

INTELBRAS Access Controllers IPS Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring IPS	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides examples for configuring IPS.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of IPS.

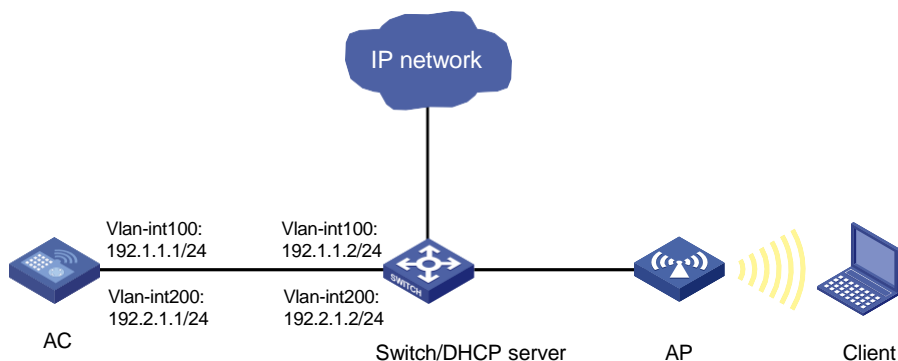
Example: Configuring IPS

Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and client. The AP and AC establish CAPWAP tunnels in VLAN 100. The client accesses the wireless network in VLAN 200.

Configure the AC to use the default IPS policy for attack detection and prevention.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AP will obtain this IP address to establish CAPWAP tunnels with the AC.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will access the wireless network in this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the port connected to the switch) to trunk. Prevent traffic from VLAN 1 from passing through the port and allow traffic from VLAN 100 and VLAN 200 to pass through the port.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a wireless service:

Create service template 1 and enter service template view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Assign the client to VLAN 200 after it comes online.

```
[AC-wlan-st-1] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-1] akm mode psk
```

```
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-1] client forwarding-location ac
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **ap1** with model **AP 3620**.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to 219801A28N819CE0002T.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-ap1] quit
```

Create AP group **group1** and add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template 1 to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

4. Configure an IP address object group named **ipsfilter** and specify subnet 192.2.1.0/24 for the object group.

```
[AC] object-group ip address ipsfilter
```

```
[AC-obj-grp-ip-ipsfilter] network subnet 192.2.1.0 24
```

```
[AC-obj-grp-ip-ipsfilter] quit
```

5. Apply the default IPS policy to a DPI application profile and activate the IPS policy settings:

Create a DPI application profile named **sec** and enter its view. Apply the default IPS policy to the DPI application profile and set the policy mode to **protect**.

```
[AC] app-profile sec
```

```
[AC-app-profile-sec] ips apply policy default mode protect
```

```
[AC-app-profile-sec] quit
```

Activate the IPS policy settings.

```
[AC] inspect activate
```

6. Configure a security policy:

Enter IPv4 security policy view.

```
[AC] security-policy ip
```

Create a rule named **ipsfilter** to permit the traffic destined for IP addresses in IP address object group **ipsfilter** and apply DPI application profile **sec** to the security group.

```
[AC-security-policy-ip] rule name ipsfilter
```

```
[AC-security-policy-ip-10-ipsfilter] destination-ip ipsfilter
```

```
[AC-security-policy-ip-10-ipsfilter] action pass
```

```
[AC-security-policy-ip-10-ipsfilter] profile sec
```

```
[AC-security-policy-ip-10-ipsfilter] quit
```

Activate rule matching acceleration.

```
[AC-security-policy-ip] accelerate enhanced enable
```

```
[AC-security-policy-ip] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLANs 100 and 200, create VLAN-interface 100 and VLAN-interface 200, and assign IP addresses to VLAN-interface 100 and VLAN-interface 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and use VLAN 200 to forward client traffic.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100 and VLAN 200.

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100.

```
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Specify the PVID of the trunk port as VLAN 100.

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] quit
```

Enable PoE on the trunk port.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100** to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24.

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
```

Specify a gateway.

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named `vlan200` to assign IP addresses and other configuration parameters to clients on subnet 192.2.1.0/24.

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
```

Specify a gateway and a DNS server.

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

Verify that the AC can use the default IPS policy to detect and prevent known network attacks. (Details not shown.)

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
object-group ip address ipsfilter
 0 network subnet 192.2.1.0 255.255.255.0
#
wlan service-template 1
  ssid service
vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface100
 ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
```

```

port trunk permit vlan 100 200
#
app-profile sec
ips apply policy default mode protect
#
wlan ap-group group1
ap ap1
ap-model AP 3620
radio 1
    radio 2
    radio enable
    service-template 1
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
security-policy ip
rule 10 name ipsfilter
    action pass
    profile sec
    destination-ip ipsfilte

```

- **Switch:**

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 192.1.1.1
network 192.1.1.0 mask 255.255.255.0
forbidden-ip 192.1.1.1 192.1.1.2
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.2
network 192.2.1.0 mask 255.255.255.0
dns-list 192.2.1.2
forbidden-ip 192.2.1.1 192.2.1.2
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk

```



```
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
poe enable
#
```

Related documentation

- *IPS Command Reference in INTELBRAS Access Controllers Command References*
- *IPS Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

URL Filtering Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring URL filtering	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides an example of configuring URL filtering.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of URL filtering and security policy.

Example: Configuring URL filtering

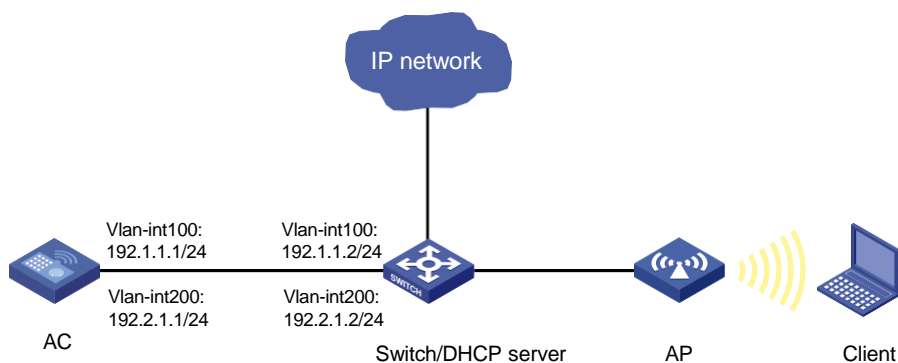
Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and client. The AP and AC establish CAPWAP tunnels in VLAN 100. The client accesses the wireless network in VLAN 200.

Configure a URL filtering policy on the AC so the AC performs the following operations:

- Permits the client to access website **<http://www.sina.com>** on the IP network.
- Drops and logs packets that match the Pre-Game URL category.
- Drops and logs packets that do not match any filtering rule in the URL filtering policy.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AP will obtain this IP address to establish CAPWAP tunnels with the AC.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will access the wireless network in this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the interface connected to the switch) to trunk. Remove the interface from VLAN 1, and allow traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a wireless service:

Create service template 1 and enter service template view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Assign the client to VLAN 200 after it comes online.

