

FutureNet NXR,WXR シリーズ

設定例集

NAT,フィルタ編

Ver 1.4.0

センチュリー・システムズ株式会社



目次

目次.....	2
はじめに	4
改版履歴	5
NXR,WXR シリーズの NAT・フィルタ機能.....	6
1. フィルタ設定.....	12
1-1. 入力(in)フィルタ設定.....	13
1-2. 転送(forward-in,forward-out)フィルタ設定	15
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.....	18
1-4. FQDN フィルタ設定	20
1-5. 通信別 IP フィルタ設定	24
1-6. ブリッジフィルタ設定	28
2. NAT 設定.....	32
2-1. IP マスカレード設定	33
2-2. 送信元 NAT(SNAT)設定	36
2-3. 宛先 NAT(DNAT)設定	40
2-4. 通信別 NAT 設定.....	44
2-5. UPnP 設定.....	47
2-6. SIP-NAT 設定 1.....	51
2-7. SIP-NAT 設定 2.....	56
3. NAT/フィルタ応用設定	61
3-1. NAT でのサーバ公開 1(ポートマッピング)設定.....	62
3-2. NAT でのサーバ公開 2(複数 IP+PPPoE)設定	66
3-3. NAT でのサーバ公開 3(複数 IP+Ethernet)設定.....	70
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	74
3-5. NAT でのサーバ公開 5(IP nat-loopback の利用)設定	79
3-6. NAT でのサーバ公開 6(DDNS の利用)設定	83
3-7. DMZ 構築(PPPoE)設定	87
4. Web 認証設定.....	93
4-1. ユーザ認証設定	94
4-2. URL 転送設定.....	98
4-3. ユーザ強制認証+URL 転送	102
4-4. Web 認証フィルタ	106
4-5. RADIUS 連携	110

4-6. ブリッジ+Web 認証設定	115
付録	118
フィルタ状態確認方法	119
NAT 状態確認方法	121
UPnP 状態確認方法.....	122
SIP-NAT 状態確認方法.....	123
Web 認証機能のユーザ認証方法.....	124
設定例 show config 形式サンプル.....	125
サポートデスクへのお問い合わせ	148
サポートデスクへのお問い合わせに関して.....	149
サポートデスクのご利用に関して	151

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 シリーズ,
NXR-230/C,NXR-350/C,NXR-1200,NXR-G100 シリーズ,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, NXR-125/CX,NXR-230/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 2 章 FutureNet NXR-120/C Ver5.24.1J
※1-5 は FutureNet NXR-120/C Ver5.24.1M
2-3 は FutureNet NXR-230/C Ver5.26.1
第 3 章 FutureNet NXR-125/CX Ver5.25.4
第 4 章 FutureNet NXR-120/C Ver5.24.1J
※4-6 は FutureNet NXR-120/C Ver5.24.1M
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 設定につい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。
- モバイルデータ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、ご注意ください。
- 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
1.2.0	DDNS を利用したサーバ公開設定例追加 Web 認証での RADIUS 連携設定例追加
1.3.0	ブリッジフィルタ設定例追加 ブリッジ+Web 認証設定例追加
1.4.0	通信別 IP フィルタ設定例追加 通信別 NAT 設定例追加

NXR,WXR 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,WXR 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。

○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

○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。

(注) NXR,WXR 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)

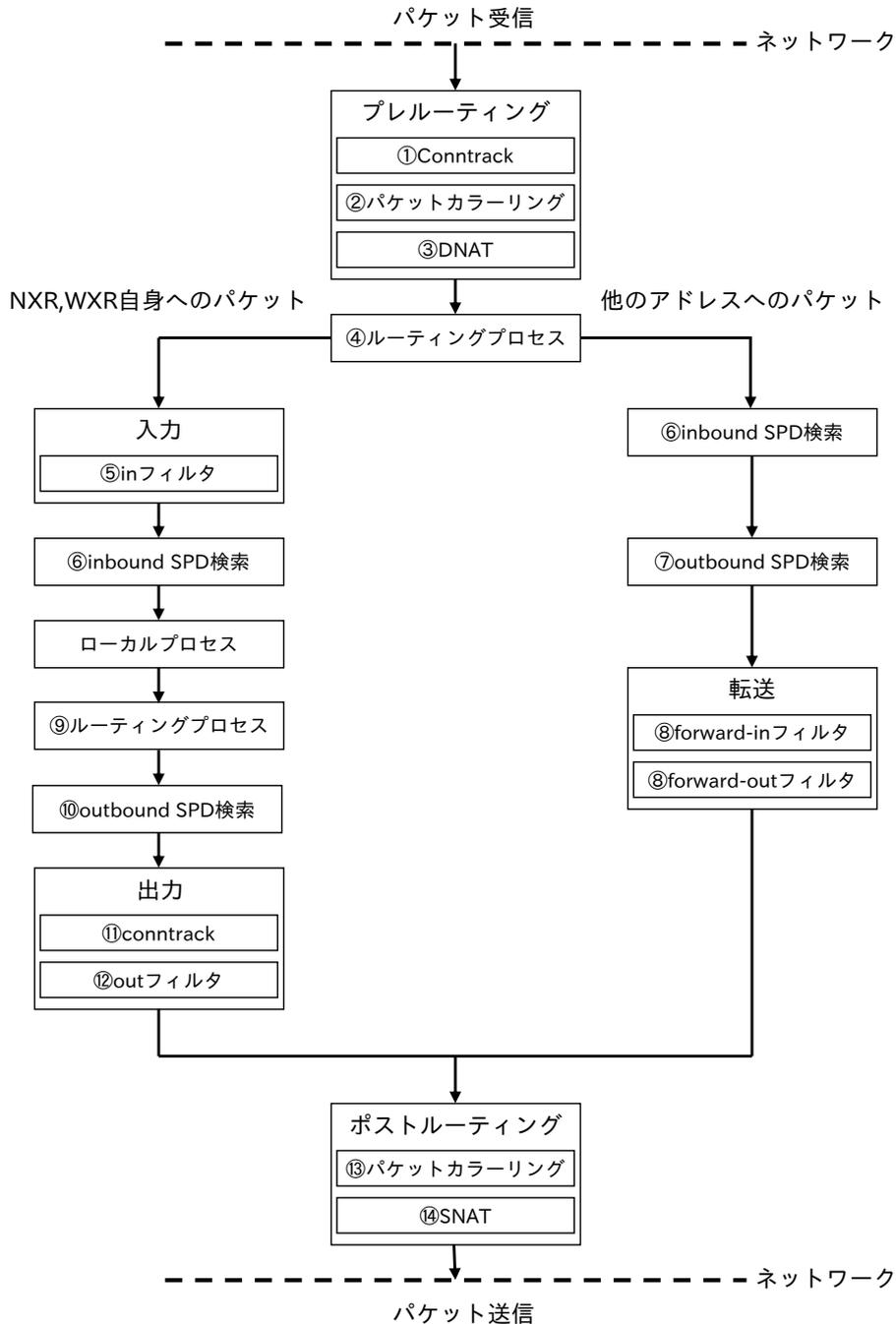
- (1) システム DNAT
- (2) UPNP 用 DNAT
- (3) ユーザ設定用宛先 NAT(DNAT)

○ 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,WXR パケットトラベリング

NXR,WXR 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 Contrack

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ー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、ポリシー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,WXR が宛先)

- パケット受信 -

① Contrack

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ー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,WXR ローカルプロセス

○ パケット送信時(NXR,WXR が送信元)

- NXR,WXR 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 Contrack

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、ポリシー検索は行われません。ポリシー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

1-2. 転送(forward-in,forward-out)フィルタ設定

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

1-4. FQDN フィルタ設定

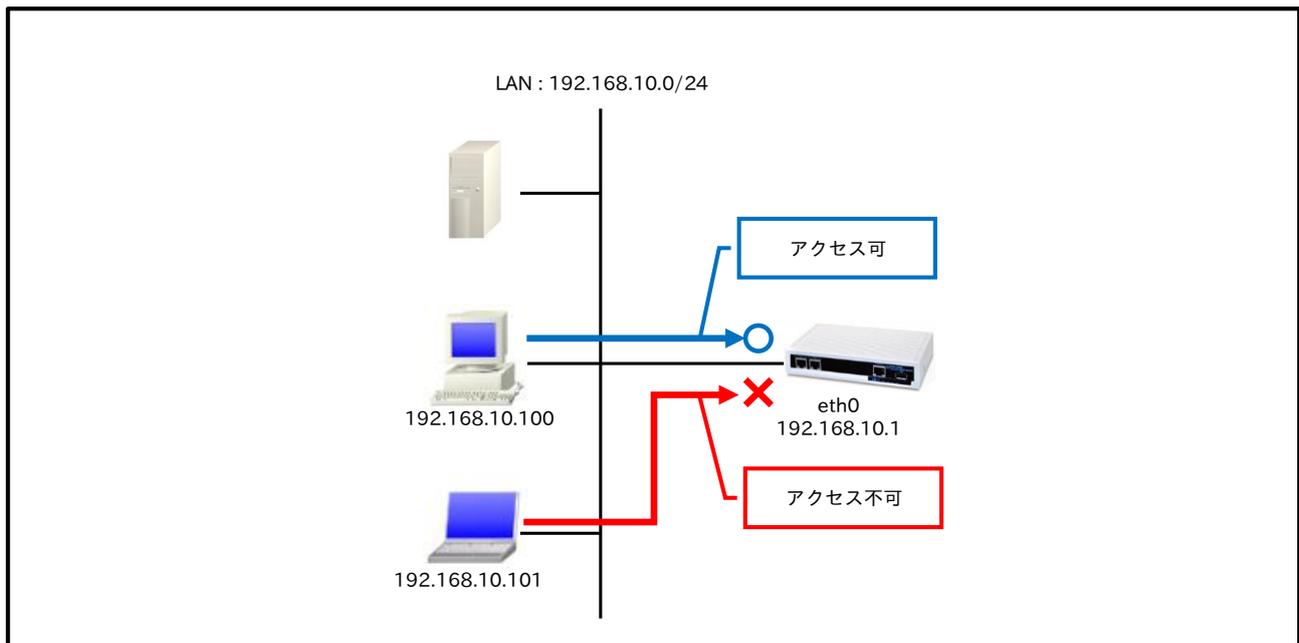
1-5. 通信別 IP フィルタ設定

1-6. ブリッジフィルタ設定

1-1. 入力(in)フィルタ設定

入力フィルタでは、ルータ宛に送信されたパケットのうちルータ自身で受信し処理するものを対象とします。この設定例では、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 アクセスは破棄します。

【 構成図 】



- ・ 入力フィルタ(in)では外部からルータ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 からルータへのアクセスについて制御したい場合には、この入力フィルタを設定します。

【 設定データ 】

設定項目			設定内容	
ethernet0 インタフェース	IP アドレス		192.168.10.1/24	
	IP アクセスグループ		in	
IP フィルタ	ルール名		eth0_in	
	eth0_in	No.1	動作	許可
			送信元 IP アドレス	192.168.10.100
			宛先 IP アドレス	192.168.10.1
			プロトコル	TCP
			送信元ポート	any
			宛先ポート	23
	eth0_in	No.2	動作	破棄
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.1
宛先ポート			23	

【 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。

IP アクセスリスト名を eth0_in とし、送信元 IP アドレス 192.168.10.100 以外からルータの LAN 側 IP アドレス 192.168.10.1 への TELNET アクセスを破棄します。

なお、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ルータ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ます。

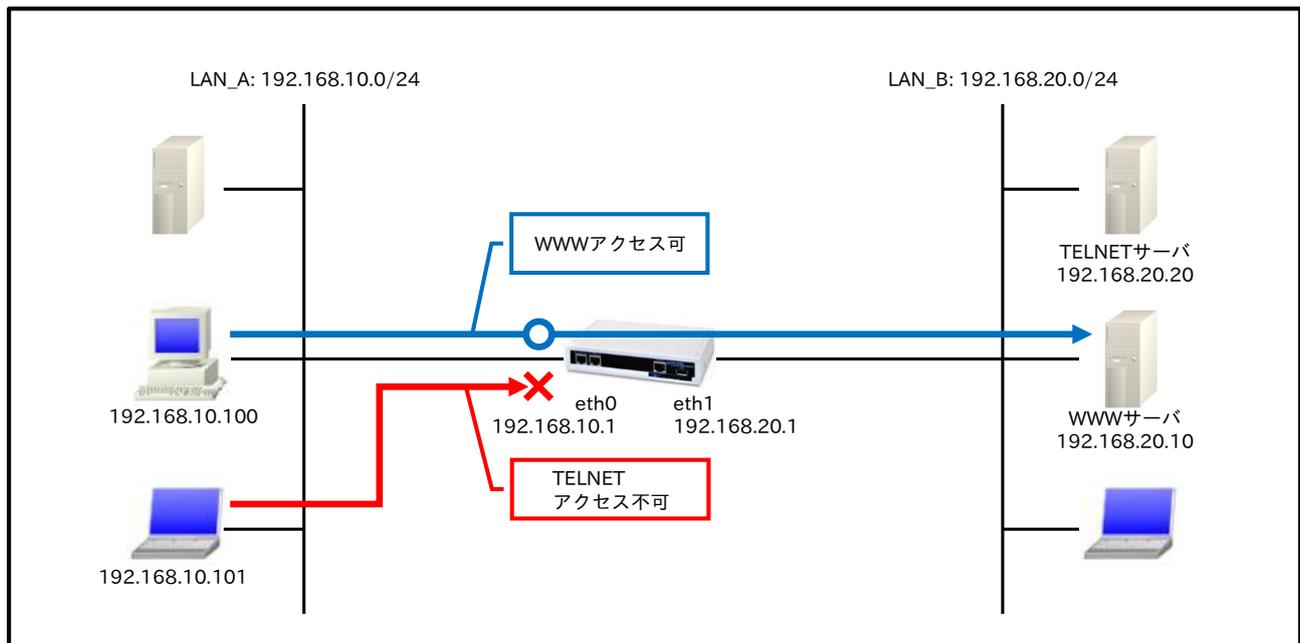
【 端末の設定例 】

	端末 1	端末 2
IP アドレス	192.168.10.100	192.168.10.101
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、ルータが内部転送(NXR,WXR 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。この設定例では、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します。

【 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 へのアクセスなどルータが内部転送する(ルーティングする)パケットを制御します。

【 設定データ 】

設定項目		設定内容		
ethernet0 インタフェース	IP アドレス	192.168.10.1/24		
	IP アクセスグループ	forward-in	eth0_forward-in	
ethernet1 インタフェース	IP アドレス	192.168.20.1/24		
IP フィルタ	ルール名		eth0_forward-in	
	eth0_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.20.10
			プロトコル	TCP
			送信元ポート	any
	宛先ポート	80		
	eth0_forward-in	No.2	動作	破棄
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.20.20
プロトコル			TCP	
送信元ポート			any	
宛先ポート	23			

【 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。

IP アクセスリスト名を eth0_forward-in とし、宛先 IP アドレス 192.168.20.10、宛先 TCP ポート番号 80 のパケットは許可しますが、宛先 IP アドレス 192.168.20.20、宛先 TCP ポート番号 23 のパケットは破棄します。

なお、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ルータが内部転送する(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 アドレスを設定します。

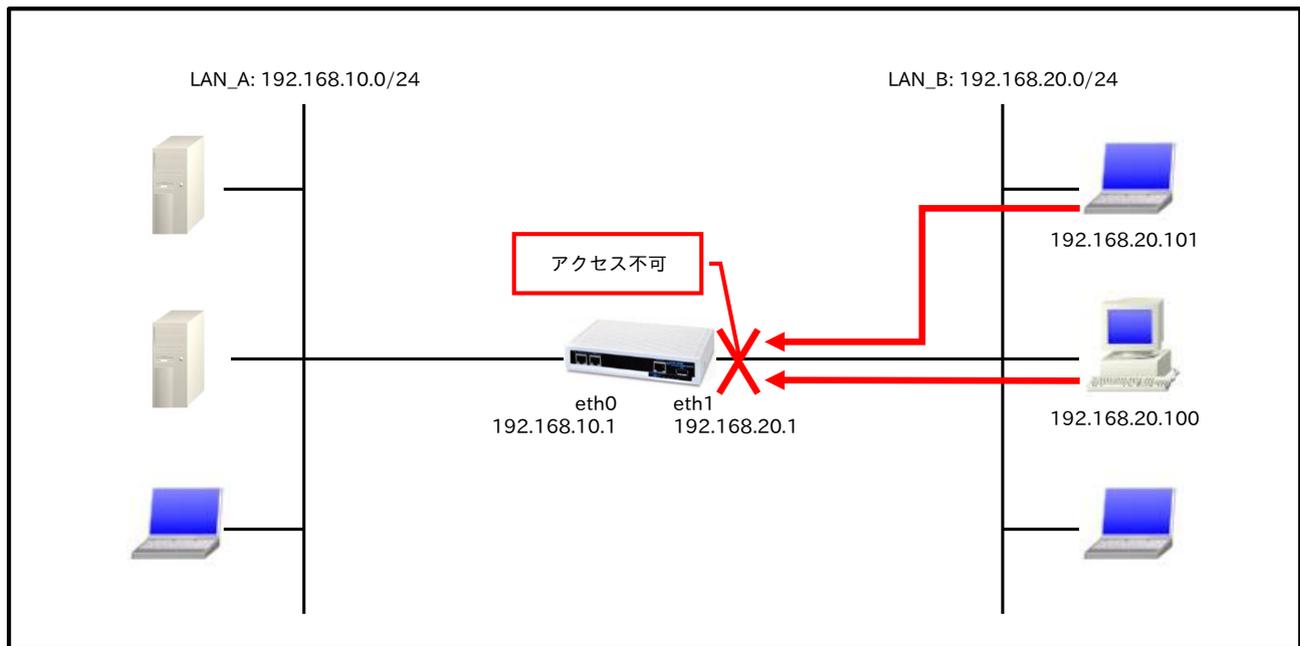
【 端末の設定例 】

	LAN_A	LAN_B		
	端末	端末	WWW サーバ	TELNET サーバ
IP アドレス	192.168.10.100	192.168.20.100	192.168.20.10	192.168.20.20
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	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。この設定例では、ethernet 1 インタフェース側からの接続要求を全て遮断します。

【 構成図 】



【 設定データ 】

設定項目		設定内容
ethernet0 インタフェース	IP アドレス	192.168.10.1/24
ethernet1 インタフェース	IP アドレス	192.168.20.1/24
	SPI フィルタ	有効

【 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 アドレスを設定します。

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

ステートフルパケットインスペクションを設定します。

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

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。

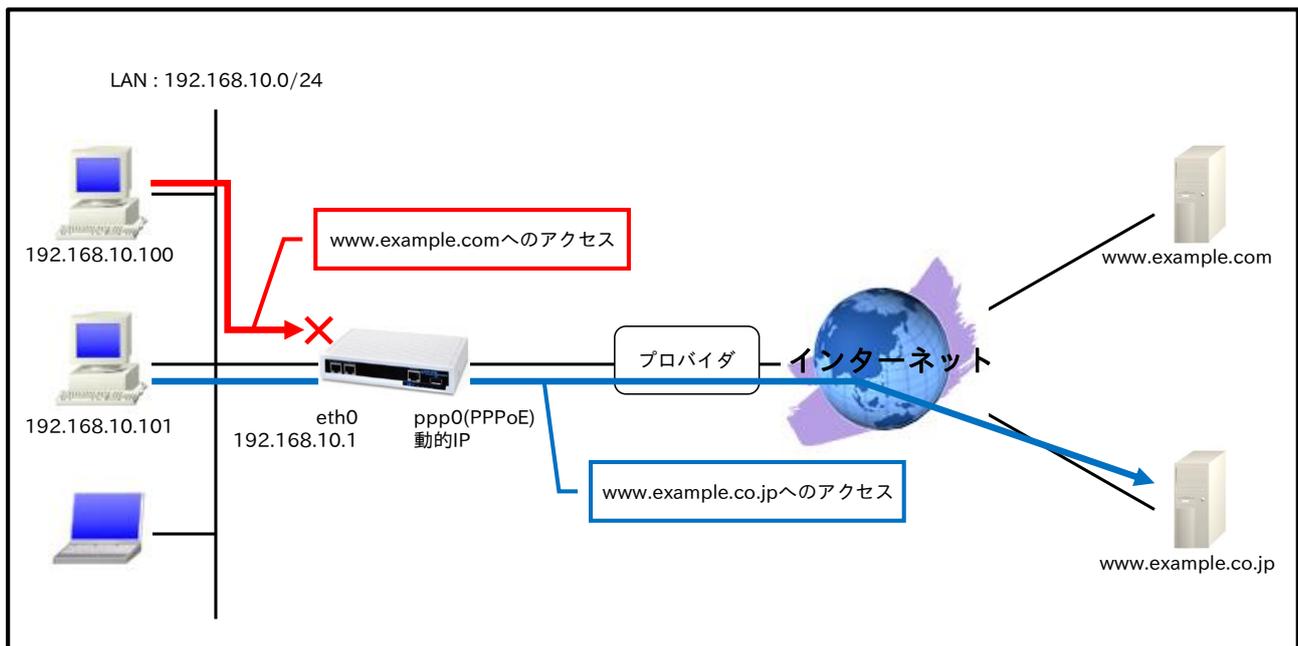
【 端末の設定例 】

	LAN_A の端末	LAN_B の端末
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	
デフォルトゲートウェイ	192.168.10.1	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。この設定例では、www.example.com の TCP ポート 80 番宛のアクセスを制限します。

