ファイアウォール

概要・基本設定

本製品には、IP トラフィックフローの開始・終了を認識し、これに応じて動的なパケットフィルタリングを行うステートフルインスペクション型のファイアウォールが搭載されています。ここでは、ファイアウォールの基本的な設定方法について説明します。

IP フィルターとの比較

IP パケットのフィルタリングは、IP モジュールの「IP フィルター」によっても提供されています。フィルタリングの機能自体はほぼ同等ですが、設定項目や設定方法に細かい差異がありますので、運用上のニーズに応じてご使用ください。
汎用設計の IP フィルターに対して、ファイアウォールはインターネット接続を念頭に置いた設計になっており、最小限の設定で高い安全性を確保できるようになっています。
詳細については後述しますが、

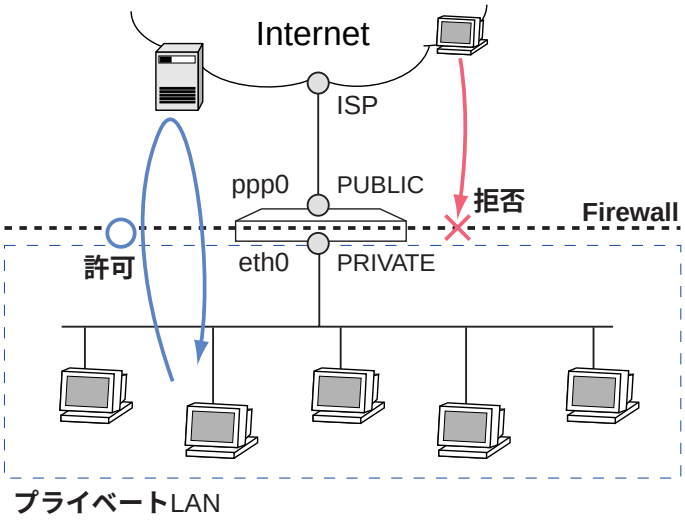
1. モジュールを有効化し、
2. ファイアウォールポリシーを作成し、
3. 外側（インターネット側）と内側（LAN 側）のインターフェースを指定する

の 3 つの手順だけで、LAN 側からインターネットへの通信は自由に行え、インターネットから LAN 側への通信はすべて拒否するという、ファイアウォールの基本ルールが有効になります。
IP フィルターがパケットごとにヘッダーを見て処理を行う単純なパケットフィルターであるのに対し、ファイアウォールはトラフィックフロー（一連のパケット）を常に意識しているため、LAN 側からの要求に対する応答パケットを通すために、Syn / Ack などによる細かい設定をする必要がありません。
たとえば、LAN 側のクライアントがインターネット上のサーバーと通信を開始したとします。ファイアウォールは、通信開始を検知すると該当セッションをテーブルに登録します。セッションは、ローカル側 IP アドレス、プロトコル、ポート、リモート側 IP アドレス、ポートなどの情報からなります。テーブルに記録されている間、セッションに該当するパケットは方向に関係なく通過させます。通信が終了するなどして一定時間通信が行われなくなると、テーブルからセッションを削除し、それ以降は同じサーバーからであっても、外部からのパケットは一切通過させません。このような処理を行うファイアウォールを、単純なパケットフィルタリング型ファイアウォールと対比して、ステートフルインスペクション型あるいはダイナミックパケットフィルタリングファイアウォールと呼びます。
また、ファイアウォールには NAT（Network Address Translation）の機能も統合されており、グローバルアドレスを 1 つしか割り当てられない端末型インターネット接続の環境においても、複数のホストがインターネットにアクセスできるよう設定できます。
さらに、ファイアウォールには、拒否・許可したパケットのログを記録する機能もあります。
なお、ファイアウォールと IP フィルターは併用できるため、基本的なセキュリティーの確保にはファイアウォールを使い、ファイアウォールで制御できない点（ICMP の方向制御など）を IP フィルターで補う設定も可能です。

基本設定

本製品をファイアウォールとして使用する上で最低限必要な手順は次のとおりです。ここでは次のような構

成のネットワークを想定しています。IP の設定までは終わっているものと仮定します。



1. ファイアウォール機能を有効にします。

   ```
   ENABLE FIREWALL ↵
   ```

2. ファイアウォールポリシーを作成します。ポリシー名は自由に付けられます。

   ```
   CREATE FIREWALL POLICY=mynet ↵
   ```

3. ファイアウォールポリシーの適用対象となる IP インターフェースを指定します。内側を PRIVATE、外側を PUBLIC に設定します。

   ```
   ADD FIREWALL POLICY=mynet INT=eth0 TYPE=PRIVATE ↵
   ADD FIREWALL POLICY=mynet INT=ppp0 TYPE=PUBLIC ↵
   ```

基本設定は以上です。
これにより、手順 3 で指定したインターフェース間のトラフィックに基本的なルールが適用され、外部（PUBLIC）から内部（PRIVATE）にはパケットが転送されなくなります。一方、内部から外部への通信は自由に行うことができます。ステートフルインスペクションにより、内部から通信を開始したときにはその状態が記憶されるため、戻りのパケットを通すために特別な設定をする必要はありません。
本製品では、上記の基本設定に独自のルールを追加することで、内部と外部のインターフェース間のやりとりを制御します。

■ 上記の基本設定だけでも十分実用的な運用が可能ですが、下記の設定を追加することにより、さらに快適に使用することができます。ここでは例だけを示します。詳細は他のセクションをご覧ください。

- ICMP パケットがファイアウォールを通過できるようにします。基本ルールでは、ICMP パケットはどちらの方向にもまったく転送されません（内部からの PING も通らないので注意してください）。

  ```
  ENABLE FIREWALL POLICY=mynet ICMP_F=PING,UNREACH ↵
  ```

- Ident プロキシー機能をオフにして、インターネット上のメールサーバーとの通信がすばやく行われるようにします。

  ```
  DISABLE FIREWALL POLICY=mynet IDENTPROXY ↵
  ```

- 拒否したパケットのログをとりたい場合は、次のコマンドを実行します。

  ```
  ENABLE FIREWALL POLICY=mynet LOG=DENY ↵
  ```

- 端末型接続のようにグローバルアドレスが 1 つしかない場合は、ダイナミック ENAT を使います。

  ```
  ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=eth0 GBLINT=ppp0 ↵
  ```

ここまでを基本設定と考えていただいてもかまいません。

インターフェースと基本ルール

ファイアウォールのインターフェースは次の 3 種類に分類されます。

- PRIVATE（内部）インターフェース：ファイアウォールで保護すべき内部ネットワーク側インターフェース。TYPE=PRIVATE でポリシーに追加されたインターフェースのこと
- PUBLIC（外部）インターフェース：ファイアウォールの外側に位置するインターフェース。TYPE=PUBLIC でポリシーに追加されたインターフェースのこと
- その他のインターフェース：ファイアウォールの管理対象でないインターフェース

各インターフェースの配下にあるホスト間の通信可否は次のとおりです。ただし ICMP は除きます。詳細は次節「ICMP パケットの扱い」をご覧ください。

送信元→宛先	PRIVATE	PUBLIC	**その他**
PRIVATE	○	○	×
PUBLIC	×	○	○
その他	×	○	○

表 1: インターフェース間の通信可否（ICMP を除く）

PRIVATE 側から PUBLIC 側へは通信を開始できますが、PRIVATE 以外のインターフェース（PUBLIC、その他）から PRIVATE 側への通信はすべて遮断します。これが基本ルールです。
ファイアウォールの動作をさらに細かく制御したい場合は、ADD FIREWALL POLICY RULE コマンド（36 ページ）で PRIVATE か PUBLIC インターフェースに独自ルールを追加します。独自ルールには次の種類があります。

- 拒否ルール：基本ルールでは素通しされるトラフィックを遮断する。通常 PRIVATE インターフェースに設定する。
- 許可ルール：基本ルールでは遮断されるトラフィックを通過させる。通常 PUBLIC インターフェースに設定する。

✎ 「その他」インターフェースに独自ルールを設定することはできません。

ICMP パケットの扱い

ファイアウォールは、前記の基本ルールと独自ルールにしたがってトラフィックを制御しますが、ICMP パケットだけはルールの例外扱いとなります。デフォルトの設定（ICMP 転送オフ時）では、PRIVATE・PUBLIC 間および PRIVATE・その他間では ICMP はどちら向きにも転送されません。

送信元→宛先	PRIVATE	PUBLIC	その他
PRIVATE	○	×	×
PUBLIC	×	○	○
その他	×	○	○

表 2: ICMP の通信可否（転送オフ時）

PRIVATE・PUBLIC 間で ICMP パケットの転送が行われるようにするには、ENABLE FIREWALL POLICY コマンド（51 ページ）の ICMP_FORWARDING パラメーターに転送する ICMP メッセージのタイプを指定します。ICMP メッセージをすべて通すなら ALL を指定します。転送をオンにしたときの ICMP の通信可否は次のようになります。

送信元→宛先	PRIVATE	PUBLIC	その他
PRIVATE	○	○	×
PUBLIC	○	○	○
その他	×	○	○

表 3: ICMP の通信可否（転送オン時）

✎ ICMP の転送をオンにしても、PRIVATE・その他間では転送されません（PRIVATE・その他間では、ICMP も含め、いっさい通信ができません）。

✎ ICMP は双方向とも通すか、まったく通さないかの設定しかできません。ファイアウォールの独自ルールでも ICMP パケットの通過・拒否は制御できませんので、片側からのみ通すような設定をしたい場合は IP フィルターを併用してください。

本体インターフェース宛ての通信

また、各インターフェース配下から本製品のインターフェース宛ての通信（Telnet など）可否は次のとおりです。

送信元→宛先 I/F	PRIVATE	PUBLIC	その他
PRIVATE	○	○	×
PUBLIC	×	×	×
その他	×	○	○

表 4: インターフェース配下から本体インターフェース宛ての通信可否

✎ 「その他」インターフェース配下から本体に対して Telnet が可能な点にご注意ください。

ルールの追加

上記の基本設定にルールを追加するには、ADD FIREWALL POLICY RULE コマンド（36 ページ）を使います。以下、いくつか例を示します。

✎ ルールを追加するときは、RULE パラメーターで指定するルール番号が重ならないようにしてください。また、ルールのチェックは番号の若い順に行われ、最初にマッチしたものが適用されるため、ルールの順序にも留意してください。

✎ ファイアウォールルールの設定ではコマンドラインが長くなりがちなので、適宜省略形を用いるようにしてください。以下の例でも省略形を使っています。

トラフィックを制限する

デフォルトでは内部から外部へのパケットをすべて通しますが（ICMP を除く）、予期せぬ発呼や情報の漏洩を防ぐため、不要なトラフィックを遮断することができます。

■ 次の例では、内部（eth0）からの MS-Networks パケット（Windows ネットワークなどで使用されるパケット）を遮断しています。ファイアウォールの基本ルールにより、その他のパケットはこれまでどおり通過が許可されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=DENY INT=eth0 PROT=TCP PORT=135 ↵
ADD FIREWALL POLICY=mynet RULE=2 AC=DENY INT=eth0 PROT=UDP PORT=135 ↵
ADD FIREWALL POLICY=mynet RULE=3 AC=DENY INT=eth0 PROT=TCP PORT=137-139 ↵
ADD FIREWALL POLICY=mynet RULE=4 AC=DENY INT=eth0 PROT=UDP PORT=137-139 ↵
ADD FIREWALL POLICY=mynet RULE=5 AC=DENY INT=eth0 PROT=TCP PORT=445 ↵
```

5 つのコマンドは、「eth0 インターフェースで受信した TCP、UDP パケットのうち、終点ポート番号が 135、137～139 のもの、および、TCP パケットのうち終点ポート番号が 445 番のものを破棄する」の意味になります。

■ 特定アドレスへのアクセスを禁止することもできます。この場合は REMOTEIP パラメーターで終点 IP アドレスを指定します。IP アドレスは範囲で指定することも可能です。次の例では、内部から 12.34.56.0～12.34.56.255 の範囲へのアクセスを禁止しています。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=DENY INT=eth0 PROT=ALL
  REMOTEIP=12.34.56.0-12.34.56.255 ↵
```

このコマンドは、「eth0 インターフェースで受信した IP パケットのうち、終点 IP アドレスが 12.34.56.0～12.34.56.255 のものを破棄する」の意味になります。

✎ デフォルトでは ICMP はファイアウォールを通過しません。ICMP の転送を有効にするには、ENABLE FIREWALL POLICY コマンド（51 ページ）の ICMP_FORWARDING オプションを使う必要があります。

