ACL Configuration Guide

Omada SDN Controller 4.1.5 or above

1910012994 REV1.0.0

January 2021

CONTENTS

1 Overview

ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets. These rules can be applied to specific clients or groups whose traffic passes through the gateway, switches and EAPs.

Omada SDN controller provides three types of ACL, namely Gateway ACL, Switch ACL and EAP ACL. Gateway ACL filters the packets passing through the router based on the ACL rules, limiting the internal users' access to the external network and protecting the LAN security. Switch ACL filters traffic as it passes through a switch, and permits or denies packets crossing specified interfaces or VLANs. EAP ACL isolates the guest network from the local wired network and other wireless clients based on ACL rules for security consideration.

The controller filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized by their created time. The rule created earlier is checked for a match with higher priority. You can also manually reorder the rules by dragging these entries. If no rules match, the device forwards the packet because of an implicit Permit All clause. For example, if you want to deny certain users to access a server group, you need to ceate a Deny rule for them; If you only want to allow one user to access a server group, you should create a Permit rule for this user first and then a Deny rule for other users.

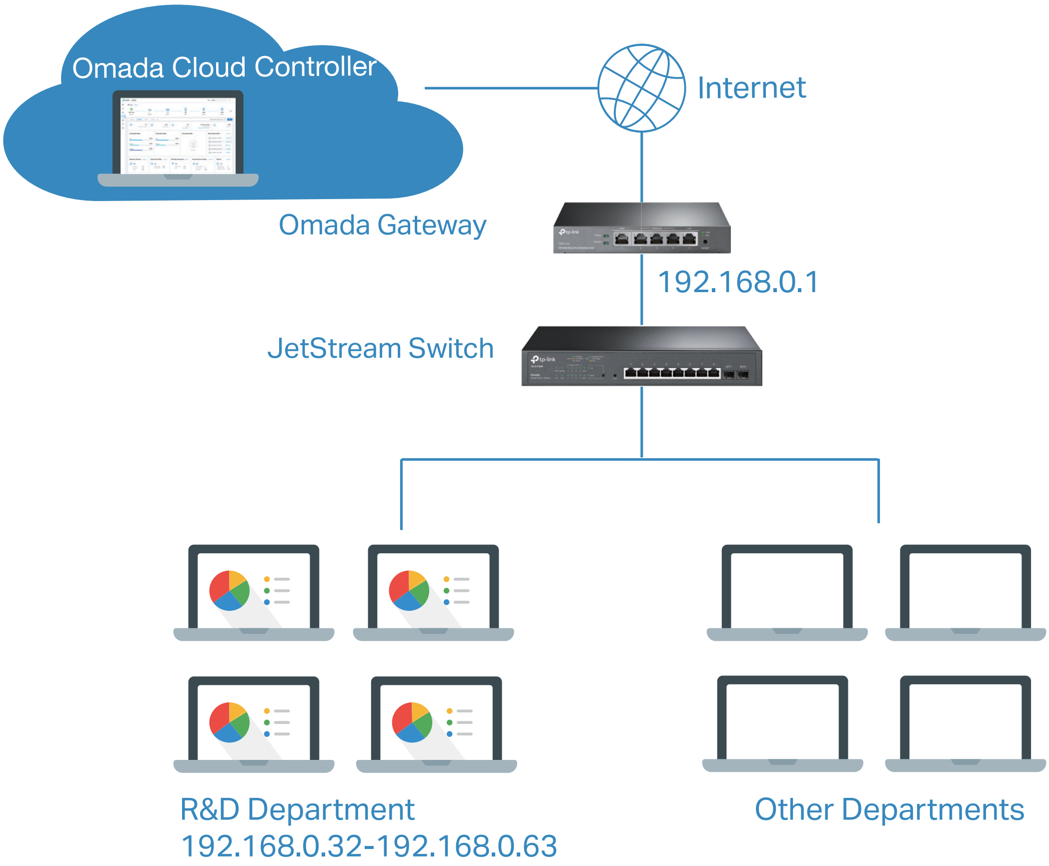
2 Configuration Example for ACL

2. 1 Gateway ACL

Gateway ACLs are configured on the controller, and then applied to the gateway to control traffic which is sourced from LAN ports and forwarded to the WAN ports. You can set the Network, IP address, and port number of a packet as packet-filtering criteria in ACL rules. Note that the gateway cannot use access control to restrict communications between devices and clients in LANs.

Network Requirements

The R&D and some other departments are connected to a layer 2 switch and access the internet via the gateway. To limit the acts of the R&D department users, it is required that the R&D users have no access to the internet. For other departments, there is no limitation.



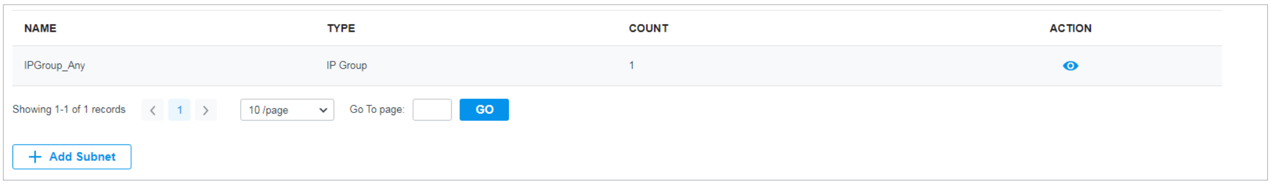
Configuration Scheme

1) Add an IP group for the R&D department in **Profiles** module.

2) Create a rule to restrict the data packets from the R&D department to be sent to the internet.

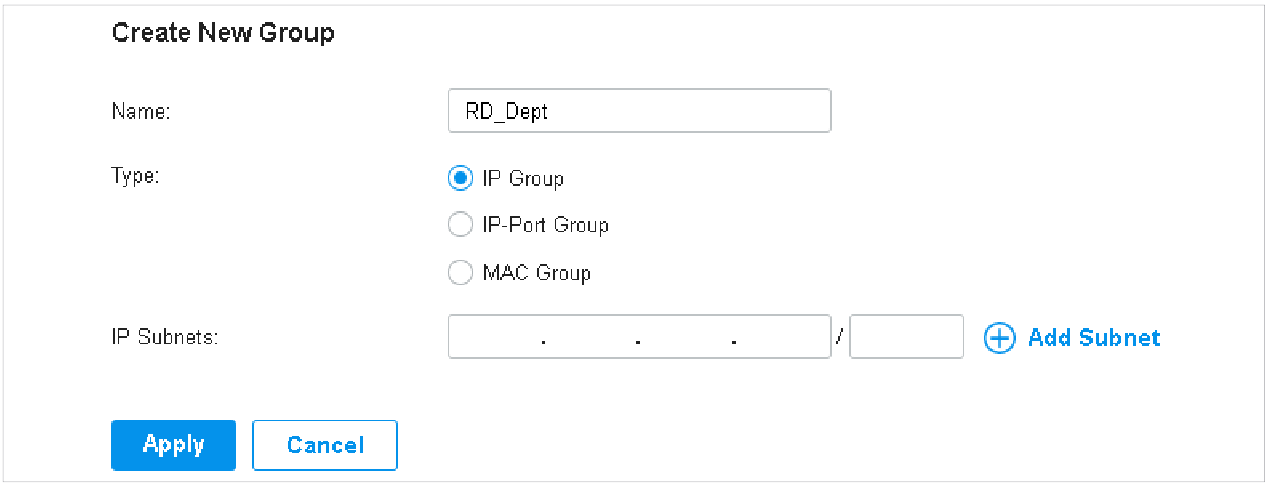
Follow the steps below to configure the ACL rule.