```
[AC-wlan-st-1] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-1] client forwarding-location ac
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create a manual AP named **ap1**, and specify the AP model.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to 219801A28N819CE0002T.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-ap1] quit
```

Create AP group **group1** and add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template **1** to radio **2** in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio **2**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

4. Configure an IP address object group named **urlfilter** and specify subnet 192.2.1.0/24 for the object group.

```
[AC] object-group ip address urlfilter
```

```
[AC-obj-grp-ip-urlfilter] network subnet 192.2.1.0 24
```

```
[AC-obj-grp-ip-urlfilter] quit
```

5. Configure URL filtering:

Create a URL category named **news**, set its severity level to 2000, and enter URL category view.

```
[AC] url-filter category news severity 2000
```

Create URL filtering rule **1** to match HTTP packets that contain host name **www.sina.com** in the URL.

```
[AC-url-filter-category-news] rule 1 host text www.sina.com
```

```
[AC-url-filter-category-news] quit
```

Create a URL filtering policy named **urlnews** and enter URL filtering policy view.

```
[AC] url-filter policy urlnews
```

In the URL filtering policy, specify action **permit** for URL category **news**.

```
[AC-url-filter-policy-urlnews] category news action permit
```

In the URL filtering policy, specify action **drop** for predefined URL category **Pre-Games** and enable logging for the matching packets.

```
[AC-url-filter-policy-urlnews] category Pre-Games action drop logging
```

In the URL filtering policy, set the default actions to **drop** and **logging**.

```
[AC-url-filter-policy-urlnews] default-action drop logging
```

```
[AC-url-filter-policy-urlnews] quit
```

6. Configure a DPI application profile:

Create a DPI application profile named **sec** and enter DPI application profile view.

```
[AC] app-profile sec
```

Apply URL filtering policy **urlnews** to the DPI application profile.

```
[AC-app-profile-sec] url-filter apply policy urlnews
[AC-app-profile-sec] quit
```

Activate the URL filtering policy and rule settings.

```
[AC] inspect activate
```

7. Apply the DPI application profile to a security policy:

Enter IPv4 security policy view.

```
[AC] security-policy ip
```

Create a rule named **urlfilter** to permit the traffic from IP addresses in IP address object group **urlfilter** and apply DPI application profile **sec** to the security policy.

```
[AC-security-policy-ip] rule name urlfilter
[AC-security-policy-ip-13-urlfilter] source-ip urlfilter
[AC-security-policy-ip-13-urlfilter] action pass
[AC-security-policy-ip-13-urlfilter] profile sec
[AC-security-policy-ip-13-urlfilter] quit
```

Activate rule matching acceleration.

```
[AC-security-policy-ip] accelerate enhanced enable
[AC-security-policy-ip] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward CAPWAP tunnel traffic between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. This VLAN will be used to forward wireless client packets.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the interface connected to the AC) to trunk. Remove the interface from VLAN 1, and allow traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 (the interface connected to the AP) to trunk. Remove the interface from VLAN 1, allow traffic from VLAN 100 to pass through the interface, and set the PVID of the interface to 100.

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP settings:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100 to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
```

Specify a gateway.

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200 to assign IP addresses and other configuration parameters to clients on subnet 192.2.1.0/24.**

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
```

Specify a gateway and a DNS server.

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

Verify that the client can access website **http://www.sina.com on the IP network. (Details not shown.)**

Verify that the device drops and logs the client's HTTP requests to game resources. (Details not shown.)

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
object-group ip address urlfilter
0 network subnet 192.2.1.0 255.255.255.0
```



```

#
wlan service-template 1
    ssid service
vlan 200
client forwarding-location ac
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
service-template enable
#
interface Vlan-interface100
    ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
url-filter policy urlnews
    default-action drop logging
    category news action permit
    category Pre-Games action drop logging
#
url-filter category news severity 2000
    rule 1 host text www.sina.com
#
app-profile sec
    url-filter apply policy urlnews
#
wlan ap-group group1
    ap ap1
    ap-model AP 3620
radio 1
    radio 2
    radio enable
    service-template 1
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
security-policy ip
    rule 13 name urlfilter
    action pass
    profile sec

```

