NAT の設定

実習内容と目標

このラボでは以下のことを学びます：

- NAT の基本的なコンフィギュレーションを習得します。
- NAPT のコンフィギュレーション方法を習得します。
- Easy IP のコンフィギュレーション方法を習得します。
- NAT Server のコンフィギュレーション方法を習得します。

ネットワーク図

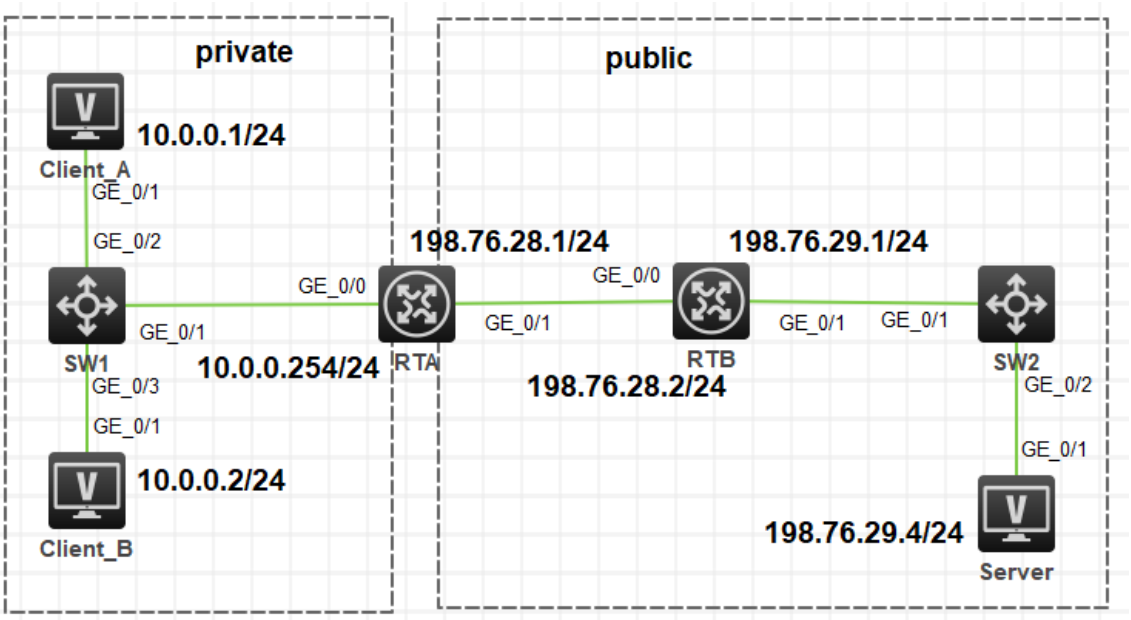

図 14.1 実習ネットワーク

上の図は、テストトポロジを示しています。2 つの MSR3620（RTA と RTB）、2 つの S5820V2（SW1 と SW2）、および 3 つの PC（Client_A、Client_B と Server）です。

Client_A と Client_B はプライベートネットワーク上にあり、RTA はゲートウェイと NAT デバイスとして機能し、1 つのプライベートネットワークポート（G0/0）と 1 つのパブリックネットワークを持ち、RTB がゲートウェイとして機能します。

トポロジには、いくつかの NAT アプリケーションが含まれます。 Easy IP は最も単純で、主にダイヤルアップアクセスシナリオで使用されます。 基本的な NAT は NAPT ほど使われておりません。 NAPT は、パブリックネットワーク IP アドレスの使用を改善でき、パブリックサーバーシナリオへの

プライベートクライアントアクセスに適用できます。 NAT サーバーは、プライベートサービスからパブリックネットワークへのシナリオに適用できます。

実習装置

本実験に必要な主な設備機材 実験装置名前とモデル番号	バージョン	数量	特記事項
MSR36-20	Version7.1	2	ルーター
S5820V2	Version7.1	2	スイッチ
PC	Windows 7	3	ホスト
ネットワークケーブルの接続	--	6	ストレートケーブル

実習手順

タスク 1:基本的な NAT の設定をする

このテストでは、プライベートネットワーククライアントの Client_A と Client_B がパブリックネットワークサーバーにアクセスする必要があります。 RTB はプライベートネットワークルートを格納しないため、RTA で基本的な NAT を構成して、パブリックネットワークアドレスを Client_A と Client_B に動的に割り当てます。

