Secure Shell-pakketuitwisseling begrijpen

Inhoud

Inleiding

Dit document beschrijft de uitwisseling op pakketniveau tijdens SSH-onderhandeling (Secure Shell).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van basisbeveiligingsconcepten:

- Verificatie
- Vertrouwelijkheid
- Integriteit
- Belangrijkste uitwisselingsmethoden

Gebruikte componenten

Dit document is niet beperkt tot specifieke hardwareversie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie.

SSH-protocol

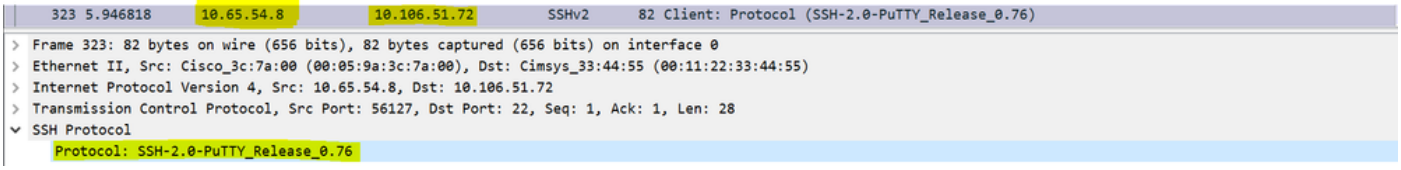
Het SSH-protocol is een methode voor beveiligde externe aanmelding van de ene computer naar de andere. SSH-toepassingen zijn gebaseerd op een client-serverarchitectuur, waarbij een SSH-client wordt verbonden met een SSH-server.

SSH exchange

1. De eerste stap van SSH wordt genoemd Identification String Exchange.

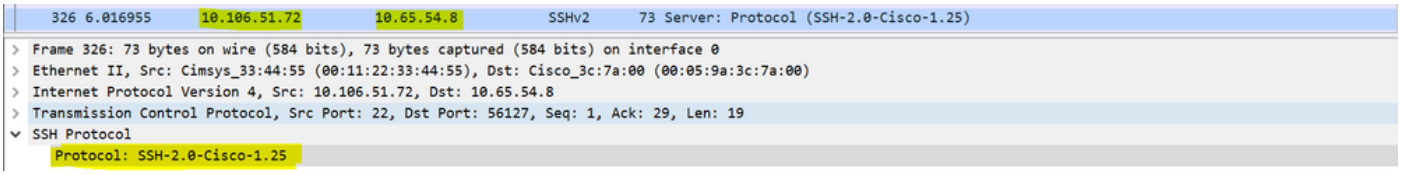
a. De client maakt een pakket en stuurt het naar de server met daarin:

- SSH-protocolversie
- Softwareversie



De versie van het clientprotocol is SSH2.0 en de softwareversie is Putty_0.76.

b. De server reageert met zijn eigen Identification String Exchange, inclusief zijn SSH-protocolversie en softwareversie.