【 構成図 】



【 設定データ 】

設定項目		設定内容	
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24	
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0	
	ppp0 の IP アドレス	動的 IP アドレス	
	IP マスカレード	有効	
	IP アクセスグループ	forward-out	
	SPI フィルタ	有効	
	MSS 自動調整	オート	
	ISP 接続用ユーザ ID	test1@example.jp	
	ISP 接続用パスワード	test1pass	
スタティックルート	宛先 IP アドレス	0.0.0.0/0	
	ゲートウェイ(インタフェース)	ppp0	
IP フィルタ	ルール名	ppp0_forward-out	
	ppp0_forward-out	動作	破棄
		送信元 IP アドレス	any
		宛先 IP アドレス	www.example.com
		プロトコル	TCP
		送信元ポート	any
宛先ポート	80		
DNS	サービス	有効	
FastForwarding		有効	

【 設定例 】

```
nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip access-list ppp0_forward-out deny any www.example.com tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-out ppp0_forward-out
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config
```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <IP アクセスリスト設定>

```
nrx120(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。

IP アクセスリスト名を ppp0_forward-out とし、宛先 FQDNwww.example.com,宛先 TCP ポート番号 80 のパケットを破棄します。

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。

(注) 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. <PPP アカウント設定>

```
nxr120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

5. <WAN 側(ppp0)インタフェース設定>

```
nxr120(config)#interface ppp 0  
nxr120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
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
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、IP アクセスリスト ppp0_forward-out を forward-out フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nxr120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

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
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

7. <DNS 設定>

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

DNS サービスを有効にします。

8. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

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	

1-5. 通信別 IP フィルタ設定

ここでは主な通信別に IP フィルタの設定例を紹介します。なお、下記 IP フィルタとは別に動的フィルタとしてステートフルパケットインスペクション機能もあります。この機能は主に WAN 側インタフェースで利用します。ステートフルパケットインスペクション機能の設定例は [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](#)をご参照下さい。

【 設定例 】

〔ルータへのアクセス〕

ルータへのアクセスを制御する場合、パケット受信インタフェースにおいて「ip access-group in」コマンドで IP アクセスリストを登録する必要があります。

<ルータへの TELNET アクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [ルータの IP アドレス] tcp [送信元ポート番号] 23
(config)#interface [受信インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) ルータとの通信を暗号化したい場合は、SSH を利用する必要があります。(TELNET の通信は暗号化されていません)

<ルータへの SSH アクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [ルータの IP アドレス] tcp [送信元ポート番号] 22
(config)#interface [受信インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) ssh-server port コマンドで SSH サーバのポート番号を変更した場合は、宛先ポート番号に変更後のポート番号を指定して下さい。

<ルータへの HTTP アクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [ルータの IP アドレス] tcp [送信元ポート番号] 880
(config)#interface [受信インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

<ルータへの ICMP アクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [ルータの IP アドレス] icmp
(config)#interface [受信インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

全ての送信元 IP アドレスを許可する場合は、[送信元 IP アドレス]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

<ルータへの ICMP エコーリクエストを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [ルータの IP アドレス] icmp 8 0
(config)#interface [受信インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

全ての送信元 IP アドレスを許可する場合は、[送信元 IP アドレス]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) ICMP ではタイプとコードを指定することができます。なおタイプ 8 コード 0 は ICMP エコーリクエストを表しています。

<WAN 側からルータへの IPsec のネゴシエーションとトンネルを利用した通信を許可する (NAT トラバーサルは除く)>

```
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] udp 500 500
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] 50
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

対向機器の IP アドレスが動的 IP アドレスの場合は、[対向機器の IP アドレス]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

<WAN 側からルータへの IPsec のネゴシエーションとトンネルを利用した通信を許可する (NAT トラバーサルのみ)>

```
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] udp [対向機器の送信元ポート番号] 500
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] udp [対向機器の送信元ポート番号] 4500
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

対向機器の IP アドレスが動的 IP アドレスの場合や全ての送信元ポート番号を許可する場合は、[対向機器の IP アドレス],[対向機器の送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

<WAN 側からルータへの IPsec のネゴシエーションとトンネルを利用した通信を許可する (ESP プロトコルと NAT トラバーサルの混在環境)>

```
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] udp [対向機器の送信元ポート番号] 500
```

```
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] udp [対向機器の送信元ポート番号] 4500
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] 50
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

対向機器の IP アドレスが動的 IP アドレスの場合や全ての送信元ポート番号を許可する場合は、[対向機器の IP アドレス],[対向機器の送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) ESP プロトコルの場合は 1,3 行目の設定を NAT トラバーサルの場合は 1,2 行目の設定を利用します。

<WAN 側からルータへの L2TP のネゴシエーションとトンネルを利用した通信を許可する (overUDP は除く)>

```
(config)#ip access-list [IP アクセスリスト名] permit [対向機器の IP アドレス] [ルータの IP アドレス] 115
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group in [IP アクセスリスト名]
```

対向機器の IP アドレスが動的 IP アドレスの場合は、[対向機器の IP アドレス]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

【ルータ経由の通信】

ルータ経由の通信を制御する場合、パケット受信インタフェースにおいて「ip access-group forward-in」コマンドで IP アクセスリストを登録する必要があります。

<WAN 側から LAN 内の HTTP サーバへのアクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の HTTP サーバの IP アドレス] tcp [送信元ポート番号] 80
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group forward-in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

(☞) NAT を合わせて設定する場合、[<HTTP サーバを外部に公開する>](#)をご参照下さい。

<WAN 側から LAN 内の SSH サーバへのアクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の SSH サーバの IP アドレス] tcp [送信元ポート番号] 22
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group forward-in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

(☞) NAT を合わせて設定する場合、[<SSH サーバを外部に公開する>](#)をご参照下さい。

<WAN 側から LAN 内のサーバへの ICMP アクセスを許可する>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内のサーバの IP アドレス] icmp
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group forward-in [IP アクセスリスト名]
```

全ての送信元 IP アドレスを許可する場合は、[送信元 IP アドレス]に「any」を設定します。

(☞) NAT を合わせて設定する場合、[<WAN 側から LAN 内のサーバへの ICMP アクセスをパススルーする>](#)をご参照下さい。

<WAN 側から LAN 内の IPsec サーバへの IPsec 通信をパススルーする>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の IPsec サーバの IP アドレス]
udp [送信元ポート番号] 500
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の IPsec サーバの IP アドレス]
udp [送信元ポート番号] 4500
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の IPsec サーバの IP アドレス] 50
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group forward-in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

(☞) NAT を合わせて設定する場合、設定例は[<WAN 側から LAN 内の IPsec サーバへの IPsec 通信をパススルーする>](#)をご参照下さい。

(☞) ESP プロトコルと NAT トラバーサル混在環境を想定しています。

(☞) 3 行目の設定の「50」は ESP のプロトコル番号を表しています。

<WAN 側から LAN 内の PPTP サーバへの PPTP 通信をパススルーする>

```
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の PPTP サーバの IP アドレス] tcp
[送信元ポート番号] 1723
(config)#ip access-list [IP アクセスリスト名] permit [送信元 IP アドレス] [LAN 内の PPTP サーバの IP アドレス] 47
(config)#interface [WAN 側インタフェース]
(config-if)#ip access-group forward-in [IP アクセスリスト名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

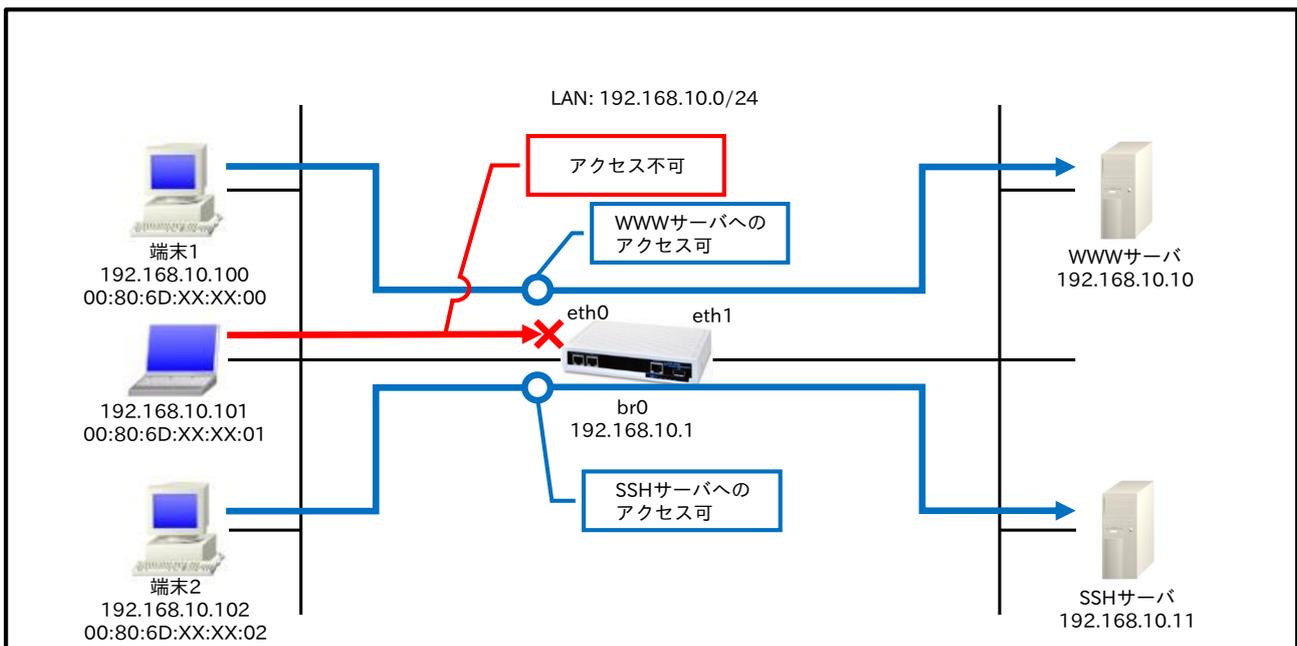
(☞) NAT を合わせて設定する場合、設定例は[<WAN 側から LAN 内の PPTP サーバへの PPTP 通信をパススルーする>](#)をご参照下さい。

(☞) 2 行目の設定の「47」は GRE のプロトコル番号を表しています。

1-6. ブリッジフィルタ設定

ブリッジフィルタは、ブリッジインタフェースで動作するフィルタです。ブリッジフィルタでは、MAC アドレス、IP アドレス、VLAN IDなどを条件としてレイヤ2レベルでのフィルタリングが可能です。この設定例では、特定の端末から WWW サーバ、SSH サーバへのアクセスは許可するが、それ以外の端末からのアクセスは破棄します。

【 構成図 】



- ・ ブリッジフィルタは、ブリッジインタフェースで登録した Ethernet0 インタフェースで行います。
- ・ 端末 1 から WWW サーバへの通信(ARP リクエスト,TCP ポート番号 80)を許可します。
- ・ 端末 2 から SSH サーバへの通信(ARP リクエスト,TCP ポート番号 22)を許可します。
- ・ その他端末からのルータ宛およびルータ経由の通信を破棄します。

【 設定データ 】

設定項目		設定内容		
ブリッジインタフェース	bridge0 の IP アドレス		192.168.10.1/24	
	ブリッジ対象インタフェース		ethernet0 ethernet1	
	ブリッジアクセスグループ	in	br0_eth0-in	
		forward-in	br0_eth0-forward-in	
ブリッジフィルタ	ルール名		br0_eth0-forward-in	
	br0_eth0-forward-in	No.1	動作	許可
			フィールド	ARP
			OPCODE	Request
			送信元 MAC アドレス	00:80:6D:XX:XX:00
			送信元 IP アドレス	192.168.10.100
	br0_eth0-forward-in	No.2	宛先 IP アドレス	192.168.10.10
			動作	許可
フィールド			IP	

			送信元 MAC アドレス	00:80:6D:XX:XX:00
			送信元 IP アドレス	192.168.10.100
			宛先 IP アドレス	192.168.10.10
			プロトコル	TCP
			宛先ポート	80
		No.3	動作	許可
			フィールド	ARP
			OPCODE	Request
			送信元 MAC アドレス	00:80:6D:XX:XX:02
			送信元 IP アドレス	192.168.10.102
		No.4	宛先 IP アドレス	192.168.10.11
			動作	許可
			フィールド	IP
			送信元 MAC アドレス	00:80:6D:XX:XX:02
			送信元 IP アドレス	192.168.10.102
	No.5	宛先 IP アドレス	192.168.10.11	
		プロトコル	TCP	
		宛先ポート	22	
		動作	破棄	
	ルール名			br0_eth0-in
br0_eth0-in	No.1	動作	破棄	
		フィールド	any	
		送信元 MAC アドレス	any	
		宛先 MAC アドレス	any	

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#bridge access-list br0_eth0-forward-in permit 1 arp
nrx120(config-bridge-acl)#opcode request
nrx120(config-bridge-acl)#sender-mac 00:80:6D:XX:XX:00
nrx120(config-bridge-acl)#sender-ip 192.168.10.100
nrx120(config-bridge-acl)#target-ip 192.168.10.10
nrx120(config-bridge-acl)#exit
nrx120(config)#bridge access-list br0_eth0-forward-in permit 2 ip
nrx120(config-bridge-acl)#mac source 00:80:6D:XX:XX:00
nrx120(config-bridge-acl)#source 192.168.10.100
nrx120(config-bridge-acl)#destination 192.168.10.10
nrx120(config-bridge-acl)#protocol tcp
nrx120(config-bridge-acl)#destination-port 80
nrx120(config-bridge-acl)#exit
nrx120(config)#bridge access-list br0_eth0-forward-in permit 3 arp
nrx120(config-bridge-acl)#opcode request
nrx120(config-bridge-acl)#sender-mac 00:80:6D:XX:XX:02
nrx120(config-bridge-acl)#sender-ip 192.168.10.102
nrx120(config-bridge-acl)#target-ip 192.168.10.11
nrx120(config-bridge-acl)#exit
nrx120(config)#bridge access-list br0_eth0-forward-in permit 4 ip
nrx120(config-bridge-acl)#mac source 00:80:6D:XX:XX:02
nrx120(config-bridge-acl)#source 192.168.10.102
nrx120(config-bridge-acl)#destination 192.168.10.11
nrx120(config-bridge-acl)#protocol tcp
nrx120(config-bridge-acl)#destination-port 22
nrx120(config-bridge-acl)#exit
nrx120(config)#bridge access-list br0_eth0-forward-in deny 5 any any any
nrx120(config)#bridge access-list br0_eth0-in deny 1 any any any
nrx120(config)#interface bridge 0

```

```
nxr120(config-bridge)#ip address 192.168.10.1/24
nxr120(config-bridge)#bridge port 1 ethernet 0
nxr120(config-bridge)#bridge port 2 ethernet 1
nxr120(config-bridge)#bridge port 1 access-group in br0_eth0-in
nxr120(config-bridge)#bridge port 1 access-group forward-in br0_eth0-forward-in
nxr120(config-bridge)#exit
nxr120(config)#exit
nxr120#save config
```

【 設定例解説 】

1. <ブリッジアクセスリスト設定>

```
nxr120(config)#bridge access-list br0_eth0-forward-in permit 1 arp
nxr120(config-bridge-acl)#opcode request
nxr120(config-bridge-acl)#sender-mac 00:80:6D:XX:XX:00
nxr120(config-bridge-acl)#sender-ip 192.168.10.100
nxr120(config-bridge-acl)#target-ip 192.168.10.10
```

ブリッジアクセスリスト名を br0_eth0-forward-in、Ethernet タイプを ARP とします。そして、OP コードが Request(ARP Request)、送信元 MAC アドレス 00:80:6D:XX:XX:00、送信元 IP アドレス 192.168.10.100、宛先 IP アドレス 192.168.10.100 のフレームを許可します。

```
nxr120(config)#bridge access-list br0_eth0-forward-in permit 2 ip
nxr120(config-bridge-acl)#mac source 00:80:6D:XX:XX:00
nxr120(config-bridge-acl)#source 192.168.10.100
nxr120(config-bridge-acl)#destination 192.168.10.10
nxr120(config-bridge-acl)#protocol tcp
nxr120(config-bridge-acl)#destination-port 80
```

ブリッジアクセスリスト名を br0_eth0-forward-in、Ethernet タイプを IP(IPv4)とします。そして、送信元 MAC アドレス 00:80:6D:XX:XX:00、送信元 IP アドレス 192.168.10.100、宛先 IP アドレス 192.168.10.100、宛先 TCP ポート番号 80 のフレームを許可します。

```
nxr120(config)#bridge access-list br0_eth0-forward-in permit 3 arp
nxr120(config-bridge-acl)#opcode request
nxr120(config-bridge-acl)#sender-mac 00:80:6D:XX:XX:02
nxr120(config-bridge-acl)#sender-ip 192.168.10.102
nxr120(config-bridge-acl)#target-ip 192.168.10.11
```

ブリッジアクセスリスト名を br0_eth0-forward-in、Ethernet タイプを ARP とします。そして、OP コードが Request(ARP Request)、送信元 MAC アドレス 00:80:6D:XX:XX:02、送信元 IP アドレス 192.168.10.102、宛先 IP アドレス 192.168.10.11 のフレームを許可します。

```
nxr120(config)#bridge access-list br0_eth0-forward-in permit 4 ip
nxr120(config-bridge-acl)#mac source 00:80:6D:XX:XX:02
nxr120(config-bridge-acl)#source 192.168.10.102
nxr120(config-bridge-acl)#destination 192.168.10.11
nxr120(config-bridge-acl)#protocol tcp
nxr120(config-bridge-acl)#destination-port 22
```

ブリッジアクセスリスト名を br0_eth0-forward-in、Ethernet タイプを IP(IPv4)とします。そして、送信元 MAC アドレス 00:80:6D:XX:XX:02、送信元 IP アドレス 192.168.10.102、宛先 IP アドレス 192.168.10.11、宛先 TCP ポート番号 22 のフレームを許可します。

```
nxr120(config)#bridge access-list br0_eth0-forward-in deny 5 any any any
```

ブリッジアクセスリスト名を br0_eth0-forward-in、Ethernet タイプ,送信元,宛先 MAC アドレス any のフレームを破棄します。

```
nxr120(config)#bridge access-list br0_eth0-in deny 1 any any any
```

ブリッジアクセスリスト名を br0_eth0-in、Ethernet タイプ,送信元,宛先 MAC アドレス any のフレームを破棄します。

(注) これらブリッジアクセスリスト設定は bridge0 インタフェース設定で登録します。

(注) ブリッジ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. <bridge0 インタフェース設定>

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

bridge0 インタフェースの IP アドレスを設定します。

```
nxr120(config-bridge)#bridge port 1 ethernet 0  
nxr120(config-bridge)#bridge port 2 ethernet 1
```

ブリッジインタフェースで利用するインタフェースを設定します。

```
nxr120(config-bridge)#bridge port 1 access-group in br0_eth0-in
```

ブリッジアクセスリスト設定で設定した br0_eth0-in をブリッジポート 1 の in フィルタに適用します。これによりブリッジポート 1(ethernet0 インタフェース)で受信したルータ自身宛のフレームに対してブリッジアクセスリストによるチェックが行われます。