1. Go to Settings > Profiles > Groups. By default, there is an entry covering all IPs, and it is not editable and deletable. Click +Add Subnet to add a new group entry.



NAME	TYPE	COUNT	ACTION
IPGroup_Any	IP Group	1	👁

2. Specify the name of the IP group as “RD_Dept“, and select IP Group as the type.



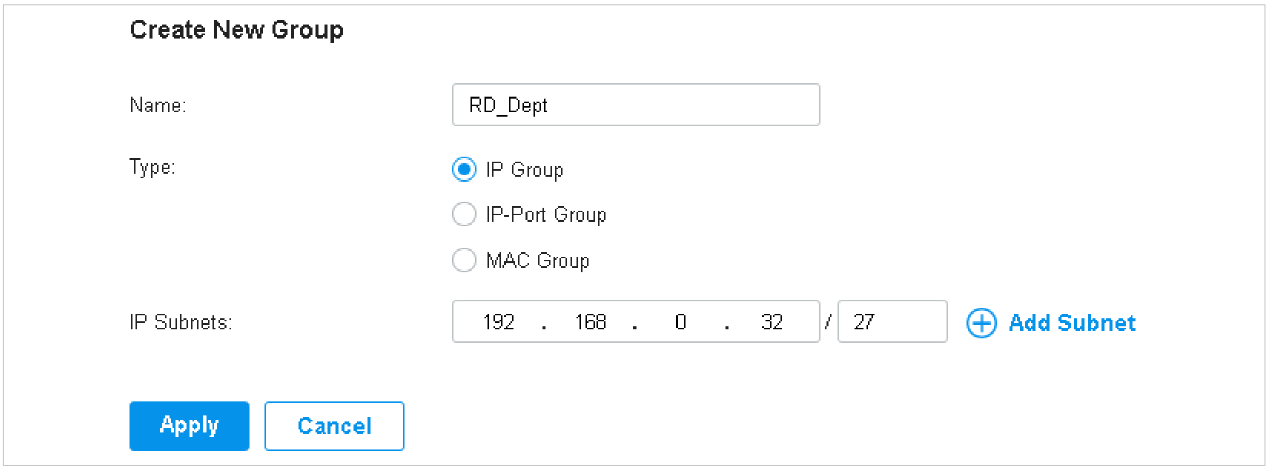
Create New Group

Name: RD_Dept

Type: ● IP Group ○ IP-Port Group ○ MAC Group

IP Subnets: . . . /

3. Specify the IP subnet as 192.168.0.32/27. IP subnet represents the range of IP addresses you want. In this example, 192.168.0.32 means the IP address and /27 means the number of bits in the mask. Click Apply.



Create New Group

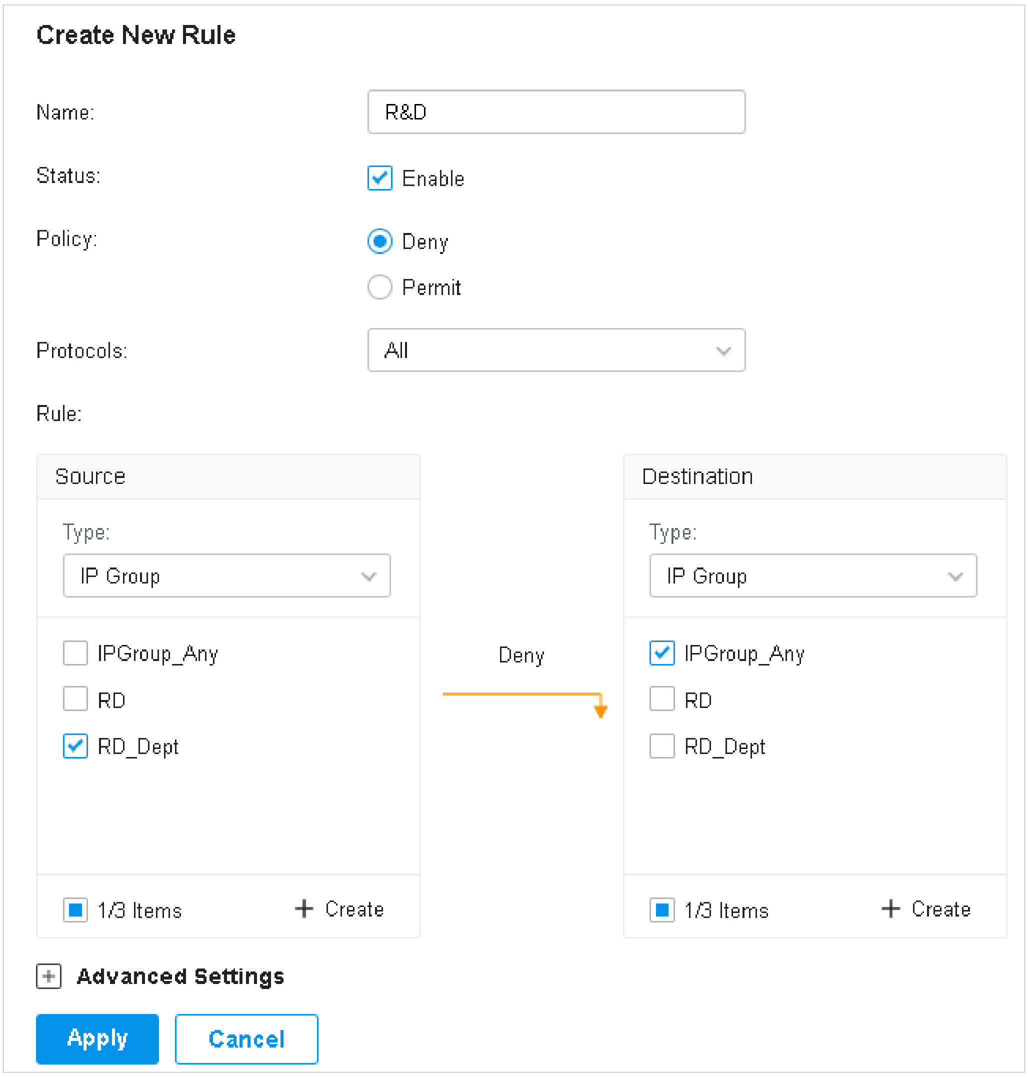
Name: RD_Dept

Type: ● IP Group ○ IP-Port Group ○ MAC Group

IP Subnets: 192 . 168 . 0 . 32 / 27

4. Go to Settings > Network Security > ACL. Under the Gateway ACL tab, click +Create New Rule.

5. Specify the name of the new rule as “R&D“. Select Deny as the rule policy, “RD_Dept” as the source IP group, “IPGROUP_ANY” as the destination IP group. Click Apply.