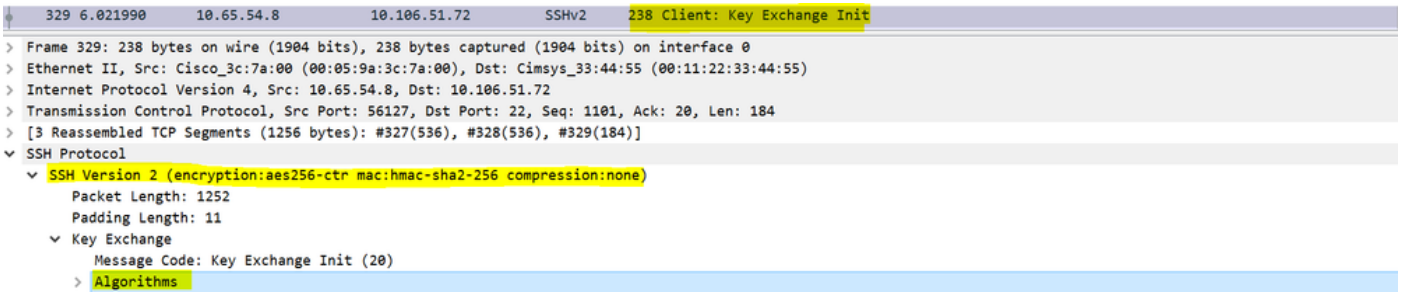


De protocolversie van de server is SSH2.0 en de softwareversie is Cisco1.25

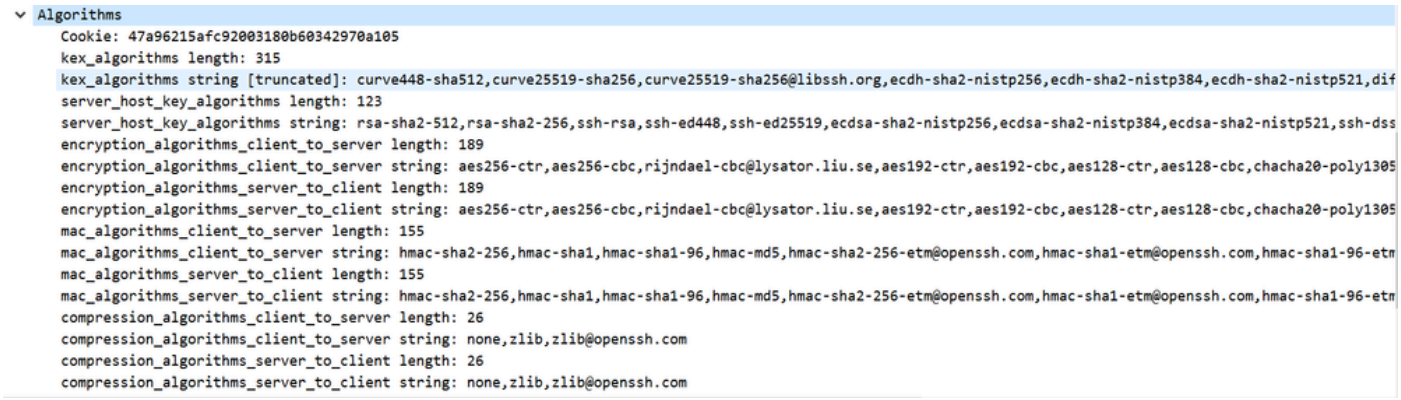
2. Volgende stap is **Algorithm Negotiation**. In deze stap onderhandelen zowel client als server over deze algoritmen:

- Keyexchange
- Versleuteling
- HMAC (op hash gebaseerde berichtverificatiecode)
- Compressie

1. De client stuurt een Key Exchange Init-bericht naar de server, met de algoritmen die worden ondersteund. De algoritmen worden gerangschikt in volgorde van voorkeur.



Key Exchange Init

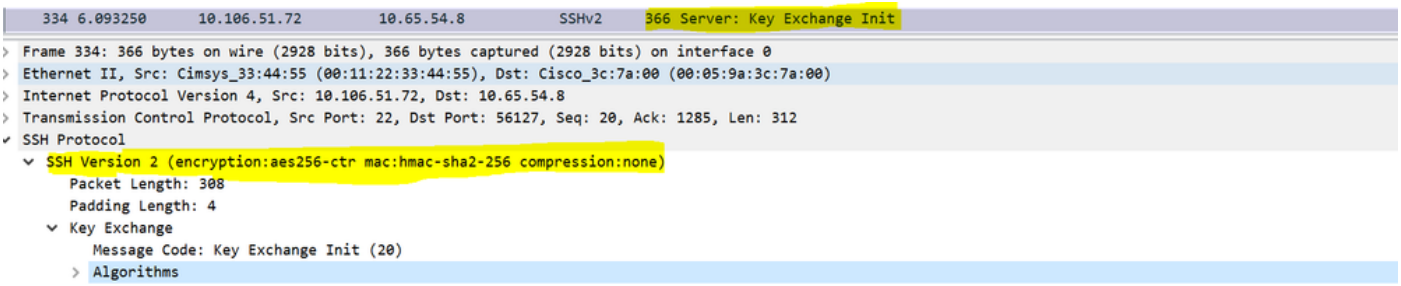


Door client ondersteunde algoritmen

b. De server reageert met zijn eigen Key Exchange Init bericht, met een lijst van de algoritmen die hij ondersteunt.

c. Aangezien deze berichten gelijktijdig worden uitgewisseld, vergelijken beide partijen hun algoritmelijsten. Als er een overeenkomst in de algoritmen door beide partijen wordt gesteund, gaan zij aan de volgende stap te werk. Als er geen exacte overeenkomst is, selecteert de server het eerste algoritme uit de lijst van de client die het ook ondersteunt.