手順 1:テスト環境を構築する

ラボの図に従ってテスト環境を構築し、RTA および RTB ポートに IP アドレスを構成します。 サーバー宛てのパケットをルーティングするには、ネクストホップ RTB G0/0 を使用して、RTB を指すように RTA で静的ルートを構成します。 RTA はサーバーに ping を実行できます。 Client_A の IP アドレスを 10.0.0.1/24 として、ゲートウェイを 10.0.0.254 として構成します。 Client_B IP アドレスを 10.0.0.2/24 として構成し、ゲートウェイを 10.0.0.254 として構成します。

表 14-1 IP アドレス割り当てスキーマ

装置	**インターフェイス**	**IP アドレス**	**ゲートウェイ**
RTA	G0/0	10.0.0.254/24	-
	G0/1	198.76.28.1/24	-
RTB	G0/0	198.76.28.2/24	-
	G0/1	198.76.29.1/24	-

Client A		10.0.0.1	10.0.0.254
Client B		10.0.0.2	10.0.0.254
Server		198.76.29.4/24	198.76.29.1/24

手順 2：基本的なコンフィギュレーション

IP アドレスとルートを設定します(RTB では、あえて RTA への static route を設定しません)。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]ip address 10.0.0.254 24

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]ip address 198.76.28.1 24

[RTA-GigabitEthernet0/1]quit

[RTA]ip route-static 0.0.0.0 0 198.76.28.2

[RTB]interface GigabitEthernet 0/0

[RTB-GigabitEthernet0/0]ip address 198.76.28.2 24

[RTB-GigabitEthernet0/0]quit

[RTB]interface GigabitEthernet 0/1

[RTB-GigabitEthernet0/1]ip address 198.76.29.1 24

[RTB-GigabitEthernet0/1]quit

手順 3：接続性をチェックします

Client_A と Client_B でそれぞれサーバー（IP アドレス 198.76.29.4）に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

以前の情報に基づいて、Client_A と Client_B はサーバーに ping を実行できません。 RTB にはプライベートネットワークへのルートがないためです。 RTB は、サーバーから送信された ping パケットのネットワークセグメント 10.0.0.0 宛てのルートを見つけることができません。

手順 4：Basic NAT を設定します

RTA で Basic NAT を設定します。

ACL を使用して、ネットワークセグメント 10.0.0.0/24 にある送信元アドレスでフローを定義します。

[RTA]acl basic 2000

[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

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

アドレス変換のためのアドレスとして 198.76.28.11 から 198.76.28.20 を用意した NAT アドレスプール 1 を作成します。

[RTA]nat address-group 1

[RTA-address-group-1]address 198.76.28.11 198.76.28.20

[RTA-address-group-1]quit

インターフェースビューに入り、ACL 2000 と NAT アドレスプール 1 を結び付けて outbound ポート経由でアドレスを割り当てます。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1 no-pat

[RTA-GigabitEthernet0/1]quit

パブリックネットワークアドレスプールのアドレスグループ 1 は、RTA で構成され、アドレス範囲は 198.76.28.11-198.76.28.20 です。 パラメータ no-pat は、1 対 1 のアドレス変換を示します。これは、ポート番号ではなく、アドレス指定されたアドレスを変換することを意味します。 この場合、RTA は、ACL2000 ルールを変更するアウトバウンドパケットのアドレスを変換します。

手順 5：接続性をチェックします

Client_A と Client_B でそれぞれサーバー（IP アドレス 198.76.29.4）に ping を実行します。 出力情報は次のとおりです。

<H3C>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=4.000 ms

56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=8.000 ms

手順 6：NAT エントリーをチェックします

RTA で NAT エントリーをチェックします。

```
[RTA]display nat session
Slot 0:
Initiator:
  Source          IP/port: 10.0.0.1/172
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Initiator:
  Source          IP/port: 10.0.0.1/171
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Total sessions found: 2

[RTA]display nat no-pat
Slot 0:
Total entries found: 0
[RTA]display nat no-pat
Slot 0:
Local     IP: 10.0.0.1
Global    IP: 198.76.28.17
Reversible: N
Type          : Outbound

Local     IP: 10.0.0.2
Global    IP: 198.76.28.16
Reversible: N
Type          : Outbound

Total entries found: 2
```

以前の情報に基づいて、この ICMP パケットの送信元アドレス 10.0.0.1 は、送信元ポート番号 249 および宛先ポート番号 2048 のパブリックネットワークアドレス 192.76.28.12 に変換されまし

た。送信元アドレス 10.0.0.2 は、 パブリックネットワークアドレス 198.76.28.11、送信元ポート番号 210、宛先ポート番号 2048。1 分後に全体を確認します。 最後のネットワークエントリは失われます。 4 分後、すべてのエントリーが失われます。 出力情報は次のとおりです。

```
[RTA]display nat session
Slot 0:
Total sessions found: 0
```

