FutureNet NXR, WXR 設定例集

NAT,フィルタ編

Ver 1.1.0

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, WXR 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-155/C-XW ， NXR-155/C-L ，
  NXR-230/C, NXR-350/C, NXR-1200, WXR-250
- 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。
  第1章～第3章 FutureNet NXR シリーズ NXR-120/C Ver5.11.0
  ※2-2，3-6は FutureNet NXR シリーズ NXR-230/C Ver5.22.4A
  第4章 FutureNet NXR シリーズ NXR-120/C Ver5.22.5
  show config 形式設定サンプルのバージョンは以下のとおりです。
  FutureNet NXR シリーズ NXR-120/C Ver5.22.5
  ※2-2，3-6のみ FutureNet NXR シリーズ NXR-230/C Ver5.22.4A
  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
1.1.0	第4章 Web 認証設定追加 設定例 show config 形式サンプル追加 送信元 NAT（SNAT）設定のベースを NXR-230/C Ver5.22.4A に変更 DMZ 構築（PPPoE）設定のベースを NXR-230/C Ver5.22.4A に変更 FutureNet サポートデスクへのお問い合わせページ更新

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

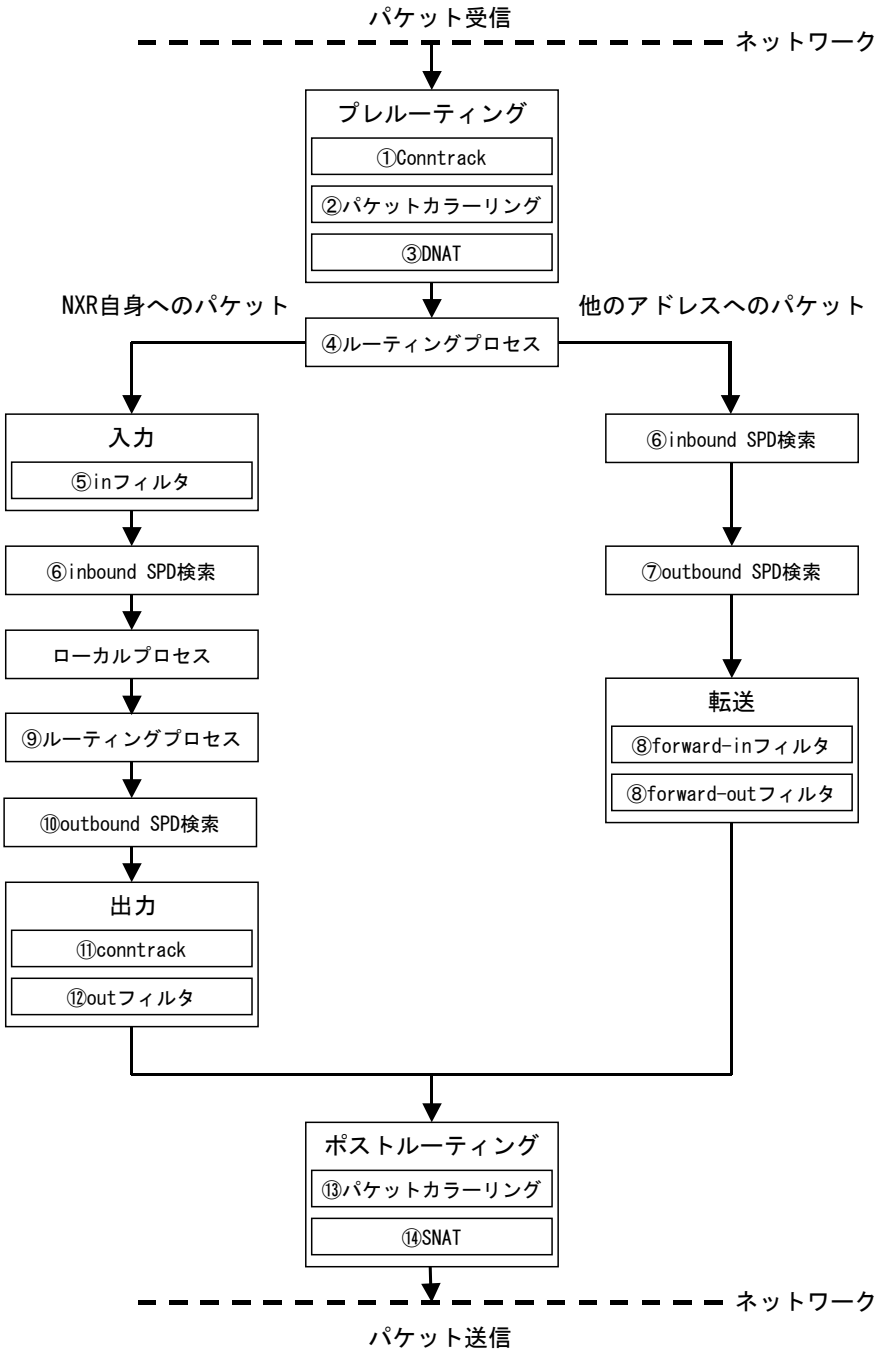
NAT の適用順位は以下のとおりです。

○ 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。

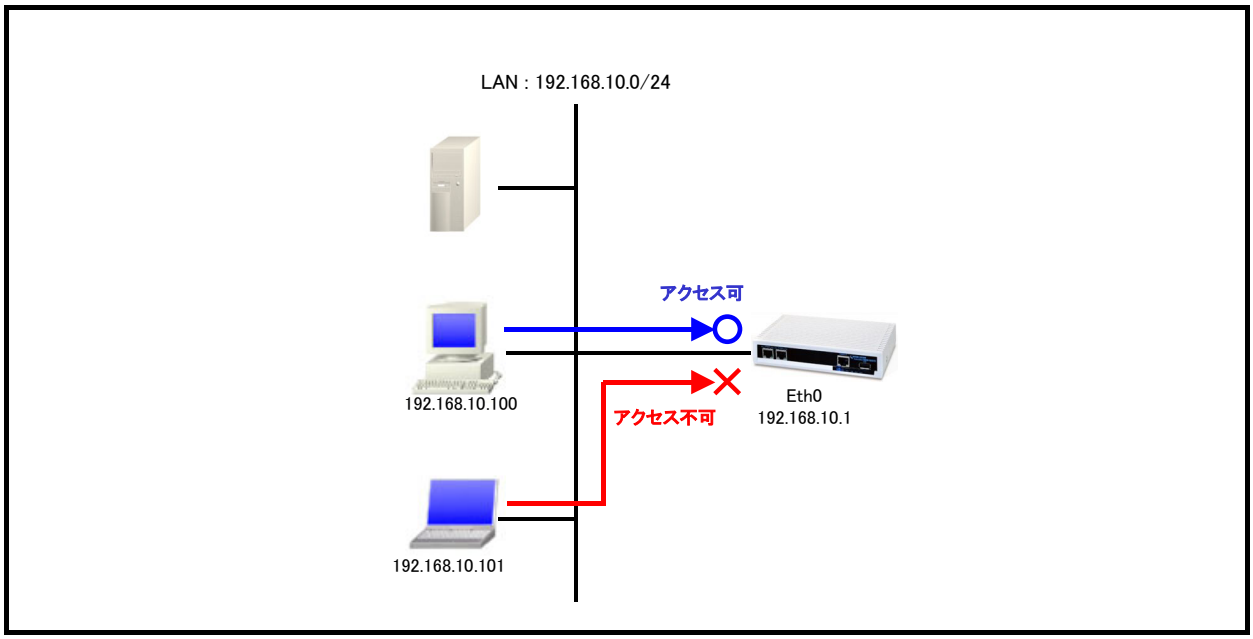
SPD には inbound SPD と outbound SPD があります。受信パケットのポリシチェックには、inbound SPD が検索されます。送信パケットのポリシチェックには、outbound SPD が検索されます。

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
Enter configuration commands, one per line.   End with CNTL/Z.
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設定です。

二行目は宛先 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設定です。

上記が送信元 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。

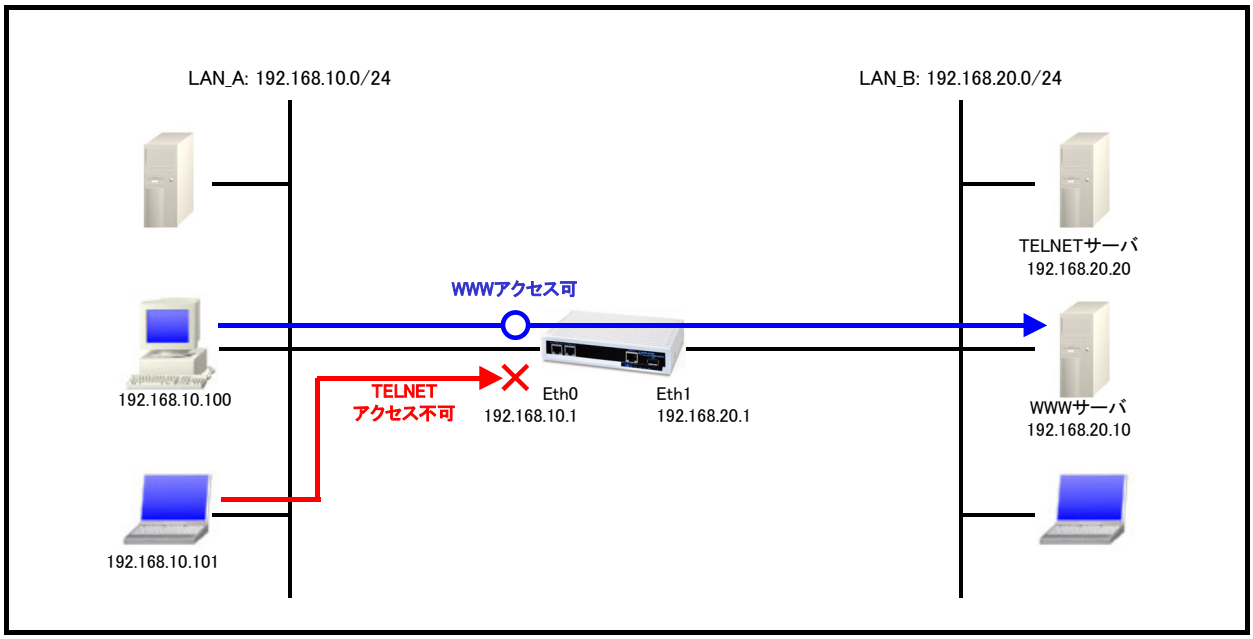
【 パソコンの設定例 】

	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
Enter configuration commands, one per line.   End with CNTL/Z.
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設定です。