```

        source-ip urlfilter
#
• Switch:
#
    dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 192.1.1.1
    network 192.1.1.0 mask 255.255.255.0
    forbidden-ip 192.1.1.1 192.1.1.2
#
dhcp server ip-pool vlan200
    gateway-list 192.2.1.2
    network 192.2.1.0 mask 255.255.255.0
    dns-list 192.2.1.2
    forbidden-ip 192.2.1.1 192.2.1.2
#
interface Vlan-interface100
    ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100
    port trunk pvid vlan 100
    poe enable
#

```

Related documentation

- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *URL Filtering Command Reference in INTELBRAS Access Controllers Command References*
- *URL Filtering Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Anti-Virus Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring anti-virus	1
Network configuration	1
Restrictions and guidelines	1
Procedures	1
Configuring the AC	1
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	8

Introduction

The following information provides an example of configuring anti-virus.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the anti-virus feature.

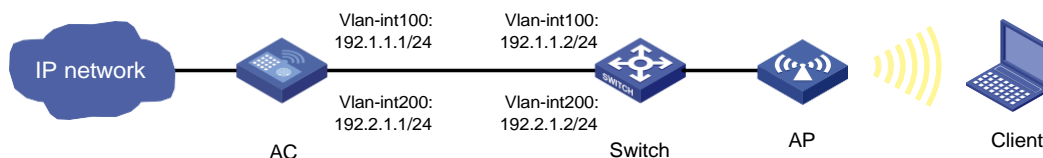
Example: Configuring anti-virus

Network configuration

As shown in [Figure 1](#), the AC connects the LAN and the Internet. The client uses a Web server and a mail server on the Internet to transport files and emails.

Configure the AC to use an anti-virus policy to detect and prevent viruses in the files and emails downloaded by the client.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Configure the AC to forward client data traffic (the centralized forwarding mode).

Procedures

Configuring the AC

Configuring basic settings

1. Configure interfaces on the AC:

Create VLAN 100. Create VLAN-interface 100 and assign an IP address to the VLAN interface. The AP will obtain this IP address to establish a CAPWAP tunnel with the AC.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200. Create VLAN-interface 200 and assign an IP address to the VLAN interface. The client will access the wireless network through this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Configure the interface connected to the switch as a trunk port that permits VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure the wireless service:

Create service template 1 and enter its view.

```
[AC] wlan service-template 1
```

Configure the SSID as **service**.

```
[AC-wlan-st-1] ssid service
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-1] akm mode psk
```

```
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-1] client forwarding-location ac
```

Assign clients coming online to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **ap1** with model **AP 3620**.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID of AP **ap1** to **219801A28N819CE0002T**.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
# Create AP group group1 and add AP ap1 to AP group group1.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
# Bind service template 1 to radio 1 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
# Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
# Bind service template 1 to radio 2 in AP group group1.
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
# Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

Configuring an object group

Create an IP address object group named **antivirus**, and specify its subnet as 192.2.1.0/24.

```
<AC> system-view
[AC] object-group ip address antivirus
[AC-obj-grp-ip-antivirus] network subnet 192.2.1.0 24
[AC-obj-grp-ip-antivirus] quit
```

Configuring an anti-virus policy

Create an anti-virus policy named **down_av** and enter its view.

```
[AC] anti-virus policy down_av
```

Configure anti-virus for FTP and SMB in download direction and specify the anti-virus action as block.

```
[AC-anti-virus-policy-down_av]inspect ftp direction download action block
[AC-anti-virus-policy-down_av]inspect smb direction download action block
```

Configure anti-virus for IMAP in download direction and specify the anti-virus action as alert.

```
[AC-anti-virus-policy-down_av]inspect imap direction download action alert
```

Set the **Alibaba** application as an application exception. Specify alert as the anti-virus action for the application exception.

```
[AC-anti-virus-policy-down_av]exception application Alibaba action alert
[AC-anti-virus-policy-down_av] quit
```

Configuring a DPI application profile and activate the anti-virus policy settings

Create a DPI application profile named **sec**, and enter its view.

```
[AC] app-profile sec
```

Apply anti-virus policy **down_av** to DPI application profile **sec**. Set the anti-virus policy mode to **protect**.

```
[AC-app-profile-sec] anti-virus apply policy down_av mode protect
[AC-app-profile-sec] quit
```

Activate the anti-virus policy settings.

```
[AC] inspect activate
```

Configuring an anti-virus security policy

Enter IPv4 security policy view.

```
[AC] security-policy ip
```

Create a security policy rule named **av**. Configure the matching conditions as the source IP address object group **antivirus**, FTP service, SMB service, IMAP service, AP **ap1**, AP group **default-group**, and SSID **service**.

```
[AC-security-policy-ip] rule name av
[AC-security-policy-ip-10-av] source-ip antivirus
[AC-security-policy-ip-10-av] service ftp
[AC-security-policy-ip-10-av] service smb
[AC-security-policy-ip-10-av] service imap
[AC-security-policy-ip-10-av] ap ap1
[AC-security-policy-ip-10-av] ap-group default-group
[AC-security-policy-ip-10-av] ssid service
```

Configure the security action as pass and specify DPI application profile **sec**.

```
[AC-security-policy-ip-10-av] action pass
[AC-security-policy-ip-10-av] profile sec
[AC-security-policy-ip-10-av] quit
```

Activate rule matching acceleration.

```
[AC-security-policy-ip] accelerate enhanced enable
[AC-security-policy-ip] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100, VLAN-interface 100, VLAN 200, VLAN-interface 200, and assign IP addresses to the VLAN interfaces. The switch will use VLAN 100 to forward CAPWAP tunnel traffic between the AC and the AP, and use VLAN 200 to forward wireless client packets.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the interface connected to the AC) to trunk. Allow traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 (the interface connected to the AP) to trunk. Allow traffic from VLAN 100 to pass through the interface.


```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP settings:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100 to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24. Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation. Specify the gateway address as 192.1.1.1.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200 to assign IP addresses and other configuration parameters to clients on subnet 192.2.1.0/24. Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation. Specify a gateway and a DNS server.**

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.1
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.1
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

View anti-virus statistics by using the **display anti-virus statistics command on the AC.**

```
[AC] display anti-virus statistics
Slot 1:
Total Block:      2
Total Redirect:   0
Total Alert:      1
Type              http      ftp      smtp      pop3      imap      smb      nfs
Block             0        1        0        0        0        1        0
Redirect           0        0        0        0        0        0        0
Alert+Permit       0        0        0        0        1        0        0
```

Configuration files

- AC:


```
#
vlan 100
```

```

#
vlan 200
#
wlan service-template 1
    ssid service
    vlan 200
    akm mode psk
    preshared-key pass-phrase cipher $c$3$29gn1DalRVhkcyZ1CKwevH+xb6Lxopy3eq/H
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group1
vlan 1
ap ap1
ap-model AP 3620
    radio 1
        radio enable
        service-template 1
    radio 2
        radio enable
        service-template 1
    gigabitethernet 1
#
object-group ip address antivirus
    0 network subnet 192.2.1.0 255.255.255.0
#
app-profile sec
    anti-virus apply policy down_av mode protect
#
security-policy ip
    rule 1 name av
        action pass
    profile sec
    source-ip antivirus

```

```

service ftp
service smb
service imap
ap ap1
ap-group default-group
ssid service

#
anti-virus policy down_av
inspect ftp direction download action block
inspect imap direction download action alert
inspect smb direction download action block
exception application Alibaba action alert

```

- **Switch:**

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.2 255.255.255.0
#
dhcp server ip-pool vlan100
network 192.1.0.0 mask 255.255.255.0
forbidden-ip 192.1.1.1 192.1.1.2
gateway-list 192.1.1.1
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.1
network 192.2.1.0 mask 255.255.255.0
forbidden-ip 192.2.1.1 192.2.1.2
dns-list 192.2.1.1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable

```

Related documentation

- *Anti-Virus Command Reference in INTELBRAS Access Controllers Command References*
- *Anti-Virus Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Data Filtering Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring data filtering	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	5
Verifying the configuration	6
Configuration files	6
Related documentation	8

Introduction

The following information provides an example of configuring data filtering.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of data filtering and security policy.