Create New Rule

Name: R&D

Status: ☑ Enable

Policy: ● Deny ○ Permit

Protocols: All

Rule:

Source

Type: IP Group

□ IPGroup_Any
□ RD
☑ RD_Dept

■ 1/3 Items + Create

Deny

Destination

Type: IP Group

☑ IPGroup_Any
□ RD
□ RD_Dept

■ 1/3 Items + Create

⊞ Advanced Settings

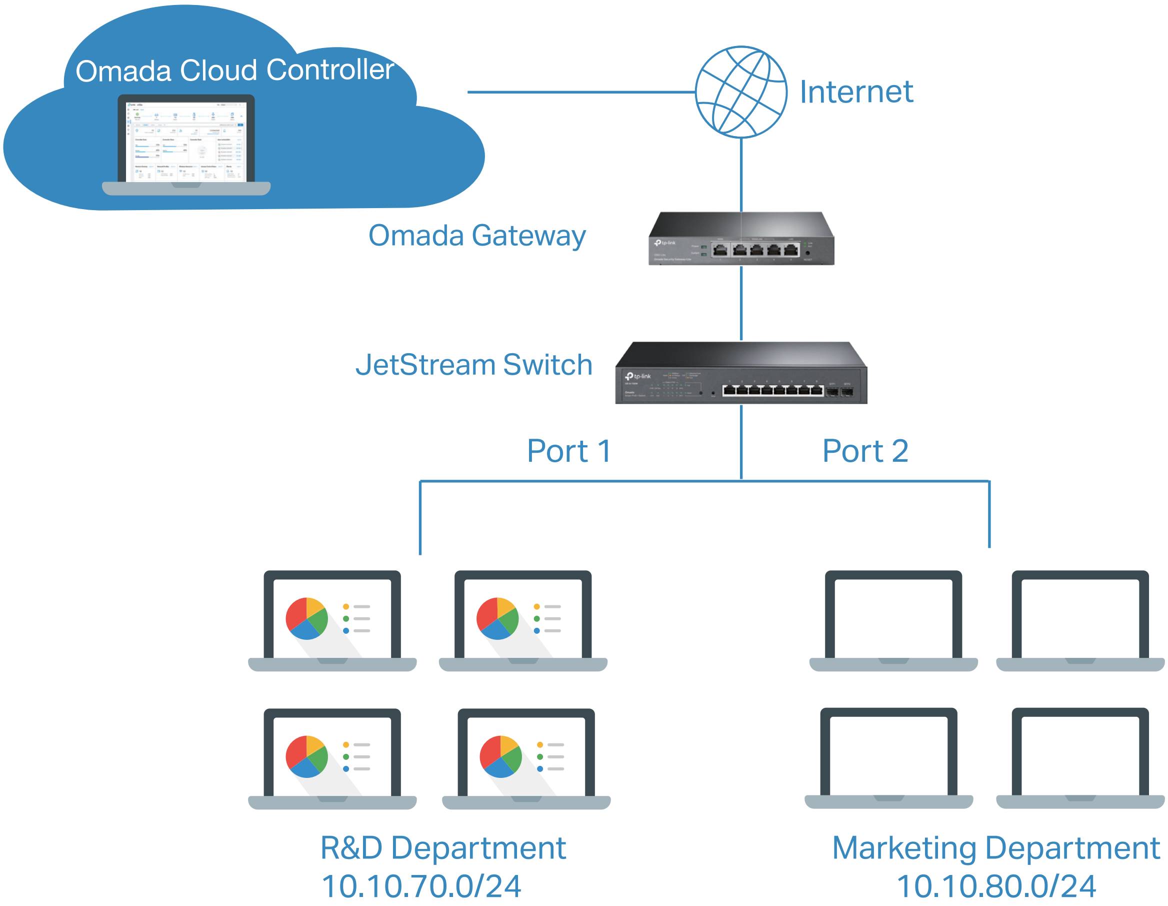
After configuration, all the data packets from the R&D department are not allowed to be transmitted from LAN to the internet at any time.

2. 2 Switch ACL

Switch ACLs are configured on the controller, and then applied to the switch to control inbound and outbound traffic through switch ports. You can set the Network, IP address, port number and MAC address of a packet as packet-filtering criteria in the rule.

Network Requirement:

A company forbids the employees in the R&D and Marketing department to access each other's resources. Computers in the R&D department are connected to the switch via port 1/0/1, and those of the Marketing department are connected to the switch via port 1/0/2.



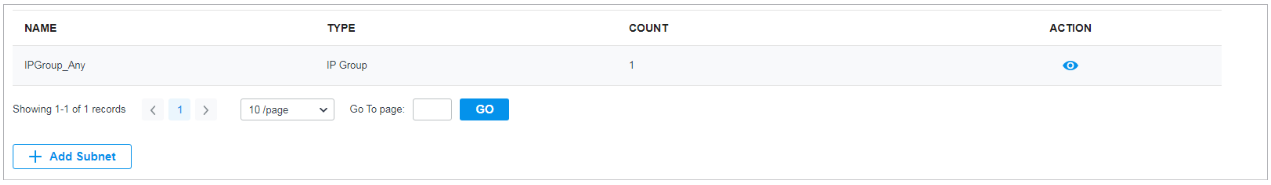
Configuration Scheme

1) Add two IP groups for the R&D department and Marketing department in **Profiles** module.

2) Create a rule to restrict the two departments from sending data packets to each other.

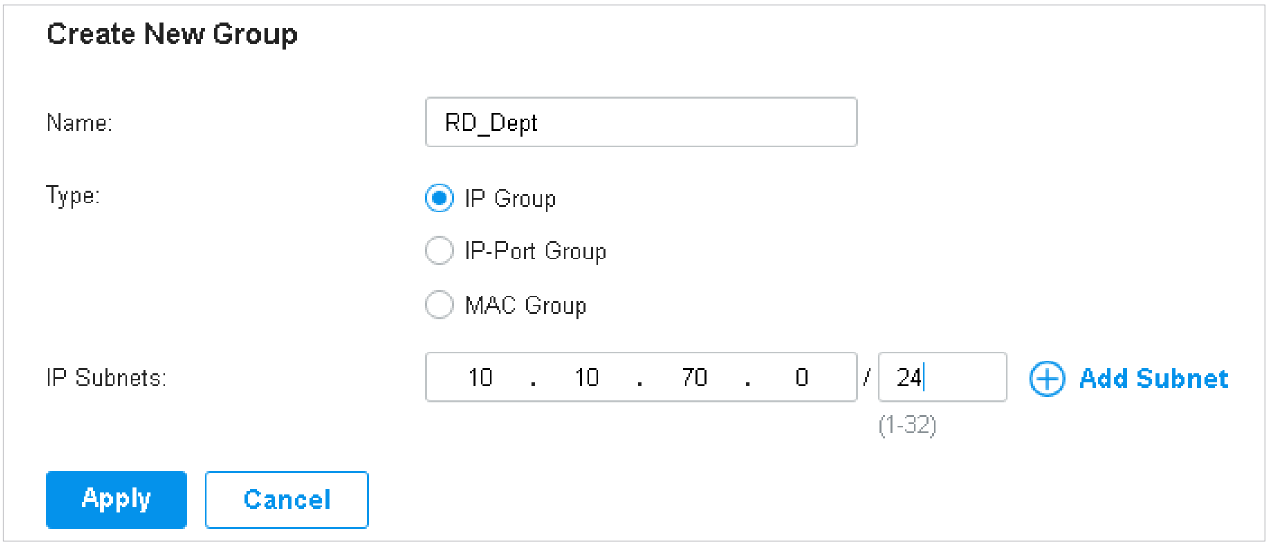
Follow the steps below to configure the ACL rule.

