**Using Advanced ACLs to Restrict Enterprise Network Access**

Student Version



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



# Using Advanced ACLs to Restrict Enterprise Network Access

## Background

The company Jan16 has deployed several PCs for its financial department and deployed a dedicated financial system server to form a LAN. The PCs and server are connected to the Internet through an egress router. To ensure the data security of the financial system, access control policies must be configured on the egress router to allow only PC1 of the financial department to access the front-end website of the financial system server and disallow the server from accessing external networks.

Figure 1-1 shows the network topology. The specific requirements are as follows:

Only PC1 of the financial department is allowed to access the front-end website of the financial system server.

The financial system server is not allowed to access external networks.

The IP addresses and interfaces of the PCs and egress router are shown in the topology.

## Objectives

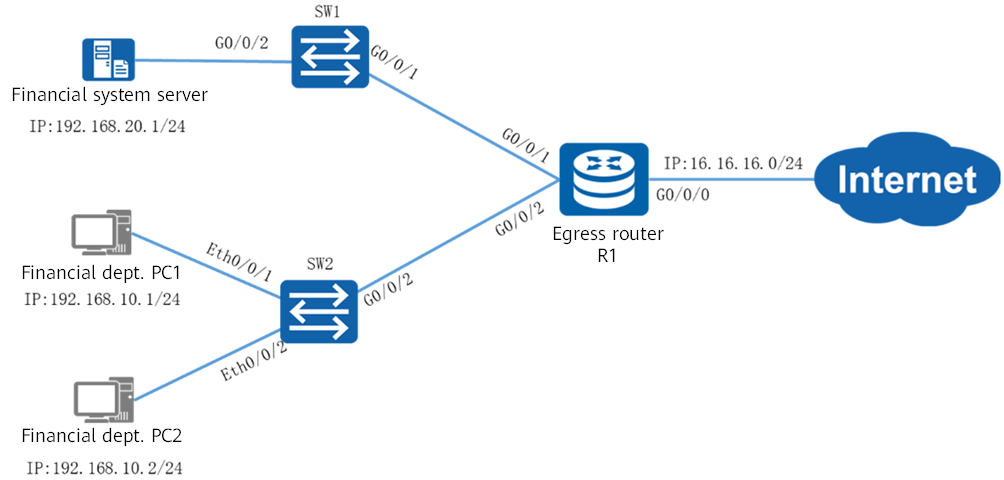
Upon completion of this task, you will be able to:

Learn how to manually configure advanced ACL

Learn how to use ACL to filter traffic

## Topology

Lab topology



An advanced ACL can match the source address, destination address, protocol, and port number of IP packets, and permit or deny the matching packets accordingly. In this project, access control policies need to be configured on the egress router to restrict the access to and from the financial system server. That is, allow PC1 of the financial department to access port 80 of the financial system server, and disallow the server to access external networks.

The IP address planning and interface planning can be referred in the appendix.

## Implementation

### Roadmap

1. Configure interfaces on the egress router.
2. Configure advanced ACLs.
3. Configure IP addresses for the financial system server and PCs of the financial department.

### Procedure

Configure interfaces on the egress router R1.

Configure advanced ACLs.

#Configure an advanced ACL on the egress router to allow PC1 of the financial department to access port 80 of the financial system server. Apply the ACL to G0/0/1 of the egress router.

[R1]

#Configure an advanced ACL on the egress router to deny access from the financial system server to external networks. Apply the ACL to G0/0/0 of the egress router.

[R1]

Configure IP addresses for the financial system server and PCs of the financial department.

Configure the IP addresses of PCs and financial system server referred by the appendix.

* 1. **Verification**

Check the ACL configuration on R1.

[R1]

Test the connectivity between the

PCs of the financial department and port 80 of the financial system server.

You can use a Router to function as financial system server，open the WEB management function and the default WEB management port is 80.

#Access financial system server from PC1

[C:\~]$ telnet 192.168.20.1 80

Connecting to 192.168.20.1:80...

Connection established.

To escape to local shell, press 'Ctrl+Alt+]'.

Get

HTTP/1.0 400 Bad Request

Server: AR

Date: tue, 22 dec 2020 07:26:20 GMT

Pragma: no-cache

Cache-Control: no-store

Content-Length: 11

Connection: Close

The PC1 can open the 80 port of financial system server.

#Access financial system server from PC2

[C:\~]$ telnet 67.0.0.2 80

Connecting to 67.0.0.2:80...

The PC2 can‘t open the 80 port of financial system server.

Test the connectivity between the financial system server and an external network.

#Ping the external network from the financial system server.

<AR2>ping 16.16.16.15

PING 16.16.16.15: 56 data bytes, press CTRL\_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

--- 16.16.16.15 ping statistics ---

5 packet(s) transmitted

0 packet(s) received

100.00% packet loss

The ping result shows that the financial system server cannot access the external network.

# Ping the external network from PC1.

[C:\~]$ ping 16.16.16.15

Pinging 16.16.16.15 with 32 bytes of data:

Reply from 16.16.16.15: bytes=32 time<1ms TTL=255

Reply from 16.16.16.15: bytes=32 time<1ms TTL=255

Reply from 16.16.16.15: bytes=32 time<1ms TTL=255

Reply from 16.16.16.15: bytes=32 time<1ms TTL=255

Ping statistics for 16.16.16.15:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

----**End**

## Appendix

IP address planning

| Device | Interface | IP Address |
| --- | --- | --- |
| R1 | G0/0/0 | 16.16.16.16/24 |
| R1 | G0/0/1 | 192.168.10.254/24 |
| R1 | G0/0/2 | 192.168.20.254/24 |
| SW1 | G0/0/1 | N/A |
| SW1 | G0/0/2 | N/A |
| SW2 | G0/0/2 | N/A |
| SW2 | Eth0/0/1 | N/A |
| SW2 | Eth0/0/2 | N/A |
| Financial system server | Eth0/0/1 | 192.168.20.1/24 |
| PC1 | Eth0/0/1 | 192.168.10.1/24 |
| PC2 | Eth0/0/1 | 192.168.10.2/24 |

Interface planning

| Local Device | Local Interface | Peer Device | Peer Interface |
| --- | --- | --- | --- |
| R1 | G0/0/0 | Internet | - |
| R1 | G0/0/1 | SW1 | G0/0/1 |
| R1 | G0/0/2 | SW2 | G0/0/2 |
| SW1 | G0/0/1 | R1 | G0/0/1 |
| SW1 | G0/0/2 | Financial system server | Eth0/0/1 |
| SW2 | Eth0/0/1 | PC1 | Eth0/0/1 |
| SW2 | Eth0/0/2 | PC2 | Eth0/0/1 |
| SW2 | G0/0/2 | R1 | G0/0/2 |
| Financial system server | Eth0/0/1 | SW1 | G0/0/2 |
| PC1 | Eth0/0/1 | SW2 | Eth0/0/1 |
| PC2 | Eth0/0/1 | SW2 | Eth0/0/2 |