Example: Configuring data filtering

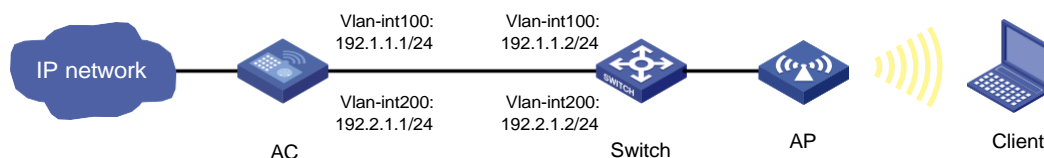
Network configuration

As shown in [Figure 1](#), the AC connects to the external network.

Configure data filtering on the AC so the AC performs the following operations:

- Blocks HTTP packets that contain the **uri** or **abc.*abc** string in the URI field or message body.
- Blocks download FTP traffic that contains the **www.abcd.com/** string.
- Logs the blocked packets.

Figure 1 Network diagram



Restrictions and guidelines

- Use the actual serial ID of an AP to uniquely identify that AP.
- Configure the AC to forward client traffic.

Procedures

Configuring the AC

Configuring the basic AC features

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AP will obtain this IP address to establish CAPWAP tunnels with the AC.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will access the wireless network in this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the interface connected to the switch) to trunk, and allow traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a wireless service:

Create service template 1 and enter service template view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Set the AKM mode to PSK and configure simple character string **12345678** as the PSK.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Set the AES-CCMP cipher suite for frame encryption, and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client traffic. If the default client traffic forwarding location is the same as the configuration in this step, you can skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Assign the client to VLAN 200 after it comes online.

```
[AC-wlan-st-1] vlan 200
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```


3. Configure the AP:

❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **ap1**, and specify the AP model.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to 219801A28N819CE0002T.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-ap1] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template 1 to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

Bind service template 1 to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
```

```
return
```

Configuring an object group

Configure an IP address object group named **datafilter** and specify subnet 192.2.1.0/24 for the object group.

```
<AC> system-view
```

```
[AC] object-group ip address datafilter
```

```
[AC-obj-grp-ip-datafilter] network subnet 192.2.1.0 24
```

```
[AC-obj-grp-ip-datafilter] quit
```

Configuring data filtering

1. Configure keyword groups:

Create a keyword group named **kg1** and enter its view.

```
[AC] data-filter keyword-group kg1
```

Create two keyword match patterns that match the **uri** text string and the **abc.*abc** regular expression string, respectively.

```
[AC-data-filter-kgroup-kg1] pattern 1 text uri
```

```
[AC-data-filter-kgroup-kg1] pattern 2 regex abc.*abc
```

```
[AC-data-filter-kgroup-kg1] quit
```

Create a keyword group named **kg2** and enter its view.

```
[AC] data-filter keyword-group kg2
```

Create a keyword match pattern that matches the **www.abcd.com/** text string.

```
[AC-data-filter-kgroup-kg2] pattern 1 text www.abcd.com
```

```
[AC-data-filter-kgroup-kg2] quit
```

2. Configure a data filtering policy:

Create a data filtering policy named **p1** and enter its view.

```
[AC] data-filter policy p1
```

Create a data filtering rule named **r1** and enter its view.

```
[AC-data-filter-policy-p1] rule r1
```

Configure the rule to drop and log both upload and download HTTP traffic that matches keyword group **kg1**.

```
[AC-data-filter-policy-p1-rule-r1] keyword-group kg1
```

```
[AC-data-filter-policy-p1-rule-r1] application type http
```

```
[AC-data-filter-policy-p1-rule-r1] direction both
```

```
[AC-data-filter-policy-p1-rule-r1] action drop logging
```

```
[AC-data-filter-policy-p1-rule-r1] quit
```

Create a data filtering rule named **r2** and enter its view.

```
[AC-data-filter-policy-p1] rule r2
```

Configure the rule to drop and log download FTP traffic that matches keyword group **kg2**.

```
[AC-data-filter-policy-p1-rule-r2] keyword-group kg2
```

```
[AC-data-filter-policy-p1-rule-r2] application type ftp
```

```
[AC-data-filter-policy-p1-rule-r2] direction download
```

```
[AC-data-filter-policy-p1-rule-r2] action drop logging
```

```
[AC-data-filter-policy-p1-rule-r2] quit
```

```
[AC-data-filter-policy-p1] quit
```

Applying the data filtering policy to a DPI application profile

Create a DPI application profile named **profile1** and enter its view.

```
[AC] app-profile profile1
```

Apply data filtering policy **p1** to the DPI application profile.

```
[AC-app-profile-profile1] data-filter apply policy p1
```

```
[AC-app-profile-profile1] quit
```

Activate the data filtering policy and rule settings.

```
[AC] inspect activate
```

Applying the DPI application profile to a security policy

Enter IPv4 security policy view.

```
[AC] security-policy ip
```

Create a security policy rule named **inspect1**. Configure the rule to permit packets from IP addresses in IP address object group **datafilter** and apply DPI application profile **profile1** to the security policy.

```
[AC-security-policy-ip] rule name inspect1
```

```
[AC-security-policy-ip-l4-inspect1] source-ip datafilter
```

```
[AC-security-policy-ip-l4-inspect1] action pass
```

```
[AC-security-policy-ip-l4-inspect1] profile profile1
```

```
[AC-security-policy-ip-l4-inspect1] quit
```

Activate rule matching acceleration.

```
[AC-security-policy-ip] accelerate enhanced enable
```

```
[AC-security-policy-ip] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward CAPWAP tunnel traffic between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. This VLAN will be used to forward wireless client packets.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the interface connected to the AC) to trunk, and allow traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 (the interface connected to the AP) to access, and allow only traffic from VLAN 100 to pass through the interface.

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP settings:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100** to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24.

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
```

Specify a gateway.

