FutureNet NXR シリーズ

NAT,フィルタ設定例集

Ver 1.0.0

センチュリー・システムズ株式会社

目次

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- 本書に記載されている会社名，製品名は、各社の商標および登録商標です。
- 本ガイドは、以下の FutureNet NXR 製品に対応しております。
  - NXR-120/C, NXR-125/CX, NXR-130/C, NXR-155/C-WM, NXR-1200
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet NXR-120/C の以下のバージョンをベースに作成しております。
  FutureNet NXR シリーズ NXR-120/C Ver5.11.0（一部例のみ NXR-130/C Ver5.11.0）
  各種機能において、ご使用されている製品およびファームウェアのバージョンによっては一部機能，コマンドおよび設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に適宜読みかえてご参照および設定を行って下さい。
- 本バージョンでは IPv4 のみを対象とし、IPv6 の設定に関しては本バージョンでは記載しておりません。
- 設定した内容の復帰（流し込み）を行う場合は、CLI では「copy」コマンド，GUI では設定の復帰を行う必要があります。
- モバイル通信端末をご利用頂く場合で契約内容が従量制またはそれに準ずる場合、大量のデータ通信を行うと利用料が高額になりますので、ご注意下さい。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。

改版履歴

Version	更新内容
1.0.0	初版

NXR シリーズの NAT・フィルタ機能

■ フィルタリング機能

・ 静的フィルタ

NXR シリーズではアクセスリストによる条件定義によりパケットのフィルタリングを行います。アクセスリストは作成しただけではフィルタとして動作しません。そのためインタフェースの入力（in），転送（forward-in,forward-out），出力（out）に対して適用することによりフィルタとして動作し、パケットの制御を行います。

IP アクセスリストによるフィルタリング時に設定可能なマッチ条件とマッチ時の動作に関しては下記の通りです。

〇マッチ条件

- 送信元 IP アドレス，ネットマスク指定
- 宛先 IP アドレス，ネットマスク指定
- プロトコル指定(既知のプロトコル名指定と任意のプロトコル番号入力)
- 送信元ポート指定（TCP,UDP のみ、範囲指定可）
- 宛先ポート指定（TCP,UDP のみ、範囲指定可）
- ICMP タイプ/コード指定（ICMP 指定時のみ）
- 送信元 MAC アドレス指定

〇マッチ時の動作

- permit　許可されたパケットとして判断されます。
- deny　　許可されていないパケットとして破棄されます。

(☞) なお NXR シリーズではフィルタでアクセスリストを利用する場合、アクセスリスト作成時の暗黙ルールとしてアクセスリストの最後尾に全て許可のルールが設定されます。

・動的フィルタ（ステートフルパケットインスペクション）

ステートフルパケットインスペクション機能はパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより例えば自動的に WAN からの不要なアクセスを制御することが可能で、簡単な設定でより高度な安全性を保つことができます。

またステートフルパケットインスペクション機能を有効にすると、そのインタフェースへのアクセスは原則不可となります。(静的フィルタ設定やセッション情報がある場合は除く)

よって DNAT 機能を利用して LAN 内にあるサーバを外部に公開するような場合は、静的フィルタ設定を行い外部から指定したサービスにアクセスできるように設定しておく必要があります。

・IP フィルタの優先順位

入力(in)/転送(forward-in, forward-out)/出力(out)時にフィルタリングが適用される順番は以下のとおりです。なお IPsec インプット/アウトプットポリシチェック(Policy Based IPsec のパケットのみが対象)は、実際に SPD(Security Policy Database)を検索するわけではなく、ESP 化されてきたパケット/ESP 化するべきパケットの判断のみを行い、この判定にマッチしたパケットが許可されます。

○ 入力

(1) システムフィルタ
- Invalid status drop
- TCP コネクション数制限

(2) IPsec インプットポリシチェック
IPsec ESP(Policy Based)化されてきたものは許可します。

(3) 入力(in)フィルタ

(4) ステートフルパケットインスペクション

(5) サービス用フィルタ(Web 設定画面アクセス用フィルタなど)

○ 転送

(1) システムフィルタ
- Invalid status drop
- Session limit

(2) IPsec インプット/アウトプットポリシチェック
IPsec ESP(Policy Based)化されてきたものか、アウトバウンドポリシにマッチするものは許可します。

(3) UPNP フィルタリング

(4) 転送(forward-in, forward-out)フィルタ

(5) ステートフルパケットインスペクションチェック(入力/転送時のみ)

(6) WEB 認証用転送(webauth-filter forward-in, forward-out)フィルタ

○ 出力

(1) IPsec アウトプットポリシチェック
IPsec アウトバウンドポリシ(Policy Based)にマッチするものは許可します。

(2) 出力(out)フィルタ

■ NAT 機能

・ IP マスカレード機能

インタフェースよりパケットを出力する際にパケットの送信元 IP アドレスや TCP/UDP ポート番号をパケットを出力するインタフェースの IP アドレス, TCP/UDP ポート番号に自動的に変換してパケットを送信する機能です。

これにより複数のプライベート IP アドレスをある１つのグローバル IP アドレスに変換するといったことが可能となるため､グローバル IP アドレスを１つしか保有していなくても複数のコンピュータからインターネットにアクセスすることができるようになります。

・ 送信元 NAT(SNAT)機能

IP パケットの送信元 IP アドレスや TCP/UDP ポート番号を変換する機能です。
IP マスカレード機能とは異なり､例えばプライベート IP アドレスをどのグローバル IP アドレスに変換するかをそれぞれ設定できるのが送信元 NAT 機能です。
〈例〉
プライベート IP アドレスＡ　　…〉 グローバル IP アドレスＸ
プライベート IP アドレスＢ　　…〉 グローバル IP アドレスＹ
プライベート IP アドレスＣ～ Ｆ …〉 グローバル IP アドレスＺ
よって例えば IP マスカレード機能を設定せずに送信元 NAT 機能だけを設定した場合は､送信元 NAT 機能で設定された IP アドレスを持つコンピュータ以外はインターネットにアクセスできません。

・ 宛先 NAT(DNAT)機能

IP パケットの宛先 IP アドレスおよび TCP/UDP ポート番号を変換する機能です。
例えば通常はインターネット側からプライベート LAN へアクセスする事はできませんが、宛先グローバル IP アドレスをプライベート IP アドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスしているかのように見せることができます。

・NAT の優先順位

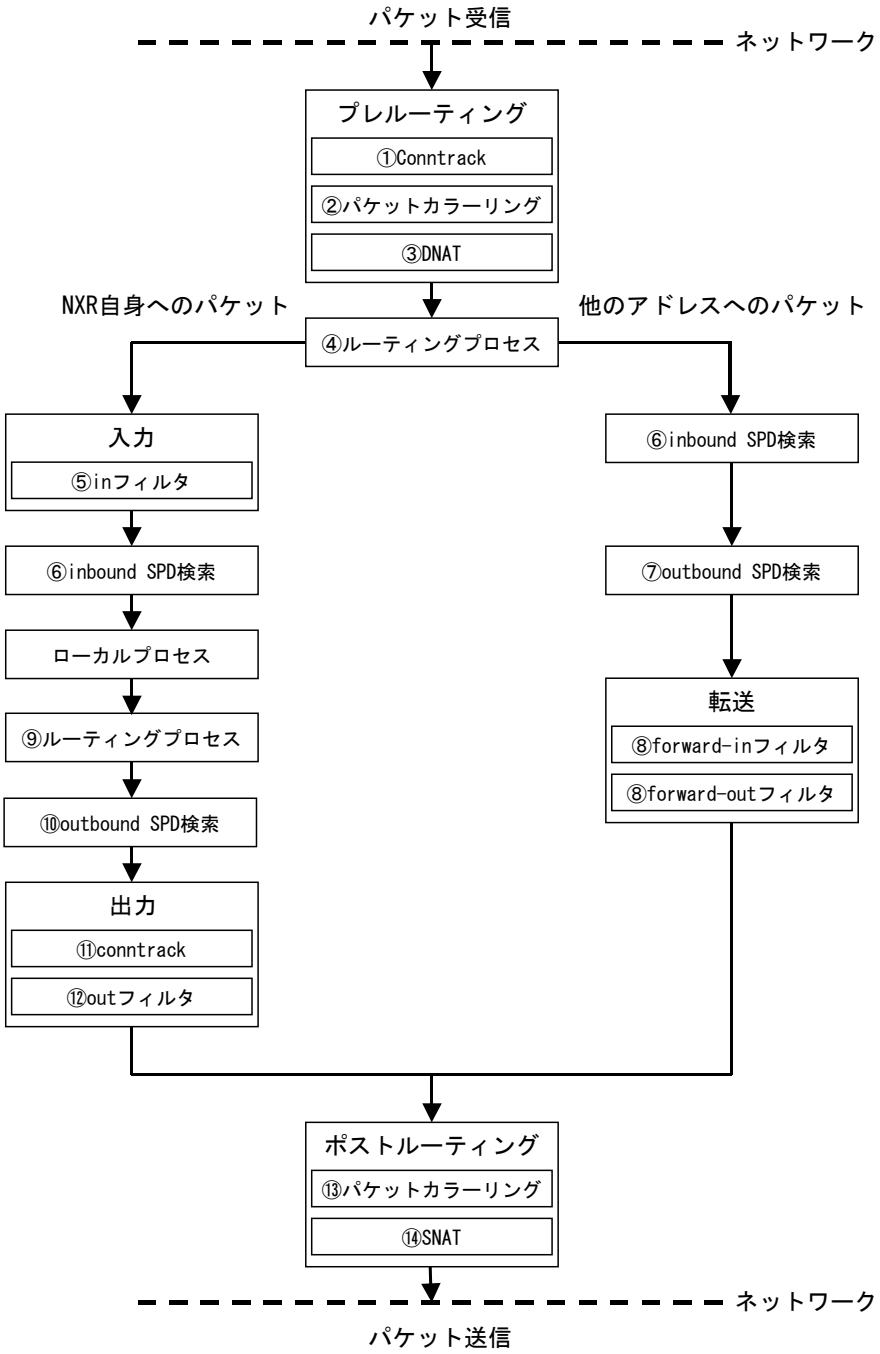
NAT の適用順位は以下のとおりです。

○ 入力(プレルーティング)
(1) システム DNAT
(2) UPNP 用 DNAT
(3) ユーザ設定用宛先 NAT(DNAT)

○ 出力(ポストルーティング)
(1) システム SNAT
(2) IPsec ポリシにマッチしたパケットは、以下の NAT は未適用となります。
(3) ユーザ設定用送信元 NAT(SNAT)
(4) IPv4 マスカレード

■ NXR パケットトラベリング

NXR がパケットを受信してから送信するまでに適用される NAT, フィルタおよびパケットカラーリングの順番は以下のとおりです。



○ パケット転送時

- パケット受信 -

① Conntrack

セッション情報の作成および参照を行います。この際 session コマンド(global node)で設定された内容に基づいてチェックが行われます。

② パケットカラーリング(入力)

③ 宛先 NAT(DNAT)

詳細は NAT の優先順位(入力)をご参照ください。

④ ルーティングプロセス

⑥ IPsec inbound SPD(※1)検索

ESP 化されてきたパケットはここでポリシチェックが行われます。ESP 化すべきパケットがプレーンテキストで送信されてきた場合は破棄されます。但し ipsec policy-ignore input が有効な場合は、ここでのチェックは行われません。

⑦ IPsec outbound SPD(※1)検索

ipsec policy-ignore output が設定されている場合は、ポリシ検索は行われません。

⑧ パケットフィルタリング

詳細は、IP フィルタの優先順位(転送)をご参照ください。

⑬ パケットカラーリング(出力)

⑭ 送信元 NAT(SNAT)

詳細は NAT の優先順位(出力)を参照してください。

- パケット送信 -

○ パケット受信時(NXR が宛先)

- パケット受信 -

① Conntrack

セッション情報の作成および参照を行います。この際 session コマンド(global node)で設定された内容に基づいてチェックが行われます。

② パケットカラーリング(入力)

③ 宛先 NAT(DNAT)

詳細は NAT の優先順位(入力)をご参照ください。

④ ルーティングプロセス

⑤ パケットフィルタリング

詳細は、IP フィルタの優先順位(入力)をご参照ください。

⑥ IPsec inbound SPD(※1)検索

ESP 化されてきたパケットはここでポリシチェックが行われます。ESP 化すべきパケットがプレーンテキストで送信されてきた場合は破棄されます。但し ipsec policy-ignore input が有効な場合は、ここでのチェックは行われません。

-->ESP パケットの場合、認証/復号処理後、①へ戻ります。

--> NXR ローカルプロセス

○ パケット送信時(NXR が送信元)

- NXR ローカルプロセスがパケットを送出 -

⑨ ルーティングプロセス

⑩ IPsec outbound SPD(※1)検索

⑪ Conntrack

セッション情報の作成および参照を行います。この際 session コマンド(global node)で設定された内容に基づいてチェックが行われます。

⑫ パケットフィルタリング(出力)

詳細は、IP フィルタの優先順位(出力)をご参照ください。

⑬ パケットカラーリング(出力)

⑭ 送信元 NAT(SNAT)

詳細は NAT の優先順位(出力)をご参照ください。

SNAT される場合この後で再度 IPsec outbound SPD 検索が行われます。但し ipsec policy-ignore output が設定されている場合は、ポリシ検索は行われません。ポリシにマッチしたパケットは暗号化処理を行い、パケットフィルタリング(出力) --> ポストルーティングを通過し、ESP パケットが出力されます。

- パケット送信 -

(注 1)

IPsec を使用するにあたって、どのようなパケットに対してどのようなアクション{discard(パケット廃棄する)、bypass(IPsec 処理を行わない)、apply(IPsec を適用する)}を行うかを定めたルールが SP (Security Policy)で、SP を格納するデータベースが SPD(Security Policy Database)です。