```
nxr120(config-bridge)#bridge port 1 access-group forward-in br0_eth0-forward-in
```

ブリッジアクセスリスト設定で設定した br0_eth0-forward-in をブリッジポート 1 の forward-in フィルタに適用します。これによりブリッジポート 1(ethernet0 インタフェース)で受信したルータが内部転送する(透過する)フレームに対してブリッジアクセスリストによるチェックが行われます。

【 端末の設定例 】

	端末 1	端末 2	WWW サーバ	SSH サーバ
IP アドレス	192.168.10.100	192.168.10.102	192.168.10.10	192.168.10.11
サブネットマスク	255.255.255.0			

2. NAT 設定

2-1. IP マスカレード設定

2-2. 送信元 NAT(SNAT)設定

2-3. 宛先 NAT(DNAT)設定

2-4. 通信別 NAT 設定

2-5. UPnP 設定

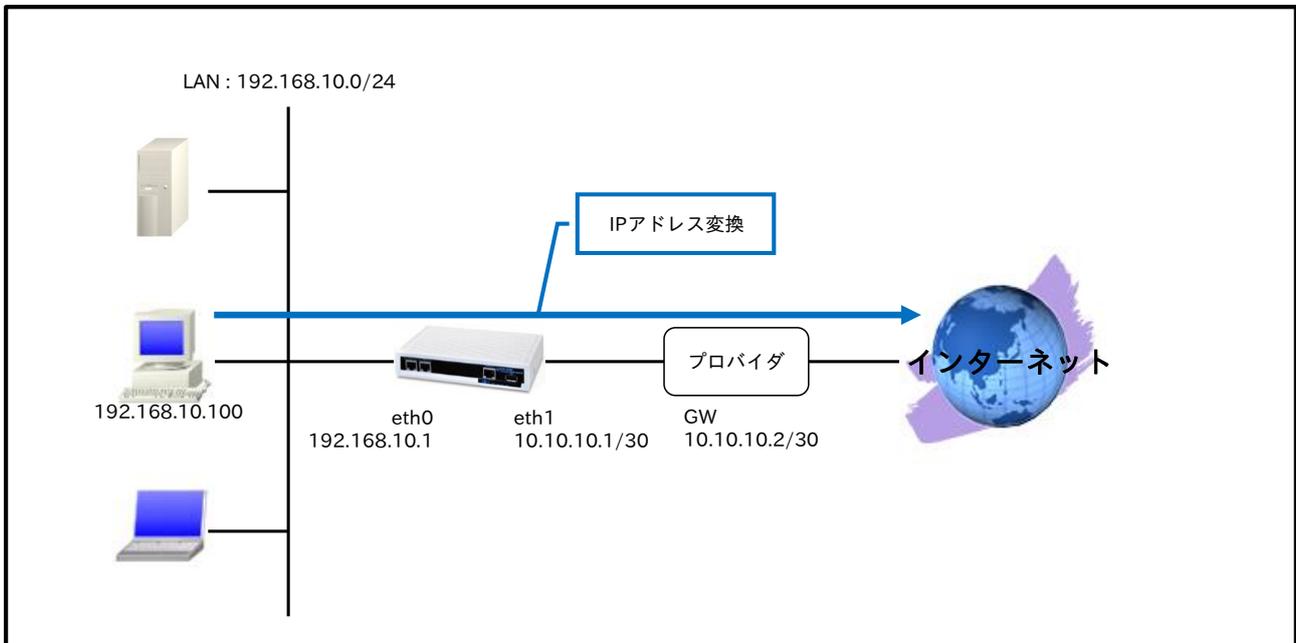
2-6. SIP-NAT 設定 1

2-7. SIP-NAT 設定 2

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 】



【 設定データ 】

設定項目		設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
	ethernet1 の IP アドレス	10.10.10.1/30
WAN 側インタフェース	IP マスカレード	有効
	SPI フィルタ	有効
	MSS 自動調整	オート
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(IP アドレス)	10.10.10.2
DNS	サービス	有効
	DNS サーバ	プライマリ 10.255.1.1 セカンダリ 10.255.1.2
FastForwarding		有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 10.10.10.2
nrx120(config)#interface ethernet 1
nrx120(config-if)#ip address 10.10.10.1/30
nrx120(config-if)#ip masquerade
nrx120(config-if)#ip spi-filter
    
```

```
nrx120(config-if)#ip tcp adjust-mss auto
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#address 10.255.1.1
nrx120(config-dns)#address 10.255.1.2
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config
```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(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。

3. <WAN 側(ethernet1)インタフェース設定>

```
nrx120(config)#interface ethernet 1
nrx120(config-if)#ip address 10.10.10.1/30
```

ethernet1 インタフェースの IP アドレスを設定します。

```
nrx120(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。

```
nrx120(config-if)#ip spi-filter
nrx120(config-if)#ip tcp adjust-mss auto
```

ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

4. <DNS 設定>

```
nrx120(config)#dns
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

```
nrx120(config-dns)#address 10.255.1.1
nrx120(config-dns)#address 10.255.1.2
```

プロバイダから通知されているプライマリ,セカンダリ DNS サーバアドレスを設定します。

5. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

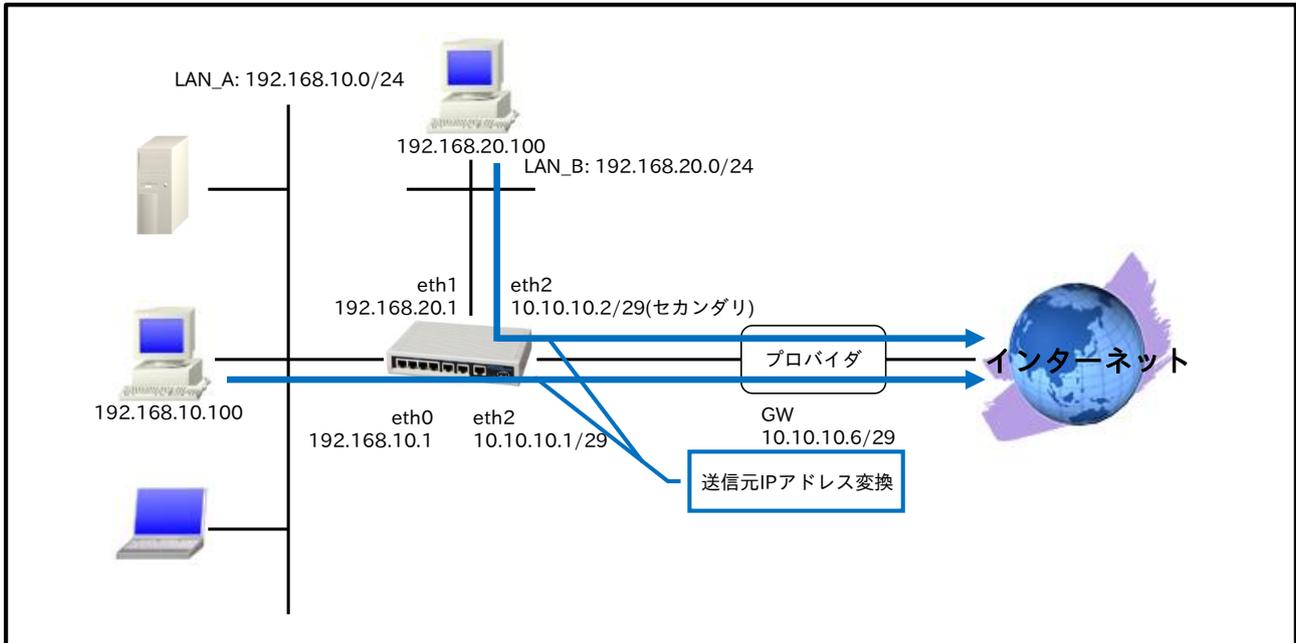
【 端末の設定例 】

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	

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 】



【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
	ethernet1 の IP アドレス	192.168.20.1/24		
WAN 側インタフェース	ethernet2 の IP アドレス	10.10.10.1/29		
	ethernet2 の IP アドレス(セカンダリ)	10.10.10.2/29		
	SNAT グループ	eth2_snat		
	SPI フィルタ	有効		
スタティックルート	MSS 自動調整	オート		
	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(IP アドレス)	10.10.10.6		
	ルール名	eth2_snat		
SNAT	eth2_snat	No.1	送信元 IP アドレス	192.168.10.0/24
		No.2	宛先 IP アドレス	any
	変換後送信元 IP アドレス		10.10.10.1	
	送信元 IP アドレス	192.168.20.0/24		
		宛先 IP アドレス	any	
		変換後送信元 IP アドレス	10.10.10.2	
DNS	サービス	有効		
	ルートサーバ	有効		
FastForwarding		有効		

【 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 10.10.10.6
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)#ip tcp adjust-mss auto
nxr230(config-if)#exit
nxr230(config)#dns
nxr230(config-dns)#service enable
nxr230(config-dns)#root enable
nxr230(config-dns)#exit
nxr230(config)#fast-forwarding enable
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 10.10.10.6
```

デフォルトルートを設定します。

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。

SNAT 名を eth2_snat とし、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、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 に変換します。

なお、この SNAT 設定は ethernet2 インタフェース設定で登録します。

(☞) SNAT 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 アドレスを設定します。

```
nxr230(config-if)#ip snat-group eth2_snat
```

SNAT 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 で設定した IP アドレス変換が行われます。

```
nxr230(config-if)#ip spi-filter  
nxr230(config-if)#ip tcp adjust-mss auto
```

ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

6. <DNS 設定>

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

DNS サービスを有効にします。

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

ルート DNS サーバを有効に設定します。

(☞) ルート DNS サーバを有効にする以外に、DNS サーバアドレスを address コマンドで指定する方法もあります。

7. <ファストフォワーディングの有効化>

```
nxr230(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

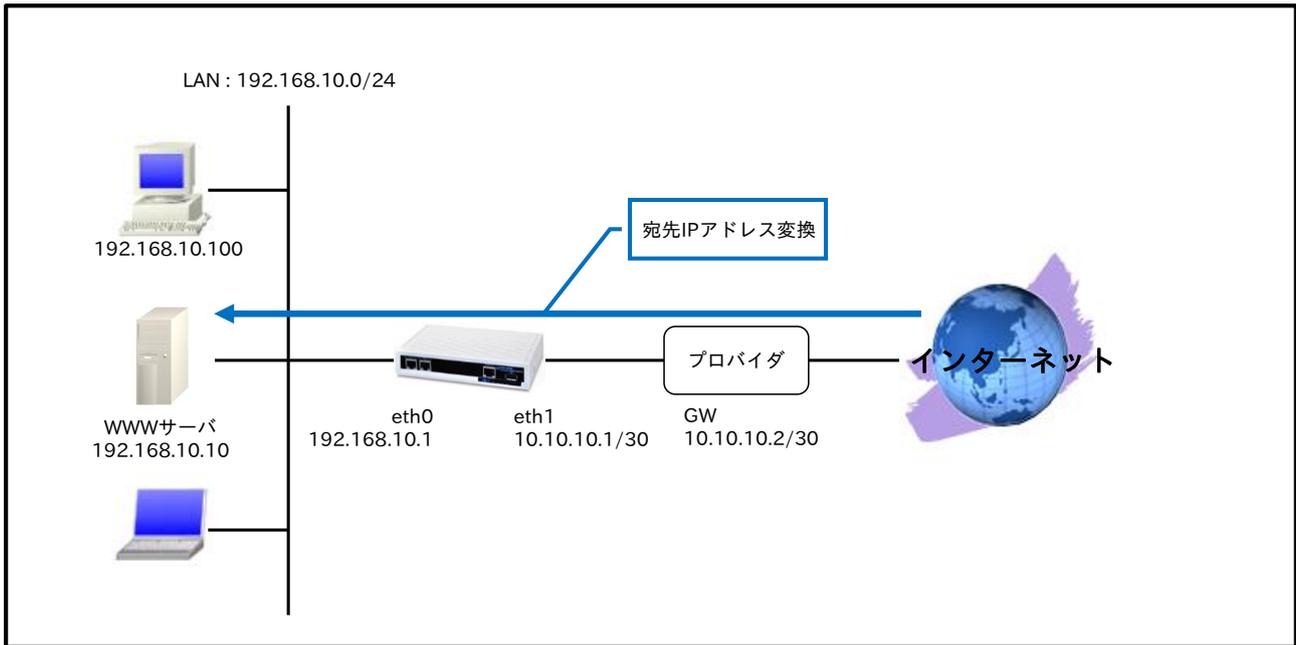
【 端末の設定例 】

	LAN_A の端末	LAN_B の端末
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	
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバ		

2-3. 宛先 NAT(DNAT)設定

LAN 内にあるプライベート IP アドレスのサーバをインターネット経由でアクセスさせる場合など、宛先 NAT(DNAT)を設定することでルータ経由でのアクセスが可能になります。この設定例では、DNAT 設定を利用して WWW サーバを外部に公開します。

【 構成図 】



【 設定データ 】

設定項目		設定内容	
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24	
WAN 側インタフェース	ethernet1 の IP アドレス	10.10.10.1/30	
	DNAT グループ	eth1_dnat	
	IP マスカレード	有効	
	IP アクセスグループ	forward-in	
	SPI フィルタ	有効	
	MSS 自動調整	オート	
	スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(IP アドレス)	10.10.10.2	
DNAT	ルール名	eth1_dnat	
	eth1_dnat	プロトコル	TCP
		送信元 IP アドレス	any
		送信元ポート	any
		宛先 IP アドレス	10.10.10.1
		宛先ポート	80
変換後宛先 IP アドレス	192.168.10.10		
IP フィルタ	ルール名	eth1_forward-in	
	eth1_forward-in	動作	許可
		送信元 IP アドレス	any
		宛先 IP アドレス	192.168.10.10
		プロトコル	TCP
送信元ポート	any		

		宛先ポート	80
DNS	サービス		有効
	ルートサーバ		有効
FastForwarding			有効

【 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)#ip tcp adjust-mss auto
nxr120(config-if)#exit
nxr120(config)#dns
nxr120(config-dns)#service enable
nxr120(config-dns)#root enable
nxr120(config-dns)#exit
nxr120(config)#fast-forwarding enable
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。

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。DNAT 名を eth1_dnat とし、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 に変換します。

なお、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>

```
nrx120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
```

IP アクセスリスト名を eth1_forward-in とし、宛先 IP アドレス 192.168.10.10、宛先 TCP ポート番号 80 のパケットを許可します。

なお、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。フィルタリングしたい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>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#ip address 10.10.10.1/30
```

ethernet1 インタフェースの IP アドレスを設定します。

```
nrx120(config-if)#ip dnat-group eth1_dnat
```

DNAT 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 で設定した IP アドレス変換が行われます。

```
nrx120(config-if)#ip masquerade  
nrx120(config-if)#ip access-group forward-in eth1_forward-in  
nrx120(config-if)#ip spi-filter  
nrx120(config-if)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。

また IP アクセスリスト eth1_forward-in を forward-in フィルタに適用します。そして TCP MSS の調整機能をオートに設定します。

6. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

```
nrx120(config-dns)#root enable
```

ルート DNS サーバを有効に設定します。

(☞) ルート DNS サーバを有効にする以外に、DNS サーバアドレスを address コマンドで指定する方法もあります。

7. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

	端末	WWW サーバ
IP アドレス	192.168.10.100	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	192.168.10.1	

2-4. 通信別 NAT 設定

ここでは通信別に NAT の設定例を紹介します。

【 設定例 】

〔宛先 IP アドレスを変換する(DNAT の利用)〕

ルータで受信したパケットの宛先 IP アドレスを変換する場合、パケット受信インタフェースにおいて「ip dnat-group」コマンドで DNAT ルール名を登録する必要があります。

<HTTP サーバを外部に公開する>

```
(config)#ip dnat [DNAT ルール名] tcp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 80 [LAN 内の HTTP サーバの IP アドレス]
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内の HTTP サーバへのアクセスを許可する>](#)をご参照下さい。

<HTTP サーバを外部に公開する(公開用ポート TCP8080,サーバポート TCP80)>

```
(config)#ip dnat [DNAT ルール名] tcp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 8080 [LAN 内の HTTP サーバの IP アドレス] 80
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内の HTTP サーバへのアクセスを許可する>](#)をご参照下さい。

<SSH サーバを外部に公開する>

```
(config)#ip dnat [DNAT ルール名] tcp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 22 [LAN 内の SSH サーバの IP アドレス]
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内の SSH サーバへのアクセスを許可する>](#)をご参照下さい。

<WAN 側から LAN 内のサーバへの ICMP アクセスをパススルーする>

```
(config)#ip dnat [DNAT ルール名] 1 [送信元 IP アドレス] [ルータの IP アドレス] [LAN 内のサーバの IP アドレス]
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレスを許可する場合は、[送信元 IP アドレス]に「any」を設定します。

ルータの IP アドレスが動的 IP アドレスの場合は、[ルータの IP アドレス]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内のサーバへの ICMP アクセスを許可する>](#)をご参照下さい。

(☞) 1 行目の設定の「1」は ICMP のプロトコル番号を表しています。

<WAN 側から LAN 内の IPsec サーバへの IPsec 通信をパススルーする>

```
(config)#ip dnat [DNAT ルール名] udp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 500 [LAN 内の IPsec サーバの IP アドレス]
(config)#ip dnat [DNAT ルール名] udp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 4500 [LAN 内の IPsec サーバの IP アドレス]
(config)#ip dnat [DNAT ルール名] 50 [送信元 IP アドレス] [ルータの IP アドレス] [LAN 内の IPsec サーバの IP アドレス]
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内の IPsec サーバへの IPsec 通信をパススルーする>](#)をご参照下さい。

(☞) ESP プロトコルと NAT トラバーサル混在環境を想定しています。

(☞) 3 行目の設定の「50」は ESP のプロトコル番号を表しています。

<WAN 側から LAN 内の PPTP サーバへの PPTP 通信をパススルーする>

```
(config)#ip dnat [DNAT ルール名] tcp [送信元 IP アドレス] [送信元ポート番号] [ルータの IP アドレス] 1723 [LAN 内の PPTP サーバの IP アドレス]
(config)#ip dnat [DNAT ルール名] 47 [送信元 IP アドレス] [ルータの IP アドレス] [LAN 内の PPTP サーバの IP アドレス]
(config)#interface [WAN 側インタフェース]
(config-if)#ip dnat-group [DNAT ルール名]
```

全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

(☞) フィルタを合わせて設定する場合、設定例は[<WAN 側から LAN 内の PPTP サーバへの PPTP 通信をパススルーする>](#)をご参照下さい。

(☞) 2 行目の設定の「47」は GRE のプロトコル番号を表しています。

[送信元 IP アドレスを変換する(SNAT の利用)]

ルータから送信するパケットの送信元 IP アドレスを変換する場合、パケット送信インタフェースにおいて「ip snat-group」コマンドで SNAT ルール名を登録する必要があります。

<LAN から WAN へのアクセス時に SNAT 対象の送信元 IP アドレス指定する>

```
(config)#ip snat [SNAT ルール名] [SNAT 変換対象の送信元 IP アドレス] [送信元ポート番号] any any [ルータの WAN 側 IP アドレス]  
(config)#interface [WAN 側インタフェース]  
(config-if)#ip snat-group [SNAT ルール名]
```

全ての送信元ポート番号を許可する場合は、[送信元ポート番号]に「any」を設定します。

<LAN から WAN へのアクセス時に SNAT 対象の宛先 IP アドレス指定する>