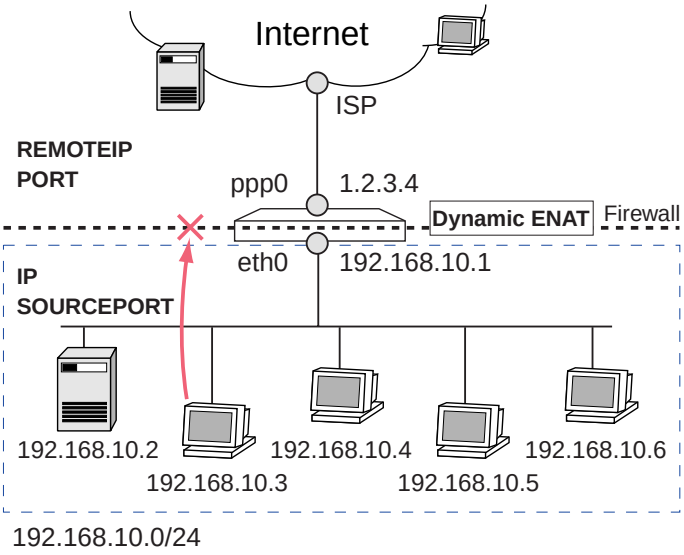
■ また、特定の内部ホストが外部にアクセスできないようにすることもできます。この場合は IP パラメーターで始点 IP アドレスを指定します。IP アドレスは範囲で指定することも可能です。次の例では、内部ホ

スト 192.168.10.3 からのパケットを破棄するよう設定しています。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=DENY INT=eth0 PROT=ALL
  IP=192.168.10.3 ↵
```

このコマンドは、「eth0 インターフェースで受信した IP パケットのうち、始点 IP アドレスが 192.168.10.3 のものを破棄する」の意味になります。

■ 内部からのトラフィックを制限するときのパラメーターの指定方法をまとめます



パラメーター	指定する内容
ACTION	内部から外部への転送を拒否するため DENY を指定します。
INTERFACE	内部（PRIVATE）インターフェースを指定します。
PROTOCOL	対象となるプロトコルを指定します。TCP、UDP を指定した場合は PORT の指定も必要です。ALL を指定した場合は ICMP を除くすべての IP パケットが対象となります。また、プロトコル番号による指定も可能です。
REMOTEIP	終点 IP アドレス。パケットの宛先となる外部ホストの IP アドレスです（範囲指定可）。省略時はすべての終点 IP アドレスが対象となります。
PORT	終点ポート番号。パケットの宛先となる外部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。
IP	始点 IP アドレス。パケットの送信元となる内部ホストの IP アドレスです（範囲指定可）。省略時はすべての始点 IP アドレスが対象となります。
SOURCEPORT	始点ポート番号。パケットの送信元となる内部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合のみ有効。省略時はすべての始点ポートが対象となります。

表 5:

アクセスを許可する

デフォルトでは外部からのパケットをすべて拒否しますが、内部の Web サーバーにだけはアクセスさせたいような場合に、特定の IP アドレス、または、IP アドレス・ポート宛てのパケットのみ通過を許可する設定ができます。ただし、外部からのパケットを許可することはファイアウォールに穴をあけることであり、セキュリティー低下のリスクが伴いますので設定には十分ご注意ください。

■ 次の例では、PRIVATE・PUBLIC 間で NAT を使用していないことを前提に、外部（ppp0）から内部ホスト 4.4.4.2 へのアクセスを許可しています。ファイアウォールの基本ルールにより、その他のホストに対するアクセスはこれまでどおり拒否されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=ALL IP=4.4.4.2 ↵
```

このコマンドは、「ppp0 インターフェースで受信した IP パケットのうち、終点 IP アドレスが 4.4.4.2 のものを通過させる」の意味になります。

✎ PROTOCOL=ALL はすべての IP プロトコルの意味ですが、ICMP は含まれません。ICMP の転送を有効にするには、ENABLE FIREWALL POLICY コマンド（51 ページ）の ICMP_FORWARDING オプションを使う必要があります。

■ 次の例では、外部（ppp0）から内部の Web サーバー（4.4.4.2 の TCP ポート 80 番）へのアクセスのみを許可しています。ファイアウォールの基本ルールにより、その他のアドレス・ポートへのアクセスはこれまでどおり拒否されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=TCP IP=4.4.4.2
  PORT=80 ↵
```

このコマンドは、「ppp0 インターフェースで受信した TCP パケットのうち、終点 IP アドレスが 4.4.4.2 で、終点ポートが 80 のものを通過させる」の意味になります。

■ 特定ホストからのみアクセスを許可する設定も可能です。これには REMOTEIP パラメーターを使用します。次の例では、外部のホスト 12.34.56.78 からのみ内部（PRIVATE 側）へのアクセスを許可しています。ファイアウォールの基本ルールにより、その他のホストからのアクセスはこれまでどおり拒否されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=ALL
  REMOTEIP=12.34.56.78 ↵
```

このコマンドは、「ppp0 インターフェースで受信した IP パケットのうち、始点 IP アドレスが 12.34.56.78 のものを通過させる」の意味になります。

■ NAT を使用しているインターフェースを通じてアクセスを受け入れる場合は、NAT の変換前後の両方のアドレスを指定する必要があります。たとえば、192.168.1.2 と 4.4.4.2 を一対一で変換するスタティック NAT を設定している場合、外部（ppp0）から 4.4.4.2（実際は 192.168.1.2）へのアクセスを許可するには次のようにします。ファイアウォールの基本ルールにより、その他のホストに対するアクセスはこれまでどおり拒否されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=ALL GBLIP=4.4.4.2
  IP=192.168.1.2 ↵
```

このコマンドは、「ppp0 インターフェースで受信した IP パケットのうち、終点 IP アドレスが 4.4.4.2 のものを、終点アドレスを 192.168.1.2 に書き換えた上で通過させる」の意味になります。

✎ この設定が機能するためには、あらかじめスタティック NAT の設定が必要です。この例では、次のような設定になります。また、下記のスタティック NAT の設定だけでは、グローバル側からのパケットがファイアウォールの基本ルールで遮断されるため、前述のような許可ルールも必須です。スタティック NAT の設定詳細については、「スタティック NAT」をご覧ください。

```
ADD FIREWALL POLICY=mynet NAT=STANDARD INT=eth0 IP=192.168.1.2
  GBLINT=ppp0 GBLIP=4.4.4.2 ↵
```

■ スタティック NAT を使用している場合、前例のようにすべての IP パケットを通過させる設定だけでなく、特定のトラフィックだけを通過させる設定も可能です。たとえば、192.168.1.2 と 4.4.4.2 を一対一で変換するスタティック NAT を設定している場合、外部（ppp0）から 4.4.4.2（実際は 192.168.1.2）への Web アクセス（終点ポートが TCP80 番）だけを許可するには次のようにします。ファイアウォールの基本ルールにより、その他のホストに対するアクセスはこれまでどおり拒否されます。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=4.4.4.2
  GBLPORT=80 IP=192.168.1.2 PORT=80 ↵
```

このコマンドは、「ppp0 インターフェースで受信した IP パケットのうち、終点 IP アドレスが 4.4.4.2 で終点ポートが 80 番の TCP パケットを、終点アドレスを 192.168.1.2 に書き換えた上で通過させる」の意味になります。

■ 外部からのトラフィックを許可するときのパラメーターの指定方法をまとめます

パラメーター	指定する内容
ACTION	外部から内部への転送を許可するため ALLOW を指定します。
INTERFACE	外部（PUBLIC）インターフェースを指定します。
PROTOCOL	対象となるプロトコルを指定します。TCP、UDP を指定した場合は PORT の指定も必要です。ALL を指定した場合は ICMP を除くすべての IP パケットが対象となります。また、プロトコル番号による指定も可能です。
IP	終点 IP アドレス。パケットの宛先となる内部ホストの IP アドレスです（範囲指定可）。省略時はすべての終点 IP アドレスが対象となります。
PORT	終点ポート番号。パケットの宛先となる内部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。
REMOTEIP	始点 IP アドレス。パケットの送信元となる外部ホストの IP アドレスです（範囲指定可）。省略時はすべての始点 IP アドレスが対象となります。

SOURCEPORT	始点ポート番号。パケットの送信元となる外部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合のみ有効。省略時はすべての始点ポートが対象となります。

表 6: NAT を使っていない場合

パラメーター	指定する内容
ACTION	外部から内部への転送を許可するため ALLOW を指定します。
INTERFACE	外部（PUBLIC）インターフェースを指定します。
PROTOCOL	対象となるプロトコルを指定します。TCP、UDP を指定した場合は GBLPORT、PORT の指定も必要です。ALL を指定した場合は ICMP を除くすべての IP パケットが対象となります。また、プロトコル番号による指定も可能です。
IP	転送後の終点 IP アドレス。パケットの最終的な宛先となるプライベートアドレスで、内部ホストに実際に割り当てられているアドレスを示します。GBLIP で指定したグローバルアドレス（外から見た終点 IP アドレス）に対応するアドレスを指定してください。
PORT	転送後の終点ポート番号。パケットの最終的な宛先となるポート番号で、内部ホストの実際のポート番号です。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。GBLPORT で指定したグローバル側ポート番号（外から見た終点ポート）に対応するポート番号を指定してください。
GBLIP	転送前の終点グローバル IP アドレス。外部から見た場合の終点 IP アドレスです。NAT 変換後のプライベートアドレス（最終的な宛先アドレス）は IP パラメーターで指定します。
GBLPORT	転送前の終点グローバルポート番号。外部から見た場合の終点ポート番号です。NAT 変換後のプライベートポート番号（最終的な宛先ポート）は PORT パラメーターで指定します。
REMOTEIP	始点 IP アドレス。パケットの送信元となる外部ホストの IP アドレスです（範囲指定可）。省略時はすべての始点 IP アドレスが対象となります。
SOURCEPORT	始点ポート番号。パケットの送信元となる外部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合のみ有効。省略時はすべての始点ポートが対象となります。

表 7: NAT を使っている場合

インターフェース NAT

本製品のファイアウォールには、NAT（Network Address Translation）の機能が統合されています（ファイアウォール NAT）。ファイアウォール NAT は、インターフェース単位で設定を行うため「インターフェース NAT」とも呼びます。

インターフェース NAT の設定では、常に 2 つのインターフェース（INT、GBLINT）を指定する必要があります。パケットがこれら 2 つのインターフェース間で転送された場合に限ってアドレス変換が行われる、というのがインターフェース NAT のポイントになります。以下、NAT の種類ごとに例を挙げながら説明し

ます。

スタティック NAT

スタティック NAT（Network Address Translation）は、ルーターなどの中継ノードで IP パケットのアドレスを付け替える機能です。スタティック NAT では、プライベートアドレスをグローバルアドレスに 1 対 1 で固定的に変換します。プライベートアドレスで運用しているサーバーを、ファイアウォールの外からはグローバルアドレスを持っているかのように見せかけることができます。
スタティック NAT の設定は、グローバル側インターフェースが PPP であるか Ethernet であるかによって異なります。以下、それぞれのケースについてスタティック NAT の設定方法をまとめます。
ここでは、次のようなネットワーク構成を仮定します。

- ISP からグローバルアドレス 8 個（1.1.1.0 / 29 = 1.1.1.0〜1.1.1.7）を取得している
- プライベート側（eth0）のネットワークアドレスは 192.168.10.0 / 24
- プライベート側のサーバー（192.168.10.5）をスタティック NAT により 1.1.1.5 として外部に公開する。

ADD FIREWALL POLICY NAT コマンド（33 ページ）でスタティック NAT ルールの設定を行い、ADD FIREWALL POLICY RULE コマンド（36 ページ）でサーバーへのパケットを通過させるルールを追加します。

1. 192.168.10.5 → 1.1.1.5 のスタティック NAT ルールを設定します。スタティック NAT 変換は、INT（eth0）で受信した IP パケットが GBLINT（ppp0）側にルーティングされたときに行われます。

   ```
   ADD FIREWALL POLICY=net NAT=STANDARD INT=eth0 IP=192.168.10.5
     GBLINT=ppp0 GBLIP=1.1.1.5 ↵
   ```

2. 1.1.1.5（192.168.10.5）宛てのパケットを通過させるルールを追加します。

   ```
   ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROT=ALL
     GBLIP=1.1.1.5 IP=192.168.10.5 ↵
   ```

   なお、1.1.1.5 の特定ポートだけに通信を限定させたい場合は、PROTOCOL パラメーターでプロトコルを指定し、GBLPORT パラメーターでグローバル側ポート番号を、PORT パラメーターでプライベート側ポート番号を指定します。次の例では HTTP だけを許可しています。

   ```
   ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROT=TCP
     GBLIP=1.1.1.5 GBLPO=HTTP IP=192.168.10.5 PO=HTTP ↵
   ```

   ✎ これらのルールを設定しないと、ファイアウォールの基本ルールにより、1.1.1.5 宛てのパケットが ppp0 インターフェースで破棄されてしまいます。

ダイナミック ENAT

ダイナミック ENAT（Network Address Translation）は、ルーターなどの中継ノードで IP パケットのアドレスとポート番号を付け替えることにより、プライベート IP アドレスしか持たないホストがグローバル

ネットワークにアクセスできるようにする機能です。グローバルアドレスを 1 個しか割り当てられてない場合でも、ENAT を利用することにより多くのホストがグローバルネットワークにアクセスできるようになります。

■ 次の例では、内部インターフェース側の全ホストが、外部インターフェースに割り当てられた 1 個のグローバル IP アドレスを共有して外部と通信します（各トラフィックはポート番号によって識別されます）。内部側の複数ホストが同時に外部と通信できます。INTERFACE（INT と省略）パラメーターにプライベート側インターフェース名を、GBLINTERFACE（GBLINT と省略）パラメーターにグローバル側インターフェース名を指定してください。

```
ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=eth0 GBLINT=ppp0 ↵
```

