H3C スイッチシリーズ

ACLの設定例

ドキュメントバージョン:6W100-20190628

内容

はじめに

この文書では、ACLの設定例を示します。

前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されません。

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。

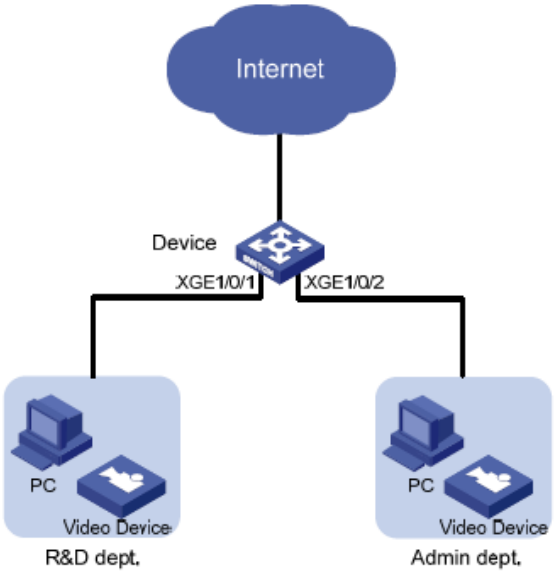
このドキュメントでは、ACLの基本的な知識があることを前提としています。

例:MACアドレスによるパケットのフィルタリング

ネットワーク構成

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配備されています。ビデオデバイスは、000f-e2というプレフィクスが付いたMACアドレスを使用します。デバイスにパケットフィルタリングを設定して、毎日8:30～18:00の間だけ発信ビデオデータが通過できるようにします。

図1ネットワークダイアグラム



解析

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では、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。

使用されるソフトウェアのバージョン

この設定例は、S5024-CMW710-R6328P03で作成および確認されたものです。

手順

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> system-view

[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、送信元MACアドレスに000f-e2というプレフィクスが付いたパケットが時間1の間だけ通過できるようにします。

[Device] acl mac 4000

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

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

[Device-acl-mac-4000] quit

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

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] packet-filter mac 4000 inbound

[Device-GigabitEthernet1/0/1] quit

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] packet-filter mac 4000 inbound

[Device-GigabitEthernet1/0/2] 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ることを確認します。

[Device] display packet-filter interface inbound

Interface: GigabitEthernet1/0/1

Inbound policy:

MAC ACL 4000

Interface: GigabitEthernet1/0/2

Inbound policy:

