Konfigurieren der vorinstallierten Schlüssel zur Verschlüsselung auf einem Router

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Verschlüsselung des aktuellen und neuen vorinstallierten Schlüssels in einem Router einrichten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- Cisco IOS XE® Softwareversion 16.9

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. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

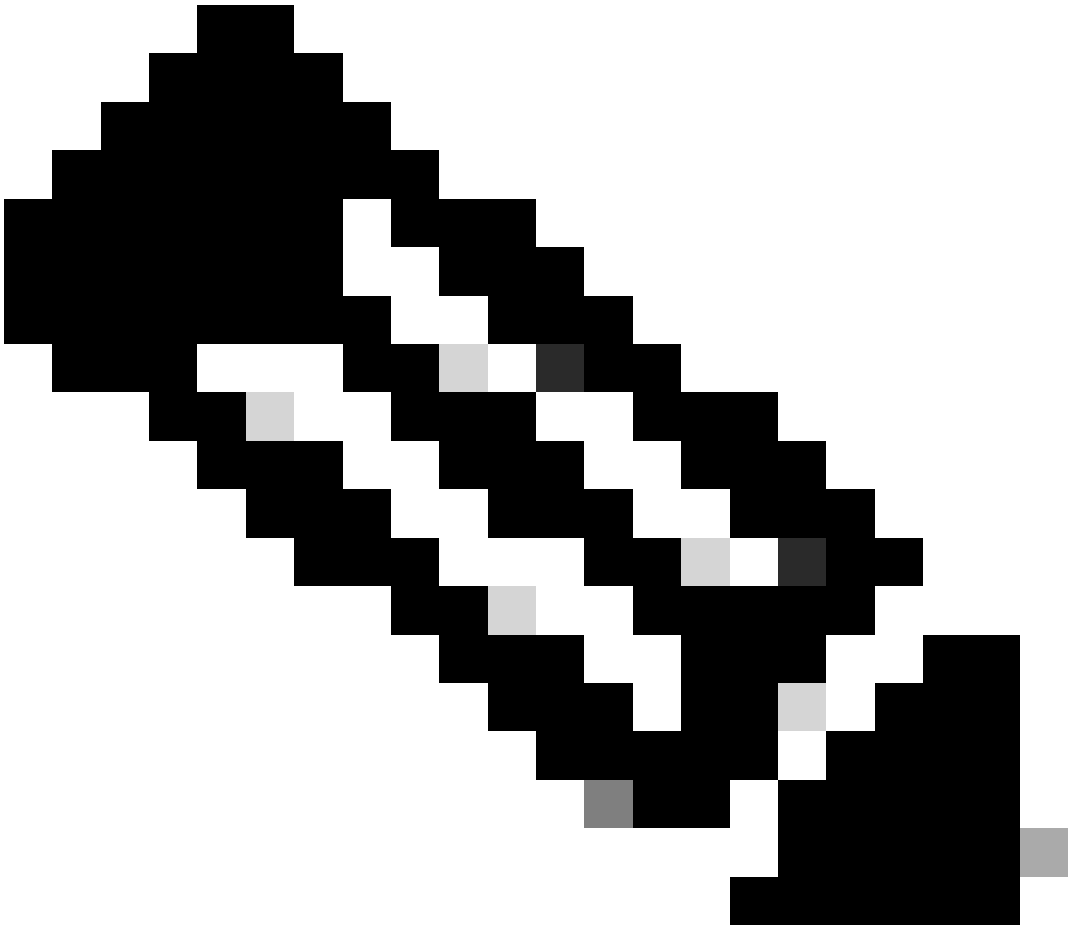
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