二行目は宛先 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。

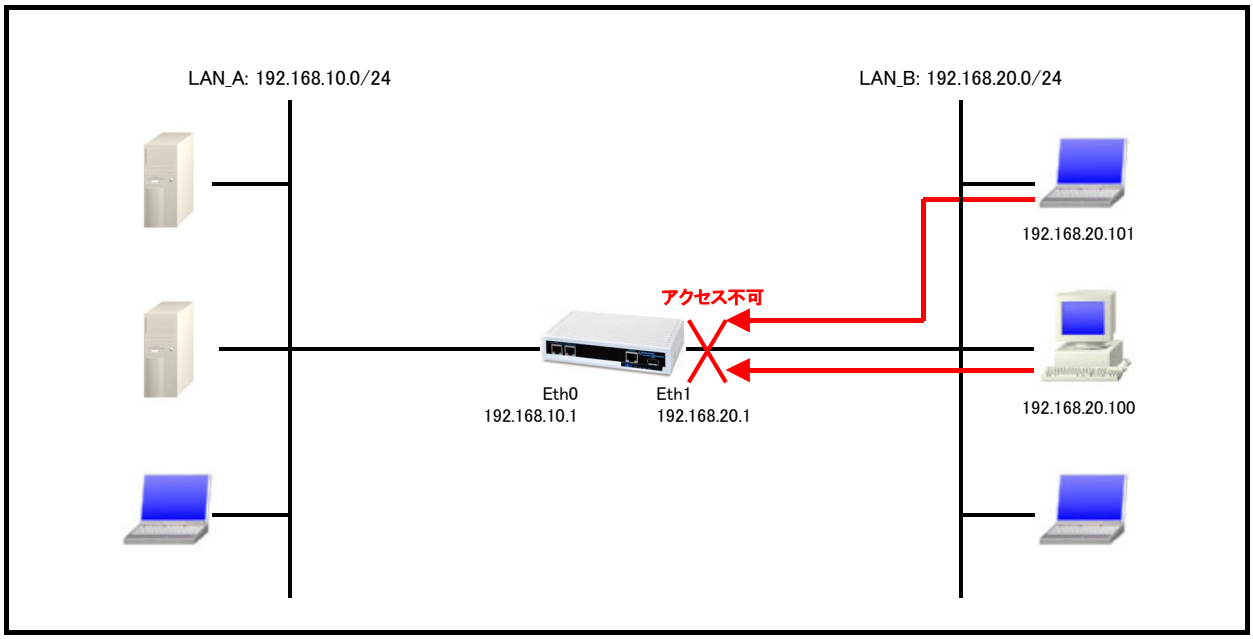
【 サーバ,パソコンの設定例 】

	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
Enter configuration commands, one per line.   End with CNTL/Z.
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。

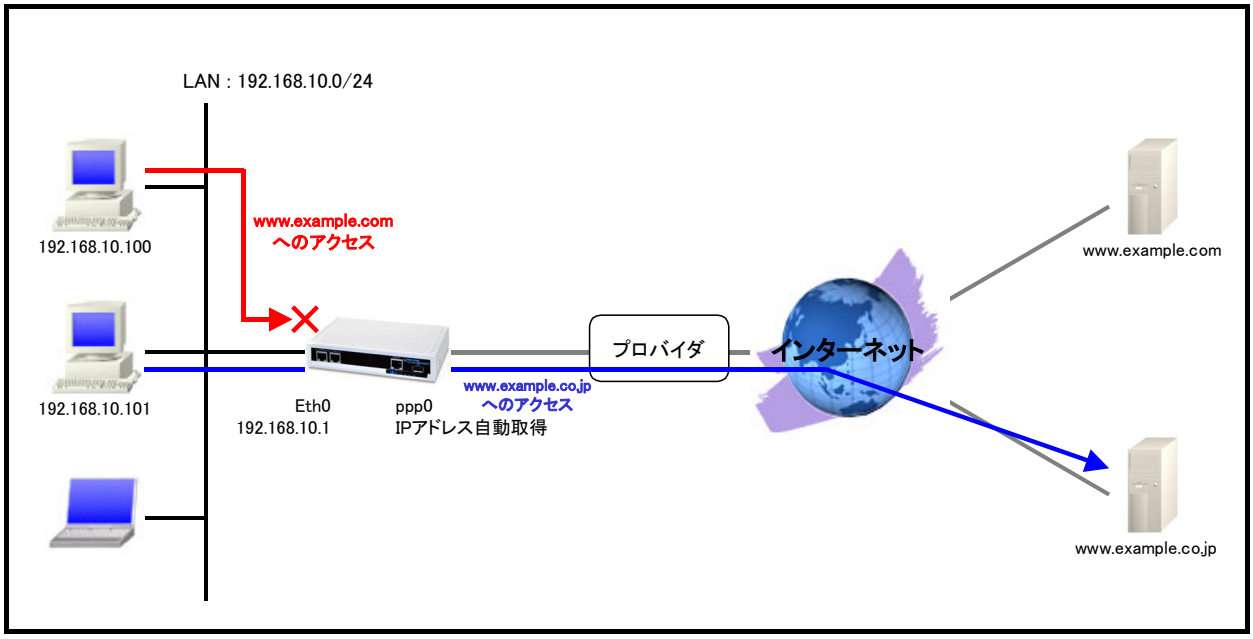
【 パソコンの設定例 】

	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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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。

これは宛先 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。

4. ＜WAN 側（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 】

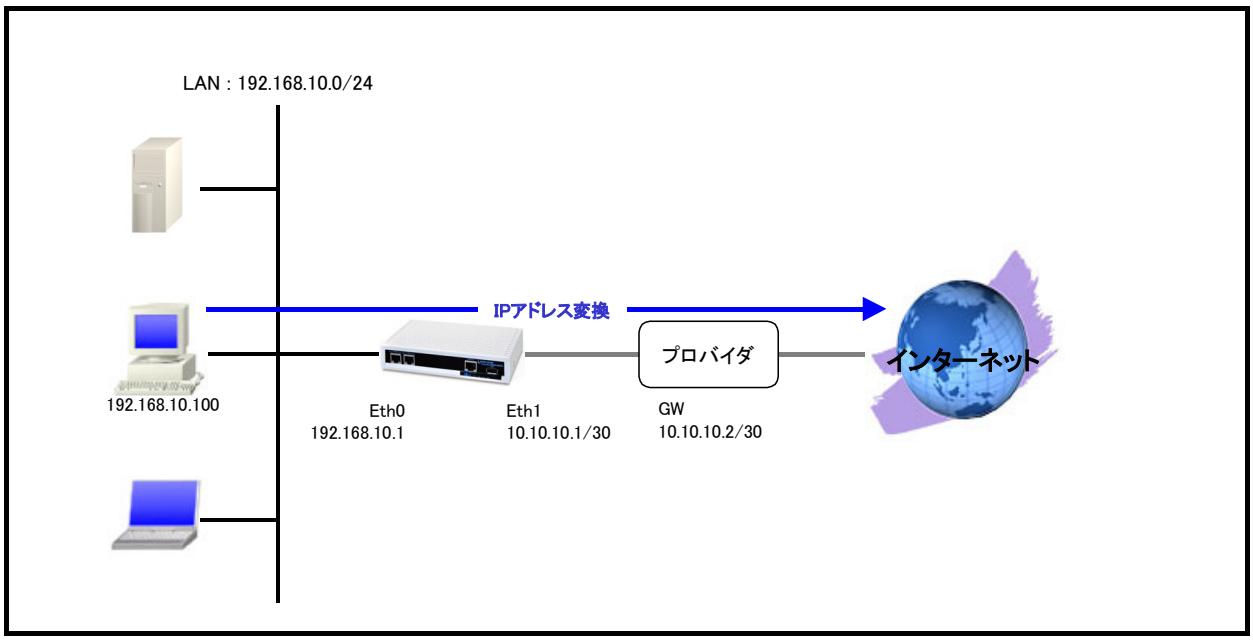
	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1

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
Enter configuration commands, one per line.   End with CNTL/Z.
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 10.10.10.1/30
nxr120(config-if)#ip masquerade
nxr120(config-if)#ip spi-filter
nxr120(config-if)#no ip redirects
nxr120(config-if)#exit
nxr120(config)#ip route 0.0.0.0/0 10.10.10.2
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. ＜LAN 側（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. ＜WAN 側（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。

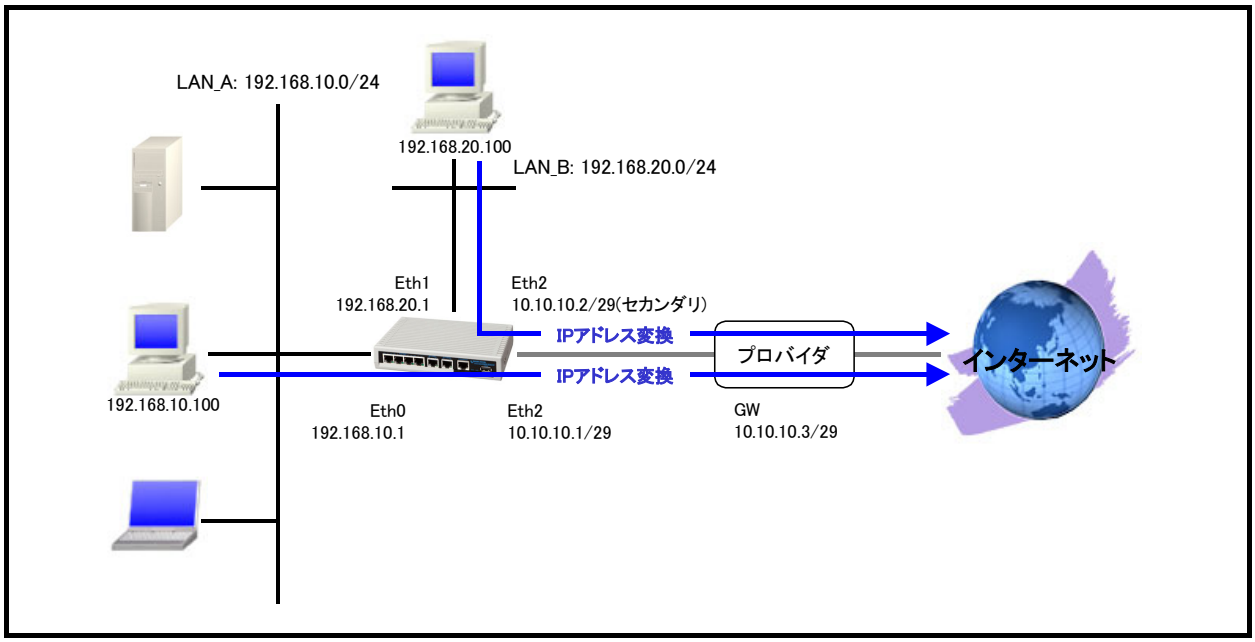
【 パソコンの設定例 】

	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 】

```
nxr230#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr230(config)#interface ethernet 0
nxr230(config-if)#ip address 192.168.10.1/24
nxr230(config-if)#exit
nxr230(config)#interface ethernet 1
nxr230(config-if)#ip address 192.168.20.1/24
nxr230(config-if)#exit
nxr230(config)#ip route 0.0.0.0/0 10.10.10.3
nxr230(config)#ip snat eth2_snat ip 192.168.10.0/24 any 10.10.10.1
nxr230(config)#ip snat eth2_snat ip 192.168.20.0/24 any 10.10.10.2
nxr230(config)#interface ethernet 2
nxr230(config-if)#ip address 10.10.10.1/29
nxr230(config-if)#ip address 10.10.10.2/29 secondary
nxr230(config-if)#ip snat-group eth2_snat
nxr230(config-if)#ip spi-filter
nxr230(config-if)#exit
nxr230(config)#dns
nxr230(config-dns)#service enable
nxr230(config-dns)#root enable
nxr230(config-dns)#exit
nxr230(config)#exit
nxr230#save config
```

