



**SSL-TLS VPN 3.0 Certification Report**

**For:  
Array Networks, Inc.**

Prepared by:

ICSA Labs  
1000 Bent Creek Blvd., Suite 200  
Mechanicsburg, PA 17050  
USA

<http://www.icsalabs.com>

Document Version 1.0

## **Array Networks, Inc.** Array SPX Series SSL VPN Access Gateways Version Array SP Rel.SP.8.0.0.1 Build 0

### **Executive Summary**

#### **Introduction**

ICSA Labs tests candidate SSL-TLS VPN products against publicly available criteria developed by a consortium of SSL-TLS VPN vendors with input from industry analysts and the end user community. The criteria are defined in two modules, the Baseline Module and the VPN Module. An ICSA Labs certified SSL-TLS VPN product must satisfy all the mandatory requirements in both modules. The certification criteria for both modules are located in the SSL-TLS section of the ICSA Labs website.

This report documents the results of each phase of testing. The report also records the hardware, software, documentation submitted by the vendor, configuration steps used by ICSA Labs Analysts, and any updates or patches that were required to meet the requirements.

#### **Scope of Assessment**

The following is a summary of the Baseline and VPN requirements:

1. **Documentation** – The vendor supplied documentation must be adequate and accurate for administration of the product.
2. **Protocol and Cryptography Implementation** – The SSL/TLS protocol and underlying cryptography must be implemented properly.
3. **X.509 Certificate Management and Validation** – The product must support X.509 certificate management such as secure enrollment and renewal. Where appropriate, the product must support proper validation of client side certificates.
4. **Administration** – The product must have secure administrative capabilities including strong authentication, secure remote access, and support role based administration.
5. **Authentication and Authorization** – The product must support secure user authentication mechanisms and granular control of access to resources. The product must also have the ability to perform integrity checks of the client system before a session is established.
6. **Security Testing** – The product must prevent unauthorized access and protect against common exploits and attacks.
7. **Functional Testing** – The product must support different categories of common applications. When operating in a reverse web proxy mode the product must prevent leaking of internal network information.
8. **Session Control** – The product must provide automatic and administrative controls over user sessions. The product must have the ability to clean session related data after termination. Split tunneling behavior must be documented, and can be disabled.
9. **Persistence** – Configuration settings and log data must persist in the event of an unexpected system reset.

10. **Logging** – The product must have the ability to accurately log the required data for system and session related events.

### **Summary of Findings**

Array networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 has satisfied all mandatory certification criteria and achieved ICSA Labs SSL-TLS VPN Product Certification. The certification is valid only for the product and version specified in this report. During the testing period, this version will remain certified and will be continuously deployed at ICSA Labs for periodic testing. This report makes no claims regarding previous or subsequent versions of this product.

## **System Components**

### **Introduction**

ICSA Labs requires that vendors submit all hardware, software, and documentation necessary to comply with the criteria. For the purposes of this document, the term Product Under Test (PUT) refers to the complete system submitted by the vendor for certification testing including all documentation, hardware, firmware, software, host operating systems, and management systems. Common network services such as Syslog, DNS, NTP, etc. are provided by ICSA Labs and are not considered part of the PUT.

### **Hardware**

- Array SPX 2000 appliance
- Array SPX 5000 appliance

### **Software**

- Version Array SP Rel.SP.8.0.0.1 Build 0
- Symantec On-Demand Manager Version 2.6 Build 2309

### **Product Family Description**

This section lists the members of the certified product family. A representative set of models was submitted for testing and listed in the Hardware section above. In order to submit a family of products for certification, the vendor must attest that:

- The vendor designs and maintains control over the entire set of hardware, firmware, and software for each member of the product family.
- The vendor software, including but not limited to the functional software and the operating system software, is uniform across the product family.
- The management interface(s) for the members of the product family are uniform and completely consistent.
- Each member in the product family has an equivalent set of functionality.
- The functional, integration, and regression testing conducted by the vendor is uniform and consistent across the product family.