1. Go to Settings > Profiles > Groups. By default, there is an entry covering all IPs, and it is not editable and deletable. Click +Add Subnet to add two new group entries.



NAME	TYPE	COUNT	ACTION
IPGroup_Any	IP Group	1	👁

2. Specify the name of the IP group as “RD_Dept“, select IP Group as the type, and specify the IP subnet for R&D department. Click Apply.



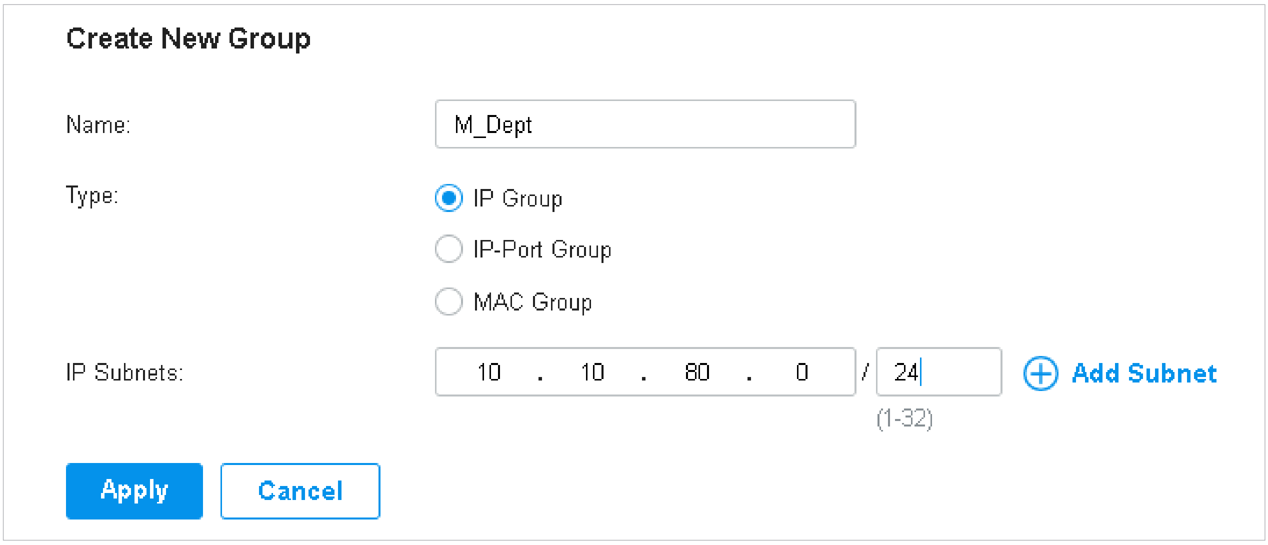
Create New Group

Name: RD_Dept

Type:
● IP Group
○ IP-Port Group
○ MAC Group

IP Subnets: 10 . 10 . 70 . 0 / 24 (1-32)

3. Specify the name of the IP group as “M_Dept“, select IP Group as the type, and specify the IP subnet for marketing department. Click Apply.



Create New Group

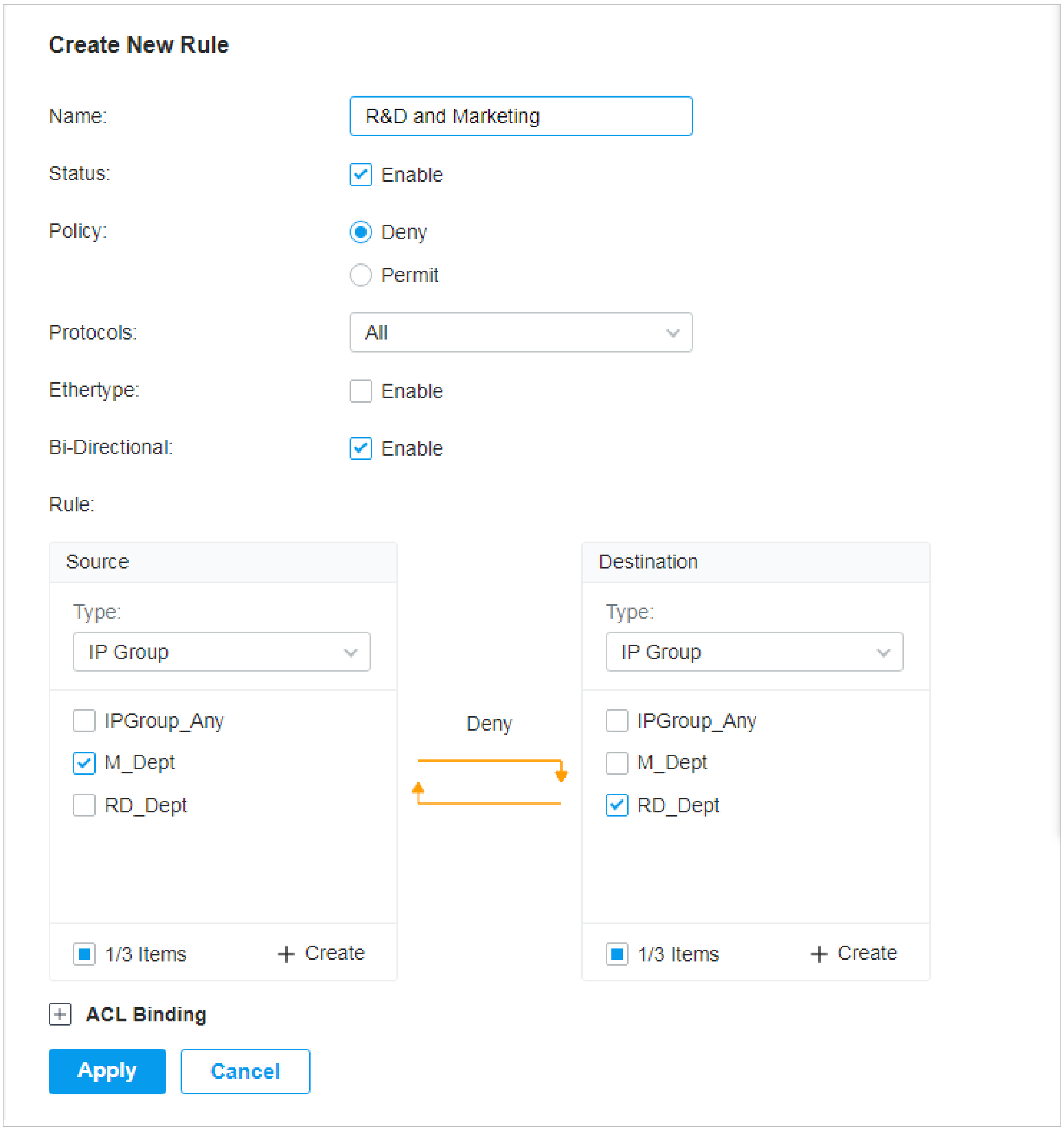
Name: M_Dept

Type:
● IP Group
○ IP-Port Group
○ MAC Group

IP Subnets: 10 . 10 . 80 . 0 / 24 (1-32)