MAC ACL 4000

time1の時間範囲内で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time1の時間範囲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 GigabitEthernet1/0/1
 packet-filter mac 4000 inbound
#
interface GigabitEthernet1/0/2
 packet-filter mac 4000 inbound
#
 time-range time1 08:30 to 18:00 daily
#
acl mac 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
```

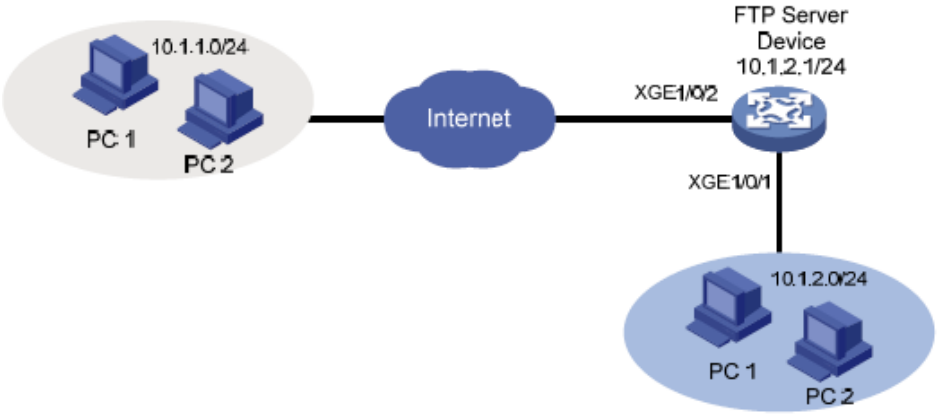
例:FTPアクセスの制御

ネットワーク構成

図2に示すように、デバイスはFTPサーバーです。次の要件を満たすように、デバイスにFTPアクセスコントロールを設定します。

- サブネット10.1.2.0/24のユーザーは、いつでもFTPサーバーにアクセスできます。
- サブネット10.1.1.0/24のユーザーは、就業日(月曜日～金曜日)の就業時間中(8:30～18:00)にFTPサーバーにアクセスできます。
- 資格のあるユーザーには、レベル15のユーザーロールが割り当てられます。

図2ネットワークダイアグラム



解析

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。

- ACLに2つのルールを設定します。1つのルールはサブネット10.1.2.0/24からのパケットを許可します。もう1つのルールはサブネット10.1.1.0/24からのパケットを許可し、就業日の就業時間中にのみ有効になります。
- ACLを使用して、FTPサーバーへのアクセスを制御します。

使用されるソフトウェアのバージョン

この設定例は、S5024-CMW710-R6328P03で作成および確認されたものです。

手順

月曜から金曜までの就業時間8:30～18:00の時間範囲**ftp**を設定します。

<Device> system-view

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

IPv4基本ACL 2000を作成します。

[Device] acl basic 2000

サブネット10.1.2.0/24からのパケットを許可するようにルールを設定します。

[Device-acl-ipv4-basic-2000] rule permit source 10.1.2.0 0.0.0.255

ftpの時間範囲内でサブネット10.1.1.0/24からのパケットを許可するルールを設定します。

[Device-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255 time-range ftp

[Device-acl-ipv4-basic-2000]quit

デバイス上のFTPサーバーを有効にします。

[Device] ftp server enable

ftpという名前のローカルユーザーを追加し、このユーザーにFTPサービスの使用を許可します。

[Device] local-user ftp

[Device-luser-manage-ftp] service-type ftp

ローカルユーザーのパスワードを設定します。

[Device-luser-manage-ftp] password simple 123456

ローカルユーザーにレベル15のユーザーロールを割り当てます。

[Device-luser-manage-ftp] authorization-attribute user-role level-15

[Device-luser-manage-ftp] quit

FTPサーバーへのアクセスを制御するには、ACL 2000を使用します。

[Device] ftp server acl 2000

設定の確認

10.1.2.100のホストを使用して、通信日の就業時間中にFTPサーバーにログインできることを確認します。

Microsoft Windows [Version 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1

Connected to 10.1.2.1.

220 FTP service ready.

User (10.1.2.1:(none)): ftp

331 Password required for ftp.

Password:

230 User logged in.

10.1.1.100のホストを使用して、就業日の就業時間中にFTPサーバーにログインできることを確認します。

Microsoft Windows [Version 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1

Connected to 10.1.2.1.

220 FTP service ready.

User (10.1.2.1:(none)): ftp

331 Password required for ftp.

Password:
230 User logged in.
10.1.2.100のホストを使用して、営業時間外にFTPサーバーにログインできることを確認します。
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
10.1.1.100のホストを使用して、営業時間外にFTPサーバーにログインできないことを確認します。
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1
ftp>
ftp> ls
Not connected.

設定ファイル

