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

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

Single-Ended Installation of DCB Encrypted Tunnels

DCB's encrypted tunnel devices are available in several variations:

- ET family, using TCP/IP transport and AES encryption
- UT family, using UDP/IP transport and AES encryption
- XT family, using either TCP or UDP transport, and AES encryption
- FT family, using either TCP or UDP transport, and FIPS encryption

It is desirable to change the security level model a bit in some installations and run the tunnel in a “single-ended” mode. The tunnel is normally installed in-line between the secured LAN and the unsecured gateway router to the other site, with the tunnel being the only device that touches both the secure and insecure LAN segments. In some smaller applications, this installation model doesn’t fit well with the available network topology.

The tunnel device may be installed in these applications by using it as a single-ended bridge. That is, only one ethernet connection is used to connect the tunnel device to the LAN. There are security implications of using this method, but the security and bridging is sufficient in many cases.

The method is simple. Do not enable the “LAN2” (and “LAN3” on certain models) ethernet port(s) on the tunnel device. If those ports are left disabled, all connectivity is provided through the “LAN1” port, and the encrypted connection to the other tunnel device is via this same path. In addition, the “**Gateway**” field of the “LAN1” configuration must contain the IP address of the local gateway router to allow a path to the external network.

The tunnel devices at either the remote, host, or both may be used in this manner. Figure 1 below diagrams such an arrangement, with sample LAN addresses shown.

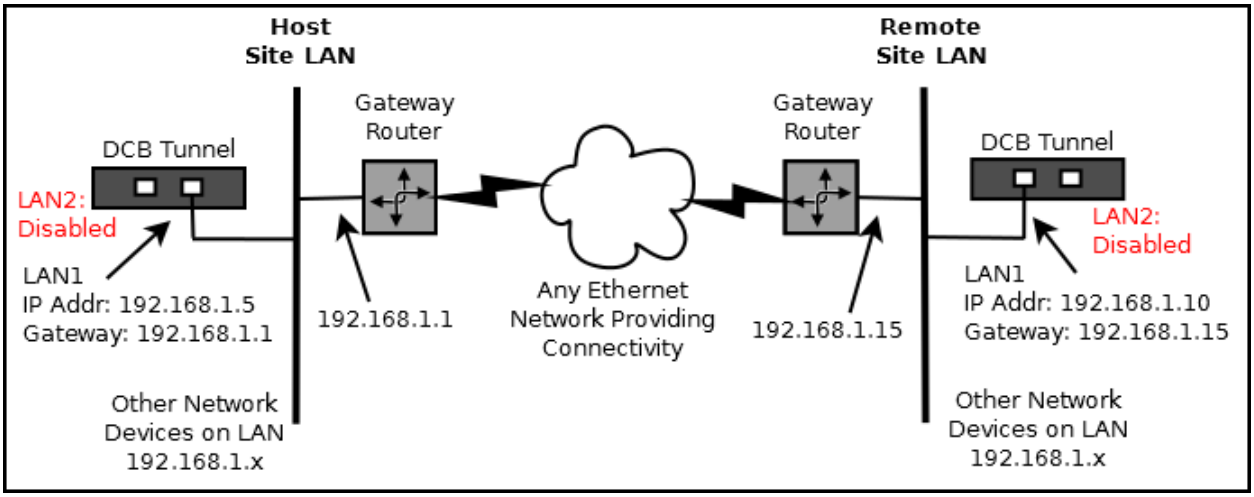

Figure 1: Example of Single-Ended Installation, Both Host and Remote Sites

This method does lower the security somewhat by transporting the encrypted packets on the same ethernet wire as the clear information. In strict secure installations, this is never allowed, as an attacker's job is easier if he can compare plain text to encrypted text. In most installations, where bridging functionality is the most important feature, and the encryption is only a modest requirement, this should not provide a weakness that is easily exploitable: Remember, the attack still must break the AES or FIPS encryption to extract keys, and the session keys are automatically changed periodically.

The most significant security weakness this method provides is allowing the secure LAN segment to be visible to the gateway router. That opens up the tunnel device's management port to an insecure path. If this method is used, set up "**Access Control**" under "**Administration**" to limit IP addresses to those on the local network.

If the tunnel device is used strictly for bridging without encryption as in many applications, there is no down side to using this method. The tunnel device is used in this manner to provide a bridged link to a few nodes in a "foreign" network without having to be involved with the foreign network's configuration.

Since this method works well with ad-hoc networks and small office installations, it may be used at the remote offices while the more common "in-the-path" method is used at the host site.

Configuration Hints for Single-Ended Installation:

1. Use only the "LAN1" port. "LAN2" (and "LAN3" if applicable) should be disabled.
2. On the "LAN1" screen, fill-in the **Gateway** field, which is left blank for the more common "in-the-path" topology.
3. For ET family devices, Enable "**TCP No Delay**" in the "**Ethernet Tunnel ->Advanced"** configuration screen (this is the default).