

# ファイアウォール

概要・基本設定	4
IP フィルターとの比較	4
基本設定	4
インターフェースと基本ルール	6
ルールの追加	8
トラフィックを制限する	8
アクセスを許可する	10
インターフェース NAT	13
ルール NAT	20
アクセスリストによるルール	25
RADIUS サーバーを利用したルール	27
ルールの時間制限	28
ルールの確認・修正・削除	29
ルールの処理順序	29
ファイアウォールの動作監視	30
ログ	30
イベント通知	33
トリガー	35
アカウンティング	36
デバッグオプション	37
セッションの確認	39
ダイナミックインターフェース	40
テンプレートの作成	40
テンプレートの使用	42
アプリケーション検出・遮断機能 (Application Detection System : ADS)	42
サポートする Winny バージョン	43
Winny 関連のログ	43
その他設定	43
UPnP	46
基本設定	46
コマンドリファレンス編	48
機能別コマンド索引	48
ADD FIREWALL MONITOR	50
ADD FIREWALL POLICY APPRULE	51

ADD FIREWALL POLICY DYNAMIC . . . . .	52
ADD FIREWALL POLICY INTERFACE . . . . .	54
ADD FIREWALL POLICY LIMITRULE . . . . .	56
ADD FIREWALL POLICY LIST . . . . .	58
ADD FIREWALL POLICY NAT . . . . .	60
ADD FIREWALL POLICY RULE . . . . .	63
ADD FIREWALL POLICY UDPPORTTIMEOUT . . . . .	67
CREATE FIREWALL POLICY . . . . .	69
CREATE FIREWALL POLICY DYNAMIC . . . . .	70
DELETE FIREWALL MONITOR . . . . .	71
DELETE FIREWALL POLICY APPRULE . . . . .	72
DELETE FIREWALL POLICY DYNAMIC . . . . .	73
DELETE FIREWALL POLICY INTERFACE . . . . .	74
DELETE FIREWALL POLICY LIMITRULE . . . . .	75
DELETE FIREWALL POLICY LIST . . . . .	76
DELETE FIREWALL POLICY NAT . . . . .	77
DELETE FIREWALL POLICY RULE . . . . .	78
DELETE FIREWALL POLICY UDPPORTTIMEOUT . . . . .	79
DELETE FIREWALL SESSION . . . . .	80
DESTROY FIREWALL POLICY . . . . .	81
DESTROY FIREWALL POLICY DYNAMIC . . . . .	82
DISABLE FIREWALL . . . . .	83
DISABLE FIREWALL MONITOR . . . . .	84
DISABLE FIREWALL NOTIFY . . . . .	85
DISABLE FIREWALL POLICY . . . . .	86
DISABLE FIREWALL POLICY IDENTPROXY . . . . .	88
DISABLE FIREWALL POLICY P2PFILTER . . . . .	89
DISABLE FIREWALL POLICY TCPSETUPPROXY . . . . .	90
DISABLE UPNP . . . . .	91
DISABLE UPNP ACTION . . . . .	92
DISABLE UPNP L4PORT . . . . .	93
ENABLE FIREWALL . . . . .	94
ENABLE FIREWALL MONITOR . . . . .	95
ENABLE FIREWALL NOTIFY . . . . .	96
ENABLE FIREWALL POLICY . . . . .	97
ENABLE FIREWALL POLICY IDENTPROXY . . . . .	99
ENABLE FIREWALL POLICY P2PFILTER . . . . .	100
ENABLE FIREWALL POLICY TCPSETUPPROXY . . . . .	101
ENABLE UPNP . . . . .	102
ENABLE UPNP ACTION . . . . .	103
ENABLE UPNP L4PORT . . . . .	104
SET FIREWALL MAXFRAGMENTS . . . . .	105

