Prueba V2Ray: Una Guía Paso a Paso

V2Ray es una plataforma versátil para crear proxies que permiten sortear restricciones de red y mejorar la privacidad en línea. En esta guía, te guiaremos a través de la instalación y configuración de V2Ray en un servidor Ubuntu. Cubriremos los pasos de instalación, archivos de configuración, problemas comunes y métodos de verificación para asegurarnos de que todo funcione sin problemas.

Índice

Instalación

Comienza descargando e instalando V2Ray utilizando el script de instalación proporcionado.

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

Ejecuta el Script de Instalación:

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

Salida de Instalación:

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

info: V2Ray v5.22.0 está instalado.

Nota: El script sugiere eliminar software dependiente si es necesario:

```bash
apt purge curl unzip
```

Configuración

Configuración de V2Ray (`config.json`)

Este archivo JSON define las configuraciones de entrada y salida para 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"
    }
}
```

Puntos clave: - Inbounds: Define los puntos de entrada para las conexiones entrantes. Aquí, está configurado para usar el protocolo `vmess` en el puerto `1080`. - Outbounds: Especifica hacia dónde se debe enviar el tráfico. El protocolo `freedom` permite que el tráfico pase sin restricciones. - Logging: Configurado para registrar información de acceso y errores con fines de depuración. - Security: El campo `security` está configurado como `aes-256-gcm` para una encriptación mejorada.

Configuración del Proxy (`config.yaml`)

Este archivo YAML configura los ajustes de proxy, DNS y las reglas para el enrutamiento del tráfico.

```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: "Mi Proxy VMess"
```

```
    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
```

Puntos clave: - Puertos: Configura varios puertos para tráfico HTTP, SOCKS y mixto. - DNS: Configura ajustes de DNS con rangos de IP falsas y servidores de nombres especificados. - Proxies: Define un proxy VMess con cifrado utilizando `aes-128-gcm`. - Grupos de proxies: Permite la selección entre diferentes opciones de proxy. - Reglas: Dirige el tráfico según rangos de IP y ubicaciones geográficas.

Nota: Asegúrate de que el `cipher` en la configuración del proxy coincida con el ajuste de `security` en el `config.json`.

Gestión del Servicio V2Ray

V2Ray es una herramienta poderosa para la gestión de proxies y la protección de la privacidad. A continuación, se presentan algunos comandos útiles para gestionar el servicio V2Ray en tu sistema.

Iniciar el Servicio V2Ray

Para iniciar el servicio V2Ray, utiliza el siguiente comando:

```
sudo systemctl start v2ray
```

Detener el Servicio V2Ray

Si necesitas detener el servicio V2Ray, ejecuta:

```
sudo systemctl stop v2ray
```

Reiniciar el Servicio V2Ray

Para reiniciar el servicio V2Ray, utiliza:

```
sudo systemctl restart v2ray
```

Verificar el Estado del Servicio V2Ray

Puedes verificar el estado del servicio V2Ray con el siguiente comando:

```
sudo systemctl status v2ray
```

Habilitar el Servicio V2Ray para que se Inicie Automáticamente

Para asegurarte de que el servicio V2Ray se inicie automáticamente al arrancar el sistema, ejecuta:

```
sudo systemctl enable v2ray
```

Deshabilitar el Inicio Automático del Servicio V2Ray

Si deseas deshabilitar el inicio automático del servicio V2Ray, utiliza:

```
sudo systemctl disable v2ray
```

Ver los Registros del Servicio V2Ray

Para ver los registros del servicio V2Ray y diagnosticar posibles problemas, puedes usar:

```
sudo journalctl -u v2ray
```

Estos comandos te ayudarán a gestionar eficientemente el servicio V2Ray en tu sistema. ¡Asegúrate de utilizarlos según sea necesario!

Después de la instalación y configuración, necesitas gestionar el servicio de V2Ray utilizando `systemctl`.

Habilitando e Iniciando V2Ray

Habilitar V2Ray para Iniciar al Arranque:

```
sudo systemctl enable v2ray
```

Iniciar el Servicio de V2Ray:

```
sudo systemctl start v2ray
```

Salida Esperada:

```
Se creó un enlace simbólico /etc/systemd/system/multi-user.target.wants/v2ray.service → /etc/systemd/sy
```

Verificar el Estado del Servicio:

```
sudo systemctl status v2ray
```

Salida de ejemplo:

```
 v2ray.service - Servicio de V2Ray
   Cargado: cargado (/etc/systemd/system/v2ray.service; habilitado; predeterminado del proveedor: habili
   Activo: activo (en ejecución) desde Lun 2024-04-27 12:55:00 UTC; hace 1 minuto y 30 segundos
   PID Principal: 14425 (v2ray)
    Tareas: 8 (límite: 4915)
   Memoria: 36.7M
   CGroup: /system.slice/v2ray.service
           14425 /usr/local/bin/v2ray run -config /usr/local/etc/v2ray/config.json
```

Problemas comunes y solución de problemas

Fallo de Autenticación al Habilitar V2Ray

Mensaje de Error:

```
==== AUTENTICACIÓN PARA org.freedesktop.systemd1.manage-unit-files ====
Se requiere autenticación para gestionar archivos de servicios o unidades del sistema.
Autenticando como: Ubuntu (ubuntu)
Contraseña:
polkit-agent-helper-1: pam_authenticate falló: Error de autenticación
==== AUTENTICACIÓN FALLIDA ====
No se pudo habilitar la unidad: Acceso denegado
```

Solución:

Asegúrate de usar `sudo` para ejecutar comandos que requieran privilegios administrativos.

Comando Correcto:

```
sudo systemctl enable v2ray
```

Verificación

Después de iniciar el servicio V2Ray, verifica que esté funcionando correctamente.

Verificar Procesos en Ejecución

```
ps aux | grep v2ray
```

Nota: El comando anterior no necesita traducción, ya que es una instrucción en el lenguaje de programación Bash. Sin embargo, si necesitas una explicación en español, aquí está:

Este comando se utiliza para listar todos los procesos en ejecución y filtrar aquellos que contengan la palabra “v2ray”. `ps aux` muestra todos los procesos del sistema, y `grep v2ray` filtra los resultados para mostrar solo los procesos relacionados con “v2ray”.

Salida de ejemplo:

```
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
```

Probar la conectividad usando Telnet

```
telnet tu_ip_del_servidor 1080
```

Comportamiento Esperado:

- Si la conexión es exitosa, verás una respuesta del servicio V2Ray.
- Para salir de Telnet, presiona `Ctrl + ]` y luego escribe `quit`.

Conclusión

Configurar V2Ray en un servidor Ubuntu implica instalar el software, configurar los ajustes de entrada y salida, gestionar el servicio con `systemctl` y verificar su funcionamiento. Siguiendo esta guía, deberías tener una configuración funcional de V2Ray que mejore tu privacidad en la red y permita eludir restricciones de manera efectiva.

Si encuentras algún problema o tienes preguntas, ¡no dudes en dejar un comentario a continuación!

Consejos Adicionales

- Seguridad: Asegúrate siempre de que tu UUID de V2Ray y las contraseñas estén protegidas.
- Actualizaciones: Actualiza V2Ray regularmente para aprovechar las últimas funciones y parches de seguridad.
- Monitoreo: Utiliza los registros ubicados en `/var/log/v2ray/` para monitorear el rendimiento y solucionar problemas.

¡Feliz proxy!