Informazioni su Secure Shell Packet Exchange

Sommario

Introduzione

In questo documento viene descritto lo scambio a livello di pacchetto durante la negoziazione SSH (Secure Shell).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei concetti base relativi alla sicurezza:

- Autenticazione
- Riservatezza
- Integrità
- Metodi di scambio chiave

Componenti usati

Il documento può essere consultato per tutte le versioni hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti.

Protocollo SSH

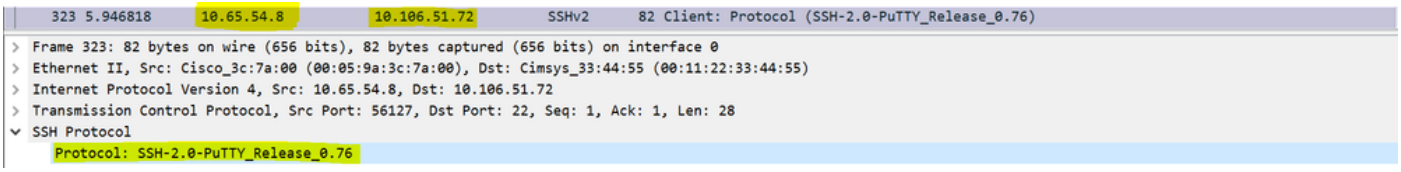
Il protocollo SSH è un metodo per effettuare in modo sicuro il login remoto da un computer all'altro. Le applicazioni SSH si basano su un'architettura client-server e connettono un'istanza del client SSH a un server SSH.

SSH Exchange

1. La prima fase del SSH è denominata Identification String Exchange.

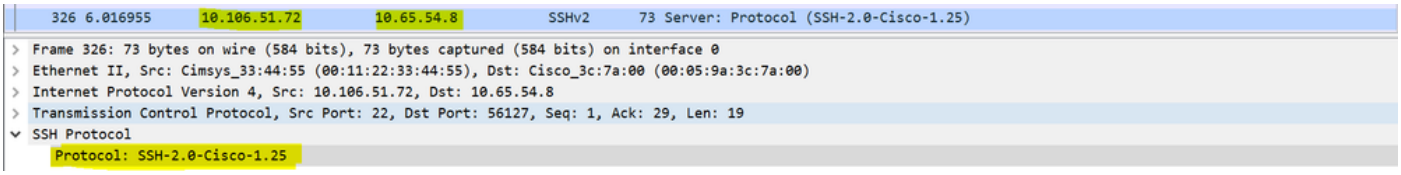
a. Il client crea un pacchetto e lo invia al server contenente:

- Versione protocollo SSH
- Versione del software



La versione del protocollo client è SSH2.0, la versione del software è Putty_0.76.

b. Il server risponde con la propria stringa di identificazione Exchange, incluse la versione del protocollo SSH e la versione del software.

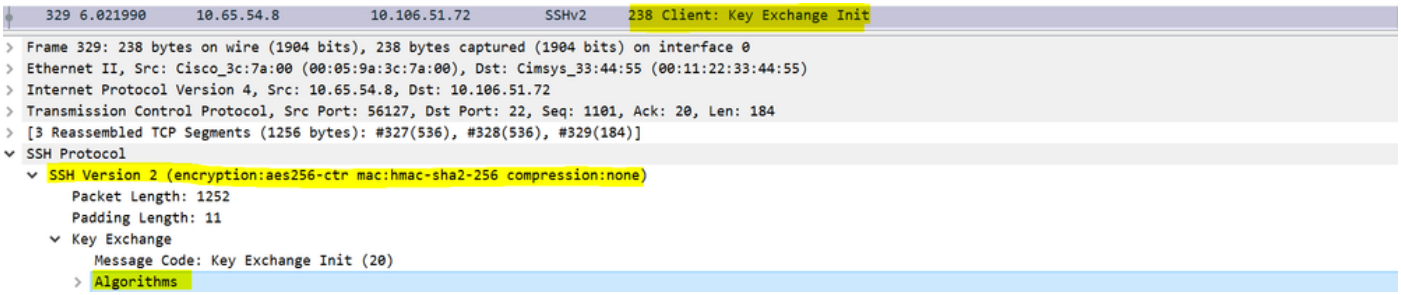


La versione del protocollo del server è SSH2.0, la versione del software è Cisco 1.25