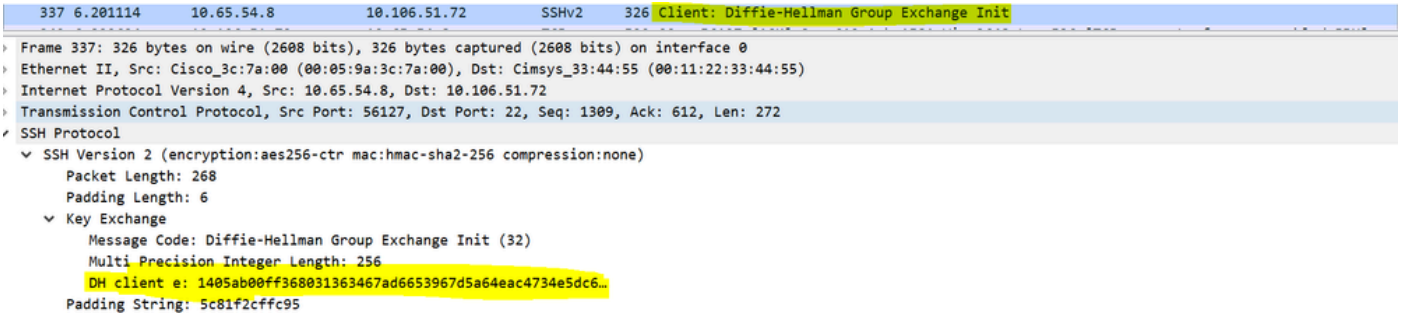
d. Als de client en server het niet eens kunnen worden over een gemeenschappelijk algoritme, mislukt de sleuteluitwisseling.



Exchange-nit voor servers

Key Exchange3. Hierna gaan beide partijen de fase in om gedeeld geheim te genereren met behulp van DH-sleuteluitwisseling en authenticeren de server:

a. De client genereert een sleutelpaarPublic and Privateen verstuurt de openbare DH-toets in het DH Group Exchange Init-pakket. Dit sleutelpaar wordt gebruikt voor de berekening van geheime sleutels.



Client DH Public Key & Diffie-Hellman groep Exchange Init

b. De server genereert een eigenPublic and Privatesleutelpaar. Het gebruikt de openbare sleutel van de cliënt en zijn eigen belangrijkste paar om het gedeelde geheim te berekenen.

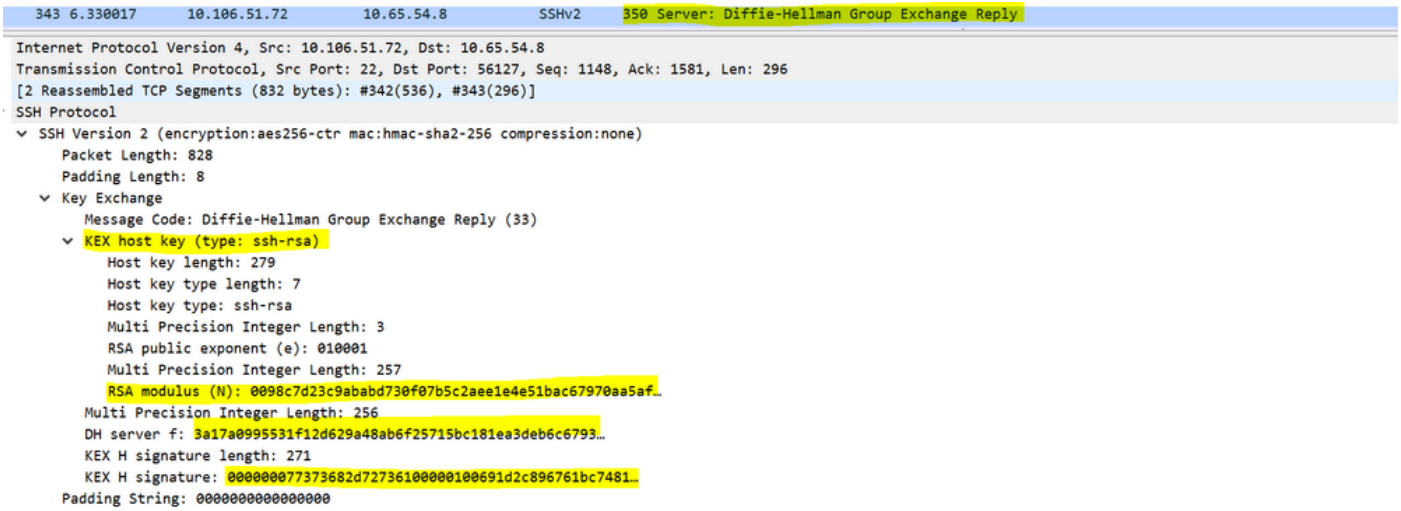
c. De server berekent ook een Exchange-hash met deze ingangen:

