Digi TransPort CIP Best Practices Guide

Contents

1. Abstract and Introduction

This document outlines configuring Digi TransPort routers to adhere to NERC CIP security requirements. These settings are based on real world configurations observed at electric utilities, discussions with their security consultants and reviewing the CIP standards.

These major Digi TransPort features should be configured for security and monitoring the router:

- Configure and enable the stateful inspection (SPI) firewall on WAN interfaces
- Use encryption and authentication via IPsec VPN, SSL, SSH, SFTP and/or X.509 certificates
- Segment the network via VLAN or Ethernet port isolation as needed
- Configure user accounts, admin levels and remote authentication (RADIUS / TACACS+)
- Monitor and manage the router via SNMP v3 and/or Digi remote management platforms
- Log events can be stored via Syslog; including event alarm support via SNMP, email and/or SMS.

Notes

- This document is based on CIP Version 5 regulations which may be modified or sections never ratified. Please verify the applicable regulations as needed.
- Digi TransPort settings are based on firmware version 52xx. Device configuration settings are subject to change.
- This document does not apply to Digi TransPort WR21 “Standard” version which does not provide stateful firewall or VPN.

- Wi-Fi is an option on some TransPort models, but is not covered in this document since it is rarely, if ever, used in environments where CIP rules apply. However, since Wi-Fi uses Ethernet instances, the same Ethernet rules apply to Wi-Fi, in addition to advanced Wi-Fi specific security such as WPA2 Enterprise.

Disclaimer

This document was written as a guide to aid the user in configuring the Digi TransPort router. Digi makes no claims these instructions will guarantee the Digi TransPort, attached network and/or devices will pass a CIP audit.

Corrections and Suggestions:

We welcome your feedback. Please send any feedback to info@digi.com or call us at 952-912-3444.

2. CIP Regulations

This document is functionally organized for configuration of the Digi TransPort router based on these CIP regulations (with links to the appropriate sections):

CIP REG	Function	TransPort Function/Configuration
CIP-001-1a	Sabotage reporting	Logging and Alarming
CIP-002-5	Reporting and categorization	Applies to procedures, not configuration
CIP-003-5	Security management controls	Outlines the rest of the CIP requirements and who manages what
CIP-004-5	User access to systems; monitoring and logging of access	- RADIUS and TACACS+ - Event logging and syslog
CIP-005-5	Electronic Security Perimeter(s) – access control and alarming	- Firewall - Dial up security - Logging and alarming (unauthorized access) - Port isolation / VLAN - SSH, SSL - VPN (encryption) - RADIUS/TACACS+ (two factor authentication)
CIP-006-5	Physical Security of BES Cyber Systems	- Digital IO on some Digi TransPort models can be used to trigger an alarm and log access, for example when a control panel door is opened, to enhance CIP required physical security. (Hardware details are not covered in this document; alarm functionality is listed under CIP-005; please contact Digi for further details). - IP-based surveillance cameras are also commonly used and access can be routed over Digi TransPort routers.

CIP REG	Function	TransPort Function/Configuration
CIP-007-5	System Security Management	- Disable / Block unused ports/services (Firewall and Network Services) - Block / disable unused Ethernet, serial, USB, etc. ports - Patch Management: sign up for alerts from Digi - Event and Firewall Logging - Alarming - User accounts (change default passwords, enforce difficult passwords, force password changes; track user levels and accounts)
CIP-008-5	Incident Reporting and Response Planning	- Retain security logs: Can be obtained via syslog
CIP-009-5	Recovery Plans for BES Cyber Systems	- Maintain backup of TransPort router configurations - Keep history of event logs that can help diagnose changes to router configs or improper access - Document firewall rules with "#" notes and document configurations
CIP-010-1	Configuration Change Management and Vulnerability Assessments	- Retain and review configurations and firmware version - Configuration changes are logged and can generate alarms
CIP-011-1	Information Protection	- Retain logs and configurations - Have copies of Digi TransPort documentation, including this document, available for training purposes - Document firewall rules with "#" notes and document configurations