NAT エントリーにはエージングタイム（エージングタイム）があります。 エージング時間が経過すると、NAT は対応するエントリーを削除します。Display session aging-time state コマンドを実行して、セッションのデフォルトのエージングタイムを照会します。

```
[RTA]display session aging-time state
SESSION is not configured.
```

HCL のルーターではデフォルトのエージングタイムが設定されていないようなので、セッションの状態を確認します。

```
[RTA]display session statistics
Slot 0:
Current sessions: 4
                TCP sessions:                    0
                UDP sessions:                    0
               ICMP sessions:                    4
             ICMPv6 sessions:                    0
          UDP-Lite sessions:                     0
               SCTP sessions:                    0
               DCCP sessions:                    0
              RAWIP sessions:                    0

History average sessions per second:
        Past hour: 0
        Past 24 hours: 0
        Past 30 days: 0
History average session establishment rate:
        Past hour: 0/s
        Past 24 hours: 0/s
        Past 30 days: 0/s

Current relation-table entries: 0
```

Session establishment rate: 0/s

TCP:	0/s
UDP:	0/s
ICMP:	0/s
ICMPv6:	0/s
UDP-Lite:	0/s
SCTP:	0/s
DCCP:	0/s
RAWIP:	0/s

Received TCP	:	0 packets	0 bytes
Received UDP	:	0 packets	0 bytes
Received ICMP	:	0 packets	0 bytes
Received ICMPv6	:	0 packets	0 bytes
Received UDP-Lite	:	0 packets	0 bytes
Received SCTP	:	0 packets	0 bytes
Received DCCP	:	0 packets	0 bytes
Received RAWIP	:	0 packets	0 bytes

session aging-time コマンドを使って NAT セッションのエージングタイムを変更してみます。
NAT でバッキング情報は以下の通りです:

```
<RTA>terminal monitor
The current terminal is enabled to display logs.
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging nat packet
<RTA>*Nov 22 12:09:21:244 2021 RTA NAT/7/COMMON:
  PACKET: (GigabitEthernet0/1-out) Protocol: ICMP
            10.0.0.2:       0 -        198.76.29.4:       0(VPN:       0) ------>
       198.76.28.12:       0 -        198.76.29.4:       0(VPN:       0)
*Nov 22 12:09:21:247 2021 RTA NAT/7/COMMON:
  PACKET: (GigabitEthernet0/1-in) Protocol: ICMP
        198.76.29.4:       0 -       198.76.28.12:       0(VPN:       0) ------>
        198.76.29.4:       0 -            10.0.0.2:       0(VPN:       0)
```

以上のデバッキング情報によると、GigabitEthernet G0/1 の出力で、ICMP 10.0.0.2 の発信元ア

ドレスのパケットは 198.76.28.12 に変換されていることが分かります。

ノート:

理論的には、各 IP アドレスには 65,536 個のポートがあります。 占有ポートと予約ポートを除いて、使用可能なポートは理論値よりはるかに少なくなります。

手順 7:コンフィギュレーションを元に戻します

RTA の Basic NAT 設定を削除します。

NAT アドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられた NAT を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク 2:NAPT の設定をする

プライベートネットワーククライアント client_A と Client_B は、パブリックネットワークサーバーにアクセスする必要があります。 パブリックネットワークアドレスが制限されているため、RTA で構成されているパブリックネットワークアドレスの範囲は 198.76.28.11-198.76.28.20 です。 RTA で NAPT を構成して、パブリックネットワークアドレスとポートを Client_A と Client_B に動的に割り当てます。

手順 1:テスト環境を構築する

テスト環境を構築します。 タスク 1 のステップ 1 と 2 を参照してください。

手順 2:接続性をチェックします

Client_A と Client_B でそれぞれサーバー(IP アドレス 198.76.29.4)に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

以前の情報に基づいて、Client_A と Client_B はサーバーに ping を実行できません。

手順 3：NAPT を設定します

ACL を使用して、ネットワークセグメント 10.0.0.0/24 にある送信元アドレスでフローを定義します。

[RTA]acl basic 2000

[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

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

NAT アドレスプール 1 を 1 つのアドレス 198.76.28.11 で構成します。

[RTA]nat address-group 1

[RTA-address-group-1]address 198.76.28.11 198.76.28.11

[RTA-address-group-1]quit

インターフェースビューで NAT アドレスを acl 2000 にバインドし、アドレスを提供します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1

