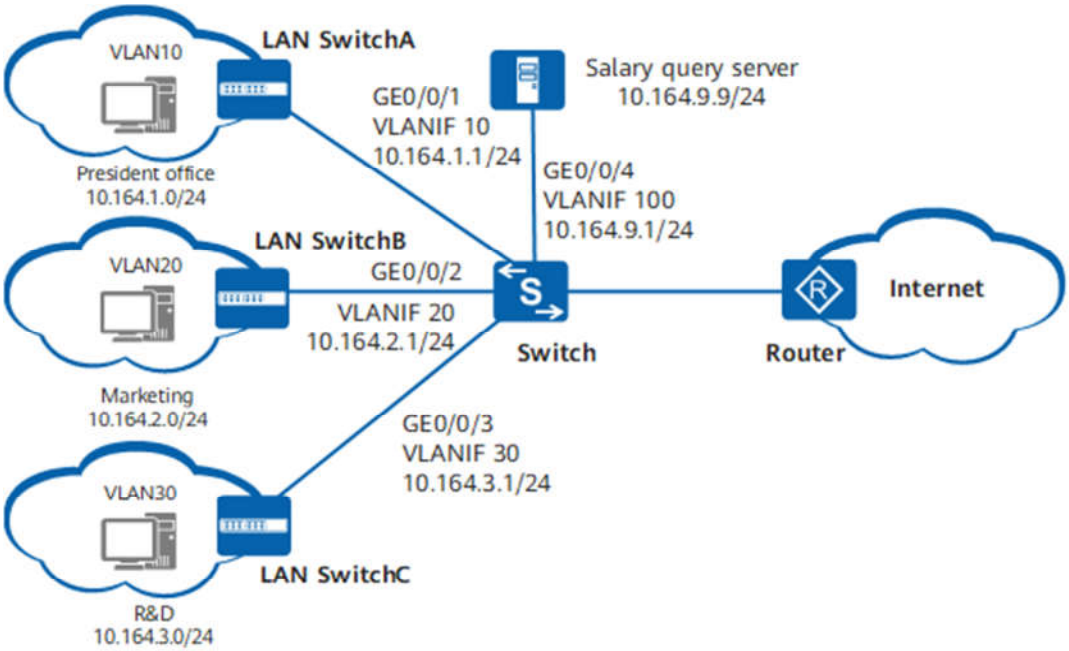
Configuração de ACL avançada com uso de time-range

Diagrama da Rede

Figura 1 Uso de ACL avançada e time-range para controlar acesso a um servidor



Requerimentos de Rede

Conforme mostrado na Figura 1, os departamentos de uma empresa são conectados por meio do Switch. Os departamentos de R&D e marketing não podem acessar o servidor de consulta de salários em 10.164.9.9 no horário comercial (8h00 às 17h30), enquanto a presidência pode acessar o servidor a qualquer momento.

Roteiro de Configuração

As seguintes configurações são executadas no Switch. O roteiro de configuração é o seguinte:

1. Configure o intervalo de tempo, ACL avançado e classificador de tráfego baseado em ACL para filtrar pacotes de usuários para o servidor no intervalo de tempo

especificado. Desta forma, você pode restringir o acesso de diferentes usuários ao servidor no intervalo de tempo especificado.

2. Configure um comportamento de tráfego para descartar os pacotes que correspondem à ACL.

3. Configure e aplique uma política de tráfego para que a ACL e o comportamento do tráfego tenham efeito.

Procedimento

1. Adicione interfaces às VLANs e atribua endereços IP às interfaces VLANIF

   # Adicione GE0/0/1 a GE0/0/3 às VLANs 10, 20 e 30, respectivamente, adicione GE0/0/4 à VLAN 100 e atribua endereços IP a essas interfaces VLANIF. As configurações em GE0/0/1 e VLANIF 10 são usadas como exemplo aqui. As configurações em GE0/0/2, GE0/0/3 e GE0/0/4 são semelhantes às de GE0 / 0/1, e as configurações em VLANIF 20, VLANIF 30 e VLANIF 100 são semelhantes às de VLANIF 10..

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30 100
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Switch-Vlanif10] quit
```

2. Configure uma faixa de horário.

   # Configure uma faixa de horário das 8:00 às 17:30.

```
[Switch] time-range satime 8:00 to 17:30 working-day
```

3. Configure ACLs.

   # Configure uma ACL para o departamento de marketing não acessar o servidor de salários.

