a Hewlett Packard Enterprise company

AOS-Switch 和 AOS-CX
怎么限制 SSH 的 IP 范围

2021.12.13

目录

1 需求

用户希望限制 SSH 登录交换机的 IP 地址范围，因为接口和 VLAN 较多，不想通过 ACL 在接口或者 VLAN 上来限制，而是通过全局进行配置。

这里以 2930F 和 6300F 为例来测试。

2 AOS-Switch

2.1 Authorized IP Manager 功能介绍

Introduction

The Authorized IP Managers feature uses IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This covers access through the following means:

- Telnet and other terminal emulation applications
- The WebAgent
- SSH
- SNMP versions 1, 2 and 3 (with a correct community name)
- TFTP

When configured in the switch, the Authorized IP Managers feature takes precedence over local passwords, TACACS+, and RADIUS. This means that the IP address of a networked management device must be authorized before the switch will attempt to authenticate the device by invoking any other access security features. If the Authorized IP Managers feature disallows access to the device, then access is denied. Thus, with authorized IP managers configured, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch Authorized IP Managers configuration.

Use Authorized IP Managers along with other access security features to provide a more comprehensive security fabric than if you use only one or two security options.

NOTE: When no Authorized IP Manager rules are configured, the access method feature is disabled and access is not denied.

For each authorized manager address, you can configure either of these access levels:

- **Manager**

  Enables full access to all screens for viewing, configuration, and all other operations available.

- **Operator**

  Allows read-only access. (This is the same access that the switch allows for the operator-level password feature.)

Configure up to 100 authorized manager entries, where each entry applies to either a single management station or a group of stations.

CAUTION: Configuring Authorized IP Managers does not protect access to the switch through a modem or direct connection to the Console (RS-232) port. Also, if an unauthorized station "spoofs" an authorized IP address, it can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network security by keeping physical access to the switch restricted to authorized personnel, using the user name/password and other security features available in the switch, and preventing unauthorized access to data on your management stations.

通过 Authorized IP Manager 可以设置哪些 IP 或子网可以 SSH 到交换机，注意：

1. 未配置任何 Authorized IP Manager 时，等于此功能未开启，所有 IP 都会被允许；
2. 一旦配置了 Authorized IP Manager，等于此功能开启，未添加的 IP 一律禁止访问；
3. 终端通过 SSH 登录交换机时，优先根据 Authorized IP Manager 来判断终端 IP 是否被允许，允许的 IP 会再进入认证阶段（本地认证、tacacs 认证或者 radius 认证），认证通过才能访问；
4. Authorized IP Manager 可以设置 manager 和 operator 权限，认证也会设置访问权限，只有 Authorized IP Manager 和认证都设置了 manager 权限，用户才能获得 manager 权限，所以建议 Authorized IP Manager 统一设置 manager 权限，由认证来控制用户的访问权限；
5. Authorized IP Manager 只能设置允许的 IP 或子网，不能设置禁止的 IP 或子网，所以能实现允许 A 子网，A 子网以外的都禁止，不能实现允许 A 子网，而禁止 A 子网中的部分 IP；
6. 可以设置多条 Authorized IP Manager（最多 100 条）来允许多个 IP 或子网。

2.2 测试举例

2930F 管理 IP 为 10.5.11.2，我们需要实现允许 10.5.11.0/24 子网 SSH 登录交换机，其它子网不允许 SSH 登录交换机：

配置允许 10.5.11.0/24 子网 SSH 登录交换机：

```
Aruba-2930F-8G-PoEP-2SFPP(config)# ip authorized-managers 10.5.11.0 255.255.255.0 access ma
nager access-method ssh
```

```
8320-3# ssh admin@10.5.11.2

load pubkey "/home/remote_user/.ssh/id_rsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_rsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_dsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_dsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_ecdsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_ecdsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_ed25519": Permission denied

load pubkey "/home/remote_user/.ssh/id_ed25519": Permission denied

kex_exchange_identification: Connection closed by remote host

8320-3#
```

```
8320-4# ssh admin@10.5.11.2

We'd like to keep you up to date about:

  * Software feature updates

  * New product announcements

  * Special events

Please register your products now at:  www.hpe.com/networking/register




admin@10.5.11.2's password:

Aruba JL258A 2930F-8G-PoE+-2SFP+ Switch

Software revision WC.16.08.0002



 (C) Copyright 2019 Hewlett Packard Enterprise Development LP



                        RESTRICTED RIGHTS LEGEND

 Confidential computer software. Valid license from Hewlett Packard Enterprise

 Development LP required for possession, use or copying. Consistent with FAR
```

```
 12.211 and 12.212, Commercial Computer Software, Computer Software

 Documentation, and Technical Data for Commercial Items are licensed to the

 U.S. Government under vendor's standard commercial license.



Press any key to continue

Your previous successful login (as manager) was on 2021-12-09 01:36:36

 from 10.5.11.250



Aruba-2930F-8G-PoEP-2SFPP#
```

