H3C MSRルーターのACL設定例(Comware V7)

内容

はじめに 1

前提条件 1

例:MACアドレスによるパケットのフィルタリング 1

- ネットワーク要件 1
- 要件分析 1
- 使用しているソフトウェアのバージョン 2
- 設定手順 2
- 設定の確認 2
- 設定ファイル 3

例:IPアドレスによるパケットのフィルタリング 4

- ネットワーク要件 4
- 要件分析 4
- 使用しているソフトウェアのバージョン 5
- 設定の制約事項およびガイドライン 5
- 設定手順 5
- 設定の確認 6
- 設定ファイル 7

例:TCPパケットのフィルタリング 9

- ネットワーク要件 9
- 要件分析 9
- 使用しているソフトウェアのバージョン 10
- 設定手順 10
- 設定の確認 11
- 設定ファイル 12

関連ドキュメント 12

はじめに

このマニュアルでは、ACLの設定例について説明します。

前提条件

この文書は、Comware V 7ベースのMSRルーターに適用されます。例の手順と情報は、ルーターのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

このドキュメントの設定例は、ラボ環境で作成および検証されたものであり、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、すべてのコマンドがネットワークに与える潜在的な影響を理解していることを確認してください。

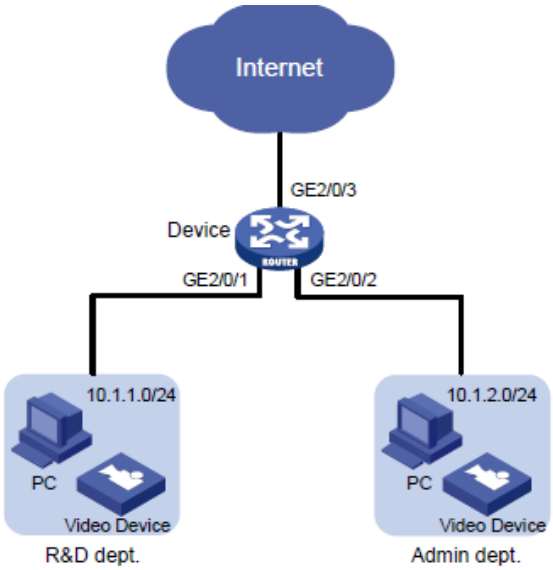
この文書では、ACLの基本的な知識があることを前提としています。

例:MACアドレスによるパケットのフィルタリング

ネットワーク要件

図1に示すように、研究開発部門と管理部門にはビデオデバイスが導入されています。ビデオデバイスは、000f-e2のプレフィクスが付いたMACアドレスを使用します。発信ビデオデータが毎日8:30から18:00までしか通過できないように、デバイスにACLを設定します。

図1 ネットワークダイアグラム



要件分析

ビデオデバイスのMACアドレスは固定されているため、イーサネットフレームヘッダーACLを使用して、MACアドレスでパケットをフィルタリングできます。ACLで、同じプレフィクスを持つMACアドレスに一致するMACアドレスとマスクを指定します。

使用しているソフトウェアのバージョン

この設定例は、R0106で作成および検証されています。

設定手順

#インターフェイスにIPアドレスを割り当てます。

<Device> system-view

[Device] interface gigabitethernet 2/0/1

[Device-GigabitEthernet2/0/1] ip address 10.1.1.1 24

[Device-GigabitEthernet2/0/1] quit

[Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] ip address 10.1.2.1 24

[Device-GigabitEthernet2/0/2] quit

[Device] interface gigabitethernet 2/0/3

[Device-GigabitEthernet2/0/3] ip address 200.1.1.2 24

[Device-GigabitEthernet2/0/3] quit

#毎日8:30から18:00までの時間範囲に時間範囲time1を作成します。

[Device] time-range time1 8:30 to 18:00 daily

#イーサネットフレームヘッダーACL 4000を設定して、000f-e2のプレフィクスが付いた送信元MACアドレスを持つパケットがtime 1で設定した時間の間だけ通過できるようにします。

[Device] acl number 4000

[Device-acl-ethernetframe-4000] rule permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1

[Device-acl-ethernetframe-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000

[Device-acl-ethernetframe-4000] quit

#ACL 4000を適用して、GigabitEthernet 2/0/1およびGigabitEthernet 2/0/2の着信パケットをフィルタリングします。

[Device] interface gigabitethernet 2/0/1

[Device-GigabitEthernet2/0/1] packet-filter 4000 inbound

[Device-GigabitEthernet2/0/1] quit

[Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] packet-filter 4000 inbound