```
(config)#ip snat [SNAT ルール名] [送信元 IP アドレス] [送信元ポート番号] [宛先 IP アドレス] [宛先ポート番号] [ルータの WAN 側 IP アドレス]  
(config)#interface [WAN 側インタフェース]  
(config-if)#ip snat-group [SNAT ルール名]
```

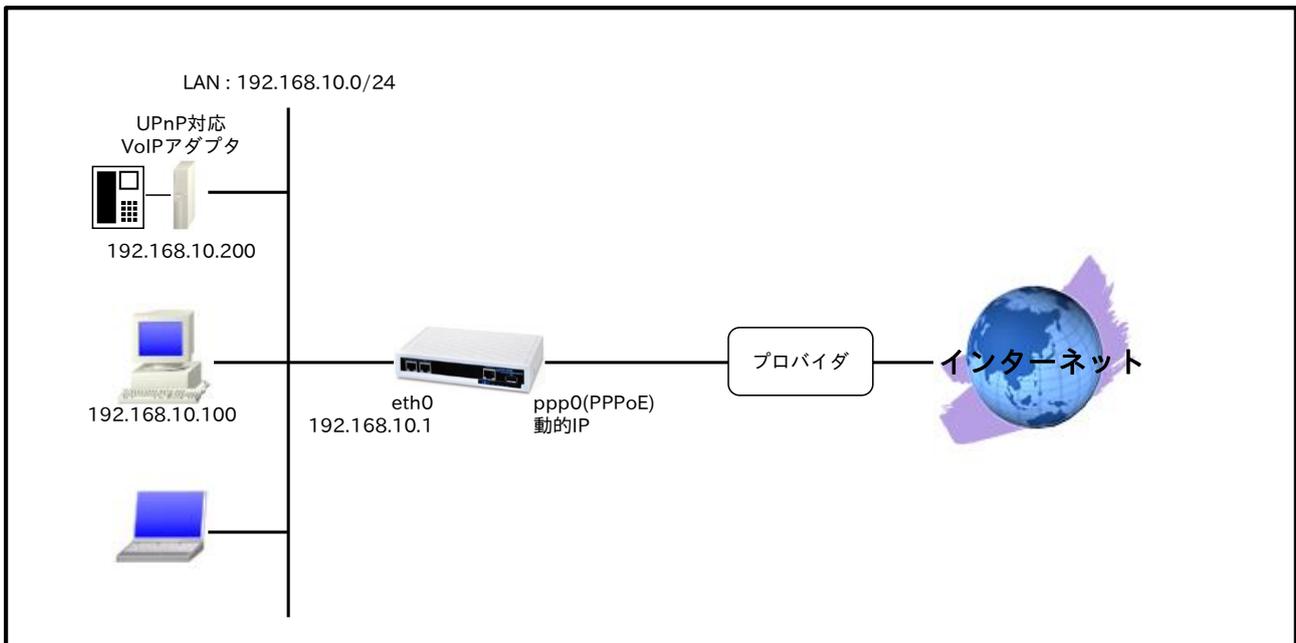
全ての送信元 IP アドレス,送信元ポート番号を許可する場合は、[送信元 IP アドレス],[送信元ポート番号]に「any」を設定します。

全ての宛先ポート番号を許可する場合は、[宛先ポート番号]に「any」を設定します。

2-5. 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ルータ配下で利用する場合、UPnP 機能を設定することで利用できるようになります。

【 構成図 】



【 設定データ 】

設定項目		設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	IP マスカレード	有効
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
	ISP 接続用パスワード	test1pass
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(インタフェース)	ppp0
UPnP	サービス	有効
	WAN 側インタフェース	ppp0
	listen IP アドレス	192.168.10.1/24
	無通信切断タイマー	3600 秒
DNS	サービス	有効
FastForwarding		有効

【 設定例 】

```
nxr120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr120(config)#interface ethernet 0
```

```
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#upnp
nrx120(config-upnp)#external interface ppp 0
nrx120(config-upnp)#listen ip 192.168.10.1/24
nrx120(config-upnp)#timeout 3600
nrx120(config-upnp)#service enable
nrx120(config-upnp)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config
```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

4. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

5. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

6. <UPnP 設定>

```
nrx120(config)#upnp
```

UPnP を設定します。

```
nrx120(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。

```
nrx120(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。

```
nrx120(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。

```
nrx120(config-upnp)#service enable
```

UPnP サービスを有効にします。

7. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

8. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(※) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズ

ガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

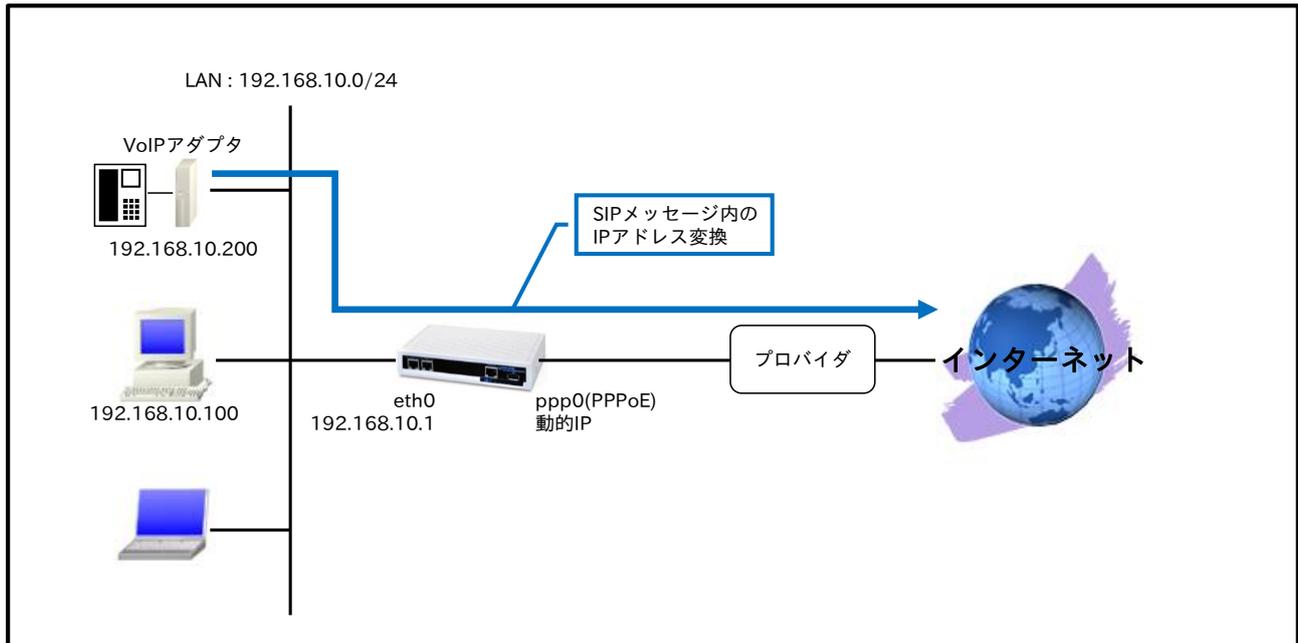
	UPnP 対応端末	UPnP 対応 VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	
デフォルトゲートウェイ	192.168.10.1	
DNS サーバ		

※VoIP アダプタの SIP に関する設定は除く

2-6. 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 】



- この設定例の 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

【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0		
	ppp0 の IP アドレス	動的 IP アドレス		
	DNAT グループ	ppp0_dnat		
	IP マスカレード	有効		
	IP アクセスグループ	forward-in	ppp0_forward-in	
	SPI フィルタ	有効		
	MSS 自動調整	オート		
	ISP 接続用ユーザ ID	test1@example.jp		
	ISP 接続用パスワード	test1pass		
スタティックルート	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(インタフェース)	ppp0		
DNAT	ルール名	ppp0_dnat		
	ppp0_dnat	No.1	プロトコル	UDP
			送信元 IP アドレス	any
			送信元ポート	any

			宛先 IP アドレス	any
			宛先ポート	5060
			変換後宛先 IP アドレス	192.168.10.200
		No.2	プロトコル	UDP
			送信元 IP アドレス	any
			送信元ポート	any
			宛先 IP アドレス	any
			宛先ポート(始点)	5090
			宛先ポート(終点)	5091
			変換後宛先 IP アドレス	192.168.10.200
IP フィルタ	ルール名			ppp0_forward-in
		No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.200
			プロトコル	UDP
			送信元ポート	any
			宛先ポート	5060
		No.2	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.200
			プロトコル	UDP
			送信元ポート	any
		宛先ポート(始点)	5090	
		宛先ポート(終点)	5091	
SIP-NAT				有効
DNS	サービス			有効
FastForwarding				有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#sip-nat enable
nrx120(config)#ip dnat ppp0_dnat udp any any any 5060 192.168.10.200
nrx120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5060
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <SIP-NAT 設定>

```
nrx120(config)#sip-nat enable
```

SIP-NAT を有効にします。

4. <DNAT 設定>

```
nrx120(config)#ip dnat ppp0_dnat udp any any any 5060 192.168.10.200  
nrx120(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。

DNAT 名を ppp0_dnat とし、宛先 UDP ポート番号 5060,5090~5091 のパケットの宛先 IP アドレスを 192.168.10.200 に変換します。

なお、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 アダプタへの着信用の設定です。

5. <IP アクセスリスト設定>

```
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5060  
nrx120(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。

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.200,宛先 UDP ポート番号 5060,5090~5091 のパケットを許可します。

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 アダプタへの着信用の設定です。

6. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip dnat-group ppp0_dnat  
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

8. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

9. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

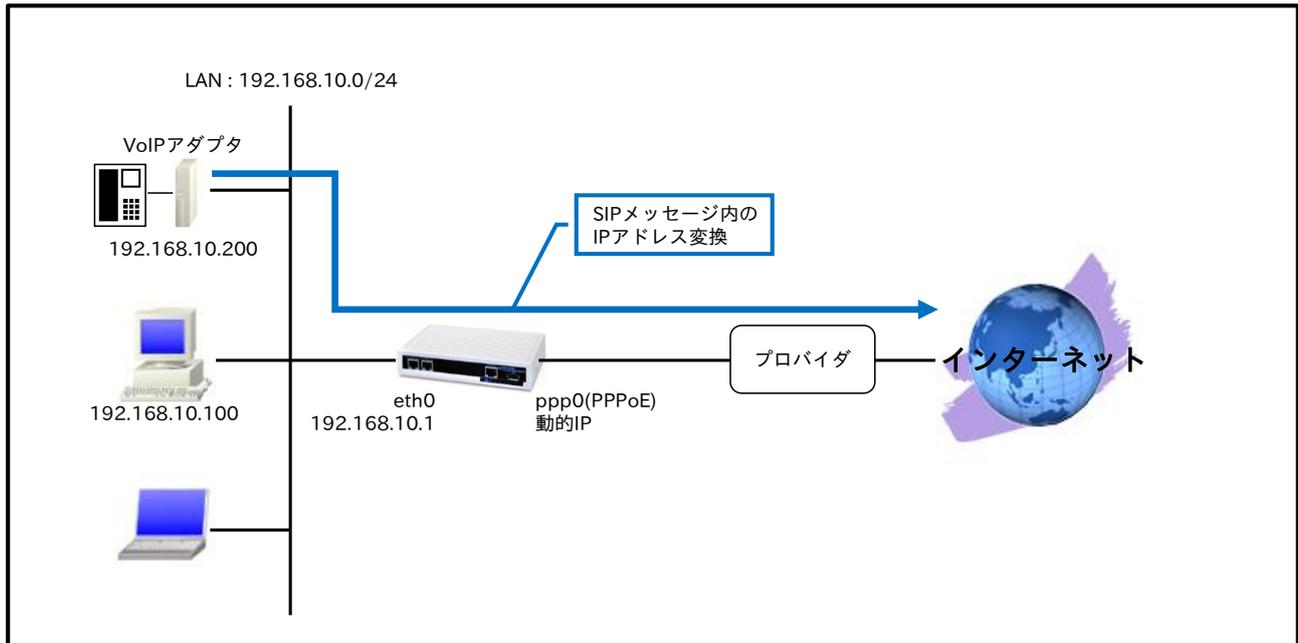
	端末	VoIP アダプタ
IP アドレス	192.168.10.100	192.168.10.200
サブネットマスク	255.255.255.0	
デフォルトゲートウェイ	192.168.10.1	
DNS サーバ		

※VoIP アダプタの SIP に関する設定は除く

2-7. 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 以外など、一部の IP 電話サービスにおいて REGISTER の宛先 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ます、この設定を行うことで通話できるようになります。

【 構成図 】



- この設定例の 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

【 設定データ 】

設定項目		設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	DNAT グループ	ppp0_dnat
	IP マスカレード	有効
	IP アクセスグループ	forward-in
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
	ISP 接続用パスワード	test1pass
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(インタフェース)	ppp0
DNAT	ルール名	ppp0_dnat
	ppp0_dnat No.1 プロトコル	UDP

			送信元 IP アドレス	any
			送信元ポート	any
			宛先 IP アドレス	any
			宛先ポート	5064
			変換後宛先 IP アドレス	192.168.10.200
		No.2	プロトコル	UDP
			送信元 IP アドレス	any
			送信元ポート	any
			宛先 IP アドレス	any
			宛先ポート(始点)	5090
			宛先ポート(終点)	5091
			変換後宛先 IP アドレス	192.168.10.200
IP フィルタ	ルール名		ppp0_forward-in	ppp0_forward-in
		No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.200
			プロトコル	UDP
			送信元ポート	any
			宛先ポート	5064
		No.2	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.200
			プロトコル	UDP
			送信元ポート	any
		宛先ポート(始点)	5090	
		宛先ポート(終点)	5091	
SIP-NAT				有効
	SIP-NAT 対象ポート番号			5060,5064
DNS	サービス			有効
FastForwarding				有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#sip-nat enable
nrx120(config)#sip-nat port 5060 5064
nrx120(config)#ip dnat ppp0_dnat udp any any any 5064 192.168.10.200
nrx120(config)#ip dnat ppp0_dnat udp any any any range 5090 5091 192.168.10.200
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5064
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any range 5090 5091
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable

```

```
nrx120(config-dns)#exit  
nrx120(config)#fast-forwarding enable  
nrx120(config)#exit  
nrx120#save config
```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <SIP-NAT 設定>

```
nrx120(config)#sip-nat enable
```

SIP-NAT を有効にします。

```
nrx120(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。

(☞) 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>

```
nrx120(config)#ip dnat ppp0_dnat udp any any any 5064 192.168.10.200  
nrx120(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。

DNAT 名を ppp0_dnat とし、宛先 UDP ポート番号 5064,5090~5091 のパケットの宛先 IP アドレスを 192.168.10.200 に変換します。

なお、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 アダプタへの着信用の設定です。

5. <IP アクセスリスト設定>

```
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.200 udp any 5064  
nrx120(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。

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.200,宛先 UDP ポート番号

5064,5090~5091 のパケットを許可します。

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 アダプタへの着信用の設定です。

6. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip dnat-group ppp0_dnat  
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

8. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

9. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

	端末	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	
デフォルトゲートウェイ	192.168.10.1	
DNS サーバ		

※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

3-2. NAT でのサーバ公開 2(複数 IP+PPPoE)設定

3-3. NAT でのサーバ公開 3(複数 IP+Ethernet)設定

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

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

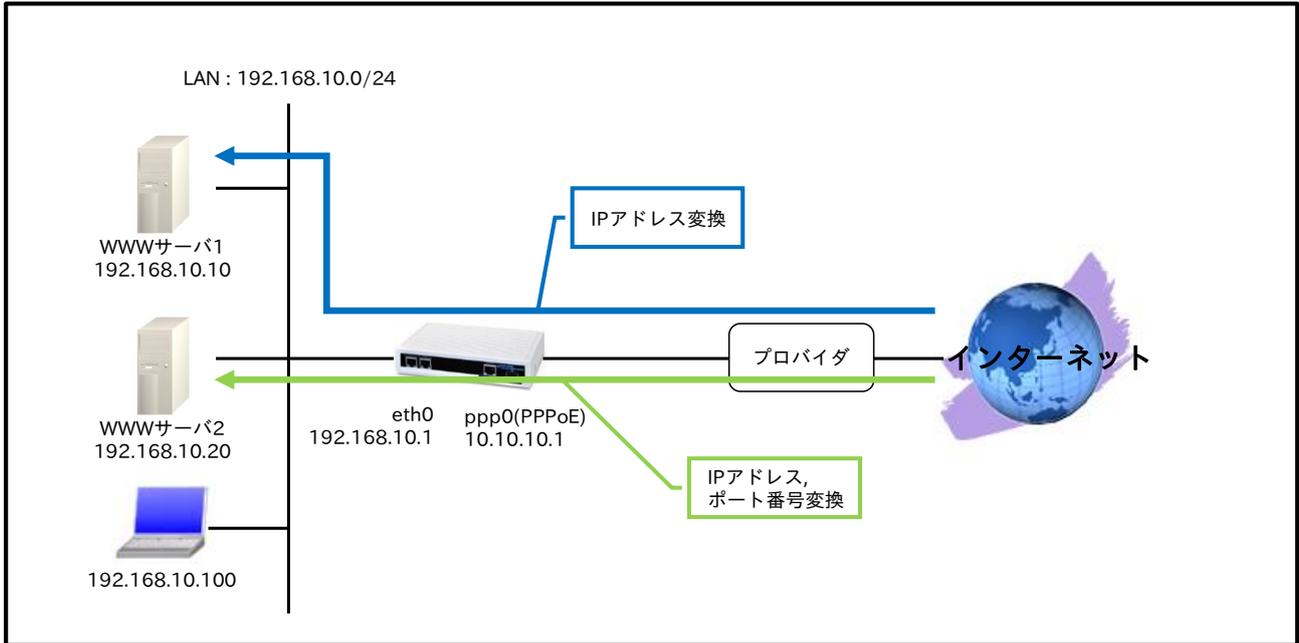
3-6. NAT でのサーバ公開 6(DDNS の利用)設定

3-7. DMZ 構築(PPPoE)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。この設定例では、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できるようにします。

【 構成図 】



【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0		
	ppp0 の IP アドレス	10.10.10.1/32		
	DNAT グループ	ppp0_dnat		
	IP マスカレード	有効		
	IP アクセスグループ	forward-in	ppp0_forward-in	
	SPI フィルタ	有効		
	MSS 自動調整	オート		
	ISP 接続用ユーザ ID	test1@example.jp		
	ISP 接続用パスワード	test1pass		
スタティックルート	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(インタフェース)	ppp0		
DNAT	ルール名	ppp0_dnat		
	ppp0_dnat	No.1	プロトコル	TCP
			送信元 IP アドレス	any
			送信元ポート	any
		宛先 IP アドレス	10.10.10.1	
		宛先ポート	80	
		変換後宛先 IP アドレス	192.168.10.10	
	No.2	プロトコル	TCP	
		送信元 IP アドレス	any	
		送信元ポート	any	

			宛先 IP アドレス	10.10.10.1
			宛先ポート	8080
			変換後宛先 IP アドレス	192.168.10.20
			変換後宛先ポート	80
IP フィルタ	ルール名		ppp0_forward-in	
	ppp0_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.10
			プロトコル	TCP
			送信元ポート	any
	宛先ポート	80		
	ppp0_forward-in	No.2	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.20
プロトコル			TCP	
送信元ポート			any	
宛先ポート	80			
DNS	サービス		有効	
FastForwarding			有効	

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip nat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip nat ppp0_dnat tcp any any 10.10.10.1 8080 192.168.10.20 80
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address 10.10.10.1/32
nrx120(config-ppp)#ip nat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#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。

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 10.10.10.1 8080 192.168.10.20 80
```

DNAT 名を ppp0_dnat とし、宛先 IP アドレス 10.10.10.1 のパケットのうち、宛先 TCP ポート番号 80 のパケットの宛先 IP アドレスは 192.168.10.10 に、宛先 TCP ポート番号 8080 のパケットの宛先 IP アドレスは 192.168.10.20、宛先 TCP ポート番号 80 に変換します。

なお、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
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.10、宛先 TCP ポート番号 80、宛先 IP アドレス 192.168.10.20、宛先 TCP ポート番号 80 のパケットを許可します。

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。

5. <PPP アカウント設定>

```
nxr120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID、パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

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
```

ppp0 インタフェースの IP アドレスを設定します。

```
nrx120(config-ppp)#ip dnat-group ppp0_dnat  
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

7. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

8. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

9. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

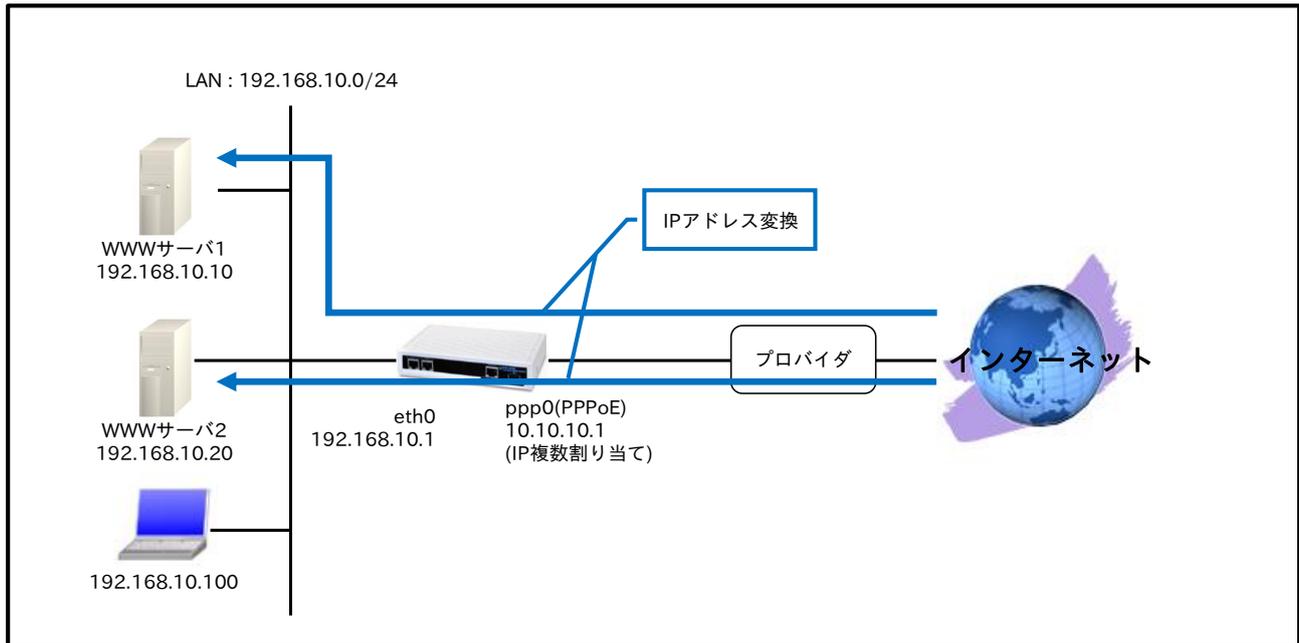
【 端末の設定例 】

	端末	WWW サーバ 1	WWW サーバ 2
IP アドレス	192.168.10.100	192.168.10.10	192.168.10.20
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	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、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 設定をすることで、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。この設定例では、WAN 回線に PPPoE を利用します。