```
#
 time-range ftp 08:30 to 18:00 working-day
#
 acl basic 2000
  rule 0 permit source 10.1.2.0 0.0.0.255
  rule 5 permit source 10.1.1.0 0.0.0.255 time-range ftp
#
 local-user ftp class manage
 password hash
$h$6$HVOQzdJMVPtVd0A7$hFeYeT1ic7AgOPJ/z/Ci9db347bnJ2krcnzA+lD++iG
0jC5qSybNhuH7zi70tH4d42Y3mYtsqNaBGsN0f0ilvA==
 service-type ftp
 authorization-attribute user-role level-15
 authorization-attribute user-role network-operator
#
 ftp server enable
 ftp server acl 2000
```

例:IPアドレスによるパケットのフィルタリング

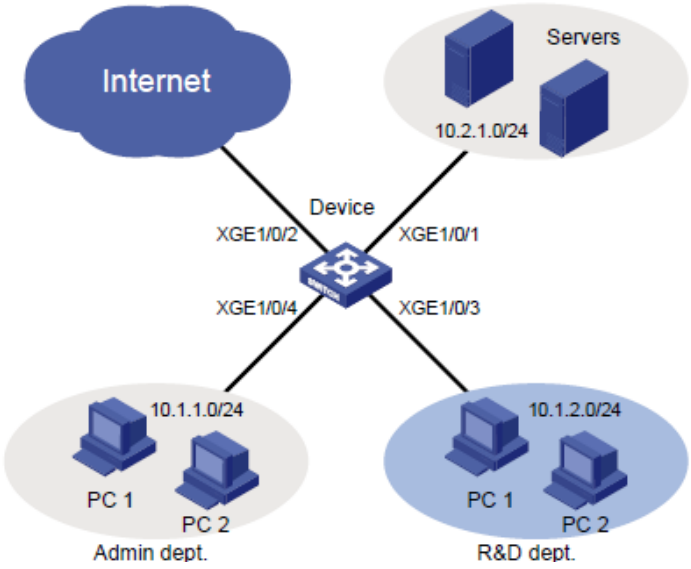
ネットワーク構成

図3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パケットフィルタリングを設定します。

- 管理部門はいつでもインターネットとサーバーにアクセスできますが、研究開発部門にはアクセスできません。
- 研究開発部門は、就業日(月～金)の就業時間内(8:30～18:00)にはサーバーにのみアクセスできます。インターネットおよびサーバーにはアクセスできますが、就業時間外には管理部門にアクセスできません。

図3ネットワークダイアグラム



解析

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R&D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ように拡張ACLを設定します。
  - ACLを適用して、GigabitEthernet 1/0/4の着信パケットをフィルタリングします。
- R&D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。
  - 稼働日(月曜～金曜)の稼働時間の時間範囲(8:30～18:00)を作成します。
  - 拡張ACLを作成し、次のルールを設定します。
    - サブネット10.2.1.0/24宛てのパケットだけが通過でき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。
    - R&D部門が管理部門にアクセスすることを拒否するには、サブネット10.1.1.0/24宛てのパケットを拒否するルールを設定します。
  - ACLを適用して、GigabitEthernet 1/0/3の着信パケットをフィルタリングします。

使用されるソフトウェアのバージョン

この設定例は、S5024-CMW710-R6328P03で作成および確認されたものです。

制約事項とガイドライン

ACLルールを設定して、R&D部門が就業日の就業時間中にサーバーだけにアクセスできるようにする場合は、拒否ルールの前に許可ルールを設定します。許可ルールを設定しないと、インターフェイスは就業日の就業時間中にすべてのパケットを拒否します。

手順

管理部門が研究開発部門にアクセスできないようにする

IPv4拡張ACL 3000を作成します。

<Device> system-view

[Device] acl advanced 3000

サブネット10.1.2.0/24宛てのパケットが通過することを拒否するルールを設定します。

[Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255

[Device-acl-ipv4-adv-3000] quit

ACL 3000を適用して、GigabitEthernet 1/0/4上の着信パケットをフィルタリングします。

[Device] interface gigabitethernet 1/0/4

[Device-GigabitEthernet1/0/4] packet-filter 3000 inbound

[Device-GigabitEthernet1/0/4] quit

R&D部門のアクセス制御の設定

月曜から金曜までの時間範囲8:30～18:00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 advanced 3001

サブネット10.2.1.0/24宛てのパケットが勤務時間中に通過できるようにするルールを設定します。

[Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255 time-range worktime

worktimeの時間中のすべてのIPパケットの通過を拒否するルールを設定します。

[Device-acl-ipv4-adv-3001] rule deny ip time-range worktime

サブネット10.1.1.0/24宛てのパケットが通過することを拒否するルールを設定します。

[Device-acl-ipv4-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255

[Device-acl-ipv4-adv-3001] quit

ACL 3001を適用して、GigabitEthernet 1/0/3上の着信パケットをフィルタリングします。

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] packet-filter 3001 inbound

[Device-GigabitEthernet1/0/3] 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ることを確認します。

[Device] display packet-filter interface inbound

Interface: GigabitEthernet1/0/3

Inbound policy:

IPv4 ACL 3001

Interface: GigabitEthernet1/0/4

Inbound policy:

IPv4 ACL 3000

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

C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Request timed out.

Request timed out. Request timed out. Request timed out.

Ping statistics for 173.194.127.242:

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

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

C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50 Reply from 173.194.127.242: bytes=32 time=30ms TTL=50 Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:

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

Approximate round trip times in milli-seconds:

Minimum = 30ms, Maximum = 30ms, Average =
30ms 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ウェブサイトにpingできることを確認します。

C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms
TTL=50 Reply from 173.194.127.242: bytes=32
time=30ms TTL=50

Ping statistics for 173.194.127.242:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 30ms, Maximum = 30ms, Average =
30ms C:\>

設定ファイル

```
#
interface GigabitEthernet1/0/3
 packet-filter 3001 inbound
#
interface GigabitEthernet1/0/4
 packet-filter 3000 inbound
#
 time-range worktime 08:30 to 18:00 working-day
#
acl advanced 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip destination 10.2.1.0 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