4. Go to Settings > Network Security > ACL. Under the Switch ACL tab, click +Create New Rule .

5. Specify the name of the new rule as “R&D and Marketing“. Select Deny as the rule policy and check the box of Bi-Directional. Specify “M_Dept” as the source IP group, “RD_Dept” as the destination IP group.



Create New Rule

Name: R&D and Marketing

Status: ☑ Enable

Policy: ● Deny ○ Permit

Protocols: All

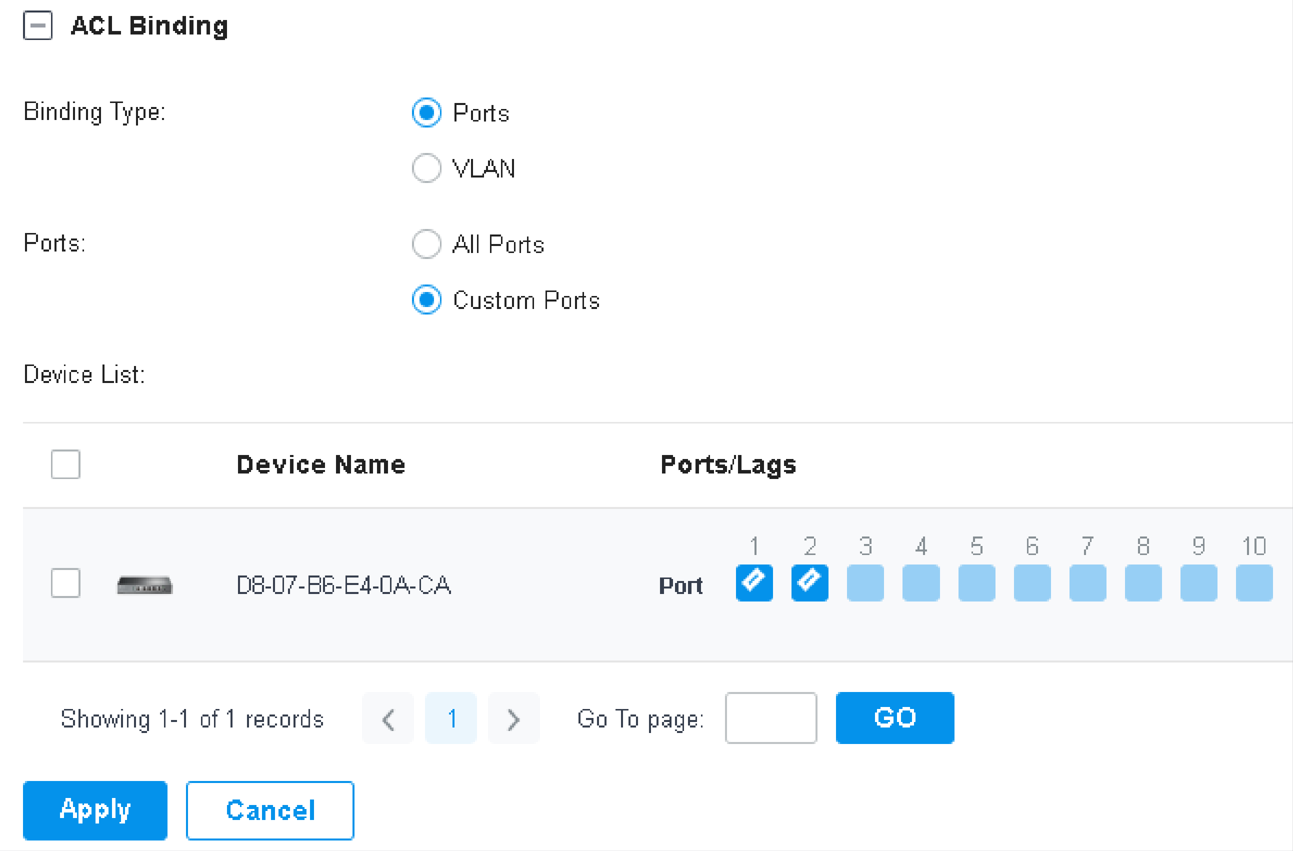
Ethertype: □ Enable

Bi-Directional: ☑ Enable

Rule:

Source	Destination
Type: IP Group	Type: IP Group
□ IPGroup_Any	□ IPGroup_Any
☑ M_Dept	□ M_Dept
□ RD_Dept	☑ RD_Dept
1/3 Items	1/3 Items

6. Select Ports as the binding type and Custom Ports as the ports. Bind the switch ACL to the switch port 1 and 2 and click Apply. Note that a switch ACL takes effect only after it is bound to a port or VLAN.



ACL Binding

Binding Type: ● Ports ○ VLAN

Ports: ○ All Ports ● Custom Ports

Device List:

