SoftEther VPN

報告者：蘇己盛

日期：2014/08/05

/dev/net/tun not found

- # mkdir -p /dev/net
  # mknod /dev/net/tun c 10 200
  # chown root:root /dev/net/tun
  # chmod 600 /dev/net/tun
- http://amdm/LectureNotes/Diaries/Topic-OS-1-2013.html
  http://lxr.free-electrons.com/source/Documentation/devices.txt

110	28.826375006	192.168.180.40	192.168.180.41	TCP	74 443→38912 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5246337 TSecr=5725851 WS
111	28.826476006	192.168.180.41	192.168.180.40	TCP	66 38912→443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=5725851 TSecr=5246337
112	28.829423006	192.168.180.40	192.168.180.41	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113	28.829442006	192.168.180.40	192.168.180.41	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
114	28.829447006	192.168.180.40	192.168.180.41	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
115	28.829643006	192.168.180.41	192.168.180.40	ICMP	120 Destination unreachable (Port unreachable)
116	28.829667006	192.168.180.41	192.168.180.40	ICMP	120 Destination unreachable (Port unreachable)
117	28.829684006	192.168.180.41	192.168.180.40	ICMP	120 Destination unreachable (Port unreachable)
118	28.851131006	192.168.180.41	140.120.13.1	DNS	102 Standard query 0x01f3 A x1.x8.x7.x3.servers.nat-traversal.uxcom.jp
119	28.874170006	192.168.180.41	192.168.180.40	TLSv1	181 Client Hello
120	28.874774006	192.168.180.40	192.168.180.41	TCP	66 443→38912 [ACK] Seq=1 Ack=116 Win=14480 Len=0 TSval=5246349 TSecr=5725863
121	28.891541006	fe80::6ef0:49ff:feb0:a	ff02::fb	MDNS	108 Standard query 0x0000 PTR 255.180.168.192.in-addr.arpa, "QM" question
122	28.891784006	192.168.180.10	224.0.0.251	MDNS	88 Standard query 0x0000 PTR 255.180.168.192.in-addr.arpa, "QM" question
123	28.893726006	192.168.180.41	192.168.180.3	SSH	162 Server: Encrypted packet (len=96)
124	28.894195006	192.168.180.3	192.168.180.41	TCP	66 34602→22 [ACK] Seq=689 Ack=3633 Win=1444 Len=0 TSval=6390900 TSecr=5725868
125	28.895467006	140.120.13.1	192.168.180.41	DNS	267 Standard query response 0x01f3 A 130.158.6.110
126	28.896022006	192.168.180.41	130.158.6.110	UDP	293 Source port: 49005 Destination port: 5004
127	28.919790006	192.168.180.41	192.168.180.40	DNS	113 Standard query 0xcbd8 DNSKEY 1ec736d9[Malformed Packet]
128	28.920405006	192.168.180.40	192.168.180.41	ICMP	141 Destination unreachable (Port unreachable)
129	28.932627006	192.168.180.40	192.168.180.41	TLSv1	1022 Server Hello, Certificate, Server Hello Done
130	28.932862006	192.168.180.41	192.168.180.40	TCP	66 38912→443 [ACK] Seq=116 Ack=957 Win=16512 Len=0 TSval=5725878 TSecr=5246364
131	28.933488006	192.168.180.41	192.168.180.40	TLSv1	376 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
132	28.933950006	192.168.180.40	192.168.180.41	TCP	66 443→38912 [ACK] Seq=957 Ack=426 Win=15552 Len=0 TSval=5246364 TSecr=5725878
133	28.942100006	192.168.180.40	192.168.180.41	TLSv1	109 Change Cipher Spec, Encrypted Handshake Message
134	28.942823006	192.168.180.41	192.168.180.40	TLSv1	357 Application Data

When a VPN client connect to server

TCP 443 (https)

TLSv1

41	1.812782000	192.168.180.41	173.194.72.94	TCP	54 48221→443 [ACK] Seq=1 Ack=1 Win=14600 Len=0
42	1.813089000	192.168.180.41	173.194.72.94	TLSv1.2	400 Client Hello
43	1.813977000	173.194.72.105	192.168.180.41	TCP	60 443→44825 [ACK] Seq=4318 Ack=724 Win=42880 Len=0
44	1.844690000	173.194.72.94	192.168.180.41	TCP	60 443→48221 [ACK] Seq=1 Ack=347 Win=42880 Len=0
45	1.846335000	173.194.72.94	192.168.180.41	TLSv1.2	1484 Server Hello
46	1.846361000	173.194.72.94	192.168.180.41	TCP	1484 [TCP segment of a reassembled PDU]
47	1.846366000	173.194.72.94	192.168.180.41	TLSv1.2	724 Certificate
48	1.846626000	192.168.180.41	173.194.72.94	TCP	54 48221→443 [ACK] Seq=347 Ack=1431 Win=17464 Len=0
49	1.846653000	192.168.180.41	173.194.72.94	TCP	54 48221→443 [ACK] Seq=347 Ack=2861 Win=20320 Len=0
50	1.846667000	192.168.180.41	173.194.72.94	TCP	54 48221→443 [ACK] Seq=347 Ack=3531 Win=23184 Len=0
51	1.849266000	192.168.180.41	173.194.72.94	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
52	1.881431000	173.194.72.94	192.168.180.41	TLSv1.2	300 New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
53	1.882191000	192.168.180.41	173.194.72.94	TLSv1.2	592 Application Data
54	1.882228000	192.168.180.41	192.168.180.3	SSH	178 Server: Encrypted packet (len=112)
55	1.882492000	192.168.180.3	192.168.180.41	TCP	66 34602→22 [ACK] Seq=49 Ack=529 Win=1444 Len=0 TSval=6784435 TSecr=6119403
56	1.954143000	173.194.72.94	192.168.180.41	TLSv1.2	1470 Application Data
57	1.954171000	173.194.72.94	192.168.180.41	TLSv1.2	1470 Application Data
58	1.954176000	173.194.72.94	192.168.180.41	TLSv1.2	1470 Application Data
59	1.954181000	173.194.72.94	192.168.180.41	TLSv1.2	1470 Application Data
60	1.954186000	173.194.72.94	192.168.180.41	TLSv1.2	1470 Application Data