### **Product Family Members**

- Array SPX 2000
- Array SPX 3000
- Array SPX 5000

## Documentation

The following documentation was submitted by the vendor:

- Array SPX CLI handbook (PN: 030200, rev B)
- Array SPX Series Web User Interface (WebUI) Guide (PN: 0302001 rev B)
- Symantec On-Demand Manger Administration Guide (Documentation Build 2.6.0.1005)
- Symantec On-Demand Quick Start Guide (Documentation Build 2.6.0.1005)

## Test Configuration

### Introduction

To configure the product for testing, ICSA Labs Analyst followed the administration guidance and chose default settings when possible. Any specific configuration that was necessary is documented in the appropriate section of this report.

### Test Description

Tests were conducted in a simple network environment with the PUT, internal resources, and external clients each connected to a separate network. The client systems were configured with Windows XP and tests were run with Internet Explorer 6.0 SP2 and Firefox 1.5 browsers.

### Initial Product Configuration

The PUT was connected to the test network in a single interface configuration. ICSA Labs Analysts performed the following actions to prepare the PUT for testing:

- Followed "Web user's Interface Setup Configuration" on page 8 of WebUI Guide to configure basic network settings using serial console connection.
- Followed "Quick Start" steps on pages 16-21 of WebUI Guide to complete configuration of required settings and to create a virtual site. A virtual site provides a single interface for external users to access internal content. Each virtual site is associated with a domain name and listens on a specified virtual IP address (VIP) and port (definition from WebUI Guide).
- Product was administered using the WebUI web interface.

## Detailed Findings

### DOCUMENTATION

#### Test Description

ICSA Labs Analysts review the administrative guidance when configuring the PUT to verify that there is adequate and accurate information relevant to performing the certification testing.

#### Findings

The following violations were initially discovered during testing. Array Networks, Inc. provided updated documentation to correct these violations and satisfy the requirements.

- Documentation did not disclose the default allow all nature of the product.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Documentation criteria. The Analysts were able to successfully install and administer the PUT using the provided documentation.

## PROTOCOL AND CRYPTOGRAPHY IMPLEMENTATION

### Test Description

ICSA Labs Analysts evaluate that the SSL/TLS protocol and cryptography are implemented without security degrading mistakes. The Analysts also verify that supported weak cipher suites are not enabled by default.

### Findings and Configuration

The following protocols and cipher suites were supported and enabled by default:

- SSLv3
- TLSv1
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

The following protocols and cipher suites were supported but not enabled by default:

- EXP-DES-CBC-SHA
- DES-CBC-SHA
- EXP-RC4-MD5

The following were the steps taken to configure the protocols and cipher suites:

- SSL protocols were configured on a per virtual site basis under Site Configuration -> Security Settings -> SSL Settings -> General
- Cipher suites were configured on a per virtual site basis under Site Configuration -> Security Settings -> SSL Settings -> Cipher Suites

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Protocols, Crypto Implementation, Random Number Generation, and Cipher Suite Support criteria. The Analysts determined that the cryptographic service provided by the SSL-TLS VPN was implemented properly and without introducing security vulnerabilities.

## X.509 CERTIFICATE MANAGEMENT AND VALIDATION

### Test Description

ICSA Labs Analysts evaluate the support for installing and replacing certificates from an external certification authority. The Analysts verify that the PUT properly validates client certificates and employs a revocation mechanism, for those products that support client-side certificate authentication.

### Findings and Configuration

ICSA Labs Analysts performed the following steps to configure the PUT certificate management functions:

- All certificate management functions were performed on a per virtual site basis under Site Configuration -> SSL Certificates. Detailed instructions for performing certificate management functions can be found on pages 75-76 of the WebUI guide.

The PUT supported client side certificate authentication. ICSA Labs Analysts performed the following actions to configure client side certificate authentication and a mechanism for revocation of client certificates:

- Enable client side certificate authentication and client certificate revocation settings on a per virtual site basis under Site Configuration -> Security Settings -> Client Authentication. Detailed instructions can be found on page 95 of the WebUI guide.