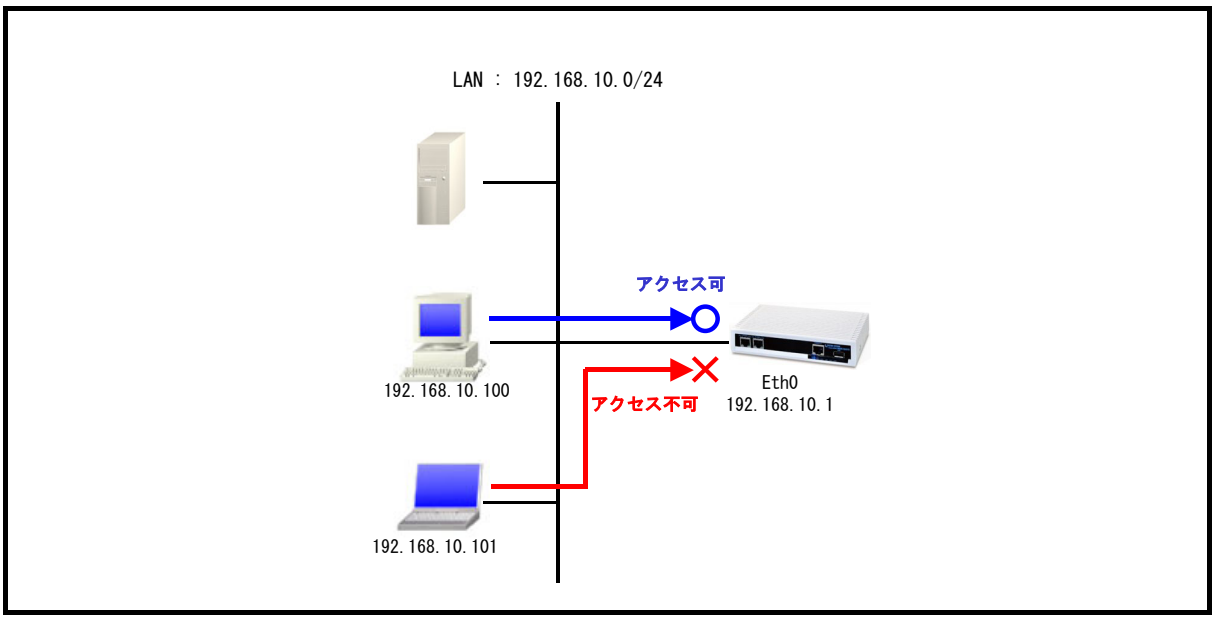
SPD には inbound SPD と outbound SPD があります。受信パケットのポリシチェックには、inbound SPD が検索されます。送信パケットのポリシチェックには、outbound SPD が検索されます。

1. フィルタ設定

1-1. 入力（in）フィルタ設定

入力フィルタではNXR宛に送信されたパケットのうち､NXR自身で受信し処理するものを対象とします。ここではLAN内で特定のIPアドレスからルータへのTELNETアクセスは許可するが､それ以外のIPアドレスからのTELNETアクセスは破棄する設定です。

【 構成図 】



- 入力(in)フィルタでは外部からNXR自身に入ってくるパケットを制御します。インターネットやLANからNXRへのアクセスについて制御したい場合には、この入力フィルタ（inフィルタ）を設定します。
- この例では送信元IPアドレス192.168.10.100,宛先IPアドレス192.168.10.1へのTELNETアクセスは許可するが、その他のIPアドレスから宛先IPアドレス192.168.10.1へのTELNETアクセスは破棄するeth0_inというIPアクセスリストを作成します。
- 作成したIPアクセスリスト名eth0_inをEthernet0インタフェースのinフィルタに適用します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#ip access-list eth0_in permit 192.168.10.100 192.168.10.1 tcp any 23
nxr120(config)#ip access-list eth0_in deny any 192.168.10.1 tcp any 23
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#ip access-group in eth0_in
nxr120(config-if)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list eth0_in permit 192.168.10.100 192.168.10.1 tcp any 23
nxr120(config)#ip access-list eth0_in deny any 192.168.10.1 tcp any 23
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を eth0_in とします。

一行目の設定は送信元 IP アドレス 192.168.10.100 宛先 IP アドレス 192.168.10.1 宛先 TCP ポート番号 23 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 192.168.10.1 宛先 TCP ポート番号 23 のパケットを破棄するための設定です。

これが送信元 IP アドレス 192.168.10.100 以外からの NXR への TELNET アクセスを破棄するルールとなります。

この IP アクセスリスト設定は Ethernet0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

2. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

```
nxr120(config-if)#ip access-group in eth0_in
```

IP アクセスリスト設定で設定した eth0_in を in フィルタに適用します。これにより Ethernet0 インタフェースで受信した NXR 自身宛のパケットに対して IP アクセスリストによるチェックが行われ Ethernet0 インタフェースでは送信元 IP アドレス 192.168.10.100 以外からの NXR への TELNET アクセスを破棄するようになります。

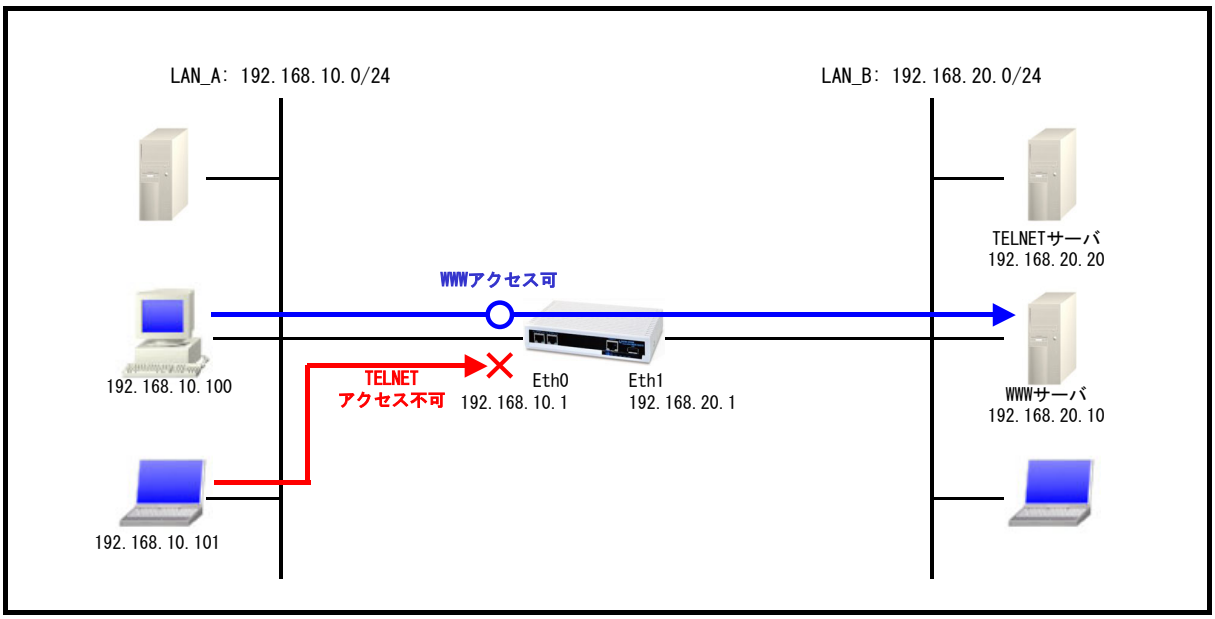
【 パソコンの設定例 】

	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0

1-2. 転送（forward-in,forward-out）フィルタ設定

転送フィルタでは NXR で内部転送（NXR がルーティング）するパケットを制御するときに利用します。ここでは LAN_B に設置されている WWW サーバ，TELNET サーバに対して WWW サーバへのアクセスは許可するが、TELNET サーバへのアクセスは破棄する設定です。

【 構成図 】



- 転送フィルタ(forward-in,forward-out)ではLAN からインターネットへのアクセスやインターネットから LAN 内サーバへのアクセス、LAN から LAN へのアクセスなど NXR で内部転送する(NXR がルーティングする)パケットを制御します。
- この例では宛先 IP アドレス 192.168.20.10 TCP ポート番号 80（HTTP）へのアクセスは許可し、宛先 IP アドレス 192.168.20.20 TCP ポート番号 23（TELNET）へのアクセスは破棄する eth0_forward-in という IP アクセスリストを作成します。
- 作成した IP アクセスリスト名 eth0_forward-in を Ethernet0 インタフェースの forward-in フィルタに適用します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#ip access-list eth0_forward-in permit any 192.168.20.10 tcp any 80
nxr120(config)#ip access-list eth0_forward-in deny any 192.168.20.20 tcp any 23
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#ip access-group forward-in eth0_forward-in
nxr120(config-if)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 192.168.20.1/24
nxr120(config-if)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜IPアクセスリスト設定＞

```
nxr120(config)#ip access-list eth0_forward-in permit any 192.168.20.10 tcp any 80
nxr120(config)#ip access-list eth0_forward-in deny any 192.168.20.20 tcp any 23
```

フィルタの動作を規定するルールリストを作成します。

ここではIPアクセスリスト名をeth0_forward-inとします。

一行目の設定は宛先IPアドレス192.168.20.10 宛先TCPポート番号80のパケットを許可するための設定です。

二行目の設定は宛先IPアドレス192.168.20.20 宛先TCPポート番号23のパケットを破棄するための設定です。

このIPアクセスリスト設定は、Ethernet0インタフェース設定で登録します。

(☞) IPアクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

2. ＜Ethernet0インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0インタフェースのIPアドレスに192.168.10.1/24を設定します。

```
nxr120(config-if)#ip access-group forward-in eth0_forward-in
```

IPアクセスリスト設定で設定したeth0_forward-inをforward-inフィルタに適用します。これによりEthernet0インタフェースで受信したNXRで内部転送する(NXRがルーティングする)パケットに対してIPアクセスリストによるチェックが行われます。

3. ＜Ethernet1インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 192.168.20.1/24
```

Ethernet1インタフェースのIPアドレスに192.168.20.1/24を設定します。

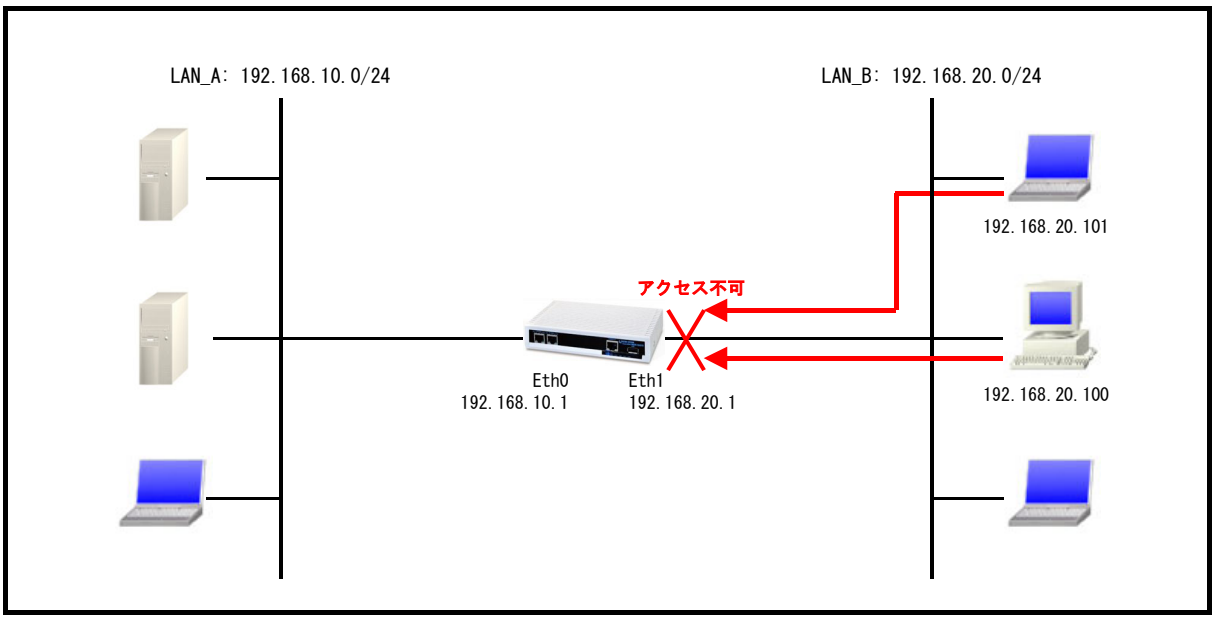
【 サーバ,パソコンの設定例 】

	LAN Aの パソコン	LAN Bの WWWサーバ	LAN Bの TELNETサーバ	LAN Bの パソコン
IPアドレス	192.168.10.100	192.168.20.10	192.168.20.20	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.20.1	192.168.20.1

1-3. 動的フィルタ（ステートフルパケットインスペクション）設定

ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリングともいわれる機能です。ここではEthernet1インタフェース側からの接続要求を全て遮断する設定です。

【 構成図 】



・ Ethernet1インタフェースで動的フィルタ（ステートフルパケットインスペクション）を有効にし、Ethernet1インタフェース側からの接続要求を遮断します。
ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより例えば自動的にWANからの不要なアクセスを制御することが可能です。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 192.168.20.1/24
nxr120(config-if)#ip spi-filter
nxr120(config-if)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 192.168.20.1/24
```

