V2Ray ausprobieren: Eine Schritt-für-Schritt-Anleitung

V2Ray ist eine vielseitige Plattform zum Erstellen von Proxys, um Netzwerkbeschränkungen zu umgehen und die Online-Privatsphäre zu verbessern. In dieser Anleitung führen wir Sie durch die Installation und Konfiguration von V2Ray auf einem Ubuntu-Server. Wir behandeln Installationsschritte, Konfigurationsdateien, häufige Probleme und Überprüfungsmethoden, um sicherzustellen, dass alles reibungslos funktioniert.

Inhaltsverzeichnis

Installation

Beginnen Sie damit, V2Ray herunterzuladen und mithilfe des bereitgestellten Installationsskripts zu installieren.

```
ubuntu@ip-172-26-0-236:~$ curl -L https://raw.githubusercontent.com/v2fly/fhs-install-v2ray/master/insta
```

Führen Sie das Installationsskript aus:

```
chmod +x in.sh
sudo ./in.sh
```

Hinweis: Der obige Code ist ein Bash-Befehl, der die Ausführungsberechtigung für die Datei `in.sh` erteilt und sie dann mit Administratorrechten ausführt. Da es sich um einen Codeblock handelt, wurde er nicht übersetzt.

Installationsausgabe:

```
[Install]
WantedBy=multi-user.target
```

info: V2Ray v5.22.0 ist installiert.

```
Hinweis: Das Skript schlägt vor, abhängige Software bei Bedarf zu entfernen:
```

```bash
apt purge curl unzip
```

Konfiguration

V2Ray-Konfiguration (`config.json`)

Diese JSON-Datei definiert die Einstellungen für eingehende und ausgehende Verbindungen in V2Ray.

```
{
    "inbounds": [
        {
            "port": 1080,
            "listen": "0.0.0.0",
            "protocol": "vmess",
            "settings": {
                "clients": [
                    {
                        "id": "9f02f6b2-1d7d-4b10-aada-69e050f1be6b",
                        "level": 0,
                        "alterId": 0,
                        "email": "example@v2ray.com",
                        "security": "auto"
                    }
                ]
```

```
            },
            "streamSettings": {
                "network": "tcp"
            },
            "sniffing": {
                "enabled": true,
                "destOverride": [
                    "http",
                    "tls"
                ]
            },
            "tag": "vmess-inbound",
            "udp": true
        }
    ],
    "outbounds": [
        {
            "protocol": "freedom",
            "settings": {},
            "tag": "outbound-freedom",
            "udp": true
        }
    ],
    "log": {
        "loglevel": "debug",
        "access": "/var/log/v2ray/access.log",
        "error": "/var/log/v2ray/error.log"
    },
    "stats": {
        "enabled": false
    },
    "environment": {
        "v2ray.vmess.aead.forced": "false"
    }
}
```

Hauptpunkte: - Inbounds: Definiert die Einstiegspunkte für eingehende Verbindungen. Hier

wird das `vmess`-Protokoll auf Port `1080` verwendet. - Outbounds: Gibt an, wohin der Datenverkehr gesendet werden soll. Das `freedom`-Protokoll ermöglicht den ungehinderten Durchfluss des Datenverkehrs. - Logging: Konfiguriert, um Zugriffs- und Fehlerinformationen für Debugging-Zwecke zu protokollieren. - Sicherheit: Das Feld `security` ist auf `aes-256-gcm` gesetzt, um eine verbesserte Verschlüsselung zu gewährleisten.

Proxy-Konfiguration (`config.yaml`)

Diese YAML-Datei konfiguriert die Proxy-Einstellungen, DNS und Regeln für das Traffic-Routing.

```yaml
port: 7890
socks-port: 7891
mixed-port: 7892
allow-lan: true
mode: Rule
log-level: info
external-controller: 0.0.0.0:9090
experimental:
  ignore-resolve-fail: true

dns:
  enable: false
  listen: 0.0.0.0:53
  enhanced-mode: fake-ip
  fake-ip-range: 198.18.0.1/16
  default-nameserver:
    - 119.29.29.29
    - 223.5.5.5
  nameserver:
    - https://223.5.5.5/dns-query
    - https://1.12.12.12/dns-query
  fake-ip-filter:
    - "*.lan"
    - "*.localdomain"
    - "*.example"
    - "*.invalid"
    - "*.localhost"
```

```
    - "*.test"
    - "*.local"

proxies:
  - name: "Mein VMess-Proxy"
    type: vmess
    server: 54.254.0.0
    port: 1080
    uuid: "9f02f6b2-1d7d-4b10-aada-0000"
    alterId: 0
    cipher: "aes-128-gcm"
    udp: true

proxy-groups:
  - name: "Proxy"
    type: select
    proxies:
      - "My VMess Proxy"
```

rules: - IP-CIDR,192.168.0.0/16,DIRECT - IP-CIDR,10.0.0.0/8,DIRECT - IP-CIDR,127.0.0.0/8,DIRECT - GEOIP,CN,DIRECT - MATCH,Proxy

Hauptpunkte:
- Ports: Konfiguriert verschiedene Ports für HTTP, SOCKS und gemischten Datenverkehr.
- DNS: Richtet DNS-Einstellungen mit Fake-IP-Bereichen und spezifizierten Nameservern ein.
- Proxies: Definiert einen VMess-Proxy mit Verschlüsselung durch `aes-128-gcm`.
- Proxy-Gruppen: Ermöglicht die Auswahl zwischen verschiedenen Proxy-Optionen.
- Regeln: Leitet den Datenverkehr basierend auf IP-Bereichen und geografischen Standorten.

