DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600
800.432.2638 Toll Free
217.897.1331 Fax
www.dcbnet.com

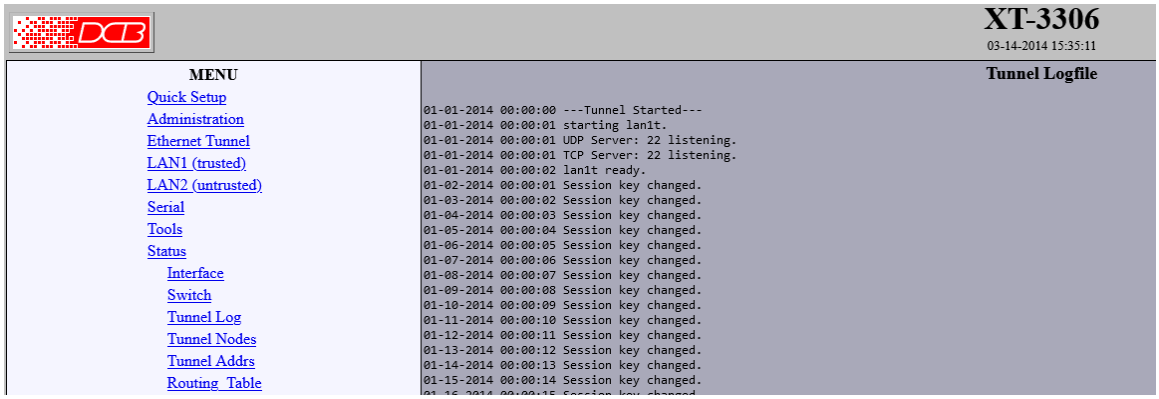
DATA COMM FOR BUSINESS

What Are Those Tunnel Log Entries? Should I be worried?

10/09/2023

When analyzing the logs from DCB Tunnels (XT, UT, and ET; the FT logs are more complicated, but similar) there are often log entries that are surprising to the new user. We'll discuss some of these here.

This is what a relatively empty tunnel log looks like on the server unit with no remote connections:



It shows that the tunnel started, a LAN interface was started, and the unit is listening for UDP and TCP connections, then the LAN interface is ready for connections. Later on it shows that the session key was changed. If it was set up to only connect with UDP, then there would be no TCP server listening; if configured for TCP only, there would be no UDP sever listening.

Normal activity shows up similar to the entries on this log:

```
04-23-2023 01:04:19 Session key changed.
04-24-2023 01:04:20 Session key changed.
04-24-2023 18:17:03 Marking connection with jmccain as inactive
04-24-2023 18:18:42 jmccain connected from address 98.177.116.228:57651
04-24-2023 18:18:42 Marking connection with jmccain as active
04-24-2023 18:18:56 jmccain connected from address 166.170.46.227:4056
04-25-2023 01:04:21 Session key changed.
04-26-2023 01:04:22 Session key changed.
04-26-2023 10:54:10 Marking connection with jmccain as inactive
04-26-2023 11:04:01 awhite connected from address 72.26.186.183:55423
04-26-2023 11:08:52 Marking connection with awhite as inactive
04-27-2023 01:04:23 Session key changed.
04-27-2023 10:53:25 Closing connection with jmccain due to inactivity
04-27-2023 10:53:26 Removing Client jmccain
04-27-2023 11:08:07 Closing connection with awhite due to inactivity
04-27-2023 11:08:08 Removing Client awhite
04-28-2023 01:04:24 Session key changed.
04-29-2023 01:04:25 Session key changed.
04-30-2023 01:04:26 Session key changed.
04-30-2023 14:03:57 jmccain connected from address 98.177.116.228:50450
05-01-2023 01:04:27 Session key changed.
05-02-2023 01:04:28 Session key changed.
```

This log snippit shows new remote connections, sessions marked as inactive (which conserves system resources), client connections removed, etc. Entries include the date/time stamp, action, client name, and originating IP address and originating port number.

DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600
800.432.2638 Toll Free
217.897.1331 Fax
www.dcbnet.com

Log entries that concern many people are connection attempts from unrecognized IP addresses. The log below shows a number of refused connection entries. When a tunnel is port scanned, it's passphrase or shared secret is incorrect, or an unknown client tries to connect, it denies the connection. If the denial is from a known client because of passphrase or shared secret mismatch, then a client name is listed, if the client doesn't pass the first authentication phase, then it shows "unknown client name".

When TCP mode is enabled and the unit is getting port scanned, the more common error messages will be similar to one of the following:

Remote 192.168.2.82:36774 connected
Connection 192.168.2.82:36774 terminated

Or

Remote 192.168.2.82:36774 connected
Connection 192.168.2.82:36774 terminated - bad packet

In both cases the connection is being quickly terminated. The is because the server attempts to decrypt the packet and there is either insufficient data or the data does not pass the validation test.

A "connection denied" error message will only occur when the "shared secret" is correct. So this error message is unlikely to occur as the result of a port-scan. In most cases, the user has the shared secret correct but has an error in the user's name or passphrase.

