

Oct 19 00:01:13 dnsmasq-dhcp[10841]: DHCPREQUEST(br0) 192.168.2.13 f0:c8:50:c6:fd:26
yoran-huawai
Oct 19 00:01:13 dnsmasq-dhcp[10841]: DHCPREQUEST(br0) 192.168.2.13 f0:c8:50:c6:fd:26
Oct 19 00:01:13 dnsmasq-dhcp[10841]: DHCPACK(br0) 192.168.2.13 f0:c8:50:c6:fd:26
yoran-huawai
Oct 19 00:57:19 openvpn[10773]: TLS: tls_process: killed expiring key
Oct 19 00:57:20 openvpn[10773]: TLS: soft reset sec=0 bytes=263305/-1 pkts=1426/0
Oct 19 00:57:20 openvpn[10773]: VERIFY OK: depth=1, C=US, ST=CA, L=LosAngeles, O=Private
Internet Access, OU=Private Internet Access, CN=Private Internet Access, name=Private Internet
Access, emailAddress=secure@privateinternetaccess.com
Oct 19 00:57:20 openvpn[10773]: VERIFY OK: depth=0, C=US, ST=CA, L=LosAngeles, O=Private
Internet Access, OU=Private Internet Access, CN=860ca334e88ffde3c925a7f0598ee9bf,
name=860ca334e88ffde3c925a7f0598ee9bf
Oct 19 00:57:20 openvpn[10773]: WARNING: 'link-mtu' is used inconsistently, local='link-mtu 1558',
remote='link-mtu 1542'
Oct 19 00:57:20 openvpn[10773]: WARNING: 'cipher' is used inconsistently, local='cipher
AES-128-CBC', remote='cipher BF-CBC'
Oct 19 00:57:20 openvpn[10773]: Data Channel Encrypt: Cipher 'AES-128-CBC' initialized with 128
bit key
Oct 19 00:57:20 openvpn[10773]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for
HMAC authentication
Oct 19 00:57:20 openvpn[10773]: Data Channel Decrypt: Cipher 'AES-128-CBC' initialized with 128
bit key
Oct 19 00:57:20 openvpn[10773]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for
HMAC authentication
Oct 19 00:57:20 openvpn[10773]: Control Channel: TLSv1.2, cipher TLSv1/SSLv3
DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Oct 19 01:16:19 dnsmasq-dhcp[10841]: DHCPREQUEST(br0) 192.168.2.13 f0:c8:50:c6:fd:26
Oct 19 01:16:19 dnsmasq-dhcp[10841]: DHCPACK(br0) 192.168.2.13 f0:c8:50:c6:fd:26
yoran-huawai
Oct 19 01:16:19 dnsmasq-dhcp[10841]: DHCPREQUEST(br0) 192.168.2.13 f0:c8:50:c6:fd:26
Oct 19 01:16:19 dnsmasq-dhcp[10841]: DHCPACK(br0) 192.168.2.13 f0:c8:50:c6:fd:26
yoran-huawai
Oct 19 01:57:20 openvpn[10773]: TLS: soft reset sec=0 bytes=146198/-1 pkts=1171/0
Oct 19 01:57:37 openvpn[10773]: [860ca334e88ffde3c925a7f0598ee9bf] Inactivity timeout
(--ping-restart), restarting
Oct 19 01:57:37 openvpn[10773]: SIGUSR1[soft,ping-restart] received, process restarting
Oct 19 01:57:37 openvpn[10773]: Restart pause, 5 second(s)
Oct 19 01:57:42 openvpn[10773]: WARNING: No server certificate verification method has been
enabled. See <http://openvpn.net/howto.html#mitm> for more info.
