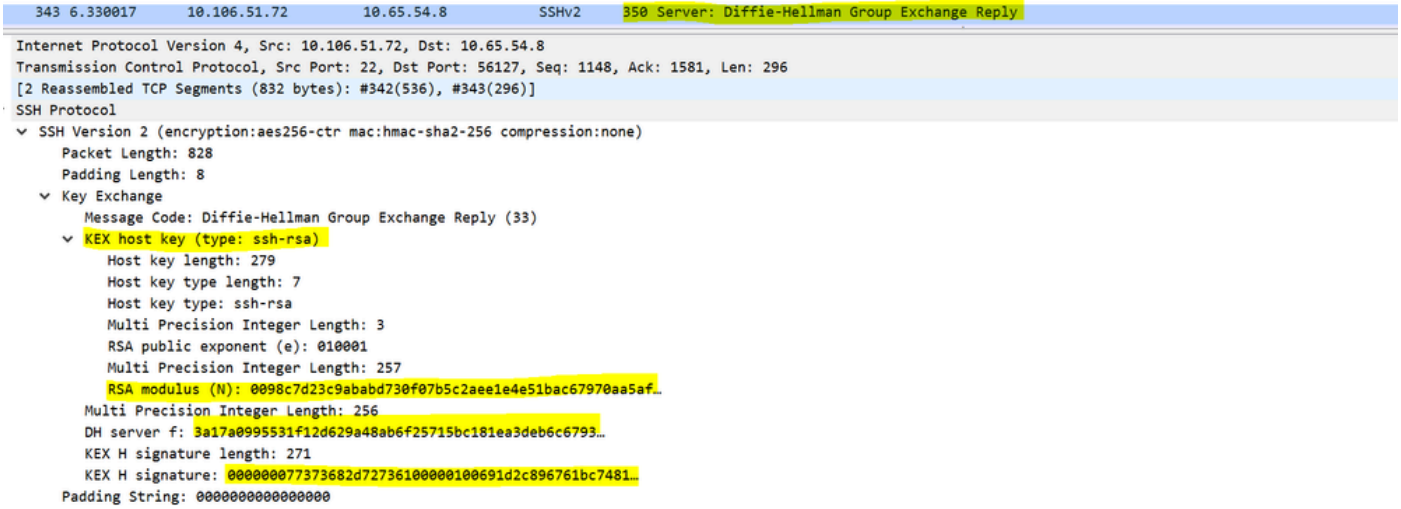
c. Der Server berechnet auch einen Exchange-Hash mit folgenden Eingaben:

- Client-Identifizierungszeichenfolge
- Server-Identifizierungszeichenfolge
- Nutzlast des Kunden KEXINIT
- Nutzlast des Servers KEXINIT
- Server Öffentlicher Schlüssel von Host-Schlüsseln (RSA-Schlüsselpaar)
- Öffentlicher Client-DH-Schlüssel
- Öffentlicher Serverschlüssel
- Gemeinsamer geheimer Schlüssel

d. Nach dem Computing des Hash signiert der Server ihn mit seinem privaten RSA-Schlüssel.

e. Der Server erstellt eine Nachricht mit dem Namen DH_Exchange_Reply, die Folgendes enthält:

- RSA - Öffentlicher Serverschlüssel (zur Unterstützung des Clients bei der Serverauthentifizierung)
- DH-Öffentlicher Schlüssel des Servers (zur Berechnung des gemeinsamen geheimen Schlüssels)
- HASH (zur Authentifizierung des Servers und zum Nachweis, dass der Server den gemeinsamen geheimen Schlüssel generiert hat, da der geheime Schlüssel Teil der Hash-Berechnung ist)