07-10-2023 17:00:45

Tunnel Logfile

```
07-10-2023 01:57:27 166.137.106.48:48572 connection denied, - unknown client name.
07-10-2023 01:59:56 166.137.106.48:20742 connection denied, - unknown client name.
07-10-2023 02:02:00 166.137.106.48:21219 connection denied, - unknown client name.
07-10-2023 02:04:14 166.137.106.48:48427 connection denied, - unknown client name.
07-10-2023 02:06:09 166.137.106.48:33290 connection denied, - unknown client name.
07-10-2023 02:08:42 166.137.106.48:63471 connection denied, - unknown client name.
07-10-2023 02:11:08 166.137.106.48:38753 connection denied, - unknown client name.
07-10-2023 02:12:58 166.137.106.48:5165 connection denied, - unknown client name.
07-10-2023 02:15:08 166.137.106.48:62197 connection denied, - unknown client name.
07-10-2023 02:17:27 166.137.106.48:24306 connection denied, - unknown client name.
07-10-2023 02:19:33 166.137.106.48:44290 connection denied, - unknown client name.
07-10-2023 02:22:00 166.137.106.48:25502 connection denied, - unknown client name.
```

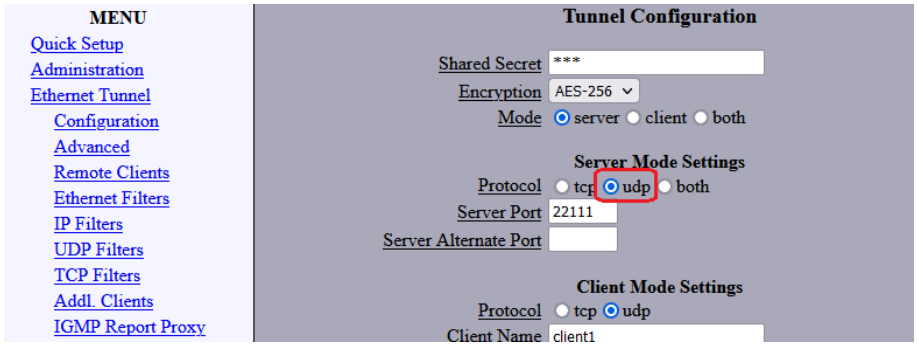
There are a number of other anomalies that are logged, and most are self explanatory, such as switching to a backup or primary path, out of sequence packets, etc.

There are several ways to minimize these log entries. If connections are not from one of your client devices, then it is likely due to port scanning or SSH intrusion attempts. Are your clients connecting in UDP mode or TCP mode? If all your clients are connecting in UDP mode, we recommend disabling TCP support in the server. Doing so will eliminate these connection attempts. **UDP mode will not respond to port scanning and appears as a "black hole" to the scanning device.** This is configured on the Tunnel Configuration screen.

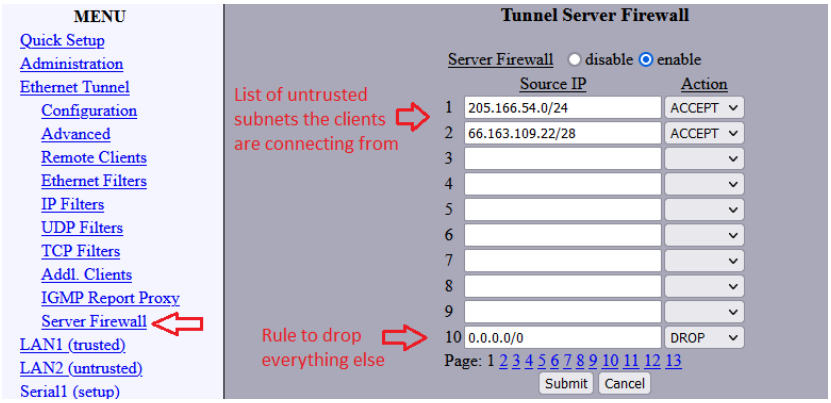
DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600
800.432.2638 Toll Free
217.897.1331 Fax
www.dcbnet.com

DATA COMM FOR BUSINESS



If you need to use TCP mode, then we recommend that the server port be set to use a non-standard port number. For example, instead of port 22 use port 22111. High number ports are less likely to be scanned. If the client devices are connecting from known network subnets, we might also recommend using the "Ethernet Tunnel – Firewall" option on the server to limit access from the subnets that the client devices reside on. Below is an example:



Another method to minimize these might be to place a firewall between the untrusted interface and the Internet. Similar to using the tunnel's built-in server firewall, but a purpose built firewall might have more fine grained filtering options.

The white paper "UT Tunnel Installation Note - "Living On a Wild Feed... Safely" is worth reading. This short application note summarizes the options and requirements for directly connecting the untrusted interface of encrypted tunnels to the Internet. Yes, the tunnels may be safely living on the wild side of your firewalls and if properly configured appear to be a "black hole" to your adversaries!

Another white paper, "Tunnel Product Security In Perspective" is a must-read.
Our encrypted tunnel appliances provides a LAN -to- LAN encrypted tunnel between locations. It employs a layer three (UDP/IP or TCP/IP) connection between two or more tunnel devices to create a secure, AES encrypted tunnel.

Download these and other application notes from this link:
https://www.dcbnet.com/datasheet/xtfamilyds.html#application