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200** to assign IP addresses and other configuration parameters to clients on subnet 192.2.1.0/24.

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

```
# Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation.
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2

# Specify a gateway and a DNS server.
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.1
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.1
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

Verify that the AC blocks and logs HTTP packets and FTP packets that meet the specified criteria.
(Details not shown.)

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
wlan service-template 1
    ssid service
    vlan 200
    akm mode psk
    preshared-key pass-phrase cipher $c$3$29gn1DalRVhkcyZ1CKwevH+xb6Lxopy3eq/H
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group1
    vlan 1
    ap ap1
    ap-model AP 3620
    radio 1
    radio enable
```

```

    service-template 1
radio 2
    radio enable
    service-template 1
gigabitethernet 1
#
object-group ip address datafilter
    0 network subnet 192.2.1.0 255.255.255.0
#
data-filter keyword-group kg1
    pattern 1 text uri
    pattern 2 regex abc.*abc
#
data-filter keyword-group kg2
    pattern 1 text www.abcd.com
#
data-filter policy p1
    rule r1
        keyword-group kg1
        application type http
        direction both
        action drop logging
    rule r2
        keyword-group kg2
        application type ftp
        direction download
        action drop logging
#
app-profile profile1
    data-filter apply policy p1
#
security-policy ip
    rule 1 name inspect1
        action pass
    profile profile1
    source-ip datafilter

```

- **Switch:**

```

#
    dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
    ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200

```

```

ip address 192.2.1.2 255.255.255.0
#
dhcp server ip-pool vlan100
network 192.1.0.0 mask 255.255.255.0
forbidden-ip 192.1.1.1 192.1.1.2
gateway-list 192.1.1.1
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.1
network 192.2.1.0 mask 255.255.255.0
forbidden-ip 192.2.1.1 192.2.1.2
dns-list 192.2.1.1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable

```

Related documentation

- *Data Filtering Command Reference in INTELBRAS Access Controllers Command References*
- *Data Filtering Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

File Filtering Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring file filtering	1
Network configuration	1
Restrictions and guidelines	1
Procedures	1
Configuring the AC	1
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides examples for configuring file filtering.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of file filtering.

Example: Configuring file filtering

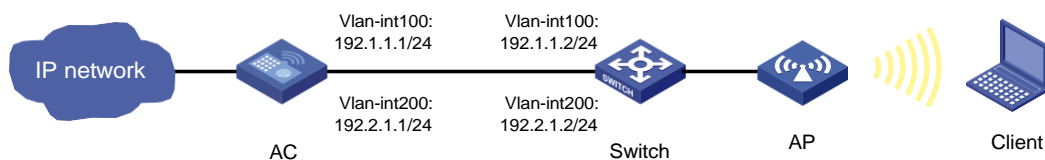
Network configuration

As shown in [Figure 1](#), the AC connects to the Internet.

Configure file filtering on the AC so the AC performs the following operations:

- Blocks files with the **pptx** or **dotx** extension.
- Logs the blocked files.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

You must set the forwarding mode to centralized forwarding mode.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AP will obtain this IP address to establish CAPWAP tunnels with the AC.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will access the wireless network in this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 (the port connected to the switch) to trunk, and allow traffic from VLAN 100 and VLAN 200 to pass through the port.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a wireless service:

Create service template 1 and enter service template view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Set the AKM mode to PSK and configure simple character string **12345678** as the PSK.

```
[AC-wlan-st-1] akm mode psk
```

```
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Set the AES-CCMP cipher suite for frame encryption, and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client traffic. If the default client traffic forwarding location is the same as the configuration in this step, you can skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Assign the client to VLAN 200 after it comes online.

```
[AC-wlan-st-1] vlan 200
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

3. Configure the AP:

❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **ap1**, and specify the AP model.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to 219801A28N819CE0002T.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template 1 to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

Bind service template 1 to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

4. Configure an IP address object group named **filefilter** and specify subnet 192.2.1.0/24 for the object group.

```
<AC> system-view
[AC] object-group ip address filefilter
[AC-obj-grp-ip-filefilter] network subnet 192.2.1.0 24
[AC-obj-grp-ip-filefilter] quit
```

5. Configure file filtering:

- a. Create a file type group named **fg1** and create two file type match patterns to match files with the **pptx** and **dotx** extensions, respectively.

```
[AC] file-filter filetype-group fg1
[AC-file-filter-fgroup-fg1] pattern 1 text pptx
[AC-file-filter-fgroup-fg1] pattern 2 text dotx
[AC-file-filter-fgroup-fg1] quit
```

- b. Create a file filtering policy named **p1** and enter file filtering policy view. Create a file filtering rule named **r1** and configure it to drop and log both upload and download HTTP packets that match file type group **fg1**.

```
[AC] file-filter policy p1
[AC-file-filter-policy-p1] rule r1
[AC-file-filter-policy-p1-rule-r1] filetype-group fg1
[AC-file-filter-policy-p1-rule-r1] application type http
[AC-file-filter-policy-p1-rule-r1] direction both
[AC-file-filter-policy-p1-rule-r1] action drop logging
[AC-file-filter-policy-p1-rule-r1] quit
[AC-file-filter-policy-p1] quit
```

6. Configure a DPI application profile and activate the file filtering policy and rule settings:

Create a DPI application profile named **profile1** and apply file filtering policy **p1** to the DPI application profile.

```
[AC] app-profile profile1
```

```
[AC-app-profile-profile1] file-filter apply policy p1
[AC-app-profile-profile1] quit
```

Activate the file filtering policy and rule settings.

```
[AC] inspect activate
```