3. Digi TransPort Documentation and Support Links

Digi TransPort documentation is available on Digi's support site at http://www.digi.com/support/. Simply select the Digi model or enter part of the name into the keyword window (e.g., "WR21") and click on the Documentation link. Pertinent docs are:

- *Digi TransPort User Guide* – the primary product manual; applies to all TransPort models
- Install and Quick Start Guides – to help you get started with setup
- Application and Quick Notes – specific instructions for tasks such as VPN config
- Knowledgebase Articles – tech notes that cover items not in an application note

Most documents are available in PDF format and can be downloaded and saved for future reference. Copies of the Digi TransPort User Guide and Install Guide are the most critical to have available.

CLI commands can be cross-referenced at the end of each functional section of the *Digi TransPort User Guide*; simply search the User Guide PDF using the info below to find the appropriate setup information.

4. Firewall

The Digi TransPort has a flexible and powerful stateful inspection firewall. Beyond just security needs, the TransPort firewall can perform port and address translation as well as re-direct traffic for WAN failover where firewall rules are used to test the health of the primary WAN connection and then redirect that traffic via another interface. The Firewall can be enabled on *any* IP interface, normally the mobile PPP interface (ppp 1 in most cases), but also on Ethernet and GRE tunnel interfaces.

Enable Firewall

Enable the Firewall on the appropriate interface(s). This most commonly will be the mobile (PPP 1) interface. Ethernet port(s) can be used as WAN port connected to a satellite, WiMAX, DSL or other non-secure modem connection.

> *Configuration - Security* > *Firewall and select the applicable interfaces.*

Firewall Config File - fw.txt

The TransPort firewall is contained in the *fw.txt* file. A sample *fw.txt* is included on TransPort. This default file will allow all outbound traffic, and block all but inbound management and IPSec traffic.

Comments are preceded with "#" and should be included to document rules. *fw.txt* can be edited using a text editor, then copied via FTP, Remote Manager or Device Cloud to the TransPort. It can also be edited in the WebUI via:

> *Configuration - Security* > *Firewall*

The WebUI editor provides basic syntax checking and is helpful for troubleshooting. A *hit counter* is listed in the first column and is used to verify which rules are being hit. The "log" option will log hits in the *fwlog.txt* file viewable via

> *Management - Network Status* > *Firewall Trace*

Configuration - Security > Firewall > Stateful Inspection Settings allow adjustment to timers and other SPI settings. Changes to these settings are rarely needed.

Firewall Rules and Syntax

As with any proper firewall, the *default* action is to *block* traffic. When the firewall is enabled on an interface all traffic is blocked unless rules are added to pass traffic.

Digi TransPort firewall rules can *log* when a rule is hit. Normally only exceptions are logged. The default firewall loaded on TransPort has a last rule, "block log break end," which essentially is there to do just that: log any traffic that does not match a rule into the Firewall Trace (remember: the default is to block, so while this rule isn't necessary, it's there so you can see the hit counter and log as needed).

Here are a few sample rules. This rule allows outbound traffic as well as the replies back in:

```
pass out break end inspect-state
```

- **pass**: Allow the traffic out
- **out**: The traffic is outbound. The direction is important
- **inspect-state**: This enables stateful-inspection on this rule to allow replies to this specific IP stream back into the TransPort.
- **break end**: If the rule matches, stop processing and go to the end of the rule-set

This is a rule to detect masquerading.

```
block in log syslog break end on ppp 1 from 192.168.1.0/16 to any
```

Here the local network is 192.168.1.0/16. Any packets received on PPP 1 (the cellular WAN connection) masquerading to be on the local network (i.e., from 192.168.1.0) are blocked and the attempt is logged into the local firewall trace and to a Syslog server.