このコマンドは、「eth0 のインターフェースで受信した IP パケットが ppp0 側にルーティングされる場合、始点アドレスを ppp0 のインターフェースに割り当てられているグローバル IP アドレスに書き換えて送信する」の意味になります。また、外部からの戻りパケットは、終点アドレスに逆向きのアドレス変換（グローバル→プライベート）を施した上で内部の送信元に送り返されます。

■ 複数グローバル IP を割り当てられる専用線接続などのように、GBLINT で指定したインターフェースが Unnumbered の場合は、GBLIP パラメーターでダイナミック ENAT 用の IP アドレスを明示する必要があります。ISP から割り当てられたグローバルアドレスのうちの 1 個を指定してください。なお、Unnumbered、Numbered にかかわらず、GBLINT には NAT 変換時にパケットを送り出すインターフェースを指定してください。

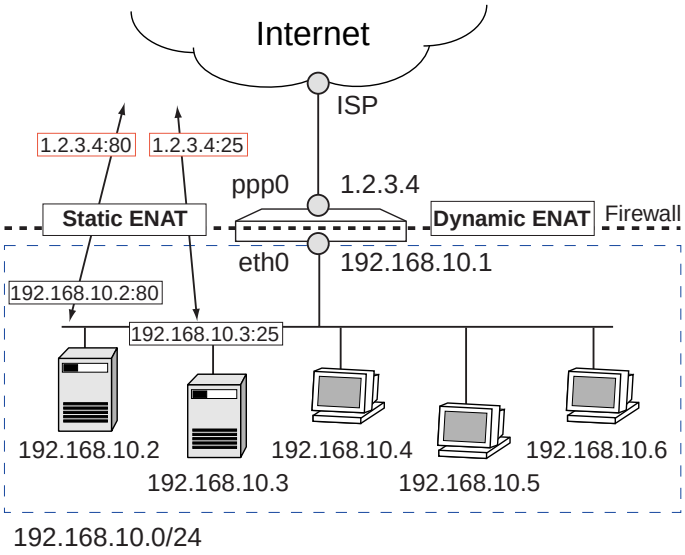
```
ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=eth0-1 GBLINT=ppp0
  GBLIP=1.2.3.6 ↵
```

このコマンドは、「eth0-1 のインターフェースで受信した IP パケットが ppp0 側にルーティングされる場合、始点アドレスを ISP から割り当てられているグローバル IP アドレス 1.2.3.6 に書き換えて送信する」の意味になります。また、外部からの戻りパケットは、終点アドレスに逆向きのアドレス変換（グローバル→プライベート）を施した上で内部の送信元に送り返されます。

スタティック ENAT（ポート/プロトコル転送）

端末型接続のように 1 個しかグローバルアドレスがない場合であっても、スタティック ENAT（ポート / プロトコル転送）機能を用いることにより、グローバル側インターフェースの特定ポート宛てに送られたパケットを、内部ホストの特定ポートに転送することができます。この機能を利用すると、グローバルアドレスが 1 つしかない環境でも、複数のサーバー（サービス）を外部に公開することができます。

■ 次の例では、ルーターの（PPP インターフェースの）80 番ポートに宛てられた TCP パケットを、LAN 側の Web サーバー（192.168.10.2 の 80 番ポート）に転送しています。また、ルーターの 25 番ポートに宛てられた TCP パケットを、LAN 側のメールサーバー（192.168.10.3 の 25 番ポート）に転送しています。この構成では、インターネット上のホストからは、ルーター自身が Web サーバーやメールサーバーであるかのように見えますが、実際にはプライベート IP アドレスを持つ内部のサーバーが応答します。



以下、コマンドラインが長くなるため適宜省略形を使っています。

1. スタティック ENAT は、ダイナミック ENAT を使用していることが前提となります。ここでは、LAN（eth0）側の全ホストが、WAN（ppp0）側に割り当てられたグローバルアドレスを使って外部と通信できるように設定します。

   ```
   ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=eth0 GBLINT=ppp0 ↵
   ```

2. ルーターの 80 番ポートに届いたパケットを、LAN 側の Web サーバー（192.168.10.2）に転送するためのルールを設定します。

   ```
   ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=1.2.3.4
     GBLPO=80 IP=192.168.10.2 PORT=80 ↵
   ```

   このコマンドは、「ppp0 インターフェースで受信した TCP パケットのうち、終点 IP アドレスが 1.2.3.4 で終点ポートが 80 のものを、アドレス変換してホスト 192.168.10.2 の 80 番ポートに転送する」の意味になります。また、内部サーバーからの戻りパケットは、逆向きのアドレス変換（プライベート→グローバル）を施した上で送信元に送り返されます。

   ✎ グローバル IP アドレスが動的に割り当てられる場合は、GBLIP に 0.0.0.0 を指定します。

3. ルーターの 25 番ポートに届いたパケットを、LAN 側のメールサーバー（192.168.10.3）に転送するためのルールを設定します。

   ```
   ADD FIRE POLI=mynet RU=2 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=1.2.3.4
     GBLPO=25 IP=192.168.10.3 PORT=25 ↵
   ```

   このコマンドは、「ppp0 インターフェースで受信した TCP パケットのうち、終点 IP アドレスが 1.2.3.4 で終点ポートが 25 のものを、アドレス変換してホスト 192.168.10.3 の 25 番ポートに転送する」の意味になります。

■ 同じ Well-known ポートを使うサーバーを複数公開したい場合、外部からのアクセスはいくらか変則的になりますが、GBLPORT をサーバーごとに変えることで可能となります。ここでは、内部に 192.168.10.5、192.168.10.10 の 2 つの Web サーバーがあるものとします。次の例では、外部から 1.2.3.4 の TCP ポート 80 番へのアクセスは 192.168.10.5 に、同じくポート 8080 番へのアクセスは 192.168.10.10 の Web サービスに転送します。

```
ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=1.2.3.4
  GBLPO=80 IP=192.168.10.5 PORT=80 ↵
ADD FIRE POLI=mynet RU=2 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=1.2.3.4
  GBLPO=8080 IP=192.168.10.10 PORT=80 ↵
```

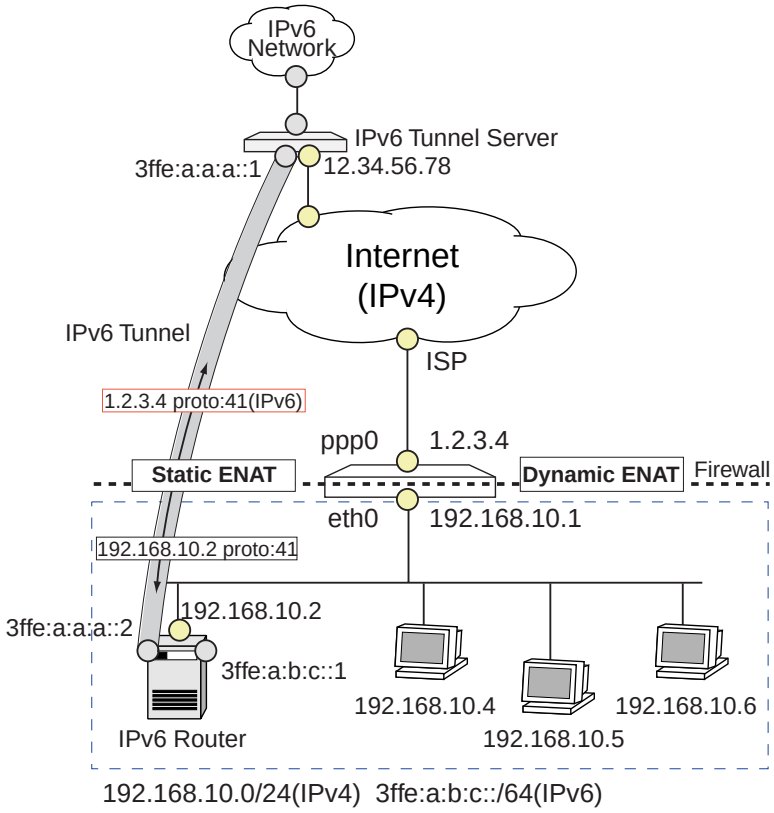
この場合、外部から 192.168.10.10 の Web サーバーにアクセスするには、URL の中でポート番号 8080 を指定する必要があります。ブラウザーの URL 欄に次のように入力します。

`http://1.2.3.4:8080/ ...` **（実際は** `192.168.10.10` **の** `Web` **サーバーにアクセスすることになる）**

192.168.10.5 の Web サーバーは標準の Web サービスポートである 80 番を使っているので、URL でポート番号を指定する必要はありません。

`http://1.2.3.4/ ...` **（実際は** `192.168.10.5` **の** `Web` **サーバーにアクセスすることになる）**

■ 少し特殊なケースですが、TCP / UDP ポート番号ではなく、IP ヘッダーのプロトコル番号をもとに内部への転送を行うこともできます。次の例では、PRIVATE 側にある IPv6 ルーター（192.168.10.2）が、IPv4 インターネット上の IPv6 トンネルサーバー（12.34.56.78）との間にトンネルを張り、LAN を IPv6 ネットワークにトンネル接続しています。



インターネット上にトンネルを張るには、トンネルの両エンドに互いに到達可能なグローバルアドレスが必要ですが、この環境ではLAN側のIPv6ルーターにグローバルアドレスがありません。そこで、スタティックENATのプロトコル転送機能を利用して、本製品のWAN側インターフェース（1.2.3.4）宛てに届いたIPv6-over-IPv4トンネリングパケット（IPプロトコル41）を、LAN側のIPv6ルーターに転送する設定を行います。これにより、トンネルサーバーからは本製品のPPPインターフェースが、LAN側に存在するIPv6ルーターのインターフェースに見えます。

```
ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=ppp0 PROTO=41 REMOTEIP=12.34.56.78
  GBLIP=1.2.3.4 IP=192.168.10.2 ↵
```

このコマンドは、「ppp0インターフェースで受信したプロトコル番号41（IPv6）のIPパケットのうち、始点IPアドレスが12.34.56.78で終点IPアドレスが1.2.3.4のものを、アドレス変換してLAN側の192.168.10.2に転送する」の意味になります。また、内部からの戻りパケットは、逆向きのアドレス変換（プライベート→グローバル）を施した上で送信元に送り返されます。

■ スタティックENAT（ポート/プロトコル転送）の設定におけるパラメーターの指定方法をまとめます（ダイナミックENATの併用が必須です）

パラメーター	指定する内容
ACTION	外部から内部への転送を許可するので常にALLOWとなります。
INTERFACE	外部（PUBLIC）インターフェースを指定します。

PROTOCOL	転送するプロトコルを指定します。通常は TCP か UDP です。その場合、GBLPORT と PORT の指定も必要です。ALL を指定した場合は ICMP を除くすべての IP パケットが対象となります。また、プロトコル番号による指定も可能です。
GBLIP	転送前の終点 IP アドレス。外部インターフェースに割り当てられたグローバル IP アドレスを指定します。IPCP（PPP）や DHCP などで動的にアドレスを取得している場合は 0.0.0.0 を指定します。
GBLPORT	転送前の終点ポート番号。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。
IP	転送後の終点 IP アドレス。転送先ホストのプライベート IP アドレスです。
PORT	転送後の終点ポート番号。転送先のポート番号です。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。
REMOTEIP	始点 IP アドレス。外部の送信者の IP アドレスです（範囲指定可）。省略時はすべての始点 IP アドレスが対象になります。
SOURCEPORT	始点ポート番号。外部の送信者のポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合のみ有効。省略時はすべての始点ポートが対象となります。

表 8:

ルールの確認・修正・削除

■ ファイアウォールポリシーに設定されたルールの内容を確認するには、SHOW FIREWALL POLICY コマンド（58 ページ）を使います。

■ ルールを修正するには SET FIREWALL POLICY RULE コマンド（54 ページ）を使います。

■ ルールを削除するには DELETE FIREWALL POLICY RULE コマンド（43 ページ）を使います。

ファイアウォールルールの処理順序

1. 新しく開始されたセッションまたはフロー（以下、フローとします）の向きによって、マッチするルールがなかったときのデフォルトの動作が決定されます。PRIVATE インターフェース側から開始されたフローはデフォルト許可、PUBLIC 側から開始されたフローはデフォルト拒否となります。以後、番号の若いものから順にルールがチェックされていきます。ひとつもマッチするルールがなかった場合は、最初に決めたデフォルトの動作を行います。
2. 新規フローのプロトコルタイプ（PROTOCOL）と一致するルールがないかチェックします。プロトコルが一致するルールがなかった場合、デフォルトの動作を実行します。
3. プロトコルが TCP か UDP の場合、終点ポート（PORT）をチェックします。一致するルールがなかった場合はデフォルトの動作を実行します。
4. プロトコルが TCP か UDP の場合、始点ポート（SOURCEPORT）をチェックします。一致するルールがなかった場合はデフォルトの動作を実行します。
5. リモート IP アドレス（REMOTEIP）をチェックします。PRIVATE 側からのフローでは終点 IP アド