□	Device Name	Ports/Lags
□	D8-07-B6-E4-0A-CA	Port 1 ☑ 2 ☑ 3 4 5 6 7 8 9 10

Showing 1-1 of 1 records

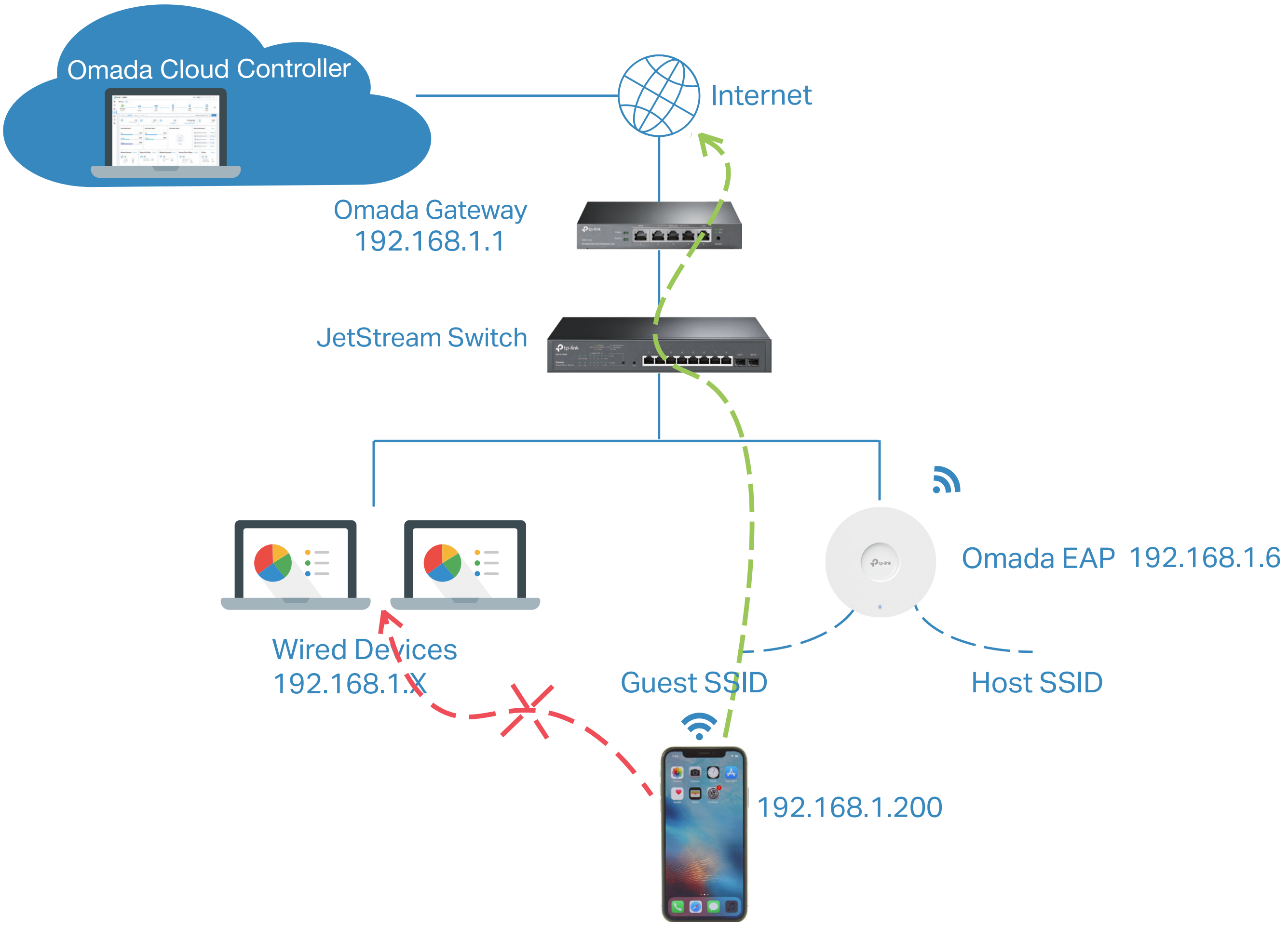
After configuration, the R&D department and marketing department are not allowed to send data packets to each other.

2.3 EAP ACL

EAP ACLs are configured on the controller, and then applied to the EAPs to control traffic in wireless networks. You can set the Network, IP address, port number and SSID of a packet as packet-filtering criteria in the rule.

Network Requirement:

Some customers may want to provide Wi-Fi access to the Internet for visitors. But they don’t want the visitor to access the local wired network or other wireless clients for security consideration.



Configuration Scheme

1) Add two IP groups for the wired devices and the gateway in **Profiles** module.

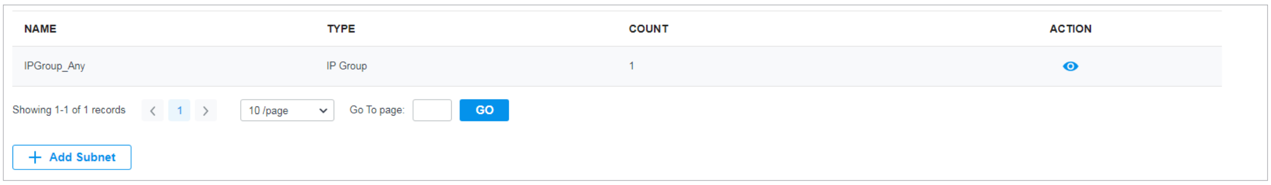
2) Add a new wireless network called Guest for visitors.

3) Create a Permit rule to allow the wireless devices connected to the guest network to get access to the internet through gateway.

4) Create a Deny rule to restrict these wireless devices from sending data packets to the devices in the subnet (192.168.1.0 -- 192.168.1.255) .

Follow the steps below to configure the ACL rule.

1. Go to Settings > Profiles > Groups. By default, there is an entry covering all IPs, and it is not editable and deletable. Click +Add Subnet to add a new group entry.

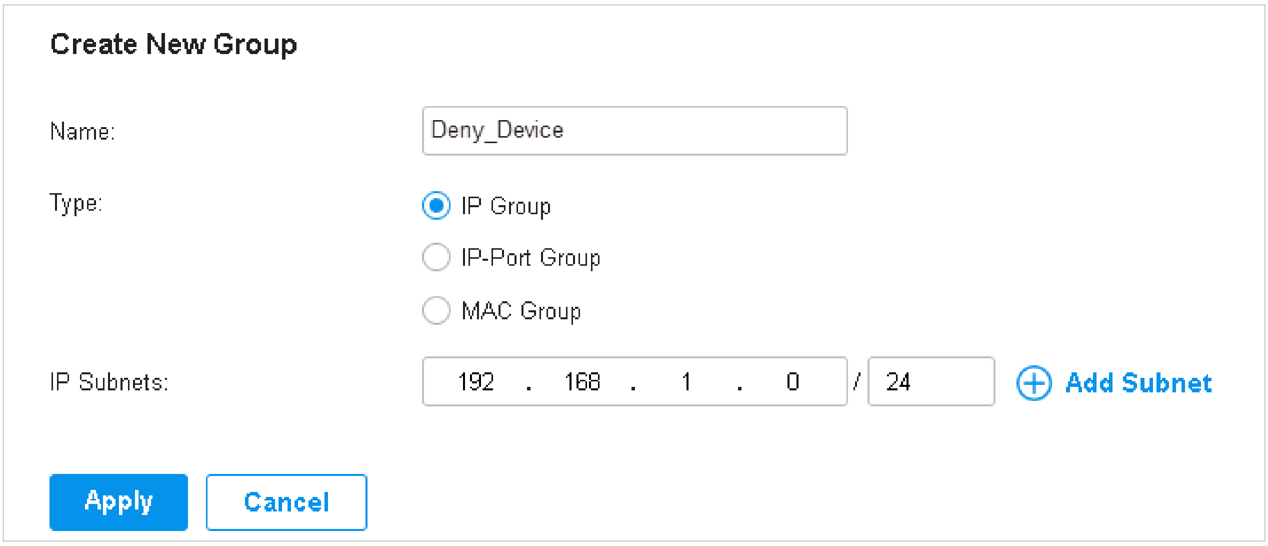


NAME	TYPE	COUNT	ACTION
IPGroup_Any	IP Group	1	👁

Showing 1-1 of 1 records < 1 > 10 /page Go To page: GO

+ Add Subnet

2. Specify the name of the IP group as "Deny_Device", select IP Group as the type, and specify the IP subnet as 192.168.1.0/24. Click Apply.