Ethernet1 インタフェースの IP アドレスに 192.168.20.1/24 を設定します。

```
nxr120(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

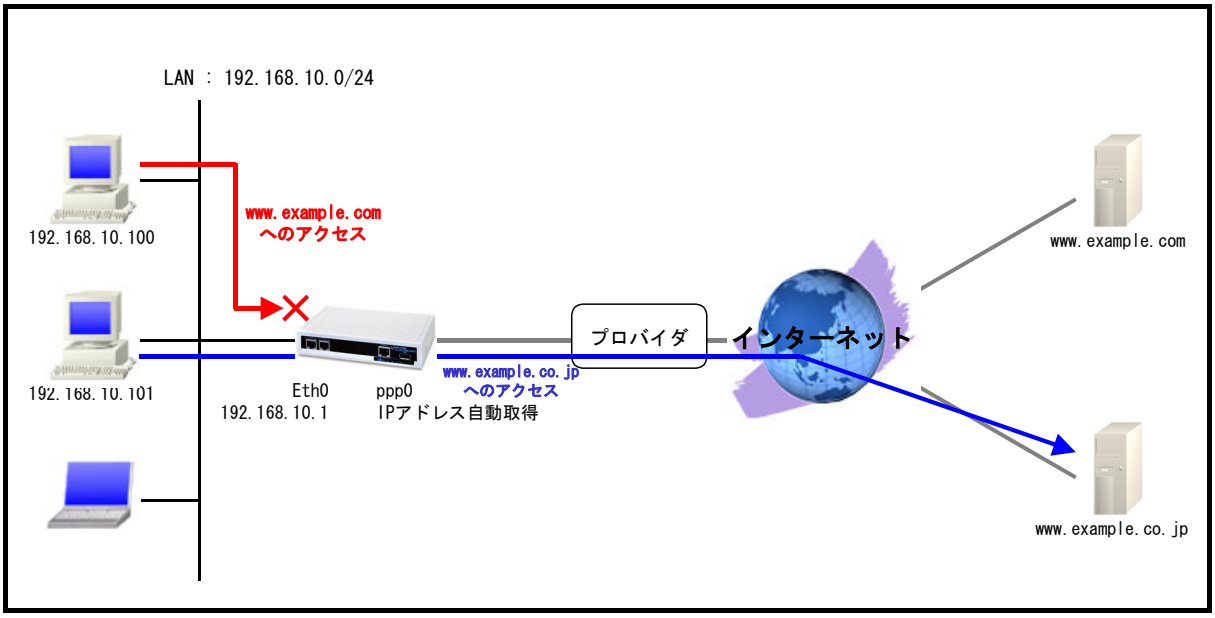
【 パソコンの設定例 】

	パソコン
IP アドレス	192.168.20.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.20.1

1-4. FQDN フィルタ設定

IP アクセスリスト設定では送信元 IP アドレス,宛先 IP アドレスを FQDN 形式で設定することが可能です。これにより指定した FQDN に対応する IP アドレスが複数ある場合でも、その IP アドレスを一つ一つアクセスリストに設定する必要はなく、対応する FQDN を指定するだけでフィルタすることが可能です。
ここでは www.example.com の TCP ポート 80 番宛のアクセスを制限する設定例になります。

【 構成図 】



- IP アクセスリスト設定で宛先 FQDN として www.example.com, 宛先 TCP ポート番号 80 を破棄する設定をします。
- ppp0 インタフェースで IP マスカレードを有効にし、NXR 配下の複数の端末がインターネットアクセスできるように、送信元 IP アドレスおよびポート番号を変換します。
- DNS 機能を有効にし、IP アクセスリスト設定で指定した FQDN の名前解決ができるようにすること、および NXR 配下の端末からの DNS リクエストを中継できるようにします。
- ppp0 インタフェースで動的フィルタ（ステートフルパケットインスペクション）を有効にし、ppp0 インタフェース側からの接続要求を遮断します。
  ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
  該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
  これにより自動的に WAN からの不要なアクセスを制御することが可能です。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#ip access-list ppp0_forward-out deny any www.example.com tcp any 80
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address negotiated
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-out ppp0_forward-out
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合は、ゲートウェイとして ppp インタフェースを指定します。

3. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-out deny any www.example.com tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_forward-out とします。

宛先 FQDN www.example.com 宛先 TCP ポート番号 80 のパケットを破棄するように設定します。

この IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行ういインタフェースでの登録が必要になります。

4. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr120(config-ppp)#ip address negotiated
```
IP アドレスを negotiated（自動取得）に設定します。

```
nxr120(config-ppp)#ip masquerade
```
IP マスカレードを設定します。

```
nxr120(config-ppp)#ip access-group forward-out ppp0_forward-out
```
IP アクセスリスト設定で設定した ppp0_forward-out を forward-out フィルタに適用します。これにより NXR を経由して ppp0 インタフェースから送信されるパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr120(config-ppp)#ip spi-filter
```
ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-ppp)#ip tcp adjust-mss auto
```
TCP MSS の調整機能をオートに設定します。
TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr120(config-ppp)#no ip redirects
```
ICMP リダイレクト機能を無効に設定します。

```
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```
PPPoE 接続で使用するユーザ ID とパスワードを設定します。
ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

5. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
```
Ethernet1 インタフェースを設定します。

```
nxr120(config-if)#no ip address
```
Ethernet1 インタフェースに IP アドレスを割り当てない設定をします。
PPPoE 接続でプロバイダ等から割り当てられる IP アドレスは Ethernet インタフェースではなく ppp インタフェースに割り当てられますので、PPPoE のみで使用する場合は IP アドレスの設定は不要です。

```
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェース上で ppp0 インタフェースを使用するための設定をします。

PPPoE で ppp インタフェースを使用する場合は、pppoe-client コマンドによるインタフェース設定での登録が必要になります。

6. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

【 パソコンの設定例 】

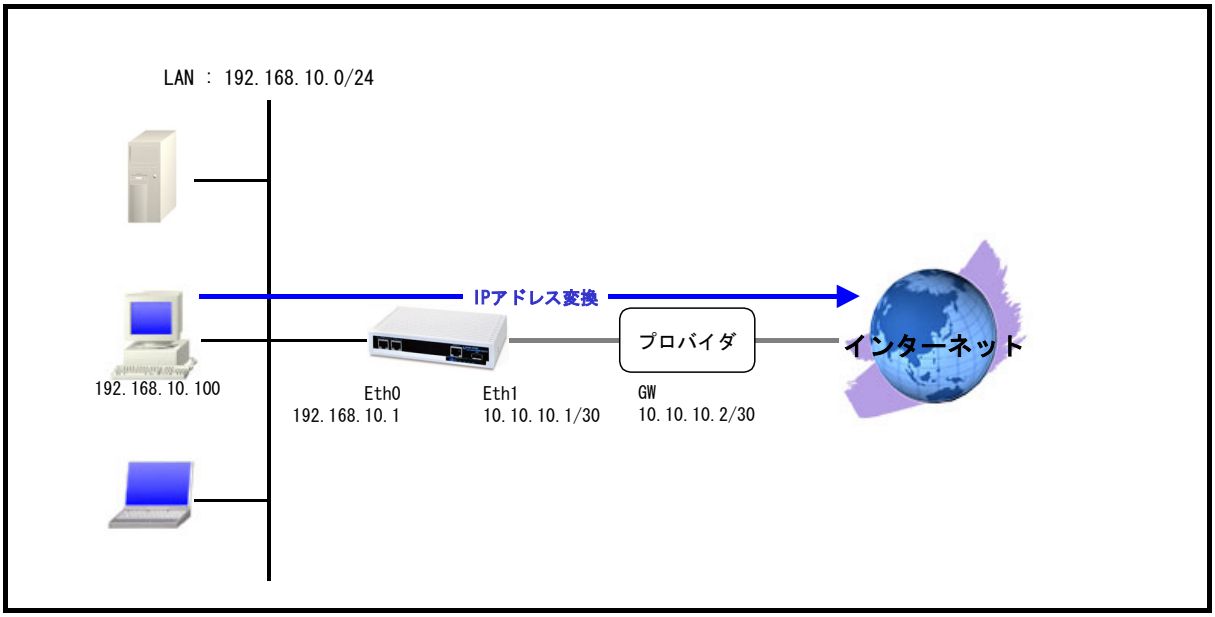
	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1

2. NAT 設定

2-1. IP マスカレード設定

送信元 IP アドレスを IP マスカレードの設定を有効にしたインタフェースの IP アドレスに変換します。

【 構成図 】



- Ethernet0 インタフェースを LAN 側，Ethernet1 インタフェースを WAN 側とします。
- Ethernet1 インタフェースで IP マスカレードを有効にし Ethernet1 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。
- この設定例では Ethernet1 インタフェースでステートフルパケットインスペクションを有効にしています。
- この設定例では DNS サービスを有効にし、ルート DNS サーバ設定を有効にします。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 10.10.10.2
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/30
nxr120(config-if)#ip masquerade
nxr120(config-if)#ip spi-filter
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#root enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 10.10.10.2
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

3. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/30
```

Ethernet1 インタフェースの IP アドレスに 10.10.10.1/30 を設定します。

```
nxr120(config-if)#ip masquerade
```

IP マスカレードを設定します。

これにより Ethernet1 インタフェースからパケットが送信される際に送信元 IP アドレスを Ethernet1 インタフェースの IP アドレスに変換します。

```
nxr120(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

4. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

```
nxr120(config-dns)#root enable
```

この設定例ではルート DNS サーバを利用するため、ルート DNS サーバを有効に設定します。

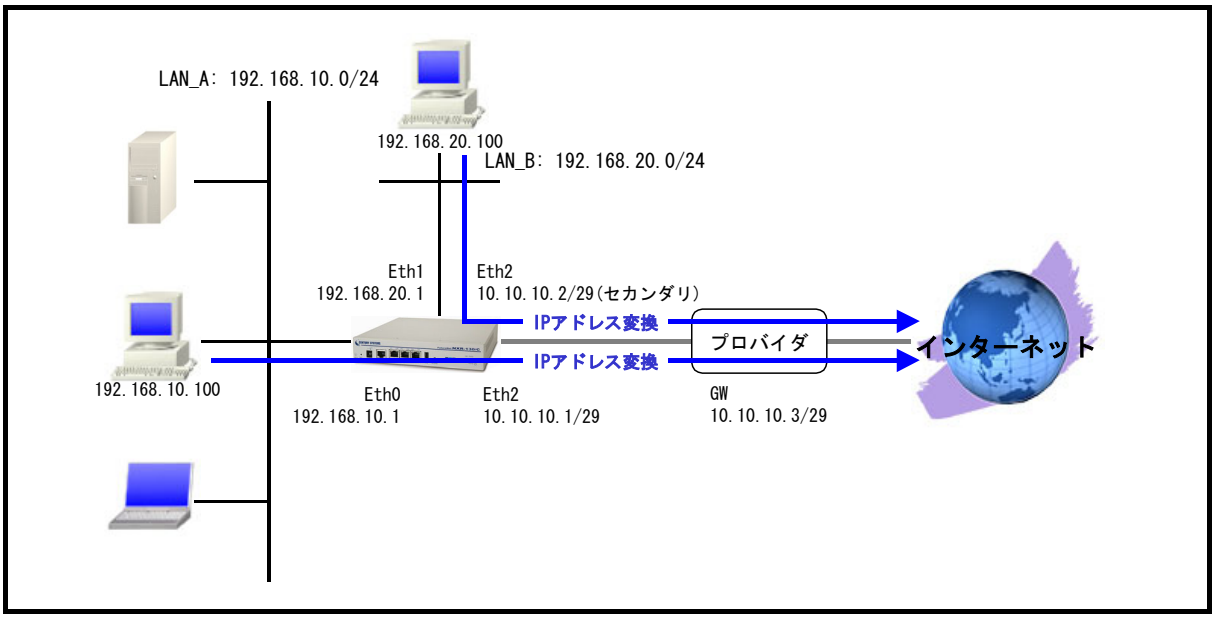
【 パソコンの設定例 】

	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1

2-2. 送信元 NAT（SNAT）設定

送信元 NAT（SNAT）設定では、ある特定のネットワークやホストを指定し送信元 IP アドレスの変換を行うことができます。例えばセグメント毎に異なるグローバル IP アドレスを利用する際に使用します。

【 構成図 】



- Ethernet0，1 インタフェースを LAN 側，Ethernet2 インタフェースを WAN 側とします。
- Ethernet0，1 インタフェースが属するネットワークからのパケットで Ethernet2 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。
  その際 192.168.10.0/24 のネットワークから送信されたパケットは送信元 IP アドレスを 10.10.10.1 に、192.168.20.0/24 のネットワークから送信されたパケットは送信元 IP アドレスを 10.10.10.2 に変換します。
- この設定例では Ethernet2 インタフェースでステートフルパケットインスペクションを有効にしています。
- この設定例では DNS サービスを有効にし、ルート DNS サーバ設定を有効にしています。

【 設定例 】

```
nxr130#configure terminal
nxr130(config)#interface ethernet 0
nxr130(config-if)#ip address 192.168.10.1/24
nxr130(config-if)#exit
nxr130(config)#interface ethernet 1
nxr130(config-if)#ip address 192.168.20.1/24
nxr130(config-if)#exit
nxr130(config)#ip route 0.0.0.0/0 10.10.10.3
nxr130(config)#ip snat eth2_snat ip 192.168.10.0/24 any 10.10.10.1
nxr130(config)#ip snat eth2_snat ip 192.168.20.0/24 any 10.10.10.2
nxr130(config)#interface ethernet 2
nxr130(config-if)#ip address 10.10.10.1/29
nxr130(config-if)#ip address 10.10.10.2/29 secondary
nxr130(config-if)#ip snat-group eth2_snat
nxr130(config-if)#ip spi-filter
nxr130(config-if)#exit
nxr130(config)#dns
nxr130(config-dns)#service enable
nxr130(config-dns)#root enable
nxr130(config-dns)#exit
nxr130(config)#exit
nxr130#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr130(config)#interface ethernet 0
nxr130(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜Ethernet1 インタフェース設定＞