[Device-GigabitEthernet2/0/2] quit

#デフォルトルートを設定します。

[Device] ip route-static 0.0.0.0 0.0.0.0 200.1.1.1

設定の確認

#ACLがパケットフィルタリングに正常に適用されていることを確認します。

[Device] display packet-filter interface inbound

```
Interface: GigabitEthernet2/0/1
 In-bound policy:
  ACL 4000
  MAC default action: Permit
Interface: GigabitEthernet2/0/2
 In-bound policy:
  ACL 4000
  MAC default action: Permit
```

#時間範囲time1の間に、ビデオデバイスが外部ネットワークと通信できることを確認します(詳細は省略)。

#ビデオデバイスが時間範囲time1を超えて外部ネットワークと通信できないことを確認します(詳細は省略)。

設定ファイル

```
#
interface GigabitEthernet2/0/1
  port link-mode route
  combo enable copper
  ip address 10.1.1.1 255.255.255.0
  packet-filter 4000 inbound
#
interface GigabitEthernet2/0/2
  port link-mode route
  combo enable copper
  ip address 10.1.2.1 255.255.255.0
  packet-filter 4000 inbound
#
interface GigabitEthernet2/0/3
  port link-mode route
  combo enable copper
  ip address 200.1.1.2 255.255.255.0
#
  ip route-static 0.0.0.0 0 200.1.1.1
#
  time-range time1 08:30 to 18:00 daily
#
acl number 4000
  rule 0 permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
  rule 5 deny source-mac 000f-e200-0000 ffff-ff00-0000
```

例:IPアドレスによるパケットのフィルタリング

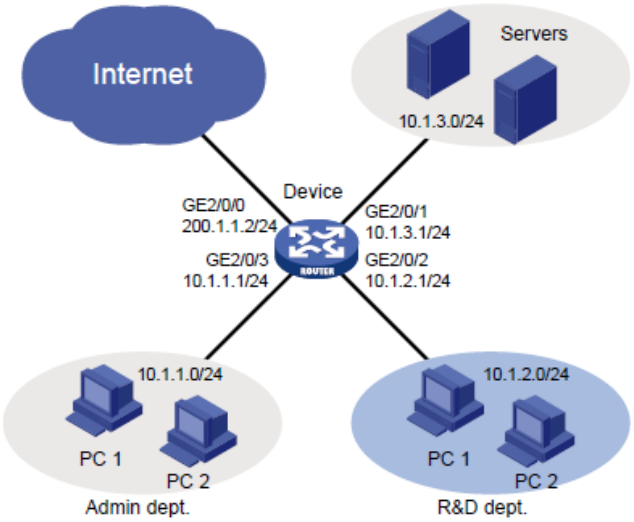
ネットワーク要件

図2に示すように、企業の内部ネットワークは、デバイスを介してインターネットに接続します。研究開発部門、管理部門、およびサーバーは、異なるサブネット上にあります。

次の要件を満たすようにACLを設定します。

- 管理部門は、インターネットとサーバーにはいつでもアクセスできますが、研究開発部門にはいつでもアクセスできません。
- 研究開発部門は、業務時間内(月～金曜日の8:30～18:00)はサーバーのみにアクセスできます。インターネットやサーバーにはアクセスできますが、業務時間外は管理部門にはアクセスできません。

図2 ネットワークダイアグラム



要件分析

ネットワーク要件を満たすには、次のタスクを実行する必要があります。

- 管理部門による研究開発部門へのアクセスを拒否するには、次のタスクを実行します。
  - サブネット10.1.2.0/24宛てのパケットを拒否する高度なACLを設定します。
  - ACLを適用して、GigabitEthernet 2/0/3上の着信パケットをフィルタリングします。
- 研究開発部門のアクセス制御を実装するには、次のタスクを実行します。
  - 稼働時間の時間範囲を作成します(月曜日から金曜日の8:30～18:00)。
  - 詳細ACLを作成し、次のルールを設定します。
    - サブネット10.1.3.0/24宛てのパケットのみを通過させるようにルールを設定します。時間範囲内でアクティブになるようにルールを設定します。
    - 研究開発部門による管理部門へのアクセスを拒否するには、サブネット10.1.1.0/24宛てのパケットを拒否する規則を設定します。
  - ACLを適用して、Ten-GigabitEthernet 2/0/2上の着信パケットをフィルタリングします。