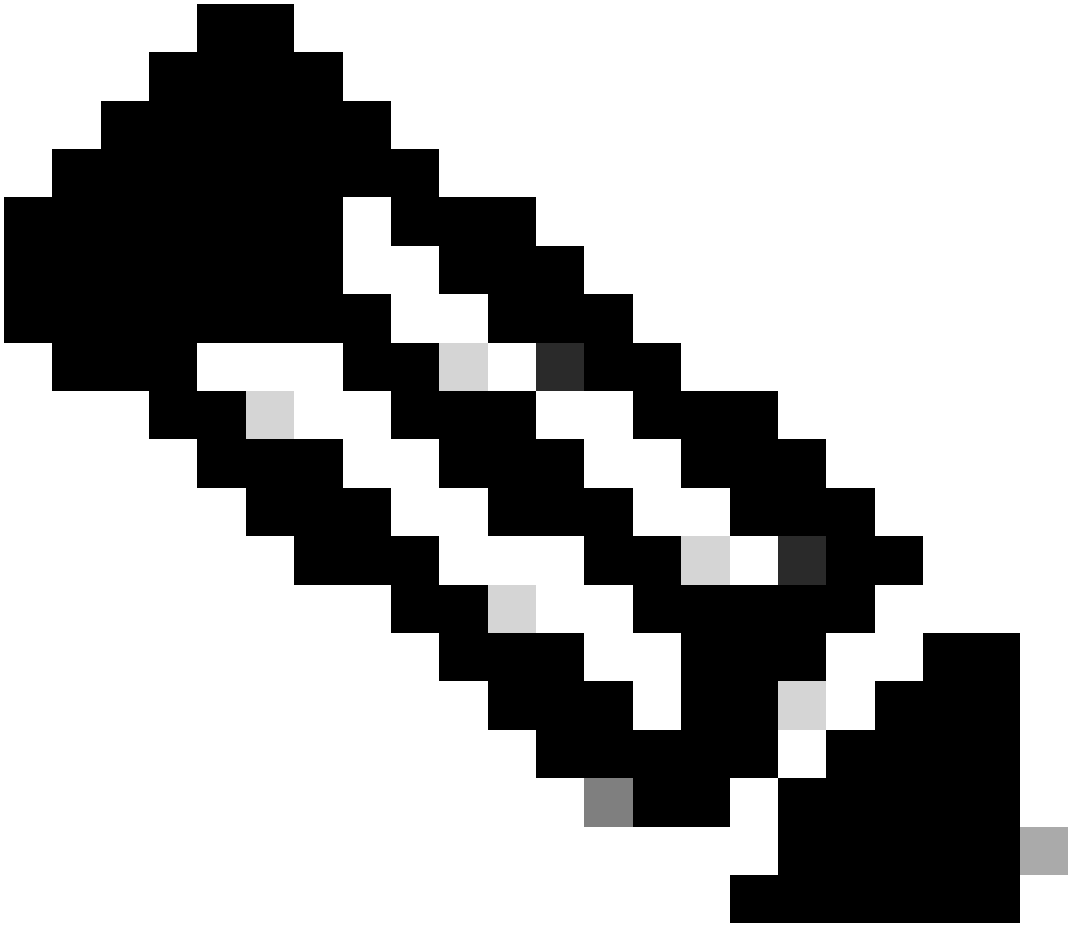
Die Cisco IOS Software, Version 12.3(2)T, bietet eine neue Funktionalität, mit der der Router den vorinstallierten ISAKMP-Schlüssel (Internet Security Association and Key Management Protocol) im sicheren Format Typ 6 im nichtflüchtigen RAM (Non-Volatile RAM, NVRAM) verschlüsseln kann. Der vorinstallierte Schlüssel, der verschlüsselt werden soll, kann entweder als Standard, unter einem ISAKMP-Keyring, im aggressiven Modus oder als Gruppenkennwort unter einem Easy VPN (EzVPN)-Server oder Client-Setup konfiguriert werden.

Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.



Hinweis: Verwenden Sie das Command Lookup Tool (Tool für die Suche nach Befehlen), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.



Hinweis: Nur registrierte Cisco Benutzer können auf das interne Cisco Tool und die zugehörigen Informationen zugreifen.

Diese beiden Befehle wurden eingeführt, um die Verschlüsselung mit vorinstalliertem Schlüssel zu ermöglichen:

- key config-key password-encryption [Primärschlüssel]
- Kennwort-Verschlüsselungsrate