```
nxr130(config)#interface ethernet 1
nxr130(config-if)#ip address 192.168.20.1/24
```

Ethernet1 インタフェースの IP アドレスに 192.168.20.1/24 を設定します。

3. ＜スタティックルート設定＞

```
nxr130(config)#ip route 0.0.0.0/0 10.10.10.3
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. ＜SNAT 設定＞

```
nxr130(config)#ip snat eth2_snat ip 192.168.10.0/24 any 10.10.10.1
nxr130(config)#ip snat eth2_snat ip 192.168.20.0/24 any 10.10.10.2
```

SNAT の動作ルールを作成します。

ここでは SNAT ルール名を eth2_snat とします。

一行目の設定は送信元 IP アドレス 192.168.10.0/24 のパケットの送信元 IP アドレスを 10.10.10.1 に変換するための設定です。

二行目の設定は送信元 IP アドレス 192.168.20.0/24 のパケットの送信元 IP アドレスを 10.10.10.2 に変換するための設定です。

この SNAT 設定は、Ethernet2 インタフェース設定で登録します。

(☞) SNAT 設定を設定しただけでは送信元 IP アドレスの変換機能は動作しません。送信元 IP アドレスの変換を行うインタフェースでの登録が必要になります。

5. ＜Ethernet2 インタフェース設定＞

```
nxr130(config)#interface ethernet 2
nxr130(config-if)#ip address 10.10.10.1/29
```

Ethernet2 インタフェースの IP アドレスに 10.10.10.1/29 を設定します。

```
nxr130(config-if)#ip address 10.10.10.2/29 secondary
```

Ethernet2 インタフェースのセカンダリ IP アドレスとして 10.10.10.2/29 を設定します。

```
nxr130(config-if)#ip snat-group eth2_snat
```

SNAT 設定で設定した eth2_snat を適用します。これにより Ethernet2 インタフェースで SNAT 設定で設定した IP アドレス変換が行われます。

```
nxr130(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

6. ＜DNS 設定＞

```
nxr130(config)#dns
nxr130(config-dns)#service enable
```

DNS サービスを有効に設定します。

```
nxr130(config-dns)#root enable
```

この設定例ではルート DNS サーバを利用するため、ルート DNS サーバを有効に設定します。

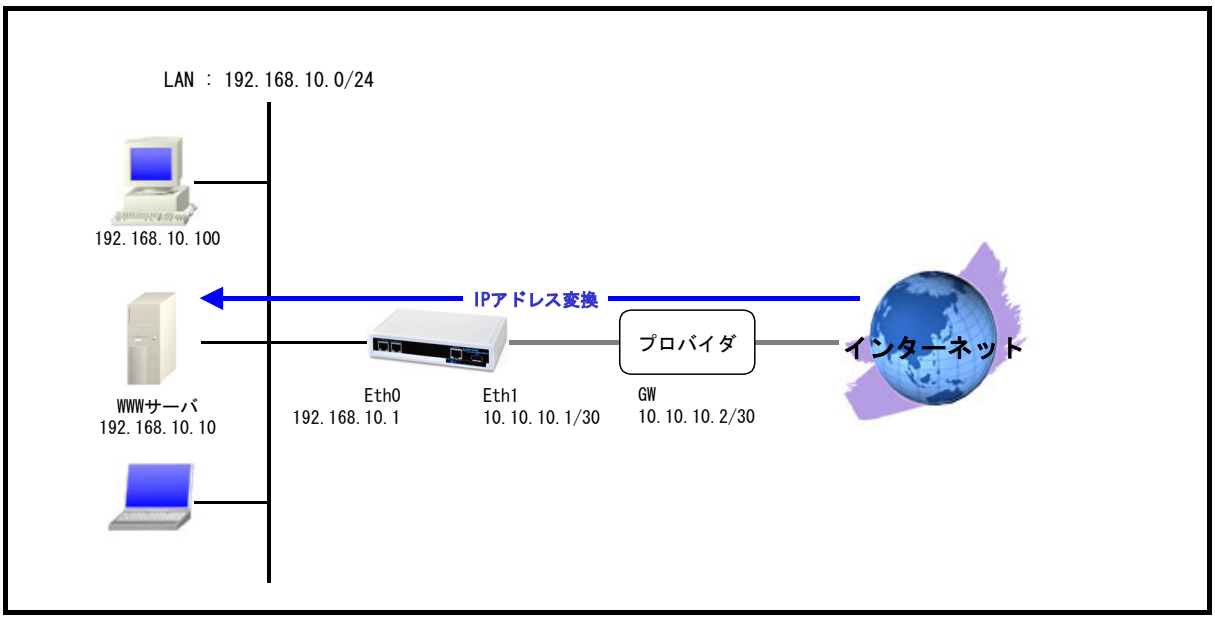
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバの IP アドレス	192.168.10.1	192.168.20.1

2-3. 宛先 NAT（DNAT）設定

プライベート IP アドレスのネットワーク内にあるサーバをインターネット経由でアクセスさせる場合、宛先 NAT（DNAT）を設定することにより NXR 経由でのアクセスが可能になります。
この設定例は WWW サーバを DNAT 設定を利用して外部に公開する設定です。

【 構成図 】



- Ethernet0 インタフェースを LAN 側，Ethernet1 インタフェースを WAN 側とします。
- Ethernet1 インタフェースで宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットを受信した場合は、宛先 IP アドレスを 192.168.10.10 に変換します。
- この設定例では Ethernet1 インタフェースでステートフルパケットインスペクションを有効にしています。そのため Ethernet1 インタフェースで宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 へのアクセスを許可するフィルタを設定します。
- この設定例では DNS サービスを有効にし、ルート DNS サーバ設定を有効にしています。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 10.10.10.2
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/30
nxr120(config-if)#ip dnat-group eth1_dnat
nxr120(config-if)#ip masquerade
nxr120(config-if)#ip access-group forward-in eth1_forward-in
nxr120(config-if)#ip spi-filter
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#root enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 10.10.10.2
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

3. ＜DNAT 設定＞

```
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を eth1_dnat とします。

宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定をします。

この DNAT 設定は、Ethernet1 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレスの変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を eth1_forward-in とします。

宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するように設定します。

このIPアクセスリスト設定は、Ethernet1インタフェース設定で登録します。

(☞) IPアクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜Ethernet1インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/30
```

Ethernet1インタフェースのIPアドレスに10.10.10.1/30を設定します。

```
nxr120(config-if)#ip dnat-group eth1_dnat
```

DNAT設定で設定したeth1_dnatを適用します。これによりEthernet1インタフェースでDNAT設定で設定したIPアドレス変換が行われます。

```
nxr120(config-if)#ip masquerade
```

IPマスカレードを設定します。

```
nxr120(config-if)#ip access-group forward-in eth1_forward-in
```

IPアクセスリスト設定で設定したeth1_forward-inをforward-inフィルタに適用します。これによりEthernet1インタフェースで受信したNXRを経由するパケットに対してIPアクセスリストによるチェックが行われます。

```
nxr120(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的にWANからの不要なアクセスを制御することが可能です。

6. ＜DNS設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNSサービスを有効に設定します。

```
nxr120(config-dns)#root enable
```

この設定例ではルートDNSサーバを利用するため、ルートDNSサーバを有効に設定します。

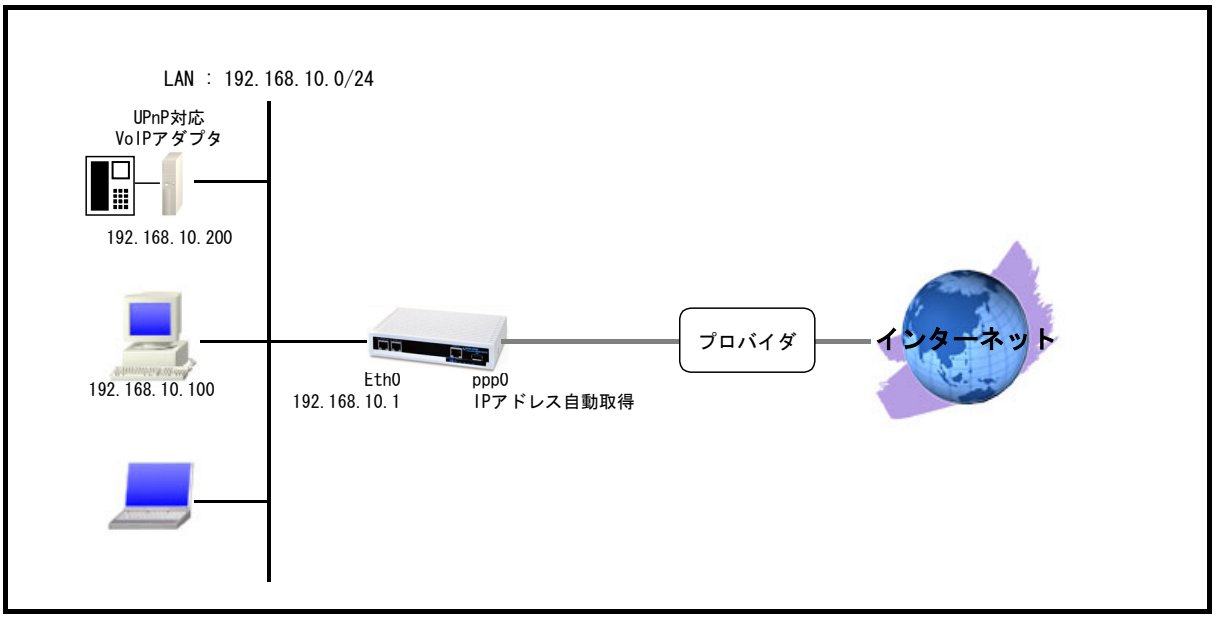
【 サーバ，パソコンの設定例 】

	WWW サーバ	パソコン
IP アドレス	192.168.10.10	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	-	192.168.10.1

2-4. UPnP 設定

UPnP 対応の VoIP アダプタや UPnP 対応のアプリケーションなどを NXR 配下で利用する場合は、UPnP 機能を設定します。

【 構成図 】



- Ethernet0 インタフェースを LAN 側, ppp0 インタフェースを WAN 側とします。
- ppp0 インタフェースで IP マスカレードを有効にし、NXR 配下の複数の端末がインターネットアクセスできるように、送信元 IP アドレスおよびポート番号を変換します。
- UPnP で NAT 外部側を ppp0 インタフェース, 内部側を Ethernet0 インタフェース(192.168.10.1/24)とします。
- DNS 機能を有効にし、NXR 配下の端末からの DNS リクエストを中継できるようにします。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address negotiated
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#upnp
nxr120(config-upnp)#external interface ppp 0
nxr120(config-upnp)#listen ip 192.168.10.1/24
nxr120(config-upnp)#timeout 3600
nxr120(config-upnp)#service enable
nxr120(config-upnp)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合はゲートウェイとして ppp インタフェースを指定します。

3. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr120(config-ppp)#ip address negotiated
```

IP アドレスを negotiated（自動取得）に設定します。

```
nxr120(config-ppp)#ip masquerade
```

IP マスカレードを設定します。

```
nxr120(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。
TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr120(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。
ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

4. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
```

Ethernet1 インタフェースを設定します。

```
nxr120(config-if)#no ip address
```

Ethernet1 インタフェースに IP アドレスを割り当てない設定をします。
PPPoE 接続でプロバイダ等から割り当てられる IP アドレスは Ethernet インタフェースではなく ppp インタフェースに割り当てられますので、PPPoE のみで使用する場合は IP アドレスの設定は不要です。

```
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェース上で ppp0 インタフェースを使用するための設定をします。
PPPoE で ppp インタフェースを使用する場合は、pppoe-client コマンドによるインタフェース設定での登録が必要になります。

5. ＜UPnP 設定＞

```
nxr120(config)#upnp
```

UPnP を設定します。

```
nxr120(config-upnp)#external interface ppp 0
```

WAN 側インタフェースとして ppp0 を設定します。

LAN 内の UPnP 対応機器に対しては、ここで設定したインタフェースの IP アドレスを通知します。

```
nxr120(config-upnp)#listen ip 192.168.10.1/24
```

LAN 配下の機器からのポートマッピング要求に対応する IP アドレスを設定します。

```
nxr120(config-upnp)#timeout 3600
```

ポートマッピングによって設定された NAT エントリを監視して、通過パケットが一定時間なかった場合にポート情報を削除するためのタイマー(秒)を設定します。

```
nxr120(config-upnp)#service enable
```

UPnP サービスを有効にします。

6. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

【 パソコン, VoIP アダプタの設定例 】

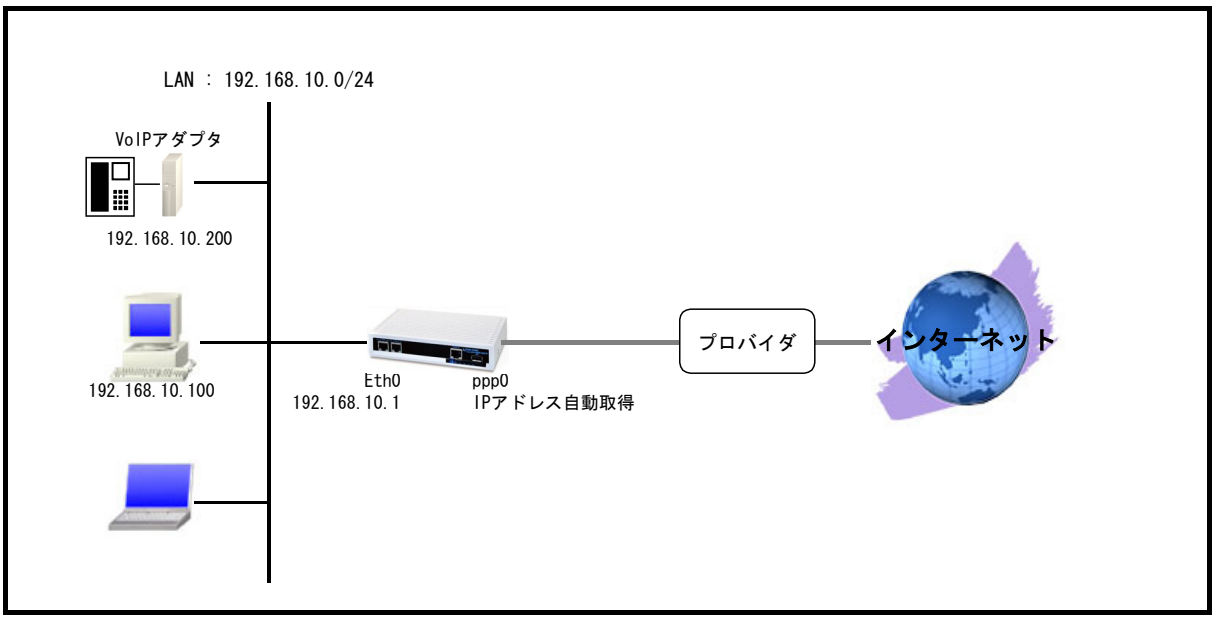
	UPnP 対応のパソコン	UPnP 対応 VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1	192.168.10.1

