

Secure Shell-pakketuitwisseling begrijpen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[SSH-protocol](#)

[SSH exchange](#)

[Gerelateerde informatie](#)

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

```
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
v SSH Protocol
  Protocol: SSH-2.0-PuTTY_Release_0.76
```

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.

```
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
v SSH Protocol
  Protocol: SSH-2.0-Cisco-1.25
```

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.

```
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)]
v 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
```

Key Exchange 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

```

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.

```

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

```

Exchange-init 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 sleutelpaar *Public* and *Private* en verstuurt de openbare DH-toets in het DH Group Exchange Init-pakket. Dit sleutelpaar wordt gebruikt voor de berekening van geheime sleutels.

```

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

```

Client DH Public Key & Diffie-Hellman groep Exchange Init

b. De server genereert een eigen Public and Private sleutel paar. 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-sleutel paar)
- 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)

```
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
```

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.

Warning



Continue connecting to an unknown server and add its host key to a cache?

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's RSA key details are:

Algorithm: ssh-rsa 2048
 SHA-256: [REDACTED]
 MD5: [REDACTED]

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

[Copy key fingerprints to clipboard](#)

Yes No Cancel Help

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 .

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
  
```

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.