The rule broken down is:

- **block**: Block the traffic
- **in**: The traffic is inbound
- **log syslog**: Log this to the Event Log and Syslog (can optionally set an alarm)
- **break end**: If the rule matches, stop processing and go to the end of the rule-set
- **on ppp 1**: The traffic is coming in on interface ppp 1 (i.e., a WAN interface)
- **from 192.168.1.0/16**: This is the masqueraded source address
- **to any**: The packet is destined for any address

The firewall can also translate and forward inbound traffic as one would do with NAT port-forwarding (which is also supported, but the firewall provides more power and flexibility). This rule would take in-bound DNP traffic from an application using port 5000 (rather than the normal 20000) and forward it to an Ethernet-connected device (meter, recloser, etc) that can only listen on port 20000:

```
pass in break end proto tcp from any to addr-ppp 1 port=5000 -> to
192.168.1.101 port=20000
```

Broken down (in addition to the info above):

- **proto tcp & port=5000**: This is inbound TCP traffic on port 5000
- **from any**: The source could be from anywhere. You can be granular here for more security; e.g., "from 10.1.2.3" or "from 10.1.2.0/24"
- **to addr-ppp 1**: The traffic's destination IP address is ppp 1 (i.e., the cellular WAN interface)
- **-> to 192.168.1.101 port=20000**: The "->" symbol used with the "to" verb tells the TransPort to forward the traffic to 192.168.1.101 and translate the TCP port to 20000

The TransPort firewall can also be used to test traffic and mark an interface Out-of-Service (OOS); this is primarily used in problem detection and failover scenarios.

Details on configuring firewall rules are in the *Digi TransPort User Guide* "FIREWALL SCRIPTS" section.

5. Port Isolation, VLAN and DMZ

The built-in Ethernet switch on the four- and two-port TransPort models provide easy segmentation for up to four distinct and separate physical Ethernet networks. This is called “Port Isolate” mode.

In Port Isolate mode the router will only respond to its Ethernet 0 IP address on physical port “LAN 0”, its Ethernet 1 IP address on physical port “LAN 1”, etc. The router will not respond to its Ethernet 1 address on port “LAN 0” unless routing has been configured appropriately via *Configuration - Network > IP Routing/Forwarding > Static Routes*.

Configure Port Isolate vs. Hub Mode via:

> *Configuration – Network > Interfaces > Ethernet > Advanced*

Changing this setting requires a reboot of the router. This setting is sticky to the Ethernet switch, not stored in the default config.da0 file; resetting to factory does not clear this setting.

One or more of these networks can be designated as a DMZ where the TransPort’s routing and firewall can segregate and direct traffic as required.

Hub Groups allow groups of Ethernet ports to be grouped, yet still remain segregated from other ports. Hub Groups provide something similar to a hybrid between Port Isolate and Hub Mode.

VLAN tagging is supported for network segmentation when using Ethernet Hub Mode or only one Ethernet port present. VLAN tagging prevents traffic from one VLAN being visible on another VLAN.

> *Configuration - Interfaces > Ethernet > ETH n > VLANs*

6. Users, User Access to the Router, and Passwords

The default username and password should be changed from the default.

Multiple users can be configured on the Digi TransPort with various access levels (including Read-Only).

RADIUS and TACACS+ are supported and recommended for login authentication, password control and are generally required for two-factor authentication.

Configuration is via:

> *Configuration – Security > Users > User n*
> *Configuration – Security > RADIUS*
> *Configuration – Security > TACACS+*

X.509 certificates are supported for SSH, SSL and HTTPS authentication.

> *Administration > X.509 Certificate Management*

User administrative access to the Digi TransPort is available via several methods:

- WebUI via HTTP or HTTPS. This is an either/or setting (meaning HTTP or HTTPS but not both) via *Configuration - Network > Network Services*
- Command Line (CLI) via serial port, Telnet or SSH.
    - By default the serial port is available for login to the CLI. Serial Port access can be disabled via *Configuration - Network > Interfaces > Serial > Serial Port n.* Access to serial devices, e.g.: recloser, meter, etc. can be configured as needed and to prevent user login access via the serial port.
    - Telnet server cannot be specifically disabled, however Telnet over SSL can be selected via *Configuration - Network > Network Services* and/or Telnet access can be blocked via the firewall.
    - SSH is configurable via *Configuration - Network > SSH Server*; including the ability to use ports other than 22.
- Alternate ports: The TransPort listens on normal service ports (22, 23, 80, etc) as well at 8000 + the normal service port; e.g., 8022, 8023, 8080, 8443.
- Pre- and post-login banners for Telnet and SSH are configurable via *Configuration – Systems> General*