※VoIP アダプタの SIP に関する設定は除く

2-5. SIP-NAT 設定 1

通常の NAT や IP マスカレード機能では IP ヘッダの IP アドレスのみ変換しますが、SIP-NAT 機能では SIP メッセージ中の IP アドレスを変換することが可能です。これにより、NAT 配下においても VoIP 端末を利用することが可能になります。

【 構成図 】



- 本設定例の VoIP アダプタで利用を想定しているポート番号は以下のとおりです。
  SIP サーバ：UDP5060
  RTP：UDP5090
  RTCP：UDP5091
- SIP-NAT 機能を有効にします。
- NXR 配下の VoIP アダプタに対する着信に対応するため、DNAT および IPv4 アクセスリストを設定します。
- ppp0 インタフェースで IP マスカレードを有効にし、NXR 配下の複数の端末がインターネットアクセスできるように送信元 IP アドレスおよびポート番号を変換します。
- DNS 機能を有効にし、NXR 配下の端末からの DNS リクエストを中継できるようにします。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#sip-nat enable
nxr120(config)#ip dnat ppp0_dnat udp any any any 5060 192.168.10.200
nxr120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5060
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address negotiated
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合は、通常ゲートウェイとして ppp インタフェースを指定します。

3. ＜SIP-NAT 設定＞

```
nxr120(config)#sip-nat enable
```

SIP-NAT 機能を有効にします。

4. ＜DNAT 設定＞

```
nxr120(config)#ip dnat ppp0_dnat udp any any any 5060 192.168.10.200
nxr120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

一行目の設定は宛先 UDP ポート番号 5060 のパケットの宛先 IP アドレスを 192.168.10.200 に変換するための設定です。
二行目の設定は宛先 UDP ポート番号 5090～5091 のパケットの宛先 IP アドレスを 192.168.10.200 に変換するための設定です。
この DNAT 設定は、ppp0 インタフェース設定で登録します。
(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス,ポート番号の変換を行うインタフェースでの登録が必要になります。
(☞) この DNAT 設定は VoIP アダプタへの着信に対応するための設定です。

5. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5060
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
```

フィルタの動作を規定するルールリストを作成します。
ここでは IP アクセスリスト名を ppp0_forward-in とします。
一行目の設定は宛先 IP アドレス 192.168.10.200 宛先 UDP ポート番号 5060 のパケットを許可するための設定です。
二行目の設定は宛先 IP アドレス 192.168.10.200 宛先 UDP ポート番号 5090～5091 のパケットを許可するための設定です。
なおこの IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。
(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。
(☞) このフィルタ設定は VoIP アダプタへの着信に対応するための設定です。

6. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr120(config-ppp)#ip address negotiated
```

IP アドレスを negotiated（自動取得）に設定します。

```
nxr120(config-ppp)#ip dnat-group ppp0_dnat
```

DNAT 設定で設定した ppp0_dnat を適用します。これにより ppp0 インタフェースで DNAT 設定で設定した IP アドレス変換が行われます。

```
nxr120(config-ppp)#ip masquerade
```

IP マスカレードを設定します。

```
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
```

IP アクセスリスト設定で設定した ppp0_forward-in を forward-in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR を経由するパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr120(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr120(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

7. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。

Ethernet1 インタフェースの設定は 2-4. UPnP 設定の＜Ethernet1 インタフェース設定＞と同等ですので詳細はそちらをご参照下さい。

8. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効にします。

【 パソコン, VoIP アダプタの設定例 】

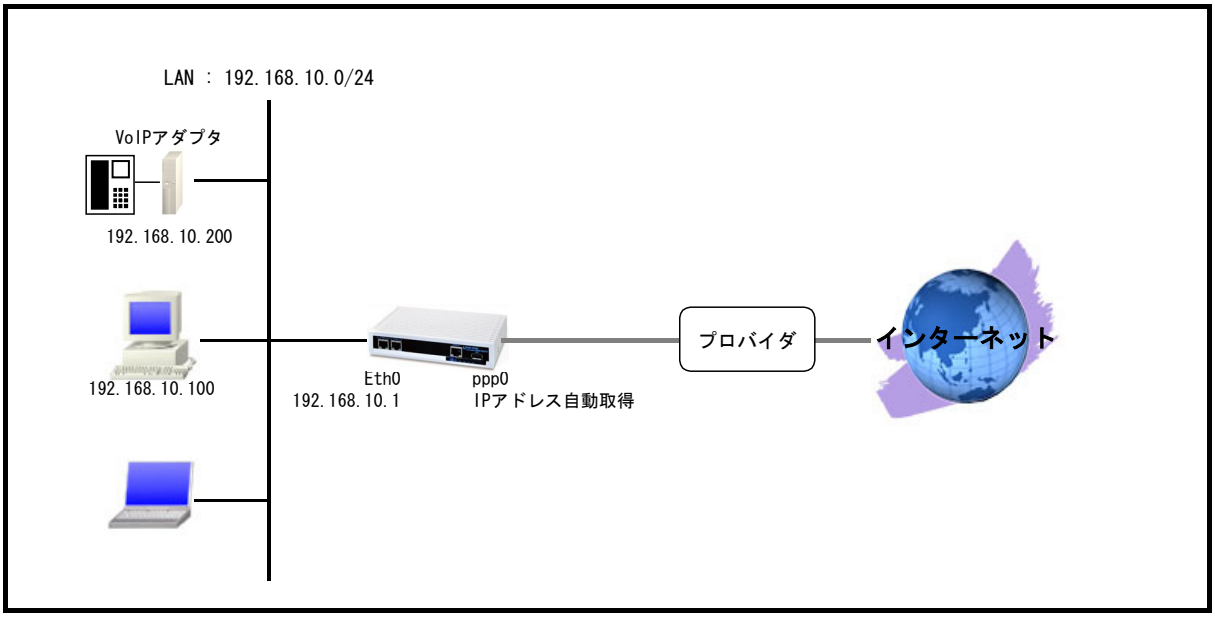
	パソコン	VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1	192.168.10.1

※VoIP アダプタの SIP に関する設定は除く

2-6. SIP-NAT 設定２

自身の SIP ポートまたは SIP サーバの UDP ポート番号が 5060 以外の場合、この設定例に記載されているような設定が必要となります。
一部の IP 電話サービスにおいて REGISTER の送信先 SIP サーバの IP アドレスと INVITE の送信元 IP アドレスが異なる場合があり、この設定を行わなかった場合通話できない可能性があります。

【 構成図 】



- 本設定例の VoIP アダプタで利用を想定しているポート番号は以下のとおりです。
  SIP サーバ：UDP5060
  SIP：UDP5064
  RTP：UDP5090
  RTCP：UDP5091
- SIP-NAT 機能を有効にし、SIP-NAT 対象のポート番号として SIP サーバで利用する UDP5060, 5064 を設定します。
- NXR 配下の VoIP アダプタに対する着信に対応するため、DNAT および IPv4 アクセスリストを設定します。
- ppp0 インタフェースで IP マスカレードを有効にし、NXR 配下の複数の端末がインターネットアクセスできるように送信元 IP アドレスおよびポート番号を変換します。
- DNS 機能を有効にし、NXR 配下の端末からの DNS リクエストを中継できるようにします。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#sip-nat enable
nxr120(config)#sip-nat port 5060 5064
nxr120(config)#ip dnat ppp0_dnat udp any any any 5064 192.168.10.200
nxr120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5064
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip address negotiated
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合は、通常ゲートウェイとして ppp インタフェースを指定します。

3. ＜SIP-NAT 設定＞

```
nxr120(config)#sip-nat enable
```

SIP-NAT 機能を有効にします。

```
nxr120(config)#sip-nat port 5060 5064
```

UDP ポート番号 5060 および 5064 を宛先とするパケットを SIP-NAT 対象とするよう設定します。これにより Registrar の宛先である SIP サーバの IP アドレスと INVITE の送信元である SIP サーバの IP アドレスが異なる場合でも VoIP を利用することができます。

4. ＜DNAT 設定＞

```
nxr120(config)#ip dnat ppp0_dnat udp any any any 5064 192.168.10.200
nxr120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

一行目の設定は宛先 UDP ポート番号 5064 のパケットの宛先 IP アドレスを 192.168.10.200 に変換するための設定です。

二行目の設定は宛先 UDP ポート番号 5090～5091 のパケットの宛先 IP アドレスを 192.168.10.200 に変換するための設定です。

この DNAT 設定は ppp0 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス,ポート番号の変換を行うインタフェースでの登録が必要になります。

(☞) この DNAT 設定は VoIP アダプタへの着信に対応するための設定です。

5. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5064
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_forward-in とします。

一行目の設定は宛先 IP アドレス 192.168.10.200 宛先 UDP ポート番号 5064 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 192.168.10.200 宛先 UDP ポート番号 5090～5091 のパケットを許可するための設定です。

なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

(☞) このフィルタ設定は VoIP アダプタへの着信に対応するための設定です。

6. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip address negotiated
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

ppp0 インタフェースを設定します。

ppp0 インタフェースの設定は 2-5. SIP-NAT 設定 1 の＜ppp0 インタフェース設定＞と同等ですので詳細はそちらをご参照下さい。

7. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。

Ethernet1 インタフェースの設定は 2-4. UPnP 設定の＜Ethernet1 インタフェース設定＞と同等ですので詳細はそちらをご参照下さい。

8. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効にします。

【 パソコン，VoIP アダプタの設定例 】

	パソコン	VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1	192.168.10.1

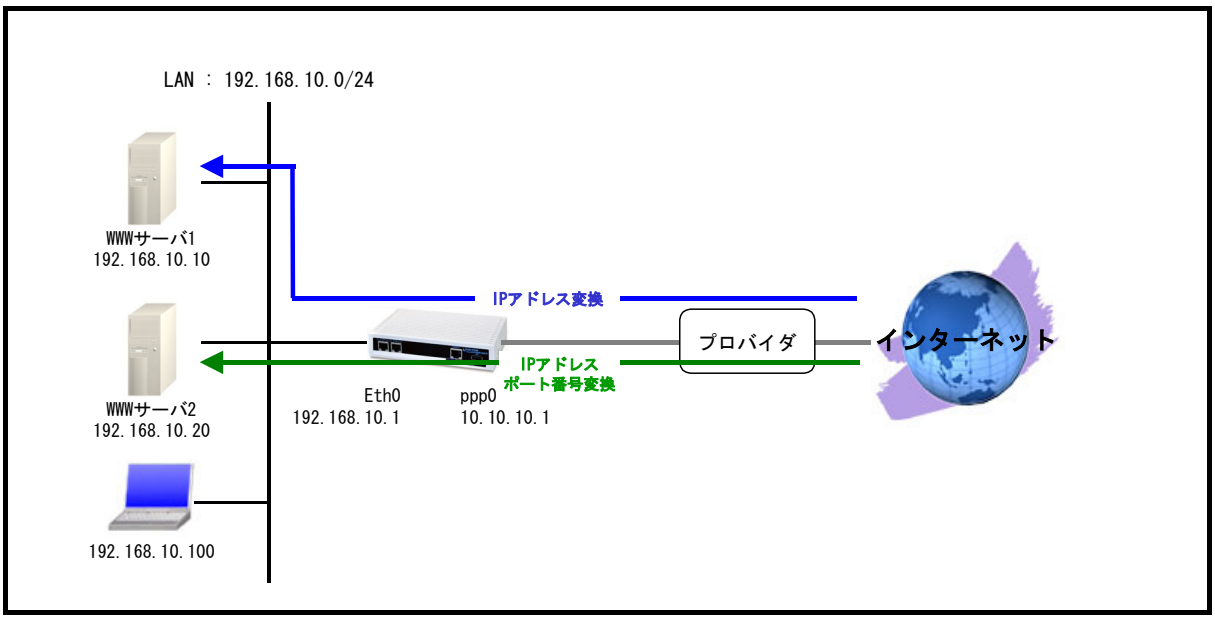
※VoIP アダプタの SIP に関する設定は除く

3. NAT/フィルタ応用設定

3-1. NAT でのサーバ公開１（ポートマッピング）設定

DNAT 機能では宛先 IP アドレス変換時にポート番号も変換することが可能です。ここでは WAN 側で受信時のポート番号を分けておくことで、グローバル IP アドレスが１つでも複数の WEB サーバに対してアクセスが可能になる設定です。