- Identificatietekenreeks clients
- Serveridentificatietekenreeks
- payload van client KEXINIT
- Payload of Server KEXINIT
- Openbare sleutel van servers met hostsleutels (RSA-sleutelpaar)
- Openbare sleutel voor klanten
- DH openbare sleutel voor servers
- Gedeelde geheime sleutel

d. Na computerhash ondertekent de server de hash met zijn RSA Private-toets.

e. De server construeert een bericht DH_Exchange_Reply dat het volgende bevat:

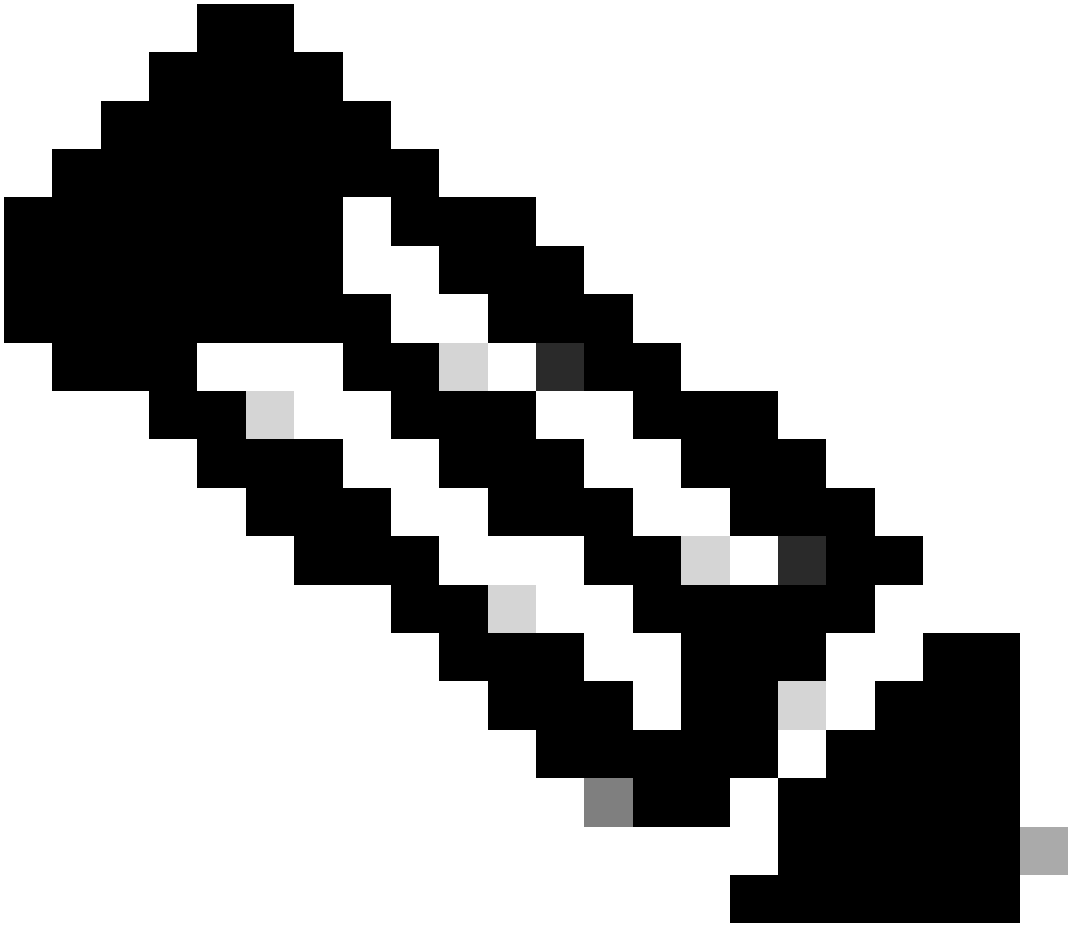
- RSA-Public Key of Server (om de client te helpen bij het verifiëren van de server)
- DH-Public key van Server (voor het berekenen van het gedeelde geheim)
- HASH (om de server te verifiëren en te bewijzen dat de server het gedeelde geheim heeft gegenereerd, aangezien de geheime sleutel deel uitmaakt van de hashberekening)