[RTA-GigabitEthernet0/1]quit

パラメータ no-pat は伝送されず、NAT がパケット内のポートを変換することを示します。

手順 4：接続性をチェックします

Client_A と Client_B でそれぞれサーバー（IP アドレス 198.76.29.4）に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=7.000 ms

手順 5：NAT エントリーをチェックします

RTA の nat エントリーをチェックします。

[RTA]display nat session verbose

Slot 0:

Initiator:

Source IP/port: 10.0.0.1/191

Destination IP/port: 198.76.29.4/2048

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/3
Destination IP/port: 198.76.28.11/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 14:55:05 TTL: 22s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes
Initiator:
Source IP/port: 10.0.0.2/227
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/2
Destination IP/port: 198.76.28.11/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -

Start time: 2021-11-22 14:54:53 TTL: 9s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 2

以前の情報に基づいて、送信元 IP アドレス 10.0.0.1 と 10.0.0.2 は、同じパブリックネットワークアドレス 198.76.28.11 に変換されます。 ただし、10.0.0.1 のポートは 12289 で、10.0.0.2 のポートは 12288 です。RTA が 198.76.28.11 宛ての応答パケットを受信すると、RTA はパケットを変換用に指定されたポートにより 10.0.0.1 と 10.0.0.2 のどちらに転送するかを区別します。 NAPT はこのメソッドを使用して、IP 層とトランスポート層でパケットを変換します。 これにより、パブリック IP アドレスの使用が大幅に改善されます。

手順 6:コンフィギュレーションを元に戻します

RTA の NAPT 設定を削除します。

NAT アドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられた NAT を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク 3:Easy IP の設定をする

プライベートネットワーククライアント Client_A および Client_B は、パブリックネットワークサーバーにアクセスする必要があります。 パブリックネットワークポートの IP アドレスを使用して、パブリックネットワークアドレスとポートを Client_A と Client_B に動的に割り当てます。

手順 1:テスト環境を構築する

テスト環境を構築します。 タスク 1 のステップ 1 と 2 を参照してください。

手順 2:接続性をチェックします

Client_A と Client_B でそれぞれサーバー(IP アドレス 198.76.29.4)に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順 3：East IP を設定します

RTA で Easy IP を設定します。

ACL を使用して、ネットワークセグメント 10.0.0.0/24 にある送信元アドレスでフローを定義します。

[RTA]acl basic 2000

[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

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

インターフェースビューで NAT アドレスを acl 2000 にバインドし、アドレスを提供します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat outbound 2000

[RTA-GigabitEthernet0/1]quit

手順 4：接続性をチェックします

Client_A と Client_B でそれぞれサーバー（IP アドレス 198.76.29.4）に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=7.000 ms

手順 5：NAT エントリーをチェックします

RTA で NAT エントリーをチェックします。

[RTA]display nat session verbose

Slot 0:

Initiator:

Source IP/port: 10.0.0.1/200

Destination IP/port: 198.76.29.4/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/5
Destination IP/port: 198.76.28.1/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 15:56:36 TTL: 15s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes
Initiator:
Source IP/port: 10.0.0.2/238
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/4
Destination IP/port: 198.76.28.1/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 15:56:30 TTL: 9s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 2

[RTA]display nat session

Slot 0:

Total sessions found: 0

[RTA]display nat session

Slot 0:

Initiator:

Source IP/port: 10.0.0.1/202

Destination IP/port: 198.76.29.4/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet0/0

Initiator:

Source IP/port: 10.0.0.2/239

Destination IP/port: 198.76.29.4/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet0/0

Total sessions found: 2

以前の情報に基づいて、10.0.0.1 および 10.0.0.2 にアドレス指定された送信元 IP は、RTA のアウトバウンドポートアドレス 198.76.28.1 に変換されました。

NAT 構成後、Client_A がサーバーに ping を実行できる場合、サーバーは Client_A に ping を実行できますか？ 出力情報は次のとおりです。

<Server>ping 10.0.0.1

Ping 10.0.0.1 (10.0.0.1): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

RTA には 10.0.0.0/24 へのルートがありません。 そのため、サーバーは Client_A に ping を実行できません。 サーバーの ICMP 応答パケットはサーバーアドレス 198.76.29.4 を送信元アドレスとして使用し、RTA アウトバウンドアドレス 198.76.28.1 を宛先アドレスとして使用するため、Client_A はサーバーに ping を実行できます。 Client_A の実際のソースアドレスは 10.0.0.1 で