Create New Group

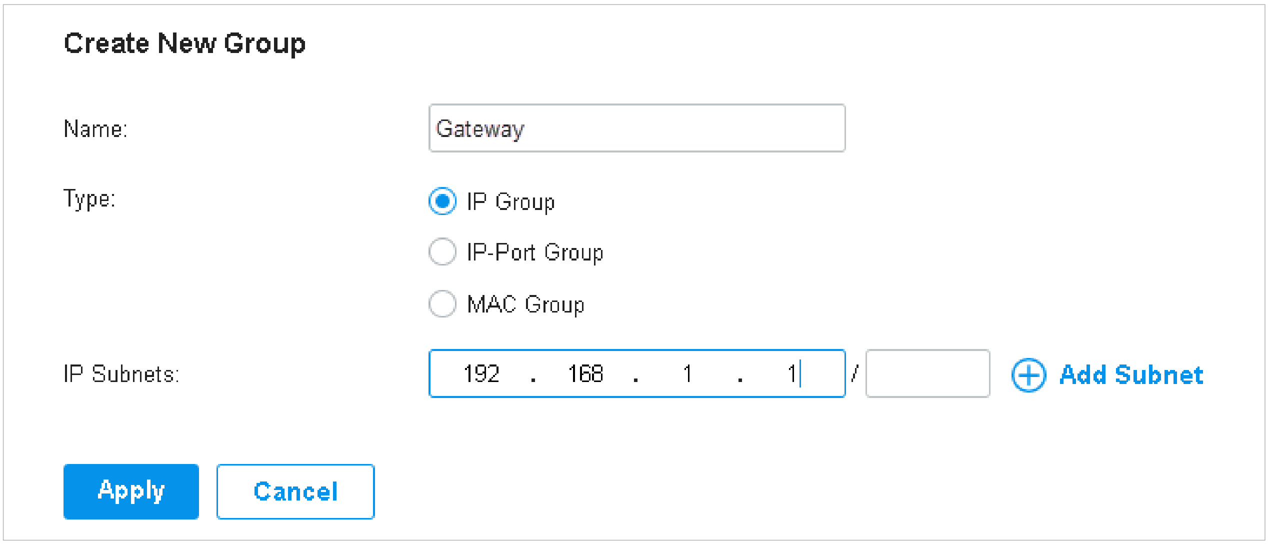
Name: Deny_Device

Type:
● IP Group
○ IP-Port Group
○ MAC Group

IP Subnets: 192 . 168 . 1 . 0 / 24 ⊕ Add Subnet

Apply Cancel

3. Specify the name of the IP group as "Gateway", select IP Group as the type, and specify the IP subnet as 192.168.1.1. Click Apply.



Create New Group

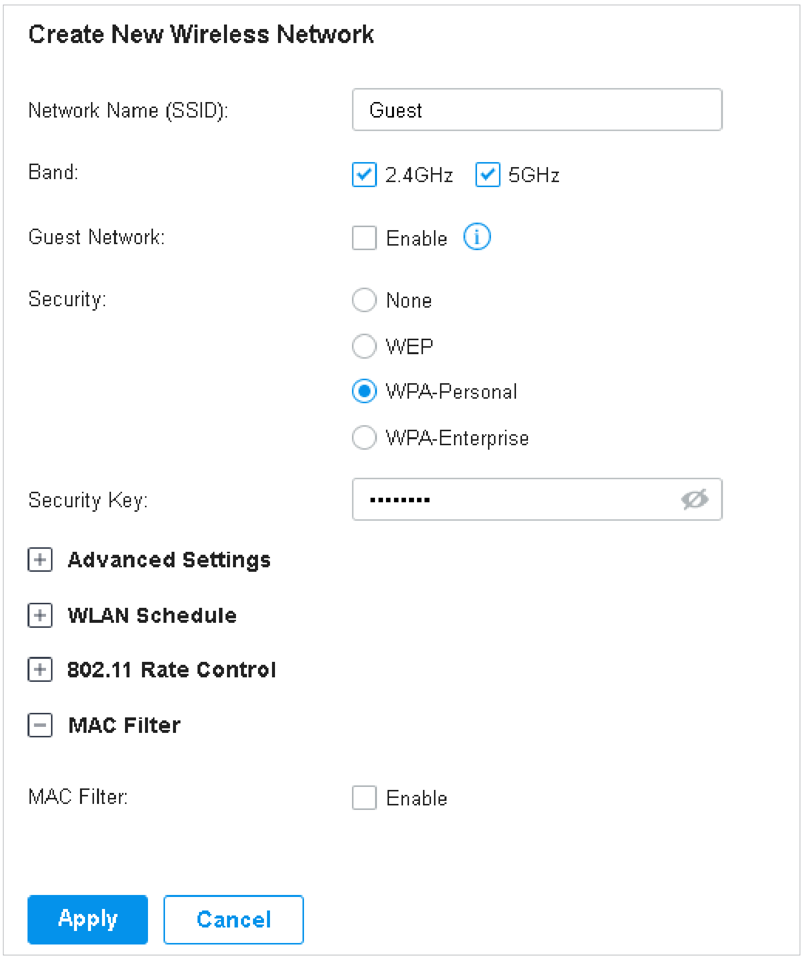
Name: Gateway

Type:
● IP Group
○ IP-Port Group
○ MAC Group

IP Subnets: 192 . 168 . 1 . 1 / ⊕ Add Subnet

Apply Cancel

4. Go to Settings > Wireless Networks. Click +Create New Wireless Network. Specify the network name and security key. Click Apply.