The following violations were initially discovered during testing. Array Networks, Inc. provided updated software to correct these violations and satisfy the requirements.

- PUT did not properly validate certificate revocation mechanism.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the X.509 Certificate Management and Validation criteria. The Analysts were able to successfully install, update, and view the SSL-TLS VPN server certificate. Testing also confirmed that the PUT properly validated client side certificates before granting access.

## ADMINISTRATION

### Test Description

ICSA Labs Analysts evaluate that the PUT enables administrators to have secure control and auditing capabilities, and that no unauthorized administrative actions can be performed.

### Findings and Configuration

ICSA Lab Analysts configured the PUT for strong administrator authentication, different levels of administration, and secure remote access as outlined below. The Analysts also verified the PUT has the capability to monitor and terminate user sessions and view critical statistics of the SSL-TLS VPN system.

The Analysts performed the following actions to configure the PUT for strong administrator authentication:

- Physically secure appliance.
- Configure console access.
- Disable remote access.

Although the above method was sufficient to meet criteria requirements for strong administrator authentication, it should be noted that the PUT supports strong administrator authentication using SecurID over the RADIUS protocol without next tokencode mode. Array Networks, Inc. supplied the following steps for configuration.

- Enable AAA for Admin Authentication for the Base System under Administrators -> Admin Authentication -> General.
- Select RADIUS for Rank 1 of Authentication Method Ranking for the Base System under Administrators -> Admin Authentication -> Method.
- Add SecurID server RADIUS details under Administrators -> Admin Authentication -> RADIUS.

The Analysts performed the following actions to configure the PUT's different levels of administration:

- Role based administration was configured following guidance provided on page 38 of the WebUI guide.

The following violations were initially discovered during testing. Array Networks, Inc. provided updated software to correct these violations and satisfy the requirements.

- Not all required critical statistics of the SSL-TLS VPN system were available.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Administration criteria. The ICSA Lab Analysts were able to securely administer the PUT and manage users using available functions.

### Notes

SSL Service status is indicated as enabled/disabled which is the desired state and not actually the current status. Array Networks, Inc. has attested that this is a reasonable method for checking the SSL Service status since there are no known situations where the administrative interface will indicate that the SSL Service is enabled, even though the service is actually disabled.

## AUTHENTICATION AND AUTHORIZATION

### Test Description

ICSA Labs Analysts evaluate the user authentication mechanisms and controls for authorized users to access private resources. Analysts also evaluate the capability of the SSL-TLS VPN to execute integrity checking of the client system before establishing a session.

### Findings and Configuration

The PUT supported RADIUS, LDAPS, Active Directory using LDAPS, local user database, and X.509 certificates for user authentication and X.509 certificate-challenge and SecurID for strong authentication. The Analysts configured and tested as noted.

The following lists the authentication mechanisms that were tested:

- RADIUS
- LDAPS
- Active Directory using LDAPS
- Local user database
- X.509 Certificates

The Analysts performed the following actions to define the PUT's web based filters and access security policy:

- Access security policy was configured on a per virtual site basis using Access Control Lists under Access Policies -> ACLs. Detailed instructions can be found on pages 127-128 of the WebUI guide.
- Web based filters were configured on a per virtual site basis under Access Policies -> URL Filtering. Detailed instructions can be found on pages 129-131 of the WebUI guide.

The Analysts performed the following actions to configure the PUT's client system integrity checking function:

- Client system integrity checking required the use of Symantec On-Demand Manager to configure the integrity checking policy.
- Download Symantec On-Demand Manager from the WebUI under Site Configuration -> Security Settings -> Client Security -> General Settings.
- Install Symantec On-Demand Manager.