【 構成図 】



【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0		
	ppp0 の IP アドレス	10.10.10.1/32		
	DNAT グループ	ppp0_dnat		
	IP マスカレード	有効		
	IP アクセスグループ	forward-in	ppp0_forward-in	
	SPI フィルタ	有効		
	MSS 自動調整	オート		
	ISP 接続用ユーザ ID	test1@example.jp		
	ISP 接続用パスワード	test1pass		
スタティックルート	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(インタフェース)	ppp0		
DNAT	ルール名	ppp0_dnat		
	ppp0_dnat	No.1	プロトコル	TCP
			送信元 IP アドレス	any
			送信元ポート	any
		宛先 IP アドレス	10.10.10.1	
		宛先ポート	80	
		変換後宛先 IP アドレス	192.168.10.10	
	No.2	プロトコル	TCP	
		送信元 IP アドレス	any	
		送信元ポート	any	
送信元ポート		any		

			宛先 IP アドレス	10.10.10.2
			宛先ポート	80
			変換後宛先 IP アドレス	192.168.10.20
IP フィルタ	ルール名			ppp0_forward-in
	ppp0_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.10
			プロトコル	TCP
			送信元ポート	any
	ppp0_forward-in	No.2	宛先ポート	80
			動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.20
プロトコル			TCP	
			送信元ポート	any
			宛先ポート	80
DNS	サービス			有効
FastForwarding				有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip nat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip nat ppp0_dnat tcp any any 10.10.10.2 80 192.168.10.20
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address 10.10.10.1/32
nrx120(config-ppp)#ip nat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <DNAT 設定>

```
nrx120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10  
nrx120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.2 80 192.168.10.20
```

DNAT 名を ppp0_dnat とし、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 アドレスは 192.168.10.10 に、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 アドレスは 192.168.10.20 に変換します。

なお、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>

```
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80  
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.20 tcp any 80
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.10,宛先 TCP ポート番号 80、宛先 IP アドレス 192.168.10.20,宛先 TCP ポート番号 80 のパケットを許可します。

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。

5. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

6. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address 10.10.10.1/32
```

ppp0 インタフェースの IP アドレスを設定します。

```

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
    
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```

nxr120(config-ppp)#ppp username test1@example.jp
    
```

ISP 接続用ユーザ ID を設定します。

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
    
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

8. <DNS 設定>

```

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

DNS サービスを有効にします。

9. <ファストフォワーディングの有効化>

```

nxr120(config)#fast-forwarding enable
    
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

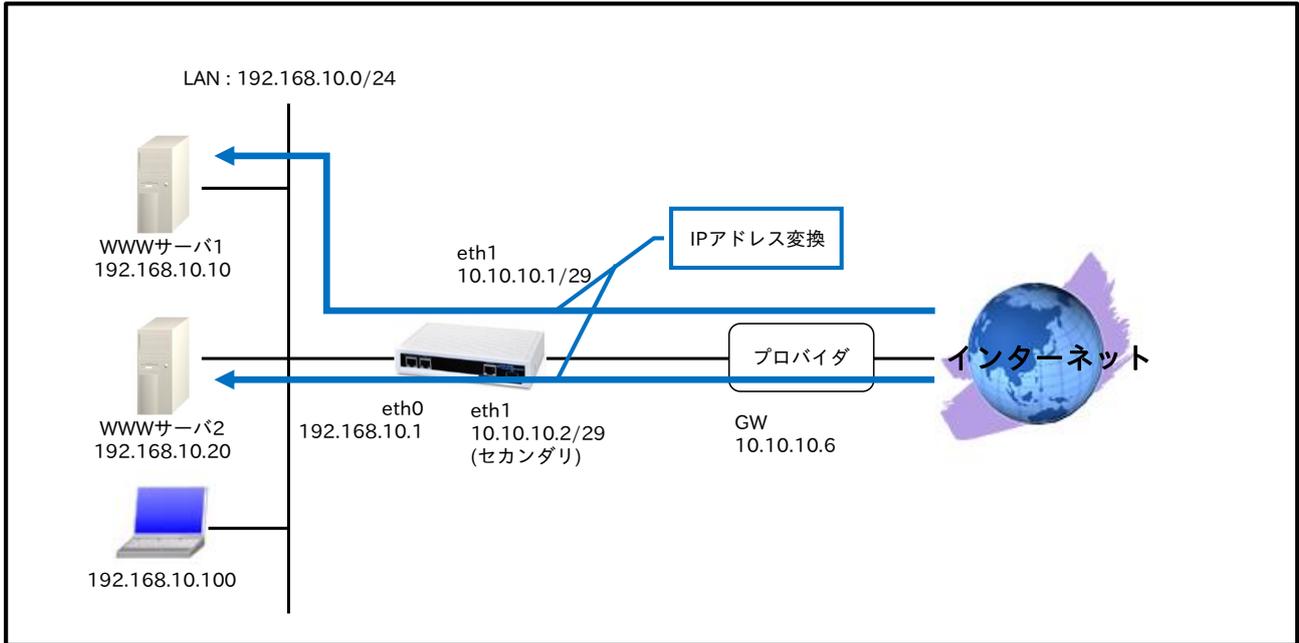
【 端末の設定例 】

	端末	WWW サーバ 1	WWW サーバ 2
IP アドレス	192.168.10.100	192.168.10.10	192.168.10.20
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	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、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 設定をすることで、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。この設定例では、WAN 回線に Ethernet を利用します。

【 構成図 】



【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
	ethernet1 の IP アドレス	10.10.10.1/29		
	ethernet1 の IP アドレス(セカンダリ)	10.10.10.2/29		
WAN 側インタフェース	DNAT グループ	eth1_dnat		
	IP マスカレード	有効		
	IP アクセスグループ	forward-in		
	SPI フィルタ	有効		
	MSS 自動調整	オート		
スタティックルート	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(IP アドレス)	10.10.10.6		
DNAT	ルール名	eth1_dnat		
	eth1_dnat	No.1	プロトコル	TCP
			送信元 IP アドレス	any
			送信元ポート	any
		No.2	宛先 IP アドレス	10.10.10.1
			宛先ポート	80
			変換後宛先 IP アドレス	192.168.10.10
	eth1_dnat	No.2	プロトコル	TCP
			送信元 IP アドレス	any
			送信元ポート	any
宛先 IP アドレス			10.10.10.2	
		宛先ポート	80	

			変換後宛先 IP アドレス	192.168.10.20
IP フィルタ	ルール名			eth1_forward-in
	eth1_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.10
			プロトコル	TCP
			送信元ポート	any
			宛先ポート	80
	eth1_forward-in	No.2	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	192.168.10.20
宛先ポート			80	
DNS	サービス			有効
	DNS サーバ	プライマリ		10.255.1.1
		セカンダリ		10.255.1.2
FastForwarding				有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 10.10.10.6
nrx120(config)#ip dnat eth1_dnat tcp any any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip dnat eth1_dnat tcp any any 10.10.10.2 80 192.168.10.20
nrx120(config)#ip access-list eth1_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ip access-list eth1_forward-in permit any 192.168.10.20 tcp any 80
nrx120(config)#interface ethernet 1
nrx120(config-if)#ip address 10.10.10.1/29
nrx120(config-if)#ip address 10.10.10.2/29 secondary
nrx120(config-if)#ip dnat-group eth1_dnat
nrx120(config-if)#ip masquerade
nrx120(config-if)#ip access-group forward-in eth1_forward-in
nrx120(config-if)#ip spi-filter
nrx120(config-if)#ip tcp adjust-mss auto
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#address 10.255.1.1
nrx120(config-dns)#address 10.255.1.2
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#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。

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 名を eth1_dnat とし、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 アドレスは 192.168.10.10 に、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 アドレスは 192.168.10.20 に変換します。

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

IP アクセスリスト名を eth1_forward-in とし、宛先 IP アドレス 192.168.10.10,宛先 TCP ポート番号 80、宛先 IP アドレス 192.168.10.20,宛先 TCP ポート番号 80 のパケットを許可します。

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

ethernet1 インタフェースの IP アドレスおよびセカンダリ IP アドレスを設定します。

```
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)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、eth1_dnat を

DNAT グループに、IP アクセスリスト eth1_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

6. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

```
nrx120(config-dns)#address 10.255.1.1  
nrx120(config-dns)#address 10.255.1.2
```

プロバイダから通知されているプライマリ,セカンダリ DNS サーバアドレスを設定します。

7. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(🔗) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

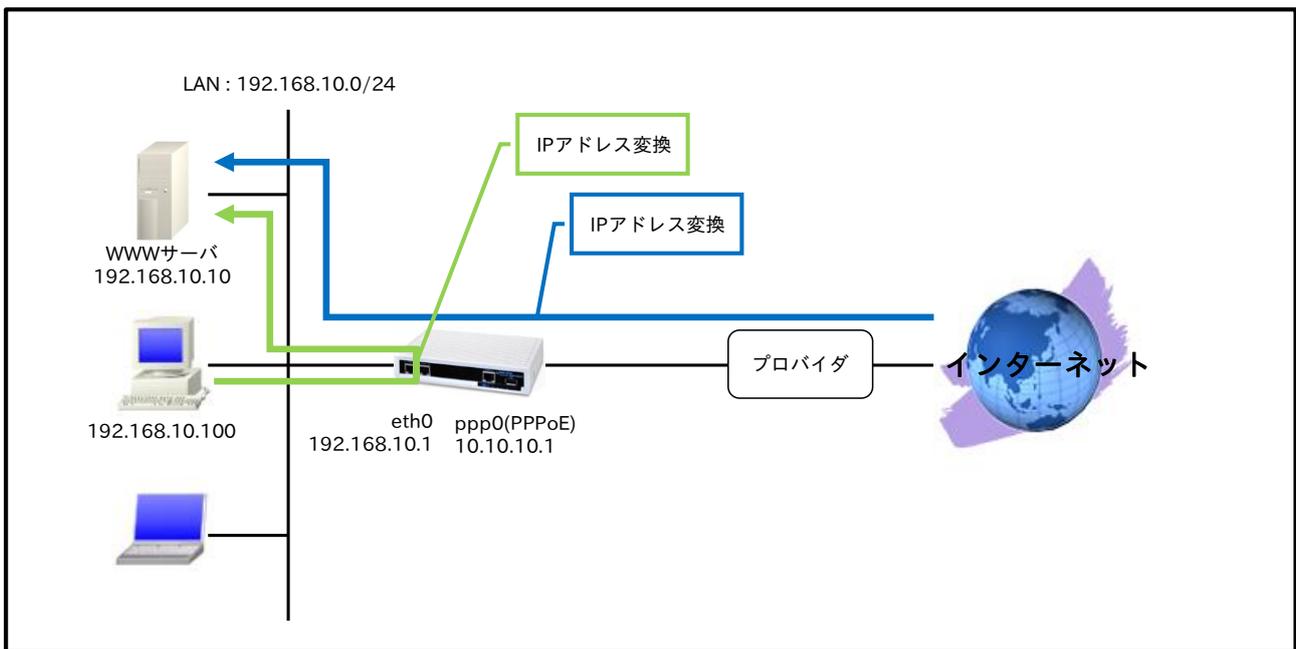
	端末	WWW サーバ 1	WWW サーバ 2
IP アドレス	192.168.10.100	192.168.10.10	192.168.10.20
サブネットマスク		255.255.255.0	
デフォルトゲートウェイ		192.168.10.1	
DNS サーバ	192.168.10.1		

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 アドレスでアクセスすることも可能です。この設定例では、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します。

【 構成図 】



【 設定データ 】

設定項目		設定内容	
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24	
	DNAT グループ	eth0_dnat	
	SNAT グループ	eth0_snat	
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0	
	ppp0 の IP アドレス	10.10.10.1/32	
	DNAT グループ	ppp0_dnat	
	IP マスカレード	有効	
	IP アクセスグループ	forward-in	
	SPI フィルタ	有効	
	MSS 自動調整	オート	
	ISP 接続用ユーザ ID	test1@example.jp	
	ISP 接続用パスワード	test1pass	
スタティックルート	宛先 IP アドレス	0.0.0.0/0	
	ゲートウェイ(インタフェース)	ppp0	
DNAT	ルール名	ppp0_dnat	
	ppp0_dnat	プロトコル	TCP
		送信元 IP アドレス	any
		送信元ポート	any
		宛先 IP アドレス	10.10.10.1

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

		宛先ポート	80
		変換後宛先 IP アドレス	192.168.10.10
	ルール名		eth0_dnat
	eth0_dnat	プロトコル	TCP
		送信元 IP アドレス	192.168.10.0/24
		送信元ポート	any
		宛先 IP アドレス	10.10.10.1
宛先ポート		80	
	変換後宛先 IP アドレス	192.168.10.10	
SNAT	ルール名		eth0_snat
	eth0_snat	プロトコル	TCP
		送信元 IP アドレス	192.168.10.0/24
		送信元ポート	any
		宛先 IP アドレス	192.168.10.10
		宛先ポート	80
変換後送信元 IP アドレス	192.168.10.1		
IP フィルタ	ルール名		ppp0_forward-in
	ppp0_forward-in	動作	許可
		送信元 IP アドレス	any
		宛先 IP アドレス	192.168.10.10
		プロトコル	TCP
		送信元ポート	any
宛先ポート	80		
DNS	サービス		有効
FastForwarding			有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip dnat eth0_dnat tcp 192.168.10.0/24 any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip snat eth0_snat tcp 192.168.10.0/24 any 192.168.10.10 80 192.168.10.1
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#ip dnat-group eth0_dnat
nrx120(config-if)#ip snat-group eth0_snat
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address 10.10.10.1/32
nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#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
```

DNAT 名を ppp0_dnat とし、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 に変換します。

なお、この DNAT 設定は ppp0 インタフェース設定で登録します。

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

DNAT 名を eth0_dnat とし、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 に変換します。

なお、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 名を eth0_snat とし、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 に変換します。

なお、この SNAT 設定は ethernet0 インタフェース設定で登録します。

(☞) SNAT 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 アドレスを設定します。

```
nxr120(config-if)#ip dnat-group eth0_dnat  
nxr120(config-if)#ip snat-group eth0_snat
```

eth0_dnat を DNAT グループに、eth0_snat を SNAT グループに適用します。

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。

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
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.10,宛先 TCP ポート番号 80

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

のパケットを許可します。

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。

6. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address 10.10.10.1/32
```

ppp0 インタフェースの IP アドレスを設定します。

```
nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

8. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

9. <DNS 設定>

```
nrx120(config)#dns
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズ

ガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

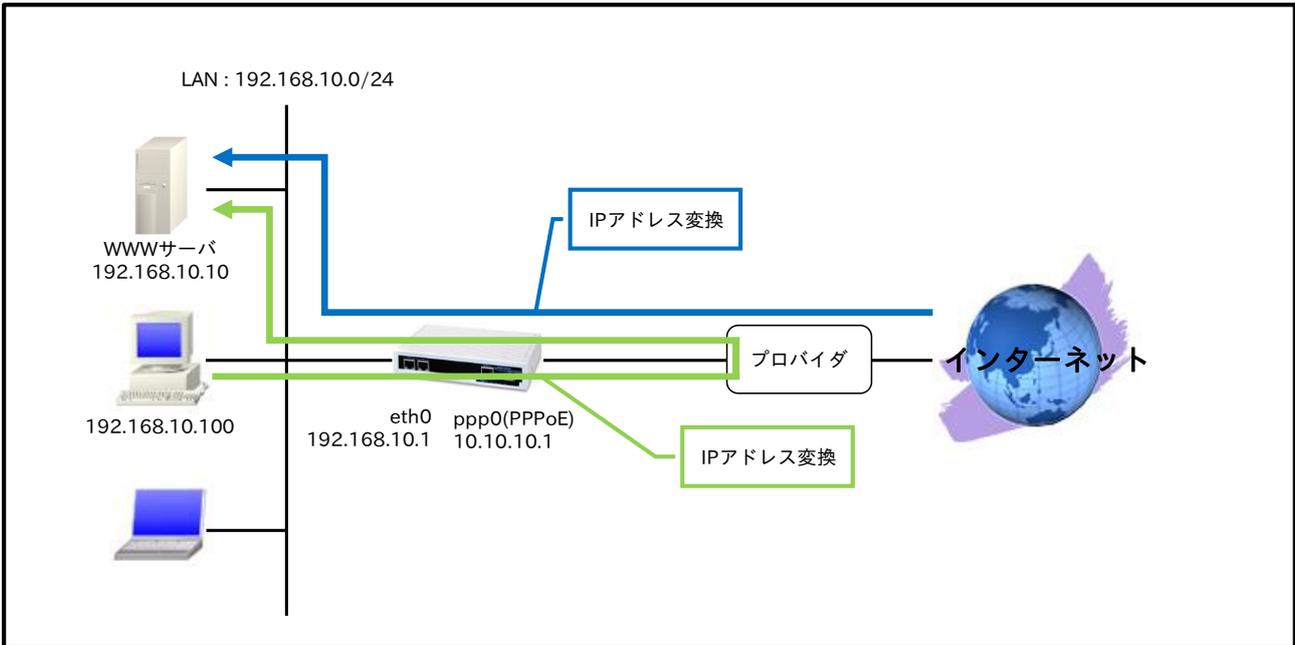
【 端末の設定例 】

	端末	WWW サーバ
IP アドレス	192.168.10.100	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	192.168.10.1	

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

この設定例では、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 配下の端末からグローバル IP アドレスでアクセスします。

【 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、ルータ自身で受信せず一旦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。

(注) 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(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。

【 設定データ 】

設定項目		設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	10.10.10.1/32
	IP nat-loopback	有効
	DNAT グループ	ppp0_dnat
	IP マスカレード	有効
	IP アクセスグループ	forward-in
	SPI フィルタ	有効

	MSS 自動調整		オート
	ISP 接続用ユーザ ID		test1@example.jp
	ISP 接続用パスワード		test1pass
スタティックルート	宛先 IP アドレス		0.0.0.0/0
	ゲートウェイ(インタフェース)		ppp0
DNAT	ルール名		ppp0_dnat
	ppp0_dnat	プロトコル	TCP
		送信元 IP アドレス	any
		送信元ポート	any
		宛先 IP アドレス	10.10.10.1
		宛先ポート	80
変換後宛先 IP アドレス	192.168.10.10		
IP フィルタ	ルール名		ppp0_forward-in
	ppp0_forward-in	動作	許可
		送信元 IP アドレス	any
		宛先 IP アドレス	192.168.10.10
		プロトコル	TCP
		送信元ポート	any
宛先ポート	80		
DNS	サービス		有効
FastFowarding			有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip nat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address 10.10.10.1/32
nrx120(config-ppp)#ip nat-loopback
nrx120(config-ppp)#ip nat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <DNAT 設定>

```
nrx120(config)#ip dnat ppp0_dnat tcp any any 10.10.10.1 80 192.168.10.10
```

DNAT 名を ppp0_dnat とし、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 に変換します。

なお、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>

```
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.10,宛先 TCP ポート番号 80 のパケットを許可します。

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。

5. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

6. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address 10.10.10.1/32
```

ppp0 インタフェースの IP アドレスを設定します。

```
nrx120(config-ppp)#ip nat-loopback
```

ip nat-loopback 機能を有効にします。

```

nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto

```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```

nrx120(config-ppp)#ppp username test1@example.jp

```

ISP 接続用ユーザ ID を設定します。

7. <ethernet1 インタフェース設定>

```

nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0