Users and User Passwords can be changed via *Configuration – Security> Users> User n*. RADIUS and TACACS+ can also be used for password and third-party token authentication. Hashed passwords are stored in the **pwds.da0** file in the TransPort's file system.

Remote Administrative access (i.e. via WAN port) to the TransPort can be completely *disabled* via the "nocfg" option applied to PPP or ETH WAN interfaces via the CLI command:

```
eth|ppp n nocfg 0|1|2|3
```

Where 0 = No restrictions; 1 = Disable management; 2 = Disable return; RST 3 = Disable management and return RST. For example to completely hide the mobile, PPP 1 interface:

```
ppp 1 nocfg 3
```

See the *Digi TransPort User Guide* for full details.

7. Dial-Up Security

While rarely used today, there are still occasions when a dial-up/out (POTS) modem might still be used. Some TransPort models support external modems via serial port while others have an embedded POTS modem. There are generally two modes of operation for dial-up modems: CLI access to the TransPort itself and PPP over serial for IP routing.

User Access to TransPort Itself

Similar to connecting directly to the serial port, the TransPort provides various ways to control access. See the sections in this document on securing user access to the serial port for details.

PPP via Dial-up Modem

Many security options exist to secure PPP access. PAP, CHAP, RADIUS and options to allow answering based on caller-ID. The dial-in PPP instance is normally PPP 0, depending on device configuration.

Configuration - Network > Interfaces > Advanced > PPP 0 and *> Advanced* and *> PPP Negotiation*

8. VPN and Encryption

IPsec ESP and SSL are provided on Digi TransPort to protect and authenticate data transmission and access to the router. 3DES and AES encryption up to 256 bits and SHA-1 authentication hash algorithm are supported; AES 192 or 256 and SHA1 are recommended. X.509 digital certificates and SCEP can be used for authentication. X-Auth and ModeCFG are also supported if the TransPort is required to behave as a "VPN Client".

IPSec or OpenVPN SSL may be required even when using private carrier plans to further protect the traffic over the air and through the carrier's network.

Access to serial devices such as PLCs, RTUs and meters connected to Digi TransPort or other Digi device serial ports can be encrypted by several methods:

- IPSec VPN or OpenVPN (application will access serial devices via LAN port IP address, not the mobile IP address)
- SSL or SSH tunneling (assuming the head-end application supports SSL or SSH)
- Encrypted RealPort, Digi's COM port re-director driver

Configuration:

Configuration – Network > Virtual Private Networking (VPN) > IPsec *
Configuration – Security> Users> User n (for peer IDs and pre-shared keys) *
Configuration – Network > Virtual Private Networking (VPN) > OpenVPN
Configuration – Network > SSL
Configuration - Network > Interfaces > Serial > RealPort
Administration > X.509 Certificate Management

(* A LAN-to-LAN IPSec wizard is available via the Wizards menu and is recommended for first time VPN setup.)

9. Logging and Alarms: Track and monitor access

Digi TransPort's Event Log tracks access and changes to the device. The Event Log can be replicated to Syslog. Event logging and alarms are fully configurable via the Event Handler so that some events can be logged while others are omitted. For example, logging of user access and changes is needed but not ADSL or cellular events. The event log file is "eventlog.txt" and can be viewed manually or via

Management – Event Log

Events, such as user login failures, can be configured to raise alarms via the Event Handler. Alarms, which also create Event Log entries, can be sent via email, SNMP and SMS text messages (when SMS is supported by the carrier plan and/or device):

Configuration – Alarms

Firewall hits can be logged by adding the "log" and/or "syslog" option to a rule. These log entries are stored in the "fwlog.txt" file and viewable via the WebUI:

Management-Network Status > Firewall Trace

See the "Firewall Scripts" section of the *TransPort User Guide* for more detail.