使用しているソフトウェアのバージョン

この設定例は、R0106で作成および検証されています。

設定の制約事項およびガイドライン

勤務時間中にR&D部門がサーバーだけにアクセスできるようにACLルールを設定する場合は、denyルールの前にpermitルールを設定します。そうしないと、勤務時間中にインターフェイスがすべてのパケットを拒否します。

設定手順

1. デバイス上のインターフェイスにIPアドレスを割り当てます。

   #GigabitEthernet 2/0/0にIPアドレスを割り当てます。

   <Device> system-view

   [Device] interface gigabitethernet 2/0/0

   [Device-GigabitEthernet2/0/0] ip address 200.1.1.2 24

   [Device-GigabitEthernet2/0/0] quit

   #他のインターフェイスにIPアドレスを割り当てます(詳細は省略)。

2. デフォルトルートを設定します。

   [Device] ip route-static 0.0.0.0 0.0.0.0 200.1.1.1

3. 管理部門によるR&D部門へのアクセスを拒否します。

   #IPv4拡張ACL 3000を作成します。

   [Device] acl number 3000

   #サブネット10.1.2.0/24宛てのパケットの通過を拒否するルールを設定します。

   [Device-acl-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255

   [Device-acl-adv-3000] quit

   #ACL 3000を適用して、Ten-GigabitEthernet 2/0/3上の着信パケットをフィルタリングします。

   [Device] interface gigabitethernet 2/0/3

   [Device-GigabitEthernet2/0/3] packet-filter 3000 inbound

   [Device-GigabitEthernet2/0/3] quit

4. R&D部門のアクセス制御を設定します。

   #月曜日から金曜日の8:30から18:00までの時間範囲worktimeを設定します。

   [Device] time-range worktime 8:30 to 18:00 working-day

   #IPv4拡張ACL 3001を作成します。

   [Device] acl number 3001

   #サブネット10.1.3.0/24宛てのパケットが就業時間中に通過できるように規則を設定します。

   [Device-acl-adv-3001] rule permit ip destination 10.1.3.0 0.0.0.255 time-range worktime

   #すべてのIPパケットが就業時間中に通過することを拒否するルールを設定します。

   [Device-acl-adv-3001] rule deny ip time-range worktime

#サブネット10.1.1.0/24宛てのパケットの通過を拒否するルールを設定します。

[Device-acl-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255

[Device-acl-adv-3001] quit

#ACL 3001を適用して、GigabitEthernet 2/0/2上の着信パケットをフィルタリングします。

[Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] packet-filter 3001 inbound

[Device-GigabitEthernet2/0/2] quit

設定の確認

#ACLがパケットフィルタリングに正常に適用されていることを確認します。

[Device] display packet-filter interface inbound

Interface: GigabitEthernet2/0/2

In-bound policy:

ACL 3001

IPv4 default action: Permit

Interface: GigabitEthernet2/0/3

In-bound policy:

ACL 3000

IPv4 default action: Permit

#月曜日の9時30分に、研究開発部門からインターネット上のWebサイトにpingを実行できないことを確認します。

C:\>ping www.abc.com

Pinging www.abc.com [199.181.132.250] with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 199.181.132.250:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

#月曜日の9時30分に、管理部門からインターネット上のWebサイトにpingを実行できることを確認します。

C:\>ping www.abc.com

Pinging www.abc.com [199.181.132.250] with 32 bytes of data:

Reply from 199.181.132.250: bytes=32 time=1ms TTL=122

Reply from 199.181.132.250: bytes=32 time<1ms TTL=122

Reply from 199.181.132.250: bytes=32 time<1ms TTL=122

Reply from 199.181.132.250: bytes=32 time<1ms TTL=122

Ping statistics for 199.181.132.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
#月曜日の19:30に研究開発部門からインターネット上のWebサイトにpingできることを確認します。
C:\>ping www.abc.com
Pinging www.abc.com [199.181.132.250] with 32 bytes of data:
Reply from 199.181.132.250: bytes=32 time=1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122

Ping statistics for 199.181.132.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