す。 つまり、ICMP 接続は Client_A によって開始され、RTA がアドレスを変換してパケットを転送するようにトリガーする必要があります。 NAT は RTA アウトバウンドポート GigibitEthernet0/1 に対して有効であることに注意してください。 そのため、サーバーからクライアントに ping を実行するためにICMP パケットを送信しても、RTA をトリガーしてアドレスを変換することはできません。 サーバーで Client_A に ping を実行する方法を知るには、タスク 4 に進みます。

手順 6:コンフィギュレーションを元に戻します

RTA の Easy IP 設定を削除します。

NAT アドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられた NAT を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク 4:NAT Server の設定をする

Client_A は、ICMP サービスを外部に提供する必要があります。 Client_A を静的パブリックネットワークアドレス 198.76.28.11 および RTA のポートにマップします。

手順 1:接続性をチェックします

Client_A と Client_B でそれぞれサーバー(IP アドレス 198.76.29.4)に ping を実行します。 出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順 2:NAT Server を設定します

RTA に NAT Server を設定します。

[RTA]interface GigabitEthernet 0/1

アウトバウンドポートのプライベートネットワークサーバーアドレスとパブリックネットワークアドレスに 1 対 1 の NAT マッピングを実装します。

[RTA-GigabitEthernet0/1]nat server protocol icmp global 198.76.28.11 inside 10.0.0.1

[RTA-GigabitEthernet0/1]quit

手順 3：接続性をチェックします

サーバーから Client_A ネットワークアドレス 198.76.28.11 に ping を実行します。

サーバーは Client_A に ping を実行できます。

<Server>ping 198.76.28.11

Ping 198.76.28.11 (198.76.28.11): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.28.11: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 198.76.28.11: icmp_seq=1 ttl=253 time=8.000 ms

56 bytes from 198.76.28.11: icmp_seq=2 ttl=253 time=8.000 ms

56 bytes from 198.76.28.11: icmp_seq=3 ttl=253 time=5.000 ms

56 bytes from 198.76.28.11: icmp_seq=4 ttl=253 time=7.000 ms

手順 4：NAT エントリーをチェックします

RTA で NAT Server エントリーをチェックします。

[RTA]dis nat session verbose

Slot 0:

Initiator:

  Source IP/port: 198.76.29.4/191

  Destination IP/port: 198.76.28.11/2048

  DS-Lite tunnel peer: -

  VPN instance/VLAN ID/Inline ID: -/-/-

  Protocol: ICMP(1)

  Inbound interface: GigabitEthernet0/1

Responder:

  Source IP/port: 10.0.0.1/191

  Destination IP/port: 198.76.29.4/0

  DS-Lite tunnel peer: -

  VPN instance/VLAN ID/Inline ID: -/-/-

  Protocol: ICMP(1)

  Inbound interface: GigabitEthernet0/0

State: ICMP_REPLY

Application: OTHER

Role: -

Failover group ID: -

Start time: 2021-11-22 16:45:42 TTL: 22s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

手順 5:コンフィギュレーションを元に戻します

RTA で NAT Server 設定を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat server protocol icmp global 198.76.28.11

NAT アドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられた NAT を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

NAT サーバーは、プライベートネットワークサーバーにアクセスするためのパブリックネットワーククライアントの要件を満たす必要があります。 NAT サーバーは、パブリックネットワーククライアントがアクセスするプライベートネットワークアドレス/ポートをマップします。 実際のアプリケーションでは、プライベートネットワーク内の Web サーバーまたは FTP サーバーがパブリックネットワークの顧客にサービスを提供する必要がある場合、NAT サーバーを使用してパブリックネットワークアドレスをプライベートネットワークサーバーにマップできます。 Client_A がサーバーに ping を実行した場合、ping は正常に実行できますか？ Client_B がサーバーに ping を実行した場合も、ping は正常に実行できますか？

RTA の NAT サーバー構成コマンドに基づいて、Client_A が FTP サーバーの場合、FTP サービスを外部に提供できますか？ 答えはイエスです。 NAT サーバー構成を変更します。 NAT サーバーの構成は次のとおりです。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat server protocol tcp global 198.76.28.11 ftp inside 10.0.0.1 ftp

[RTA-GigabitEthernet0/1]quit

質問:

1. このテストでは、パブリックネットワークアドレスプールにパブリックネットワークポートアドレスが含まれています。 別のアドレスセグメントが追加された場合、RTB をどのように構成する必要がありますか？

答え:

RTB のパブリックネットワークアドレスプール宛ての静的ルートを追加します。

2. nat server コマンドの global-address はインターネットアドレスである必要がありますか？

答え:
いいえ、実際には、グローバルアドレスは内部アドレスを基準にしています。 nat server コマンドを実行して構成されたポートは、グローバルネットワークに接続されます。