De vooraf gedeelde sleutel versleutelen in een router configureren

Inhoud

Inleiding

Dit document beschrijft hoe u codering van zowel huidige als nieuwe vooraf gedeelde sleutels in een router kunt instellen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversie:

- Cisco IOS XE®-softwarerelease 16.9

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. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

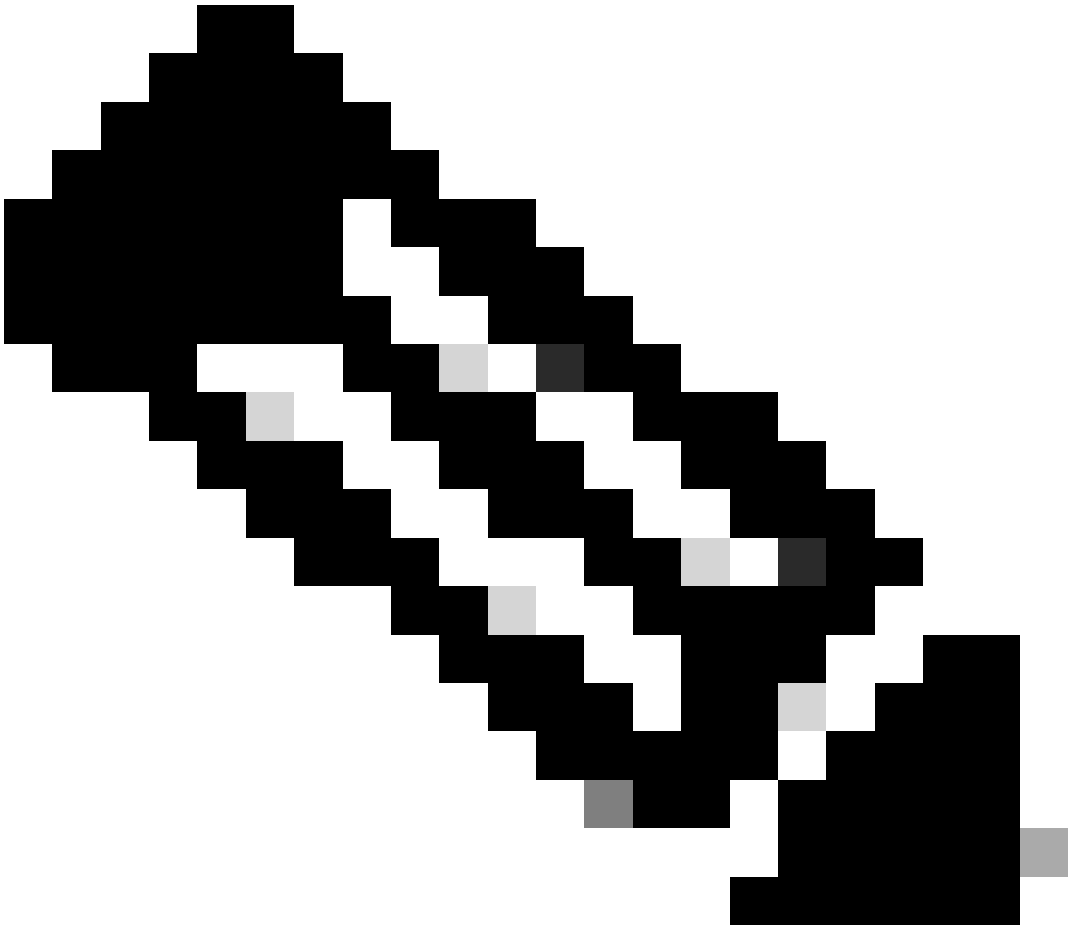
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