【 設定例解説 】

1. ＜LAN 側(ethernet0)インタフェース設定＞

```
nxr230(config)#interface ethernet 0
nxr230(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. ＜LAN 側(ethernet1)インタフェース設定＞

```
nxr230(config)#interface ethernet 1
nxr230(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＞

```
nxr230(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＞

```
nxr230(config)#ip snat eth2_snat ip 192.168.10.0/24 any 10.10.10.1
nxr230(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 に変換する設定です。

二行目は送信元 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. ＜WAN 側(ethernet2)インタフェース設定＞

```
nxr230(config)#interface ethernet 2
nxr230(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。

```
nxr230(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。

```
nxr230(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。

```
nxr230(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＞

```
nxr230(config)#dns
nxr230(config-dns)#service enable
```

DNS サービスを有効に設定します。

```
nxr230(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。

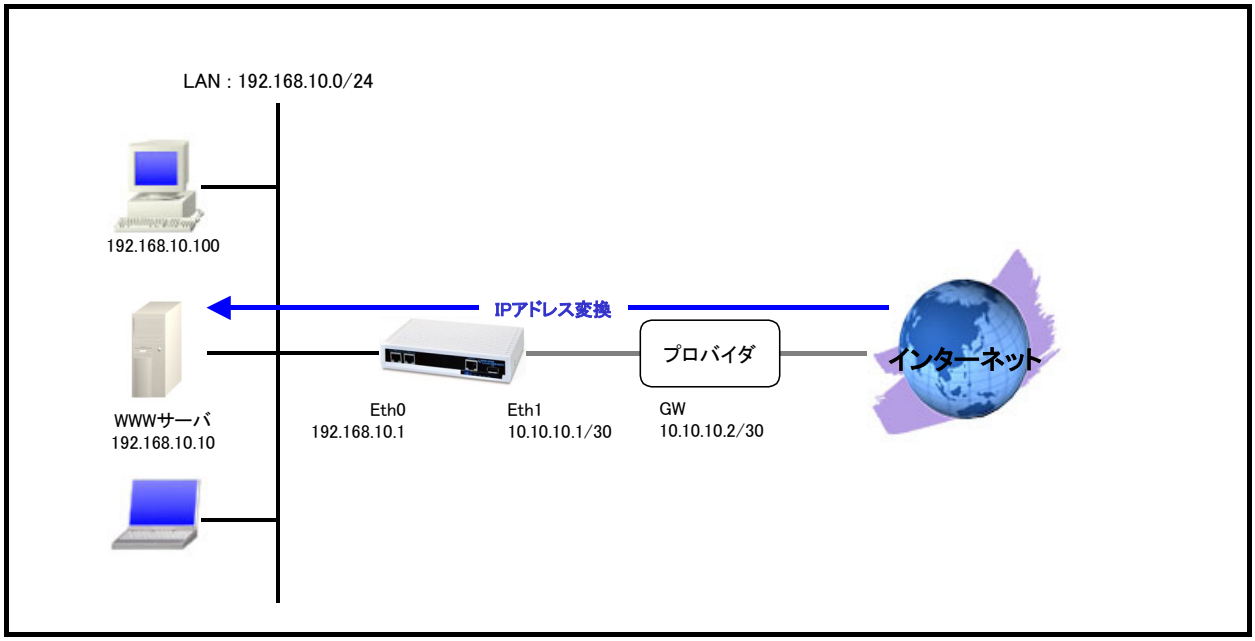
【 パソコンの設定例 】

	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。
この設定例では WWW サーバを DNAT 設定を利用して外部に公開します。

【 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ます。

【 設定例 】

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側(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。

これは宛先 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。

これは宛先 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. ＜WAN 側(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。

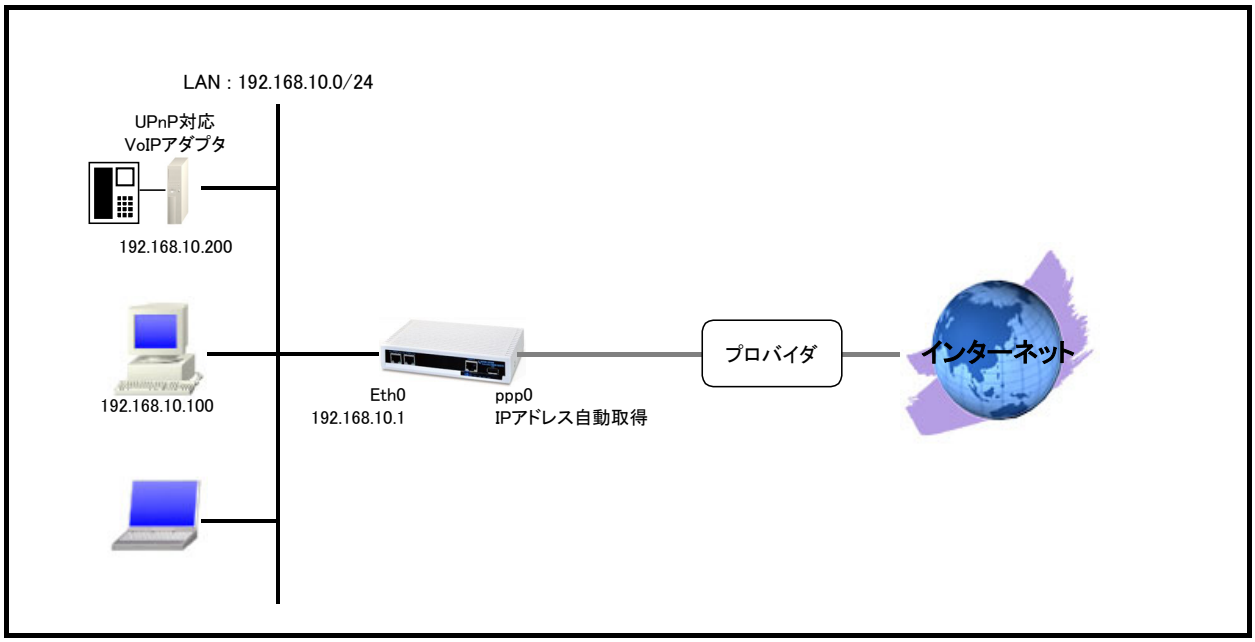
【 サーバ, パソコンの設定例 】

	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 機能を設定することで利用できます。

【 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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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. ＜WAN 側（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 】

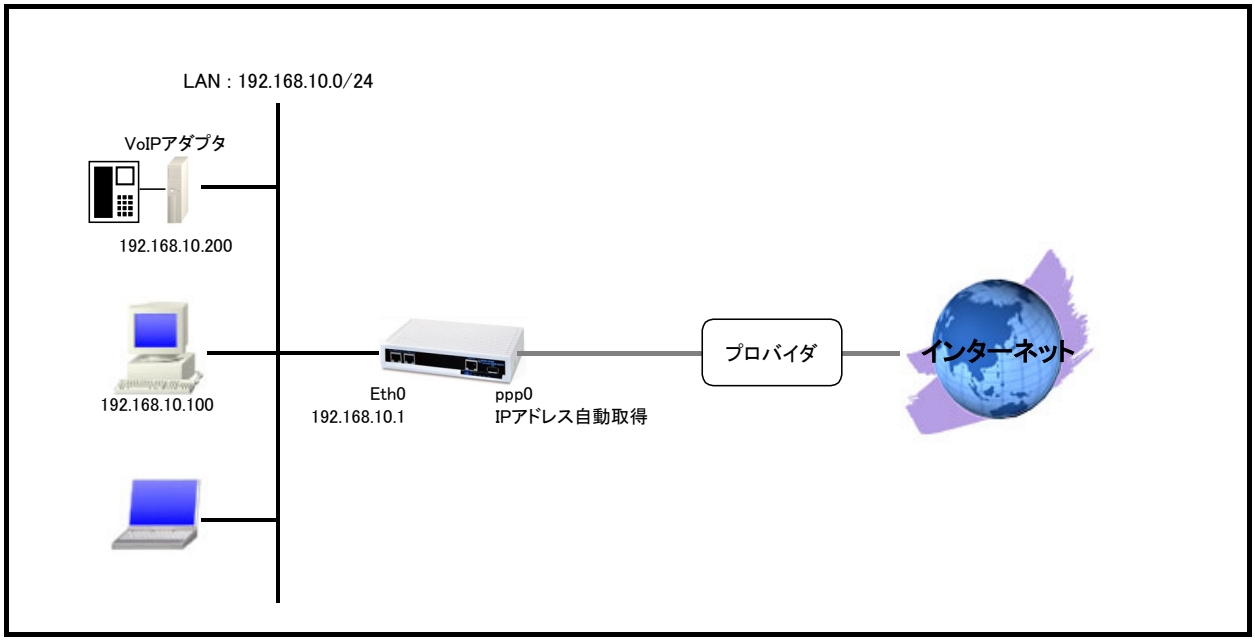
	UPnP 対応パソコン	UPnP 対応 VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1	192.168.10.1

※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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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 に変換する設定です。

二行目は宛先 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設定です。

二行目は宛先 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. ＜WAN 側(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 】

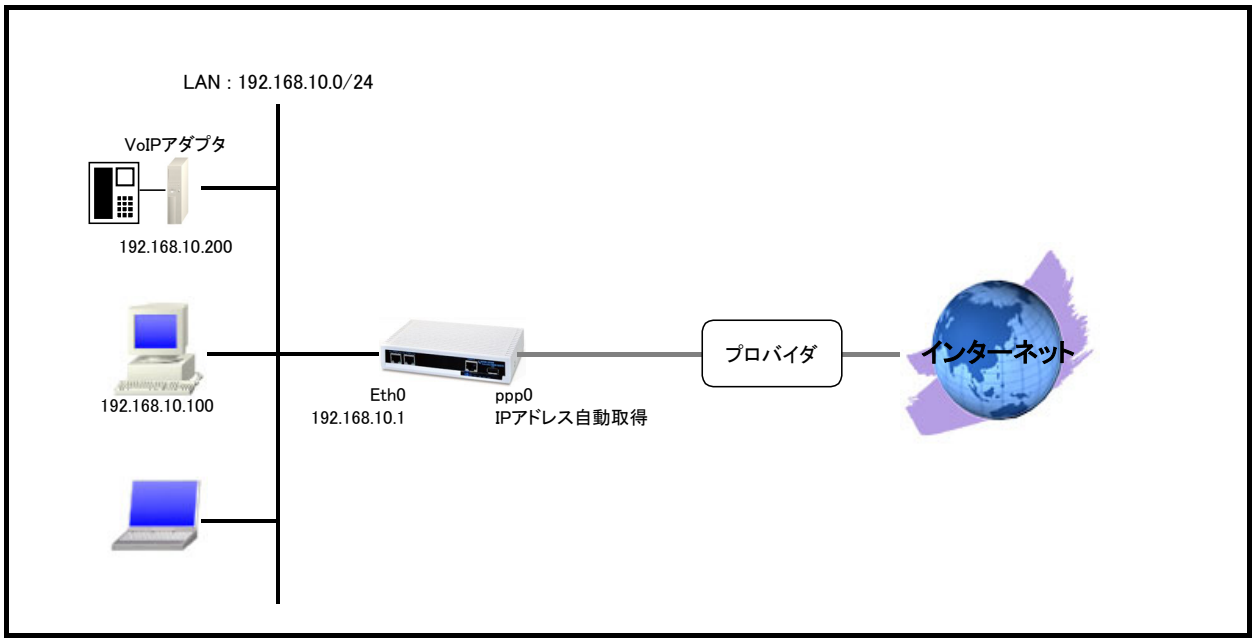
	パソコン	VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1	192.168.10.1

※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
Enter configuration commands, one per line.   End with CNTL/Z.
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 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. ＜LAN 側（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 に変換する設定です。

二行目は宛先 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設定です。

二行目は宛先 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. ＜WAN 側(ppp0)インタフェース設定＞

