DIGITAL EDGE CASE STUDY:

VPN Hub Architecture for Secure Access and Control of Energy Producing Equipment.

Submitted by:

Youssef Hanzaz
Network Security Engineer
Digital Edge Ventures
7 Teleport Drive
Staten Island, NY 10311

1. Executive Summary

One of our clients is a full-service energy solutions provider. They provide cost effective, environmentally friendly energy solutions for prime power, secure power, peak shaving and stand-by energy requirements.

Starting as a simple alert system on gas turbine failures, they grew into a premier solution to operating a microgrid. Their goal is to empower clients with resources to better manage their energy through education, advisory, reporting, and savings.

2. Client Profile

Currently, the client follows an approach where access to PLC devices is achieved by individually working with each client to place a pre-configured Cisco ASA appliance within a customer network, followed by configuring port forwards to ensure connectivity. When everything is done properly, initiating VPN sessions from external networks and accessing PLC devices is possible.

At times, this proves to be difficult due to the effort required for customized configurations of each ASA to meet the specifics of each individual client.

3. Solution

VPN Hub is the core of our solution, a Hub to spoke architecture combining security and efficiency within its design and conceptualization.

4. Architectural Concepts

Security

- Establishing site to site can be only made using a dial out connection from the spoke to the HUB.
- Network devices hardening (only required services are enabled on the network devices).
- Remote Open VPN users are configured following the principle of least privileged.
- Firmware upgrades are done periodically.
- Real time monitoring.
- Change control.
- Daily Configuration backups.
- Uses the secure protocols defined below:

Type	Protocol Used	Comment
Site to site	SSTP	Secure Socket Tunneling Protocol between HUB and spokes.
Client to site	OPEN VPN	Open VPN protocol for remote users that authenticate to the HUB firewall.
Site to site	EoIP on top of an SSTP tunnel	Tunnel that enable a remote user to configure the network parameters for a remote IOT device using his physical address.

Efficiency

- Scalable solution (HUB running as a VM with perpetual license given the ability to calibrate resources as needed).
- The architecture guarantees high Uptime.
- Uses Spokes Firewalls as FTP proxy to store FTP data from PLC on each site.
- Ability to configure new IOT devices without IP address using EOIP on top of SSTP tunnel.
- Configured SMTP relay to forward alerts from PLC to external mail server.
- Cost and time effective.
- Simplified Administration using IP mapping.
- Streamlined SOP's.

5. EoIP on top of SSTP Tunnel