設定ファイル

```
#
interface GigabitEthernet2/0/0
 port link-mode route
 combo enable copper
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 combo enable copper
 ip address 10.1.3.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 packet-filter 3001 inbound
#
interface GigabitEthernet2/0/3
 port link-mode route
 combo enable copper
```

```
 ip address 10.1.1.1 255.255.255.0
 packet-filter 3000 inbound
#
 ip route-static 0.0.0.0 0 200.1.1.1
#
 time-range worktime 08:30 to 18:00 working-day
#
acl number 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl number 3001
 rule 0 permit ip destination 10.1.3.0 0.0.0.255 time-range worktime
 rule 5 deny ip time-range worktime
 rule 10 deny ip destination 10.1.1.0 0.0.0.255
#
```

例:TCPパケットのフィルタリング

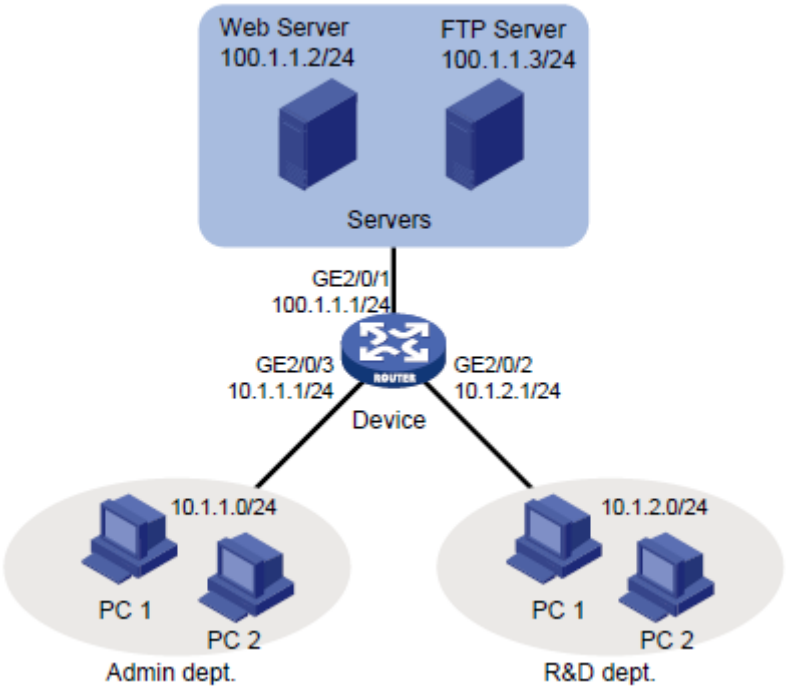
ネットワーク要件

図3に示すように、研究開発部門、管理部門、サーバーは異なるネットワーク上にあり、デバイスを介して接続されています。

次の要件を満たすようにACLを設定します。

- Webサーバーは、管理部門にのみHTTPサービスを提供します。TCP接続は、ホストによってのみ開始できます。
- FTPサーバーは、R&D部門にのみFTPサービスを提供します。TCP接続は、ホストまたはFTPサーバーのいずれかによって開始できます。

図3 ネットワークダイアグラム



要件分析

ネットワーク要件を満たすには、次のタスクを実行する必要があります。

- ホストによって開始されたWebサーバーへのTCP接続を許可するには、次のタスクを実行します。
  - 確立されたTCP接続を介してWebサーバーから送信されるパケットが通過できるように、次のように詳細ACLルールを設定します。
    - 確立されたTCP接続を照合するには、規則にestablishedキーワード(ACKまたはRSTフラグビットセット)を指定します。
    - TCPイニシエータは通常、1023より大きいTCPポート番号を使用するため、確立されたTCP接続に一致させるには、1023より大きいポート番号の範囲を指定します。
  - Webサーバーが存在するサブネットからホストが存在するサブネットに送信されるパケットを拒否する詳細ACLルールを設定します。
- FTPでは、データ転送にTCPポート20を使用し、FTP制御にポート21を使用します。FTPトラフィ

ックを識別するには、ACLルールでTCPポート20および21を指定する必要があります。

- HTTPパケットを識別するには、ACLルールでTCPポート80を指定します。

使用しているソフトウェアのバージョン

この設定例は、R0106で作成および検証されています。

設定手順

1. デバイス上のインターフェイスにIPアドレスを割り当てます。

   #GigabitEthernet 2/0/1にIPアドレスを割り当てます。

   [Device] interface gigabitethernet 2/0/1

   [Device-GigabitEthernet2/0/1] ip address 100.1.1.1 24

   #他のインターフェイスにIPアドレスを割り当てます(詳細は省略)。

2. 管理部門のアクセス制御を設定します。

   #IPv4拡張ACL 3000を作成します。

   <Device> system-view

   [Device] acl number 3000

   #Webサーバーからサブネット10.1.1.0/24上のホストへのTCPパケットを許可するルールを設定します。TCPポート番号は1023より大きく、ACKまたはRSTフラグが設定されています。