7. Configure a security policy:

Enter IPv4 security policy view.

```
[AC] security-policy ip
```

Create a security policy rule named **inspect1**. Configure the rule to permit packets from IP addresses in IP address object group **filefilter** and apply DPI application profile **profile1** to the security policy.

```
[AC-security-policy-ip] rule name inspect1
[AC-security-policy-ip-14-inspect1] source-ip filefilter
[AC-security-policy-ip-14-inspect1] action pass
[AC-security-policy-ip-14-inspect1] profile profile1
[AC-security-policy-ip-14-inspect1] quit
```

Activate rule matching acceleration.

```
[AC-security-policy-ip] accelerate enhanced enable
[AC-security-policy-ip] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLANs 100 and 200, create VLAN-interface 100 and VLAN-interface 200, and assign IP addresses to VLAN-interface 100 and VLAN-interface 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and use VLAN 200 to forward client traffic.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 100 and VLAN 200.

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on the trunk port.

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100** to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24.

```
[Switch] dhcp server ip-pool vlan100
```

```
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
```

Specify a gateway.

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
```

```
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200** to assign IP addresses and other configuration parameters to clients on subnet 192.2.1.0/24.

```
[Switch] dhcp server ip-pool vlan200
```

```
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
```

Specify a gateway and a DNS server.

```
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.1
```

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.1
```

```
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

Verify that the AC blocks and logs files that meet the specified criteria. (Details not shown.)

Configuration files

- AC:

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
wlan service-template 1
```

```
ssid service
```

```
vlan 200
```

```
akm mode psk
```

```
preshared-key pass-phrase cipher $c$3$29gn1DalRVhkcyZ1CKwevH+xb6Lxopy3eq/H
```

```
cipher-suite ccmp
```

```
security-ie rsn
```

```
service-template enable
```

```
#
```

```

interface Vlan-interface100
 ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
 vlan 1
 ap ap1
 ap-model AP 3620
 radio 1
  radio enable
  service-template 1
 radio 2
  radio enable
  service-template 1
 gigabitethernet 1
#
object-group ip address filefilter
 0 network subnet 192.2.1.0 255.255.2
#
file-filter policy p1
 rule r1
  filetype-group fg1
  application type http
  direction both
  action drop logging
#
file-filter filetype-group fg1
 pattern 1 text pptx
 pattern 2 text dotx
#
app-profile profile1
 file-filter apply policy p1
#
security-policy ip
 rule 1 name inspect1
  action pass
  profile profile1
  source-ip filefilter

```

- Switch:

```

#
    dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
    ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.2 255.255.255.0
#
dhcp server ip-pool vlan100
    network 192.1.0.0 mask 255.255.255.0
    forbidden-ip 192.1.1.1 192.2.1.2
    gateway-list 192.1.1.1
#
dhcp server ip-pool vlan200
    gateway-list 192.2.1.1
    network 192.2.1.0 mask 255.255.255.0
    forbidden-ip 192.2.1.1 192.2.1.2
    dns-list 192.2.1.1
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable

```

Related documentation

- *File Filtering Command Reference in INTELBRAS Access Controllers Command References*
- *File Filtering Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Application Audit and Management

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring application audit and management	1
Network configuration	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides examples for configuring application audit and management.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of application audit and management.

Example: Configuring application audit and management

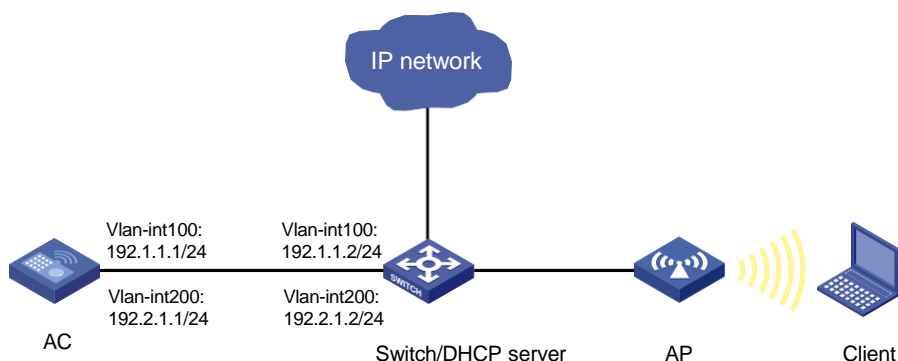
Network configuration

As shown in [Figure 1](#), the switch assigns IP addresses to the AP and the client. The AP and the AC establish a CAPWAP tunnel through VLAN 100, and the client accesses the wireless network through VLAN 200. The working hours of the company are 8:00:00 through 18:00:00 from Monday to Friday.

Configure an application audit and management policy on the AC to meet the following requirements:

- Permit login from all QQ accounts during working hours.
- Generate audit logs.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to VLAN-interface 100.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to VLAN-interface 200.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, remove it from VLAN 1, assign it to VLAN 100 and VLAN 200, and set its PVID to VLAN 100.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

2. Configure wireless services:

Create service template 1 and enter service template view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Configure the PSK AKM mode and the **12345678** plaintext key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Configure CCMP as the cipher suite and RSN as the security IE.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Enable the service template..

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In a large network, use AP groups to configure APs as a best practice.

Create an AP named **ap1**, with model **AP 3620**.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to **219801A28N819CE0002T**.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create an AP group named **group1**, and create an AP grouping rule by AP names to add AP **ap1** to the AP group.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Enter radio view of radio 1, and bind service template 1 to the radio.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

Enter radio view of radio 2, and bind service template 1 to the radio.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

4. Configure a time range named **work** to cover 8:00:00 through 18:00:00 from Monday to Friday.

```
<AC> system-view
[AC] time-range work 08:00 to 18:00 working-day
```

5. Create an IPv4 address object group named **audit**, and configure an IPv4 address object with the IPv4 address of **192.2.1.0** and mask length of **24**..

```
[AC] object-group ip address audit
[AC-obj-grp-ip-audit] network subnet 192.2.1.0 24
[AC-obj-grp-ip-audit] quit
```

6. Configure an application audit and management policy:

Enter application audit and management view.

```
[AC] uapp-control
```

Create an audit policy named **audit-qq** and enter its view.

```
[AC-uapp-control] policy name audit-qq audit
```