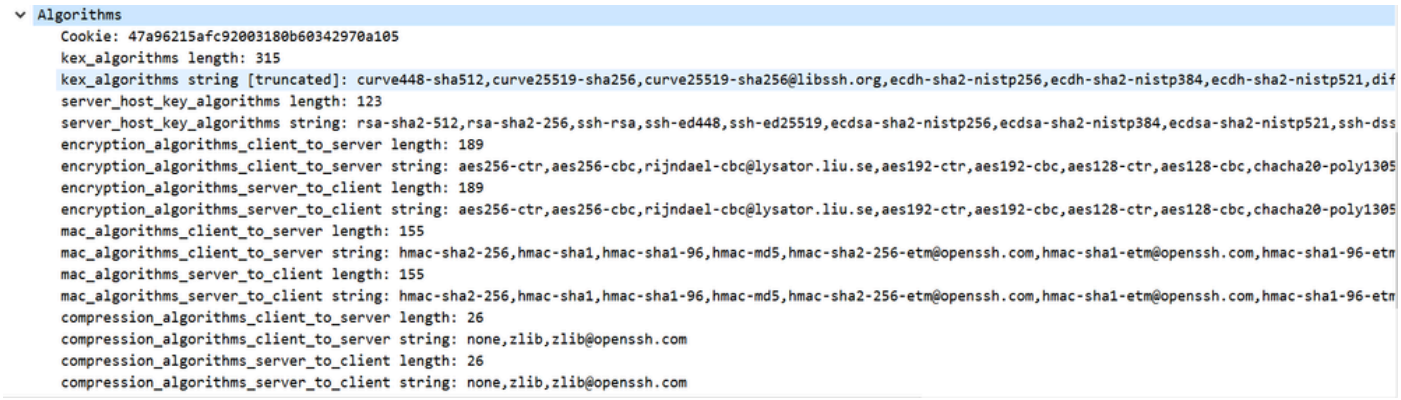
2. Il passo successivo è **Algorithm Negotiation**. In questo passo, sia il client che il server negoziano i seguenti algoritmi:

- Scambio chiave
- Crittografia
- HMAC (codice di autenticazione del messaggio basato su hash)
- Compressione

1. Il client invia un messaggio di inizializzazione scambio chiave al server, specificando gli algoritmi supportati. Gli algoritmi sono elencati in ordine di preferenza.



Inizializzazione scambio chiave

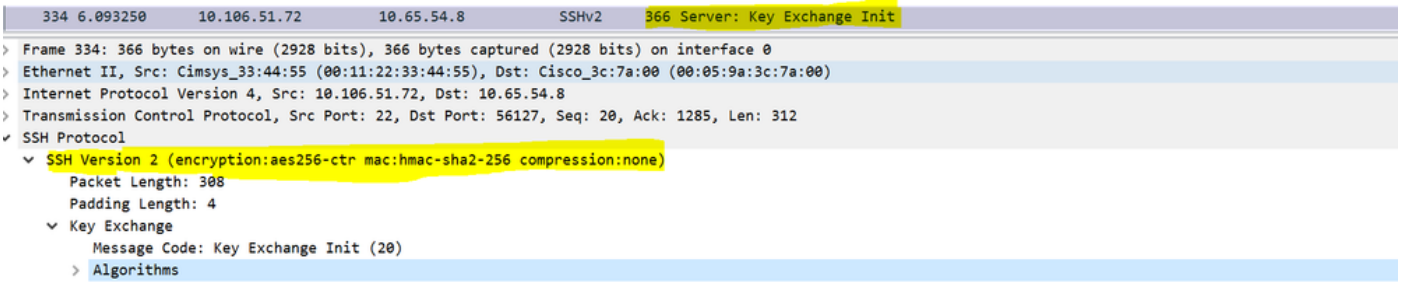


Algoritmi supportati dal client

b. Il server risponde con il proprio messaggio di inizializzazione scambio chiave, elencando gli algoritmi supportati.

c. Poiché questi messaggi vengono scambiati contemporaneamente, entrambe le parti confrontano i propri elenchi di algoritmi. Se esiste una corrispondenza negli algoritmi supportati da entrambi i lati, questi procedono al passaggio successivo. Se non esiste una corrispondenza esatta, il server seleziona il primo algoritmo dall'elenco del client supportato.