```
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
```

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＜WAN 側(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

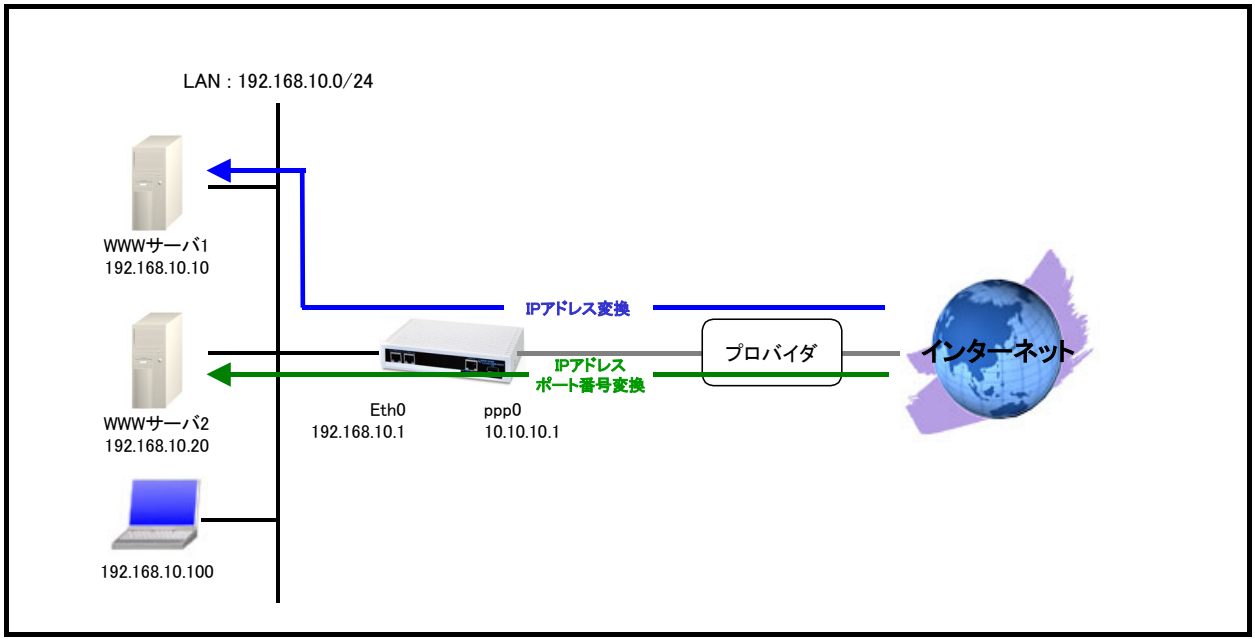
※VoIP アダプタの SIP に関する設定は除く

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 へのアクセスを許可します。
- 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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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 に変換する設定です。

二行目は宛先 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 192.168.10.20 宛先 TCP ポート番号 80 に変換する設定です。

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設定です。

二行目は宛先 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. ＜WAN 側（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。

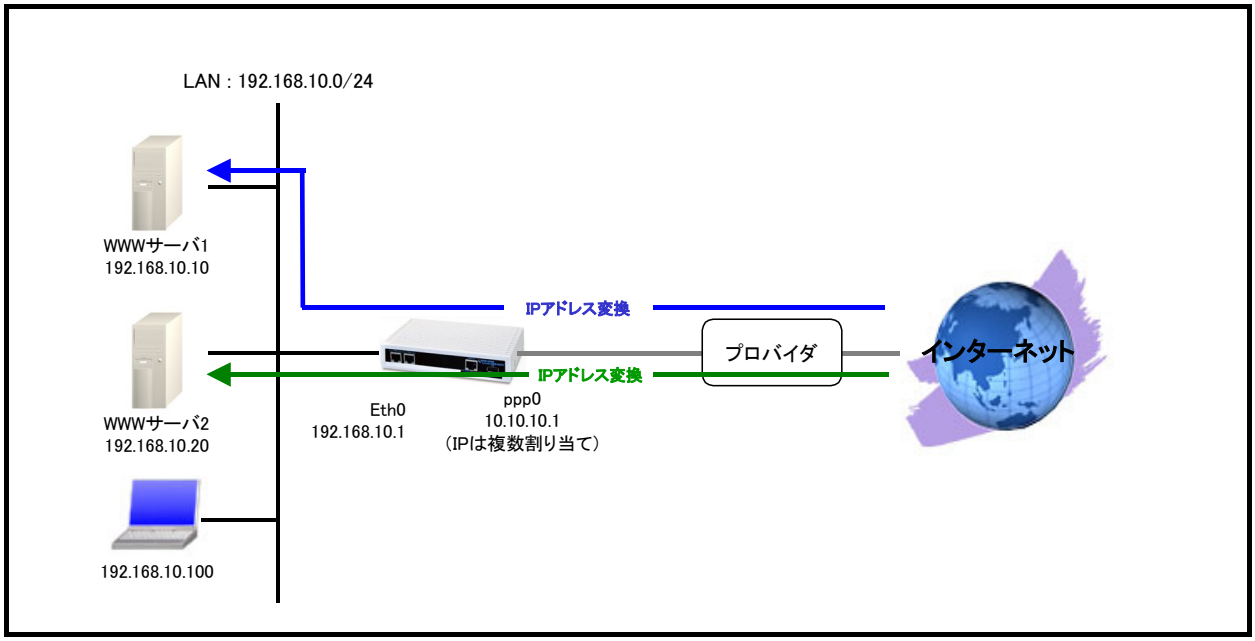
【 パソコンの設定例 】

	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ている場合、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への DNAT を設定することで異なるグローバル IP アドレスでそれぞれのサーバにアクセスさせることができます。ここでは WAN 回線に PPPoE を利用した例となります。

【 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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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 に変換する設定です。

二行目は宛先 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設定です。

二行目は宛先 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. ＜WAN 側（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＜WAN 側（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。

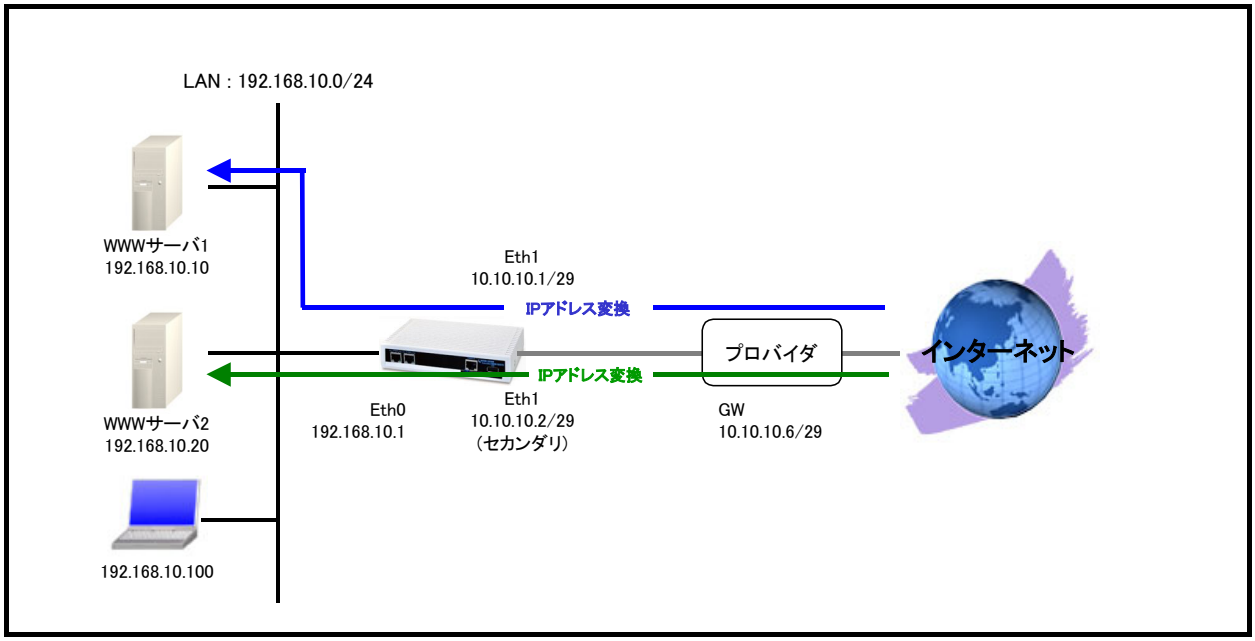
【 サーバ, パソコンの設定例 】

	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ている場合、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への DNAT を設定することで異なるグローバル IP アドレスでそれぞれのサーバにアクセスさせることができます。ここでは WAN 回線に Ethernet を利用した例となります。

【 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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側（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 に変換する設定です。

二行目は宛先 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設定です。

二行目は宛先 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. ＜WAN 側（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。

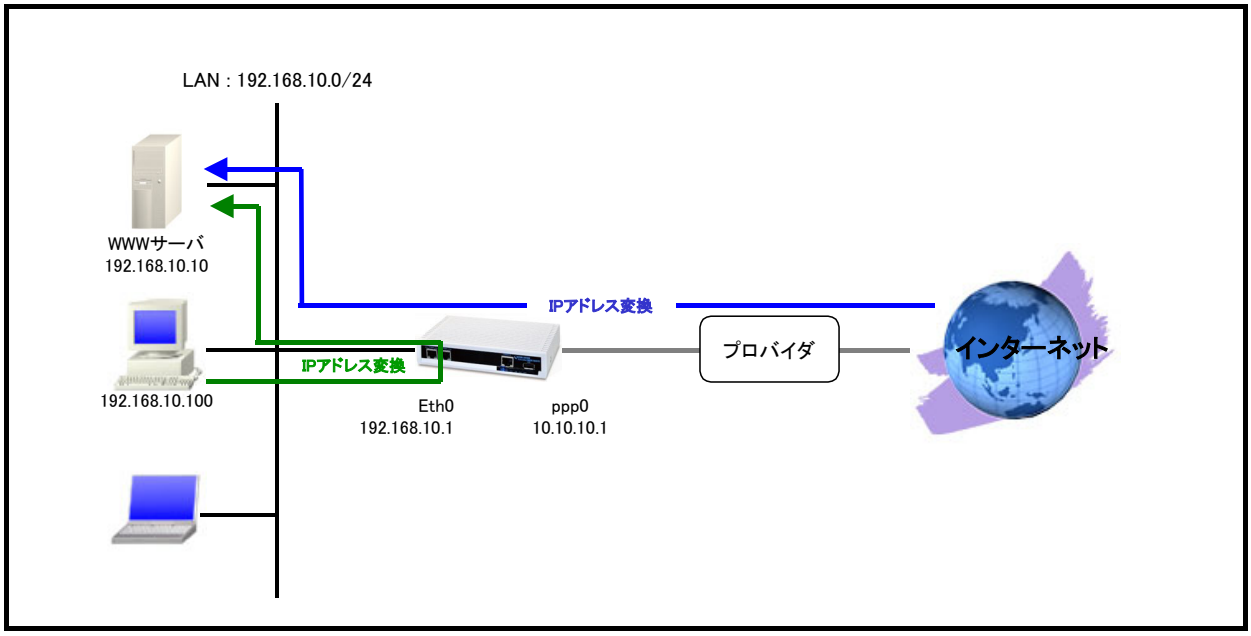
【 サーバ, パソコンの設定例 】

	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。この設定例は NAT を利用して外部に公開している LAN 内の WWW サーバにグローバル IP アドレスでアクセスする設定です。

【 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）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
Enter configuration commands, one per line.   End with CNTL/Z.
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。

このルールでは DNAT ルール名を ppp0_dnat とします。

この設定は宛先 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。

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

このルールでは DNAT ルール名を eth0_dnat とします。

これは送信元 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 に変換する設定です。

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。

これは送信元 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 に変換する設定です。

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. ＜LAN 側（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。

これは宛先 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。

6. ＜WAN 側（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**＜WAN 側（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。

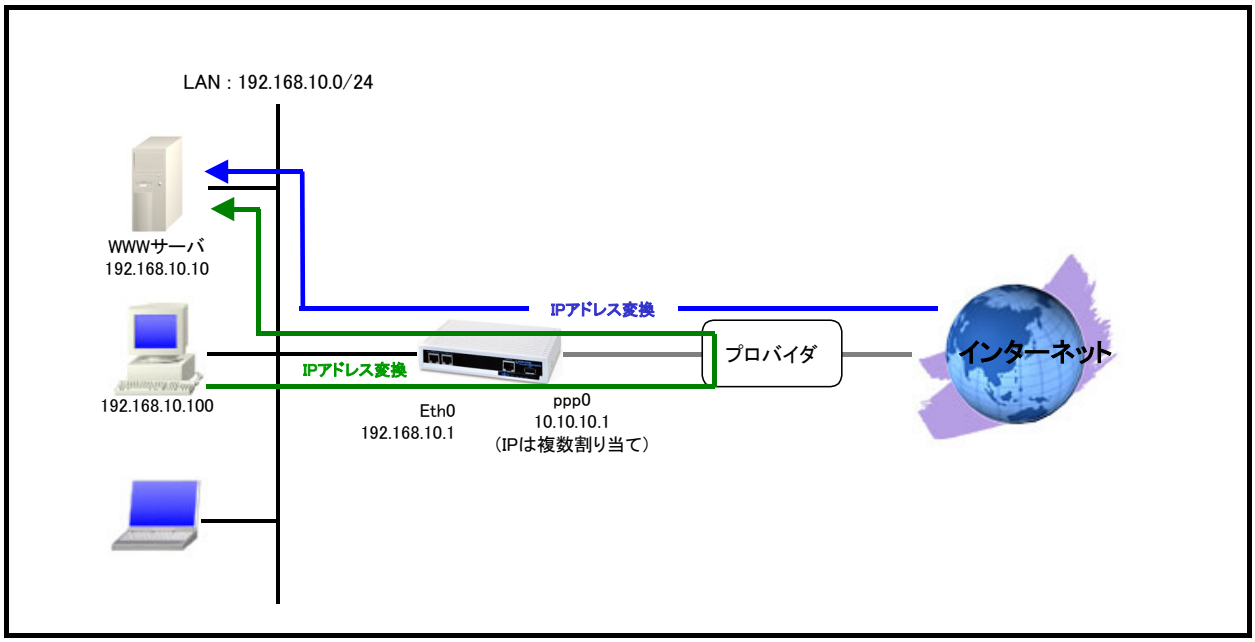
【 サーバ, パソコンの設定例 】

	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	ー	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 NAT 配下の端末よりグローバル IP アドレスでアクセスする設定例です。

【 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なります。
  (☞) 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、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。
- 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。
- 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。
- 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
Enter configuration commands, one per line.   End with CNTL/Z.
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. ＜LAN 側(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。

これは宛先 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
```