Specify IPv4 address object group **audit** as a match criterion for audit policy **audit-qq**.

```
[AC-uapp-control-policy-audit-qq] source-address ipv4 audit
```

Specify time range **work** for audit policy **audit-qq**.

```
[Device-uapp-control-policy-audit-qq] time-range work
```

Configure an audit rule to permit login from all QQ accounts and generate audit logs.

```
[AC-uapp-control-policy-audit-qq] rule 1 app QQ behavior Login bhcontent any keyword
equal any action permit audit-logging
[AC-uapp-control-policy-audit-qq] quit
[AC-uapp-control] quit
# Activate the configuration.
[AC] inspect activate
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLANs 100 and 200, create VLAN-interface 100 and VLAN-interface 200, and assign IP addresses to VLAN-interface 100 and VLAN-interface 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and use VLAN 200 to forward client traffic.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, remove it from VLAN 1, assign it to VLAN 100 and VLAN 200, and set its PVID to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, remove it from VLAN 1, assign it to VLAN 100, and set its PVID to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100 to assign IP addresses and other configuration parameters to clients on subnet 192.1.1.0/24.**

```
[Switch] dhcp server ip-pool vlan100
```

```

[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
# Exclude IP addresses 192.1.1.1 and 192.1.1.2 from dynamic allocation.
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
# Specify a gateway.
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit

# Create a DHCP address pool named vlan200 to assign IP addresses and other configuration
parameters to clients on subnet 192.2.1.0/24.
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
# Exclude IP addresses 192.2.1.1 and 192.2.1.2 from dynamic allocation.
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
# Specify a gateway and a DNS server.
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
[Switch-dhcp-pool-vlan200] quit

```

Verifying the configuration

Verify that the device permits the login requests and generates audit log messages when QQ accounts attempt to access the Internet. (Details not shown.)

Configuration files

- AC:


```

#
vlan 100
#
vlan 200
#
object-group ip address audit
 0 network subnet 192.2.1.0 255.255.255.0
#
wlan service-template 1
  ssid service
  vlan 200
  akm mode psk
  preshared-key pass-phrase cipher $c$3$29gn1DalRVhkcyZ1CKwevH+xb6Lxopy3eq/H
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
interface Vlan-interface100
  ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 192.2.1.1 255.255.255.0
#

```

```

interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group1
vlan 1
ap ap1
ap-model AP 3620
    radio 1
        radio enable
        service-template 1
    radio 2
        radio enable
        service-template 1
    gigabitethernet 1
#
time-range work 08:00 to 18:00 working-day
#
wlan ap ap1 model WAP722S-HI
    serial-id 219801A2F98205P00031
    radio 1
        radio enable
        service-template 1
    radio 2
        radio enable
        service-template 1
#
uapp-control
    policy name audit-qq audit
        time-range work
        source-address ipv4 audit
        rule 1 app QQ behavior Login bhcontent any keyword equal any action permit
audit-logging

```

- **Switch:**

```

#
    dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 192.1.1.1

```

```

network 192.1.1.0 mask 255.255.255.0
forbidden-ip 192.1.1.1 192.1.1.2
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.2
network 192.2.1.0 mask 255.255.255.0
dns-list 192.2.1.2
forbidden-ip 192.2.1.1 192.2.1.2
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
poe enable
#

```

Related documentation

- *Application Audit and Management Command Reference in INTELBRAS Access Controllers Command References*
- *Application Audit and Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Policy Command Reference in INTELBRAS Access Controllers Command References*
- *Security Policy Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers Application Rate Limiting Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring application rate limiting	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides an example for configuring application rate limiting.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

The following information applies to Comware-based access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access points.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

Example: Configuring application rate limiting

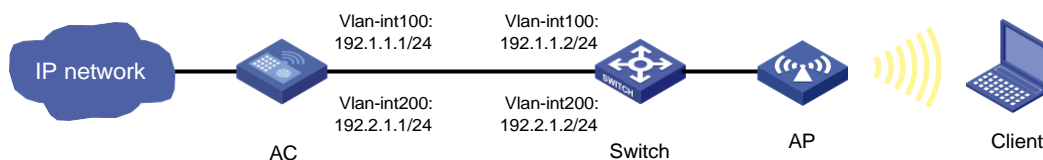
Network configuration

As shown in [Figure 1](#), the AC is connected to the Internet. Configure application rate limiting on the AC to finely manage and control applications.

Configure application rate limiting to meet the following requirements:

- Limit both the maximum uplink bandwidth and maximum downlink bandwidth to 30720 kbps for the clients accessing the iQiYiPPS application on the Internet.
- Guarantee both the uplink bandwidth of 30720 kbps and the downlink bandwidth of 30720 kbps for the clients accessing the FTP application on the Internet.

Figure 1 Network diagram



Restrictions and guidelines

- Use the actual serial ID of an AP to uniquely identify that AP.
- You must set the forwarding mode to centralized forwarding mode.

Procedures

Configuring the AC

Configuring basic AC functions

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100. Assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with APs.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 100. Assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

Set the link type to trunk for interface GigabitEthernet 1/0/1 connecting the AC and the switch, and assign it to VLANs 100 and 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a wireless service:

Create wireless service template 1 and enter its view.

```
[AC] wlan service-template 1
```

Configure SSID service.

```
[AC-wlan-st-1] ssid service
```

Configure the PSK AKM mode and the **12345678** plaintext key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Configure CCMP as the cipher suite and RSN as the security IE.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Assign clients coming online through service template 1 to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Enable wireless service template 1.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In a large network, use AP groups to configure APs as a best practice.

Create an AP named **ap1**, with model **AP 3620**.

```
[AC] wlan ap ap1 model AP 3620
```

Set the serial ID to **219801A28N819CE0002T**.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create an AP group named **group1**, and create an AP grouping rule by AP names to add AP **ap1** to the AP group.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

Enter radio view of radio 1, and bind service template 1 to the radio.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

Enter radio view of radio 2, and bind service template 1 to the radio.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

Configure application rate limiting

1. Configure traffic profiles:

Create a traffic profile named **aiqiyi**, and enter its view.