Connect to https://www.google.com

TCP 443 (https)
TLSv1.2

```
506 798.543959 192.168.180.40   140.120.13.1     DNS      96 Standard query 0xc432  AAAA x4.x9.x8.xe.servers-v6.ddns.uxcom.jp
507 798.545484 140.120.13.1     192.168.180.40   DNS     273 Standard query response 0xc432  AAAA 2001:240:140a:1::10
508 798.546407 192.168.180.40   140.120.13.1     DNS      96 Standard query 0x6327  A x4.x9.x8.xe.servers-v6.ddns.uxcom.jp
509 798.547215 140.120.13.1     192.168.180.40   DNS     167 Standard query response 0x6327
510 798.547556 192.168.180.40   140.120.13.1     DNS      96 Standard query 0x782b  A x4.x9.x8.xe.servers-v6.ddns.uxcom.jp
511 798.548216 140.120.13.1     192.168.180.40   DNS     167 Standard query response 0x782b
512 800.169384 192.168.180.40   130.158.6.113    UDP      43 Source port: 61922  Destination port: avt-profile-1
513 800.216130 130.158.6.113    192.168.180.40   UDP      70 Source port: avt-profile-1  Destination port: 61922
```

When a VPN server start

DNS request servers-v6.ddns.uxcom.jp

8097	1519.79663	192.168.180.41	192.168.180.40	TLSv1	471	Application Data
8098	1519.79696	192.168.180.40	192.168.180.41	TCP	66	https > 38869 [ACK] Seq=75421 Ack=72239 Win=5281 Len=0 TSval=4543310 TSecr=5022810
8099	1519.79713	192.168.180.40	192.168.180.41	UDP	125	Source port: safetynetp Destination port: 50857
8100	1520.05393	192.168.180.40	192.168.180.41	TLSv1	272	Application Data
8101	1520.05441	192.168.180.41	192.168.180.40	TLSv1	487	Application Data
8102	1520.05444	192.168.180.41	192.168.180.40	TCP	66	38869 > https [ACK] Seq=72239 Ack=75627 Win=5281 Len=0 TSval=5022874 TSecr=4543374
8103	1520.05461	192.168.180.40	192.168.180.41	TCP	66	https > 38866 [ACK] Seq=72988 Ack=73894 Win=5281 Len=0 TSval=4543374 TSecr=5022874
8104	1520.54012	192.168.180.41	192.168.180.40	UDP	131	Source port: 50857 Destination port: safetynetp
8105	1520.54014	192.168.180.41	192.168.180.40	UDP	210	Source port: 50857 Destination port: safetynetp
8106	1520.54058	192.168.180.40	192.168.180.41	UDP	135	Source port: safetynetp Destination port: 50857
8107	1521.56672	192.168.180.40	192.168.180.41	UDP	123	Source port: safetynetp Destination port: 50857
8108	1521.56677	192.168.180.41	192.168.180.40	UDP	118	Source port: 50857 Destination port: safetynetp
8109	1522.03870	192.168.180.40	130.158.6.113	UDP	43	Source port: 61922 Destination port: avt-profile-1
8110	1522.08686	130.158.6.113	192.168.180.40	UDP	70	Source port: avt-profile-1 Destination port: 61922
8111	1522.33641	192.168.180.41	192.168.180.40	UDP	127	Source port: 50857 Destination port: safetynetp
8112	1522.33675	192.168.180.40	192.168.180.41	UDP	109	Source port: safetynetp Destination port: 50857
8113	1523.10666	192.168.180.41	192.168.180.40	UDP	130	Source port: 50857 Destination port: safetynetp
8114	1523.61991	192.168.180.40	192.168.180.41	UDP	132	Source port: safetynetp Destination port: 50857
8115	1523.73564	192.168.180.40	192.168.180.41	UDP	216	Source port: safetynetp Destination port: 50857
8116	1523.73654	192.168.180.41	192.168.180.40	UDP	213	Source port: 50857 Destination port: safetynetp

During VPN client connection

UDP safetynetp (port 40000)

SafetyNET p

- **SafetyNET p** is a standard for Ethernet-based fieldbus communication in automation technology.