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。

これは宛先 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. ＜WAN 側(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。

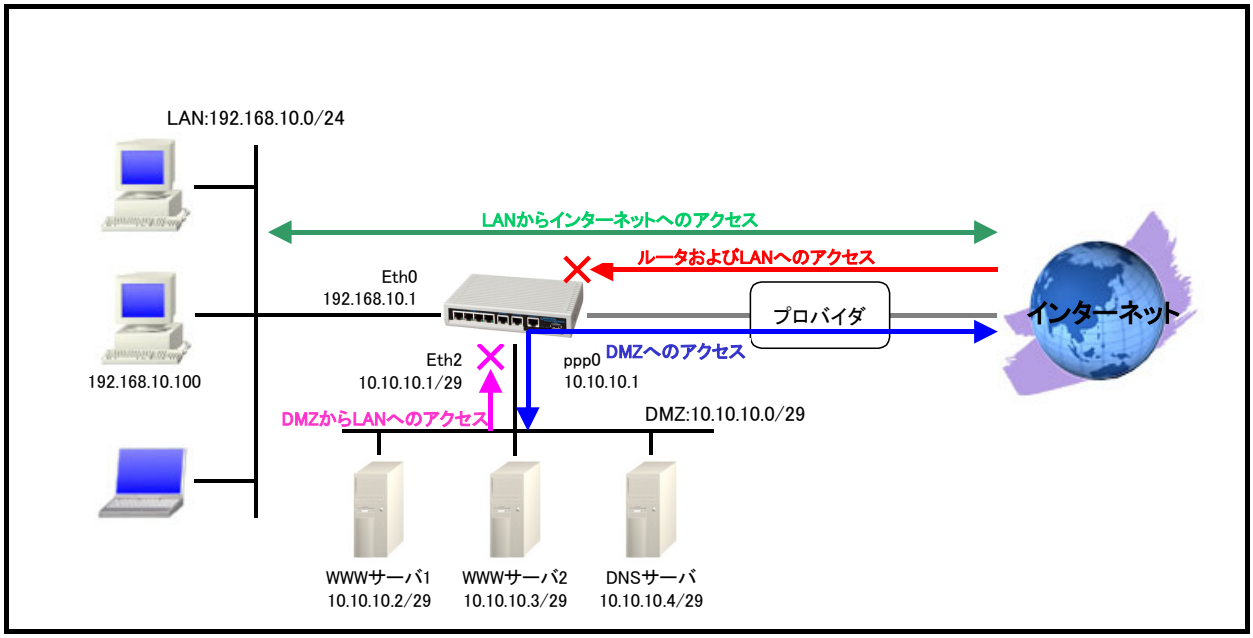
【 サーバ, パソコンの設定例 】

	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	ー	192.168.10.1

3-6. DMZ 構築(PPPoE)設定

NXR-230/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。
- 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原則破棄しますが、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)
    (DNS サーバの名前解決およびゾーン転送用に送信元 10.10.10.4 宛先 TCP,UDP ポート番号 53 を許可)
- 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 機能を有効にし 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 】

```
nxr230#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr230(config)#interface ethernet 0
nxr230(config-if)#ip address 192.168.10.1/24
nxr230(config-if)#exit
nxr230(config)#ip route 0.0.0.0/0 ppp 0
nxr230(config)#ip snat ppp0_snat ip 192.168.10.0/24 any 10.10.10.1
nxr230(config)#ip access-list ppp0_in deny any 10.10.10.1 icmp 8 0
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.2 tcp any 80
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.3 tcp any 80
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 tcp any 53
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 udp any 53
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.0/29 icmp
nxr230(config)#ip access-list ppp0_forward-out permit 10.10.10.4 any tcp any 53
nxr230(config)#ip access-list ppp0_forward-out permit 10.10.10.4 any udp any 53
nxr230(config)#interface ppp 0
nxr230(config-ppp)#ip address 10.10.10.1/32
nxr230(config-ppp)#ip snat-group ppp0_snat
nxr230(config-ppp)#ip access-group in ppp0_in
nxr230(config-ppp)#ip access-group forward-in ppp0_forward-in
nxr230(config-ppp)#ip access-group forward-out ppp0_forward-out
nxr230(config-ppp)#ip spi-filter
nxr230(config-ppp)#ip tcp adjust-mss auto
nxr230(config-ppp)#no ip redirects
nxr230(config-ppp)#ppp username test1@centurysys password test1pass
nxr230(config-ppp)#exit
nxr230(config)#interface ethernet 1
nxr230(config-if)#no ip address
nxr230(config-if)#pppoe-client ppp 0
nxr230(config-if)#exit
nxr230(config)#interface ethernet 2
nxr230(config-if)#ip address 10.10.10.1/29
nxr230(config-if)#ip spi-filter
nxr230(config-if)#exit
nxr230(config)#dns
nxr230(config-dns)#address 10.10.10.4
nxr230(config-dns)#service enable
nxr230(config-dns)#exit
nxr230(config)#exit
nxr230#save config
```

【 設定例解説 】

1. ＜LAN 側(ethernet0)インタフェース設定＞

```
nxr230(config)#interface ethernet 0
nxr230(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＞

```
nxr230(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＞

```
nxr230(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。

これは送信元 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 に変換する設定です。

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＞

```
nxr230(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。

これは宛先 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。

```
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.2 tcp any 80
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.3 tcp any 80
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 tcp any 53
nxr230(config)#ip access-list ppp0_forward-in permit any 10.10.10.4 udp any 53
nxr230(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設定です。

二行目は宛先 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設定です。

三行目は宛先 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設定です。

四行目は宛先 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設定です。

五行目は宛先 IP アドレス 10.10.10.0/29 の ICMP パケットを許可する設定です。

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。

```
nxr230(config)#ip access-list ppp0_forward-out permit 10.10.10.4 any tcp any 53
nxr230(config)#ip access-list ppp0_forward-out permit 10.10.10.4 any udp any 53
```

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

一行目は送信元 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設定です。

二行目は送信元 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. ＜WAN 側(ppp0)インタフェース設定＞

```
nxr230(config)#interface ppp 0
```

ppp0 インタフェースを設定します。

```
nxr230(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。

```
nxr230(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。

```
nxr230(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。

```
nxr230(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。

```
nxr230(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 ppp0 インタフェースから送信する 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。

```
nxr230(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。

```
nxr230(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。

```
nxr230(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
nxr230(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＞

```
nxr230(config)#interface ethernet 1
nxr230(config-if)#no ip address
nxr230(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. ＜DMZ 側(ethernet2)インタフェース設定＞

```
nxr230(config)#interface ethernet 2
nxr230(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。

```
nxr230(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＞

```
nxr230(config)#dns
nxr230(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。