【 構成図 】



- ppp0 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 80 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.10（WWW サーバ 1）に変換します。
- ppp0 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 8080 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.20, TCP ポート番号 80（WWW サーバ 2）に変換します。
- ppp0 インタフェースで宛先 IP アドレス 192.168.10.10 および 192.168.10.20 TCP ポート番号 80 へのアクセスは許可します。
- IP マスカレードを設定し ppp0 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。これにより NXR 配下の複数台の端末からインターネットアクセスが可能になります。
- ppp0 インタフェースでステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも NXR 配下の端末からのアクセスは自由に行えるようにします。
- DNS 機能を有効にすることにより NXR 配下の端末からの名前解決要求(クエリ要求)を ISP より取得した DNS サーバに転送します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 8080 192.168.10.20 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. <Ethernet0 インタフェース設定>

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. <スタティックルート設定>

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合は、ゲートウェイとして ppp インタフェースを指定します。

3. <DNAT 設定>

```
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 8080 192.168.10.20 80
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

一行目の設定は宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定です。

二行目の設定は宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 8080 のパケットの宛先 IP アドレスを 192.168.10.10 宛先 TCP ポート番号 80 に変換するための設定です。

この DNAT 設定は、ppp0 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス,ポート番号の変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_forward-in とします。

一行目の設定は宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 192.168.10.20 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

この IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr120(config-ppp)#ip address 10.10.10.1/32
```

IP アドレスを 10.10.10.1/32 に設定します。

```
nxr120(config-ppp)#ip dnat-group ppp0_dnat
```

DNAT 設定で設定した ppp0_dnat を適用します。これにより ppp0 インタフェースで DNAT 設定で設定した IP アドレス変換が行われます。

```
nxr120(config-ppp)#ip masquerade
```

IP マスカレードを設定します。

```
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
```

IP アクセスリスト設定で設定した ppp0_forward-in を forward-in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR を経由するパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr120(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。
TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr120(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。
ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

6. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
```

Ethernet1 インタフェースを設定します。

```
nxr120(config-if)#no ip address
```

Ethernet1 インタフェースに IP アドレスを割り当てない設定をします。
PPPoE 接続でプロバイダ等から割り当てられる IP アドレスは Ethernet インタフェースではなく ppp インタフェースに割り当てられますので、PPPoE のみで使用する場合は IP アドレスの設定は不要です。

```
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェース上で ppp0 インタフェースを使用するための設定をします。
PPPoE で ppp インタフェースを使用する場合は、pppoe-client コマンドによるインタフェース設定での登録が必要になります。

7. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

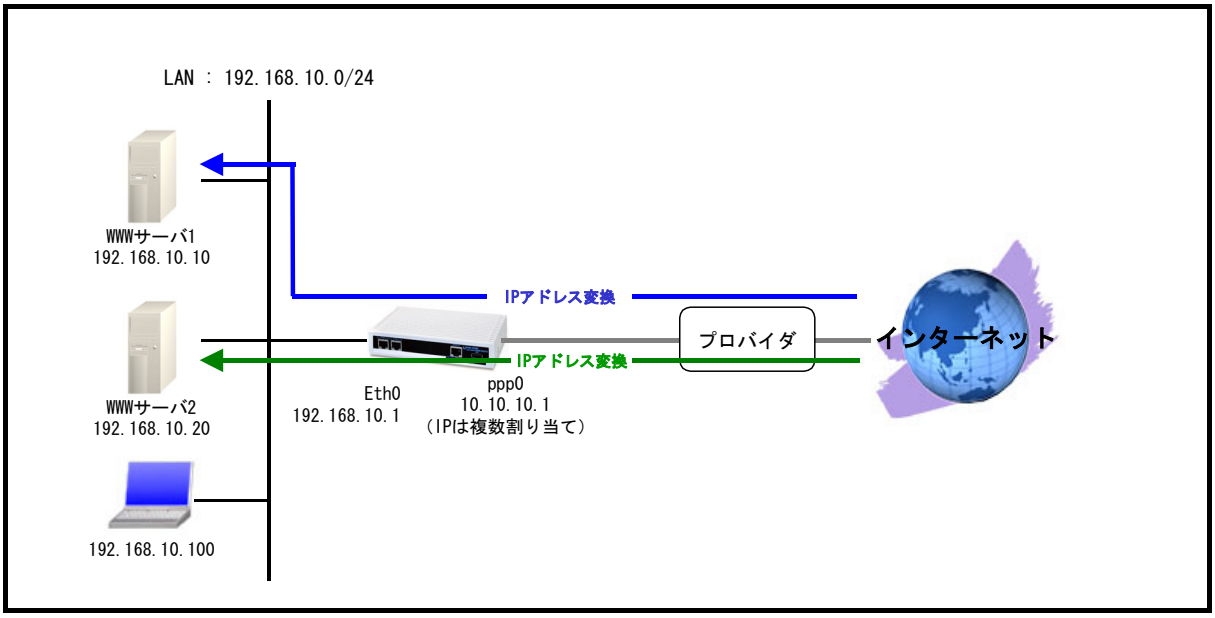
【 パソコンの設定例 】

	WWW サーバ１	WWW サーバ２	パソコン
IP アドレス	192.168.10.10	192.168.10.20	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	―	―	192.168.10.1

3-2. NAT でのサーバ公開２（複数 IP＋PPPoE）設定

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎に LAN 内のプライベート IP アドレスを持ったサーバに対して DNAT 設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスさせることができます。ここでは WAN 回線に PPPoE を利用した例になります。

【 構成図 】



- ppp0 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 80 のパケットを受信した場合はパケットの宛先 IP アドレスを 192.168.10.10（WWW サーバ１）に変換します。
- ppp0 インタフェースで宛先 IP アドレス 10.10.10.2, TCP ポート番号 80 のパケットを受信した場合はパケットの宛先 IP アドレスを 192.168.10.20（WWW サーバ２）に変換します。
- ppp0 インタフェースで宛先 IP アドレス 192.168.10.10 および 192.168.10.20 TCP ポート番号 80 へのアクセスは許可します。
- IP マスカレードを設定し ppp0 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。これにより NXR 配下の複数台の端末からインターネットアクセスが可能になります。
- ppp0 インタフェースでステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも NXR 配下の端末からのアクセスは自由に行えるようにします。
- DNS 機能を有効にすることにより NXR 配下の端末からの名前解決要求(クエリ要求)を ISP より取得した DNS サーバに転送します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.2 80 192.168.10.20
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合は、ゲートウェイとして ppp インタフェースを指定します。

3. ＜DNAT 設定＞

```
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.2 80 192.168.10.20
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

一行目の設定は宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定です。

二行目の設定は宛先 IP アドレス 10.10.10.2 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.20 に変換するための設定です。

この DNAT 設定は、ppp0 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス,ポート番号の変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_forward-in とします。

一行目の設定は宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 192.168.10.20 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

この IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

ppp0 インタフェースを設定します。

ppp0 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の＜ppp0 インタフェース設定＞と同等ですので、詳細はそちらをご参照下さい。

6. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。

Ethernet1 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の＜Ethernet1 インタフェース設定＞と同等ですので、詳細はそちらをご参照下さい。

7. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

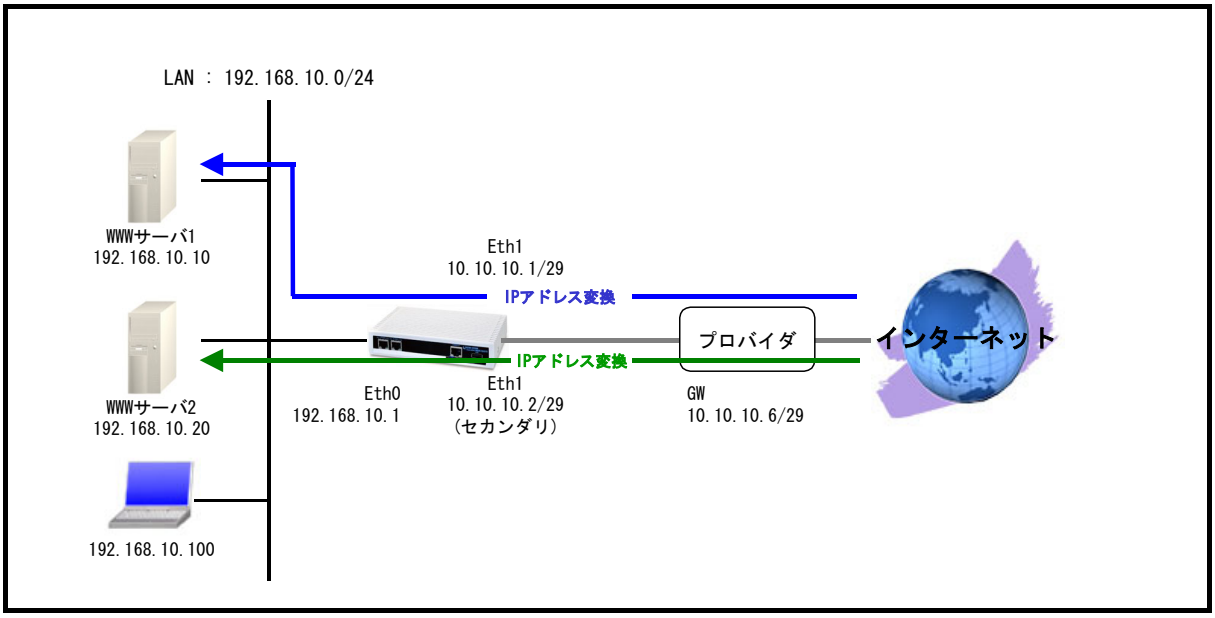
【 サーバ，パソコンの設定例 】

	WWW サーバ１	WWW サーバ２	パソコン
IP アドレス	192.168.10.10	192.168.10.20	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	―	―	192.168.10.1

3-3. NAT でのサーバ公開３（複数 IP＋Ethernet）設定

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎に LAN 内のプライベート IP アドレスを持ったサーバに対して DNAT 設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスさせることができます。ここでは WAN 回線に Ethernet を利用した例になります。

【 構成図 】



- Ethernet1 インタフェースで複数 IP アドレスを利用するためにセカンダリ IP アドレスを設定します。
- Ethernet1 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 80 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.10（WWW サーバ１）に変換します。
- Ethernet1 インタフェースで宛先 IP アドレス 10.10.10.2, TCP ポート番号 80 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.20（WWW サーバ２）に変換します。
- Ethernet1 インタフェースで宛先 IP アドレス 192.168.10.10 および 192.168.10.20 TCP ポート番号 80 へのアクセスは許可します。
- IP マスカレードを設定し Ethernet1 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。これにより NXR 配下の複数台の端末からインターネットアクセスが可能になります。
- Ethernet1 インタフェースでステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも NXR 配下の端末からのアクセスは自由に行えるようにします。
- DNS 機能を有効にすることにより NXR 配下の端末からの名前解決要求(クエリ要求)をルート DNS サーバに転送します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 10.10.10.6
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.2 80 192.168.10.20
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.20 tcp any 80
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/29
nxr120(config-if)#ip address 10.10.10.2/29 secondary
nxr120(config-if)#ip dnat-group eth1_dnat
nxr120(config-if)#ip masquerade
nxr120(config-if)#ip access-group forward-in eth1_forward-in
nxr120(config-if)#ip spi-filter
nxr120(config-if)#no ip redirects
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#root enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 10.10.10.6
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

3. ＜DNAT 設定＞

```
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip dnat eth1_dnat tcp any any 10.10.10.2 80 192.168.10.20
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を eth1_dnat とします。

一行目の設定は宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定です。

二行目の設定は宛先 IP アドレス 10.10.10.2 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.20 に変換するための設定です。

この DNAT 設定は、Ethernet1 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス，ポート番号の変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#ip access-list eth1_forward-in permit any 192.168.10.20 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を eth1_forward-in とします。

一行目の設定は宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 192.168.10.20 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

この IP アクセスリスト設定は、Ethernet1 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#ip address 10.10.10.1/29
```

Ethernet1 インタフェースの IP アドレスに 10.10.10.1/29 を設定します。

```
nxr120(config-if)#ip address 10.10.10.2/29 secondary
```

Ethernet1 インタフェースのセカンダリ IP アドレスとして 10.10.10.2/29 を設定します。

```
nxr120(config-if)#ip dnat-group eth1_dnat
```

DNAT 設定で設定した eth1_dnat を適用します。これにより Ethernet1 インタフェースで DNAT 設定で設定した IP アドレス変換が行われます。

```
nxr120(config-if)#ip masquerade
```

IP マスカレードを設定します。

```
nxr120(config-if)#ip access-group forward-in eth1_forward-in
```

IP アクセスリスト設定で設定した eth1-forward-in を forward-in フィルタに適用します。これにより Ethernet1 インタフェースで受信した NXR を経由するパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr120(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-if)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

6. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