SET FIREWALL MONITOR . . . . .	106
SET FIREWALL POLICY . . . . .	107
SET FIREWALL POLICY ATTACK . . . . .	108
SET FIREWALL POLICY LIMITRULE . . . . .	111
SET FIREWALL POLICY RULE . . . . .	112
SET FIREWALL POLICY UDPPORTTIMEOUT . . . . .	114
SHOW FIREWALL . . . . .	115
SHOW FIREWALL ACCOUNTING . . . . .	118
SHOW FIREWALL ARP . . . . .	120
SHOW FIREWALL EVENT . . . . .	122
SHOW FIREWALL MONITOR . . . . .	124
SHOW FIREWALL POLICY . . . . .	125
SHOW FIREWALL POLICY ATTACK . . . . .	134
SHOW FIREWALL POLICY LIMITRULE . . . . .	136
SHOW FIREWALL POLICY P2PFILTER . . . . .	138
SHOW FIREWALL POLICY UDPPORTTIMEOUT . . . . .	139
SHOW FIREWALL SESSION . . . . .	141
SHOW UPNP . . . . .	144
SHOW UPNP COUNTER . . . . .	146
SHOW UPNP INTERFACE . . . . .	149

## 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。

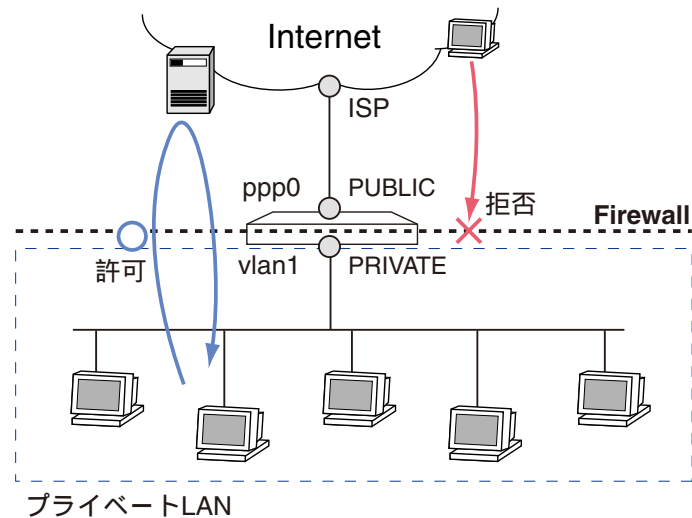
また、通信状態を保持しておくステートフルインスペクションは、NAT（Network Address Translation）と共通の部分が多いため、ファイアウォールには NAT の機能も統合されています。本製品には、IP モジュールの NAT 機能（レンジ NAT）もありますが、ファイアウォールを使う場合、レンジ NAT は使えません。ファイアウォール内蔵の NAT 機能を使ってください。ファイアウォールの NAT 機能には、インターフェース単位で設定するインターフェース NAT と、ファイアウォールルールの一部として記述するルール NAT があります。詳細は本章の「インターフェース NAT」「ルール NAT」をご覧ください。

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したり、重大なイベントの発生時に自動通知を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 ㇿ
```

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 ㇿ
```

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=vlan1 TYPE=PRIVATE ㇿ
```

```
ADD FIREWALL POLICY=mynet INT=ppp0 TYPE=PUBLIC ㇿ
```

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=vlan1 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には次の 3 種類があります。

- 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（63 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。

- NAT ルール：ルール NAT の変換ルールを定義する。
- ◇ 「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（97 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での通信

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での通信（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での通信可否

- 「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

前記の基本設定に独自ルールを追加するには、ADD FIREWALL POLICY RULE コマンド (63 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小さい順に行われ、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 (vlan1) 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=vlan1 PROT=TCP PORT=135 ↓
ADD FIREWALL POLICY=mynet RULE=2 AC=DENY INT=vlan1 PROT=UDP PORT=135 ↓
ADD FIREWALL POLICY=mynet RULE=3 AC=DENY INT=vlan1 PROT=TCP
PORT=137-139 ↓
ADD FIREWALL POLICY=mynet RULE=4 AC=DENY INT=vlan1 PROT=UDP
PORT=137-139 ↓
ADD FIREWALL POLICY=mynet RULE=5 AC=DENY INT=vlan1 PROT=TCP PORT=445 ↓
```

