Answer ID
1309

AP9606 Web/SNMP Management Card security

Question

What kind of security does the AP9606 Web SNMP Management Card offer?

Answer

The Web/SNMP Management card provides several different security options. The security aspects of the card should provide a reasonable level of access and authentication control. The management card does not does not currently use any type of encryption. All of the data and communication between the card and the client interfaces such as telnet and the web server, is readable by capturing the network traffic going to and from the card. The card provides basic authentication using user names and passwords to control access as well as IP verification. The card also provides a greater level security by enabling MD5 authentication for the web interface.

User names and passwords

The Admin and device manager user's user names and passwords are used for logging into the Control Console and web interfaces. User names, passwords, and community names are transferred over the network in plain text. This means that some who can monitor your network traffic could determine the user names and passwords required to access the management card. Similar devices have the same constraints due to the limitations of the protocols.

Port assignments

To enable users to hide the interfaces, one can change the TCP port that the Telnet, FTP and web servers utilize to a non-standard port. You can use ports

from 5000-65535. Changing the port provides an extra level of security acting as an extra password.

MD5 Authentication

The web interface option for MD5 authentication enables a higher level of access security than provided by the basic http authentication scheme. The scheme is very similar to the methods used in the CHAP and PAP remote access protocols. When enabled the web server will request a user name and a password phrase (distinct from the passwords). As opposed to the basic scheme, the user name and password phrase are not transmitted over the network. The small Java login applet combines the user name, password phrase and session unique challenge number and calculates an MD5 hash number. This number is then returned to the server so that it can verify that the user indeed has the correct login information. By only passing the hash number back, there is no information that can reveal the login information. In addition to the login authentication, each form post for configuration or control operations is also authenticated with a unique challenge and hash response. The scheme does not involve and encryption so pages are still transmitted in their plain-text form, in addition after the authentication login, subsequent page access is restricted by IP address and a hidden session cookie. Since the MD5 authentication scheme is available only for the web interface, it is important to disable the less secure interfaces including Telnet, FTP and SNMP. For SNMP it is possible to just disable write access so that read and trap facilities are still available. The MD5 authentication scheme provides a much higher level

of security than the plain-text type access methods. However, sophisticated, malicious attacks are almost impossible to guard against. Utilizing well-configured firewalls is an essential element in any security scheme.

Other keywords: AP9606 Web/SNMP Management Card security, Powernet SNMP, web, arakni, arachne, power-net, power net, secure, security, safe, safety, web/SNMP management card webcard