レス、PUBLIC 側からのフローでは始点 IP アドレスです。一致するルールがなかった場合はデフォルトの動作を実行します。

6. ローカル IP アドレス（IP または GBLIP）をチェックします。PRIVATE 側からのフローでは始点 IP アドレス、PUBLIC 側からのフローでは終点 IP アドレスです。終点 IP アドレスは、NAT を使用している場合は PUBLIC 側の送信元ホストから見えるグローバル IP アドレス（GBLIP）、NAT を使用していない場合は PRIVATE 側ホストの IP アドレス（IP）になります。

ファイアウォールの動作監視

ファイアウォールの運用にあたっては、ルールを適切かつ正しく設定することはもちろんですが、ファイアウォールの周辺でどのような活動が行われているかを調べることも重要です。本製品のログ機能を利用すれば、このような監視作業を効果的に行うことができます。

ログ

ファイアウォールの動作を監視する場合、ログはもっとも基本的な資料になります。デフォルトでは、攻撃などの重大イベントしか記録されませんので、以下のコマンドを実行して必要なログオプションを有効にしてください。

■ ファイアウォールで拒否されたパケットのログをとるには、ENABLE FIREWALL POLICY コマンド（51 ページ）の LOG パラメーターに記録するパケットの種類を指定します。たとえば、ファイアウォールで拒否されたすべてのパケットを記録するには、次のようにします。

```
ENABLE FIREWALL POLICY=mynet LOG=DENY ↵
```

LOG パラメーターにはほかにもさまざまなオプションを指定できます。LOG パラメーターには複数の項目をカンマ区切りで指定することができます。

オプション名	対象パケット
INATCP	外部（PUBLIC 側）からの TCP セッション開始を許可
INAUDP	外部からの UDP フロー開始を許可
INAICMP	外部からの ICMP 要求を許可
INAOTHER	外部からの IP フロー開始（TCP、UDP、ICMP 以外）を許可
INALLOW	外部からのセッション / フロー開始を許可。INATCP、INAUDP、INAICMP、INAOTHER をすべて指定したのに等しい。
OUTATCP	内部（PRIVATE 側）からの TCP セッション開始を許可
OUTAUDP	内部からの UDP フロー開始を許可
OUTAICMP	内部からの ICMP 要求を許可
OUTAOTHER	内部からの IP フロー開始（TCP、UDP、ICMP 以外）を許可
OUTALLOW	内部からのセッション / フロー開始を許可。OUTATCP、OUTAUDP、OUTAICMP、OUTAOTHER をすべて指定したのと等しい。
ALLOW	内外からのセッション / フロー開始を許可
INDTCP	外部からの TCP セッション開始を遮断

INDUDP	外部からの UDP フロー開始を遮断
INDICMP	外部からの ICMP 要求を遮断
INDOTHER	外部からの IP フロー開始（TCP、UDP、ICMP 以外）を遮断
INDENY	外部からのセッション / フロー開始を遮断。INDTCP、INDUDP、INDICMP、INDOTHER をすべて指定したのに等しい。
OUTDTCP	内部からの TCP セッション開始を遮断
OUTDUDP	内部からの UDP フロー開始を遮断
OUTDICMP	内部からの ICMP 要求を遮断
OUTDOTHER	内部からの IP フロー開始（TCP、UDP、ICMP 以外）を遮断
OUTDENY	内部からのセッション / フロー開始を遮断。OUTDTCP、OUTDUDP、OUTDICMP、OUTDOTHER をすべて指定したのに等しい。
DENY	内外からのセッション / フロー開始を遮断
INDDTCP	外部からの TCP セッション開始を遮断し、IP パケットの先頭最大 192 バイトを記録
INDDUDP	外部からの UDP フロー開始を遮断し、IP パケットの先頭最大 192 バイトを記録
INDDICMP	外部からの ICMP 要求を遮断し、IP パケットの先頭最大 192 バイトを記録
INDDOTHER	外部からの IP フロー開始（TCP、UDP、ICMP 以外）を遮断し、IP パケットの先頭最大 192 バイトを記録
INDDUMP	外部からのセッション / フロー開始を遮断し、IP パケットの先頭最大 192 バイトを記録
OUTDDTCP	内部からの TCP セッション開始を遮断し、IP パケットの先頭最大 192 バイトを記録
OUTDDUDP	内部からの UDP フロー開始を遮断し、IP パケットの先頭最大 192 バイトを記録
OUTDDICMP	内部からの ICMP 要求を遮断し、IP パケットの先頭最大 192 バイトを記録
OUTDDOTHER	内部からの IP フロー開始（TCP、UDP、ICMP 以外）を遮断し、IP パケットの先頭最大 192 バイトを記録
OUTDDUMP	内部からのセッション / フロー開始を遮断し、IP パケットの先頭最大 192 バイトを記録
DENYDUMP	内外からのセッション / フロー開始を遮断し、IP パケットの先頭最大 192 バイトを記録

表 9: ファイアウォールのログオプション一覧

■ ファイアウォールに関するログは次のコマンドで見ることができます。

```
SHOW LOG MODULE=FIRE ↵
```

または

```
SHOW LOG TYPE=FIRE ↵
```

■ 大量のログメッセージが記録されている場合などに、最新のメッセージだけを見たい場合は、TAIL オプションを付けます。

```
SHOW LOG MODULE=FIRE TAIL（最新の 20 メッセージを表示） ↵
SHOW LOG MODULE=FIRE TAIL=10（同 10 メッセージを表示） ↵
```

```
Manager > show log module=fire

Date/Time   S Mod  Type  SType Message
------------------------------------------------------------------------------
28 10:39:45 4 FIRE FIRE  INDIC ICMP - Source 172.16.28.32 Dest 172.16.28.255
                               Type 9 Code 0
28 10:39:45 4 FIRE FIRE  INDIC bad ICMP message type to pass
28 10:40:05 4 FIRE FIRE  INDUD UDP - Source 172.16.28.120:137 Dest
                               172.16.28.255:137
28 10:40:05 4 FIRE FIRE  INDUD flow rejected by policy rule
28 10:40:06 4 FIRE FIRE  INDUD UDP - Source 172.16.28.120:137 Dest
                               172.16.28.255:137
28 10:40:06 4 FIRE FIRE  INDUD flow rejected by policy rule
28 10:40:41 3 FIRE FIRE  OUTDT TCP - Source 192.168.10.1:1045 Dest
                               172.16.28.1:139
28 10:40:41 3 FIRE FIRE  OUTDT flow rejected by policy rule
------------------------------------------------------------------------------
```

■ ファイアウォールのログオプションのうち、INATCP、INAUDP、INAICMP、INAOTHER、INALLOW に対応するメッセージのログレベル（Severity）は 2 です。ログ機能のデフォルト設定では、ログレベル 3 以上のメッセージだけを保存するようになっているため、SHOW LOG コマンド（「運用・管理」の 224 ページ）を実行しても前記のメッセージは表示されません。これらのメッセージが記録されるようにするには、ログメッセージフィルターの設定を変更する必要があります。
たとえば、次のコマンドを実行すれば、ファイアウォール関連のメッセージはすべて、ログレベルに関係なく「TEMPORARY」ログ（RAM 上に記録されるログ）に保存されるようになります。

```
ADD LOG OUTPUT=TEMPORARY MODULE=FIRE ↵
```

デバッグオプション

ファイアウォールポリシーのデバッグオプションをオンにするには、ENABLE FIREWALL POLICY コマンド（51 ページ）の DEBUG パラメーターを使います。オプションには、パケットダンプの表示（PKT）と処理プロセスの表示（PROCESS）があります。

■ デバッグオプション PKT をオンにすると、コンソールに IP パケットの先頭 56 バイトが 16 進ダンプされるようになります。

```
ENABLE FIREWALL POLICY=mynet DEBUG=PKT ↵
```

```
Manager >
FIRE ICMP  45000024 c6070000 01018e04 ac101c20 ac101cff 0900421e 01020168
```

```
           96571c20 00000000

Manager >
FIRE TCP   4500003c c87c4000 40060c3d ac101cb4 ac101ca0 05e70017 3398573f
           00000000 a0027d78 19d20000 020405b4 0402080a 0d82ac62 00000000
```

■ デバッグオプション PROCESS をオンにすると、コンソールに IP パケットの処理過程が逐次表示されるようになります。

```
ENABLE FIREWALL POLICY=mynet DEBUG=PROCESS ↵
```

```
FIRE UDP   4500004d 218a0000 4011dc10 c0a80a05 ac101c01 ff780035 00393422
           067f0100 00010000 00000000 076f6374 6f766572 0274770e 616c6c69

FIREWALL new flow - UDP - session ID 8b2e
FIREWALL packet sent to UDP handler
FIREWALL flow 8b2e found for packet
FIREWALL packet sent to UDP handler
FIREWALL packet passed - UDP OUT - passed by rule 0

FIRE UDP   4500004d 218b0000 4011dc0f c0a80a05 ac101c01 ff770035 00394f22
           06800100 00010000 00000000 076f6374 6f766572 0274770e 616c6c69

FIREWALL new flow - UDP - session ID 9a14
FIREWALL packet sent to UDP handler
FIREWALL flow 9a14 found for packet
FIREWALL packet sent to UDP handler
FIREWALL packet passed - TCP OUT - passed by rule 0

FIRE TCP   4500003c 218c0000 4006db77 c0a80a05 ac101cb4 e2360017 d71d5199
           00000000 a0024000 1d930000 020405b4 01030300 0101080a 000064b7

FIREWALL new flow - TCP - session ID a9c5
FIREWALL packet sent to TCP handler
FIREWALL flow a9c5 found for packet
FIREWALL packet sent to TCP handler direction IN
FIREWALL flow a9c5 found for packet
FIREWALL packet sent to TCP handler direction OUT
FIREWALL flow a9c5 found for packet
FIREWALL packet sent to TCP handler direction OUT
FIREWALL flow a9c5 found for packet
FIREWALL packet sent to TCP handler direction IN
FIREWALL flow a9c5 found for packet
FIREWALL packet sent to TCP handler direction IN
```

■ デバッグオプションを無効にするには、DISABLE FIREWALL POLICY コマンド（47 ページ）の DEBUG パラメーターを使います。

```
DISABLE FIREWALL POLICY=mynet DEBUG=PKT ↵
```

■ 現在有効なデバッグオプションは SHOW FIREWALL POLICY コマンド（58 ページ）で確認します。「Enabled Debug Options」に有効なオプションが表示されます。

ファイアウォールセッションの確認

■ 現在ファイアウォールを介して行われている通信セッションを確認するには SHOW FIREWALL SESSION コマンド（63 ページ）を使います。

```
Manager > show firewall session

Policy : net
Current Sessions
--------------------------------------------------------------------------------
3612 UDP      IP: 192.168.10.100:64499      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:13842   Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:44:35 07-Mar-2002
     Seconds to deletion .................. 264
158f UDP      IP: 192.168.10.100:64500      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:5519    Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:44:13 07-Mar-2002
     Seconds to deletion .................. 246
7527 UDP      IP: 192.168.10.100:64501      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:29991   Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:41:11 07-Mar-2002
     Seconds to deletion .................. 60
5e9e TCP      IP: 192.168.10.100:65484      Remote IP: 172.17.28.103:22
          Gbl IP: 172.17.28.185:24222   Gbl Remote IP: 172.17.28.103:22
     TCP state ............................ closed
     Start time ........................... 17:35:17 07-Mar-2002
     Seconds to deletion .................. 54
--------------------------------------------------------------------------------
```

■ 各セッションの統計情報を確認するには、SHOW FIREWALL SESSION コマンド（63 ページ）に COUNTER オプションを付けます。

```
Manager > show firewall session counter

Policy : net
Current Sessions
--------------------------------------------------------------------------------
43fa TCP      IP: 192.168.10.100:65480      Remote IP: 172.17.22.10:80
          Gbl IP: 172.17.28.185:17402   Gbl Remote IP: 172.17.22.10:80
     Packets from private IP .............. 8
     Octets from private IP ............... 558
     Packets to private IP ................ 8
     Octets to private IP ................. 6881
     TCP state ............................ closed
     Start time ........................... 17:51:26 07-Mar-2002
     Seconds to deletion .................. 300
c296 TCP      IP: 192.168.10.100:65483      Remote IP: 172.17.24.1:23
```

```
          Gbl IP: 172.17.28.185:49814   Gbl Remote IP: 172.17.24.1:23
     Packets from private IP ..... 11
     Octets from private IP ..... 555
     Packets to private IP ..... 12
     Octets to private IP ..... 554
     TCP state ..... timeWait
     Start time ..... 17:49:33 07-Mar-2002
     Seconds to deletion ..... 246
ea27 UDP      IP: 192.168.10.100:64433      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:59943   Gbl Remote IP: 172.17.28.1:53
     Packets from private IP ..... 1
     Octets from private IP ..... 75
     Packets to private IP ..... 1
     Octets to private IP ..... 149
     Start time ..... 17:50:05 07-Mar-2002
     Seconds to deletion ..... 270
------------------------------------------------------------------------------
```

■ 特定のセッションを強制的に終了させるには、SHOW FIREWALL SESSION コマンド（63 ページ）で該当セッションの ID を確認してから、次のコマンドを実行します。

```
DELETE FIREWALL SESSION=c296 ↵
```