```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

8. <DNS 設定>

```

nrx120(config)#dns
nrx120(config-dns)#service enable

```

DNS サービスを有効にします。

9. <ファストフォワーディングの有効化>

```

nrx120(config)#fast-forwarding enable

```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

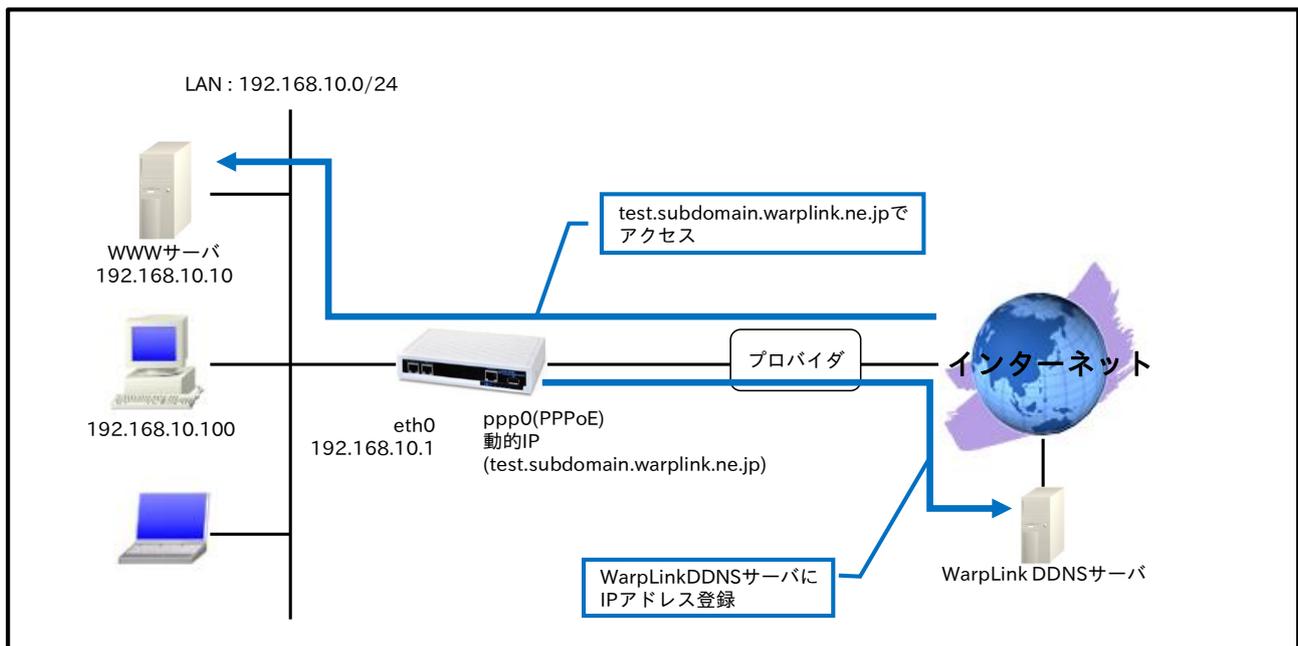
【 端末の設定例 】

	端末	WWW サーバ
IP アドレス	192.168.10.100	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	192.168.10.1	

3-6. NAT でのサーバ公開 6(DDNS の利用)設定

ダイナミック DNS を利用することで、公開サーバへのアクセスに IP アドレスではなく FQDN を利用することができ、ルータの WAN 側 IP アドレスが不定の環境でも外部からサーバにアクセスすることができます。この設定例では、ダイナミック DNS サービスとして弊社が提供している WarpLinkDDNS サービスを使用します。

【 構成図 】



- ルータで WarpLink 機能を設定し、WarpLinkDDNS サービスを動作させます。
(※) WarpLinkDDNS サービスは弊社が提供している有償の DDNS サービスとなります。
詳細は下記 URL からご確認下さい。
<http://www.warplink.ne.jp/ddns/index.html>
- ルータは自身の IP アドレスを WarpLinkDDNS サーバに登録します。そして、サーバにアクセスしたい端末は WarpLinkDDNS サーバに登録されているルータの FQDN を指定してアクセスします。

【 設定データ 】

設定項目		設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	DNAT グループ	ppp0_dnat
	IP マスカレード	有効
	IP アクセスグループ	forward-in
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
ISP 接続用パスワード	test1pass	
スタティックルート	宛先 IP アドレス	0.0.0.0/0

	ゲートウェイ(インタフェース)	ppp0	
DNAT	ルール名	ppp0_dnat	
	ppp0_dnat	プロトコル	TCP
		送信元 IP アドレス	any
		送信元ポート	any
		宛先 IP アドレス	any
		宛先ポート	80
変換後宛先 IP アドレス	192.168.10.10		
IP フィルタ	ルール名	ppp0_forward-in	
	ppp0_forward-in	動作	許可
		送信元 IP アドレス	any
		宛先 IP アドレス	192.168.10.10
		プロトコル	TCP
送信元ポート	any		
宛先ポート	80		
WarpLink	サービス	有効	
	WarpLinkDDNS サービス接続用ユーザ ID	warplinksample	
	WarpLinkDDNS サービス接続用パスワード	warplinksamplepass	
DNS	サービス	有効	
FastForwarding		有効	

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ip dnat ppp0_dnat tcp any any any 80 192.168.10.10
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip dnat-group ppp0_dnat
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#warplink
nrx120(config-warplink)#service enable
nrx120(config-warplink)#account username warplinksample password warplinksamplepass
nrx120(config-warplink)#exit
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <DNAT 設定>

```
nrx120(config)#ip dnat ppp0_dnat tcp any any any 80 192.168.10.10
```

DNAT 名を ppp0_dnat とし、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 に変換します。

なお、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>

```
nrx120(config)#ip access-list ppp0_forward-in permit any 192.168.10.10 tcp any 80
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 192.168.10.10、宛先 TCP ポート番号 80 のパケットを許可します。

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。

5. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID、パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

6. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip dnat-group ppp0_dnat  
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip access-group forward-in ppp0_forward-in  
nrx120(config-ppp)#ip spi-filter
```

```
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、ppp0_dnat を DNAT グループに、IP アクセスリスト ppp0_forward-in を forward-in フィルタに適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

7. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

8. <WarpLink 設定>

```
nrx120(config)#warplink  
nrx120(config-warplink)#service enable
```

WarpLink サービスを有効にします。

```
nrx120(config-warplink)#account username warplinksample password warplinksamplepass
```

WarpLinkDDNS サービス接続用のユーザ ID とパスワードを設定します。

9. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

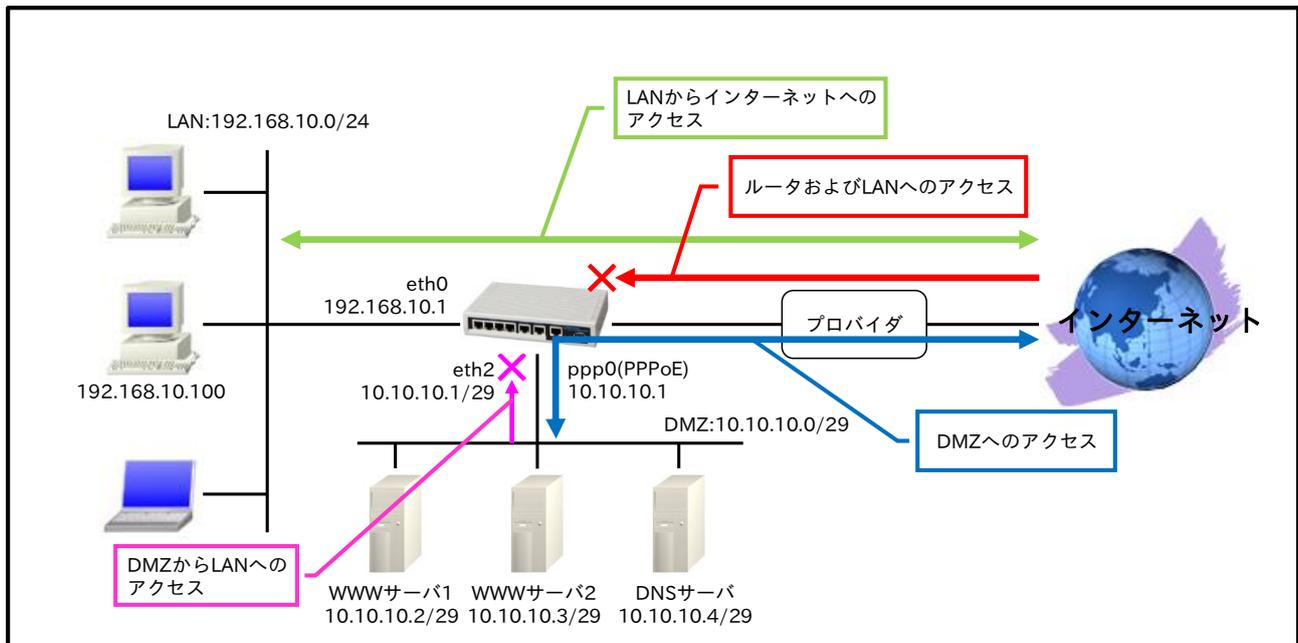
【 端末の設定例 】

	端末	WWW サーバ
IP アドレス	192.168.10.100	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	192.168.10.1	

3-7. 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、かつ 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は原則破棄しますが、以下のアクセスのみ許可します。
 - 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 IP アドレス 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、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。

【 設定データ 】

設定項目		設定内容		
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24		
DMZ 側インタフェース	ethernet2 の IP アドレス	10.10.10.1/29		
	SPI フィルタ	有効		
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0		
	ppp0 の IP アドレス	10.10.10.1/32		
	SNAT グループ	ppp0_snat		
	IP アクセスグループ	in	ppp0_in	
		forward-in	ppp0_forward-in	
		forward-out	ppp0_forward-out	
	SPI フィルタ	有効		
	MSS 自動調整	オート		
ISP 接続用ユーザ ID	test1@example.jp			
ISP 接続用パスワード	test1pass			
スタティックルート	宛先 IP アドレス	0.0.0.0/0		
	ゲートウェイ(インタフェース)	ppp0		
SNAT	ルール名	ppp0_snat		
	ppp0_snat	プロトコル	IP	
		送信元 IP アドレス	192.168.10.0/24	
		宛先 IP アドレス	any	
		変換後送信元 IP アドレス	10.10.10.1	
IP フィルタ	ルール名	ppp0_in		
	ppp0_in	動作	破棄	
		送信元 IP アドレス	any	
		宛先 IP アドレス	10.10.10.1	
		プロトコル	ICMP	
		タイプ	8	
		コード	0	
	ルール名	ppp0_forward-in		
	ppp0_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	10.10.10.2
			プロトコル	TCP
			送信元ポート	any
			宛先ポート	80
		No.2	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	10.10.10.3
			プロトコル	TCP
			送信元ポート	any
			宛先ポート	80
No.3		動作	許可	
		送信元 IP アドレス	any	
		宛先 IP アドレス	10.10.10.4	
		プロトコル	TCP	
		送信元ポート	any	
		宛先ポート	53	
No.4		動作	許可	
		送信元 IP アドレス	any	
	宛先 IP アドレス	10.10.10.4		
	プロトコル	UDP		
	送信元ポート	any		
	宛先ポート	53		
No.5	動作	許可		
	送信元 IP アドレス	any		
	宛先 IP アドレス	10.10.10.0/29		
	プロトコル	ICMP		
	ppp0_forward-out	No.1	動作	許可
			送信元 IP アドレス	10.10.10.4

			宛先 IP アドレス	any
			プロトコル	TCP
			送信元ポート	any
			宛先ポート	53
	No.2	動作	許可	
		送信元 IP アドレス	10.10.10.4	
		宛先 IP アドレス	any	
		プロトコル	UDP	
			送信元ポート	any
			宛先ポート	53
DNS	サービス			有効
	DNS サーバ	プライマリ		10.10.10.4
FastForwarding				有効

【 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-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)#ppp account username test1@example.jp password test1pass
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)#ppp username test1@example.jp
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)#service enable
nxr230(config-dns)#address 10.10.10.4
nxr230(config-dns)#exit
nxr230(config)#fast-forwarding enable
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。

3. <SNAT 設定>

```
nxr230(config)#ip snat ppp0_snat ip 192.168.10.0/24 any 10.10.10.1
```

SNAT 名を ppp0_snat とし、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 に変換します。

なお、この SNAT 設定は ppp0 インタフェース設定で登録します。

(☞) SNAT 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
```

IP アクセスリスト名を ppp0_in とし、宛先 IP アドレス 10.10.10.1,ICMP タイプ 8 コード 0(ICMP Echo Request)のパケットを許可します。

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。

```
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
```

IP アクセスリスト名を ppp0_forward-in とし、宛先 IP アドレス 10.10.10.2~10.10.10.3,宛先 TCP ポート番号 80 のパケットを許可します。また、宛先 IP アドレス 10.10.10.4,宛先 TCP ポート番号 53 および UDP ポート番号 53 のパケットを許可します。また、宛先 IP アドレス 10.10.10.0/29 の ICMP パケットを許可します。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。

```
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
```

IP アクセスリスト名を ppp0_forward-out とし、送信元 IP アドレス 10.10.10.4,宛先 TCP ポート番号 53 および UDP ポート番号 53 のパケットを許可します。

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。

5. <PPP アカウント設定>

```
nxr230(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。
(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

6. <WAN 側(ppp0)インタフェース設定>

```
nxr230(config)#interface ppp 0  
nxr230(config-ppp)#ip address 10.10.10.1/32
```

ppp0 インタフェースの IP アドレスを設定します。

```
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
```

ステートフルパケットインスペクションを有効に設定します。また、ppp0_snat を SNAT グループに、IP アクセスリスト ppp0_in を in フィルタ、ppp0_forward-in を forward-in フィルタ、ppp0_forward-out を forward-out フィルタにそれぞれ適用します。そして、TCP MSS の調整機能をオートに設定します。

```
nxr230(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

7. <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
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

8. <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  
nxr230(config-if)#ip spi-filter
```

ethernet2 インタフェースの IP アドレスを設定します。また、ステートフルパケットインスペクションを有効に設定します。

9. <DNS 設定>

```
nxr230(config)#dns  
nxr230(config-dns)#service enable  
nxr230(config-dns)#address 10.10.10.4
```

DNS サービスを有効にします。また、DNS サーバアドレスとして DMZ の DNS サーバを設定します。

10. <ファストフォーワーディングの有効化>

```
nxr230(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 端末の設定例 】

	端末	WWW サーバ 1	WWW サーバ 2	DNS サーバ
IP アドレス	192.168.10.100	10.10.10.2	10.10.10.3	10.10.10.4
サブネットマスク	255.255.255.0	255.255.255.248		
デフォルトゲートウェイ	192.168.10.1	10.10.10.1		
DNS サーバ	192.168.10.1			

4. Web 認証設定

4-1. ユーザ認証設定

4-2. URL 転送設定

4-3. ユーザ強制認証+URL 転送

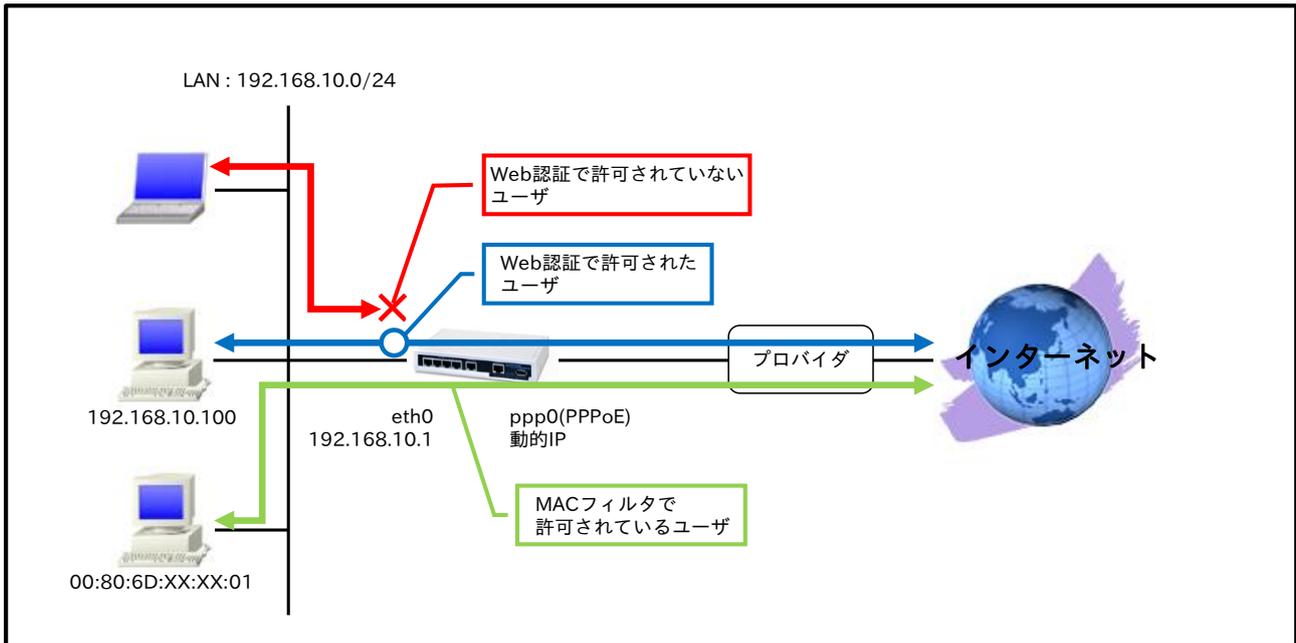
4-4. Web 認証フィルタ

4-5. RADIUS 連携

4-1. ユーザ認証設定

Web 認証ではルータ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できます。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 】



- ・ ルータ配下の端末はルータの 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ルータ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破棄することができます。

【 設定データ 】

	設定項目	設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	IP マスカレード	有効
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
	ISP 接続用パスワード	test1pass
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(インタフェース)	ppp0
Web 認証	認証方式	HTTP Basic
	接続許可時間(アイドルタイムアウト)	600 秒
	ログ取得	有効
	ローカル認証用ユーザ ID	test
	ローカル認証用パスワード	testpass
	MAC アクセスリスト	動作

		MAC アドレス	00:80:6D:XX:XX:01
		インタフェース	ethernet0
LED	AUX1		ppp0 アップ時点灯
DNS	サービス		有効
FastFowarding			有効

【 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)#ppp account username test1@example.jp password test1pass
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)#ppp username test1@example.jp
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:XX:XX:01 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)#fast-forwarding enable
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。

3. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

4. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

5. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

6. <システム LED 設定>

```
nrx120(config)#system led aux 1 interface ppp 0
```

ppp0 インタフェースのアップ/ダウンを aux1 LED で表示するように設定します。

7. <Web 認証設定>

```
nrx120(config)#web-authenticate  
nrx120(config-webauth)#authenticate basic
```

Web 認証(Basic 認証)を行うよう設定します。

```
nrx120(config-webauth)#close idle-timeout 600
```

認証で許可されたユーザとの間で、無通信状態になってから 600 秒経過すると通信を遮断するよう設定します。

```
nrx120(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 ID、パスワードを設定します。