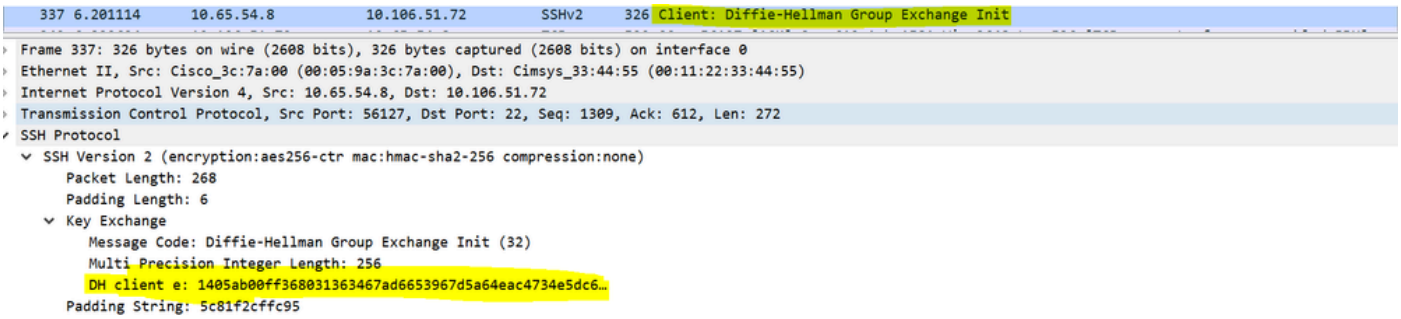
d. Se il client e il server non concordano su un algoritmo comune, lo scambio di chiave non riesce.



Inizializzazione scambio chiave server

3. Dopo questa operazione, entrambi i dispositivi entrano nella **Key Exchange**fase di generazione del segreto condiviso utilizzando lo scambio di chiave DH e autenticano il server:

a. Il client genera una coppia di chiaviPublic and Privatee invia la chiave pubblica DH nel pacchetto Init di Exchange del gruppo DH. Questa coppia di chiavi viene utilizzata per il calcolo della chiave segreta.



Inizializzazione scambio chiave pubblica DH client e gruppo Diffie-Hellman

b. Il server genera una propria coppiaPublic and Privatedi chiavi. Utilizza la chiave pubblica del client e la sua coppia di chiavi per calcolare il segreto condiviso.

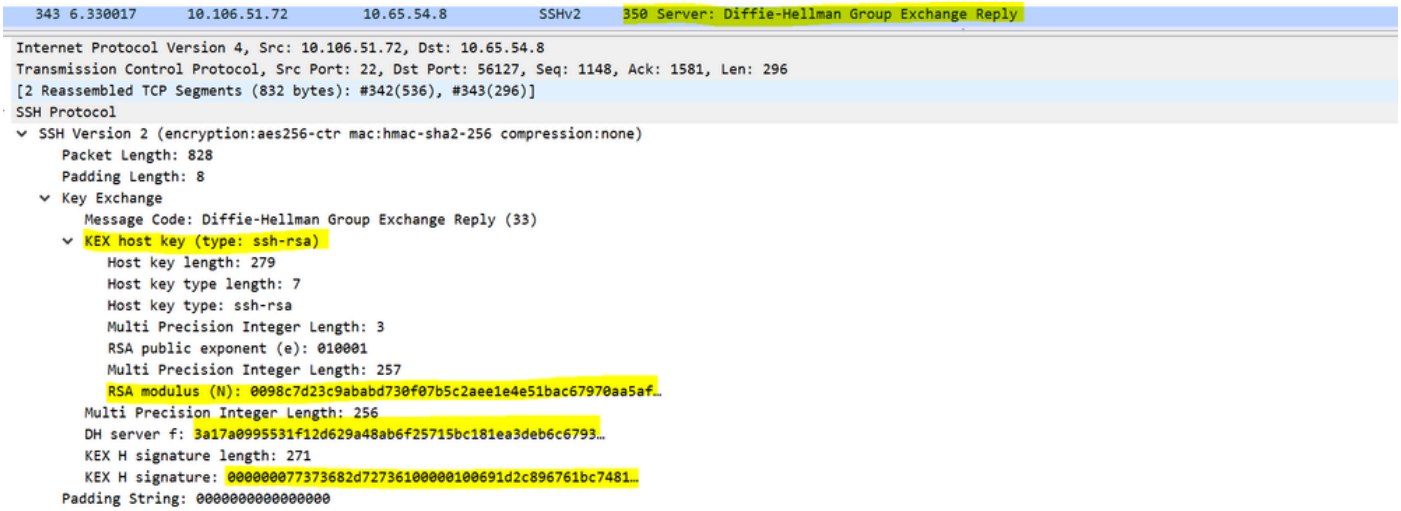
c. Il server calcola anche un hash di Exchange con questi input:

