

Secure Console Communication Using the Virtual Command Center

Executive Summary

The Virtual Command Center (VCC) offers secure console communication, today, using Global Maintech's EBus cards on secured private networks. When console traffic must pass over insecure networks like the Internet, it is possible to use encrypted Virtual Private Networks or VPNs to communicate with EBus cards.

In addition, there are several alternatives available that will allow the use of state of the art, secure communication with VCC and without EBus cards. All require some effort by the customer. Conversion of an existing VCC installation to a secure communication environment can be accomplished incrementally with minimal interruption of the existing system.

Unfortunately, our software-only customers have been using telnet to communicate with their servers. While Telnet is widespread, it is an inherently insecure protocol. Recognizing this fact, Global Maintech is planning on making the secure shell or SSH protocol available on Linux VCC. However, no firm deadline has been set for completion.

Alternatives

There are both hardware and software alternatives available. If desired, the alternatives can coexist with each other, as well as with the current VCC software-only environment.

Hardware - EBus Cards

Of course the easiest solution is to deploy EBus cards to control the consoles. Using these cards, servers can be booted and controlled in every facet of their operation. To insure security, EBus cards are deployed on secure private networks, separated from other internal networks by VCC servers. If these cards must be accessible from insecure networks, VPNs are employed. EBus cards provide the highest level of security and are the solution of choice for Global Maintech's customers, including large banks, insurance companies and utilities where security is of paramount concern. They are available for both the Alpha and Linux VCC systems.

This is not a complete discussion of the features and advantages of EBus cards, however. If you are interested in EBus cards, please contact Global Maintech.

Software

There are two software solutions available. One is stunnel and the other is SSH. These are available with Linux VCC out of the box. Both are also available for the Tru64 UNIX 4.0D and 5.1 from The Written Word <<http://www.thewrittenword.com>>. Since they are both open source, each can also be installed on Tru64 UNIX by building the packages

from source. Customers should be aware that building and installing these packages requires the installation of several other open source packages.

stunnel

The stunnel package <<http://www.stunnel.org>> is an open source package that uses the open source OpenSSL package to encrypt older non-encrypted protocols using state of the art encryption. Instead of telnetting from the VCC server to port 23 on server1, a user would telnet to an arbitrary unused port such as 12345 on localhost, 127.0.0.1. The stunnel daemon would be watching port 12345 on local host. Based on its configuration file, know that port 12345 indicated a telnet session to server1. On server1, the stunnel daemon would decrypt the data stream and pass it to port 23 on localhost. Additional ports must be designated in the stunnel configuration file for each server the VCC wishes to connect to, in effect substituting an unused local port number for an IP address. For example, server2 might be port 13241, etc.

The VCC system.cfg file allows telnet terminals to be defined specifying both IP address and port number. For stunnel, all IP addresses would be localhost and each console would be defined specifying a separate, unused, port. Of course the stunnel configuration file must be maintained.

SSH

The most commonly used secure console protocol in the industry today is SSH. OpenSSH <<http://www.openssh.org>> uses the OpenSSL, also. It provides an analog to telnet, using state of the art encryption. In addition, it provides a host of other features that will not be discussed in this document.

To use SSH with VCC, specify telnet terminals that contact localhost. Then have operations personnel enter the command “ssh operator@server1”, where operator is the user name being logged in and server1 is server being contacted. They will be prompted for a password or pass phrase, depending on how ssh is configured on the server. In fact due to ssh’s features, even the password/phrase can be bypassed.

Conclusion

Secure communication with server consoles is available via EBus cards, stunnel and SSH. SSH is in the Linux VCC development plans. Global Maintech personnel are available to assist in your upgrade planning, deployment and maintenance phases. Arrangements can be made to try out the EBus solution on a limited basis.