



Array SPX ATF Deployment Guide

United States of America:

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

Declaration of Conformity

We, Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, CA. 95035, 1-866-692-7729, declare under our sole responsibility that the product(s) Array Networks, Inc. Array Appliance complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

WARNING: This is a Class "A" digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. In a residential area, operation of this equipment is likely to cause harmful interference, in which case the user may be required to take adequate measures. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Copyright©2009 Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, CA. 95035, USA. All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and compilation. No part of this document may be reproduced in any form by any means without prior written authorization of Array Networks, Inc. **Documentation is provided "as is" without warranty of any kind, either expressed or implied, including any kind of implied or expressed warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.**

Array Networks, Inc. reserves the right to change any products described herein at any time, and without notice. Array Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Array Networks, Inc. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Array Networks, Inc.

Contacting Array Networks

Please use the following information to contact us at Array Networks:

URL Address: <http://www.arraynetworks.net/>

Our web site includes product information, software updates, white papers, and release information.

Telephone: 866-MY-ARRAY
408-240-8700
408-240-8753 (fax)

Telephone access to Array Networks, Inc. is available Monday through Friday, 7 A.M. to 7 P.M. PST.

Address: Array Networks, Inc.
1371 McCarthy Blvd.
Milpitas, California 95035

Contents

Authorized Traffic Forwarding (ATF) Support	5
Preparing the SPX for ATF	5
Deployment Scenario 1	6
Configuring ATF via the WebUI for Deployment Scenario 1	6
Configuring ATF via the CLI for Deployment Scenario 1	7
Deployment Scenario 2	7
Configuring ACLs via the CLI for Deployment Scenario 2	8
Secure User Access	10

Note: Users not familiar with basic configuration steps, terminologies or procedures for the SPX should consult SPX Application Guide, CLI Handbook and or WebUI Guide for general configuration related information or contact customer support.

Authorized Traffic Forwarding (ATF) Support

ATF is a clientless access method used to authorize traffic and to secure intranet and Internet access when L3 client is used. There may be several types of end users such as guest, contractor, employee (even employee department groups such as Finance or Engineering, etc.) where different users have different access rights to different resources (servers, files, etc.). In this clientless access mode, the SPX would act as a gateway, forwarding packets “to” and “from” destinations based on authentication and authorization rules.

When the end user requests any web page, the user is sent to the login portal.

After logging in, the source IP/MAC address pairs are stored to identify users. At the same time, the configured authorization ACLs will be assigned to this user to control/restrict access to the network for security purposes. For example, if this user is an employee, then he/she can access both Intranet and Internet. But if the user is a guest, only the Internet can be accessed.

The ATF status indicator is displayed on the user's portal page to show the session information, including session start timer, session last time, session logout information, etc.

Users may optionally start L3 client to secure the data they are accessing.

Preparing the SPX for ATF

Make certain that the SPX is correctly configured for the destination deployment. Among key configuration elements, verify that the network settings concerning IP Address, routes, DNS, virtual portals and AAA are correct. It is also important to have already set up users and users groups as necessary.

To make sure SPX will intercept the user's Web access, so that user can be redirected to the login portal, the SPX must serve as the default router or stay in the path between the client network and the destination network. You can achieve this by configuring the DHCP to assign the virtual portal or the virtual portal's interface as the client's default gateway.

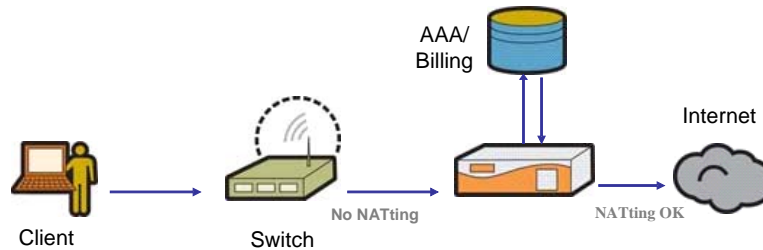
Note: Using SPX as the DHCP server is supported but not required for ATF.

Note: Using SPX as the client computer's DNS server is supported but not required for ATF.

Note: Routing within the network needs to be configured so that returning traffic from the Internet or Corporate network to the client behind SPX will go to SPX to be forwarded it back to the client.

Note: If the SPX will be deployed as the DNS server, then the virtual portal's FQDN must be added as a host entry so that it can be resolved (use CLI command -> ip dns host).

Deployment Scenario 1



With Deployment Scenario 1, the Client, based on credentials (AAA), will be allowed to access only the Internet and destination points beyond the internal network. With the DHCP settings configured to point to the virtual portal's interface as the default route, the guest user is seamlessly directed to the outside network.