5つのコマンドは、「vlan1 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=vlan1 PROT=ALL
REMOTEIP=12.34.56.0-12.34.56.255 ↵
```

このコマンドは、「vlan1 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。

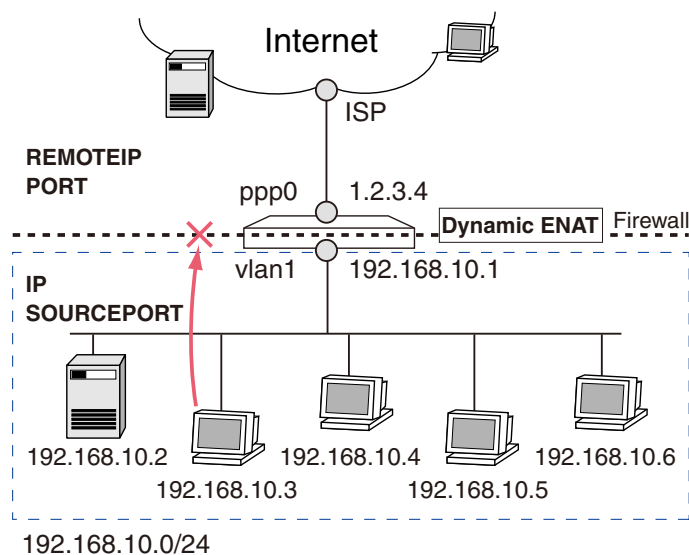
＼ デフォルトでは ICMP はファイアウォールを通過しません。ICMP の転送を有効にするには、ENABLE FIREWALL POLICY コマンド (97 ページ) の ICMP\_FORWARDING オプションを使う必要があります。

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=vlan1 PROT=ALL
IP=192.168.10.3 ↵
```

このコマンドは、「vlan1 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 については「PROTOCOL=ALL」を指定していたとしても、別途 ICMP の転送を有効にしておかないとファイアウォールを通過できません。ICMP の転送を有効にするには、ENABLE FIREWALL POLICY コマンド（97 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=vlan1 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。

NAT を使用している場合に、外部からルーター自身に対するパケットを通過させたい場合は、GBLIP と IP に同じアドレスを指定します。たとえば、ルーター (4.4.4.1) 宛ての ISAKMP パケット (終点ポートが UDP 500 番) を受け入れたい場合は次のようにします。これは、自動鍵交換による IPsec とファイアウォールを併用する場合に必須の設定です。詳細は「IPsec」の章をご覧ください。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=ppp0 PROT=UDP GBLIP=4.4.4.1
    GBLPORT=500 IP=4.4.4.1 PORT=500 ↵
```

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 アドレスがルーター自身 (4.4.4.1) で終点ポートが 500 番の UDP パケットを受け入れる」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、インターフェース単位で設定するインターフェース NAT と、アドレス単位で指定するルール NAT の 2 種類の NAT 機能が実装されています。

ルール NAT では、インターフェース NAT よりも細かい制御が可能ですが、その分設定も複雑になります。よほど特殊な設定をしたいとき以外はインターフェース NAT を使うようにしてください。また、両者は併用可能ですが、設定の見通しが悪くなりがちなので、通常はどちらか一方だけを使うようにしてください。

- ✧ インターフェース NAT とルール NAT の両方を設定した場合、ルール NAT のほうが優先的に適用されます。設定の見通しをよくするためにも、通常はどちらか一方のみをご使用ください。

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。

インターフェース NAT は、アドレス変換のパターンによって次の 4 種類に分類できます。

- スタティック NAT
- ダイナミック NAT
- ダイナミック ENAT
- スタティック ENAT

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 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 で固定的に変換する NAT です。アドレスが固定なので、プライベート側、グローバル側のどちらからでも通信を開始できます（ただし、グローバル側から通信を開始できるようにするには、明示的な許可ルールの設定が必要です）。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 の設定に使うパラメーターは次のとおりです。ここで「内 IF」は PRIVATE インター

フェース、「外 IF」は PUBLIC インターフェース、「内 IP」は NAT 前のプライベートアドレス、「外 IP」は NAT 後のグローバルアドレスを示します。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=内 IF GBLINT=外 IF IP=内 IP GBLIP=外 IP ↓
```

