AG 9.4 Security Advisory

Version: 1.2
Last Update: April 10, 2024

Contact us:
Array Networks Inc.
1371 McCarthy Boulevard Milpitas,
California 95035, USA
Email: info@arraynetworks.com
Telephone: (408)240-8700 (Monday through Friday, 9 A.M. to 5 P.M. PST)
Toll Free: 1-866-692-7729 (1-866-MY-ARRAY)
Support: 1-877-992-7729 (1-877-99-ARRAY)
Fax: (408)240-8754
http://www.arraynetworks.com/

Legal Notice

WARNING:
Modifications made to the Array Networks unit, unless expressly approved by Array Networks, could void the user's authority to operate the equipment.

Document Feedback

Array Networks values your opinion and strives to ensure that the documentation you receive is clear, concise, and provides the appropriate information required for you to use each Array Networks application efficiently.

If you would like to provide feedback on this document, you can submit your questions or suggestions to the Array Networks Support team and they will be forwarded to the appropriate development teams for review and consideration in a future release.

In addition to the provided documentation, many additional resources are available to help you understand and work with your Array Networks applications. For more information on these resources, see the Array Networks website.

Array Customer Support

To contact Array Networks Customer Support, please call 1-877-992-7729 or email the support team at support@arraynetworks.com.

Revision History

Date	Description
2023-03-24	First version.
2023-06-07	Recommended versions are changed to 9.4.0.486 and 9.4.0.292.89.
2023-07-04	Recommended versions: Added Netgate 9.4.0.59.
2024-04-10	• Recommended versions: Updated 9.4.0.486 to 9.4.0.505 • In Management Interface, updated the following: ▪ Added the step to turn off the WebUI/RESTful API/XML-RPC interface. ▪ Added the step to configure the **admin access** command to restrict the source IP address.

Contents

Preface

As the internet and other information technology evolves, the security risk of network environment is increasingly significant. To enhance AG's security and better fulfil the needs of enterprise users, a more robust security solution has been provided.

Solution

If you have several AGs, the settings (excluding network and ACL) of these AGs need to be the same. We suggest you configure and bolster your AGs according to the following instructions as needed.

Recommended versions: AG 9.4.0.505, AG 9.4.0.292.89, and Netgate 9.4.0.59

Access Tunnel Control

Management Interface

1. We suggest you turn on the management interface of the WebUI, RESTful API, and XML-RPC only when you configure your AG. After the configuration is completed, turn off the management interface to avoid vulnerability exploitation. For people who use only WebUI, RESTful API, or XML-RPC to control the AG, we suggest them create a strong password for the administrator account, specify an intranet to manage IP addresses, and use a single host to control the AG to reduce the security risk.

   To turn off the interfaces, run the following commands:

   ```
   AN(config)#webui off
   AN(config)#restapi off
   AN(config)#xmlrpc off
   ```

   To turn on the interfaces, run the following commands:

   ```
   AN(config)#webui on
   AN(config)#webui ip 192.168.XXX.XXX
   AN(config)#restapi on
   AN(config)#restapi ip 192.168.XXX.XXX
   AN(config)#xmlrpc on https
   AN(config)#xmlrpc ip 192.168.XXX.XXX
   ```

   In the preceding example, 192.168.XXX.XXX is the intranet management IP address. You need to configure the management IP address for your AG as needed. (Enable the preceding services *only* when it's necessary.)

2. Turn on the SSH interface. You need to specify a static intranet management IP address for the SSH. Do not set a long idle timeout for an SSH connection. We suggest you use the default, which is 5 minutes. Next, set a secure cipher suite for the SSH, and disable the CBC mode in the SSH protocol.

```
AN(config)#ssh on
AN(config)#ssh ip 192.168.XXX.XXX
AN(config)#ssh idletimeout 5
AN(config)#ssh ciphersuite
"arcfour128,arcfour256,arcfour,aes128-ctr,aes192-ctr,aes256-ctr"
```

3. Source IP address restriction.

   After you restrict the source IP address for a WebUI/RESTful API/XML-RPC/SSH management interface, if you need to change this setting, you need to restart the management interface to apply the new setting. The source IP address can be restricted as follows:

```
AN(config)#admin access xxx.xxx.xxx.xxx 255.255.255.255
```

   You can configure more than one **admin access** commands, but the IP address cannot be conflicted or overlapped. If there is an IP address conflict or overlap, the WebUI/RESTful API/XML-RPC/SSH service will be affected.

   An IP address conflict or overlap example is shown below:

```
AN(config)#admin access 192.168.100.XXX 255.255.255.0
AN(config)#admin access 192.168.XXX.XXX 255.255.0.0
```

   In the preceding example, the address 192.168.XXX.XXX 255.255.255.0 occupies 24 bits, and 192.168.XXX.XXX 255.255.0.0 occupies 16 bits. The address 192.168.XXX.XXX 255.255.0.0 contains 192.168.XXX.XXX 255.255.255.0. If the preceding settings are used, there will be an IP address overlap. As a result, the IP address cannot be configured like this.

4. If your environment doesn't need a virtual site, we suggest you not to create it. If you create a virtual site, set the virtual site's SSL protocol to TLS v1.2, and set a secure cipher suite.

   The following cipher suites support TLC v1.2:

- AES256-SHA256
- AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA25

5. Taking a CSR as an example, run the following commands to configure a cipher suite.

```
vsite(config)#ssl csr 2048
vsite(config)#ssl start
vsite(config)#ssl settings protocol "TLSv12"
vsite(config)#ssl settings ciphersuite
"AES256-SHA256:AES128-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-A ES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256"
```

Password Security

1. Create an administrator account. "xxx" is your administrator account.

```
AN(config)#admin user xxx
```

After an administrator account is created, delete the default “array” administrator account immediately. We suggest you create only necessary accounts, and use strong passwords to increase the security of the passwords.

2. Create the password for the "enable" mode.

```
AN(config)#passwd enable
```

Product Development, Product Launch, and Secure Installation

Debug Mode

To disable the debug mode of components or programs to prevent sensitive information leakage, run the following command:

```
AN(config)#debug disable
```

System Management and Security Maintenance

Log Auditing

1. Create a secure Syslog server. 192.168.XXX.XXX is the intranet IP address of the Syslog server. You can configure your address as needed.

   ```
   AN(config)#log host 192.168.XXX.XXX
   ```

   We suggest you set an intranet IP address for your Syslog server, add the Syslog server on the AG, and synchronously back up the local log to the Syslog server, in case you cannot track the attackers' behavior after they delete the local log.

2. Enable the logging.

   ```
   AN(config)#log on
   ```

   The routine check for the log is important for analyzing anomalies and discovering potential threats.

Insecure Protocol

When you use AG, avoid using insecure protocols to prevent data leakage.

Insecure protocols:

- TFTP
- FTP
- Telnet
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1
- HTTP
- SNMP v1/v2
- SSH v1.x

Sensitive Data Protection

Do not use any password manager to manage the files that contain sensitive data, such as accounts, certificates, password files, and private key files.

Network Deployment

- We suggest you set an intranet IP address for your AG. Do not expose your AG on the internet.
- When you analyze AG's service ports, you can create rules for the external firewall and open only AG's service ports.
- AG doesn't actively initiate an external connection. You can create rules for the external firewall to forbid AG's management or service IP address to actively initiate an external connection.
- Enables AG's built-in firewall.

```
AN(config)#accesslist permit
AN(config)#webwall port1 on
```