Verschlüsselung

IPsec nutzt Verschlüsselung, um Daten im Übertragungsprozess zu schützen, indem es den Payload von IP-Paketen verschlüsselt.

Schlüsseltausch

IPsec verwendet das Internet Key Exchange (IKE) Protokoll für sichere Verbindungen und Verhandlungen zur Verschlüsselung und Authentifizierung.

Tunnel- und Transportmodus

IPsec kann entweder im Tunnelmodus (verschlüsselt das gesamte IP-Paket) oder im Transportmodus (verschlüsselt nur den Payload des IP-Pakets) arbeiten.

Algorithmeterstützunnung

IPsec unterstützt eine Reihe von Verschlüsselungs- und Authentifizierungsalgorithmen, darunter AES, DES, 3DES, HMAC-SHA1, HMAC-SHA256, und HMAC-SHA384.

Kompatibilität

IPsec ist mit den meisten Betriebssystemen und Netzwerkgeräten kompatibel.

Authentifizierung

IPsec sorgt mit einer Authentifizierung dafür, dass nur berechtigte Parteien auf die verschlüsselten Daten zugreifen können.

Configuration

```
crypto isakmp policy 10
encryption aes 256
hash sha
authentication pre-share
group 2
lifetime 3600
```

Virtual Tunnel Interface

```
interface Tunnel0
ip address 172.16.0.1 255.255.255.252
tunnel source 10.0.0.1
tunnel destination 10.0.0.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile MyProfile
```

By **midastgk**
cheatography.com/midastgk/

Published 31st January, 2023.
Last updated 31st January, 2023.