- パケットを「内 IF」から「外 IF」に転送したとき、始点 IP アドレスが「内 IP」であれば「外 IP」に書き換えます。
- パケットを「外 IF」で受信したとき、終点 IP アドレスが「外 IP」であれば「内 IP」に書き換えます。

スタティック NAT の設定をしていても、外側から内側への通信は基本ルールにより拒否されます。外側からの通信開始を可能にするには、「外 IF」に次のような許可ルールを設定してください。

```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=外 IF PROTOCOL=プロトコル IP=内 IP GBLIP=外 IP ↓
```

あるいは、PUBLIC インターフェースをポリシーに追加するときに「METHOD=PASSALL」を指定する方法もあります。この場合、許可ルールは不要です。

- ※ NAT 用の IP アドレスとして、実インターフェースに割り当てられていない IP アドレスを指定した場合、本製品は NAT 用 IP アドレスへの ARP Request に自動的に応答します。

### ダイナミック NAT

ダイナミック NAT は、プライベート側インターフェースで受信したパケットの始点アドレスを、あらかじめプールされたグローバルアドレス内の使用されていないアドレスに動的変換する多対多の NAT です。グローバルアドレスが固定でないため、グローバル側から通信を開始することはできません。

- ※ ダイナミック NAT は、他の NAT に比べてメリットが少ないためあまり使われません。

ダイナミック NAT の設定に使うパラメーターは次のとおりです。ここで、「内 IF」は PRIVATE インターフェース、「外 IF」は PUBLIC インターフェース、「外 IP 範囲」は NAT 後のグローバルアドレスとして使うアドレス範囲を示します。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=内 IF GBLINT=外 IF GBLIP=外 IP 範囲
```

- パケットを「内 IF」から「外 IF」に転送したとき、始点 IP アドレスを「外 IP 範囲」内の空いているアドレスに書き換えます。また、変換前後のアドレスの組み合わせ（内 IP・外 IP）をテーブルに登録します。
- パケットを「外 IF」で受信したとき、終点 IP アドレスが「外 IP 範囲」内であれば、テーブルを検索し、終点 IP アドレスを「内 IP」に書き換えます。

ダイナミック NAT を使う場合、「外 IF」が Ethernet か VLAN のときは「外 IP 範囲」への ARP に対し

て本製品が代理応答する必要があります。そのためには、「外 IP 範囲」へのスタティック経路を優先度 0 で登録してください。

たとえば、グローバルアドレスとして 1.1.1.2~1.1.1.4 を使うダイナミック NAT を設定する場合、次のような経路を登録してください (PRIVATE 側インターフェースを vlan1 とします)。「PREF=0」を忘れないようご注意ください。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan1 GBLINT=eth0
    GBLIP=1.1.1.2-1.1.1.4 ↵
ADD IP ROUTE=1.1.1.2 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0 ↵
ADD IP ROUTE=1.1.1.3 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0 ↵
ADD IP ROUTE=1.1.1.4 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0 ↵
```

※ NAT 用の IP アドレスとして、実インターフェースに割り当てられていない IP アドレスを指定した場合、本製品は NAT 用 IP アドレスへの ARP Request に自動的に応答します。

### 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。ダイナミック ENAT ではグローバル側から通信を開始することはできませんが、次節の「スタティック ENAT」を併用すればグローバル側からの通信も可能です。