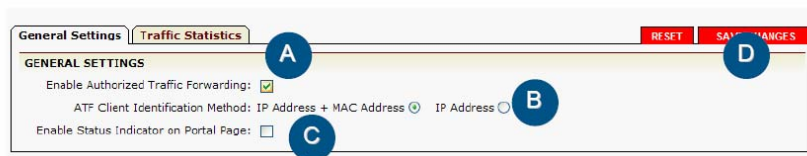
Note: No NAT on switch. If NAT is configured on the switch, SPX will not be able to see the client's real IP address, therefore unable to track the client authentication by the IP address.

Note: NATting maybe used on the SPX for routing.

Configuring ATF via the WebUI for Deployment Scenario 1

Proceed to this location within the WebUI:

Virtual Site Home-> Access Methods -> ATF



- [A]** Enable the authorized traffic forwarding feature for the virtual site.
- [B]** Administrators may choose to have users authenticated by their unique IP address or the IP address and MAC address.
- [C]** ATF client indicator will show the end user's session status.
- [D]** "Save Changes" or "Reset" link.

Configuring ATF via the CLI for Deployment Scenario 1

- [.] Enable ATP: **atf on**
- [.] Enable ATF client indicator: **atf client on**
- [.] Administrators may choose to have users authenticated by their unique IP address or the IP address and MAC address. Use the CLI command: **atf clientid {ipmac|iponly}**

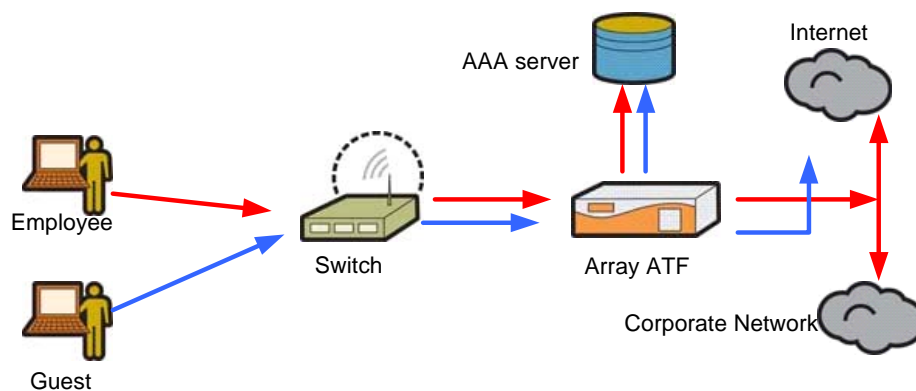
Note: To use MAC to track the client authentication, please make sure the SPX sees the packets from the client directly without any hops in the middle.

Enable ATF:

```
example(config)$atf on  
example(config)$atf client on
```

Deployment Scenario 2

This deployment has both company employees as well as guest users on the same subnet where the employees will need access to the internal as well as external network while limiting the guest user to only access to the outside network (Internet). The directing of the guest user straight to the outside Internet and still allowing the employee the freedom access other internal corporate network resources is achieved with Access Control Lists (ACLs).



In the deployment pictured here, both the employee and the guest log onto the corporate network from the same subnet location. However, the employee is permitted by ACLs to access both the internal corporate network as well as the Internet and the guest is simply permitted by ACL to only access the Internet.

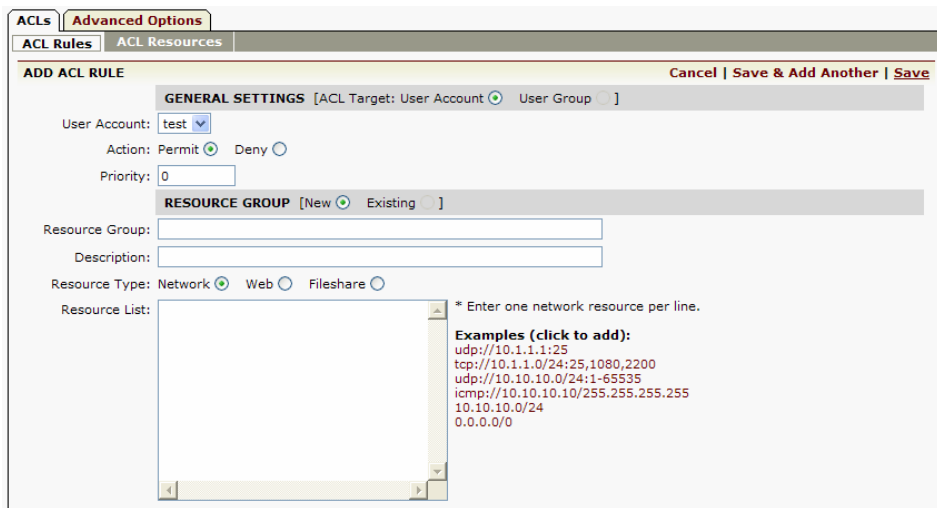
With ACLs, when a specific user attempts to access a destination or other resource on the internal network, that user's credentials are checked against all configured ACLs to see if they have the necessary permissions. If the user has the correct permissions, then they are forwarded to the network destination. If the user does not have the correct permissions or is expressly denied access, the connection will be terminated.