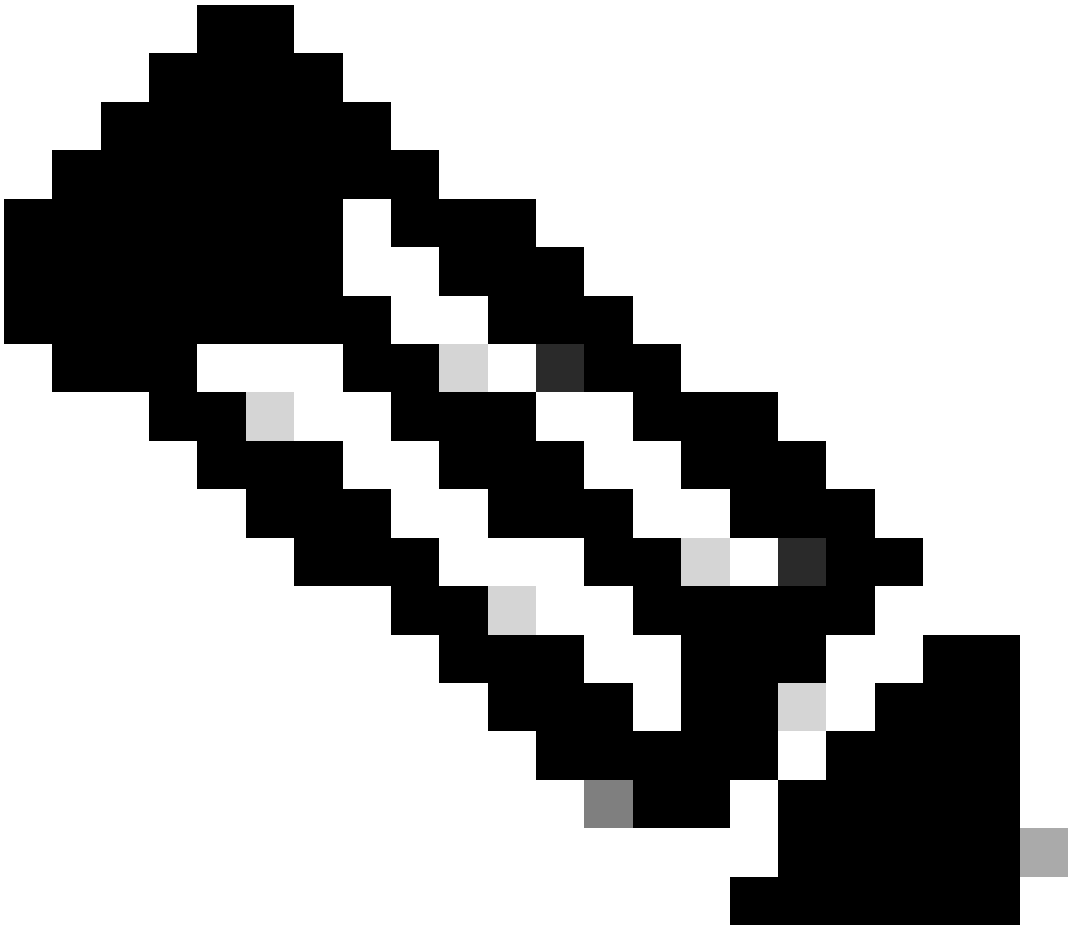


Server DH Public Key & Diffie-Hellman Group Exchange-Antwort

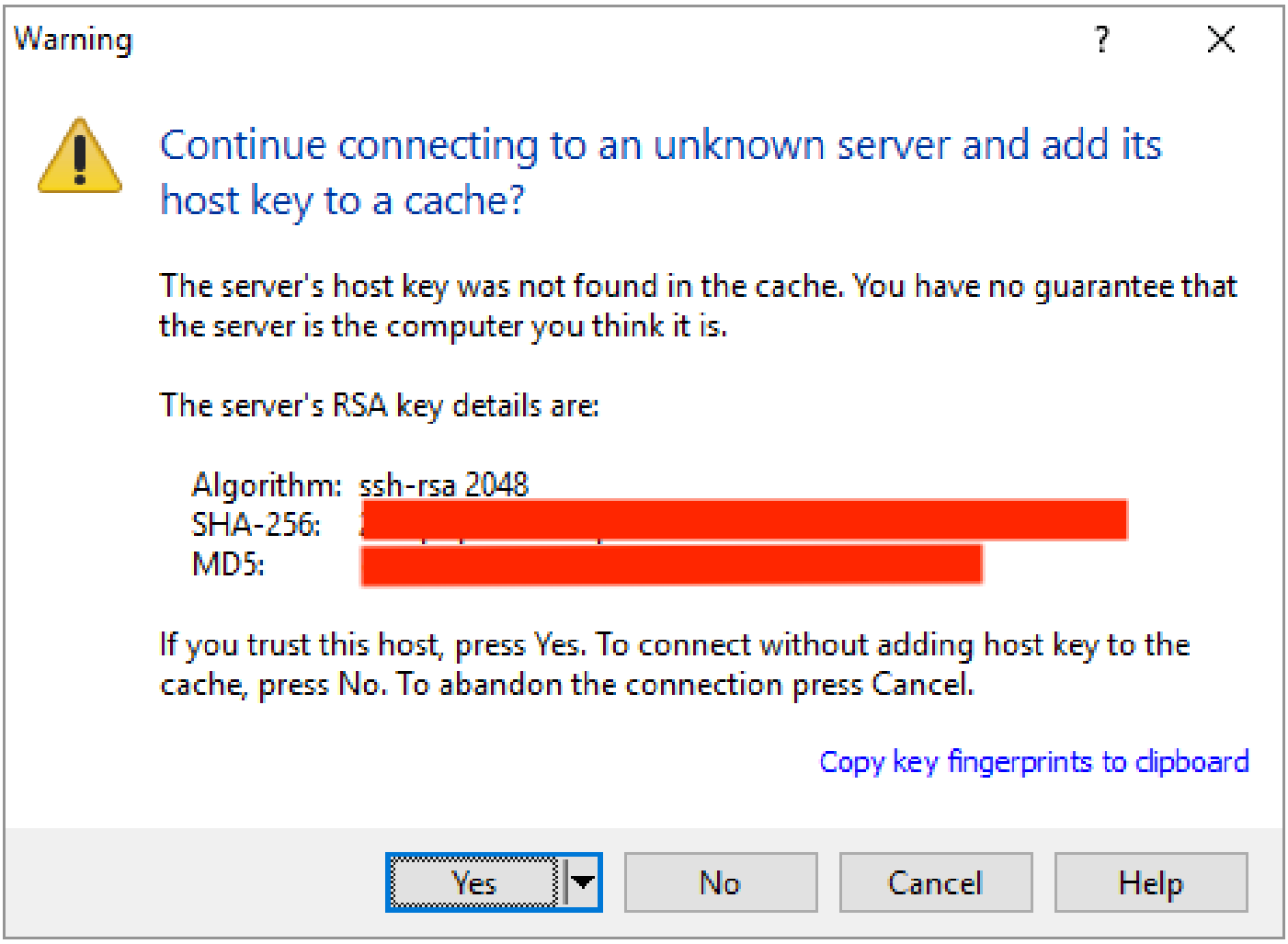
f. Nach dem Empfang von DH_Exchange_Reply berechnet der Client den Hash auf die gleiche Weise und vergleicht ihn mit dem empfangenen Hash, wobei er ihn mit dem öffentlichen RSA-Schlüssel des Servers entschlüsselt.

