2024-02-10 01:07:52 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBCInto your configuration and/or add BF-CBC to --data-ciphers.
2024-02-10 01:07:52 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data ch
annel offLoad.
2024-02-10 01:07:52 OpenVPN 2.6.7 aarch64-unknown-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [H/PKT
INFO] [AEAD] [DCO]
2024-02-10 01:07:52 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-02-10 01:07:52 DCO version: N/A
2024-02-10 01:07:52 TCP/UDP: Preserving recently used remote address: LAF_INET152.4.198.155:1194
2024-02-10 01:07:52 Socket Buffers: R=[212992212992] S=[212992→212992]lachine Inrormacio.
2024-02-10 01:07:52 UDPv4 Link local： （not bound）
2024-02-10 01:07:52 UDPy4 link remote: [AF
2024-02-10
_INET152.4.198.155:1194
01:07:52 TLS: Initial packet from [AF_INET152.4.198.155:1194, 510=207a951f b3707cle
2024-02-10
01:07:52 VERIFY OK: depth=1, CN=Changele
2024-02-10
01:07:52 VERIFY KU OK
2024-02-10 01:07:52 Validating certificate extended key usage
2024-02-10 01:07:52 # Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentic ation
2024-02-10 01:07:52 VERIFY EKU OK
2024-02-10 01:07:52 VERIFY OK: depth=®, CN=server
2024-02-10 01:07:52 Control Channel: TLSv1.3, cipher TLSv1.3 TLS.
_AES_256_GCM_SHA384, peer certificate: 2048 bits
RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-02-10 01:07:52 [server] Peer Connection Initiated with [AF_INET]52.4.198.155:1194
2024-02-10 01:07:52 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-02-10 01:07:52 TLS: ls_multi_process: initial untrusted session promoted to trusted
2024-02-10 01:07:53 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-02-10 01:07:53 PUSH: Received control message: 'PUSH_REPLY, route 10.10.0.0 255.255.0.0, route-metric 1000, ro ute-gateway 10.6.0.1, topology subnet, ping 5, ping-restart 120, ifconfig 10.6.2.229 255.255.128.0, peer-id 38'
2024-02-10 01:07:53 OPTIONS IMPORT：-ifconfig/up options modified
2024-02-10 01:07:53 OPTIONS IMPORT: route options modified

2024-02-10 01:07:53 OPTIONS IMPORT: route-related options modified
2024-02-10 01:07:53 Using peer cipher 'AES-256-CBC'
2024-02-10 01:07:53 net_route_v4_best gw query: dst 0.0.0.0
2024-02-10 01:07:53 net_route_v4.
_best_gw result: via 10.0.2.2 dev etho
2024-02-10 01:07:53 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth®
HWADDR=f6:43:5:03:2a: f4
2024-02-10 01:07:53 TUN/TAP device tune opened
Expires
1h 45m 30s
2024-02-10 01:07:53 net_iface_mtu_set: mtu 1500
1500 For tuno
2024-02-10 01:07:53 net_iface_up: set tun® up
2024-02-10 01:07:53 net_addr_V4_add: 10.6.2.229/17 dev tung
2024-02-10 01:07:53 net_route_v4_add: 10.10.0.0/16 via 10.6.0.1 dev [NULL] table ®
metric 1000
2024-02-10 01:07:53 Initialization Sequence Completed
2024-02-10 01:07:53 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 38
2024-02-10 01:07:53 Timers: ping 5, ping-restart 120
2024-02-10 01:07:53 Protocol options: explicit-exit-notify 3
*[*C2024-02-10 01:12:45 event_wait : Interrupted system call (fd=-1, code=4)
2024-02-10 01:12:45 SIGTERM received, sending exit notification to peer
2024-02-10 01:12:48 net_route_v4_del: 10.10.0.0/16 via 10.6.0.1 dev [NULL] table
0
metric 1000
2024-02-10 01:12:48 Closing TUN/TAP interface
2024-02-10 01:12:48 net_addr_v4_del: 10.6.2.229 dev tun®
2024-02-10 01:12:48 SIGTERM[soft, exit-with-notification] received, process