```
nxr120(config-webauth)#mac access-list permit 00:80:6D:XX:XX:01 ethernet 0
```

MAC アクセスリストで MAC アドレス 00:80:6D:XX:XX:01 について ethernet0 インタフェースで許可するよう設定します。

(注) 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。

8. <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。

9. <DNS 設定>

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

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

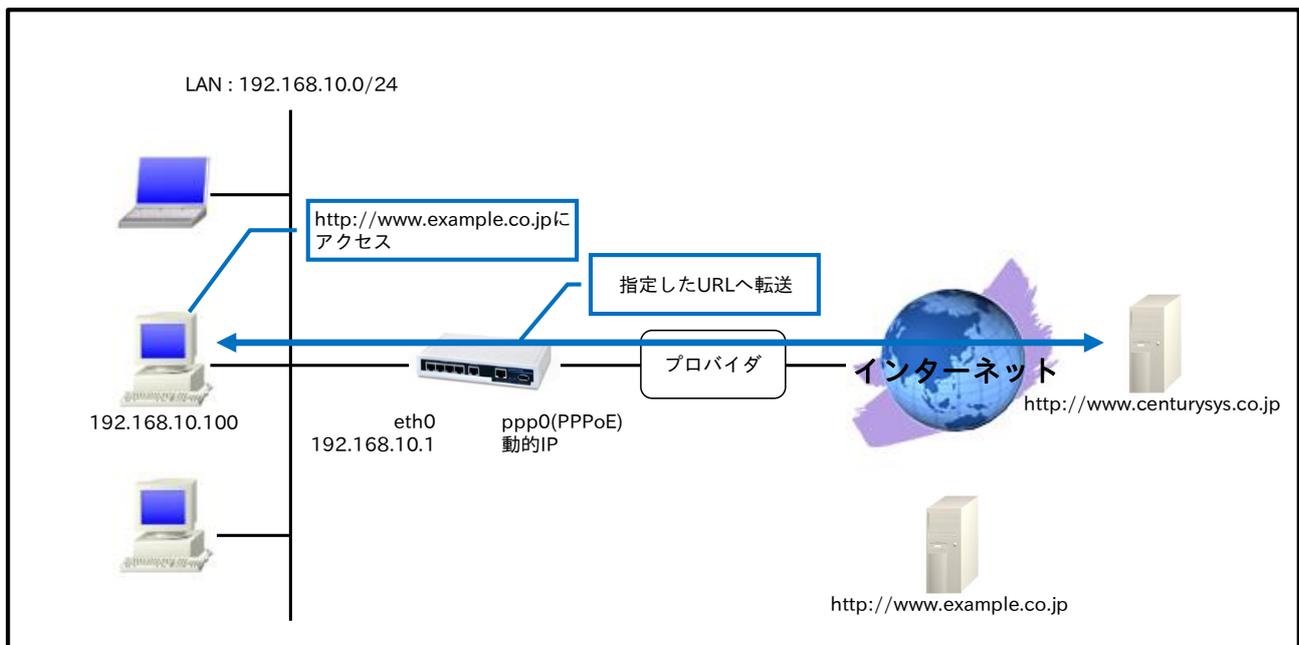
【 端末の設定例 】

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	

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、ルータ配下の端末が WEB アクセスを行った際に、あらかじめ設定した任意の URL へ転送させるということもできます。

【 構成図 】



- ・ ルータ配下の端末が TCP ポート 80 番で 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に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。

【 設定データ 】

	設定項目	設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	IP マスカレード	有効
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
	ISP 接続用パスワード	test1pass
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(インタフェース)	ppp0
Web 認証	強制認証	80 番ポート監視(リダイレクト)
	転送先 URL	http://www.centurysys.co.jp
	接続許可時間(アイドルタイムアウト)	600 秒
	ログ取得	有効
LED	AUX1	ppp0 アップ時点灯
DNS	サービス	有効
FastForwarding		有効

【 設定例 】

```
nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#system led aux 1 interface ppp 0
nrx120(config)#web-authenticate
nrx120(config-webauth)#monitor port 80 redirect
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
nrx120(config-webauth)#close idle-timeout 600
nrx120(config-webauth)#log enable
nrx120(config-webauth)#exit
% restart http-server to apply this setting.
nrx120(config)#exit
nrx120#restart http-server
http-server starting... done
nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config
```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

4. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

5. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

6. <システム LED 設定>

```
nrx120(config)#system led aux 1 interface ppp 0
```

ppp0 インタフェースのアップ/ダウンを aux1 LED で表示するように設定します。

7. <Web 認証設定>

```
nrx120(config)#web-authenticate  
nrx120(config-webauth)#monitor port 80 redirect
```

ルータ配下の端末から 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。

```
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

```
nrx120(config-webauth)#close idle-timeout 600
```

認証で許可されたユーザとの間で、無通信状態になってから 600 秒経過すると通信を遮断するよう設定します。

```
nrx120(config-webauth)#log enable
```

ログの取得を有効にします。

8. <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。

9. <DNS 設定>

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

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

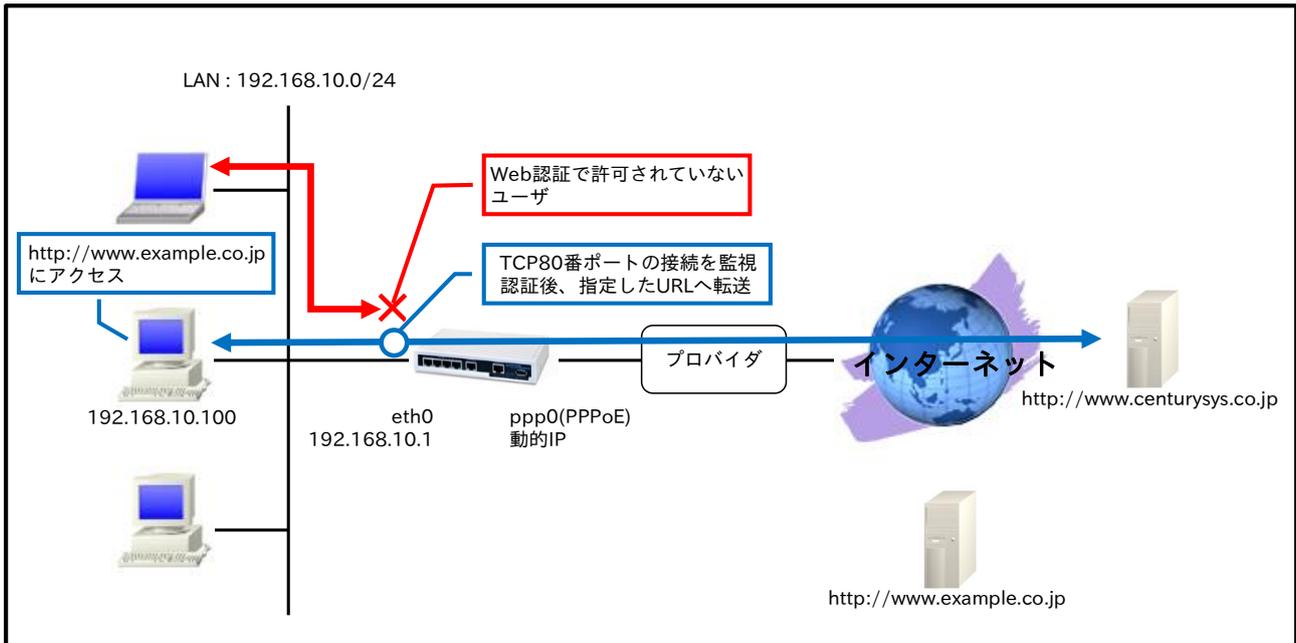
【 端末の設定例 】

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	

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、この設定例ではユーザ認証成功後、設定した URL へ転送します。

【 構成図 】



- ・ 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します。また、ユーザ認証成功後、指定した URL へ転送します。
- ・ 認証後、許可されたユーザとの間で、無通信状態になってから一定時間経過すると通信を遮断するよう設定します。

【 設定データ 】

	設定項目	設定内容
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
	ppp0 の IP アドレス	動的 IP アドレス
	IP マスカレード	有効
	SPI フィルタ	有効
	MSS 自動調整	オート
	ISP 接続用ユーザ ID	test1@example.jp
	ISP 接続用パスワード	test1pass
スタティックルート	宛先 IP アドレス	0.0.0.0/0
	ゲートウェイ(インタフェース)	ppp0
Web 認証	認証方式	HTTP Basic
	強制認証	80 番ポート監視(リダイレクト)
	転送先 URL	http://www.centurysys.co.jp
	接続許可時間(アイドルタイムアウト)	600 秒
	ログ取得	有効
	ローカル認証用ユーザ ID	test

	ローカル認証用パスワード	testpass
LED	AUX1	ppp0 アップ時点灯
DNS	サービス	有効
FastFowarding		有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#system led aux 1 interface ppp 0
nrx120(config)#web-authenticate
nrx120(config-webauth)#authenticate basic
nrx120(config-webauth)#monitor port 80 redirect
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
nrx120(config-webauth)#close idle-timeout 600
nrx120(config-webauth)#log enable
nrx120(config-webauth)#account username test password testpass
nrx120(config-webauth)#exit
% restart http-server to apply this setting.
nrx120(config)#exit
nrx120#restart http-server
http-server starting... done
nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```

nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24

```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```

nrx120(config)#ip route 0.0.0.0/0 ppp 0

```

デフォルトルートを設定します。

3. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

4. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

5. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

6. <システム LED 設定>

```
nrx120(config)#system led aux 1 interface ppp 0
```

ppp0 インタフェースのアップ/ダウンを aux1 LED で表示するように設定します。

7. <Web 認証設定>

```
nrx120(config)#web-authenticate  
nrx120(config-webauth)#authenticate basic  
nrx120(config-webauth)#monitor port 80 redirect
```

Web 認証(Basic 認証)を行い、ルータ配下の未認証端末から WEB アクセスした際、Web 認証画面をポップアップし、認証後、指定した URL へ転送します。

```
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

```
nrx120(config-webauth)#close idle-timeout 600
```

認証で許可されたユーザとの間で、無通信状態になってから 600 秒経過すると通信を遮断するよう設定し

ます。

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

ログの取得を有効にします。

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

ローカル認証用のユーザ ID、パスワードを設定します。

8. <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。

9. <DNS 設定>

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

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

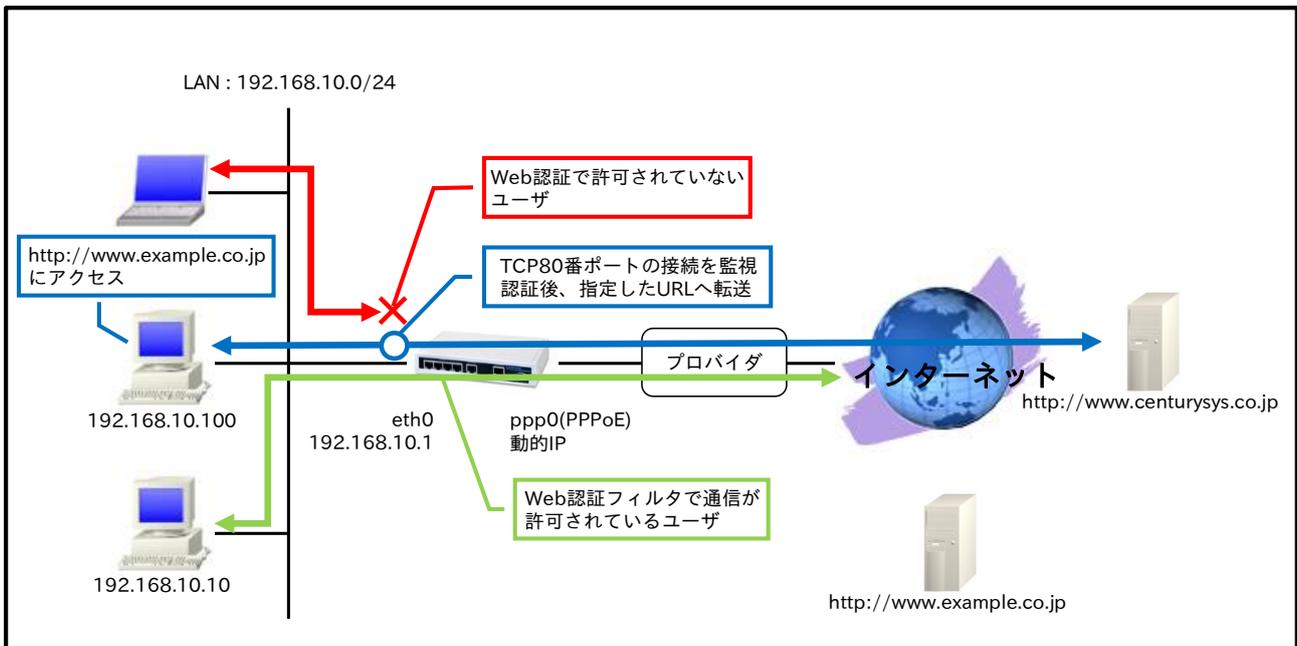
【 端末の設定例 】

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	

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,インタフェースでは Web 認証せずに通信することができます。

【 構成図 】



【 設定データ 】

設定項目		設定内容	
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24	
	Web 認証フィルタ	forward-in	
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0	
	ppp0 の IP アドレス	動的 IP アドレス	
	IP マスカレード	有効	
	SPI フィルタ	有効	
	MSS 自動調整	オート	
	ISP 接続用ユーザ ID	test1@example.jp	
	ISP 接続用パスワード	test1pass	
スタティックルート	宛先 IP アドレス	0.0.0.0/0	
	ゲートウェイ(インタフェース)	ppp0	
Web 認証	認証方式	HTTP Basic	
	強制認証	80 番ポート監視(リダイレクト)	
	転送先 URL	http://www.centurysys.co.jp	
	接続許可時間(アイドルタイムアウト)	600 秒	
	ログ取得	有効	
	ローカル認証用ユーザ ID	test	
Web 認証フィルタ	ローカル認証用パスワード	testpass	
	ルール名	eth0_web_forward-in	
	eth0_web_forward-in	動作	許可
		送信元 IP アドレス	192.168.10.10
宛先 IP アドレス		any	
LED	AUX1	ppp0 アップ時点灯	
DNS	サービス	有効	

FastForwarding	有効
----------------	----

【 設定例 】

```
nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#ip web-auth access-list eth0_web_forward-in permit 192.168.10.10 any
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#ip webauth-filter forward-in eth0_web_forward-in
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#system led aux 1 interface ppp 0
nrx120(config)#web-authenticate
nrx120(config-webauth)#authenticate basic
nrx120(config-webauth)#monitor port 80 redirect
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
nrx120(config-webauth)#close idle-timeout 600
nrx120(config-webauth)#log enable
nrx120(config-webauth)#account username test password testpass
nrx120(config-webauth)#exit
% restart http-server to apply this setting.
nrx120(config)#exit
nrx120#restart http-server
http-server starting... done
nrx120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config
```

【 設定例解説 】

1. <Web 認証アクセスリスト>

```
nrx120(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。Web 認証アクセスリスト名を eth0_web_forward-in とし、送信元 IP アドレス 192.168.10.10 のパケットを許可します。

なお、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。フィルタリングしたいインタフェースでの登録が必要になります。

2. <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 アドレスを設定します。

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

Web 認証アクセスリスト eth0_web_forward-in を webauth-filter の forward-in フィルタに適用します。

3. <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。

4. <PPP アカウント設定>

```
nxr120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID、パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

5. <WAN 側(ppp0)インタフェース設定>

```
nxr120(config)#interface ppp 0  
nxr120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

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

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nxr120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

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
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

7. <システム LED 設定>

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

ppp0 インタフェースのアップ/ダウンを aux1 LED で表示するように設定します。

8. <Web 認証設定>

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

Web 認証(Basic 認証)を行い、ルータ配下の未認証端末から WEB アクセスした際、Web 認証画面をポップアップし、認証後、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。

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

認証で許可されたユーザとの間で、無通信状態になってから 600 秒経過すると通信を遮断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。

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

ローカル認証用のユーザ ID、パスワードを設定します。

9. <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。

10. <DNS 設定>

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

DNS サービスを有効にします。

11. <ファストフォワーディングの有効化>

```
nxr120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

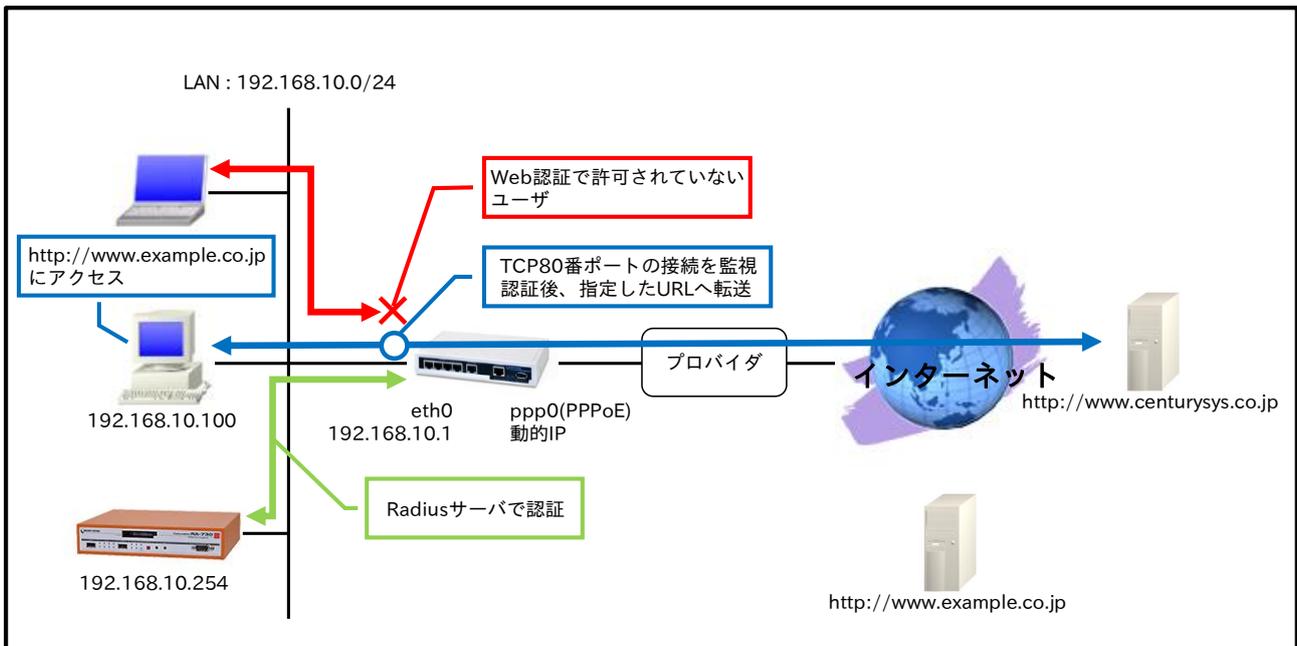
【 端末の設定例 】

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	

4-5. RADIUS 連携

Web 認証機能は、RADIUS サーバと連携することができます。これによりユーザ管理を RADIUS サーバに一任することができます。

【 構成図 】



- Web 認証機能のユーザ認証に RADIUS サーバを利用します。
- この設定例では、ユーザ認証に弊社 FutureNet RA シリーズを利用して動作確認を行っています。
<http://www.centurysys.co.jp/products/securityserver/index.html>

【 設定データ 】

設定項目		設定内容	
LAN 側インタフェース	ethernet0 の IP アドレス	192.168.10.1/24	
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0	
	ppp0 の IP アドレス	動的 IP アドレス	
	IP マスカレード	有効	
	SPI フィルタ	有効	
	MSS 自動調整	オート	
	ISP 接続用ユーザ ID	test1@example.jp	
	ISP 接続用パスワード	test1pass	
スタティックルート	宛先 IP アドレス	0.0.0.0/0	
	ゲートウェイ(インタフェース)	ppp0	
Web 認証	認証方式	HTTP Basic	
	強制認証	80 番ポート監視(リダイレクト)	
	転送先 URL	http://www.centurysys.co.jp	
	アカウント管理	RADIUS サーバ	
	RADIUS サーバ	IP アドレス	192.168.10.254
		秘密鍵(シークレット)	nrxpass
		UDP ポート番号	1812
RADIUS アトリビュート	NAS-IP-Address	192.168.10.1	
	NAS-Identifier	nrxwebauth	

	session timeout	Session-Timeout
	接続許可時間(強制切断タイムアウト)	1800 秒
LED	AUX1	ppp0 アップ時点灯
DNS	サービス	有効
FastFowarding		有効

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#interface ethernet 0
nrx120(config-if)#ip address 192.168.10.1/24
nrx120(config-if)#exit
nrx120(config)#ip route 0.0.0.0/0 ppp 0
nrx120(config)#ppp account username test1@example.jp password test1pass
nrx120(config)#interface ppp 0
nrx120(config-ppp)#ip address negotiated
nrx120(config-ppp)#ip masquerade
nrx120(config-ppp)#ip spi-filter
nrx120(config-ppp)#ip tcp adjust-mss auto
nrx120(config-ppp)#ppp username test1@example.jp
nrx120(config-ppp)#exit
nrx120(config)#interface ethernet 1
nrx120(config-if)#no ip address
nrx120(config-if)#pppoe-client ppp 0
nrx120(config-if)#exit
nrx120(config)#system led aux 1 interface ppp 0
nrx120(config)#web-authenticate
nrx120(config-webauth)#authenticate basic
nrx120(config-webauth)#monitor port 80 redirect
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
nrx120(config-webauth)#account authenticate radius
nrx120(config-webauth)#radius 192.168.10.254 password nxrpass auth-port 1812
nrx120(config-webauth)#radius attribute nas-ip-address 192.168.10.1
nrx120(config-webauth)#radius attribute nas-identifier nxrwebauth
nrx120(config-webauth)#close session-timeout 1800
nrx120(config-webauth)#radius session-timeout attribute session-timeout
nrx120(config-webauth)#exit
% restart http-server to apply this setting.
nrx120(config)#exit
nrx120#restart http-server
http-server starting... done
nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#dns
nrx120(config-dns)#service enable
nrx120(config-dns)#exit
nrx120(config)#fast-forwarding enable
nrx120(config)#exit
nrx120#save config

