

# H3C S6850 & S9850 & S9820-64H Traffic Filtering Configuration Examples

---

Copyright © 2020 New H3C Technologies Co., Ltd. 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 New H3C Technologies Co., Ltd.

Except for the trademarks of New H3C Technologies Co., Ltd., 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 traffic filtering .....	1
Network configuration .....	1
Analysis .....	2
Applicable hardware and software versions .....	3
Restrictions and guidelines .....	3
Procedures.....	3
Configuring Device A .....	3
Configuring Device B .....	4
Verifying the configuration.....	4
Configuration files .....	5
Related documentation.....	6

# Introduction

This document provides traffic filtering configuration examples.

## Prerequisites

The configuration examples in this document 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.

This document assumes that you have basic knowledge of traffic filtering.

## Example: Configuring traffic filtering

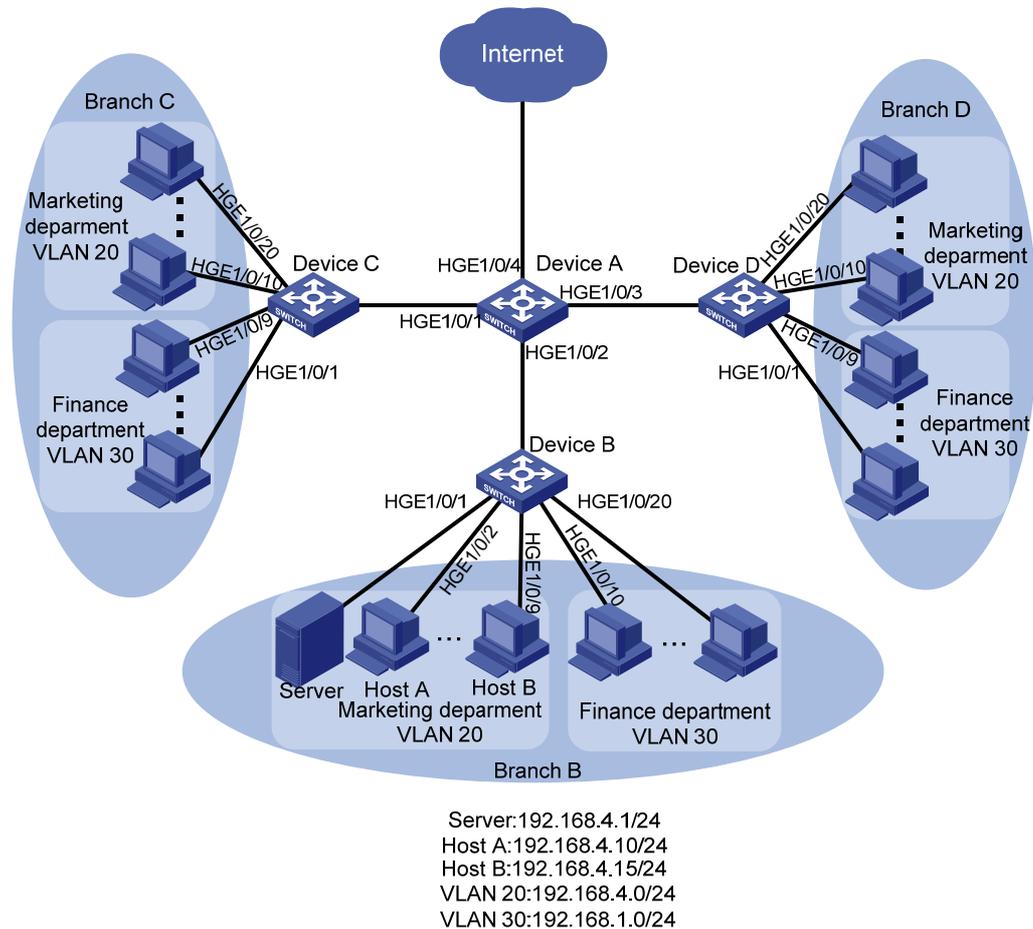
### Network configuration

As shown in [Figure 1](#), a company has three branches, each of which has a Marketing department and a Finance department. All Marketing departments belong to VLAN 20. All Finance departments belong to VLAN 30.

Configure traffic filtering to meet the following requirements:

- HTTP traffic from the Marketing department in each branch is denied.
- In Branch B, only Host A and Host B can access the server.
- The Marketing departments in three branches can access one another, and the Finance departments in three branches can access one another.

**Figure 1 Network diagram**



## Analysis

To meet the network requirements, you must perform the following tasks:

- To deny HTTP traffic from the Marketing departments, use one of the following methods:
  - Filter outgoing traffic from the subnet 192.168.4.0/24 on the interfaces that connect Device B, Device C, and Device D to Device A.  
 This method has poor scalability, because new branches require the same configuration on their access switches.
  - Filter outgoing traffic from the subnet 192.168.4.0/24 on interface HundredGigE 1/0/4 of Device A.  
 This method wastes processing capabilities of Device A, because Device A must internally forward all incoming traffic to interface HundredGigE 1/0/4.
  - Configure a QoS policy to deny HTTP traffic from the Marketing departments.  
 This method can automatically adapt to changing network topologies and also saves hardware resources by denying traffic on the incoming interface. This example uses this method.
- To allow only Host A and Host B to access the server in Branch B, perform the following tasks:
  - Configure an ACL on HundredGigE 1/0/1 to allow packets from 192.168.4.10/24 and 192.168.4.15/24.

- Set the default packet filtering action to **deny** to deny packets that do not match the configured ACL.
- To allow traffic from Marketing departments and Finance departments (except HTTP traffic) to the Internet and to allow access among Marketing departments and among Finance departments, perform the following tasks:
  - Configure HundredGigE 1/0/1 through HundredGigE 1/0/4 as trunk ports.
  - Assign these interfaces to VLAN 20 and VLAN 30.

## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6850 switch series S9850 switch series	Release 6555P01
S9820-64H switch	Release 6555P01

## Restrictions and guidelines

If a traffic behavior is configured with the **filter deny** action, all other actions in the behavior except traffic accounting do not take effect.

## Procedures

### Configuring Device A

# Create VLAN 20 and VLAN 30.

```
<DeviceA> system-view
[DeviceA] vlan 20
[DeviceA-vlan20] quit
[DeviceA] vlan 30
[DeviceA-vlan30] quit
```

# Add HundredGigE 1/0/1 through HundredGigE 1/0/4 to interface range named **myport**.

```
[DeviceA] interface range name myport interface hundredgige 1/0/1 to hundredgige
1/0/4
```

# Configures interfaces HundredGigE 1/0/1 through HundredGigE 1/0/4 as trunk ports, assign them to VLAN 20 and VLAN 30, and remove them from VLAN 1.

```
[DeviceA-if-range-myport] port link-type trunk
[DeviceA-if-range-myport] port trunk permit vlan 20 30
[DeviceA-if-range-myport] undo port trunk permit vlan 1
[DeviceA-if-range-myport] quit
```

# Configure advanced IPv4 ACL 3000 to match HTTP traffic from subnet 192.168.4.0/24.

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule deny tcp source 192.168.4.0 0.0.0.255 source-port eq
80
```

```

[DeviceA-acl-ipv4-adv-3000] quit
# Create a class named vlan20_http, and use ACL 3000 as the match criterion.
[DeviceA] traffic classifier vlan20_http
[DeviceA-classifier-vlan20_http] if-match acl 3000
[DeviceA-classifier-vlan20_http] quit
# Create a behavior named vlan20_http, and configure traffic filtering to deny traffic of the class
vlan20_http.
[DeviceA] traffic behavior vlan20_http
[DeviceA-behavior-vlan20_http] filter deny
[DeviceA-behavior-vlan20_http] quit
# Create a QoS policy named vlan20_http, and associate the class vlan20_http with the behavior
vlan20_http in the QoS policy.
[DeviceA] qos policy vlan20_http
[DeviceA-qospolicy-vlan20_http] classifier vlan20_http behavior vlan20_http
[DeviceA-qospolicy-vlan20_http] quit
# Apply the QoS policy vlan20_http to the inbound direction of VLAN 20 and VLAN 30.
[DeviceA] qos vlan-policy vlan20_http vlan 20 30 inbound

```

## Configuring Device B

```

# Configure basic IPv4 ACL 2000 to permit traffic from Host A and Host B.
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 192.168.4.10 0
[DeviceB-acl-ipv4-basic-2000] rule permit source 192.168.4.15 0
[DeviceB-acl-ipv4-basic-2000] quit
# Set the packet filtering default action to deny.
[DeviceB] packet-filter default deny
# Apply ACL 2000 to interface HundredGigE 1/0/1 to filter outgoing traffic.
[DeviceB] interface hundredgige 1/0/1
[DeviceB-HundredGigE1/0/1] packet-filter 2000 outbound

```

## Verifying the configuration

```

# Verify the QoS policy applied to the inbound direction of VLAN 20 and VLAN 30.
[DeviceA]display qos vlan-policy vlan inbound
  Direction: Inbound
  Policy: vlan20_http
  Classifier: vlan20_http
    Operator: AND
    Rule(s) :
      If-match acl 3000
    Behavior: vlan20_http
    Filter enable: Deny
Vlan 30
  Direction: Inbound
  Policy: vlan20_http
  Classifier: vlan20_http

```

```

Operator: AND
Rule(s) :
  If-match acl 3000
Behavior: vlan20_http
Filter enable: Deny

# Display application details of ACLs for incoming packet filtering on HundredGigE 1/0/1.
[DeviceB] display packet-filter verbose interface hundredgige 1/0/1 outbound
Interface: HundredGigE1/0/1
Outbound policy:
  IPv4 ACL 2000
  rule 0 permit source 192.168.4.10 0
  IPv4 default action: Deny

```

## Configuration files

- Device A:

```

#
vlan 20
#
vlan 30
#
interface range name myport interface HundredGigE1/0/1 to HundredGigE1/0/4
#
acl advanced 3000
  rule 0 deny tcp source 192.168.4.0 0.0.0.255 source-port eq www
#
traffic classifier vlan20_http operator and
  if-match acl 3000
#
traffic behavior vlan20_http
  filter deny
#
qos policy vlan20_http
  classifier vlan20_http behavior vlan20_http
#
qos vlan-policy vlan20_http vlan 20 inbound
qos vlan-policy vlan20_http vlan 30 inbound
#
interface HundredGigE1/0/1
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 20 30
#
interface HundredGigE1/0/2
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1

```

```
port trunk permit vlan 20 30
#
interface HundredGigE1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20 30
#
interface HundredGigE1/0/4
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20 30
```

- **Device B:**

```
#
acl basic 2000
rule 0 permit source 192.168.4.10 0
#
packet-filter default deny
#
interface HundredGigE1/0/1
port link-mode bridge
packet-filter 2000 outbound
#
```

## Related documentation

- *H3C S6850 & S9850 Switch Series ACL and QoS Configuration Guide-Release 655x*
- *H3C S6850 & S9850 Switch Series ACL and QoS Command Reference-Release 655x*
- *H3C S9820-64H Switch ACL and QoS Configuration Guide-Release 655x*
- *H3C S9820-64H Switch ACL and QoS Command Reference-Release 655x*