- Configure client side integrity checking policy as desired following instructions in Symantec On-Demand Manager Administration Guide
- Enable Client Security on a per virtual site basis under Configuration -> Security Settings -> Client Security -> General Settings.
- Import setup.xml file created by Symantec On-Demand Manager under Configuration -> Security Settings -> Client Security -> General Settings -> Import
- Add a location to match the location name chosen during integrity checking policy configuration under Configuration -> Security Settings -> Client Security -> Locations.
- For more detailed instructions see pages 93-95 of the WebUI guide.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Authentication and Authorization criteria. ICSA Labs Analysts successfully verified the PUT's capabilities for strong user authentication, secure authentication methods, access control, and client system integrity checking.

### Notes

Symantec On-Demand Manager requires admin rights on the local PC to execute.

## SECURITY TESTING

### Test Description

ICSA Labs Analysts evaluate the PUT's resistance to exploits and Denial-of-Service attacks commonly known within the Internet community.

### Findings and Configuration

The Analysts used a combination of in-house, open source, and commercial tools to test the PUT's ability to resist attacks. No specific configurations were used.

The following violations were initially discovered during testing. Array Networks, Inc. provided a software update to correct these violations and satisfy the requirements.

- The initial software submitted included a version of OpenSSL that contained known vulnerabilities.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Security Testing criteria. ICSA Labs Analysts determined that the PUT was not susceptible to the attacks used during testing.

### Notes

The version of OpenSSH included with the PUT was out of date. Since all configuration tasks were performed using the WebUI, SSH was disabled, and this was not considered a criteria violation.

## FUNCTIONAL TESTING

### Test Description

ICSA Labs Analysts evaluate the PUT to determine that it supports specific categories of common applications and functions properly without introducing security vulnerabilities.

### Findings and Configuration

ICSA Labs Analysts configured the PUT to allow authenticated users to access common applications such as e-mail, file services and web based applications. SSL-TLS VPN products typically support a reverse web proxy mode, layer three tunneling behavior or both.

The PUT supports accessing applications in a reverse web proxy mode and was configured as follows:

- By default the PUT allows authenticated users access to backend web resources using reverse web proxy mode by providing a URL bar that allows a user to type in the URL to a backend resource. This behavior is documented on page 128 of the WebUI guide.
- Configuring access to specific resources required adding links to the portal page as detailed on page 105 of the WebUI guide.

Additionally, Analysts verified that the PUT was capable of protecting private internal network information in a reverse web proxy mode. The PUT supports rewriting of the following URL schemes within HTML links: HTTP, HTTPS, FTP. The administrative WebUI guide page 107 provides further information regarding URL rewriting.

The PUT supports access to resources via a layer three tunneling session and was configured as follows:

- Access method L3VPN was configured following instructions found on pages 122-126 of the WebUI guide.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Functional Testing criteria and applications were executed properly in a secure manner.

## SESSION CONTROL AND SPLIT TUNNELING

### Test Description

ICSA Lab Analysts evaluate that the PUT provides sufficient control of sensitive session related data. The Analysts verify the automatic termination and re-authentication mechanisms and evaluate the cleaning of security relevant data that may have been left behind after session terminations. Where supported, both cache cleaning and virtual session functions are tested. Split tunneling behavior is also examined and verified that it can be disabled.

### Findings and Configuration

ICSA Labs Analysts configured and tested both the cache cleaning and the virtual session functionality and evaluated the capability to prevent security relevant data from being left behind. The evaluation included the most common use scenarios for both normal and unexpected session termination.

The PUT supported a virtual session mechanism and was configured as follows:

- Session control required the use of Symantec On-Demand Manager to configure the Virtual Desktop settings.
- Download Symantec On-Demand Manager from Site Configuration -> Security Settings -> Client Security -> General Settings.
- Install Symantec On-Demand Manager.
- Configure Virtual Desktop settings following instructions in Symantec On-Demand Manager Administration Guide
- Enable Client Security on a per virtual site basis under Configuration -> Security Settings -> Client Security -> General Settings.
- Import setup.xml file created by Symantec On-Demand Manager under Configuration -> Security Settings -> Client Security -> General Settings -> Import
- Add a location to match the location name chosen during integrity checking policy configuration under Configuration -> Security Settings -> Client Security -> Locations.
- For more detailed instructions see pages 93-95 of the WebUI guide.