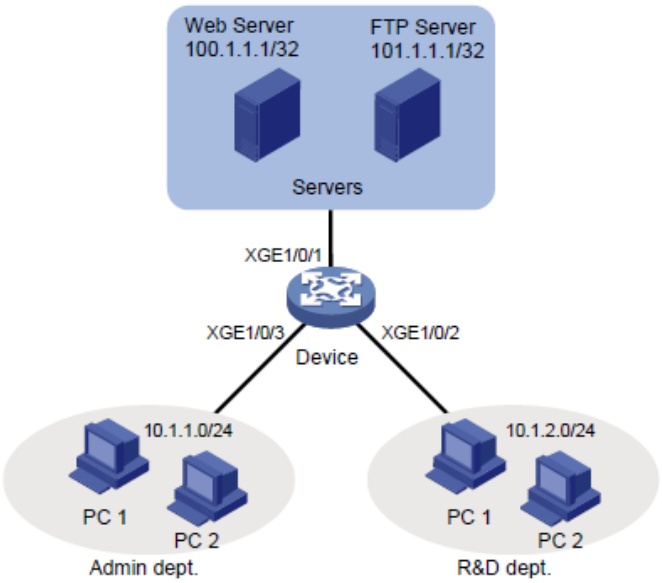
ネットワーク構成

図4に示すように、研究開発部門、管理部門、および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パケットフィルタリングを設定します。

- Webサーバーは、管理部門にのみHTTPサービスを提供します。
- FTPサーバーは、研究開発部門だけにFTPサービスを提供します。
- ホストとWebサーバー間のTCP接続は、ホストによってのみ開始できます。ホストとFTPサーバー間の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4ネットワークダイアグラム



解析

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たパケットが通過できるようにするには、詳細ACLルールを次のように設定します。
    - 確立されたTCP接続を照合するために、ルールで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接続と一致するように、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高度なACLルールを構成します。
- 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。

使用されるソフトウェアのバージョン

この設定例は、S5024-CMW710-R6328P03で作成および確認されたものです。

手順

管理部門のアクセスコントロールの構成

IPv4拡張ACL 3000を作成します。

<Device> system-view

[Device] acl advanced 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-ipv4-adv-3000] rule permit tcp established source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023

サブネット100.1.1.1/32からサブネット10.1.1.0/24へのTCPパケットのパススルーを拒否するルールを設定します。

[Device-acl-ipv4-adv-3000] rule deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255

101.1.1.1/32から送信されたFTPパケットの通過を拒否するルールを設定します。

[Device-acl-ipv4-adv-3000] rule deny tcp source 101.1.1.1 0 source-port range 20 21

[Device-acl-ipv4-adv-3000] quit

ACL 3000を適用して、GigabitEthernet 1/0/3上の発信パケットをフィルタリングします。

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] packet-filter 3000 outbound

[Device-GigabitEthernet1/0/3] quit

R&D部門のアクセス制御の設定

IPv4拡張ACL 3001を作成します。

[Device] acl advanced 3001

100.1.1.1/32から送信されたHTTPパケットのパススルーを拒否するルールを設定します。

[Device-acl-ipv4-adv-3001] rule deny tcp source 100.1.1.1 0 source-port eq 80

[Device-acl-ipv4-adv-3001] quit

ACL 3001を適用して、GigabitEthernet 1/0/2上の発信パケットをフィルタリングします。

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] packet-filter 3001 outbound

[Device-GigabitEthernet1/0/2] 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ることを確認します。

   [Device] display packet-filter interface outbound

   Interface: GigabitEthernet1/0/2
   Outbound policy:
   IPv4 ACL 3001
   Interface: GigabitEthernet1/0/3
   Outbound policy:
   IPv4 ACL 3000
2. 管理部門からFTPサーバーにTelnet接続できないことを確認します。
   C:\>telnet 101.1.1.1 21
   Connecting To 101.1.1.1...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. R&D部門からWebサーバーにTelnet接続できないことを確認します。
   C:\>telnet 100.1.1.1 80
   Connecting To 100.1.1.1...Could not open connection to the host, on port 80:
   Connect failed

C:\>

設定ファイル

```
#
interface GigabitEthernet1/0/2
 packet-filter 3001 outbound
#
interface GigabitEthernet1/0/3
 packet-filter 3000 outbound
#
acl advanced 3000
 rule 0 permit tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
 established
 rule 5 deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255
 rule 10 deny tcp source 101.1.1.1 0 source-port range ftp-data ftp
#
 acl advanced 3001
  rule 0 deny tcp source 100.1.1.1 0 source-port eq www
```