- Stringa di identificazione client
- Stringa di identificazione server
- Payload di KEXINIT client
- Payload di Server KEXINIT
- Chiave pubblica server da chiavi host (coppia di chiavi RSA)
- Chiave pubblica DH client
- Chiave pubblica DH del server
- Chiave privata condivisa

d. Dopo aver calcolato l'hash, il server lo firma con la chiave privata RSA.

e. Il server crea un messaggio DH_Exchange_Reply che include:

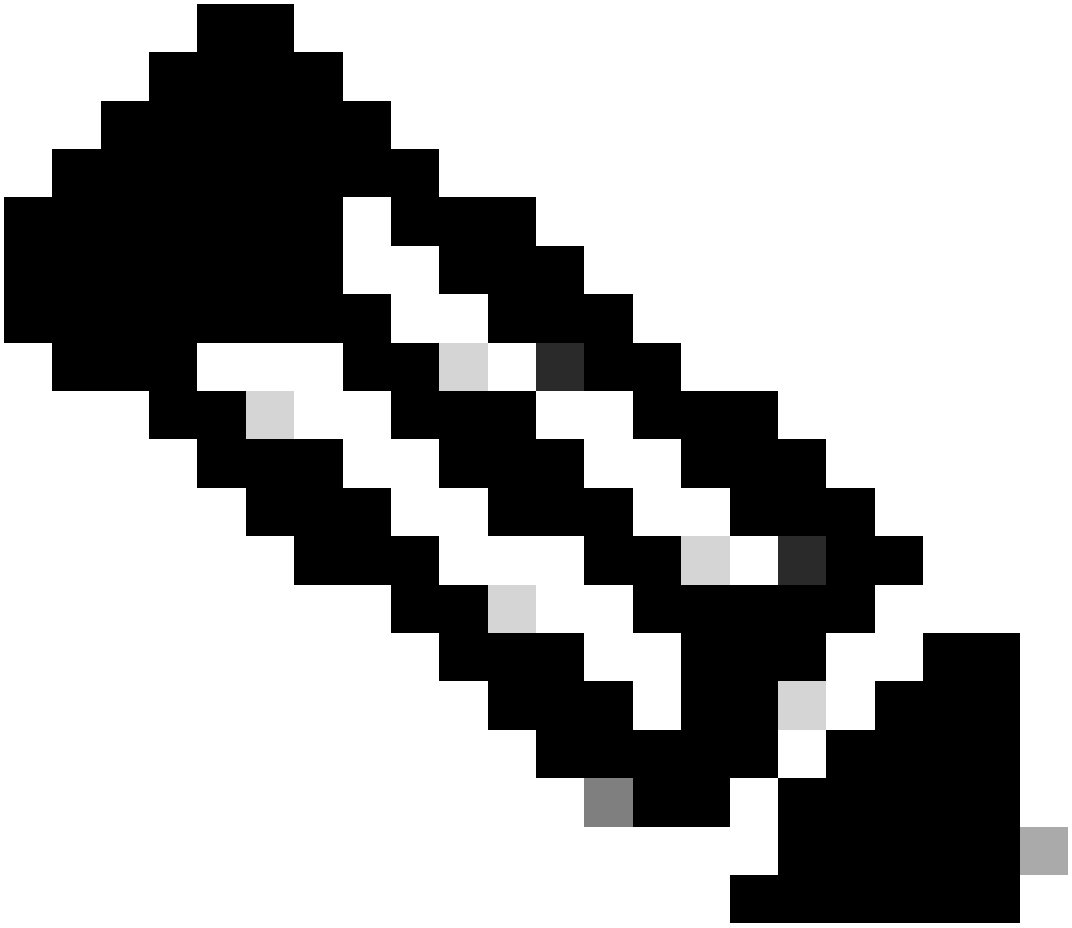
- RSA-Chiave pubblica del server (per consentire al client di autenticare il server)
- DH-Chiave pubblica del server (per il calcolo del segreto condiviso)
- HASH (per autenticare il server e dimostrare che il server ha generato il segreto condiviso, in quanto la chiave privata fa parte del calcolo dell'hash)