ダイナミック ENAT の設定に使うパラメーターは次のとおりです。ここで、「内 IF」は PRIVATE インターフェース、「外 IF」は PUBLIC インターフェース、「外 IP」は NAT 後のグローバルアドレスを示します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=内 IF GBLINT=外 IF [GBLIP=外 IP]
```

- パケットを「内 IF」から「外 IF」に転送したとき、始点 IP アドレスを「外 IF」のアドレス (GBLIP が指定されているときは「外 IP」) に、始点ポートを未使用のポート番号に書き換えます。また、変換前後のアドレス・ポートの組み合わせ (内 IP・内ポート・外 IP・外ポート) をテーブルに登録します。
- パケットを「外 IF」で受信したとき、終点 IP アドレスが「外 IF」のアドレス (GBLIP が指定されているときは「外 IP」) であれば、終点ポートをキーにテーブルを検索し、終点 IP アドレスを「内 IP」に、終点ポートを「内ポート」に書き換えます。

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=vlan1 GBLINT=ppp0 ↵
```

このコマンドは、「vlan1 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=vlan1-1 GBLINT=ppp0
    GBLIP=1.2.3.6 ↵
```

このコマンドは、「vlan1-1 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

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。

スタティック ENAT は単独では使用できません。必ず最初にダイナミック ENAT の設定をする必要があります。前節の説明の繰り返しになりますが、再度ダイナミック ENAT の設定に必要なパラメーターを挙げます。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=内 IF GBLINT=外 IF ↵
```

スタティック ENAT の設定に使うパラメーターは次のとおりです。ここで、「外 IF」は PUBLIC インターフェース、「プロトコル」は TCP、UDP などの上位プロトコル、「外 IP」はグローバルアドレス、「外ポート」は転送前のポート番号、「内 IP」はプライベートアドレス、「内ポート」は転送先のポート番号を示します。

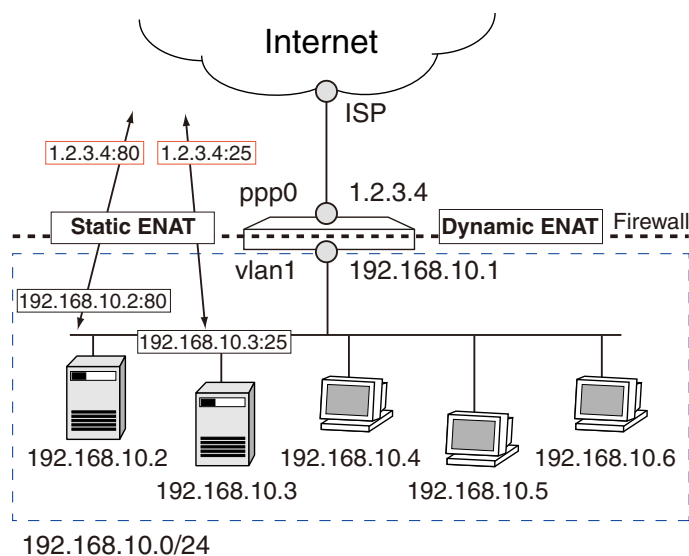
```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=外 IF PROT=プロトコル GBLIP=外 IP
    GBLPORT=外ポート IP=内 IP PORT=内ポート ↵
```

- パケットを「外 IF」で受信したとき、プロトコルが「プロトコル」で、終点 IP アドレスが「外 IP」、終点ポートが「外ポート」であれば、それぞれ「内 IP」「内ポート」に書き換えます。

ㄥ スタティック ENAT の設定は ADD FIREWALL POLICY RULE コマンド (63 ページ) で行います。

ㄥ スタティック ENAT 単独では使用できません。必ずダイナミック ENAT と組み合わせて設定してください。

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 (vlan1) 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=vlan1 GBLINT=ppp0 ㄱ
```

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 ㄱ
```