10. Time Synchronization

Time synchronization is supported via NTP or SNTP.

Configuration – System > Date and Time

SNTP is recommended where acceptable since NTP updates very frequently and can create excess data usage. If the TransPort is being used as a backup router, and NTP is required, NTP traffic can be routed over the primary link by adding a static route to the NTP server to the TransPort's routing table.

GPS can also be used as a time source on TransPort modules that support GPS.

11. Secure Direct Access to the Digi TransPort Router Itself

Block access to unused Ethernet ports

Unused Ethernet port access can be blocked physically and/or logically. Physical access can be accomplished by locking the TransPort inside a cabinet and/or via Ethernet RJ45 physical port locks. These physical locks are available via third parties.

Logical ways to block access are:

- Assign a blank address to the Ethernet port(s). This only works when the Ethernet switch is in Port Isolation mode or the unit has only one physical Ethernet port.
  NOTE: The Digi TransPort supports Logical Ethernet instances: *Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces.* Make sure no logical interfaces have IP addresses assigned.
  Port Isolate Mode: *Configuration – Network > Interfaces > Ethernet > Advanced*
  Assign IP address: *Configuration - Interfaces > Ethernet > ETH n*
- Disable DHCP Server for that Ethernet port
  Configuration – Network > DHCP Server > DHCP Server for Ethernet n

- Use the Firewall to block access; see Firewall section above for details
  Configuration - Interfaces > Ethernet > ETH n > Advanced

Restrict Access to Ethernet port(s)

To allow and control traffic to Ethernet ports use the following settings:

Disable DHCP Server

Disabling the DHCP server will require the user know the appropriate IP address settings to connect and communicate.

Configuration – Network > DHCP Server > DHCP Server for Ethernet n

Use Uncommon IP address

Standard IP addresses such as the default 192.168.1.1 are easy to guess. Use IP addresses that are rarely used and harder to guess. Combine this with disabling the DHCP server.

Configuration - Interfaces > Ethernet > ETH n

Use MAC Filtering

MAC Filtering can restrict access to known host PCs and other devices based on their Ethernet MAC addresses.

Configuration - Interfaces > Ethernet > ETH n > MAC Filtering

Disable / Block Unused Services and Change Service Ports

Generally secure access to a router for configuration is via HTTPS, SSH and SFTP (i.e., FTP over SSH). Most services can be disabled via:

Configuration - Network > Network Services

The WebUI will respond to HTTP or HTTPS but not both. Checking "Enable Secure Web Server (HTTPS)" disables HTTP access.

The firewall can block or translate any service port.

Note also the TransPort will listen on most common ports + 8000. For example the TransPort will respond on port 443 and 8443 when the Secure Web Server is enabled.

The following default services are available on most TransPort models:

Service	Default Port	Notes /Comments
Telnet	23 / 8023	TransPort will also respond on 8023.
Telnet over SSL	992	
WEB (HTTP)	80 / 8080	WebUI uses either HTTP or HTTPS but not both. TransPort will also respond on 8080.
Secure WEB (HTTPS)	443 / 8443	WebUI uses either HTTP or HTTPS but not both. TransPort will also respond on 8443.
SSH / SFTP	22 / 8022 (configurable)	TransPort will also respond on 8022.

Service	Default Port	Notes /Comments
SNMP	161 (configurable)	SNMPv1, SNMPv2c and SNMPv3 can be individually enabled or disabled
RealPort	771 (configurable)	Digi's COM port redirector protocol (works with Digi's RealPort driver)
Encrypted RealPort	1027 (configurable)	
SNTP Server	123	Typically used when the time source is GPS and the TransPort is acting a time server to a connected device
DHCP Server	67	
DNS Server	53	
FTP Server	21	
Serial port access	4000 + Serial port #	Terminal server functionality (can be changed)
SSL Server serial port access	4200 + serial port #	Terminal server functionality
XOT	1998	X.25 over TCP
ADDP	2362	Digi device discovery protocol
Device Cloud client connection	3197 / 3199	3199 is SSL. Device Cloud connections are device initiated and are only used when Device Cloud is enabled
Modbus	502	Typically used if the TransPort is acting as a Modbus TCP master to a Modbus serial slave.