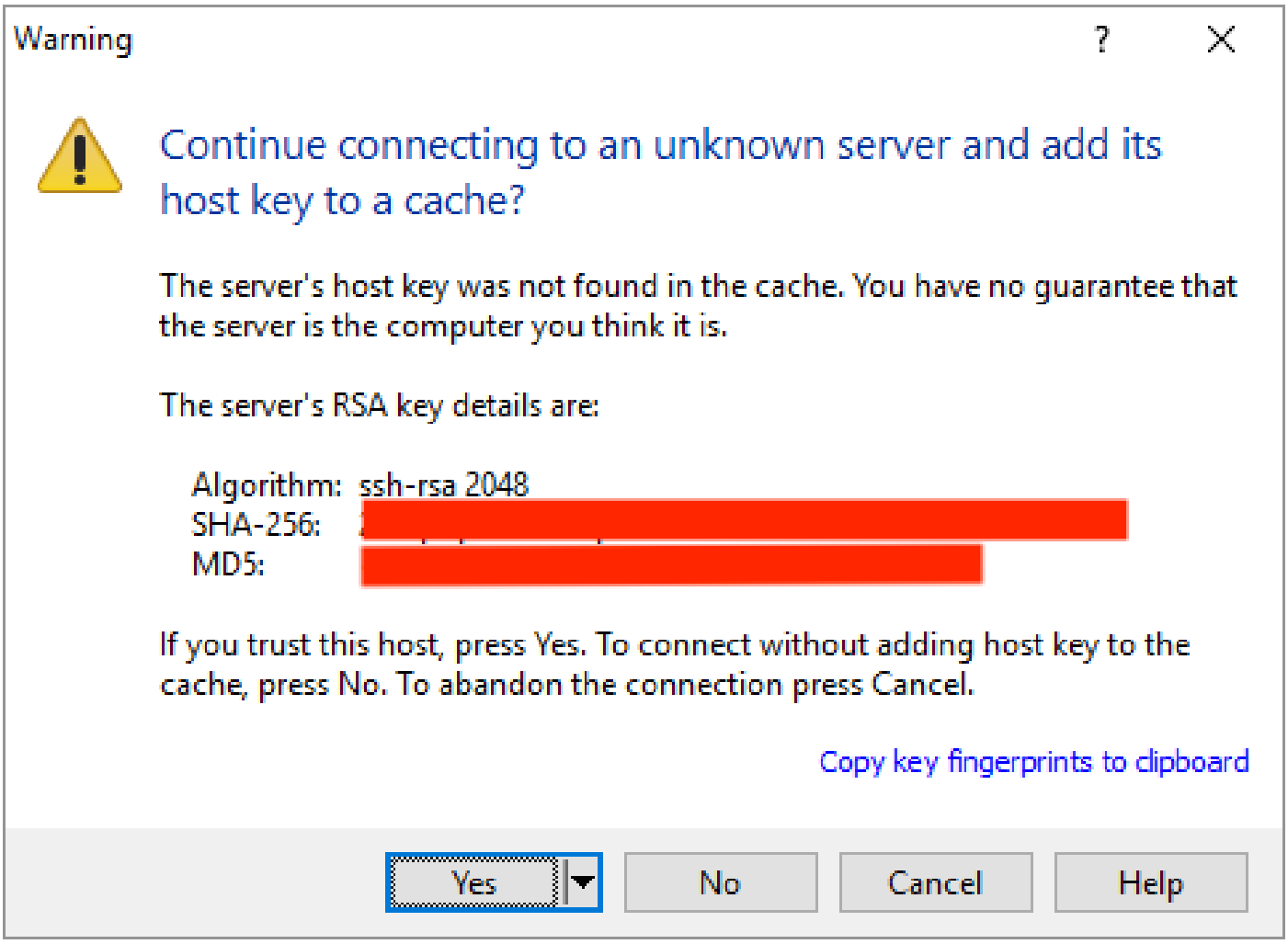
Risposta di scambio chiave pubblica DH del server e gruppo Diffie-Hellman