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。

ㄥ 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も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 ↵
```

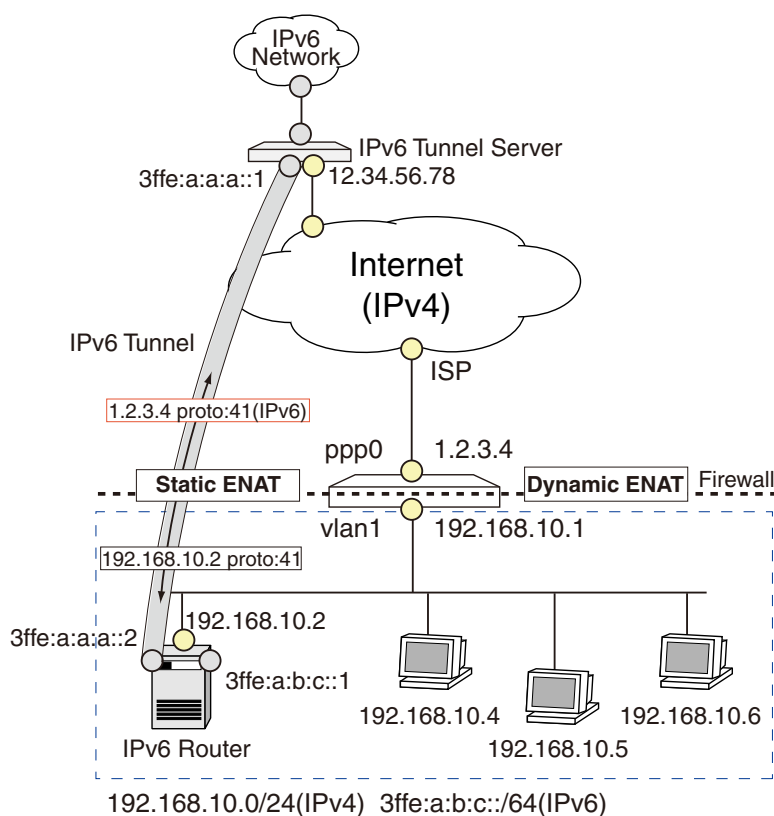
この場合、外部から 192.168.10.10 の Web サーバーにアクセスするには、URL の中でポート番号 8080 を指定する必要があります。ブラウザの URL 欄に次のように入力します。

`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 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。また、プロトコル番号による指定も可能です。ただし、スタティック ENAT では外部から内部に ICMP を転送することはできません
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:

### ENAPT (Port Restricted Cone NAT)

ENAPT(Enhanced Network Address and Port Translation)は、RFC3489でPort Restricted Cone NATと呼ばれている NAT の種類です。ENAPT は、複数のプライベート IP アドレスとポートを、グローバル IP アドレスとポートに変換します。プライベート-グローバル間の関連付けは記憶され、同じプライベート IP アドレスと送信/受信ポートの通信だけが転送されます。

設定を行うには、ADD FIREWALL POLICY NAT コマンド (60 ページ) に NAT=ENAPT オプションを指定します。

```
ADD FIREWALL POLICY=policy NAT=ENAPT INTERFACE=interface
    GBLINTERFACE=interface [GBLIP=ipadd[-ipadd]] ↵
```

### ルール NAT

ルール NAT は、アドレスベースの NAT 機能です。ADD FIREWALL POLICY RULE コマンド (63 ページ) の ACTION に NAT を指定することによって設定を行います。

ルール NAT では、インターフェース NAT より細かい制御が可能ですが、その分設定も複雑になります。通常は従来からあるインターフェース NAT をご使用ください。ルール NAT は、インターフェース NAT で対応できない特殊な設定を行いたい場合にのみ使用してください。

- ルール NAT は、ADD FIREWALL POLICY NAT コマンド (60 ページ) で設定するインターフェース NAT よりも優先的に適用されます。

ルール NAT には、次のようなアドレス変換パターンがあります。また、下記の各パターンと組み合わせて、

IP アドレスのサブネット部だけを変換する「サブネット NAT」も可能です。

- スタンダード NAT : PRIVATE PUBLIC の始点アドレス、PUBLIC PRIVATE の終点アドレスを一对一で変換する。
- エンハンスド NAT : 複数の始点 IP アドレスを 1 個の共用アドレス + 個別のポート番号に変換する。
- リバース NAT : PUBLIC PRIVATE のパケットの始点アドレスを変換する。また、PRIVATE PUBLIC のパケットの終点アドレスを変換する。
- ダブル NAT : 始点、終点の両方を変換する。

ルール NAT は原則として一方向にのみ作用します。すなわち、PUBLIC インターフェースに設定した NAT ルールは、PUBLIC PRIVATE のパケットとその戻りパケットにのみ作用します。また、PRIVATE インターフェースに設定した NAT ルールは、PRIVATE PUBLIC のパケットとその戻りパケットにのみ作用します。

- ※ ルールのアクションに NAT、NONAT を指定することは、ALLOW 同様パケットを許可することになるので注意してください。

以下、各タイプの NAT 設定について例を挙げながら解説します。

### スタンダード NAT

スタンダード NAT (NATTYPE=STANDARD) は、IP アドレスを一对一で静的に変換します。インターフェース NAT における「スタティック NAT」「スタティック ENAT」に相当します。

PRIVATE 側のホストが PUBLIC 側にあるように見せかけたい場合、PUBLIC インターフェースに次のようなスタンダード NAT ルールを適用します。

- PROTOCOL は ALL
- アドレス変換は GBLIP (グローバル) IP (プライベート)

PRIVATE 側のホスト 192.168.10.100 を、PUBLIC 側では 1.1.1.100 のように見せかけたい場合は、PUBLIC 側インターフェースに次のようなスタンダード NAT ルールを適用します。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=STANDARD INT=ppp0 PROT=ALL
    GBLIP=1.1.1.100 IP=192.168.10.100 ↵
```