Note: Only IP, TCP, UDP and ICMP ACLs are supported for ATF access. For detailed ACL configuration please refer to SPX Application Guide, CLI Handbook and or WebUI Guide for general configuration related information or contact customer support

Configuring ACLs via the WebUI for Deployment Scenario 2

Proceed to this location within the WebUI to create the necessary ACLs:

Virtual Site Home-> Access Policies -> ACLs



It is here that you may create/assign permit or deny ACL rules to individual users or groups of users.

Configuring ACLs via the CLI for Deployment Scenario 2

- [.] Use this CLI command to define a group of resources on the network, such as the resources to be accessed by employees:

```
acl resource <group_name> <ip>/<netmask>
```

- [.] Use this CLI command to assign users to the defined groups of resources and the permit/deny rules associated with each resource:

```
acl rule account <user_name> <group_name> {permit|deny} <priority>
```


Enable ATF with ACLs:

```
example(config)$atf on
example(config)$atf client on
```

```
example(config)$acl resource "Employee" "10.10.32.0/20"
example(config)$acl resource "Internet" "0.0.0.0/0"
example(config)$acl rule account "guest" "Employee" DENY 10
example(config)$acl rule account "guest" "Internet" PERMIT 100
example(config)$acl rule account "employee" "Internet" PERMIT 0
```

Based on the example network diagram on page 7 (Deployment Scenario 2), the following is an example for deploying AFT in a WiFi support network architecture. For this example, please note the following network settings were used for illustration purposes:

Virtual Portal IP and FQDN – 192.168.4.202 and wifi.example.net

External DNS Server – 10.1.1.9

IP of the SPX Interface facing the user – 192.168.4.201

Example of WiFi Support Deployment using SPX as DHCP server and DNS server. (If you have used the old Captive Portal feature of SPX, please make sure you are not specifying the <vsite name> in the 'ip dns local <ip address>' command:

Turn on DHCP server on SPX and configure the Virtual Site IP as the DNS server assigned to the clients, also configure Virtual Site IP as the default gateway assigned to the clients.

```
example(config)$ip dhcp local subnet iprange "dmz" 192.168.4.210 192.168.4.250
example(config)$ip dhcp local subnet domain "dmz" "example.net"
example(config)$ip dhcp local subnet nameserver "dmz" 192.168.4.201
example(config)$ip dhcp local subnet route "dmz" 192.168.4.201
example(config)$ip dhcp local subnet listen "dmz"
example(config)$ip dhcp local on
```

Configure SPX to act as a DNS server and add the Virtual Site FQDN to the local DNS entry, also make sure your external DNS server is configured so that SPX can use to resolve names ***.

```
example(config)$ip dns local 192.168.4.201
example(config)$ip dns nameserver 10.1.1.9    (***) external DNS server)

example(config)$ip dns host "wifi.example.net" 192.168.4.202
```

Now, enable ATF with ACLs as before.

Secure User Access

When it is required to encrypt the user's access for security reasons, especially if connecting through a wireless network, after the user logs in, a L3 VPN client can start automatically to secure all the user related data. ACLs configured for ATF will work the same way for this L3 traffic. When using L3 VPN, more advanced control can be used, including the directing of user traffic to a designated gateway, assigning a different DNS server for L3 clients, etc. Please refer to SPX Application Guide for more L3 VPN configuration and deployment strategies.

In some cases it may be desirable to only start a secure L3 VPN connection for employees but not for guest users. There are two options to accomplish this:

1. You may choose to have the employees manually start L3 VPN. You may configure the L3 VPN in such a way that if guest users do start the L3 VPN inadvertently, they won't be able to access what they are not permitted to. That can be achieved by ACLs as stated above or through limiting the network pool zones.
2. You can set up two separate networks; one for employees and the other for guest users. Employees use one interface on SPX as the default gateway and guest users use another interface on SPX as the default gateway. That way employees and guest users will have different login portals and potentially different features (i.e. with or without L3 VPN)

Note: Only one virtual portal may enable ATF on the same SPX interface.