Array Networks Security Advisory:
Blocking Unauthorized Remote Login Attempts

Revision 1.1

Last Updated: March 31, 2014

The purpose of this Array Networks Security Advisory is to recommend a number of best practices to block unauthorized remote login attempts to your Array Network appliance/s.

Overview

Malicious or DDoS attacks may target your Array Network appliance/s in order to discover and exploit possible ways to alter your configuration or even shut down the appliance. For example, a program may be written to remotely connect to your appliance and perform a brute-force-password-guessing attack. Upon successful password crack, the attacker can take over your appliance and its services. This is particularly vulnerable if your appliance is accessible through a public IP.

To best protect your appliance/s from these types of attacks, you should implement one of the recommended best practices in your production environment.

Applicable Array Networks Appliances:

- APV Application Delivery Controller: all models
- AG Secure Gateway: all models
- SPX Secure Gateway: all models

Applicable software versions:

- ArrayOS APV: all versions
- ArrayOS AG: all versions
- ArrayOS SPX: all versions

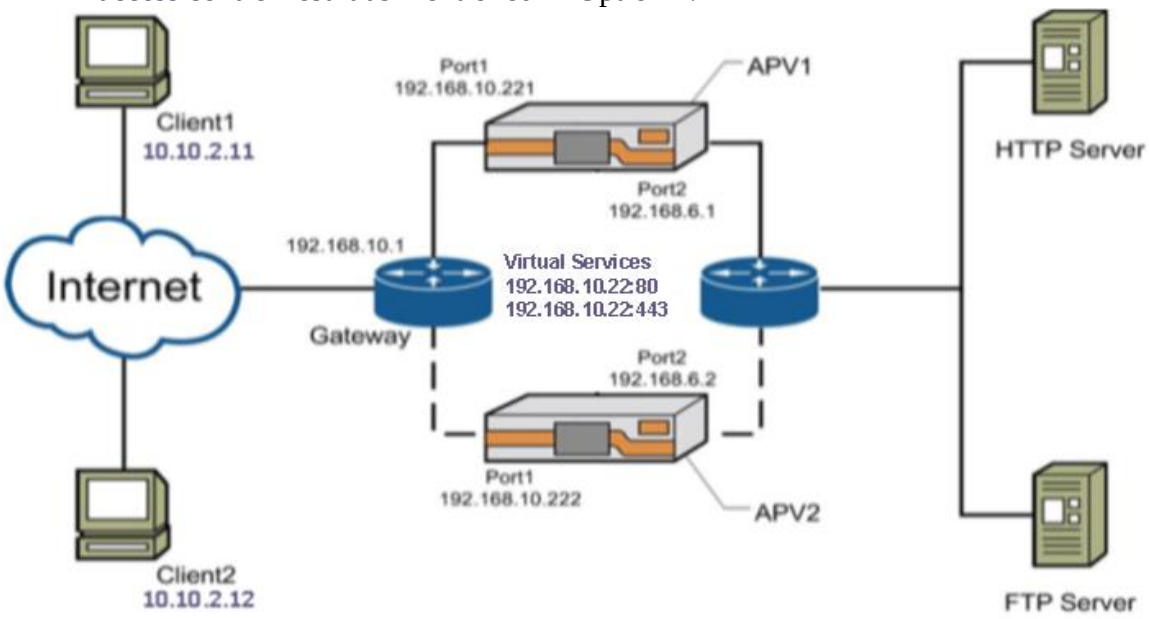
Recommended Best Practices

Option #1: Leveraging existing network infrastructure

In cases where there are upstream routers/switches/firewall devices connected to Array Networks appliance/s, users can add access control method on those devices to deny the insecure SSH accesses to the Array Network Appliance/s.

Option #2: Take advantage of the ArrayOS WebWall feature

Users can also take advantage of the ArrayOS WebWall to achieve the same access control result as mentioned in Option 1.



Based the network diagram above, the following sample WebWall configuration can be followed for strict SSH access control.

Turn on the WebWall check on the port connecting to public network.

APV1 Configuration:

APV1(config)# accessgroup 1 "port1"
#The commands below will allow all access to configured virtual services.
APV1(config)# accesslist permit tcp 0.0.0.0 0.0.0.0 0 192.168.10.22 255.255.255.255 80 1
APV1(config)# accesslist permit tcp 0.0.0.0 0.0.0.0 0 192.168.10.22 255.255.255.255 443 1
#The command below will allow a host with source IP of 10.10.2.11 to SSH to the box.
APV1(config)# accesslist permit tcp 10.10.2.11 255.255.255.255 0 192.168.10.221 255.255.255.255 22 1
APV1(config)# webwall port1 on 0
#All other traffic will be denied.

APV2 Configuration:

APV2(config)# accessgroup 1 "port1"

#The commands below will allow all access to configured virtual services.
APV2(config)# accesslist permit tcp 0.0.0.0 0.0.0.0 0 192.168.10.22 255.255.255.255 80 1
APV2(config)# accesslist permit tcp 0.0.0.0 0.0.0.0 0 192.168.10.22 255.255.255.255 443 1
#The command below will allow a host with source IP of 10.10.2.11 to SSH to the box.
APV2(config)# accesslist permit tcp 10.10.2.11 255.255.255.255 0 192.168.10.222 255.255.255.255 22 1
APV2(config)# webwall port1 on 0
#All other traffic will be denied.

Synconfig and HA will still work since they are configured to peer through port2 of both boxes on 192.168.6.0/24 subnet.

For any guidance in configuring WebWall, you are welcome to contact Array Networks TAC team. We will need the "show tech" output of each appliance. Based on existing configuration and network setup, we will be glad to provide a list commands that fit your needs and prevent attacks.

<u>Option 3:</u> Disable SSH access to the Array Networks appliance/s completely

Turn off the SSH server capability and only use the WebUI to manage the appliance/s. This can be reached by executing following commands.
ArrayOS(config)# webui on
ArrayOS(config)# ssh off

Caution: Synconfig and HA will not work when turning off SSH capability.

All of the above mentioned methods can be used to turn off WebUI access (port 8888) if desired.

Should you have any questions, please contact one of our customer service representatives at support@arraynetworks.com or Array Networks TAC telephone number (877-99-ARRAY).