```

【 設定例解説 】

1. <LAN 側(ethernet0)インタフェース設定>

```
nrx120(config)#interface ethernet 0  
nrx120(config-if)#ip address 192.168.10.1/24
```

ethernet0 インタフェースの IP アドレスを設定します。

2. <スタティックルート設定>

```
nrx120(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。

3. <PPP アカウント設定>

```
nrx120(config)#ppp account username test1@example.jp password test1pass
```

ppp0 インタフェースで使用する ISP 接続用ユーザ ID,パスワードを設定します。

(※) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

4. <WAN 側(ppp0)インタフェース設定>

```
nrx120(config)#interface ppp 0  
nrx120(config-ppp)#ip address negotiated
```

ppp0 インタフェースの IP アドレスが動的 IP アドレスの場合は、negotiated を設定します。

```
nrx120(config-ppp)#ip masquerade  
nrx120(config-ppp)#ip spi-filter  
nrx120(config-ppp)#ip tcp adjust-mss auto
```

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、TCP MSS の調整機能をオートに設定します。

```
nrx120(config-ppp)#ppp username test1@example.jp
```

ISP 接続用ユーザ ID を設定します。

5. <ethernet1 インタフェース設定>

```
nrx120(config)#interface ethernet 1  
nrx120(config-if)#no ip address  
nrx120(config-if)#pppoe-client ppp 0
```

PPPoE クライアントとして ppp0 インタフェースを使用できるように設定します。

6. <システム LED 設定>

```
nrx120(config)#system led aux 1 interface ppp 0
```

ppp0 インタフェースのアップ/ダウンを aux1 LED で表示するように設定します。

7. <Web 認証設定>

```
nrx120(config)#web-authenticate  
nrx120(config-webauth)#authenticate basic  
nrx120(config-webauth)#monitor port 80 redirect
```

Web 認証(Basic 認証)を行い、ルータ配下の未認証端末から WEB アクセスした際、Web 認証画面をポップアップし、認証後、指定した URL へ転送します。

```
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

```
nrx120(config-webauth)#account authenticate radius
```

ユーザ名、パスワードの認証に RADIUS サーバを利用するよう設定します。

(☞) この設定例では RADIUS サーバでのみ認証を行います。RADIUS への認証要求タイムアウト後、ローカル認証を行うように設定することも可能です。

```
nrx120(config-webauth)#radius 192.168.10.254 password nxrpass auth-port 1812
```

RADIUS サーバの IP アドレス、秘密鍵、認証用 UDP ポート番号を設定します。

```
nrx120(config-webauth)#radius attribute nas-ip-address 192.168.10.1  
nrx120(config-webauth)#radius attribute nas-identifier nxrwebauth
```

RADIUS サーバに通知するアトリビュートとして NAS-IP-Address、NAS-Identifier を設定します。

```
nrx120(config-webauth)#close session-timeout 1800  
nrx120(config-webauth)#radius session-timeout attribute session-timeout
```

認証で許可された通信を強制的に切断するまでの時間を設定します。

この設定例では認証に RADIUS サーバのみ利用しているため、close session-timeout コマンドで設定した値は参照されず、RADIUS サーバで指定した応答アトリビュートの値のみが参照されます。

(☞) account authenticate コマンドで radius-and-local を指定している場合、RADIUS サーバへの認証要求タイムアウト後、close session-timeout コマンドで設定した値が参照されます。

8. <HTTP サーバ再起動>

```
nrx120#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。

9. <DNS 設定>

```
nrx120(config)#dns  
nrx120(config-dns)#service enable
```

DNS サービスを有効にします。

10. <ファストフォワーディングの有効化>

```
nrx120(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(注) ファストフォワーディングの詳細および利用時の制約については、NXR,WXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

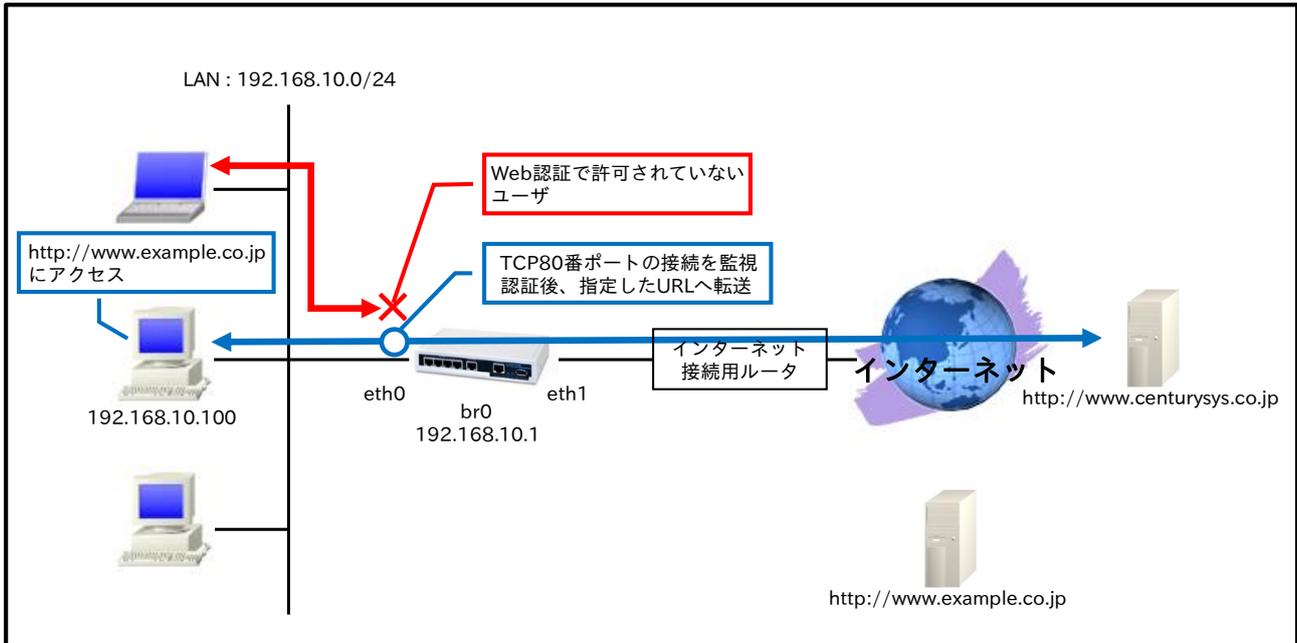
【 端末の設定例 】

	RADIUS サーバ	端末
IP アドレス	192.168.10.254	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		

4-6. ブリッジ+Web 認証設定

Web 認証機能は、ブリッジインタフェースでも利用することができます。これによりすでにルータ導入済みの環境にも Web 認証サービスを導入することができます。

【 構成図 】



- ・ 端末側で DNS サーバにインターネット接続用ルータを指定している場合、インターネットアクセス時の名前解決のみ行えるよう UDP ポート番号 53 のみ Web 認証フィルタで許可します。

【 設定データ 】

設定項目		設定内容		
ブリッジインタフェース	bridge0 の IP アドレス	192.168.10.1/24		
	ブリッジ対象インタフェース	ethernet0 ethernet1		
	Web 認証フィルタ	forward-in		
Web 認証	認証方式	HTTP Basic		
	強制認証	80 番ポート監視(リダイレクト)		
	転送先 URL	http://www.centurysys.co.jp		
	接続許可時間(アイドルタイムアウト)	600 秒		
	ログ取得	有効		
	ローカル認証用ユーザ ID	test		
	ローカル認証用パスワード	testpass		
Web 認証フィルタ	ルール名	br0_web_forward-in		
	br0_web_forward-in	No.1	動作	許可
			送信元 IP アドレス	any
			宛先 IP アドレス	any
			プロトコル	UDP
			送信元ポート	any
	宛先ポート	53		
	br0_web_forward-in	No.2	動作	許可
			送信元 IP アドレス	any
宛先 IP アドレス			any	

		プロトコル	UDP
		送信元ポート	53
		宛先ポート	any

【 設定例 】

```

nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#ip web-auth access-list br0_web_forward-in permit any any udp any 53
nrx120(config)#ip web-auth access-list br0_web_forward-in permit any any udp 53 any
nrx120(config)#interface bridge 0
nrx120(config-bridge)#ip address 192.168.10.1/24
nrx120(config-bridge)#bridge port 1 ethernet 0
nrx120(config-bridge)#bridge port 2 ethernet 1
nrx120(config-bridge)#ip webauth-filter forward-in br0_web_forward-in
nrx120(config-bridge)#exit
nrx120(config)#web-authenticate
nrx120(config-webauth)#authenticate basic
nrx120(config-webauth)#monitor port 80 redirect
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
nrx120(config-webauth)#close idle-timeout 600
nrx120(config-webauth)#log enable
nrx120(config-webauth)#account username test password testpass
nrx120(config-webauth)#exit
% restart http-server to apply this setting.
nrx120(config)#exit
nrx120#restart http-server
http-server starting... done
nrx120#save config

```

【 設定例解説 】

1. <Web 認証アクセスリスト>

```

nrx120(config)#ip web-auth access-list br0_web_forward-in permit any any udp any 53
nrx120(config)#ip web-auth access-list br0_web_forward-in permit any any udp 53 any

```

Web 認証アクセスリストを設定します。Web 認証アクセスリスト名を br0_web_forward-in とし、UDP ポート番号 53 のパケットの送受信を許可します。

なお、この Web 認証アクセスリスト設定は bridge0 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。フィルタリングしたいインタフェースでの登録が必要になります。

2. <bridge0 インタフェース設定>

```

nrx120(config)#interface bridge 0
nrx120(config-bridge)#ip address 192.168.10.1/24

```

bridge0 インタフェースの IP アドレスを設定します。

```

nrx120(config-bridge)#bridge port 1 ethernet 0
nrx120(config-bridge)#bridge port 2 ethernet 1

```

ブリッジインタフェースで利用するインタフェースを設定します。

```

nrx120(config-bridge)#ip webauth-filter forward-in br0_web_forward-in

```

Web 認証アクセスリスト br0_web_forward-in を webauth-filter の forward-in フィルタに適用します。

3. <Web 認証設定>

```
nrx120(config)#web-authenticate  
nrx120(config-webauth)#authenticate basic  
nrx120(config-webauth)#monitor port 80 redirect
```

Web 認証(Basic 認証)を行い、ルータ配下の未認証端末から WEB アクセスする際、Web 認証画面をポップアップし、認証後、指定した URL へ転送します。

```
nrx120(config-webauth)#redirect-url http://www.centurysys.co.jp
```

転送する URL を設定します。

```
nrx120(config-webauth)#close idle-timeout 600
```

認証で許可されたユーザとの間で、無通信状態になってから 600 秒経過すると通信を遮断するよう設定します。

```
nrx120(config-webauth)#log enable
```

ログの取得を有効にします。

```
nrx120(config-webauth)#account username test password testpass
```

ローカル認証用のユーザ ID、パスワードを設定します。

4. <HTTP サーバ再起動>

```
nrx120#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。

【 端末の設定例 】

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	インターネット接続用
DNS サーバ	ルータの IP アドレス

フィルタ状態確認方法

NAT 状態確認方法

UPnP 状態確認方法

SIP-NAT 状態確認方法

Web 認証機能のユーザ認証方法

設定例 show config 形式サンプル

フィルタ状態確認方法

IP フィルタの状態(IPv4 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>

```

nrx120#show ip access-list
Chain ppp0_forward-in (1 references)
No.  packets  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.  packets  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。

ブリッジフィルタの状態を確認する場合は、show bridge access-list コマンドを使用します。

<実行例>

```

nrx120#show bridge access-list
Chain br0_eth0-forward-in
No.  packets  bytes target  rule-type
  1     1      46 permit  arp
  2    16    1756 permit  ip
  3     0       0 permit  arp
  4     0       0 permit  ip
  5     4     276 deny    any

Chain br0_eth0-in
No.  packets  bytes target  rule-type
  1     5     322 deny    any

```

(☞) detail オプションを追加することにより、さらに詳細な情報を確認することができます。

<実行例>

```

nrx120#show bridge access-list detail
Chain br0_eth0-forward-in
No.  packets  bytes target  rule-type
  1     1      46 permit  arp
    opcode request
    sender-mac 00:80:6D:XX:XX:00
    sender-ip 192.168.10.100
    target-ip 192.168.10.10
  2    16    1756 permit  ip
    mac source 00:80:6D:XX:XX:00
    source 192.168.10.100
    destination 192.168.10.10
    protocol tcp
    destination-port 80
  3     0       0 permit  arp
    opcode request
    sender-mac 00:80:6D:XX:XX:02
    sender-ip 192.168.10.102
    target-ip 192.168.10.11
  4     0       0 permit  ip
    mac source 00:80:6D:XX:XX:02

```

```
source 192.168.10.102
destination 192.168.10.11
protocol tcp
destination-port 22
5      4      276    deny      any
mac source any
mac destination any
```

Chain br0_eth0-in

```
No.  packets  bytes  target  rule-type
1      5      322    deny      any
mac source any
mac destination any
```

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>

```
nrx120#show ip dnats
Chain ppp0_dnats (1 references)
No.  packets  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>

```
nrx230#show ip snats
Chain eth2_snats (1 references)
No.  packets  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>

```
nrx120#show sip-nat
SIP-NAT is on
```

また、SIP-NAT に関連した情報を含むセッション情報を表示する場合は、show ip contrack コマンドを使用します。

<実行例>

```
nrx120#show ip contrack
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

-----
contrack count is 1.
```

Web 認証機能のユーザ認証方法

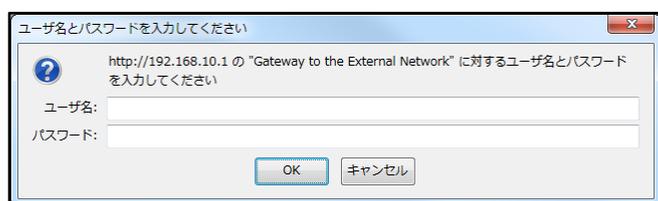
Web 認証使用時に NXR,WXR 経由で通信を行うには、原則ユーザ認証が必要となります。

(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,WXR 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,WXR 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の TCP80 番ポートへの接続を監視し、未認証ユーザから接続があった場合、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 5.24.1G (build 1/14:41 04 03 2014)  
!  
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
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 5.24.1G (build 1/14:41 04 03 2014)
!
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0  
 ip address negotiated  
 ip tcp adjust-mss auto  
 ip access-group forward-out ppp0_forward-out  
 ip masquerade  
 ip spi-filter  
 ppp username test1@example.jp  
!  
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
```

1-6. ブリッジフィルタ設定

```
!  
! Century Systems NXR-120 Series ver 5.24.1M (build 8/18:37 19 11 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
ipv6 forwarding  
no fast-forwarding enable  
!  
!  
!  
interface ethernet 0  
 ip address 192.168.0.254/24  
!  
interface ethernet 1  
 no ip address  
!  
interface bridge 0  
 bridge port 1 ethernet 0  
 bridge port 1 access-group in br0_eth0-in  
 bridge port 1 access-group forward-in br0_eth0-forward-in  
 bridge port 2 ethernet 1  
 ip address 192.168.10.1/24  
!  
dns  
 service enable  
!  
syslog  
 local enable  
!  
!  
!  
system led ext 0 signal-level mobile 0  
!  
!  
!  
!  
!  
bridge access-list br0_eth0-forward-in permit 1 arp  
 opcode request  
 sender-mac 00:80:6D:XX:XX:00  
 sender-ip 192.168.10.100  
 target-ip 192.168.10.10  
!  
bridge access-list br0_eth0-forward-in permit 2 ip  
 mac source 00:80:6D:XX:XX:00  
 source 192.168.10.100  
 destination 192.168.10.10  
 protocol tcp
```

```
destination-port 80
!
bridge access-list br0_eth0-forward-in permit 3 arp
opcode request
sender-mac 00:80:6D:XX:XX:02
sender-ip 192.168.10.102
target-ip 192.168.10.11
!
bridge access-list br0_eth0-forward-in permit 4 ip
mac source 00:80:6D:XX:XX:02
source 192.168.10.102
destination 192.168.10.11
protocol tcp
destination-port 22
!
bridge access-list br0_eth0-forward-in deny 5 any any any
!
bridge access-list br0_eth0-in deny 1 any any any
!
!
!
end
```

2-1. IP マスカレード設定

```
!
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
interface ethernet 0
ip address 192.168.10.1/24
!
interface ethernet 1
ip address 10.10.10.1/30
ip tcp adjust-mss auto
ip masquerade
ip spi-filter
!
dns
service enable
address 10.255.1.1
address 10.255.1.2
!
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 5.25.2 (build 1/19:25 19 01 2014)  
!  
hostname nxr230  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
!  
!  
!  
!  
ipv6 forwarding  
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 tcp adjust-mss auto  
 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 10.10.10.6  
!  
!  
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
!  
!  
interface ethernet 0  
 ip address 192.168.10.1/24  
!  
interface ethernet 1  
 ip address 10.10.10.1/30  
 ip tcp adjust-mss auto  
 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
```

2-5. UPnP 設定

```
!  
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)  
!
```

```
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username test1@example.jp password test1pass
!
!
interface ppp 0
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
!
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
```

2-6. SIP-NAT 設定 1

```
!
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)
!
hostname nxr120
telnet-server enable
http-server enable
!
```

```
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0  
ip address negotiated  
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@example.jp  
!  
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
```

2-7. SIP-NAT 設定 2

```
!  
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!
```

```
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0  
ip address negotiated  
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@example.jp  
!  
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!
```

```
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0  
 ip address 10.10.10.1/32  
 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@example.jp  
!  
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 10.10.10.1 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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server 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  
 ip tcp adjust-mss auto  
 ip access-group forward-in eth1_forward-in  
 ip masquerade  
 ip dnat-group eth1_dnat  
 ip spi-filter  
!  
dns  
 service enable  
 address 10.255.1.1  
 address 10.255.1.2  
!  
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0
```



```
ip address 10.10.10.1/32
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@example.jp
!
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
!
!
end
```

3-6. NAT でのサーバ公開 6(DDNS の利用)設定

```
!
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username test1@example.jp password test1pass
!
!
interface ppp 0
ip address negotiated
ip tcp adjust-mss auto
ip access-group forward-in ppp0_forward-in
```



```
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@example.jp
!
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 5.24.1G (build 1/14:41 04 03 2014)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
```

```
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!  
!  
interface ppp 0  
 ip address negotiated  
 ip tcp adjust-mss auto  
 ip masquerade  
 ip spi-filter  
 ppp username test1@example.jp  
!  
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:XX:XX:01 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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
!  
ipv6 forwarding
```

```
fast-forwarding enable
!
ppp account username test1@example.jp password test1pass
!
!
interface ppp 0
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
!
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 5.24.1G (build 1/14:41 04 03 2014)
!
hostname nxr120
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username test1@example.jp password test1pass
```

```
!  
!  
interface ppp 0  
  ip address negotiated  
  ip tcp adjust-mss auto  
  ip masquerade  
  ip spi-filter  
  ppp username test1@example.jp  
!  
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 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!  
ppp account username test1@example.jp password test1pass  
!
```

```
!  
interface ppp 0  
 ip address negotiated  
 ip tcp adjust-mss auto  
 ip masquerade  
 ip spi-filter  
 ppp username test1@example.jp  
!  
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
```

4-5. RADIUS 連携

```
!  
! Century Systems NXR-120 Series ver 5.24.1G (build 1/14:41 04 03 2014)  
!  
hostname nxr120  
telnet-server enable  
http-server enable  
!  
!  
!  
!  
ipv6 forwarding  
fast-forwarding enable  
!
```



```
no fast-forwarding enable
!
!
!
interface ethernet 0
 ip address 192.168.0.254/24
!
interface ethernet 1
 no ip address
!
interface bridge 0
 bridge port 1 ethernet 0
 bridge port 2 ethernet 1
 ip address 192.168.10.1/24
 ip webauth-filter forward-in br0_web_forward-in
!
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
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
!
ip web-auth access-list br0_web_forward-in permit any any udp any 53
ip web-auth access-list br0_web_forward-in permit any any udp 53 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

サポートデスクのご利用に関して

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/philosophy.html#tab3>

<http://www.centurysys.co.jp/company/philosophy.html#tab4>

■ ご利用頂いている NXR,WXR 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

○月○日○時○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

○月○日○時○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。
設定例集および設定例集内のログ一覧は未確認。

□ 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,WXR 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,WXR 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,WXR 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 - 17:00

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 シリーズ

設定例集

NAT,フィルタ編

Ver 1.4.0

2015 年 8 月

発行 センチュリー・システムズ株式会社

Copyright(c) 2009-2015 Century Systems Co., Ltd. All Rights Reserved.