```
[Switch] acl 3002
[Switch-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination
10.164.9.9 0.0.0.0 time-range satime
[Switch-acl-adv-3002] quit
```

Configure uma acl para o departamento de R&D não acessar o servidor de salários.

```
[Switch] acl 3003
[Switch-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Switch-acl-adv-3003] quit
```

4. Configure classificadores de tráfego baseados em ACL.

   # Configure o classificador de tráfego c_market para classificar os pacotes que correspondem a ACL 3002.

   ```
   [Switch] traffic classifier c_market
   [Switch-classifier-c_market] if-match acl 3002
   [Switch-classifier-c_market] quit
   ```

   # Configure o classificador de tráfego c_rd para classificar os pacotes que correspondem a ACL 3003.

   ```
   [Switch] traffic classifier c_rd
   [Switch-classifier-c_rd] if-match acl 3003
   [Switch-classifier-c_rd] quit
   ```

5. Configure a ação a ser feita com o tráfego.

   # Configure o comportamento do tráfego b_market para rejeitar pacotes.

   ```
   [Switch] traffic behavior b_market
   [Switch-behavior-b_market] deny
   [Switch-behavior-b_market] quit
   ```

   # Configure o comportamento do tráfego b_rd para rejeitar pacotes.

   ```
   [Switch] traffic behavior b_rd
   [Switch-behavior-b_rd] deny
   [Switch-behavior-b_rd] quit
   ```

6. Configure as políticas de tráfego.

   # Configure a política de tráfego p_market e associe o classificador de tráfego c_market e o comportamento de tráfego b_market à política de tráfego.

   ```
   [Switch] traffic policy p_market
   [Switch-trafficpolicy-p_market] classifier c_market behavior b_market
   [Switch-trafficpolicy-p_market] quit
   ```

   # Configure a política de tráfego p_rd e associe o classificador de tráfego c_rd e o comportamento de tráfego b_rd à política de tráfego.

   ```
   [Switch] traffic policy p_rd
   [Switch-trafficpolicy-p_rd] classifier c_rd behavior b_rd
   [Switch-trafficpolicy-p_rd] quit
   ```

7. Aplique a política de tráfego.

Os pacotes do departamento de marketing são recebidos por GE0 / 0/2, portanto, aplique a política de tráfego p_market para a direção de entrada de GE0 / 0/2.

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy p_market inbound
[Switch-GigabitEthernet0/0/2] quit
```

Os pacotes do departamento de P&D são recebidos por GE0/0/3, portanto, aplique a política de tráfego p_rd à direção de entrada de GE0/0/3.

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p_rd inbound
[Switch-GigabitEthernet0/0/3] quit
```

8. Verifique a configuração.

Verifique as ACLs.

```
[Switch] display acl all
 Total nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Active)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Active)
```

Verifique a configuração dos classificadores de tráfego.

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: OR
    Rule(s) : if-match acl 3002

   Classifier: c_rd
    Operator: OR
    Rule(s) : if-match acl 3003

Total classifier number is 2
```

Verifique as políticas.

```
[Switch] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
   Classifier: c_market
    Operator: OR
     Behavior: b_market
      Deny
```

```
  Policy: p_rd
   Classifier: c_rd
    Operator: OR
     Behavior: b_rd
      Deny

Total policy number is 2
```

Verifique os registros das políticas de tráfego.

```
[Switch] display traffic-policy applied-record
#
-------------------------------------------------
  Policy Name:   p_market
  Policy Index:  0
     Classifier:c_market     Behavior:b_market
-------------------------------------------------
 *interface GigabitEthernet0/0/2
    traffic-policy p_market inbound
      slot 0    :  success
-------------------------------------------------
  Policy total applied times: 1.
#
-------------------------------------------------
  Policy Name:   p_rd
  Policy Index:  1
     Classifier:c_rd     Behavior:b_rd
-------------------------------------------------
 *interface GigabitEthernet0/0/3
    traffic-policy p_rd inbound
      slot 0    :  success
-------------------------------------------------
  Policy total applied times: 1.
#
```

Os departamentos de P&D e marketing não podem acessar o servidor de consulta de salários durante o horário de trabalho (8h00 às 17h30).

Arquivos de Configuração

Arquivo de configuração do switch

```
#
sysname Switch
#
vlan batch 10 20 30 100
#
time-range satime 08:00 to 17:30 working-day
#
acl number 3002
```

```
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
traffic policy p_market match-order config
 classifier c_market behavior b_market
traffic policy p_rd match-order config
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p_market inbound
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p_rd inbound
#
interface GigabitEthernet0/0/4
```

```
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```