その他設定

本製品のファイアウォールは、各種コマンドを使って細かい動作の変更が可能です。ここでは主要な設定についてのみ説明します。詳細はコマンドリファレンスをご覧ください。

■ ping パケット（ICMP echo、echo reply）と ICMP Destination Unreachable を通す
デフォルトでは ICMP はすべて通しません（ルーター自身への ping には応答します）。

```
ENABLE FIREWALL POLICY=mynet ICMP_F=PING,UNREACH ↵
```

✎ ICMP Destination Unreachable メッセージ（ICMP タイプ 3）は、IP ホストが通信経路上の最大パケットサイズ（Path MTU）を知る目的で使用することがあります。そのため、本メッセージを遮断すると、一部のサイトにアクセスできなくなる可能性があります。

ICMP_FORWARDING に ALL を指定すると（ping だけでなく）すべての ICMP メッセージを通すようになりますが、セキュリティー的にはお勧めできません。
なお、ファイアウォールでは、ICMP については方向の制御ができません。すなわち、ICMP パケットは双方向とも通すか、まったく通さないかの設定しかできません。
内部からの PING（echo）は通すが、外部からの PING（Echo）は拒否するといった設定をしたい場合は、IP フィルターを併用してください。IP フィルターでは ICMP パケットに対する細かい制御が可能です。外部（ppp0）からのみ PING を拒否するには、次のようなフィルターを設定します。IP フィルターの詳細については、「IP」の章をご覧ください。

```
ADD IP FILTER=0 SO=0.0.0.0 PROTO=ICMP ICMPTYPE=ECHO ACTION=EXCLUDE ↵
ADD IP FILTER=0 SO=0.0.0.0 ACTION=INCLUDE ↵
SET IP INT=ppp0 FILTER=0 ↵
```

■ ping の転送をオフにするには、次のコマンドを実行します。

```
DISABLE FIREWALL POLICY=mynet ICMP_F=PING ↵
```

■ 本製品自身への外部からの ping に応答しないようにする
デフォルトでは応答します。また、内部からの PING には常に応答します。

```
DISABLE FIREWALL POLICY=mynet PING ↵
```

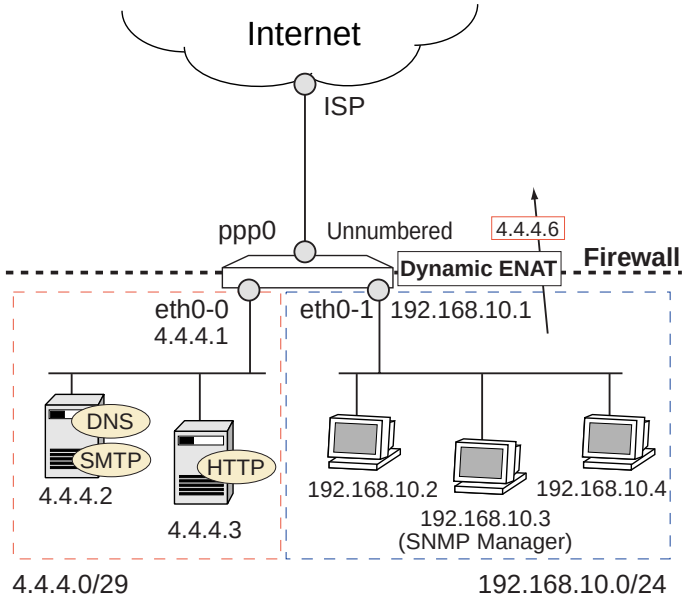
■ 外部からの ident（TCP 113 番ポート）要求に対して、RST を返すようにする
デフォルトでは、ファイアウォール外部の SMTP（メール）サーバーなどからの ident 要求に対して本製品が代理応答します（ident プロキシー機能）。しかし、外部の SMTP（メール）サーバーなどへの接続に時間がかかりすぎる場合は、DISABLE FIREWALL POLICY IDENTPROXY コマンド（49 ページ）を実行して ident プロキシーをオフにしてみてください。これにより、外部からの ident 要求に対してただちに RST を返すようになります（こちらの実装のほうが一般的なようです）。

```
DISABLE FIREWALL POLICY=mynet IDENTPROXY ↵
```

なお、ident プロキシー機能がオンのときは、ident 要求に対して本製品が proxyuser というユーザー名を返答します。

設定例

次に、独自ルールを追加した、より実際的な設定例を示します。ここでは、次のようなネットワーク構成を例に説明します。



ここでは、次のようなセキュリティーポリシーを持つファイアウォールを設定します。

- ICMP は Ping(echo / echo reply) と Unreachable のみ双方向とも許可。
- UDP は双方向とも禁止。ただし、UDP の DNS サービス（53）のみ双方向とも許可する。
- TCP は内部から外部へのみコネクションを張ることができる。ただし、以下は例外とする。
  - 内部の DNS サーバー（4.4.4.2）の DNS サービス（53）には外部から TCP のコネクションを張れる。
  - 内部のメールサーバー（4.4.4.2）の SMTP サービス（25）には外部から TCP のコネクションを張れる 。
  - 内部の Web サーバー（4.4.4.3）の HTTP サービス（80）には外部から TCP のコネクションを張れる。
- eth0-0 と eth0-1 を PRIVATE、ppp0 を PUBLIC インターフェースとして設定する。
- ファイアウォールでブロックしたパケットをログに記録する。

ルーターの設定

1. 専用線接続の設定を行います。

```
SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
CREATE TDM GROUP=isp INT=bri0 SLOTS=1-2 ↵
CREATE PPP=0 OVER=TDM-isp LQR=OFF BAP=OFF ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. 各インターフェースに IP アドレスを設定します。WAN 側が Unnumbered であるため、LAN 側（eth0）をマルチホーミングして、同一セグメント上にグローバル IP のサブネット（4.4.4.0 / 29）と

プライベート IP のサブネット（192.168.1.0/24）を作成しています。

```
ADD IP INT=eth0-0 IP=4.4.4.1 MASK=255.255.255.248 ↵
ADD IP INT=eth0-1 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=ppp0 IP=0.0.0.0 ↵
```

4. デフォルトルートを設定します。

   ```
   ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXT=0.0.0.0 ↵
   ```

5. ファイアウォールを有効にします。

   ```
   ENABLE FIREWALL ↵
   ```

6. ファイアウォールポリシーを作成します。

   ```
   CREATE FIREWALL POLICY=mypol ↵
   ```

7. ファイアウォールで拒否したパケットをログに記録するよう設定します。

   ```
   ENABLE FIREWALL POLICY=mypol LOG=DENY ↵
   ```

8. ident プロキシー機能を無効にし、外部からの ident 要求に対してただちに RST を返すようにします。

   ```
   DISABLE FIREWALL POLICY=mypol IDENTPROXY ↵
   ```

9. ファイアウォールポリシーの適用対象となるインターフェースを指定します。
   - eth0-0 と eth0-1 を PRIVATE（内部）インターフェースに設定します。

     ```
     ADD FIREWALL POLICY=mypol INT=eth0-0 TYPE=PRIVATE ↵
     ADD FIREWALL POLICY=mypol INT=eth0-1 TYPE=PRIVATE ↵
     ```

   - ppp0 を PUBLIC（外部）インターフェースに設定します。

     ```
     ADD FIREWALL POLICY=mypol INT=ppp0 TYPE=PUBLIC ↵
     ```

10. 以下、ポリシーの詳細設定を行います。
    - ICMP echo / echo reply と Unreachable を双方向で許可します。

      ```
      ENABLE FIREWALL POLICY=mypol ICMP_F=PING,UNREACH ↵
      ```

    - eth0-1 配下のプライベート LAN からインターネットに出られるよう、ダイナミック ENAT を設定します。グローバルアドレスとしては、4.4.4.6 を使います。

      ```
      ADD FIREWALL POLICY=mypol NAT=ENHANCED INT=eth0-1 GBLINT=ppp0
        GBLIP=4.4.4.6 ↵
      ```

    - UDP は、 DNS サービス（53）のみ双方向で許可します。

```
ADD FIREWALL POLICY=mypol RULE=1 ACTION=ALLOW INT=eth0-0 PROT=UDP
  PORT=DNS ↵
ADD FIREWALL POLICY=mypol RULE=2 ACTION=ALLOW INT=eth0-1 PROT=UDP
  PORT=DNS ↵
ADD FIREWALL POLICY=mypol RULE=3 ACTION=ALLOW INT=ppp0 PROT=UDP
  PORT=DNS ↵
```

- その他の UDP トラフィックは双方向で禁止します（外部からの UDP はデフォルトで禁止されるため設定する必要はありません）。

```
ADD FIREWALL POLICY=mypol RULE=4 ACTION=DENY INT=eth0-0 PROT=UDP
  PORT=ALL ↵
ADD FIREWALL POLICY=mypol RULE=5 ACTION=DENY INT=eth0-1 PROT=UDP
  PORT=ALL ↵
```

- 内部の DNS サーバー（4.4.4.2）の DNS サービス（53）には外部から TCP のコネクションを張れるようにします。

```
ADD FIREWALL POLICY=mypol RULE=6 ACTION=ALLOW INT=ppp0 IP=4.4.4.2
  PROT=TCP PORT=DNS ↵
```

- 内部のメールサーバー（4.4.4.2）の SMTP サービス（25）には外部から TCP のコネクションを張れるようにします。

```
ADD FIREWALL POLICY=mypol RULE=7 ACTION=ALLOW INT=ppp0 IP=4.4.4.2
  PROT=TCP PORT=SMTP ↵
```

- 内部の Web サーバー（4.4.4.3）の HTTP サービス（80）には外部から TCP のコネクションを張れるようにします。

```
ADD FIRE POLI=mypol RU=8 AC=ALLOW INT=ppp0 IP=4.4.4.3 PROT=TCP
  PORT=WWW ↵
```

設定は以上です。

コマンドリファレンス編

機能別コマンド索引

ADD FIREWALL POLICY APPRULE

カテゴリー：ファイアウォール / フィルタールール
対象機種：AR130、AR160

```
ADD FIREWALL POLICY=policy APPRULE=app-rule-id ACTION={ALLOW|DENY}
   INTERFACE=interface APPLICATION={FTP} [COMMAND={GET|PUT}] [PORT=port]
```

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
app-rule-id: アプリケーションルール番号（1〜299）
interface: IP インターフェース名（eth0、ppp0 など）
port: TCP / UDP ポート番号

解説

ファイアウォールポリシーにアプリケーションルールを追加する。
アプリケーションルールは、FTP の STOR（PUT）、RETR（GET）のように、アプリケーション層での通信を制御するためのルール。現時点では FTP にのみ対応している。

パラメーター

POLICY　ファイアウォールポリシー名
APPRULE　アプリケーションルール番号
ACTION　アクション。該当するアプリケーショントラフィックを通過（ALLOW）させるか、拒否（DENY）するかを指定する。
INTERFACE　IP インターフェース名
APPLICATION　アプリケーションプロトコル。現時点では FTP のみサポート。
COMMAND　アプリケーションプロトコルにおけるコマンド名。現時点では FTP の GET（RETR）と PUT（STOR）のみをサポート。本パラメーターは、APPLICATION=FTP の場合にのみ有効。
PORT　APPLICATION で指定したアプリケーションが使用するポート。標準的でないポートを使用している場合に指定する。

例

■ppp0 側からの FTP PUT（STOR）を禁止する。

```
ADD FIREWALL POLI=mynet APPRULE=1 ACT=DENY INT=ppp0 APP=FTP COMMAND=PUT
```

関連コマンド

DELETE FIREWALL POLICY APPRULE（40 ページ）

SHOW FIREWALL POLICY（58 ページ）

ADD FIREWALL POLICY INTERFACE

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

ADD FIREWALL POLICY=*policy* INTERFACE=*interface* TYPE={**PUBLIC**|**PRIVATE**}
[METHOD={DYNAMIC|PASSALL}]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
interface: IP インターフェース名（eth0、ppp0 など）

解説

ファイアウォールポリシーにインターフェースを追加する。
ファイアウォールポリシーが機能するためには、PRIVATE（内部）と PUBLIC（外部）のインターフェースがそれぞれ最低一つずつ必要。
あるインターフェースを複数のポリシーで PRIVATE インターフェースに設定することはできないが、同じインターフェースを複数のポリシーで PUBLIC インターフェースとして設定することはできる。同一ポリシー内に PRIVATE インターフェースが複数存在する場合、PRIVATE インターフェース間の通信は制限されない。

パラメーター

POLICY　ファイアウォールポリシー名
INTERFACE　IP インターフェース名。ダイナミックインターフェースは、「DYN-」＋ダイナミックインターフェーステンプレート名で指定する（例：DYN-pon）
TYPE　インターフェース種別。PUBLIC（外部）と PRIVATE（内部）がある。ファイアウォールの基本ルールでは、PRIVATE からのパケットはすべて通すが、PUBLIC からのパケットはすべて遮断する。この基本ルールをもとに、ADD FIREWALL POLICY RULE コマンドで独自のルール（通過、遮断など）を追加し、ファイアウォールの動作をカスタマイズすることができる。
METHOD　PUBLIC インターフェースの動作を指定する。DYNAMIC（デフォルト）では、ダイナミックパケットフィルタリングにより、PRIVATE 側から開始されたセッションに限り PUBLIC 側から PRIVATE にパケットを転送する。PASSALL を指定した場合は、ファイアウォールによるフィルタリングは行われない。PASSALL は、スタティック NAT を使用するインターフェースで使用する。

例

■ファイアウォールポリシー「net」の内部側（PRIVATE）インターフェースとして eth0 を、外部側（PUBLIC）インターフェースとして ppp0 を追加する。