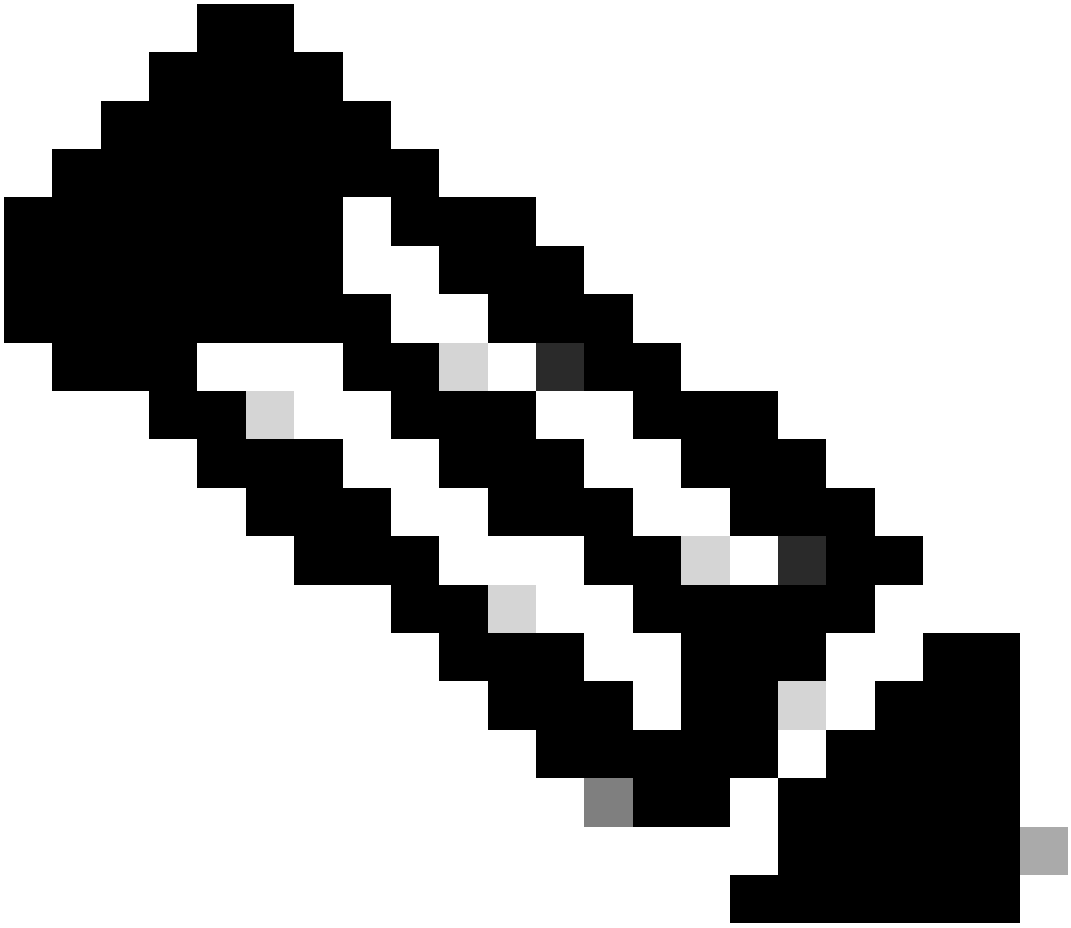
Cisco IOS-softwarerelease 12.3(2)T-code introduceert de functionaliteit waarmee de router de vooraf gedeelde sleutel van Internet Security Association en Key Management Protocol (ISAKMP) in een veilig type 6-formaat kan versleutelen in niet-vluchtig RAM, niet-vluchtig RAM (NVRAM). De te versleutelen vooraf gedeelde sleutel kan worden geconfigureerd als standaard, onder een ISAKMP-sleutelring, in agressieve modus, of als groepswachtwoord onder een eenvoudige VPN-server (EzVPN) of clientinstelling.

Configureren

In deze sectie vindt u de informatie die u kunt gebruiken om de functies te configureren die in dit document worden beschreven.



Opmerking: gebruik de Opdrachtzoekfunctie om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.



Opmerking: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

Deze twee opdrachten zijn geïntroduceerd om vooraf gedeelde sleutelcodering mogelijk te maken:

- sleutel config-sleutel wachtwoord-encryptie [primaire sleutel]
- wachtwoordcodering

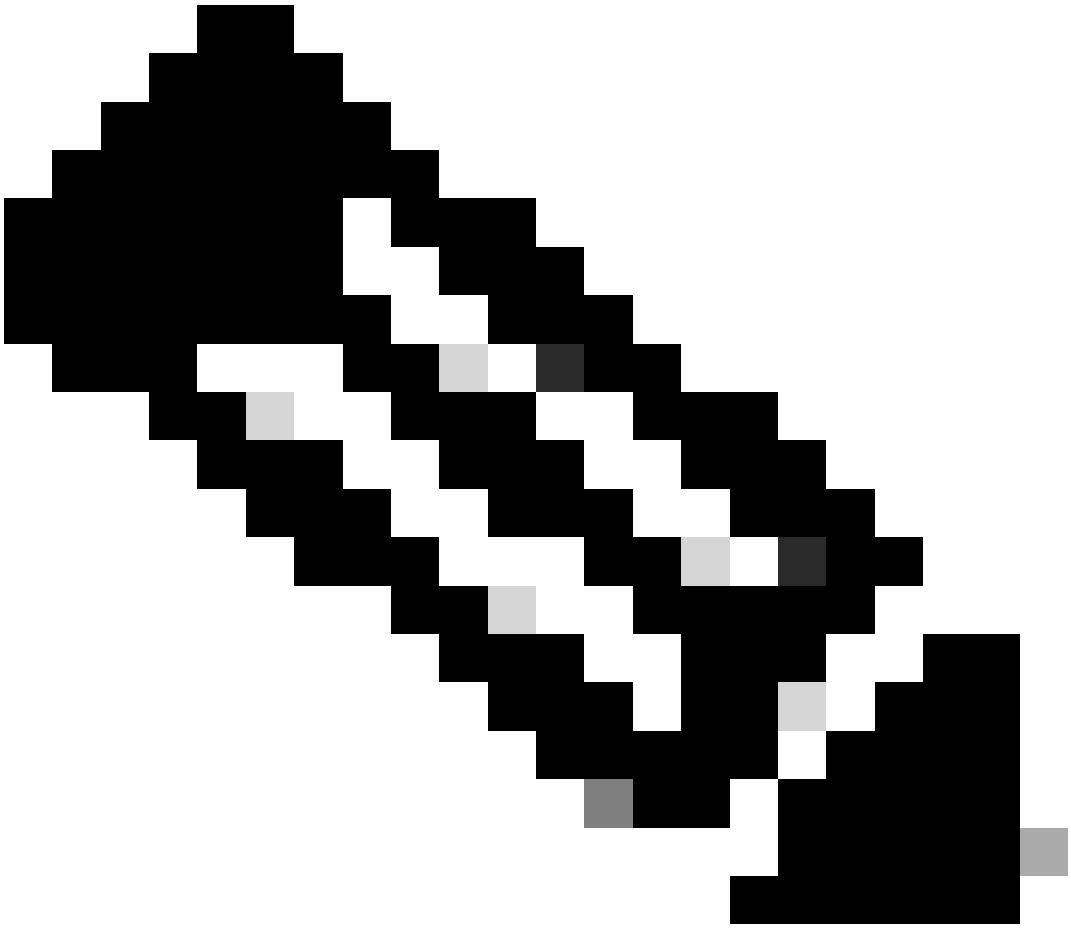
De [primaire sleutel] is het wachtwoord/de sleutel die wordt gebruikt om alle andere sleutels in de routerconfiguratie te versleutelen met het gebruik van een symmetrisch algoritme van de Advanced Encryption Standard (AES). De primaire sleutel wordt niet opgeslagen in de routerconfiguratie en kan niet op enige wijze worden gezien of verkregen terwijl verbonden met de router.