```
<AC> system-view
```

```
[AC] traffic-policy
```

```
[AC-traffic-policy] profile name aiqiyi
```

Set the maximum bandwidth to 30720 kbps for both upstream and downstream traffic.

```
[AC-traffic-policy-profile-aiqiyi] bandwidth upstream maximum 30720
```

```
[AC-traffic-policy-profile-aiqiyi] bandwidth downstream maximum 30720
```

```
[AC-traffic-policy-profile-aiqiyi] quit
```

Create a traffic profile named **profileFTP**, and enter its view.

```
[AC-traffic-policy] profile name profileFTP
```

Set the guaranteed bandwidth to 30720 kbps for both upstream and downstream traffic.

```
[AC-traffic-policy-profile-profileFTP] bandwidth upstream guaranteed 30720
```

```
[AC-traffic-policy-profile-profileFTP] bandwidth downstream guaranteed 30720
```

```
[AC-traffic-policy-profile-profileFTP] quit
```

2. Configure traffic rules:

Create a traffic rule named **aiqiyi**, and enter its view.

```
[AC-traffic-policy] rule name aiqiyi
```

Configure the predefined application iQiYiPPS as a match criterion.

```
[AC-traffic-policy-rule-1-aiqiyi] application app iQiYiPPS
```

Specify traffic profile **aiqiyi** for traffic rule **aiqiyi**.

```
[AC-traffic-policy-rule-1-aiqiyi] action qos profile aiqiyi
[AC-traffic-policy-rule-1-aiqiyi] quit
# Create a traffic rule named ruleFTP, and enter its view.
[AC-traffic-policy] rule name ruleFTP
# Configure the predefined application FTP as a match criterion.
[AC-traffic-policy-rule-2-ruleFTP] application app ftp
# Specify traffic profile profileFTP for traffic rule ruleFTP.
[AC-traffic-policy-rule-2-ruleFTP] action qos profile profileFTP
[AC-traffic-policy-rule-2-ruleFTP] quit
[AC-traffic-policy-rule-2] quit
```

3. Configure application rate limiting criteria:

```
# Enter traffic policy view.
[AC] traffic-policy
# Create a traffic rule named aiqiyi, and enter its view.
[AC-traffic-policy] rule name aiqiyi
# Configure SSID service as a match criterion in traffic rule aiqiyi.
[AC-traffic-policy-rule-1-aiqiyi] wlan ssid service
# Configure AP ap1 as a match criterion in traffic rule aiqiyi.
[AC-traffic-policy-rule-1-aiqiyi] ap ap1
[AC-traffic-policy-rule-1-aiqiyi] quit
# Create a traffic rule named ruleFTP, and enter its view.
[AC-traffic-policy] rule name ruleFTP
# Configure SSID service as a match criterion in traffic rule ruleFTP.
[AC-traffic-policy-rule-2-ruleFTP] wlan ssid service
# Configure AP ap1 as a match criterion in traffic rule ruleFTP.
[AC-traffic-policy-rule-2-ruleFTP] ap ap1
[AC-traffic-policy-rule-2-ruleFTP] quit
[AC-traffic-policy] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLANs 100 and 200 and the corresponding VLAN interfaces. Assign IP addresses to the VLAN interfaces. VLAN 100 is used for forwarding traffic in CAPWAP tunnels between the AC and APs, and VLAN 200 is used to forward wireless packets from clients.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

Set the link type to trunk for interface GigabitEthernet 1/0/1 connecting the AC and the switch, and assign it to VLANs 100 and 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Set the link type to access for interface GigabitEthernet 1/0/2 connecting APs and the switch, and assign it to VLAN 100.

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100 for allocating addresses to APs. In the address pool, specify subnet 192.1.1.0/24 for dynamic address allocation, exclude addresses 192.1.1.1 and 192.1.1.2 from address allocation, and specify the gateway address as 192.1.1.1.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 192.1.1.2
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.1
[Switch-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200 for allocating addresses to clients. In the address pool, specify subnet 192.2.1.0/24 for dynamic address allocation, exclude addresses 192.2.1.1 and 192.2.1.2 from address allocation, specify the DNS server address as needed, and specify the gateway address as 192.1.1.1.**

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 192.2.1.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.1
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.1
[Switch-dhcp-pool-vlan200] quit
```

Verifying the configuration

Verify that the traffic of the iQiYiPPS application is rate-limited, and the traffic of the FTP application is guaranteed.

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
wlan service-template 1
```

```

ssid service
vlan 200
akm mode psk
preshared-key pass-phrase cipher $c$3$29gn1DalRVhkcyZ1CKwevH+xb6Lxopy3eq/H
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface100
ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.1 255.255.255.0
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
vlan 1
ap ap1
ap-model AP 3620
radio 1
radio enable
service-template 1
radio 2
radio enable
service-template 1
gigabitethernet 1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
wlan ap ap1 model WA4320-ACN-B
serial-id 210235A1PRC183000006
radio 1
radio enable
service-template 1
radio 2
radio enable
service-template 1
#
traffic-policy
rule 3 name ruleFTP parent rule
action qos profile profileftp
application app ftp
wlan ssid service
ap ap1

```



```

rule 5 name aiqiyi
  action qos profile aiqiyi
  application app iQiYiPPS
  wlan ssid service
  ap ap1
profile name aiqiyi
  bandwidth downstream maximum 30720
  bandwidth upstream maximum 30720
profile name profileftp
  bandwidth downstream guaranteed 30720
  bandwidth upstream guaranteed 30720

```

- **Switch:**

```

#
  dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
  ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
  ip address 192.2.1.2 255.255.255.0
#
dhcp server ip-pool vlan100
  network 192.1.0.0 mask 255.255.255.0
  forbidden-ip 192.1.1.1 192.1.1.2
  gateway-list 192.1.1.1
#
dhcp server ip-pool vlan200
  gateway-list 192.2.1.1
  network 192.2.1.0 mask 255.255.255.0
  forbidden-ip 192.2.1.1 192.2.1.2
  dns-list 192.2.1.1
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
poe enable

```

Related documentation

- *Bandwidth Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

- *Bandwidth Management Command Reference in INTELBRAS Access Controllers Command References*