```
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
```

関連コマンド

CREATE FIREWALL POLICY（39 ページ）
DELETE FIREWALL POLICY INTERFACE（41 ページ）
SHOW FIREWALL POLICY（58 ページ）

ADD FIREWALL POLICY NAT

カテゴリー：ファイアウォール / ファイアウォール NAT
対象機種：AR130、AR160

ADD FIREWALL POLICY=*policy* NAT={**ENHANCED**|**STANDARD**} **INTERFACE=*interface***
GBLINTERFACE=*interface* [IP=*ipadd*] [GBLIP=*ipadd*[-*ipadd*]]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

ファイアウォールポリシーにインターフェースベースの NAT ルールを追加する。
インターフェース NAT の設定では、常に 2 つのインターフェース（INT、GBLINT）を指定する必要がある。パケットがこれら 2 つのインターフェース間で転送された場合に限ってアドレス変換が行われる、というのがインターフェース NAT の名前の由来でもあり、重要なポイントでもある。
インターフェース NAT の設定に必要なパラメーターは NAT の種類によって異なる。
・スタティック NAT（IP アドレスを 1 対 1 で固定的に変換）の場合は、NAT=STANDARD を指定し、IP（プライベート IP）、INTERFACE（プライベート側インターフェース）、GBLIP（グローバル IP）、GBLINTERFACE（グローバル側インターフェース）を指定する。
・ダイナミック NAT（IP アドレスを多対多で動的に変換）の場合は、NAT=STANDARD を指定し、INTERFACE（プライベート側インターフェース）、GBLINTERFACE（グローバル側インターフェース）、GBLIP（グローバル IP の範囲。x.x.x.a-x.x.x.b）を指定する。この場合、INTERFACE 側のプライベートアドレスを、GBLIP で指定した範囲内で空いているグローバルアドレスに変換する。ただし、他の NAT に比べてメリットが少ないため、あまり使われない。
・スタティック ENAT（IP アドレス、プロトコル（、ポート）を 1 対 1 で固定的に変換）は、本コマンドでダイナミック ENAT の設定をした上で、ADD FIREWALL POLICY RULE コマンドで設定する。
・ダイナミック ENAT（IP アドレス、プロトコル（、ポート）を多対多で動的に変換）の場合は、NAT=ENHANCED を指定し、INTERFACE（プライベート側インターフェース）、GBLINTERFACE（グローバル側インターフェース）、GBLIP（グローバル IP。オプション）を指定する。これにより、動的なポート割り当てにより、GBLINTERFACE に割り当てられた 1 つのグローバルアドレス、または、GBLIP で指定したアドレスを、INTERFACE 側のプライベートアドレスを持つホスト間で共有する。
なお、本コマンドで指定するインターフェース（INTERFACE、GBLINTERFACE）は、あらかじめ ADD FIREWALL POLICY INTERFACE コマンドでポリシーに追加しておく必要がある。

パラメーター

POLICY　ファイアウォールポリシー名
NAT　NAT の種類。STANDARD は IP アドレスのみの変換を行うもので、プライベート 1 対グローバル 1 のスタティック NAT、または、複数プライベート対複数グローバルのダイナミック NAT を使う場

合に指定する。ENHANCED は IP アドレスとポート番号の変換を行うダイナミック ENAT 使用時に指定する。

INTERFACE　プライベート側 IP インターフェース。このインターフェースで受信した IP パケットは、GBLINTERFACE で指定されたインターフェースに転送されたときにアドレス変換の対象となる。

GBLINTERFACE　グローバル側 IP インターフェース。このインターフェースで受信した IP パケットは、INTERFACE で指定されたインターフェースに渡される前にアドレス変換される。

IP　スタティック（1 対 1）NAT 時のプライベート側 IP アドレスを指定する。NAT=STANDARD の場合のみ有効。NAT=STANDARD でも、GBLIP に複数の IP アドレスを指定した場合（ダイナミック NAT の場合）は無効。

GBLIP　スタティック NAT 時のグローバル側 IP アドレス（NAT=STANDARD で IP パラメーターに 1 個のアドレスを指定した場合）、ダイナミック NAT 時のグローバル IP アドレスの範囲（NAT=STANDARD）、および、ダイナミック ENAT 時のグローバル IP アドレスを指定する。

例

■eth0 側のプライベートアドレスを ppp0 に割り当てられたグローバルアドレスに変換するダイナミック ENAT を設定する。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
```

■PPP インターフェースが Unnumbered の場合は、GBLIP パラメーターを追加して、ISP から割り当てられているグローバル IP アドレスの 1 つを指定する。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
  GBLIP=200.100.10.1
```

■ダイナミック ENAT にスタティック ENAT の設定を加えた例。ppp0 に割り当てられたアドレスの TCP ポート 80 番へ宛てられたパケットを、プライベート側端末 192.168.10.5 のポート 80 番に転送する。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
ADD FIRE POLI=net RU=1 AC=ALLOW INT=ppp0 PROT=TCP GBLIP=0.0.0.0
  GBLPORT=80 IP=192.168.10.5 PORT=80
```

■192.168.10.5 と 200.100.10.5 を相互変換するスタティック NAT の設定。ppp0 は外側インターフェースなので、通常は PUBLIC に設定されているはず。その場合は、ルールを追加してパケットを許可するよう設定しないと通信できないので注意が必要。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=eth0 IP=192.168.10.5 GBLINT=ppp0
  GBLIP=200.100.10.5
ADD FIREWALL POLICY=net RULE=1 ACTION=ALLOW INT=ppp0 PROT=ALL
  IP=192.168.10.5 GBLIP=200.100.10.5
```

備考・注意事項

スタティック ENAT（ポートフォワーディング）の設定は、ADD FIREWALL POLICY RULE コマンドで行う（コマンド例を参照）。

関連コマンド

CREATE FIREWALL POLICY（39 ページ）
DELETE FIREWALL POLICY NAT（42 ページ）
SHOW FIREWALL POLICY（58 ページ）

ADD FIREWALL POLICY RULE

カテゴリー：ファイアウォール / フィルタールール
対象機種：AR130、AR160

ADD FIREWALL POLICY=*policy* RULE=*rule-id* ACTION={**ALLOW**|**DENY**}
INTERFACE=*interface* PROTOCOL={***protocol*|**ALL**|**GRE**|**OSPF**|**SA**|**TCP**|**UDP**}
[GBLIP=*ipadd*] [GBLPORT={ALL|*port*[-*port*]}] [IP=*ipadd*[-*ipadd*]] [PORT={ALL|*port*[-*port*]|*service-name*] [REMOTEIP=*ipadd*[-*ipadd*]] [SOURCEPORT={ALL|*port*[-*port*]}]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
rule-id: ルール番号（1〜299）
interface: IP インターフェース名（eth0、ppp0 など）
protocol: IP プロトコル番号（0〜255）
ipadd: IP アドレス
port: TCP / UDP ポート番号（0〜65535）
service-name: サービス名

解説

ファイアウォールポリシーに独自ルールを追加する。
始点・終点 IP アドレスやポート番号、プロトコルにもとづき、PRIVATE・PUBLIC インターフェース間のトラフィック制御（許可・拒否）が可能。ルールは番号の若い順に検索され、最初にマッチしたものが適用される。
なお、インターフェース NAT（ADD FIREWALL POLICY NAT コマンド）でダイナミック ENAT の設定をしている場合は、本コマンドでスタティック ENAT（ポート / プロトコル転送）の設定を追加することができる。また、インターフェース NAT でスタティック NAT（一対一 NAT）の設定をしている場合は、本コマンドでスタティック NAT 対象アドレス宛パケットを通過させるよう設定しなくてはならない。

パラメーター

POLICY　ファイアウォールポリシー名
RULE　ルール番号
ACTION　アクション。ALLOW（通過）、DENY（破棄）から選択する。
INTERFACE　ルールを適用する IP インターフェース名
PROTOCOL　IP プロトコル。定義済みのプロトコル名かプロトコル番号で指定。TCP、UDP を指定したときは、PORT パラメーターも必須
GBLIP　NAT 使用時のグローバル側 IP アドレス。変換前のプライベート IP アドレスは IP パラメーターで指定する。
GBLPORT　ENAT 使用時のグローバル側ポート番号またはサービス名。ハイフン区切りで範囲指定も可能。プライベート側でのポート番号は PORT パラメーターで指定する。
IP　IP アドレス。ハイフン区切りで範囲指定も可能。NAT 使用時は、IP パラメーターでプライベート側

IP アドレスを指定し、GBLIP パラメーターで変換後のグローバル IP アドレスを指定する。

PORT　終点ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。ALL はすべてのポートにマッチする。また、ENAT 使用時は、プライベート側でのポート番号を指定する。グローバル側でのポート番号は GBLPORT パラメーターで指定する。

REMOTEIP　リモート側 IP アドレス。PUBLIC から PRIVATE へのフローでは始点アドレス、PRIVATE から PUBLIC へのフローでは終点アドレスとなる。0.0.0.0 は指定できない。

SOURCEPORT　始点ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。

サービス名	ポート番号
ECHO	7
DISCARD	9
FTP	21
TELNET	23
SMTP	25
TIME	37
DNS	53
BOOTPS	67
BOOTPC	68
TFTP	69
GOPHER	70
FINGER	79
WWW	80
HTTP	80
KERBEROS	88
RTELNET	107
POP2	109
POP3	110
SNMPTRAP	162
SNMP	161
BGP	179
RIP	520
L2TP	1701
VDOLIVE	7000
REALAUDIO	7070
REALVIDEO	7070

表 10: 定義済みのサービス名と TCP / UDP ポート番号

例

■LAN（eth0）側からの MS-Networks パケット（終点ポート 137～139）を遮断する。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=DENY INT=eth0 PROT=UDP PORT=137-139
ADD FIREWALL POLICY=mynet RULE=2 AC=DENY INT=eth0 PROT=TCP PORT=137-139
```

■終点アドレスが 200.100.10.10 のものに限り、ppp0 側からのパケットを通過させる。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=ALL
  IP=200.100.10.10
```

■終点アドレスが 200.100.10.5 で終点ポートが TCP 80 番のものに限り、ppp0 側からのパケットを通過させる。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=TCP
  IP=200.100.10.5 PORT=80
```

関連コマンド

CREATE FIREWALL POLICY（39 ページ）
DELETE FIREWALL POLICY RULE（43 ページ）
SET FIREWALL POLICY RULE（54 ページ）
SHOW FIREWALL POLICY（58 ページ）

CREATE FIREWALL POLICY

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

CREATE FIREWALL POLICY=*policy*

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ファイアウォールの動作を規定するファイアウォールポリシーを作成する。
ただし、ADD FIREWALL POLICY INTERFACE コマンドで PUBLIC と PRIVATE のインターフェースを追加するまでは、ファイアウォールとしての動作はしない。

パラメーター

POLICY　ファイアウォールポリシー名

例

■ファイアウォールポリシー「mynet」を作成する。

```
CREATE FIREWALL POLICY=mynet
```

関連コマンド

ADD FIREWALL POLICY INTERFACE（31 ページ）
ADD FIREWALL POLICY NAT（33 ページ）
ADD FIREWALL POLICY RULE（36 ページ）
DESTROY FIREWALL POLICY（45 ページ）
DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SHOW FIREWALL POLICY（58 ページ）

DELETE FIREWALL POLICY APPRULE

カテゴリー：ファイアウォール / フィルタールール
対象機種：AR130、AR160

DELETE FIREWALL POLICY=*policy* APPRULE=*app-rule-id*

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
app-rule-id: アプリケーションルール番号（1〜299）

解説

ファイアウォールポリシーからアプリケーションルールを削除する。

パラメーター

POLICY　ファイアウォールポリシー名
APPRULE　アプリケーションルール番号

関連コマンド

ADD FIREWALL POLICY APPRULE（29 ページ）
SHOW FIREWALL POLICY（58 ページ）

DELETE FIREWALL POLICY INTERFACE

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

DELETE FIREWALL POLICY=*policy* INTERFACE=*interface*

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
interface: IP インターフェース名（eth0、ppp0 など）

解説

ファイアウォールポリシーからインターフェースを削除する。

パラメーター

POLICY　ファイアウォールポリシー名
INTERFACE　IP インターフェース名

関連コマンド

ADD FIREWALL POLICY INTERFACE（31 ページ）
SHOW FIREWALL POLICY（58 ページ）

DELETE FIREWALL POLICY NAT

カテゴリー：ファイアウォール / ファイアウォール NAT
対象機種：AR130、AR160

DELETE FIREWALL POLICY=*policy* NAT={**ENHANCED**|**STANDARD**}
INTERFACE=*interface* GBLINTERFACE=*interface* [IP=*ipadd*]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

ファイアウォールポリシーからインターフェース NAT ルールを削除する。

パラメーター

POLICY　ファイアウォールポリシー名
NAT　NAT の種類。STANDARD または ENHANCED
INTERFACE　プライベート側 IP インターフェース
IP　スタティック（1 対 1）NAT 時のプライベート側 IP アドレスを指定する。NAT=STANDARD の場合のみ有効
GBLINTERFACE　グローバル側 IP インターフェース