```
nxr230(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

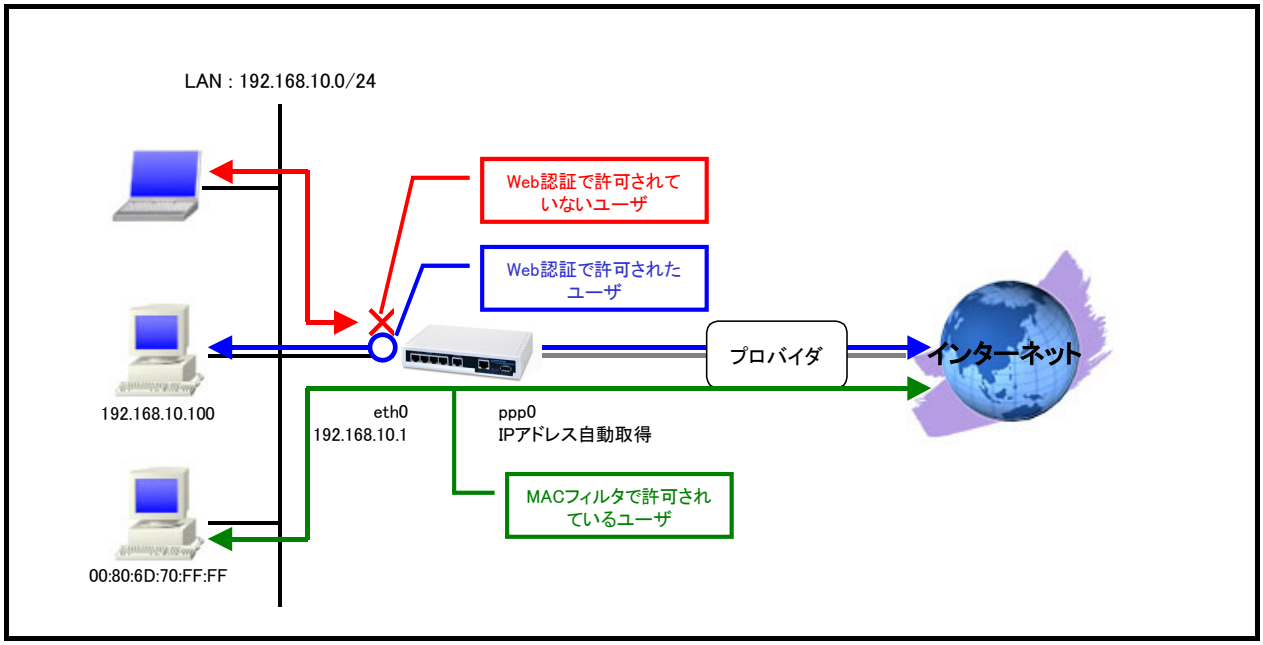
LAN	パソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバの IP アドレス	192.168.10.1

4. Web 認証設定

4-1. ユーザ認証設定

Web 認証では NXR 経由で通信を行う際にユーザ ID，パスワードによる認証を必要とするよう設定することが可能です。これにより外部へアクセスできるユーザを制限し認証が成功したユーザのみインターネットアクセスを許可するといった利用方法が可能になります。

【 構成図 】



- NXR 配下の端末は NXR の Web 認証画面でユーザ ID，パスワードを入力し認証で許可された場合のみ NXR 経由で通信することが可能です。
- Web 認証機能の MAC アクセスリストを設定することで MAC アドレス単位で認証を必要とせずに通信の許可または拒否することができます。
- 認証後許可されたユーザとの間で無通信状態となってから一定時間経過すると通信が遮断されるよう設定します。
- PPPoE はイーサネットインタフェース上で PPP セッションを確立するため、PPP インタフェースを指定したイーサネットインタフェースで利用するための登録が必要になります。
- 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。
- 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
Enter configuration commands, one per line.   End with CNTL/Z.
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)#system led aux 1 interface ppp 0
nxr120(config)#web-authenticate
nxr120(config-webauth)#authenticate basic
nxr120(config-webauth)#close idle-timeout 600
nxr120(config-webauth)#log enable
nxr120(config-webauth)#account username test password testpass
nxr120(config-webauth)#mac access-list permit 00:80:6D:70:FF:FF ethernet 0
nxr120(config-webauth)#exit
% restart http-server to apply this setting.
nxr120(config)#exit
nxr120#restart http-server
http-server starting... done
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. ＜LAN 側(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
```

LAN 側(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。ゲートウェイとして ppp0 インタフェースを指定します。

3. ＜WAN 側(ppp0)インタフェース設定＞

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

WAN 側(ppp0)インタフェースを設定します。

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

IP アドレスを設定します。

本設定例では動的 IP アドレスが割り当てられるため、IP アドレスとして negotiated を設定します。

(☞) IP アドレスに negotiated を設定した場合は、プロバイダ等から払い出された IP アドレス(IPCP で取得した IP アドレス)を利用します。

```
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。

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 アドレスはイーサネット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. ＜システム LED 設定＞

```
nxr120(config)#system led aux 1 interface ppp 0
```

ここでは ppp0 インタフェースの回線接続時に、AUX LED1が点灯するように設定します。

6. ＜Web 認証設定＞

```
nxr120(config)#web-authenticate
```

Web 認証を設定します。

```
nxr120(config-webauth)#authenticate basic
```

Web 認証(Basic 認証)を行うよう設定します。

```
nxr120(config-webauth)#close idle-timeout 600
```

Web 認証後の接続許可時間を設定します。

ここでは認証で許可されたユーザからの通信が無通信状態となってから 600 秒経過すると通信が遮断されるよう設定します。

```
nxr120(config-webauth)#log enable
```

ログの取得を有効にします。

```
nxr120(config-webauth)#account username test password testpass
```

ローカル認証用のユーザ名、パスワードを設定します。

ここではユーザ名を test、パスワードを testpass とします。

```
nxr120(config-webauth)#mac access-list permit 00:80:6D:70:FF:FF ethernet 0
```

Web 認証機能を有効にすると外部との通信には認証が必要になりますが、MAC アクセスリストで指定した MAC アドレスを持つ端末については認証を必要とせずに通信を許可または拒否することができます。

ここでは MAC アドレス 00:80:6D:70:FF:FF について Ethernet0 インタフェースで許可するよう設定します。

7. ＜HTTP サーバ再起動＞

```
nxr120#restart http-server
```

Web 認証機能を有効にする場合は HTTP サーバを起動する必要があります。

デフォルトでは HTTP サーバは起動状態になっていますので、ここでは HTTP サーバの再起動を行います。

8. ＜DNS 設定＞

```
nxr120(config)#dns
```

DNS を設定します。

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

DNS サービスを有効にします。

この設定により NXR の DNS リレーおよび DNS キャッシュ機能を利用することが可能です。

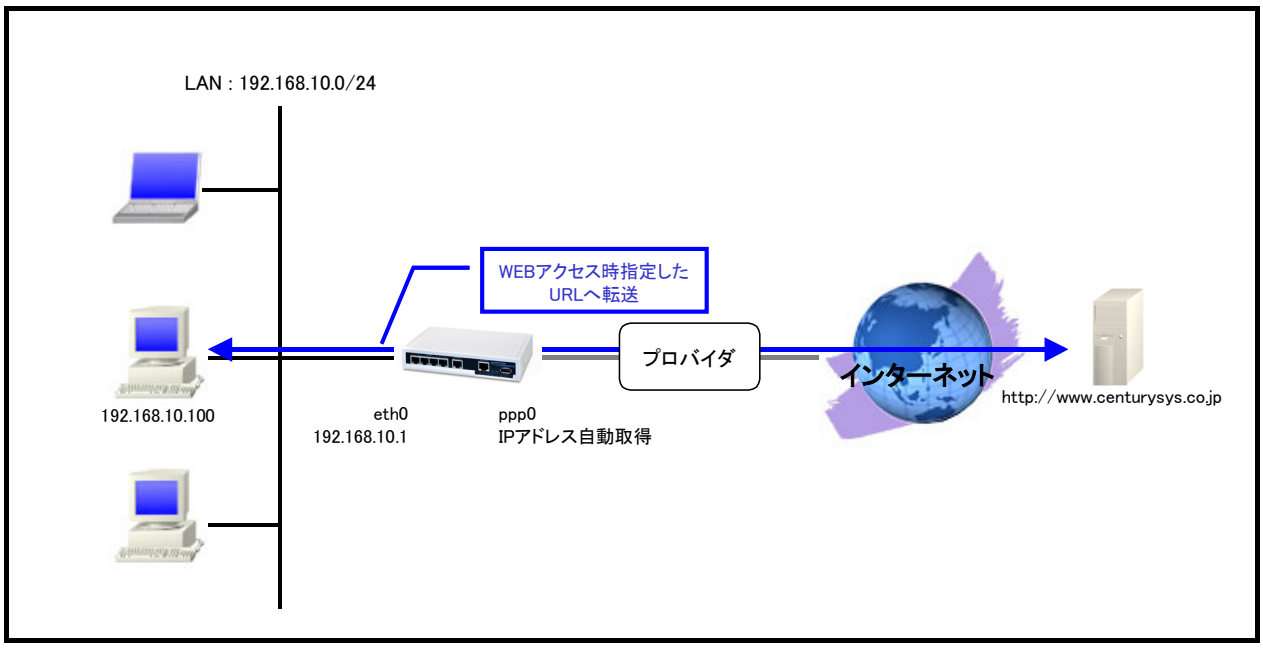
【 パソコンの設定例 】

	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

4-2. URL 転送設定

Web 認証機能では単にユーザ認証という用途だけではなく、NXR 配下の端末が WEB アクセスを行った際に NXR で設定した任意の URL へ転送させるといったことも可能です。

【 構成図 】



- NXR 配下の端末が NXR 経由で TCP ポート 80 番での Web アクセスを行った際に指定した URL へ一度転送します。
- 指定した URL へ転送(強制認証)後、そのユーザとの間で無通信状態となってから一定時間経過すると再度 Web アクセスを行った際に指定した URL へ転送します。
- PPPoE はイーサネットインタフェース上で PPP セッションを確立するため、PPP インタフェースを指定したイーサネットインタフェースで利用するための登録が必要になります。
- 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。
- 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
Enter configuration commands, one per line.   End with CNTL/Z.
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)#system led aux 1 interface ppp 0
nxr120(config)#web-authenticate
nxr120(config-webauth)#monitor port 80 redirect
nxr120(config-webauth)#redirect-url http://www.centurysys.co.jp
nxr120(config-webauth)#close idle-timeout 600
nxr120(config-webauth)#log enable
nxr120(config-webauth)#exit
% restart http-server to apply this setting.
nxr120(config)#exit
nxr120#restart http-server
http-server starting... done
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

(☞) ここに記載のない設定項目は、4-1. ユーザ認証設定が参考になりますので、そちらをご参照下さい。

1. ＜Web 認証設定＞

```
nxr120(config)#web-authenticate
```

Web 認証を設定します。

```
nxr120(config-webauth)#monitor port 80 redirect
```

NXR 配下の未認証端末から NXR 経由で Web アクセスする際、Web 認証なしで指定した URL へ転送します。

```
nxr120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

ここでは http://www.centurysys.co.jp に転送します。