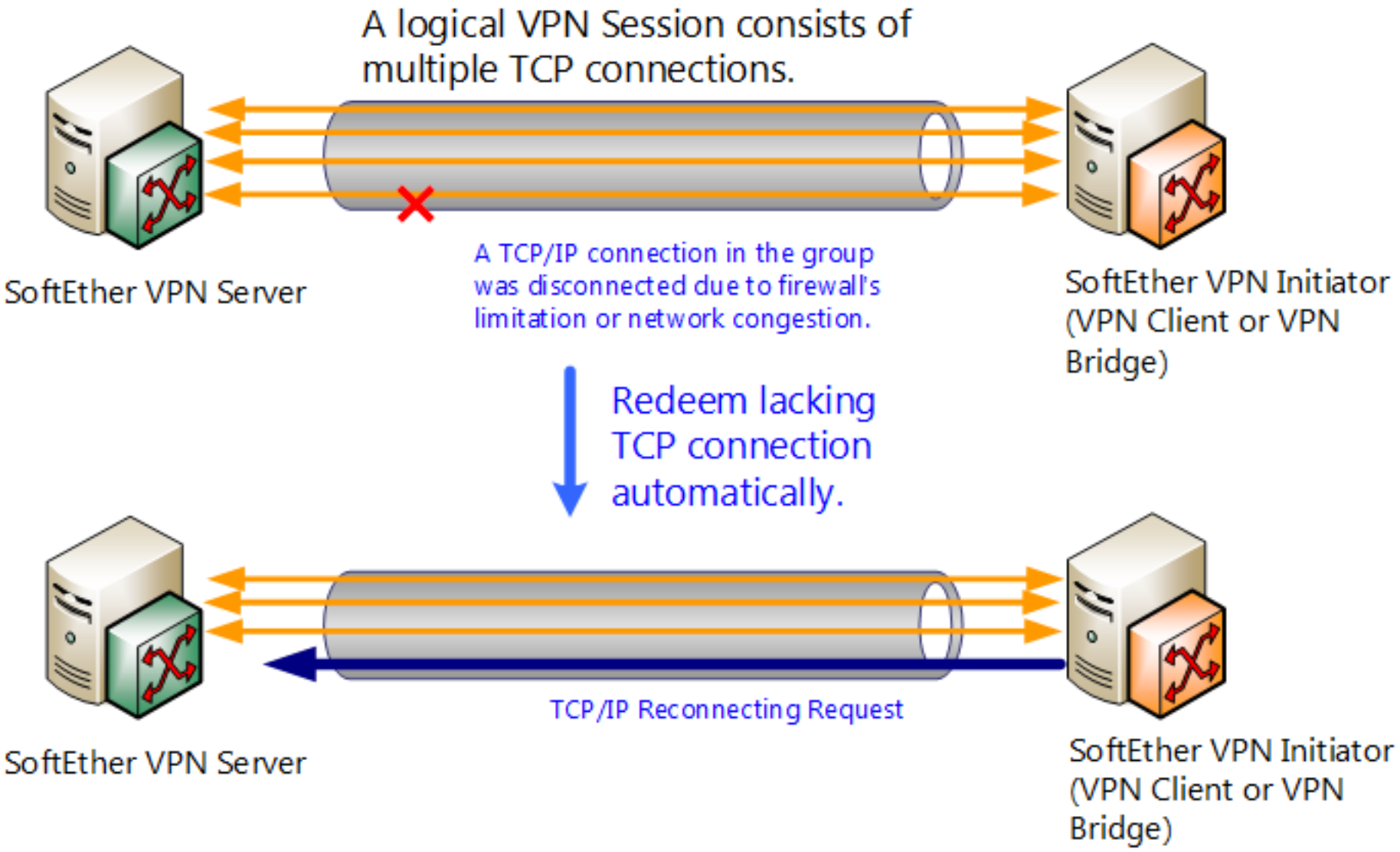
Drop port=40000

- src port 40000 -> drop
  $ sudo ovs-ofctl add-flow brLAN "table=0,udp,tp_src=40000,action=drop"
- dst port 40000 -> drop
  $ sudo ovs-ofctl add-flow brLAN "table=0,udp,tp_dst=40000,action=drop"
- Delete all flows and add initial flow
  $ sudo ovs-ofctl del-flows brLAN ; sudo ovs-ofctl add-flow brLAN "table=0,priority=0,action=normal"

Session type	Reconnection interval	Number of reconnection attempts
Ordinary VPN sessions initiated by VPN Client	Min. 5 seconds (default is 15 seconds)	0 – unlimited (default is unlimited)
Cascade connection VPN sessions initiated by VPN Server / VPN Bridge	10 seconds (fixed)	Unlimited (fixed)

Reconnection Setting when VPN Connection Fails or Becomes Disconnected during Communications

VPN session type, reconnection interval, number of reconnection attempts that can be set and the default settings



Automatic reconnection processing if disconnected while using multiple TCP/IP connections.