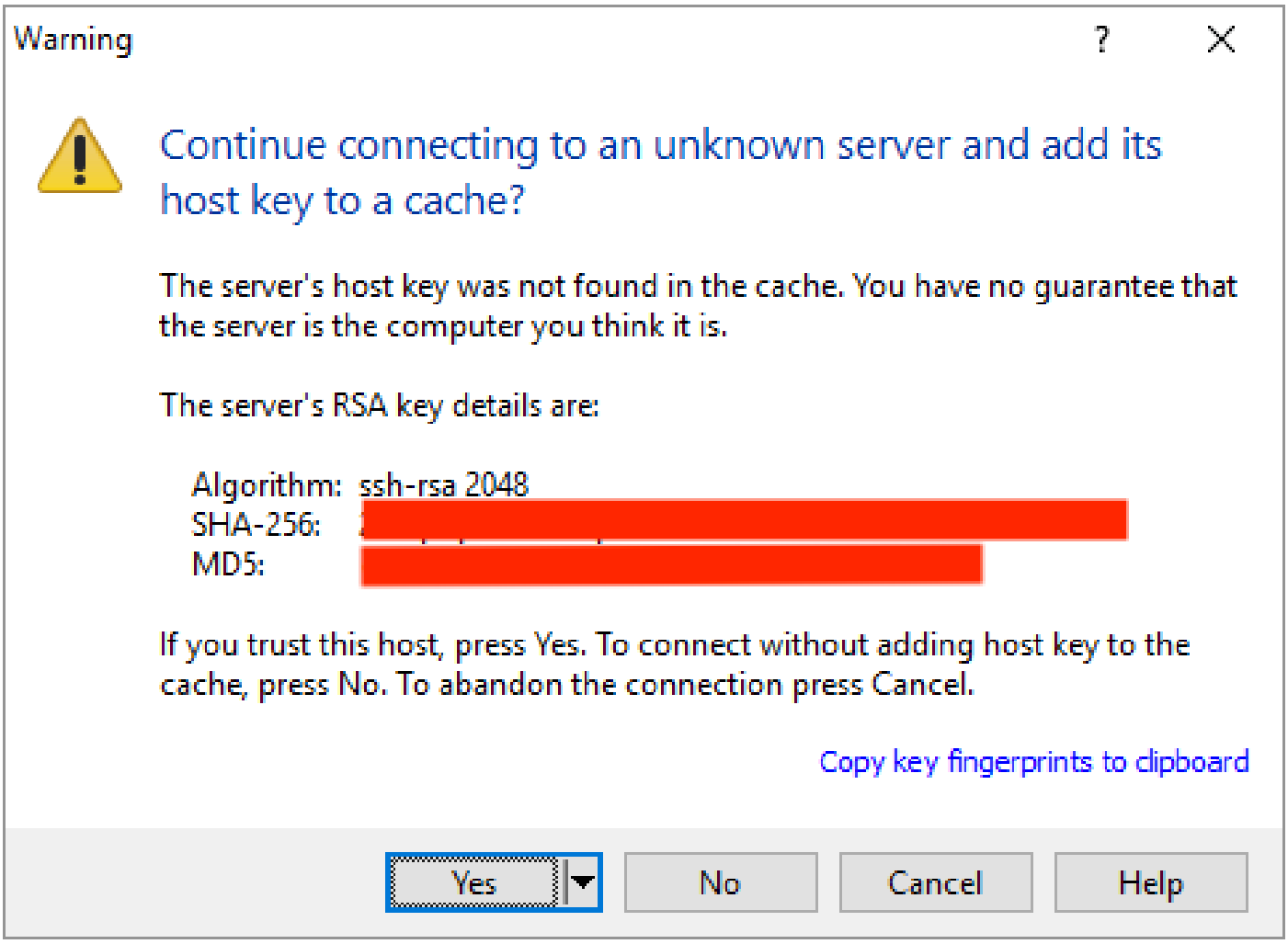
Server DH Public Key & Diffie-Hellman groep Exchange Antwoord