```
nxr120(config-webauth)#close idle-timeout 600
```

Web 認証（URL 転送）後の接続許可時間を設定します。

ここではユーザとの間で無通信状態となってから 600 秒経過後、Web アクセスした際に再度指定した URL へ転送するよう設定します。

```
nxr120(config-webauth)#log enable
```

ログの取得を有効にします。

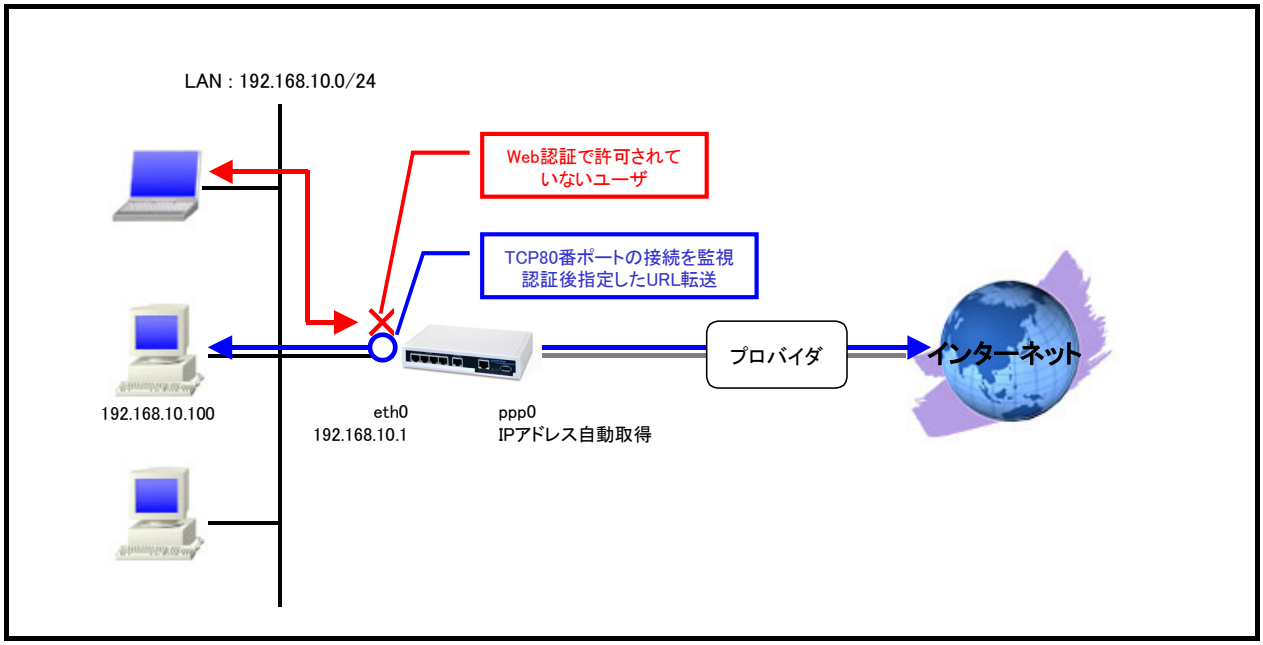
【 パソコンの設定例 】

	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

4-3. ユーザ強制認証＋URL 転送

Web 認証機能では通常外部に接続したいユーザは認証 URL へのアクセスが必要となりますが、強制認証機能では TCP80 番ポートへの接続を監視し未認証ユーザからの接続があった場合強制的に Web 認証を行います。なお本設定例ではユーザ認証成功後、NXR で設定した URL へ転送を行います。

【 構成図 】



- Web 認証機能で TCP ポート 80 番への接続を監視し、接続があった際に認証画面をポップアップするように設定することが可能です。本設定例ではユーザ認証成功後、指定した URL へ一度転送します。
- 認証後許可されたユーザとの間で無通信状態となってから一定時間経過すると通信が遮断されるよう設定します。
- PPPoE はイーサネットインタフェース上で PPP セッションを確立するため、PPP インタフェースを指定したイーサネットインタフェースで利用するための登録が必要になります。
- 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。
- 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
Enter configuration commands, one per line.   End with CNTL/Z.
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)#system led aux 1 interface ppp 0
nxr120(config)#web-authenticate
nxr120(config-webauth)#authenticate basic
nxr120(config-webauth)#monitor port 80 redirect
nxr120(config-webauth)#redirect-url http://www.centurysys.co.jp
nxr120(config-webauth)#close idle-timeout 600
nxr120(config-webauth)#log enable
nxr120(config-webauth)#account username test password testpass
nxr120(config-webauth)#exit
% restart http-server to apply this setting.
nxr120(config)#exit
nxr120#restart http-server
http-server starting... done
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

(☞) ここに記載のない設定項目は、4-1. ユーザ認証設定が参考になりますので、そちらをご参照下さい。

1. ＜Web 認証設定＞

```
nxr120(config)#web-authenticate
```

Web 認証を設定します。

```
nxr120(config-webauth)#authenticate basic
```

Web 認証(Basic 認証)を行うよう設定します。

```
nxr120(config-webauth)#monitor port 80 redirect
```

NXR 配下の未認証端末から NXR 経由で Web アクセスする際、Web 認証画面がポップアップし、認証後に指定した URL へ転送します。

```
nxr120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

ここでは http://www.centurysys.co.jp に転送します。

```
nxr120(config-webauth)#close idle-timeout 600
```

Web 認証後の接続許可時間を設定します。

ここでは認証で許可されたユーザからの通信が無通信状態となってから 600 秒経過すると通信が遮断されるよう設定します。

```
nxr120(config-webauth)#log enable
```

ログの取得を有効にします。

```
nxr120(config-webauth)#account username test password testpass
```

ローカル認証用のユーザ名、パスワードを設定します。

ここではユーザ名を test、パスワードを testpass とします。

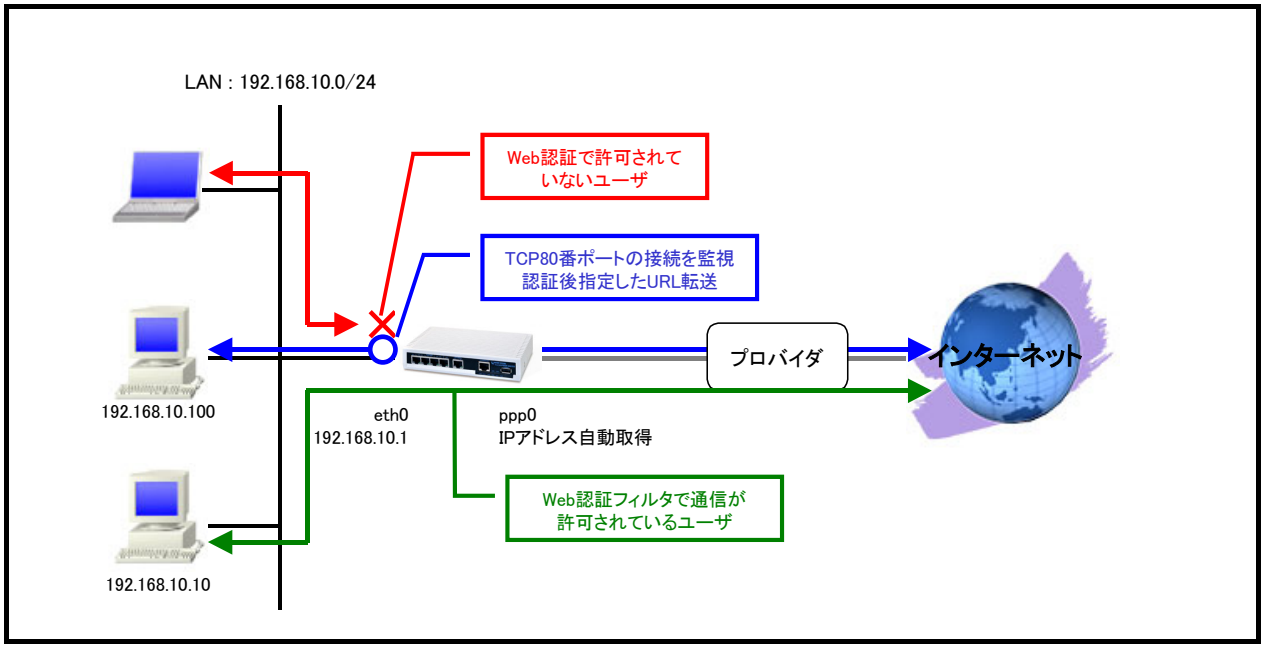
【 パソコンの設定例 】

	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

4-4. Web 認証フィルタ

Web 認証フィルタを設定することによりある特定のホスト，ネットワーク，インタフェースで Web 認証せずに通信が可能となります。

【 構成図 】



- Web 認証フィルタの動作を規定するルールリストを作成します。
- Web 認証アクセスリスト名 : eth0_web_forward-in
  - 送信元 IP アドレス 192.168.10.10 のパケットを許可します。
- この設定例では Web 認証機能で TCP ポート 80 番への接続を監視し、接続があった際に認証画面がポップアップするようにし、ユーザ認証成功後、指定した URL へ転送します。
- 認証後許可されたユーザからの通信が無通信状態となってから一定時間経過すると通信が遮断されるよう設定します。

【 設定例 】

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#ip web-auth access-list eth0_web_forward-in permit 192.168.10.10 any
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip address 192.168.10.1/24
nxr120(config-if)#ip webauth-filter forward-in eth0_web_forward-in
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)#system led aux 1 interface ppp 0
nxr120(config)#web-authenticate
nxr120(config-webauth)#authenticate basic
nxr120(config-webauth)#monitor port 80 redirect
nxr120(config-webauth)#redirect-url http://www.centurysys.co.jp
nxr120(config-webauth)#close idle-timeout 600
nxr120(config-webauth)#log enable
nxr120(config-webauth)#account username test password testpass
nxr120(config-webauth)#exit
% restart http-server to apply this setting.
nxr120(config)#exit
nxr120#restart http-server
http-server starting... done
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

(☞) ここに記載のない設定項目は、4-3. ユーザ強制認証＋URL 転送が参考になりますので、そちらをご参照下さい。

1. ＜Web 認証アクセスリスト＞

```
nxr120(config)#ip web-auth access-list eth0_web_forward-in permit 192.168.10.10 any
```

Web 認証アクセスリストを設定します。

これは送信元 IP アドレス 192.168.10.10 のパケットを許可する設定です。

この Web 認証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。

(☞) Web 認証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。

```
nxr120(config)#interface ethernet 0
nxr120(config-if)#ip webauth-filter forward-in eth0_web_forward-in
```

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。

Web 認証アクセスリスト設定で設定した eth0_web_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 を経由するパケットに対して Web 認証アクセスリストによるチェックが行われます。

【 パソコンの設定例 】

	パソコン
IP アドレス	192.168.10.10
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)を確認する場合は、show ip access-list コマンドを使用します。

<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 アクセスリスト設定は行っているが、その IP 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 references 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 の状態を確認する場合は、それぞれ以下のコマンドを使用します。