f. Dopo aver ricevuto DH_Exchange_Reply, il client calcola l'hash nello stesso modo e lo confronta con l'hash ricevuto, decrittografandolo con la chiave pubblica RSA del server.

g. Prima di decrittografare l'HASH ricevuto, il client deve verificare la chiave pubblica del server. Questa verifica viene eseguita tramite un certificato digitale firmato da un'Autorità di certificazione (CA). Se il certificato non esiste, spetta al client decidere se accettare la chiave pubblica del server.



Nota: quando si accede per la prima volta al protocollo SSH su un dispositivo che non usa un certificato digitale, è possibile che venga visualizzata una schermata di popup in cui si chiede di accettare manualmente la chiave pubblica del server. Per evitare di visualizzare questo popup ogni volta che ci si connette, è possibile scegliere di aggiungere la chiave host del server alla cache.

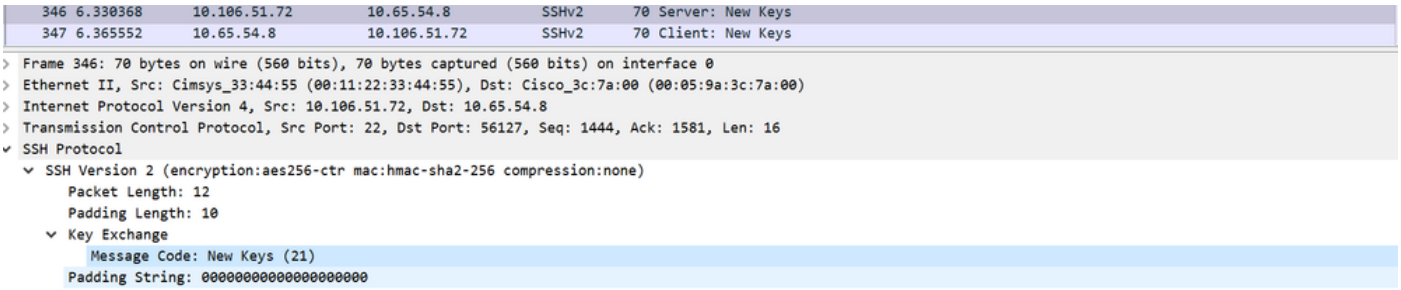


Chiave RSA del server

4. Poiché il segreto condiviso è ora generato, entrambi gli endpoint lo utilizzano per derivare queste chiavi:

- Chiavi di crittografia
- Chiavi IV: numeri casuali utilizzati come input per algoritmi simmetrici al fine di migliorare la sicurezza
- Chiavi di integrità

La fine dello scambio di chiavi è segnalata dallo scambio del NEW KEYS messaggio, che informa ciascuna parte che tutti i messaggi futuri saranno crittografati e protetti utilizzando queste nuove chiavi.



Nuove chiavi client e server

5. La fase finale è la richiesta di assistenza. Il client invia un pacchetto di richiesta del servizio SSH al server per avviare l'autenticazione dell'utente. Il server risponde con un messaggio di accettazione del servizio SSH, in cui viene richiesto al client di eseguire l'accesso. Questo scambio avviene tramite il canale sicuro stabilito.

Informazioni correlate

- https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- https://datatracker.ietf.org/doc/html/rfc4253
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).