Analysts observed during testing that some information was left behind after a session was terminated. After analysis, the Analysts determined that the data left behind was not a detriment to the security of the VPN session. Examples of data found were cached image files, html files, and javascript files related to session initiation. The WebUI guide, page 94, provides further information regarding data that may remain after session termination.

Split tunneling was enabled or disabled as follows:

- Split tunneling behavior applies only to L3VPN, and is configured when the L3VPN is setup. After initial setup, split tunneling behavior can be changed on a per virtual site basis under Access Methods -> L3VPN.

The WebUI guide page 122 provides further information regarding the split tunneling behavior.

The following violations were initially discovered during testing. Array Networks, Inc. provided updated software to correct these violations and satisfy the requirements.

- Initially, all required session related data were not removed by the cache cleaner or virtual desktop.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Session Control and Split Tunneling criteria. The Analysts also determined that the PUT using the Symantec Virtual Desktop that is integrated into the SPX properly protected the sensitive session related data within the tested cases.

## PERSISTENCE

### Test Description

ICSA Lab Analysts evaluate the PUT to determine that configuration information, administrative settings, stored log data, and date and time settings are persistent across unexpected system resets. In some cases, remote time and logging servers are used as noted.

### Findings and Configuration

After configuring and exercising the PUT, ICSA Labs Analysts removed power and recycled the system to verify that configuration and logging data was properly maintained.

To meet the requirements, the PUT was configured to use a remote logging server:

- General logging settings were configured for the Base System under Admin Tools -> Monitoring -> Logging General.
- Remote Log servers were configured under Admin Tools -> Monitoring -> Syslog Servers.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Persistence criteria. The Analysts found that the configuration information, administrative settings, stored log data, and date and time information persisted through planned and unplanned system resets.

## LOGGING

### Test Description

ICSA Lab Analysts evaluate the PUT's ability to capture, store, and present adequate information enabling the administrator to audit system and session related events. For the purposes of testing, logging was enabled at all times; however, it is not a requirement that the logging function be enabled by default. In some cases, a remote log server, such as syslog, may be required as noted.

## Findings and Configuration

The SSL-TLS Lab analysts configured the PUT to capture, then send the required logging events to a remote log server.

ICSA Labs SSL-TLS Lab analysts performed the following actions to configure the logging function:

- General logging settings were configured for the Base System under Admin Tools -> Monitoring -> Logging -> General.
- Set level to "0:DEBUG" under Admin Tools -> Monitoring -> Logging -> General.
- Remote Log servers were configured under Admin Tools -> Monitoring -> Syslog Servers.

The following violations were initially discovered during testing. Array Networks, Inc. provided updated software to correct these violations and satisfy the requirements.

- Some required log events did not contain all required log data.

Array Networks, Inc. SPX Series version Array SP Rel.SP.8.0.0.1 Build 0 met the Logging criteria. The Analysts found that the logging capabilities of the PUT permitted administrators to adequately audit system and session related events.

## TESTING INFORMATION

### Certification Date

June 1, 2007

### Test Location

ICSA Labs  
1000 Bent Creek Blvd., Suite 200  
Mechanicsburg, PA 17050  
USA  
<http://www.icsalabs.com>

### Vendor Headquarters

Array Networks, Inc.  
1371 McCarthy Blvd.  
Milpitas, CA 95035  
USA  
<http://www.arraynetworks.net>

## About ICSA Labs

ICSA Labs, an independent division of Cybertrust, Inc., offers vendor-neutral testing and certification of security products. Hundreds of the world's top security vendors submit their products for testing and certification at ICSA Labs. The end-users of security technologies rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, anti-spyware, firewall, IPsec VPN, cryptography, network intrusion prevention, PC firewall, SSL-VPN, application firewall, anti-spam and Wireless LAN. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.

### Copyright

Copyright © 2007 Cybertrust, Inc. All Rights Reserved. No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express permission in writing from ICSA Labs. ICSA Labs is a division of Cybertrust, Inc and is a registered mark of Cybertrust, Inc.