Disable USB port

The USB port can be used to load or copy configuration and other files, or can be used for extra storage for logging. The USB port can be restricted or disabled via

Configuration - Security > System

Disable or Restrict Serial Port Access

By default the serial port provides access to the command line interface. It also supports reverse telnet (e.g. TCP/UDP socket) connections. The serial port (asy 0) can be disabled via:

Configuration - Network > Interfaces > Serial > Serial Port 0

Further control is available via:

Configuration - System > General> Web / Command Line Interface

Pre- and Post-login Banners

Login banners can be created to be displayed when logging into the CLI.

Configuration - System > General

Use a text editor to create the banner files. Copy the file(s) to the TransPort via FTP.

NOTE: TransPort file names must be 12 characters or less (e.g., 8.3 format). A couple of example file names: `banrpre.txt` and `banrpst.txt`

12. Connection Persistence, Failover and Recovery

In many cases the TransPort will be used for WAN Failover via cellular for a wired or wireless primary network. The TransPort supports various mechanisms for WAN failover and for maintaining and monitoring cellular connection persistence.

Failover between Two or More Routers

When used in conjunction with a primary WAN router, the TransPort supports Virtual Router Redundancy Protocol, a Digi extension to VRRP called VRRP+, and IP routing metrics and dynamic protocols such as OSPF and BGP.

VRRP and VRRP+

Virtual Redundancy Router Protocol is an IETF standard that provides backup for two or more routers defined in a group. Standard VRRP is setup via

Configuration - Interfaces > Ethernet > ETH n > VRRP

VRRP+ uses standard VRRP, but takes it a step further by generating probes *from* the TransPort out via the primary router to a remote host. This goes beyond standard VRRP by testing routing beyond the local WAN link.

See the Digi TransPort User Guide and Application Note 031: Virtual Router Redundancy Protocol (VRRP) and VRRP+.

Failover via IP Routing

If the primary router does not support VRRP or network design does not allow for VRRP, then IP routing functions can be used – either via static or dynamic (BGP, OSPF, etc.) routing. Floating static routes are commonly used to say "the primary route is no longer available; here is a higher-metric route" which points to the TransPort's LAN port. TransPort routes can be marked out-of-service (OOS) by various functions such as dynamically marking routes OOS when interfaces are not available or via the firewall's ability to test traffic and mark interfaces OOS.

Interfaces can be monitored actively by traffic generation from the TransPort itself or passively by monitoring traffic via the firewall. See:

- *Configuration - Network > IP Routing/Forwarding*
- Route and inactivity settings on individual interfaces (e.g., "Put this interface 'Out of Service' when an always-on connection attempt fails")
- Firewall

Cellular WAN Reliability, SureLink and SIM/APN Failover

The first and most important aspect for reliable cellular communications is signal quality. The use of proper antennas and cabling is imperative. Digi TransPort routers provide external antenna connectors to allow for any type of external antennas.

In cases where signal or network issues occur the Digi TransPort has several mechanisms to detect and repair the wireless WAN (cellular) connection. By default the mobile IP session, which uses PPP, is configured to be always on, and to reattempt the connection if lost. Some carriers have timers that will sever the mobile PPP session after a few hours of inactivity; others will drop the connection once per day for billing purposes. Check with your carrier for details. In either case, if the TransPort will attempt to reestablish the connection if it senses the loss.

If the PPP connection fails, by default the TransPort will power-cycle the embedded modem after 10 failed connection attempts. This setting is adjustable. There is also an option to reboot the Digi TransPort itself after a user definable number of failed connection attempts.