取消 Authorized IP Manager 配置：

```
Aruba-2930F-8G-PoEP-2SFPP(config)# no ip authorized-managers 10.5.11.0
```

```
8320-3# ssh admin@10.5.11.2

load pubkey "/home/remote_user/.ssh/id_rsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_rsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_dsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_dsa": Permission denied
```

```
load pubkey "/home/remote_user/.ssh/id_ecdsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_ecdsa": Permission denied

load pubkey "/home/remote_user/.ssh/id_ed25519": Permission denied

load pubkey "/home/remote_user/.ssh/id_ed25519": Permission denied

The authenticity of host '10.5.11.2 (10.5.11.2)' can't be established.

RSA key fingerprint is SHA256:zzFby4zbCG48BLjJC4RLhJmDqcLm9btYL7Qj4CoSVf0.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Failed to add the host to the list of known hosts (/home/remote_user/.ssh/known_hosts).

We'd like to keep you up to date about:

  * Software feature updates

  * New product announcements

  * Special events

Please register your products now at:  www.hpe.com/networking/register




admin@10.5.11.2's password:
```

3 AOS-CX

3.1 ACL 应用到 control-plane

access-list ip

Syntax

Syntax to create an IPv4 ACL and enter its context. Plus syntax to remove an ACL:

```
access-list ip <ACL-NAME>
no access-list ip <ACL-NAME>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols `ah`, `gre`, `esp`, `igmp`, `ospf`, `pim` (`ip` is available as an alias for `any`):

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{any|ip|ah|gre|esp|igmp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
{any|<DST-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [count] [log]

no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols `sctp`, `tcp`, `udp`:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{sctp|tcp|udp}
{any|<SRC-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
{any|<DST-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
[urg] [ack] [psh] [rst] [syn] [fin] [established]
[dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>]  [fragment] [vlan <VLAN-ID>] [count] [log]

no <SEQUENCE-NUMBER>
```

apply access-list control-plane

Syntax

```
apply access-list {ip|ipv6} <ACL-NAME> control-plane vrf <VRF-NAME>
no apply access-list {ip|ipv6} <ACL-NAME> control-plane vrf <VRF-NAME>
```

Description

Applies an ACL to the specified VRF.

The `no` form of this command removes application of the ACL from the specified VRF.

Command context

`config`

Parameters

`ip|ipv6`

Specifies the ACL type: `ip` for IPv4, or`ipv6` for IPv6.

`<ACL-NAME>`

Specifies the ACL name.

`vrf` *`<VRF-NAME>`*

Specifies the VRF name.

Authority

Administrators or local user group members with execution rights for this command.

Usage

Only one ACL per type (`ip`, or `ipv6`) may be applied to a control plane VRF at a time. Therefore, using the `apply access-list control-plane` command on a VRF with an already-applied ACL of the same type, will replace the applied ACL.

Examples

Applying My_ip_ACL to control plane traffic on the default VRF:

```
switch(config)# apply access-list ip My_ip_ACL control-plane vrf default
```

Replacing My_ip_ACL with My_Replacement_ACL on the default VRF:

```
switch(config)# apply access-list ip My_Replacement_ACL control-plane vrf default
```

Remove (unapply) the My_Replacement_ACL from the default VRF. Any other interfaces or VLANs with My_Replacement_ACL applied are unaffected.

```
switch(config)# no apply access-list ip My_Replacement_ACL control-plane vrf default
```

配置 ipv4 ACL，然后将 ACL 应用到 control-plane，需要注意：

1. control-plane 每个 vrf 只能配置一条同类型的 ACL（比如 ipv4 ACL），所以我们需要把所有的策略写到这一条 ACL 下；

2. 注意 vrf control-plane ACL 是全局的，一定要配置允许的策略，比如 permit any any any，否则会导致无法登录

3.2 测试举例

6300F vrf mgmt 管理 IP 为 10.5.50.161，我们需要实现禁止 10.0.83.0/24 子网 SSH 登录交换机，其它子网都可以 SSH 登录交换机：

配置 ipv4 ACL：

```
lab5-6300-1(config)# access-list ip SSH

lab5-6300-1(config-acl-ip)# 10 deny tcp 10.0.83.0/24 any eq 22

lab5-6300-1(config-acl-ip)# 20 permit any any any

lab5-6300-1(config-acl-ip)# exit

lab5-6300-1(config)# apply access-list ip SSH control-plane vrf mgmt
```

```
8320-4# ssh admin@10.5.50.161

(C) Copyright 2017-2019 Hewlett Packard Enterprise Development LP

RESTRICTED RIGHTS LEGEND

Confidential computer software. Valid license from Hewlett Packard Enterprise
```

Development LP required for possession, use or copying. Consistent with FAR

12.211 and 12.212, Commercial Computer Software, Computer Software

Documentation, and Technical Data for Commercial Items are licensed to the

U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:

* Software feature updates

* New product announcements

* Special events

Please register your products now at: https://asp.arubanetworks.com

admin@10.5.50.161's password:

8320-3# ssh admin@10.5.50.161

ssh: connect to host 10.5.50.161 port 22: Connection timed out

8320-3#