```
nxr120(config-dns)#root enable
```

この設定例ではルート DNS サーバを利用するため、ルート DNS サーバを有効に設定します。

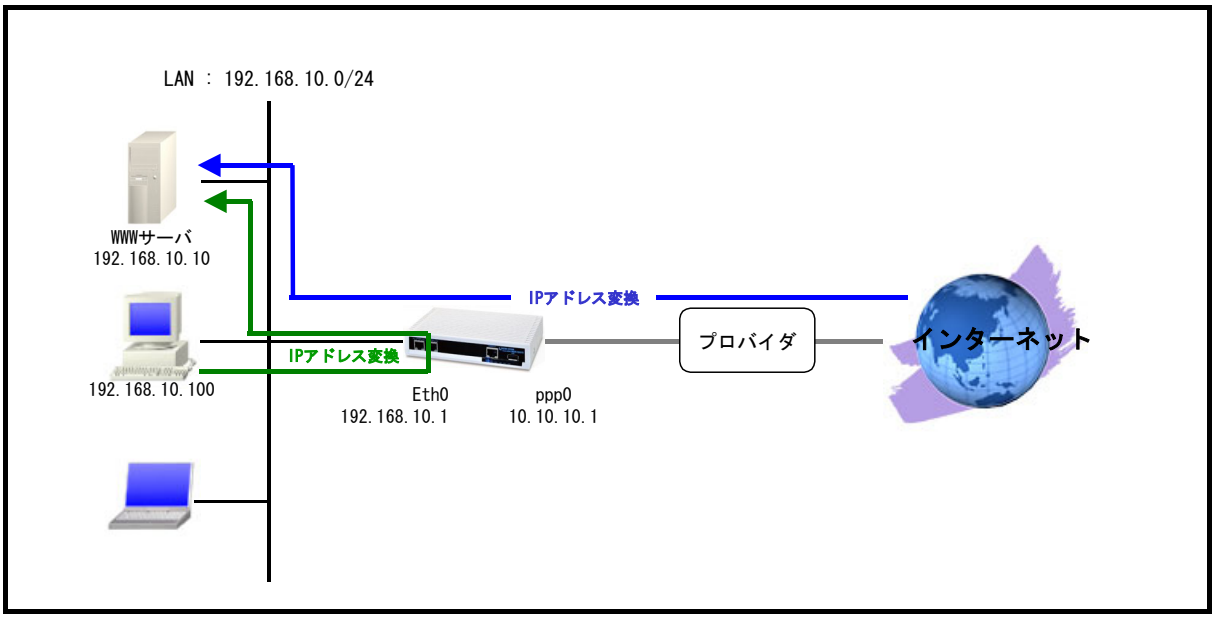
【 サーバ，パソコンの設定例 】

	WWW サーバ１	WWW サーバ２	パソコン
IP アドレス	192.168.10.10	192.168.10.20	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	―	―	192.168.10.1

3-4. NAT でのサーバ公開４（LAN 内のサーバにグローバル IP アドレスでアクセス）設定

NAT 配下の端末より NAT で外部に公開しているサーバに対してプライベート IP アドレスでのアクセスだけでなく、グローバル IP アドレスでのアクセスも可能です。ここでは NAT で公開している LAN 内の WWW サーバに対してグローバル IP アドレスでアクセスするための設定です。

【 構成図 】



- ppp0 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 80 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.10（WWW サーバ）に変換します。
- Ethernet0 インタフェースで宛先 IP アドレス 10.10.10.1, TCP ポート番号 80 のパケットを受信した場合は、パケットの送信元 IP アドレスを 192.168.10.1 宛先 IP アドレスを 192.168.10.10（WWW サーバ）に変換します。
- ppp0 インタフェースで宛先 IP アドレス 192.168.10.10 TCP ポート番号 80 へのアクセスは許可します。
- IP マスカレードを設定し ppp0 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。これにより NXR 配下の複数台の端末からインターネットアクセスが可能になります。
- ppp0 インタフェースでステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも NXR 配下の端末からのアクセスは自由に行えるようにします。
- DNS 機能を有効にすることにより NXR 配下の端末からの名前解決要求(クエリ要求)を ISP より取得した DNS サーバに転送します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
nxr120(config)#ip dnat eth0_dnat tcp 192.168.10.0/24 any 10.10.10.1 80 192.168.10.10
nxr120(config)#ip snat eth0_snat tcp 192.168.10.0/24 any 192.168.10.10 80 192.168.10.1
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#ip dnat-group eth0_dnat
nxr120(config-if)#ip snat-group eth0_snat
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜DNAT 設定＞

```
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定をします。

この DNAT 設定は ppp0 インタフェース設定で登録します。

```
nxr120(config)#ip dnat eth0_dnat tcp 192.168.10.0/24 any 10.10.10.1 80 192.168.10.10
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を eth0_dnat とします。

送信元 IP アドレス 192.168.10.0/24 宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定をします。

この DNAT 設定は、Ethernet0 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス，ポート番号の変換を行うインタフェースでの登録が必要になります。

2. ＜SNAT 設定＞

```
nxr120(config)#ip snat eth0_snat tcp 192.168.10.0/24 any 192.168.10.10 80 192.168.10.1
```

SNAT の動作ルールを作成します。

ここでは SNAT ルール名を eth0_snat とします。

送信元 IP アドレス 192.168.10.0/24 宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットの送信元 IP アドレスを 192.168.10.1 に変換するための設定をします。

この SNAT 設定は、Ethernet0 インタフェース設定で登録します。

(☞) SNAT 設定を設定しただけでは送信元 IP アドレスの変換機能は動作しません。送信元 IP アドレスの変換を行うインタフェースでの登録が必要になります。

3. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

```
nxr120(config-if)#ip dnat-group eth0_dnat
```

DNAT 設定で設定した eth0_dnat を適用します。これにより Ethernet0 インタフェースで DNAT 設定で設定した eth0_dnat のルールに基づいた IP アドレス変換が行われます。

```
nxr120(config-if)#ip snat-group eth0_snat
```

SNAT 設定で設定した eth0_snat を適用します。これにより Ethernet0 インタフェースで SNAT 設定で設定した eth0_snat のルールに基づいた IP アドレス変換が行われます。

4. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合はゲートウェイとして ppp インタフェースを指定します。

5. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_forward-in とします。

宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するように設定します。

この IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

6. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

ppp0 インタフェースを設定します。

ppp0 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の＜ppp0 インタフェース設定＞と同等ですので、詳細はそちらをご参照下さい。

7. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。

Ethernet1 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の＜Ethernet1 インタフェース設定＞と同等ですので、詳細はそちらをご参照下さい。

8. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

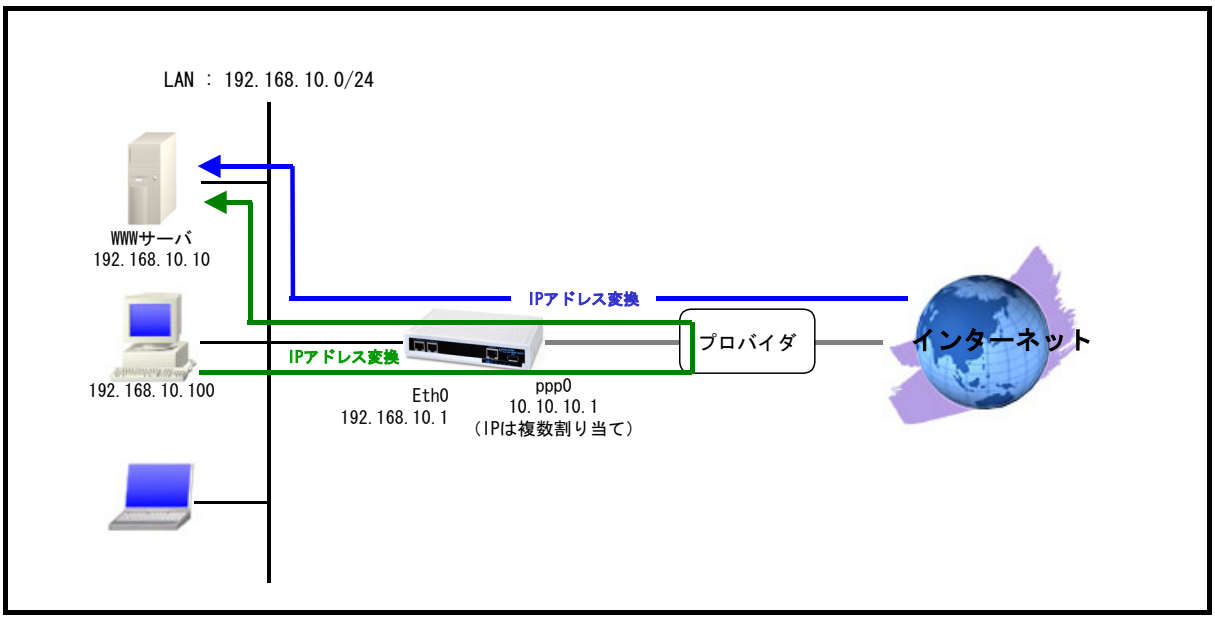
【 サーバ，パソコンの設定例 】

	WWW サーバ	パソコン
IP アドレス	192.168.10.10	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	―	192.168.10.1

3-5. NAT でのサーバ公開５（IP nat-loopback の利用）設定

IP nat-loopback 機能を利用し NAT で外部に公開しているサーバに対して NAT 配下の端末よりプライベート IP アドレスでのアクセスだけでなく、グローバル IP アドレスでのアクセスも可能にする設定例です。

【 構成図 】



- IP nat-loopback 機能はグローバル IP アドレスを持つインタフェース以外からグローバル IP アドレスに対してアクセスが行われた場合、NXR 自身で受信せずに一度ルーティングテーブルに従って転送されます。その後インターネット側から戻ってきたパケットを DNAT することで NAT 配下の端末からもグローバル IP アドレスに対してアクセスできるようにします。
  (☞)　IP nat-loopback 機能は PPP インタフェース上でのみ利用することが可能です。
- IP nat-loopback 機能を設定しているインタフェース上でステートフルパケットインスペクション（以下 SPI）が有効な場合は、フィルタ設定で通過させたいパケットをあらかじめ許可しておく、または SPI を無効にする必要があります。
- IP nat-loopback 機能を設定しているインタフェース上では IP マスカレード機能を有効に設定する必要があります。
- この設定例では ppp0 インタフェースで宛先 IP アドレス 10.10.10.1 TCP ポート番号 80 のパケットを受信した場合は、パケットの宛先 IP アドレスを 192.168.10.10 (WWW サーバ) に変換します。
- この設定例では ppp0 インタフェースで宛先 IP アドレス 192.168.10.10 TCP ポート番号 80 へのアクセスは許可します。
- IP マスカレードを設定し ppp0 インタフェースから出力されるパケットの送信元 IP アドレスを変換します。これにより NXR 配下の複数台の端末からインターネットアクセスが可能になります。
- ppp0 インタフェースでステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも NXR 配下の端末からのアクセスは自由に行えるようにします。

・ DNS 機能を有効にすることにより NXR 配下の端末からの名前解決要求(クエリ要求)を ISP より取得した DNS サーバに転送します。

【 設定例 】

```
nxr120#configure terminal
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 ppp 0
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nxr120(config)#interface ppp 0
nxr120(config-ppp)#ip address 10.10.10.1/32
nxr120(config-ppp)#ip nat-loopback
nxr120(config-ppp)#ip dnat-group ppp0_dnat
nxr120(config-ppp)#ip masquerade
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr120(config-ppp)#ip spi-filter
nxr120(config-ppp)#ip tcp adjust-mss auto
nxr120(config-ppp)#no ip redirects
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
nxr120(config-ppp)#exit
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合は、ゲートウェイとして ppp インタフェースを指定します。

3. ＜DNAT 設定＞

```
nxr120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
```

DNAT の動作ルールを作成します。

ここでは DNAT ルール名を ppp0_dnat とします。

宛先 IP アドレス 10.10.10.1 宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスを 192.168.10.10 に変換するための設定をします。

この DNAT 設定は、ppp0 インタフェース設定で登録します。

(☞) DNAT 設定を設定しただけでは宛先 IP アドレスの変換機能は動作しません。宛先 IP アドレス，ポート番号の変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
```

フィルタの動作を規定するルールリストを作成します。
ここでは IP アクセスリスト名を ppp0_forward-in とします。
宛先 IP アドレス 192.168.10.10 宛先 TCP ポート番号 80 のパケットを許可するための設定をします。
この IP アクセスリスト設定は、ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜ppp0 インタフェース設定＞

```
nxr120(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr120(config-ppp)#ip address 10.10.10.1/32
```

IP アドレスを 10.10.10.1/32 に設定します。

```
nxr120(config-ppp)#ip nat-loopback
```

IP nat-loopback 機能を設定します。

```
nxr120(config-ppp)#ip dnat-group ppp0_dnat
```

DNAT 設定で設定した ppp0_dnat を適用します。これにより ppp0 インタフェースで DNAT 設定で設定した IP アドレス変換が行われます。

```
nxr120(config-ppp)#ip masquerade
```

IP マスカレードを設定します。IP nat-loopback 機能を設定する場合は、IP マスカレード(もしくは SNAT)を設定する必要があります。

```
nxr120(config-ppp)#ip access-group forward-in ppp0_forward-in
```

IP アクセスリスト設定で設定した ppp0_forward-in を forward-in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR を経由するパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr120(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアク

セスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr120(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr120(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr120(config-ppp)#ppp username test1@centurysys password test1pass
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

6. ＜Ethernet1 インタフェース設定＞

```
nxr120(config)#interface ethernet 1
nxr120(config-if)#no ip address
nxr120(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。

Ethernet1 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の＜Ethernet1 インタフェース設定＞と同等ですので、詳細はそちらをご参照下さい。