<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 のルール設定は行っているが、その DNAT,SNAT ルールが属している 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 references 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 の状態を確認する場合は、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 の状態を確認する場合は、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 NXR のセッション情報を表示する場合は、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.
```

Web 認証機能のユーザ認証方法について

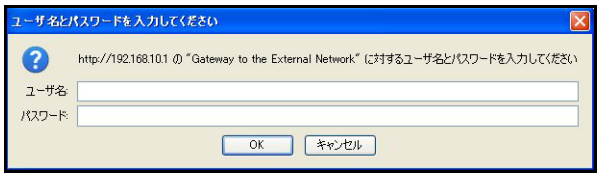
Web 認証使用時に NXR 経由での通信を行うには原則ユーザ認証が必要となります。
(URL 転送のみの利用、Web 認証を含むフィルタ、MAC フィルタは除く)

ユーザ認証の手順は以下のとおりです。

- ユーザ認証

  1. 端末から NXR の Web 認証画面にアクセスします。
     アクセスする際は以下のような形式で URL を指定します。
     http://<本装置の IP アドレス>/login.cgi
     <入力例>
     http://192.168.10.1/login.cgi

  2. アクセス後、認証画面がポップアップしますのでユーザ ID, パスワードを入力します。



  3. 認証成功時には以下のようなメッセージが表示され、NXR 経由でのアクセスが可能になります。
     You can connect to the External Network (test@192.168.10.100).
     Date: Tue Jan 1 12:00:00 2013

- ユーザ強制認証
  ユーザ強制認証では端末から NXR の Web 認証画面にアクセスすることなく TCP80 番ポートへの接続を監視し、未認証ユーザからの接続があった場合強制的に Web 認証画面をポップアップします。
  認証画面ポップアップ後はユーザ認証と同様の手順となります。

設定例 show config 形式サンプル

1-1. 入力(in)フィルタ設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
 ip address 192.168.10.1/24
 ip access-group in eth0_in
!
interface ethernet 1
 no ip address
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip access-list eth0_in permit 192.168.10.100 192.168.10.1 tcp any 23
ip access-list eth0_in deny any 192.168.10.1 tcp any 23
!
!
!
end
```

1-2. 転送(forward-in,forward-out)フィルタ設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
  ip address 192.168.10.1/24
  ip access-group forward-in eth0_forward-in
!
interface ethernet 1
  ip address 192.168.20.1/24
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip access-list eth0_forward-in permit any 192.168.20.10 tcp any 80
ip access-list eth0_forward-in deny any 192.168.20.20 tcp any 23
!
!
!
end
```

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

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
  ip address 192.168.10.1/24
!
interface ethernet 1
  ip address 192.168.20.1/24
  ip spi-filter
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
!
!
end
```

1-4. FQDN フィルタ設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-out ppp0_forward-out
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-out deny any www.example.com tcp any 80
!
!
!
end
```

2-1. IP マスカレード設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
  ip address 192.168.10.1/24
!
interface ethernet 1
  ip address 10.10.10.1/30
  no ip redirects
  ip masquerade
  ip spi-filter
!
dns
  service enable
  root enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.2
!
!
!
end
```

2-2. 送信元 NAT(SNAT)設定

```
!
! Century Systems NXR-230 Series ver 5.22.4A (build 5/17:42 23 04 2013)
!
hostname nxr230
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 192.168.20.1/24
!
interface ethernet 2
 ip address 10.10.10.1/29
 ip address 10.10.10.2/29 secondary
 ip snat-group eth2_snat
 ip spi-filter
!
dns
 service enable
 root enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.3
!
!
ip snat eth2_snat ip 192.168.10.0/24 any 10.10.10.1
ip snat eth2_snat ip 192.168.20.0/24 any 10.10.10.2
!
!
end
```

2-3. 宛先 NAT(DNAT)設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
  ip address 192.168.10.1/24
!
interface ethernet 1
  ip address 10.10.10.1/30
  ip access-group forward-in eth1_forward-in
  ip masquerade
  ip dnat-group eth1_dnat
  ip spi-filter
!
dns
  service enable
  root enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.2
!
ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
!
!
ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
!
!
end
```

2-4. UPnP 設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
upnp
 service enable
 external interface ppp 0
 listen ip 192.168.10.1/24
 timeout 3600
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
!
!
end
```

2-5. SIP-NAT 設定1

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
sip-nat enable
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5060
ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
!
!
ip dnat ppp0_dnat udp any any any 5060 192.168.10.200
ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
!
!
end
```

2-6. SIP-NAT 設定2

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
sip-nat enable
sip-nat port 5060 5064
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5064
ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
!
!
ip dnat ppp0_dnat udp any any any 5064 192.168.10.200
ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
!
!
end
```

3-1. NAT でのサーバ公開1（ポートマッピング）設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
!
!
ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
ip dnat ppp0_dnat tcp any any 10.10.10.1 8080 192.168.10.20 80
!
!
end
```

3-2. NAT でのサーバ公開2（複数 IP＋PPPoE）設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
!
!
ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
ip dnat ppp0_dnat tcp any any 10.10.10.2 80 192.168.10.20
!
!
end
```

3-3. NAT でのサーバ公開3（複数 IP＋Ethernet）設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/29
 ip address 10.10.10.2/29 secondary
 no ip redirects
 ip access-group forward-in eth1_forward-in
 ip masquerade
 ip dnat-group eth1_dnat
 ip spi-filter
!
dns
 service enable
 root enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.6
!
ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
ip access-list eth1_forward-in permit any 192.168.10.20 tcp any 80
!
!
ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
ip dnat eth1_dnat tcp any any 10.10.10.2 80 192.168.10.20
!
!
end
```

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

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
 ip snat-group eth0_snat
 ip dnat-group eth0_dnat
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
!
!
ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
ip dnat eth0_dnat tcp 192.168.10.0/24 any 10.10.10.1 80 192.168.10.10
ip snat eth0_snat tcp 192.168.10.0/24 any 192.168.10.10 80 192.168.10.1
!
!
end
```

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

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip nat-loopback
 ip tcp adjust-mss auto
 ip access-group forward-in ppp0_forward-in
 ip masquerade
 ip dnat-group ppp0_dnat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
!
!
ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10 80
!
!
end
```

3-6. DMZ 構築(PPPoE)設定

```
!
! Century Systems NXR-230 Series ver 5.22.4A (build 5/17:42 23 04 2013)
!
hostname nxr230
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip access-group forward-in ppp0_forward-in
 ip access-group forward-out ppp0_forward-out
 ip snat-group ppp0_snat
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
interface ethernet 2
 ip address 10.10.10.1/29
 ip spi-filter
!
dns
 service enable
 address 10.10.10.4
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_forward-in permit any 10.10.10.2 tcp any 80
ip access-list ppp0_forward-in permit any 10.10.10.3 tcp any 80
ip access-list ppp0_forward-in permit any 10.10.10.4 tcp any 53
ip access-list ppp0_forward-in permit any 10.10.10.4 udp any 53
ip access-list ppp0_forward-in permit any 10.10.10.0/29 icmp
ip access-list ppp0_forward-out permit 10.10.10.4 any tcp any 53
```

```
ip access-list ppp0_forward-out permit 10.10.10.4 any udp any 53
ip access-list ppp0_in deny any 10.10.10.1 icmp 8 0
!
!
ip snat ppp0_snat ip 192.168.10.0/24 any 10.10.10.1
!
!
end
```

4-1. ユーザ認証設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
web-authenticate
 authenticate basic
 close idle-timeout 600
 log enable
 account username test password testpass
 mac access-list permit 00:80:6D:70:FF:FF ethernet 0
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
!
!
end
```

4-2. URL 転送設定

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
web-authenticate
 monitor port 80 redirect
 redirect-url http://www.centurysys.co.jp
 close idle-timeout 600
 log enable
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
!
!
end
```

4-3. ユーザ強制認証＋URL 転送

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
web-authenticate
 authenticate basic
 monitor port 80 redirect
 redirect-url http://www.centurysys.co.jp
 close idle-timeout 600
 log enable
 account username test password testpass
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
!
!
end
```

4-4. Web 認証フィルタ

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
!
interface ethernet 0
 ip address 192.168.10.1/24
 ip webauth-filter forward-in eth0_web_forward-in
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
web-authenticate
 authenticate basic
 monitor port 80 redirect
 redirect-url http://www.centurysys.co.jp
 close idle-timeout 600
 log enable
 account username test password testpass
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip web-auth access-list eth0_web_forward-in permit 192.168.10.10 any
!
!
!
```

```
end
```

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。

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。
なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など)
弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。
http://www.centurysys.co.jp/company/privacy.html

■ ご利用頂いている NXR 製品を含むネットワーク構成図
(ご利用頂いている回線やルータを含むネットワーク機器の IP アドレスを記載したもの)

■ 障害・不具合の内容およびその再現手順
(いつどこで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)

□ 問い合わせ内容例1

〇月〇日〇〇時〇〇分頃より拠点 A と拠点 B の間で IPsec による通信ができなくなった。障害発生前までは問題なく利用可能だった。現在当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通は確認できたが、対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通は確認できない。
障害発生前後で拠点 B のバックアップ回線としてモバイルカードを接続し、ppp1 インタフェースの設定を行った。設定を元に戻すと通信障害は解消する。
機器の内蔵時計は NTP で同期を行っている。

□ 問い合わせ内容例2

- 発生日時
  〇月〇日〇〇時〇〇分頃
- 発生拠点
  拠点 AB 間
- 障害内容
  IPsec による通信ができなくなった。
- 切り分け内容
  ルータ配下の端末から当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通確認可能。
  対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通確認不可。
- 障害発生前後での作業
  ルータの設定変更やネットワークに影響する作業は行っていない。
- 備考
  障害発生前までは問題なく利用可能だった。
  機器の内蔵時計は拠点 A の機器で 10 分、拠点 B の機器で 5 分遅れている。

□ 問い合わせ内容例3

現在 IPsec の設定中だが、一度も IPsec SA の確立および IPsec の通信ができていない。IPsec を設定している拠点からのインターネットアクセスおよび該当拠点への Ping による疎通確認も可能。設定例集，設定例集内のログ一覧および NXR シスログ一覧は未確認。

□ 良くない問い合わせ内容例1

VPN ができない。

→VPN として利用しているプロトコルは何か。VPN のトンネルが確立できないのか、通信ができないのかなど不明。

□ 良くない問い合わせ内容例2

通信ができない。

→どのような通信がいつどこでできない（またはできなくなった）のかが不明。

NXR での情報取得方法は以下のとおりです。

※情報を取得される前に

シリアル接続で情報を取得される場合は取得前に下記コマンドを実行してください。

#terminal width 180（初期値に戻す場合は terminal no width）

■ ご利用頂いている NXR 製品での不具合発生時のログ

ログは以下のコマンドで出力されます。

#show syslog message

■ ご利用頂いている NXR 製品のテクニカルサポート情報の結果

テクニカルサポート情報は以下のコマンドで出力されます。

show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果（モバイルカード利用時のみ）

#show mobile <N> ap

#show mobile <N> phone-number

#show mobile <N> signal-level

※<N>はモバイルデバイスナンバ

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, WXR 設定例集

NAT,フィルタ編

Ver 1.1.0

2013 年 5 月

発行　センチュリー・システムズ株式会社

Copyright(c) 2009-2013 Century Systems Co., Ltd. All Rights Reserved.