

C2

Zumpyx

2026-04-18

C2 Listener Backend
 FOFA Shodan
 Redirector Nginx Caddy Web
 C2 mTLS TCP Web
 WireGuard “Disposable Front-Ends-> Hidden Listener” Caddy + Socat Web

 VPS-A
  VPS-B
  WireGuard
  C2
  VPS-C

名前	IP (内)	WireGuard 外 IP	接続先
VPS-A (東京)	192.0.2.1	10.8.0.2	Caddy (80/443 外 HTTP/HTTPS 内) Socat (8443 外 TCP/mTLS 内)
VPS-B (東京)	198.51.100.1	10.8.0.3	外 (接続先)
VPS-C (C2 東京)	外/内	10.8.0.1	C2 外 (内 8080/8443)

```
🔦 WireGuard wg genkey | tee  
privatekey | wg pubkey > publickey
```

WireGuard

XXXXXXXXXX C2 XXXXXXXX VPS-C XXXX WireGuard XXXXXXXX ServerXXXXXXXXXXXXXXXXXXXX

1. VPS-C (C2) WireGuard

```
XXXXXXXXXX/etc/wireguard/wg0.conf
```

[Interface]
Address = 10.8.0.1/24

Web Caddyfile

VPS-A VPS-B Caddy 10.8.0.1:8080

VPS-A / VPS-B /etc/caddy/Caddyfile

```
# VPS-A c2-primary.yourdomain.com / VPS-B c2-backup.yourdomain.com
c2-primary.yourdomain.com {
    tls your-email@example.com

    # C2 Profile / Profile Malleable
    @c2_paths path /api/v1/data* /static/assets/cache*
    handle @c2_paths {
        reverse_proxy 10.8.0.1:8080 {
            header_up Host {upstream_hostport}
            header_up X-Real-IP {remote_host}
            header_up X-Forwarded-For {remote_host}
        }
    }

    # 
    handle / {
        reverse_proxy https://news.ycombinator.com
    }
}
```

TCP Socat

C2 TLS TCP
Nginx/Caddy TLS

VPS-A / VPS-B Socat TCP TCP

```
nohup socat TCP4-LISTEN:8443,fork,reuseaddr TCP4:10.8.0.1:8443 > /dev/null
2>&1 &
```

* HTTPS VPS-A VPS-B 443 -> Caddy ->
Web 10.8.0.1:8080 * VPS-A VPS-B 8443 -> Socat ->
10.8.0.1:8443

“”

1. 在VPS-A上配置VPS-B的WireGuard配置
 2. 在VPS-A上配置VPS-B的IP地址和wg0.conf文件，并配置VPS-A的Peer和WireGuard的IP地址和Beacon
-

在VPS-A上

配置Bilibili的IP地址和Beacon

(Redirector) - Sliver C2 WireGuard Caddy Socat