g. Vor der Entschlüsselung des empfangenen HASH muss der Client den öffentlichen Schlüssel

des Servers überprüfen. Diese Verifizierung erfolgt über ein digitales Zertifikat, das von einer Zertifizierungsstelle (Certificate Authority, CA) signiert wird. Wenn das Zertifikat nicht vorhanden ist, muss der Client entscheiden, ob er den öffentlichen Schlüssel des Servers akzeptiert.



Hinweis: Wenn Sie SSH zum ersten Mal in ein Gerät einbinden, das kein digitales Zertifikat verwendet, werden Sie möglicherweise in einem Popup-Fenster aufgefordert, den öffentlichen Schlüssel des Servers manuell zu akzeptieren. Um zu vermeiden, dass dieses Popup bei jeder Verbindung angezeigt wird, können Sie den Host-Schlüssel des Servers Ihrem Cache hinzufügen.

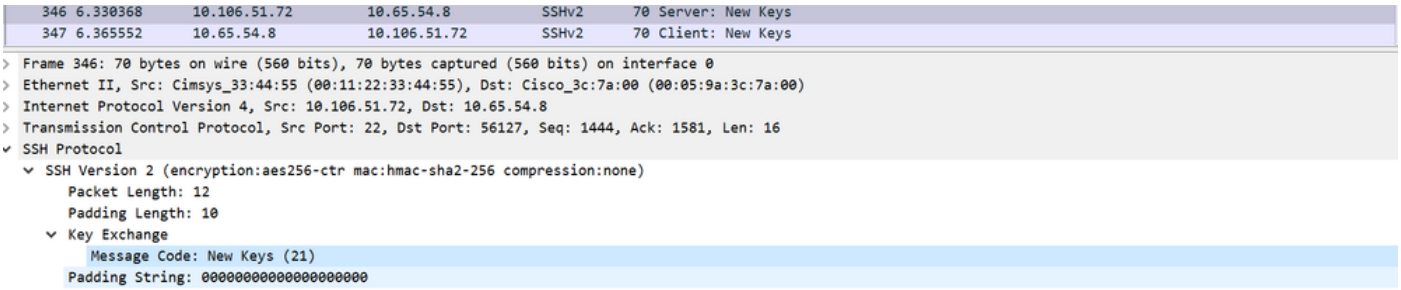


RSA-Schlüssel des Servers

4. Da der gemeinsame geheime Schlüssel jetzt generiert wird, verwenden beide Endgeräte ihn, um folgende Schlüssel abzuleiten:

- Verschlüsselungsschlüssel
- IV-Schlüssel - Dies sind Zufallszahlen, die als Eingabe für symmetrische Algorithmen verwendet werden, um die Sicherheit zu erhöhen
- Integritätsschlüssel

Das Ende des Schlüsselaustauschs wird durch den Austausch der NEW KEYS' Nachricht signalisiert, die jeden Teilnehmer darüber informiert, dass alle zukünftigen Nachrichten mit diesen neuen Schlüsseln verschlüsselt und geschützt werden.



Neue Schlüssel für Client und Server

5. Der letzte Schritt ist die Serviceanfrage. Der Client sendet ein SSH-Dienstanforderungspaket an den Server, um die Benutzerauthentifizierung zu initiieren. Der Server antwortet mit einer SSH Service Accept-Nachricht, in der der Client zur Anmeldung aufgefordert wird. Dieser Austausch erfolgt über den eingerichteten sicheren Kanal.

Zugehörige Informationen

- https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- https://datatracker.ietf.org/doc/html/rfc4253
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.