関連コマンド

ADD FIREWALL POLICY NAT（33 ページ）
SHOW FIREWALL POLICY（58 ページ）

DELETE FIREWALL POLICY RULE

カテゴリー：ファイアウォール / フィルタールール
対象機種：AR130、AR160

DELETE FIREWALL POLICY=*policy* RULE=*rule-id*

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
rule-id: ルール番号（1〜299）

解説

ファイアウォールポリシーから独自ルールを削除する。

パラメーター

POLICY　ファイアウォールポリシー名
RULE　ルール番号

関連コマンド

ADD FIREWALL POLICY RULE（36 ページ）
SET FIREWALL POLICY RULE（54 ページ）
SHOW FIREWALL POLICY（58 ページ）

DELETE FIREWALL SESSION

カテゴリー：ファイアウォール / ファイアウォールセッション
対象機種：AR130、AR160

DELETE FIREWALL SESSION={***session-number***|**ALL**}

session-number: ファイアウォールセッション ID

解説

ファイアウォールを介して行われている通信セッションを強制終了する。

パラメーター

SESSION　セッション ID。SHOW FIREWALL SESSION コマンドで確認できる。ALL を指定した場合は、すべてのセッションを終了させる。

関連コマンド

SHOW FIREWALL SESSION（63 ページ）

DESTROY FIREWALL POLICY

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

DESTROY FIREWALL POLICY=*policy*

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ファイアウォールポリシーを削除する。

パラメーター

POLICY　ファイアウォールポリシー名

関連コマンド

CREATE FIREWALL POLICY（39 ページ）
DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SHOW FIREWALL POLICY（58 ページ）

DISABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド
対象機種：AR130、AR160

DISABLE FIREWALL

解説

ファイアウォール機能を無効にする。デフォルトは無効。

関連コマンド

DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL（50 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SHOW FIREWALL（56 ページ）

DISABLE FIREWALL POLICY

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

```
DISABLE FIREWALL POLICY=policy [DEBUG={ALL|PACKET|PKT|PROCESS}]
    [ICMP_FORWARDING={ALL|PARAMETER|PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|
    UNREACHABLE}] [LOG={ALLOW|DENY|DENYDUMP|INAICMP|INALLOW|INAOTHER|INATCP|
    INAUDP|INDDICMP|INDDOTHER|INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|
    INDOTHER|INDTCP|INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|OUTATCP|OUTAUDP|
    OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|OUTDENY|OUTDICMP|
    OUTDOTHER|OUTDTCP|OUTDUDP}] [PING]
```

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ファイアウォールポリシーの各種オプション機能を無効にする。
オプションには、ICMP メッセージの転送可否、デバッグ機能、イベントログ機能などの項目がある。

パラメーター

POLICY　ファイアウォールポリシー名
DEBUG　無効にするデバッグオプション。PKT、PACKET（パケット先頭 56 バイトのダンプ表示）、PROCESS（パケット処理過程の表示）、ALL（すべて）から選択する。
ICMP_FORWARDING　転送しない ICMP メッセージタイプを指定する。カンマ区切りで複数指定可能。ALL を指定した場合は、すべての ICMP メッセージを転送しなくなる（デフォルト）。
LOG　ログへの記録を停止するファイアウォールイベントを指定する。カンマ区切りで複数指定可能。
PING　自分自身に対する PING パケット（ICMP ECHO / ECHO REPLY）の処理を停止する（破棄するようになる）。デフォルトでは自分自身への PING に応答する。

例

■PING パケットの転送を停止する。

```
DISABLE FIREWALL POLICY=mypolicy ICMP_FOWARDING=PING
```

備考・注意事項

ENAT 使用時に PING をディセーブルにすると、ICMP_FORWARDING を有効にしていても内部からの PING がとおらなくなる。

関連コマンド

DISABLE FIREWALL（46 ページ）
ENABLE FIREWALL（50 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SHOW FIREWALL（56 ページ）

DISABLE FIREWALL POLICY IDENTPROXY

カテゴリー：ファイアウォール / ident プロキシー
対象機種：AR130、AR160

DISABLE FIREWALL POLICY=*policy* IDENTPROXY

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ident プロキシー機能を無効にする。
ident プロキシーは、ファイアウォール NAT 使用時に、外部から内部への ident(RFC1413) 要求に対して代理応答する機能。無効時は、ident 接続要求に対して RST を返し、TCP コネクションをただちに終了させる。デフォルトは有効。

パラメーター

POLICY　ファイアウォールポリシー名

関連コマンド

ENABLE FIREWALL POLICY IDENTPROXY（53 ページ）

ENABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド
対象機種：AR130、AR160

ENABLE FIREWALL

解説

ファイアウォール機能を有効にする。デフォルトは無効。

関連コマンド

DISABLE FIREWALL（46 ページ）
DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SHOW FIREWALL（56 ページ）

ENABLE FIREWALL POLICY

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

ENABLE FIREWALL POLICY=*policy* [DEBUG={ALL|PACKET|PKT|PROCESS}]
[ICMP_FORWARDING={ALL|PARAMETER|PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|UNREACHABLE}] [LOG={ALLOW|DENY|DENYDUMP|INAICMP|INALLOW|INAOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|OUTATCP|OUTAUDP|OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|OUTDENY|OUTDICMP|OUTDOTHER|OUTDTCP|OUTDUDP}] [PING]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ファイアウォールポリシーの各種オプション機能を有効にする。
ICMP メッセージの転送、デバッグオプション、イベントログ機能などの設定変更ができる。

パラメーター

POLICY　ファイアウォールポリシー名
DEBUG　有効にするデバッグオプション。PKT、PACKET（パケット先頭 56 バイトのダンプ表示）、PROCESS（パケット処理過程の表示）、ALL（すべて）から選択する。
ICMP_FORWARDING　転送する ICMP メッセージタイプを指定する。カンマ区切りで複数指定可能。ALL を指定した場合は、すべての ICMP メッセージを転送する（セキュリティー的にはお勧めできない）。デフォルトでは、ICMP メッセージはいっさい転送しない。
LOG　ログに記録するファイアウォールイベントを指定する。カンマ区切りで複数指定可能。
PING　自分自身に対する PING パケット（ICMP ECHO / ECHO REPLY）に応答するよう設定する。デフォルトはオン。

例

■ICMP は Ping（Echo / EchoReply）と Unreachable のみ通過させる。

```
ENABLE FIREWALL POLICY=mypolicy ICMP_FOWARDING=PING,UNREACH
```

■ファイアウォールでブロックされたパケットをログに記録するよう設定する

```
ENABLE FIREWALL POLICY=mypollicy LOG=DENY
```

関連コマンド

DISABLE FIREWALL（46 ページ）
DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL（50 ページ）
SHOW FIREWALL（56 ページ）

ENABLE FIREWALL POLICY IDENTPROXY

カテゴリー：ファイアウォール / ident プロキシー
対象機種：AR130、AR160

ENABLE FIREWALL POLICY=*policy* IDENTPROXY

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ident プロキシー機能を有効にする。
ident プロキシーは、ファイアウォール NAT 使用時に、外部から内部への ident(RFC1413) 要求に対して代理応答する機能。ユーザー名 proxyuser で返答する。デフォルトは有効。

パラメーター

POLICY　ファイアウォールポリシー名

備考・注意事項

外部からの ident を拒否するには、DISABLE FIREWALL POLICY IDENTPROXY コマンドを実行する。この場合、ident の接続要求に対して RST を返し接続を終了させるようになる。

関連コマンド

DISABLE FIREWALL POLICY IDENTPROXY（49 ページ）

SET FIREWALL POLICY RULE

カテゴリー：ファイアウォール / フィルタールール
対象機種：AR130、AR160

SET FIREWALL POLICY=*policy* RULE=*rule-id* [PROTOCOL={*protocol*|ALL|GRE|OSPF|SA|TCP|UDP}] [GBLIP=*ipadd*] [GBLPORT={ALL|*port*[-*port*]}] [IP=*ipadd*[-*ipadd*]] [PORT={ALL|*port*[-*port*]|*service-name*}] [REMOTEIP=*ipadd*[-*ipadd*]] [SOURCEPORT={ALL|*port*[-*port*]}]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
rule-id: ルール番号（1〜299）
protocol: IP プロトコル番号（0〜255）
ipadd: IP アドレス
port: TCP / UDP ポート番号（0〜65535）
service-name: サービス名

解説

ファイアウォールルールの設定を変更する。

パラメーター

POLICY　ファイアウォールポリシー名
RULE　ルール番号
PROTOCOL　IP プロトコル。定義済みのプロトコル名かプロトコル番号で指定。TCP、UDP を指定したときは、PORT パラメーターも必須
GBLIP　NAT 使用時のグローバル側 IP アドレス。変換前のプライベート IP アドレスは IP パラメーターで指定する。
GBLPORT　ENAT 使用時のグローバル側ポート番号またはサービス名。ハイフン区切りで範囲指定も可能。プライベート側でのポート番号は PORT パラメーターで指定する。
IP　IP アドレス。ハイフン区切りで範囲指定も可能。NAT 使用時は、IP パラメーターでプライベート側 IP アドレスを指定し、GBLIP パラメーターで変換後のグローバル IP アドレスを指定する。
PORT　終点ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。ALL はすべてのポートにマッチする。また、ENAT 使用時は、プライベート側でのポート番号を指定する。グローバル側でのポート番号は GBLPORT パラメーターで指定する。
REMOTEIP　リモート側 IP アドレス。PUBLIC から PRIVATE へのフローでは始点アドレス、PRIVATE から PUBLIC へのフローでは終点アドレスとなる。0.0.0.0 は指定できない。
SOURCEPORT　始点ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。

関連コマンド

ADD FIREWALL POLICY RULE（36 ページ）

DELETE FIREWALL POLICY RULE（43 ページ）
SHOW FIREWALL POLICY（58 ページ）

SHOW FIREWALL

カテゴリー：ファイアウォール / 一般コマンド
対象機種：AR130、AR160

SHOW FIREWALL

解説

ファイアウォールのグローバル設定とポリシーの一覧を表示する。

入力・出力・画面例

```
Manager > show firewall


Firewall Configuration

Status ..................... enabled

Policy : net
  TCP Timeout (s) ................... 3600
  UDP Timeout (s) ................... 1200
  Other Timeout (s) ................. 1200
  Private Interface : eth0-1
  Private Interface : eth0-0
  Public Interface  : ppp0-0
    Method ......................... dynamic
    NAT ............................ enhanced
      Method ....................... enhanced dynamic
      Private Interface ............. eth0-1
      Global IP ..................... 4.4.4.1
```

Status	ファイアウォール機能の有効（enabled）・無効（disabled）
Policy	ファイアウォールポリシー名
TCP Timeout	TCP セッションのタイムアウト（秒）
UDP Timeout	UDP フローのタイムアウト（秒）
Other Timeout	TCP、UDP 以外のフローのタイムアウト（秒）
Private Interface	PRIVATE（内部）IP インターフェース名
Public Interface	PUBLIC（外部）IP インターフェース名
Method	PUBLIC-PRIVATE 間のパケット転送方式。dynamic（ダイナミックパケットフィルタリング）か passall（フィルタリングしない）。

NAT	NAT の種別。standard（アドレス変換）か enhanced（アドレス・ポート変換）。以下、NAT 有効時のみ表示。
NAT/Method	NAT の方式。static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか
NAT/Private Interface	NAT のプライベート側インターフェース
NAT/IP	NAT のプライベート側 IP アドレス
NAT Global IP	NAT のグローバル側 IP アドレス

表 11:

関連コマンド

ADD FIREWALL POLICY INTERFACE（31 ページ）
CREATE FIREWALL POLICY（39 ページ）
DELETE FIREWALL POLICY INTERFACE（41 ページ）
DESTROY FIREWALL POLICY（45 ページ）
DISABLE FIREWALL（46 ページ）
ENABLE FIREWALL（50 ページ）

SHOW FIREWALL POLICY

カテゴリー：ファイアウォール / ファイアウォールポリシー
対象機種：AR130、AR160

SHOW FIREWALL POLICY=*policy* [COUNTER] [SUMMARY]

policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）

解説

ファイアウォールポリシーの詳細な設定情報・統計情報等を表示する。

パラメーター

POLICY　ファイアウォールポリシー名
COUNTER　統計カウンター情報を表示する。
SUMMARY　サマリー情報を表示する。

入力・出力・画面例

```
Manager > show firewall policy

Policy : net
  TCP Timeout (s) ................... 3600
  UDP Timeout (s) ................... 1200
  Other Timeout (s) ................. 1200
  Enabled Logging Options ........... deny
  Enabled Debug Options ............. none
  Identification Protocol Proxy ..... disabled
  Enabled ICMP forwarding ........... unreachable ping
  Receive of ICMP PINGS ............. enabled
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 0
  Cache Hits ........................ 0
  Discarded ICMP Packets ............ 0
  Private Interface : eth0-1
  Private Interface : eth0-0
  Public Interface  : ppp0-0
    Method .......................... dynamic
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
      Private Interface ............. eth0-1
      Global IP ..................... 4.4.4.1
    Rule ............................ 1
      Action ........................ allow
```

```
    IP ........................... 4.4.4.2
    Protocol ..................... TCP
    Port ......................... 80
    Global IP .................... 0.0.0.0
    Global Port .................. all
  Rule ........................... 2
    Action ....................... allow
    IP ........................... 4.4.4.3
    Protocol ..................... TCP
    Port ......................... 25
    Global IP .................... 0.0.0.0
    Global Port .................. all
  Rule ........................... 3
    Action ....................... allow
    IP ........................... 4.4.4.4
    Protocol ..................... TCP
    Port ......................... 53
    Global IP .................... 0.0.0.0
    Global Port .................. all
  Rule ........................... 4
    Action ....................... allow
    IP ........................... 4.4.4.4
    Protocol ..................... UDP
    Port ......................... 53
    Global IP .................... 0.0.0.0
    Global Port .................. all
```