Na configuratie wordt de primaire sleutel gebruikt om huidige of nieuwe sleutels in de routerconfiguratie te versleutelen. Als de [primaire sleutel] niet op de opdrachtregel is gespecificeerd, vraagt de router de gebruiker om de sleutel in te voeren en deze opnieuw in te

voeren voor verificatie. Als er al een toets bestaat wordt de gebruiker gevraagd eerst de oude toets in te voeren. Toetsen worden niet versleuteld tot u de opdracht wachtwoordversleuteling uitgeeft.

De primaire sleutel kan worden veranderd (hoewel dit niet nodig is tenzij de sleutel op een bepaalde manier gecompromitteerd is) met de belangrijkste configuratie-sleutel... commando opnieuw met de nieuwe [primaire-sleutel]. Alle huidige versleutelde sleutels in de routerconfiguratie worden opnieuw versleuteld met de nieuwe sleutel.

U kunt de primaire sleutel verwijderen wanneer u de no key config-key.... Nochtans, maakt dit alle momenteel gevormde sleutels in de routerconfiguratie nutteloos (een waarschuwingsbericht toont dat dit detailleert en de primaire belangrijkste schrapping bevestigt). Aangezien de primaire sleutel niet meer bestaat, kunnen de type 6 wachtwoorden niet worden gedecrypteerd en door de router worden gebruikt.



Opmerking: om veiligheidsredenen worden de wachtwoorden in de routerconfiguratie niet gedecodeerd door de aes opdracht voor wachtwoordversleuteling te verwijderen of door de primaire sleutel te verwijderen. Zodra wachtwoorden worden versleuteld, worden ze niet gedecodeerd. Huidige versleutelde sleutels in de configuratie

---

kunnen nog steeds worden gedecrypteerd op voorwaarde dat de primaire sleutel niet wordt verwijderd.

Bovendien om debug-type berichten van de functies van de wachtwoordencryptie te zien, gebruik het bevel van het **wachtwoordregistreren** in de configuratiewijze.

Configuraties

Dit document gebruikt deze configuraties op de router:

- De huidige voorgedeelde sleutel versleutelen
- Interactief een nieuwe primaire sleutel toevoegen
- Interactief de huidige primaire sleutel wijzigen
- De primaire sleutel verwijderen

De huidige voorgedeelde sleutel versleutelen

```
    <#root>

Router#



show running-config




Building configuration...
.
.crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 10.1.1.1
.
.
endRouter#



configure terminal



Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#



key config-key password-encrypt testkey123



Router(config)#



password encryption aes



Router(config)#



^Z
```

```
Router#
Router#



show running-config




Building configuration...
.
.
password encryption aes
.
.
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key



6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB



 address 10.1.1.1
.
.
end
```

Interactief een nieuwe primaire sleutel toevoegen

```
    <#root>


Router(config)#
```

```
key config-key password-encrypt



New key:


<enter key>


Confirm key:


<confirm key>


Router(config)#
```

Interactief de huidige primaire sleutel wijzigen

```
    <#root>

Router(config)#


key config-key password-encrypt


 Old key:
```

```
<enter current key>



New key:



<enter new key>



Confirm key:



<confirm new key>



Router(config)#
*Jan  7 01:42:12.299: TYPE6_PASS: Master key change heralded,
re-encrypting the keys with the new primary key
```

De primaire sleutel verwijderen

```
    <#root>

Router(config)#



no key config-key password-encrypt



WARNING: All type 6 encrypted keys will become unusable
```

```
Continue with primary key deletion ? [yes/no]:


yes


Router(config)#
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

Gerelateerde informatie

- **Pagina voor IPsec-ondersteuning**
- **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.