7. ＜DNS 設定＞

```
nxr120(config)#dns
nxr120(config-dns)#service enable
```

DNS サービスを有効に設定します。

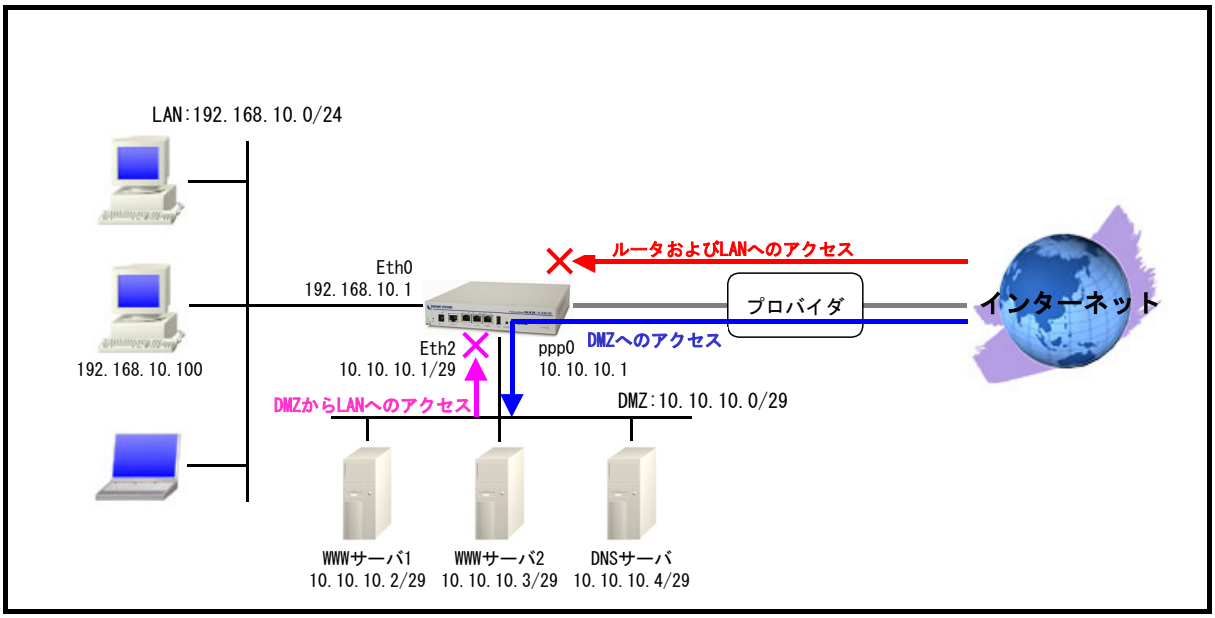
【 サーバ, パソコンの設定例 】

	WWW サーバ	パソコン
IP アドレス	192.168.10.10	192.168.10.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	―	192.168.10.1

3-6. DMZ 構築（PPPoE）設定

NXR-130/C のように３ポート（３セグメント）以上を有する製品では、インターネットに公開するサーバ群（DMZ）と社内 LAN を物理的に分けて構築することが可能です。

【 構成図 】



- Ethernet0 を LAN 側，ppp0(Ethernet1)を WAN 側，Ethernet2 を DMZ 側とします。
- Ethernet0 インタフェースが属するネットワーク 192.168.10.0/24 からのパケットで ppp0 インタフェースから出力されるパケットは、送信元 IP アドレスを 10.10.10.1 に変換します。
- ステートフルパケットインスペクションを利用しインターネット側からのアクセスを破棄しながらも Ethernet0 インタフェースが属するネットワークからのアクセスは自由に行えるようにします。
- ppp0 インタフェースでステートフルパケットインスペクションを設定しインターネット側からのアクセスに対して基本的には破棄しますが、以下のアクセスだけ許可します。
  宛先 IP アドレス 10.10.10.0/29 宛の ICMP パケット
  （ただし宛先 IP アドレス 10.10.10.1 の ICMP Echo Request は破棄）
  宛先 IP アドレス 10.10.10.2 および 10.10.10.3 宛先 TCP ポート番号 80（WWW サーバ）
  宛先 10.10.10.4 宛先 TCP,UDP ポート番号 53（DNS サーバ）
- Ethernet2 インタフェースでもステートフルパケットインスペクションを有効にし、DMZ から LAN へのアクセスおよびインターネットへの不要なアクセスを破棄します。
- DNS 機能を有効にすることにより NXR 配下の LAN 内の端末からの名前解決要求(クエリ要求)を DMZ 内の DNS サーバに転送します。

【 設定例 】

```
nxr130#configure terminal
nxr130(config)#interface ethernet 0
nxr130(config-if)#ip address 192.168.10.1/24
nxr130(config-if)#exit
nxr130(config)#ip route 0.0.0.0/0 ppp 0
nxr130(config)#ip snat ppp0_snat ip 192.168.10.0/24 any 10.10.10.1
nxr130(config)#ip access-list ppp0_in deny any 10.10.10.1 icmp 8 0
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.2 tcp any 80
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.3 tcp any 80
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 tcp any 53
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 udp any 53
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.0/29 icmp
nxr130(config)#interface ppp 0
nxr130(config-ppp)#ip address 10.10.10.1/32
nxr130(config-ppp)#ip snat-group ppp0_snat
nxr130(config-ppp)#ip access-group in ppp0_in
nxr130(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr130(config-ppp)#ip spi-filter
nxr130(config-ppp)#ip tcp adjust-mss auto
nxr130(config-ppp)#no ip redirects
nxr130(config-ppp)#ppp username test1@centurysys password test1pass
nxr130(config-ppp)#exit
nxr130(config)#interface ethernet 1
nxr130(config-if)#no ip address
nxr130(config-if)#pppoe-client ppp 0
nxr130(config-if)#exit
nxr130(config)#interface ethernet 2
nxr130(config-if)#ip address 10.10.10.1/29
nxr130(config-if)#ip spi-filter
nxr130(config-if)#exit
nxr130(config)#dns
nxr130(config-dns)#address 10.10.10.4
nxr130(config-dns)#service enable
nxr130(config-dns)#exit
nxr130(config)#exit
nxr130#save config
```

【 設定例解説 】

1. ＜Ethernet0 インタフェース設定＞

```
nxr130(config)#interface ethernet 0
nxr130(config-if)#ip address 192.168.10.1/24
```

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

2. ＜スタティックルート設定＞

```
nxr130(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。PPPoE を利用する場合で、ppp インタフェース側をゲートウェイとする場合はゲートウェイとして ppp インタフェースを指定します。

3. ＜SNAT 設定＞

```
nxr130(config)#ip snat ppp0_snat ip 192.168.10.0/24 any 10.10.10.1
```

SNAT の動作ルールを作成します。

ここでは SNAT ルール名を ppp0_snat とします。

送信元 IP アドレス 192.168.10.0/24 のパケットの送信元 IP アドレスを 10.10.10.1 に変換するための設定をします。

この SNAT 設定は ppp0 インタフェース設定で登録します。

(☞) SNAT 設定を設定しただけでは送信元 IP アドレスの変換機能は動作しません。送信元 IP アドレスの変換を行うインタフェースでの登録が必要になります。

4. ＜IP アクセスリスト設定＞

```
nxr130(config)#ip access-list ppp0_in deny any 10.10.10.1 icmp 8 0
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

宛先 IP アドレス 10.10.10.1 の ICMP Echo Request（Type8Code0）パケットを破棄するための設定をします。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

```
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.2 tcp any 80
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.3 tcp any 80
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 tcp any 53
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 udp any 53
nxr130(config)#ip access-list ppp0_forward-in permit any 10.10.10.0/29 icmp
```

ここでは IP アクセスリスト名を ppp0_forward-in とします。

一行目の設定は宛先 IP アドレス 10.10.10.2 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

二行目の設定は宛先 IP アドレス 10.10.10.3 宛先 TCP ポート番号 80 のパケットを許可するための設定です。

三行目の設定は宛先 IP アドレス 10.10.10.4 宛先 TCP ポート番号 53 のパケットを許可するための設定です。

四行目の設定は宛先 IP アドレス 10.10.10.4 宛先 UDP ポート番号 53 のパケットを許可するための設定です。

五行目の設定は宛先 IP アドレス 10.10.10.0/29 の ICMP パケットを許可するための設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングを行うインタフェースでの登録が必要になります。

5. ＜ppp0 インタフェース設定＞

```
nxr130(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr130(config-ppp)#ip address 10.10.10.1/32
```

IP アドレスを 10.10.10.1/32 に設定します。

```
nxr130(config-ppp)#ip snat-group ppp0_snat
```

SNAT 設定で設定した ppp0_snat を適用します。これにより ppp0 インタフェースで SNAT 設定で設定した IP アドレス変換が行われます。

```
nxr130(config-ppp)#ip access-group in ppp0_in
```

IP アクセスリスト設定で設定した ppp0_in を in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR 宛のパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr130(config-ppp)#ip access-group forward-in ppp0_forward-in
```

IP アクセスリスト設定で設定した ppp0_forward-in を forward-in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR を経由するパケットに対して IP アクセスリストによるチェックが行われます。

```
nxr130(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
nxr130(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。
TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
nxr130(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr130(config-ppp)#ppp username test1@centurysys password test1pass
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。
ここではユーザ ID を test1@centurysys, パスワードを test1pass とします。

6. ＜Ethernet1 インタフェース設定＞

```
nxr130(config)#interface ethernet 1
nxr130(config-if)#no ip address
nxr130(config-if)#pppoe-client ppp 0
```

Ethernet1 インタフェースを設定します。
Ethernet1 インタフェースの設定は 3-1. NAT でのサーバ公開１（ポートマッピング）設定の**＜Ethernet1 インタフェース設定＞**と同等ですので、詳細はそちらをご参照下さい。

7. ＜Ethernet2 インタフェース設定＞

```
nxr130(config)#interface ethernet 2
nxr130(config-if)#ip address 10.10.10.1/29
```

Ethernet2 インタフェースの IP アドレスに 10.10.10.1/29 を設定します。

```
nxr130(config-if)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

8. ＜DNS 設定＞

```
nxr130(config)#dns
nxr130(config-dns)#address 10.10.10.4
```

DNS サーバの IP アドレスを設定します。ここでは DMZ に設置している DNS サーバ 10.10.10.4 を指定します。

```
nxr130(config-dns)#service enable
```

DNS サービスを有効に設定します。

【 サーバ，パソコンの設定例 】

DMZ	WWW サーバ１	WWW サーバ２	DNS サーバ
IP アドレス	10.10.10.2	10.10.10.3	10.10.10.4
サブネットマスク	255.255.255.248	255.255.255.248	255.255.255.248
デフォルトゲートウェイ	10.10.10.1	10.10.10.1	10.10.10.1

LAN	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1

付録

フィルタ状態確認方法

フィルタの状態(アクセスリスト)を確認には、「show ip access-list」コマンドで確認することができます。

実行例

```
nxr120#show ip access-list
Chain ppp0_forward-in (1 references)
 No.    packts    bytes target   prot       sourceIP            destIP  option
   1       17     1776 permit    tcp      0.0.0.0/0        10.10.10.2  dpt:80
   2       14     1758 permit    tcp      0.0.0.0/0        10.10.10.3  dpt:80
   3        2      132 permit    udp      0.0.0.0/0        10.10.10.4  dpt:53
   4        4      240 permit   icmp      0.0.0.0/0     10.10.10.0/29

Chain ppp0_in (1 references)
 No.    packts    bytes target   prot       sourceIP         destIP  option
   1        4      240   deny   icmp      0.0.0.0/0     10.10.10.1  icmp type 8 code 0
```

(☞) IP アクセスリストの設定は行っているが、そのアクセスリストが属している IP アクセスリストグループがどのインタフェースにも登録されていない場合は、references の部分が(0 references)と表示されます。
この場合その IP アクセスリストグループは有効ではない状態です。

NAT 状態確認方法

DNAT/SNAT の状態を確認には、それぞれ以下のコマンドを実行することにより確認することができます。

DNAT 実行例

```
nxr120#show ip dnat
Chain ppp0_dnat (1 references)
 No.    packts     bytes    prot       sourceIP sport        destIP dport       DNAT
   1         1        52     tcp      0.0.0.0/0 any      10.10.10.1 80         192.168.10.10
```

SNAT 実行例

```
nxr130#show ip snat
Chain eth2_snat (1 references)
 No.    packts     bytes    prot          sourceIP sport         destIP dport       SNAT
   1         2       120     all   192.168.10.0/24  any       0.0.0.0/0 any         10.10.10.1
   2         4       240     all   192.168.20.0/24  any       0.0.0.0/0 any         10.10.10.2
```

(☞) DNAT,SNAT の設定は行っているが、その DNAT,SNAT が属している DNAT グループ,SNAT グループがどのインタフェースにも登録されていない場合は、references の部分が(0 references)と表示されます。
この場合その DNAT グループ,SNAT グループは有効ではない状態です。

UPnP 状態確認方法

UPnP の状態を表示する場合は、「show upnp」コマンドを使用します。

実行例

```
nxr120#show upnp
UDP:5060:192.168.10.200:5060:g101app (192.168.10.200:5060) 5060 UDP
UDP:5090:192.168.10.200:5090:g101app (192.168.10.200:5090) 5090 UDP
UDP:5091:192.168.10.200:5091:g101app (192.168.10.200:5091) 5091 UDP
```

SIP-NAT 状態確認方法

SIP-NAT の状態を表示する場合は、「show sip-nat」コマンドを使用します。

実行例

```
nxr120#show sip-nat
SIP-NAT is on
```

また SIP-NAT に関連した情報を含むセッション情報を表示するためには、「show ip conntrack」コマンドを使用します。

実行例

```
nxr120#show ip conntrack
 udp       17 3353 src=192.168.10.20 dst=10.10.10.200 sport=5060 dport=5060 packets=4 bytes=1870
src=10.10.10.200 dst=10.100.0.1 sport=5060 dport=5060 packets=4 bytes=1786 [ASSURED] mark=0
use=1

----------------------
conntrack count is 1.
```

サポートデスクへのお問い合わせ

サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くことが可能ですので、ご協力をお願い致します。

- ご利用頂いている NXR 製品の機種名,バージョン番号
- ご利用頂いている NXR 製品を含んだネットワーク構成
- 不具合の内容および不具合の再現手順（何を行った場合にどのような問題が発生したのかをできるだけ具体的にお知らせ下さい）
- ご利用頂いている NXR 製品での不具合発生時のログ（show syslog message）
- ご利用頂いている NXR 製品の設定ファイル, show tech-support コマンドの実行結果

サポートデスクのご利用に関して

電話サポート

電話番号：０４２２－３７－８９２６

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 AM - 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail： support@centurysys.co.jp

ＦＡＸサポート

FAX 番号：０４２２－５５－３３７３

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。 その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet NXR シリーズ

NAT,フィルタ設定例集

Ver 1.0.0

2011 年 4 月

発行　センチュリー・システムズ株式会社