f. Na het ontvangen van de DH_Exchange_Reply, berekent de client de hash op dezelfde manier en vergelijkt deze met de ontvangen hash, decrypteert deze met behulp van de RSA Public Key van de server.

g. Alvorens de ontvangen HASH te decrypteren, moet de client de openbare sleutel van de server verifiëren. Deze verificatie wordt uitgevoerd door middel van een digitaal certificaat dat is ondertekend door een certificeringsinstantie (CA). Als het certificaat niet bestaat, is het aan de client om te beslissen of de openbare sleutel van de server wordt geaccepteerd.



Opmerking: wanneer u voor het eerst SSH in een apparaat dat geen digitaal certificaat gebruikt, kunt u een pop-up tegenkomen waarin u wordt gevraagd om de openbare sleutel van de server handmatig te accepteren. Om te voorkomen dat deze pop-up elke keer dat u verbinding maakt, kunt u ervoor kiezen om de host-sleutel van de server aan uw cache toe te voegen.

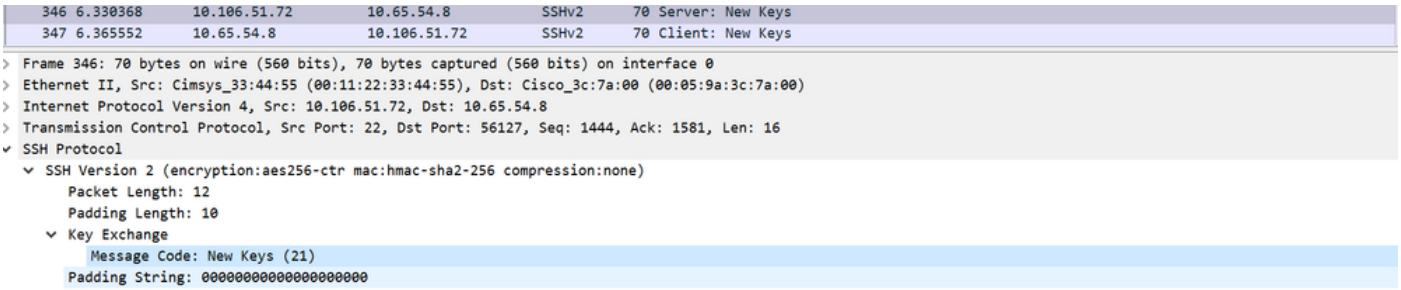


RSA-toets voor server

4. Aangezien het Gedeelde geheim nu wordt geproduceerd, gebruiken beide endsl het om deze sleutels af te leiden:

- Encryptietoetsen
- IV-toetsen - Dit zijn willekeurige getallen die worden gebruikt als invoer voor symmetrische algoritmen om de beveiliging te verbeteren
- Integriteitstoetsen

Het einde van de sleuteluitwisseling wordt aangegeven door de uitwisseling van het NEW KEYS' bericht, dat elke partij informeert dat alle toekomstige berichten versleuteld en beveiligd zullen worden met deze nieuwe sleutels .



Nieuwe toetsen voor client en server

5. De laatste stap is de serviceaanvraag. De client stuurt een pakket met SSH-serviceaanvragen naar de server om gebruikersverificatie te starten. De server reageert met een bericht van SSH Service Accept, waarin de client wordt gevraagd in te loggen. Deze uitwisseling vindt plaats via het gevestigde beveiligde kanaal.

Gerelateerde informatie

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.