Create New Wireless Network

Network Name (SSID): Guest

Band: ☑ 2.4GHz ☑ 5GHz

Guest Network: □ Enable

Security: ○ None ○ WEP ● WPA-Personal ○ WPA-Enterprise

Security Key: ••••••••

⊞ Advanced Settings

⊞ WLAN Schedule

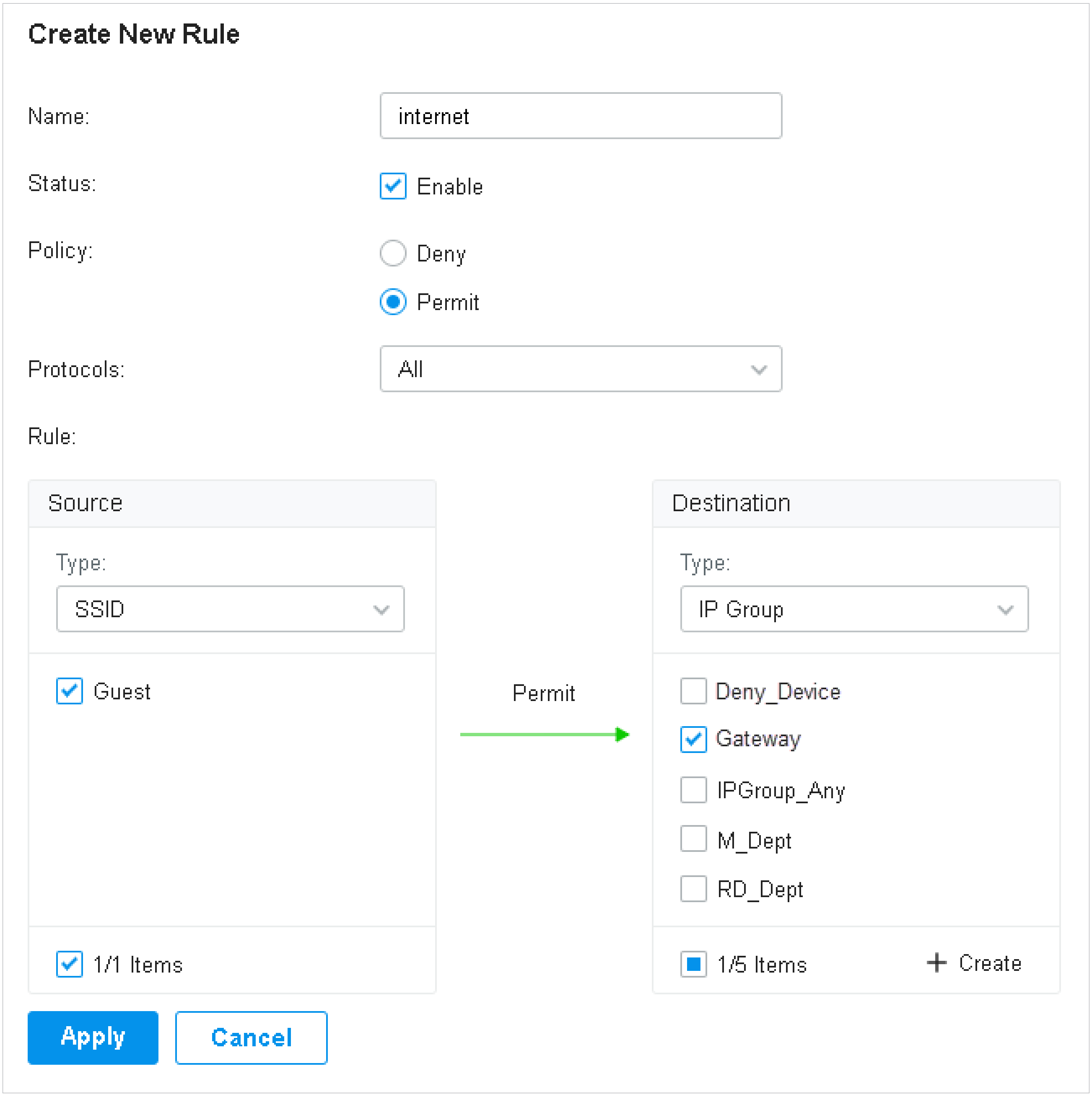
⊞ 802.11 Rate Control

⊟ MAC Filter

MAC Filter: □ Enable

5. Go to Settings > Network Security > ACL. Under the EAP ACL tab, click +Create New Rule .

6. To connect to the internet, you must not block the gateway. Specify the name of the first rule as “internet“. Select Permit as the rule policy, “Guest” as the source SSID, “Gateway” as the destination IP group. Click Apply.



Create New Rule

Name: internet

Status: ☑ Enable

Policy: ○ Deny ● Permit

Protocols: All

Rule:

Source

Type: SSID

☑ Guest

☑ 1/1 Items

Permit

Destination

Type: IP Group

□ Deny_Device

☑ Gateway

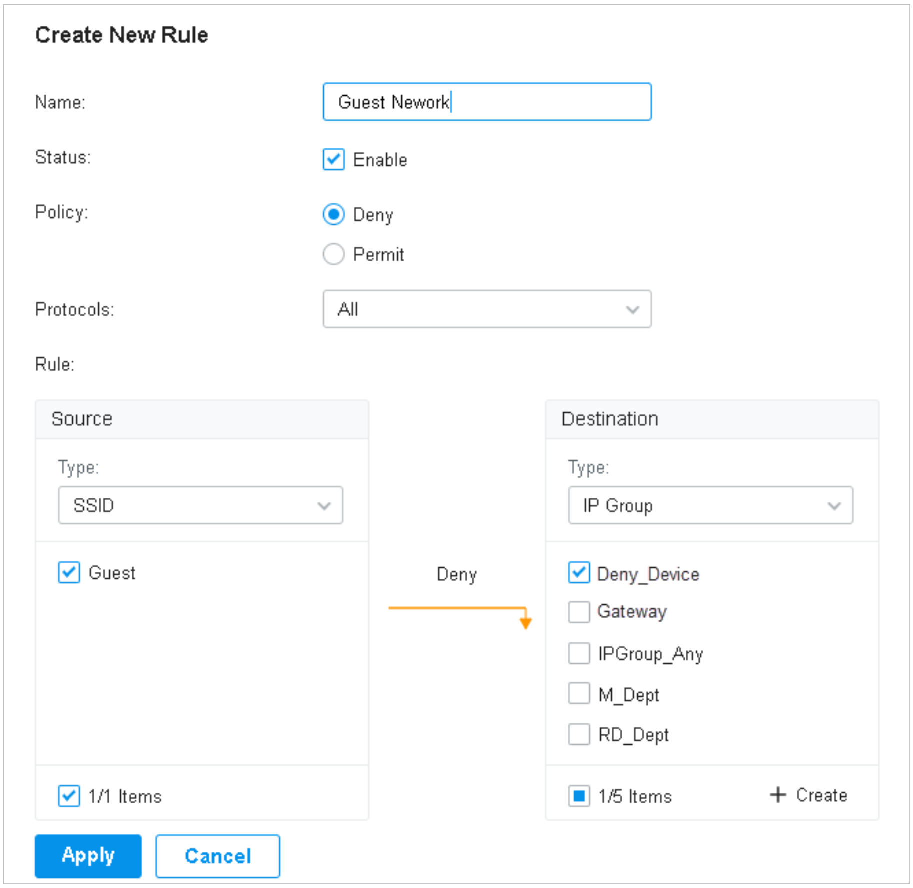
□ IPGroup_Any

□ M_Dept

□ RD_Dept

■ 1/5 Items

7. To stop the wireless devices connected to the guest network visiting wired devices, specify the name of the second rule as “Guest Network“. Select Deny as the rule policy, “Guest” as the source SSID, “Deny_Device” as the destination IP group. Click Apply.



Create New Rule

Name: Guest Nework

Status: ☑ Enable

Policy: ● Deny ○ Permit

Protocols: All

Rule:

Source

Type: SSID

☑ Guest

☑ 1/1 Items

Destination

Type: IP Group

☑ Deny_Device
□ Gateway
□ IPGroup_Any
□ M_Dept
□ RD_Dept

■ 1/5 Items

After configuration, the wirless devices connecting to the guest network cannot send data packets to the devices in the subnet (192.168.1.0 -- 192.168.1.255) .