Further link integrity monitoring is recommended to test and repair the mobile PPP session. The easiest way to configure connection persistence is via the *SureLink* Wizard built into the WebUI. The TransPort can generate traffic via pings or UDP echo to monitor return traffic. It can also use passive techniques via the Firewall. Manual settings can be adjusted via the PPP n advanced settings and via the Firewall.

Wizards > SureLink Wizard
Configuration – Network > Interfaces > Mobile > Advanced
Configuration – Network > Interfaces > Advanced > PPP n > Advanced

GSM and LTE connections can be made more robust via SIM (most TransPort routers have two SIM slots) and/or APN failover. SIM failover is easily setup via the *SIM Failover Wizard* shown under Mobile Settings > SIM selection. APN backup is handled in the Mobile settings page.

Wizards > SureLink Wizard
Configuration – Network > Interfaces > Mobile > Advanced

Refer to the applicable Digi TransPort docs, specifically "AN007: Wireless - Wide Area Network (W-WAN) Problem Detection and Recovery" and the "SIM failover" documents on the Digi TransPort support page at www.digi.com/support.

13. Backup, Restore and Storage of TransPort Configuration

CIP 009 states to secure and synchronize router configuration files. There are several mechanisms available to backup device configurations. It is important to understand the TransPort's file system and which files should be backed up.

Configuration Files:

- config.da0: primary config file (config.da1 can also be used for alternate configuration)
- pwds.da0: obfuscated passwords file
- fw.txt: firewall
- sregs.dat: serial port config if changed from default
- x3prof: X.25 PAD profile (rarely used)
- logcodes.dif: Event handler logcodes updates; may or may not be present

These files can be saved off in a number of ways.

- The easiest is via the WebUI: *Administration > Backup/Restore* utility. All selected files are stored in Zip format for easy storage and restoration to this same or different unit.
- FTP the files off using an FTP client
- Save the files via WebUI: *Administration > File Management > FLASH directory*
- Copy the files to a USB storage device (U:)
- Use a remote management platform such as Device Cloud by Etherios or Digi Remote Manager which can save configs, restore them and do other system maintenance on scheduled basis.

Digi's Remote Manager is a user-installed and maintained Windows application. It can be used to store and compare configuration files. Third party applications can be used to analyze and compare the Digi TransPort's text-based configuration files. The Event Log can be configured to send an alert if changes are made or when someone logs into the TransPort to help further secure the TransPort's configuration. See http://www.digi.com/products/cloud/digi-remote-manager for details.

Device Cloud by Etherios (a division of Digi International) is a cloud-based service that offers device management without the hassle of installing or maintaining software and hardware to manage the devices. A secure SSL connection on TCP port 3199 is initiated from the device into the Device Cloud. See http://www.digi.com/products/cloud/digi-device-cloud.

Please contact Digi sales for more details on Remote Manager and Device Cloud by Etherios.

14. Cellular Carrier Plans and Cellular RF Security

Cellular Plan IP Addressing and Secure Connectivity Options

Work with your carrier to obtain a plan that meets your security needs and your budget. A wireless WAN provider may offer plans that greatly enhance security. Here are three carrier-related options that can help with securing data traffic across the Wireless WAN:

1. Use a plan that blocks some or all traffic into the mobile (i.e., cellular) network. For example, some carriers have plans which allow only remote initiated traffic; firewalls inside the carrier network block any unsolicited inbound traffic. However, this type plan cannot be used if your application requires you to reach out to the remote site to for example poll an RTU (some carriers call this mobile terminated data) unless IPsec VPN is initiated *from* the mobile device.

2. Use a completely private plan. Here, the carrier supplies a direct connection into your network via MPLS or IPsec VPN. In many cases, private IP addresses can be assigned to the Digi TransPort's mobile interface and controlled by you, the customer; and the data never touches the Internet.

3. Use dynamic mobile IP addresses but not use Dynamic DNS. This, however, will likely restrict your application to only outbound initiated connections or require the use of VPN.