Hinweis: Stellen Sie sicher, dass der `cipher` in der Proxy-Konfiguration mit der `security`-Einstellung

---

Verwalten des V2Ray-Dienstes

Nach der Installation und Konfiguration müssen Sie den V2Ray-Dienst mit `systemctl` verwalten.

Aktivieren und Starten von V2Ray

V2Ray beim Systemstart aktivieren:

```bash
sudo systemctl enable v2ray
```

(Der Befehl bleibt auf Englisch, da es sich um einen systembasierten Befehl handelt, der nicht übersetzt wird.)

V2Ray-Dienst starten:

```
sudo systemctl start v2ray
```

Hinweis: Der Befehl bleibt auf Englisch, da es sich um einen technischen Befehl handelt, der in der Regel nicht übersetzt wird.

Erwartete Ausgabe:

```
Erstellter Symlink /etc/systemd/system/multi-user.target.wants/v2ray.service → /etc/systemd/system/v2ray
```

Überprüfen des Dienststatus:

```
sudo systemctl status v2ray
```

Beispielausgabe:

```
 v2ray.service - V2Ray-Dienst
   Geladen: geladen (/etc/systemd/system/v2ray.service; aktiviert; Hersteller-Voreinstellung: aktiviert)
   Aktiv: aktiv (laufend) seit Mo 2024-04-27 12:55:00 UTC; 1min 30s
Haupt-PID: 14425 (v2ray)
    Tasks: 8 (Limit: 4915)
   Speicher: 36,7M
   CGroup: /system.slice/v2ray.service
           14425 /usr/local/bin/v2ray run -config /usr/local/etc/v2ray/config.json
```

Häufige Probleme und Fehlerbehebung

Authentifizierungsfehler beim Aktivieren von V2Ray

Fehlermeldung:

```
==== AUTHENTIFIZIERUNG FÜR org.freedesktop.systemd1.manage-unit-files ====
Authentifizierung ist erforderlich, um Systemdienste oder Unit-Dateien zu verwalten.
Authentifizierung als: Ubuntu (ubuntu)
Passwort:
polkit-agent-helper-1: pam_authenticate fehlgeschlagen: Authentifizierung fehlgeschlagen
==== AUTHENTIFIZIERUNG FEHLGESCHLAGEN ====
Aktivierung der Unit fehlgeschlagen: Zugriff verweigert
```

Lösung:

Stellen Sie sicher, dass Sie `sudo` verwenden, um Befehle auszuführen, die administrative Berechtigungen erfordern.

Korrekte Befehlszeile:

```
sudo systemctl enable v2ray
```

Verifizierung

Nachdem Sie den V2Ray-Dienst gestartet haben, überprüfen Sie, ob er korrekt ausgeführt wird.

Laufende Prozesse überprüfen

```
ps aux | grep v2ray
```

Beispielausgabe:

```
nobody     14425  4.4  8.6 5460552 36736 ?       Ssl  12:55   0:00 /usr/local/bin/v2ray run -config /usr
ubuntu     14433  0.0  0.5   7076  2176 pts/1    S+   12:55   0:00 grep --color=auto v2ray
```

Konnektivität mit Telnet testen

```
telnet deine_server_ip 1080
```

Erwartetes Verhalten:

- Wenn die Verbindung erfolgreich ist, erhalten Sie eine Antwort vom V2Ray-Dienst.
- Um Telnet zu beenden, drücken Sie `Ctrl + ]` und geben Sie dann `quit` ein.

Fazit

Die Einrichtung von V2Ray auf einem Ubuntu-Server umfasst die Installation der Software, die Konfiguration der eingehenden und ausgehenden Einstellungen, die Verwaltung des Dienstes mit `systemctl` und die Überprüfung des Betriebs. Wenn Sie dieser Anleitung folgen, sollten Sie eine funktionierende V2Ray-Installation haben, die Ihre Netzwerkprivatsphäre verbessert und Einschränkungen effektiv umgeht.

Wenn Sie auf Probleme stoßen oder Fragen haben, können Sie gerne einen Kommentar hinterlassen!

Zusätzliche Tipps

- Sicherheit: Stellen Sie sicher, dass Ihre V2Ray-UUID und Passwörter stets sicher aufbewahrt werden.
- Updates: Aktualisieren Sie V2Ray regelmäßig, um von den neuesten Funktionen und Sicherheitsupdates zu profitieren.
- Überwachung: Nutzen Sie die Protokolle unter `/var/log/v2ray/`, um die Leistung zu überwachen und Probleme zu beheben.

Viel Spaß beim Proxying!