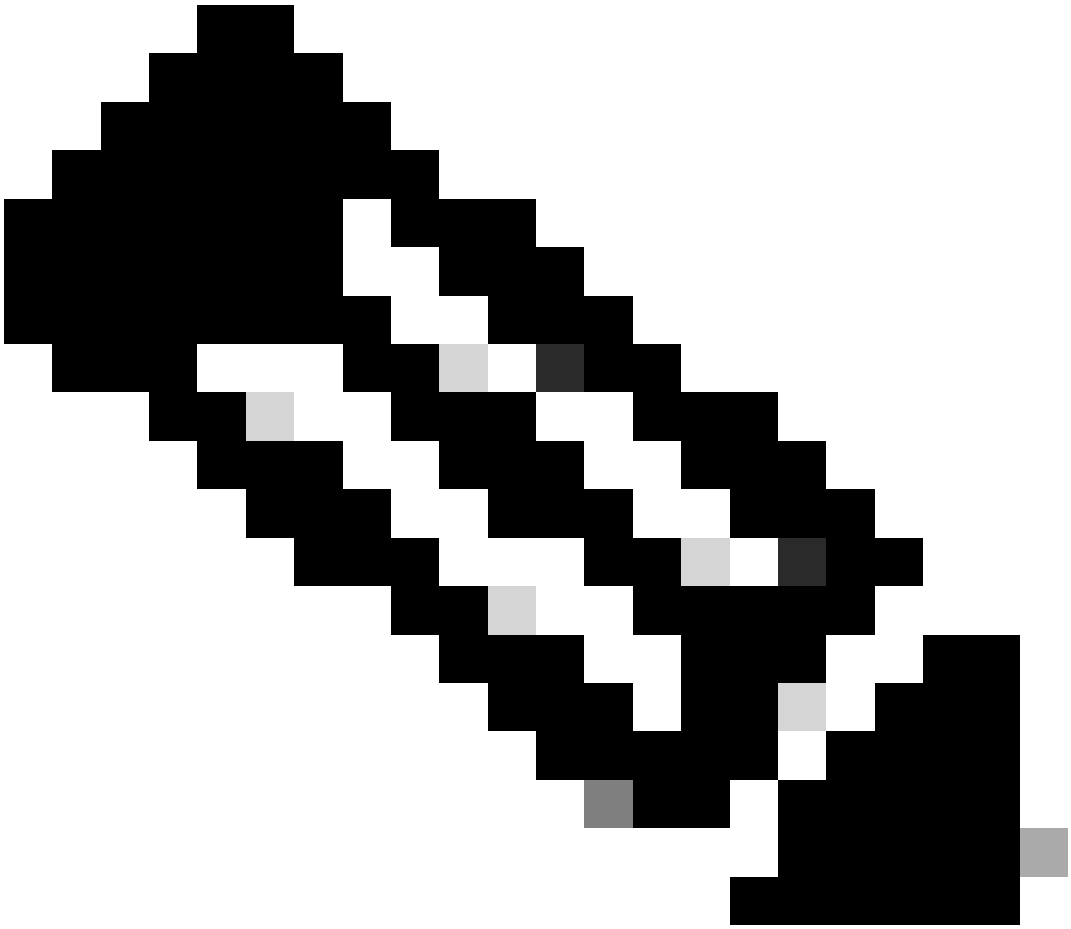
Der [Primärschlüssel] ist das Kennwort bzw. der Schlüssel, mit dem alle anderen Schlüssel in der Router-Konfiguration mithilfe eines symmetrischen Advanced Encryption Standard (AES)-Verschlüsselungsverfahrens verschlüsselt werden. Der Primärschlüssel ist nicht in der Router-Konfiguration gespeichert und kann bei der Verbindung mit dem Router nicht angezeigt oder abgerufen werden.

Nach der Konfiguration wird der Primärschlüssel zur Verschlüsselung aktueller oder neuer Schlüssel in der Router-Konfiguration verwendet. Wenn der [Primärschlüssel] nicht in der

Befehlszeile angegeben ist, fordert der Router den Benutzer zur Eingabe des Schlüssels und zur erneuten Eingabe zur Überprüfung auf. Wenn bereits ein Schlüssel vorhanden ist, wird der Benutzer aufgefordert, zuerst den alten Schlüssel einzugeben. Schlüssel werden erst verschlüsselt, wenn Sie den Befehl password encryption aes eingeben.

Der Primärschlüssel kann mit dem Befehl key config-key... erneut mit dem neuen [primary-key] geändert werden (obwohl dies nicht notwendig ist, es sei denn, der Schlüssel wurde in irgendeiner Weise kompromittiert). Alle aktuellen verschlüsselten Schlüssel in der Router-Konfiguration werden mit dem neuen Schlüssel neu verschlüsselt.

Sie können den Primärschlüssel löschen, wenn Sie den Konfigurationsschlüssel "Kein Schlüssel" eingeben... Dadurch werden jedoch alle aktuell konfigurierten Schlüssel in der Router-Konfiguration nutzlos (eine Warnmeldung zeigt diese Details an und bestätigt, dass der Primärschlüssel gelöscht wurde). Da der Primärschlüssel nicht mehr vorhanden ist, können die Typ-6-Kennwörter nicht entschlüsselt und vom Router verwendet werden.



Hinweis: Aus Sicherheitsgründen werden die Kennwörter in der Routerkonfiguration weder durch Entfernen des Primärschlüssels noch durch Entfernen des aes Befehls zur

---

Kennwortverschlüsselung entschlüsselt. Sobald Kennwörter verschlüsselt sind, werden sie nicht mehr entschlüsselt. Die aktuellen verschlüsselten Schlüssel in der Konfiguration können weiterhin entschlüsselt werden, sofern der Primärschlüssel nicht entfernt wird.

Um Meldungen vom Typ debug über Kennwortverschlüsselungsfunktionen anzuzeigen, verwenden Sie im Konfigurationsmodus den Befehl **password logging**.

Konfigurationen

In diesem Dokument werden die folgenden Konfigurationen auf dem Router verwendet:

- Aktuellen vorinstallierten Schlüssel verschlüsseln
- Neuen Primärschlüssel interaktiv hinzufügen
- Den aktuellen Primärschlüssel interaktiv ändern
- Primärschlüssel löschen

Aktuellen vorinstallierten Schlüssel verschlüsseln

```
    <#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
```

Neuen Primärschlüssel interaktiv hinzufügen
<#root>

```
Router(config)#

key config-key password-encrypt

New key:

<enter key>

Confirm key:

<confirm key>

Router(config)#
```

Den aktuellen Primärschlüssel interaktiv ändern

```
    <#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
```

Primärschlüssel löschen

```
    <#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)#
```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- **IPsec-Support-Seite**
- **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.