Policy	ファイアウォールポリシー名
TCP Timeout	TCP セッションのタイムアウト（秒）
UDP Timeout	UDP フローのタイムアウト（秒）
Other Timeout	TCP、UDP 以外のフローのタイムアウト（秒）
Enabled Logging Options	ログに記録するイベントの一覧。allow、deny、denydump、inaicmp、inallow、inaother、inatcp、inaudp、inddicmp、inddother、inddtcp、inddudp、inddump、indeny、indicmp、indother、indtcp、indudp、outaicmp、outallow、outaother、outatcp、outaudp、outddicmp、outddother、outddtcp、outddudp、outddump、outdeny、outdicmp、outdother、outdtcp、outdudp、none がある。
Enabled Debug Options	有効なデバッグオプションの一覧。all、packet、process、none。
Identification Protocol Proxy	ident プロキシーの有効・無効
Enabled ICMP forwarding	転送する ICMP メッセージの一覧。all、parameter、ping、source-quench、timeexceeded、timestamp、unreachable、none。
Receive of ICMP PINGS	自身宛ての PING パケットを処理するかどうか。
Number of Active TCP Opens	現在アクティブな TCP セッション数

Number of Active Sessions	現在アクティブなセッション数
Cache Hits	フロー検索時のキャッシュヒット数
Discarded ICMP Packets	破棄した ICMP パケット数
Private Interface	PRIVATE（内部）インターフェース名
Public Interface	PUBLIC（外部）インターフェース名
Method	PUBLIC-PRIVATE 間のパケット転送方式。dynamic か passall。
NAT	NAT の種別。standard（アドレス変換）か enhanced（アドレス・ポート変換）。NAT 有効時のみ表示
NAT/Method	NAT の方式。none、static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか。NAT 有効時のみ表示
NAT/Private Interface	NAT のプライベート側インターフェース
NAT Global IP	NAT のグローバル側 IP アドレス。
Rule	ルール番号
Action	ルールのアクション。allow か deny。
Protocol	IP プロトコルタイプ
Port	ポート番号またはサービス名。
Global IP	NAT 有効時のグローバル側 IP アドレス
Global Port	NAT 使用時のグローバル側ポート番号またはサービス名
Remote IP	リモートエンドの IP アドレス
Source Port	始点ポート番号
Apprule	アプリケーションルール番号
Application	アプリケーションプロトコル
Action	ルールのアクション。allow か deny
Command	アプリケーションコマンド

表 12:

Policy	ファイアウォールポリシー名
TCP Timeout	TCP セッションのタイムアウト（秒）
UDP Timeout	UDP フローのタイムアウト（秒）
Other Timeout	TCP、UDP 以外のフローのタイムアウト（秒）
Enabled Logging Options	ログに記録するイベントの一覧。allow、deny、denydump、inaicmp、inallow、inaother、inatcp、inaudp、inddicmp、inddother、inddtcp、inddudp、inddump、indeny、indicmp、indother、indtcp、indudp、outaicmp、outallow、outaother、outatcp、outaudp、outddicmp、outddother、outddtcp、outddudp、outddump、outdeny、outdicmp、outdother、outdtcp、outdudp、none がある。

Enabled Debug Options	有効なデバッグオプションの一覧。all、packet、process、none。
Identification Protocol Proxy	ident プロキシーの有効・無効
Enabled ICMP forwarding	転送する ICMP メッセージの一覧。all、parameter、ping、redirect、sourcequench、timeexceeded、timestamp、unreachable、none。
Receive of ICMP PINGS	自身宛ての PING パケットを処理するかどうか。
Number of Active TCP Opens	現在アクティブな TCP セッション数
Number of Active Sessions	現在アクティブなセッション数
Cache Hits	フロー検索時のキャッシュヒット数
Discarded ICMP Packets	破棄した ICMP パケット数
Private Interface	PRIVATE（内部）インターフェース名
Public Interface	PUBLIC（外部）インターフェース名
Total Packets Received	受信パケット総数
Number Flows Started	開始フロー数
Number Cache Hits	フロー検索キャッシュヒット数
Number Dropped Packets	受信後破棄パケット数
Number Unknown IP Protocols	IP プロトコル不明の受信パケット数
Number Bad ICMP Packets	ICMP エラーパケット受信数
Number Dumped ICMP Packets	ダンプした受信 ICMP パケット数
Number Spoofing Packets	Smurf 攻撃の始点アドレス詐称パケット受信数
Number Dropped GBLIP Zero	グローバル IP アドレスがゼロのためダンプした受信パケット数
Number No Spare Entries	メモリー不足のためダンプした受信パケット数
Number FTP Port Commands	有効な FTP PORT コマンド受信数
Number Bad FTP Port Commands	無効な FTP PORT コマンド受信数
Method	PUBLIC-PRIVATE 間のパケット転送方式。dynamic か passall。
NAT	NAT の種別。standard（アドレス変換）か enhanced（アドレス・ポート変換）。NAT 有効時のみ表示
NAT/Method	NAT の方式。none、static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか。NAT 有効時のみ表示
NAT/Private Interface	NAT のプライベート側インターフェース
NAT Global IP	NAT のグローバル側 IP アドレス。
Rule	ルール番号
Action	ルールのアクション。allow か deny。
IP List	本ルールが使用する IP アドレスリスト名（およびファイル名）
Hardware List	本ルールが使用する MAC アドレスリスト名（およびファイル名）

Protocol	IP プロトコルタイプ
Port	ポート番号またはサービス名。
Global IP	NAT 有効時のグローバル側 IP アドレス
Global Port	NAT 使用時のグローバル側ポート番号またはサービス名
Remote IP	リモートエンドの IP アドレス
Source Port	始点ポート番号

表 13: COUTER オプション

関連コマンド

ADD FIREWALL POLICY INTERFACE（31 ページ）
ADD FIREWALL POLICY NAT（33 ページ）
ADD FIREWALL POLICY RULE（36 ページ）
CREATE FIREWALL POLICY（39 ページ）
DELETE FIREWALL POLICY INTERFACE（41 ページ）
DELETE FIREWALL POLICY NAT（42 ページ）
DELETE FIREWALL POLICY RULE（43 ページ）
DESTROY FIREWALL POLICY（45 ページ）
DISABLE FIREWALL POLICY（47 ページ）
ENABLE FIREWALL POLICY（51 ページ）
SET FIREWALL POLICY RULE（54 ページ）
SHOW FIREWALL（56 ページ）

SHOW FIREWALL SESSION

カテゴリー：ファイアウォール / ファイアウォールセッション
対象機種：AR130、AR160

SHOW FIREWALL SESSION[=*session-number*] [POLICY=*policy*] [COUNTER]
[PORT={*port-port*|*service-name*}] [PROTOCOL={*protocol*|ALL|ICMP|OSPF|TCP|UDP}] [SUMMARY]

session-number: ファイアウォールセッション ID
policy: ファイアウォールポリシー名（1〜15 文字。英数字とアンダースコア（_）を使用可能）
port: TCP / UDP ポート番号（0〜65535）
service-name: サービス名
protocol: IP プロトコル番号（0〜255）

解説

ファイアウォールを介して行われている通信セッションの一覧を表示する。

パラメーター

SESSION　セッション ID。省略時はすべてのセッションが表示される。
POLICY　ファイアウォールポリシー名
COUNTER　各セッションの統計情報を表示する。
PORT　TCP / UDP ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。指定時は、該当ポート / サービスを使用するセッションだけが表示される。
PROTOCOL　IP プロトコル。指定時は該当プロトコルのセッションだけが表示される。
SUMMARY　サマリー情報を表示する。

入力・出力・画面例

```
Manager > show firewall session

Policy : tuna
Current Sessions
--------------------------------------------------------------------------------
e33a UDP      IP: 192.168.10.100:64521      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:58170   Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:17:50 07-Mar-2002
     Seconds to deletion .................. 300
7c81 UDP      IP: 192.168.10.100:64525      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:31873   Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:17:41 07-Mar-2002
     Seconds to deletion .................. 288
60ed UDP      IP: 192.168.10.100:64526      Remote IP: 172.17.28.1:53
```

```
          Gbl IP: 172.17.28.185:24813   Gbl Remote IP: 172.17.28.1:53
     Start time ........................... 17:17:41 07-Mar-2002
     Seconds to deletion .................. 288
4272 TCP      IP: 192.168.10.100:65489      Remote IP: 172.17.17.31:3128
          Gbl IP: 172.17.28.185:17010   Gbl Remote IP: 172.17.17.31:3128
     TCP state ............................ closed
     Start time ........................... 17:17:04 07-Mar-2002
     Seconds to deletion .................. 252
a9be TCP      IP: 192.168.10.100:65487      Remote IP: 172.29.188.31:23
          Gbl IP: 172.17.28.185:43454   Gbl Remote IP: 172.29.188.31:23
     TCP state ............................ established
     Start time ........................... 17:21:33 07-Mar-2002
     Seconds to deletion .................. 3600
e245 TCP      IP: 192.168.10.100:65486      Remote IP: 10.1.2.103:22
          Gbl IP: 172.17.28.185:57925   Gbl Remote IP: 10.1.2.103:22
     TCP state ............................ established
     Start time ........................... 17:22:39 07-Mar-2002
     Seconds to deletion .................. 3594
------------------------------------------------------------------------------

Manager >  show firewall session counter

Policy : net
Current Sessions
------------------------------------------------------------------------------
fb3b UDP      IP: 192.168.10.100:64505      Remote IP: 172.17.28.1:53
          Gbl IP: 172.17.28.185:64315   Gbl Remote IP: 172.17.28.1:53
     Packets from private IP .............. 1
     Octets from private IP ............... 75
     Packets to private IP ................ 1
     Octets to private IP ................. 152
     Start time ........................... 17:35:09 07-Mar-2002
     Seconds to deletion .................. 282
5e9e TCP      IP: 192.168.10.100:65484      Remote IP: 172.29.28.103:22
          Gbl IP: 172.17.28.185:24222   Gbl Remote IP: 172.29.28.103:22
     Packets from private IP .............. 12
     Octets from private IP ............... 1123
     Packets to private IP ................ 11
     Octets to private IP ................. 1176
     TCP state ............................ established
     Start time ........................... 17:35:17 07-Mar-2002
     Seconds to deletion .................. 3594
28c7 TCP      IP: 192.168.10.100:65485      Remote IP: 172.29.28.103:22
          Gbl IP: 172.17.28.185:10439   Gbl Remote IP: 172.29.28.103:22
     Packets from private IP .............. 11
     Octets from private IP ............... 859
     Packets to private IP ................ 9
     Octets to private IP ................. 840
     TCP state ............................ timeWait
     Start time ........................... 17:35:09 07-Mar-2002
     Seconds to deletion .................. 282
```

Policy	ファイアウォールポリシー名
hex-num	セッション ID
TCP / UDP / number	IP プロトコル（TCP、UDP、IP プロトコル番号のいずれか）
IP	外向きパケットでは始点 IP アドレス:ポート、内向きパケットでは終点 IP アドレス:ポート。いずれも PRIVATE インターフェース側で見たアドレス。
Remote IP	外向きパケットでは終点 IP アドレス:ポート、内向きパケットでは始点 IP アドレス:ポート。いずれも PRIVATE インターフェース側で見たアドレス。
Gbl IP	外向きパケットでは始点 IP アドレス:ポート、内向きパケットでは始点 IP アドレス:ポート。いずれも PUBLIC インターフェース側で見たアドレス。
Gbl Remote IP	外向きパケットでは終点 IP アドレス:ポート、内向きパケットでは始点 IP アドレス:ポート。いずれも PUBLIC インターフェース側で見たアドレス。
Packets from private IP	内部（PRIVATE）から外部（PUBLIC）に転送されたパケットの数
Octets from private IP	内部から外部に転送されたオクテット数
Packets to private IP	外部から内部に転送されたパケットの数
Octets to private IP	外部から内部に転送されたオクテット数
TCP state	TCP セッションの状態。free、closed、listen、synSent、synReceived、established、finWait1、finWait2、closeWait、lastAck、closing、timeWait、deleteTCB、synSent、synReceived、RADIUS query のいずれか。
Start time	セッション開始日時
Seconds to deletion	セッション削除までの残り時間（秒）

表 14:

関連コマンド

DELETE FIREWALL SESSION（44 ページ）
SHOW FIREWALL POLICY（58 ページ）