   [Device-acl-adv-3000] rule permit tcp established source 100.1.1.2 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023

   #サブネット100.1.1.0/24からサブネット10.1.1.0/24へのTCPパケットの通過を拒否するルールを設定します。

   [Device-acl-adv-3000] rule deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255

   #100.1.1.3/32を送信元とするFTPパケットの通過を拒否するルールを設定します。

   [Device-acl-adv-3000]rule deny tcp source 100.1.1.3 0 source-port range 20 21

   [Device-acl-adv-3000]quit

   #ACL 3000を適用して、GigabitEthernet 2/0/3上の発信パケットをフィルタリングします。

   [Device] interface gigabitethernet 2/0/3

   [Device-GigabitEthernet2/0/3] packet-filter 3000 outbound

   [Device-GigabitEthernet2/0/3] quit

3. 研究開発部門のアクセス制御を設定します。

   #IPv4拡張ACL 3001を作成します。

   [Device] acl number 3001

   #100.1.1.2/32を送信元とするHTTPパケットの通過を拒否するルールを設定します。

   [Device-acl-adv-3001] rule deny tcp source 100.1.1.2 0 source-port eq 80

   [Device-acl-adv-3001] quit

   #ACL 3001を適用して、GigabitEthernet 2/0/2上の発信パケットをフィルタリングします。

   [Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] packet-filter 3001 outbound

[Device-GigabitEthernet2/0/2] quit

設定の確認

1. ACLがパケットフィルタリングに正常に適用されていることを確認します。

   [Device] display packet-filter interface outbound

   Interface: GigabitEthernet2/0/2

   Out-bound policy:

   ACL 3001

   IPv4 default action: Permit Interface:

   GigabitEthernet2/0/3

   Out-bound policy:

   ACL 3000

   IPv4 default action: Permit

2. 管理部門からFTPサーバーにTelnetで接続できないことを確認します。

   C:\>telnet 100.1.1.3 21

   Connecting To 100.1.1.3...Could not open connection to the host, on port 21:

   Connect failed

   C:\>

3. Webサーバーから、管理部門のホストに対してpingを実行できるが、ホスト上の共有フォルダにはアクセスできないことを確認します。

   #管理部門のホストに共有フォルダを設定します。(詳細は省略)

   #Webサーバーからホストにpingを実行します。ping操作は成功します。

   C:\>ping 10.1.1.110

   Pinging 10.1.1.110 with 32 bytes of data:

   Reply from 10.1.1.110: bytes=32 time=2ms TTL=128

   Reply from 10.1.1.110: bytes=32 time=14ms TTL=128

   Reply from 10.1.1.110: bytes=32 time=1ms TTL=128

   Reply from 10.1.1.110: bytes=32 time=1ms TTL=128

   Ping statistics for 10.1.1.110:

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

   Approximate round trip times in milli-seconds:

   Minimum = 1ms, Maximum = 14ms, Average = 4ms

   C:\>

   #Webサーバーから共有フォルダにアクセスできないことを確認します(詳細は省略)。

4. 研究開発部門からWebサーバーにTelnetで接続できないことを確認します。

   C:\>telnet 100.1.1.2 80

```
Connecting To 100.1.1.2...Could not open connection to the host, on port 80:
 Connect failed
C:\>
```

設定ファイル

```
#
interface GigabitEthernet2/0/1
    port link-mode route
 combo enable copper
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
    port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 packet-filter 3001 outbound
#
interface GigabitEthernet2/0/3
    port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 packet-filter 3000 outbound
#
acl number 3000
 rule 0 permit tcp source 100.1.1.2 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
 established
 rule 5 deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 10 deny tcp source 100.1.1.3 0 source-port range ftp-data ftp
#
acl number 3001
 rule 0 deny tcp source 100.1.1.2 0 source-port eq www
```

関連ドキュメント

- *H3C MSRシリーズルーターACLおよびQoSコンフィギュレーションガイド(V7)*
- *H3C MSRシリーズルーターACLおよびQoSコマンドリファレンス(V7)*