(A side benefit to 1 and 2 above is these plans also block any unwanted billable traffic and can therefore save money in the long-run. Any connection attempt that traverses the wireless carrier network to the mobile IP address can be viewed as billable traffic, even if the mobile device blocks the connection attempt.)

RF (Radio Frequency) and Modem Security

How the Device is Identified and Authenticated

Depending on the wireless technology used (meaning GSM vs. CDMA vs. LTE) and the carrier, there are several ways the Digi cellular device is identified and authenticated on the cellular network.

GSM and LTE devices use a SIM (Subscriber Identity Module) which is typically the first level of identification to the network. The modem's IMEI or MEID (i.e., the modem serial number) can also be used to identify the device. Other information such as plan/APN name, username and password may also be required and are configured in the mobile settings on the Digi device.

CDMA (1xRTT/EvDO) modems do not use a SIM (at least in most of the world). Instead they are identified on the network by the modem's electronic serial number (ESN or MEID) and possibly additional information such as service programming code or master subsidy lock (SPC/MSL), username, and password.

Over the Air (OTA) Security

The link between the embedded modem and the cellular base station (tower), and possibly farther into the wireless carrier network, is encoded. Different carriers and technologies use various types and levels of encoding, typically 128-bit or greater for 3G devices. Frequency and code hopping also make it virtually impossible to eavesdrop on a cellular connection (expect potentially the NSA).

Check with your carrier for specifics on what security mechanisms they employ.

15. Patch Management – Firmware Updates

The TransPort's operating system, SarOS, is proprietary. Security patches are rarely needed. Digi does regularly update device firmware to add features and provide bug fixes.

The current firmware version is listed via *Administration - System Information* or the "id" command. For example this is version 5176:

```
Firmware Version:   5176 $ (May 7 2013 13:52:43)
```

Digi TransPort firmware updates and releases notes are available at no charge from our support site, www.digi.com/support. Your Digi sales person can setup proactive updates to alert you when new firmware is released.

Firmware can be updated via the WebUI, Device Cloud or Remote Manager.

The firmware update process automatically scans the files and does a checksum on the files as they are loaded. The file system can also be manually checked using the "scanr" CLI command.

16. Restrict Physical Access to Router

This requirement depends heavily on the user being sensible about placement of network devices.

The first thought is to lock the Digi router in the wiring closet, back office or secure enclosure. This makes sense from a physical security perspective, but not always from an RF signal perspective when using a cellular data network. One must weigh placing the Digi router where it gets good signal vs. placing it in a more secure location and possibly having to run antenna coax cables to external antennas.

Mounting inside metal cabinets presents similar challenges and external antennas are usually required except in some cases where plastic or fiberglass enclosures are used.

Keep a list of MAC and IP addresses, MEIDs/ESNs/IMEIs, SIM IDs and associated phone numbers so that devices can be disabled by the carrier in the event of theft.

Antenna security is also important. When necessary, mount external antennas securely to prevent theft and weather damage. Non-obtrusive, low-profile antennas are available from various sources.

In cases where the Digi router is in a visible location, physical access to the router can be minimized. First, the serial console port(s) can be disabled to prevent unauthorized local access. Firewall and/or MAC filtering can be configured to make any unused Ethernet ports inaccessible except for allowed traffic. USB ports can be disabled. Companies such as Panduit manufacture RJ45 hardware locks that cover open jacks and can only be removed with special tools.

Additionally, each power up can be reported via Syslog, SNMP, email and/or SMS to a central server so that the reason for the disconnection can be investigated.

Digi TransPort WR44 and WR41 models have Digital IO options via the T2 Telemetry module and all TransPort models except the WR11 have RS232 serial ports. These interfaces can be used to monitor simple contact closures on enclosure doors and trigger an alarm when the door is opened.

17. Summary

When properly configured, Digi TransPort routers meet the requirements of NERC CIP because they provide the stateful firewall, network segmentation via VLAN or Ethernet Port Isolation, network data encryption, authentication, and full event logging and alarming.

More information can be obtained from Digi International at www.digi.com.