Oct 19 01:57:42 openvpn[10773]: NOTE: the current --script-security setting may allow this
configuration to call user-defined scripts
Oct 19 01:57:42 openvpn[10773]: TCP/UDP: Preserving recently used remote address: [AF_INET]
46.166.190.194:1198
Oct 19 01:57:42 openvpn[10773]: Socket Buffers: R=[122880->122880] S=[122880->122880]
Oct 19 01:57:42 openvpn[10773]: UDP link local: (not bound)
Oct 19 01:57:42 openvpn[10773]: UDP link remote: [AF_INET]46.166.190.194:1198
Oct 19 01:57:42 openvpn[10773]: TLS: Initial packet from [AF_INET]46.166.190.194:1198,
sid=a4fe282b 8e9f2307
Oct 19 01:57:42 openvpn[10773]: VERIFY OK: depth=1, C=US, ST=CA, L=LosAngeles, O=Private
Internet Access, OU=Private Internet Access, CN=Private Internet Access, name=Private Internet
Access, emailAddress=secure@privateinternetaccess.com
Oct 19 01:57:42 openvpn[10773]: VERIFY OK: depth=0, C=US, ST=CA, L=LosAngeles, O=Private
Internet Access, OU=Private Internet Access, CN=860ca334e88ffde3c925a7f0598ee9bf,
name=860ca334e88ffde3c925a7f0598ee9bf
Oct 19 01:57:43 openvpn[10773]: WARNING: 'link-mtu' is used inconsistently, local='link-mtu 1558',
remote='link-mtu 1542'
Oct 19 01:57:43 openvpn[10773]: WARNING: 'cipher' is used inconsistently, local='cipher
AES-128-CBC', remote='cipher BF-CBC'
Oct 19 01:57:43 openvpn[10773]: Control Channel: TLSv1.2, cipher TLSv1/SSLv3
DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Oct 19 01:57:43 openvpn[10773]: [860ca334e88ffde3c925a7f0598ee9bf] Peer Connection Initiated
with [AF_INET]46.166.190.194:1198
Oct 19 01:57:44 openvpn[10773]: SENT CONTROL [860ca334e88ffde3c925a7f0598ee9bf]:
'PUSH_REQUEST' (status=1)
Oct 19 01:57:44 openvpn[10773]: AUTH: Received control message: AUTH_FAILED
Oct 19 01:57:44 openvpn[10773]: vpnrouting.sh tun11 1500 1622 10.31.10.6 10.31.10.5 init
Oct 19 01:57:44 openvpn-routing: Configuring policy rules for client 1
Oct 19 01:57:44 openvpn-routing: Flushing client routing table
Oct 19 01:57:44 openvpn-routing: Completed routing policy configuration for client 1
Oct 19 01:57:44 openvpn[10773]: /usr/sbin/ip route del 10.31.10.1/32
Oct 19 01:57:44 openvpn[10773]: /usr/sbin/ip route del 46.166.190.194/32
Oct 19 01:57:44 openvpn[10773]: /usr/sbin/ip route del 0.0.0.0/1
Oct 19 01:57:44 openvpn[10773]: /usr/sbin/ip route del 128.0.0.0/1
Oct 19 01:57:45 openvpn[10773]: Closing TUN/TAP interface
Oct 19 01:57:45 openvpn[10773]: /usr/sbin/ip addr del dev tun11 local 10.31.10.6 peer 10.31.10.5
Oct 19 01:57:45 openvpn[10773]: updown.sh tun11 1500 1622 10.31.10.6 10.31.10.5 init
Oct 19 01:57:46 rc_service: service 18388:notify_rc updatersolv
Oct 19 01:57:46 dnsmasq[10841]: read /etc/hosts - 5 addresses
Oct 19 01:57:46 dnsmasq[10841]: read /etc/hosts.dnsmasq - 13 addresses
Oct 19 01:57:46 dnsmasq-dhcp[10841]: read /etc/ethers - 13 addresses
Oct 19 01:57:46 dnsmasq[10841]: using nameserver 192.168.1.1#53 for domain lan
Oct 19 01:57:46 dnsmasq[10841]: using nameserver 192.168.1.1#53
Oct 19 01:57:46 openvpn[10773]: SIGTERM[soft,auth-failure] received, process exiting