DATA COMM FOR BUSINESS

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

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

UT Product Security
In Perspective

Overview:

The UT series of encrypted tunnel appliances provides a LAN -to- LAN encrypted tunnel between locations. It employs a layer three (UDP/IP) connection between two or more UT devices to create a secure, AES encrypted tunnel. For export purposes, the UT is considered a Mass Market Encryption Device by the Department of State Bureau of Industrial Security and is export limited

The UT product line meets HIPPA and most government standards for non-classified data transfer. It is not NIST FIPS 140-2 approved. For a FIPS 140 approved product, the (more expensive) FT line of encryption appliances is required.

DCB encryption products are in use by most federal government agencies including all branches of the armed forces, DHS, CDC, FBI, NPS, Border Patrol, National Laboratories, DOE, DOS, and others. They are in use by many state government agencies for law enforcement, fire service, and other life-critical areas. They are used by state law enforcement to meet the FBI's encryption requirements for communicating NCIC information and PSAP communications. One of the most common applications is in protecting US critical infrastructure. These meet US NERC-CIPS requirements and are in use by our largest power companies, as well as other critical utilities such as water, waste water, oil and gas pipeline, and transportation industries.

How it works:

While extensive filtering is available, the tunnel typically transports all specified valid ethernet packets between locations. Technically, it functions as a “learning bridge”. Viewing the packet stream data in transit shows only an encrypted stream of seemingly random bytes. Workstations with data flowing in the tunnel can not view anything on the transit networks.

When a client unit powers up, it attempts to create a tunnel with a server unit. This begins with a secure two-way handshake exchange to validate both the server and client, followed by establishment and transfer of session encryption keys. Periodically, new session keys are renegotiated. If the intermediate path is interrupted, a new connection is immediately attempted, and there is a protocol for back-up connections, re-connection, and such.

Since the tunnel transports all valid ethernet packets, multicast as well as non-routable ethernet packets are able to be transported via the tunnel over layer three networks such as the Internet or corporate networks, that don't provide for non-routable or multicast packets. Commonly used frames that are difficult to use with routers and other security devices, such as SIP, RTCP, and RTSP, are handled as well. No intermediate network re-configuration is required to transport these within a tunnel.. the transporting network only sees a single encrypted UDP/IP data stream.

DATA COMM FOR BUSINESS

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

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

How secure is it?

Although no security product is perfect, and all may be breached eventually if attacked by a powerful enough adversary, we began manufacturing the UT in 2008 and to our knowledge have never experienced an attacker breach a configured UT tunnel. The UT is used by virtually every US government agency and in critical infrastructure applications. Many of these customers regularly scan the devices and use red team attack consultants and auditors.

The tunnel is normally encrypted using AES-256, the current US government standard encryption method.

The encrypt/decrypt bulk encryption keys are generated randomly from ANSI x9.31 Appendix A.2.4 section 3 RNG. The shared secret the user enters is not actually used for bulk encryption, it's the seed that we use to derive session keys. Those keys are derived using a public domain algorithm detailed in RFC 2898. The UT runs at least 1000 iterations of that algorithm to generate the real-time session keys.

DCB does not publish scan results of penetration audits. Customers are encouraged to share their red team results with us, and we can explain any false positive hits that a scan reports. The UT also contains a built-in port audit tool that lists all ports with internet connections with and without server processes, protocol, Rx and Tx, local address and foreign address.

The UT should be a "black hole" when viewed from the Internet side. If its untrusted port is the only connection to the Internet from your local network, then all your devices that are connected to the secure port are inaccessible to and from the internet. They will not be able to connect to the Internet, nor will any Internet devices be able to connect to them.

The untrusted port of a properly configured UT will ONLY communicate with another UT that's configured as one of its partners. The UT's cryptographically authenticate with each other, establish session keys, and establish the tunnel. No other traffic is allowed into the UT or out of the untrusted port if it is properly configured.

DATA COMM FOR BUSINESS

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

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

Increasing UT network security, “Best Practices”:

Proper configuration and network design is necessary to maintain resiliency of a UT network. To maintain the hardness of the UT, a few common sense steps are always advised. Remember that the easiest way to view data on the trusted side of the UT is to have access to the trusted LAN that is independent of the UT. The UT can provide a trusted tunnel to another site, filter what goes through that tunnel, and prevent nefarious packets from crossing the tunnel, it has no control on the rest of a site's LAN.

While most customers prefer minimal configuration on the UT, and that is adequate for the vast majority of installations, we recommend some common, simple steps to increase security.

Always use a complex secure shared secret. The secret may be up to 51 characters in length and may contain any printable ASCII characters except for quote or backslash characters.

If a UT is connected directly to the Internet on its untrusted port, (the most common installation method) and not through some other filtering firewall, we suggest the following configuration steps to maintain adequate security:

Disable ping response.

Enable Remote Syslog to monitor the system. (and monitor the syslog)

Regularly check the “Audit Ports” status screen.

Use a tagged VLAN for management access that is separate from other VLANs.

Use the extensive filtering... Ethernet, IP, UDP, TCP filtering rules.

Disable untrusted ports that aren’t needed.

By default, the configuration or administration interface is restricted to access from the trusted LAN ports. **We recommend not changing that operation.**

However, if you require administration access via the untrusted port, use the following configurations to better protect the administration interface of the UT.

Enable web server port 443 instead of port 80 to force HTTPS instead of HTTP. For more obscurity, use some other random port, noting that you'll have to enter that port number (eg. :5432) in the HTTPS address.

Use a complex and unique password for each unit. Make them as long as possible to complicate brute force attacks.

DATA COMM FOR BUSINESS

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

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

Configure "Accepted Web IP Source Addresses" in the Admin Access Control. This will only allow admin from pre-defined IP address or subnets.

If you are more concerned, enable the optional higher security authentication method with password rules, aging, auto time-out. Note that this greatly complicates the access as it enables session timeouts and requires a user to re-enter their credentials in a long session. It also enables password rules (length, characters, aging, etc). This is a bit of trouble for the technicians, but may be required in some high security installations (critical infrastructure protection sites).

If you are even more concerned, you can **generate web certificates and require web browser authentication via certificates.** This is rarely used due to the complexity, even in more secure installations.