Radiflow

Securicon Endorses Radiflow's RF-3180 Secure Gateway as a NERC-CIP Enabler

CIARA, THE FIRST OT-BAS PLATFORM

BLACK & VEATCH

securicon

Securicon, LLC
5400 Shawnee Road
Suite 206
Alexandria, VA 22312

May 30, 2018

Radiflow
900 Corporate Drive
Mahwah, New Jersey 07430

To Whom It May Concern,

Between January and April 2018, Securicon conducted a series of tests on the Radiflow 3180 Gateway. The testing examined the device from the perspective of the security of the device itself, its reliability and integrity in an operational context, and its ability to act as a "NERC CIP Enablement Device". While some issues were identified early in the testing cycle, Radiflow was quick to remediate or mitigate the issues reported. As a result of testing and remediation, Securicon has found the Radiflow 3180 performed as advertised.

As an access point into an Electronic Security Perimeter (ESP), Securicon found that the device did provide the functionality and integrity that one would expect from an ESP Access Point. However, the 3180 does not natively provide multifactor authentication (MFA), nor malware protection, but is configurable to meet these requirements through external means.

The 3180 device supports Radius and LDAP which can be configured with an external MFA authentication process to implement the missing MFA capability.

Securicon also found that the 3180 firewall supports DPI for whitelisting of several specific ICS/SCADA protocols but not a full-fledged means to combat malware or viruses. According to Radiflow this was intentional to avoid latency for the critical SCADA sessions and the malware inspection is designed to be done by an external passive IDS monitoring solution to fully meet all the CIP requirements.

The 3180 provides a proxy function for accessing devices inside the ESP. This function enables non-compliant devices to be accessed in a secure manner by providing a front-end to the authentication process for the device or devices inside the ESP. While this will not make the devices themselves compliant, it can be used to provide a compliant access capability for non-compliant devices.

During testing, Securicon attempted various flooding types to create a DoS scenario. This was accomplished by utilizing HPING3 and macof to generate a large amount of various types of layer2 and layer 3 traffic, with the device staying up and still processing traffic and login requests. The device performed well under load and did NOT enter a DoS condition.

The lack of native MFA and DPI malware inspection notwithstanding, augmenting the 3180 with appropriate compensating controls would, indeed, satisfy the CIP requirements and make the 3180 a significant component of a NERC CIP enablement strategy and could itself be a compensating control for non-compliant devices within an ESP.

Paul W. Hurley
CEO

Phone: 703-914-2780
Fax: 703-914-2785
www.securicon.com
info@securicon.com