同じ構成で、ホスト 192.168.10.100 の Telnet サービスだけを外部に公開するには次のようにします。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=STANDARD INT=ppp0 PROT=TCP
    GBLIP=1.1.1.100 GBLPO=23 IP=192.168.10.100 PO=23 ↵
```

- ※ NAT 用の IP アドレスとして、実インターフェースに割り当てられていない IP アドレスを指定した場合、本製品は NAT 用 IP アドレスへの ARP Request に自動的に応答します。

ルール NAT は原則一方向です。したがって、ルールをどのインターフェースに適用するかによって設定や動作が異なります。

- PUBLIC インターフェースにルールを適用した場合は、外 内のパケットの終点アドレスが GBLIP と一致する場合に、終点アドレスが IP に書き換えられます。

- PRIVATE インターフェースにルールを適用した場合は、内 外のパケットの始点アドレスが IP と一致する場合に、始点アドレスが GBLIP に書き換えられます。

上記の設定例は、PUBLIC 側から通信が開始されることを前提とし、外 内のパケットとその戻りについてのみ上記ルールを適用します。PRIVATE 側のホストが単独で通信を開始した場合は上記ルールは適用されません。

完全に双方向の変換を行いときは、PRIVATE インターフェースにも NAT ルールを追加してください。

```
ADD FIREWALL POLICY=net RULE=2 AC=NAT NATTYPE=STANDARD INT=vlan1 PROT=ALL
IP=192.168.10.100 GBLIP=1.1.1.100 ↵
```

サブネット単位でスタンダード NAT の変換を行うには、NATMASK パラメーターでネットマスクを指定します。「サブネット単位で NAT を行う」とは、IP アドレスのサブネット部だけを変換し、ホスト部はそのままにすることを示します。

192.168.10.17 ~ 192.168.10.30 ( 192.168.10.16/28 ) と 1.1.1.17 ~ 1.1.1.30 ( 1.1.1.16/28 ) を一対一で変換するには、次のようにします。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=STANDARD INT=vlan1 PROT=ALL
IP=192.168.10.16 GBLIP=1.1.1.16 NATMASK=255.255.255.240 ↵
```

## エンハンスド NAT

エンハンスド NAT ( NATTYPE=ENHANCED ) は、指定したインターフェースで受信したパケットの始点 IP アドレスを別の 1 個の IP アドレスに変換する NAT です。送信元の識別は、変換後に異なる始点ポート番号を使うことによって実現します。

vlan1 で受信したパケットの始点アドレスを 1.1.1.10 に書き換えるには次のようにします。始点ポート番号はセッションごとに自動的に割り当てられます。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=ENHANCED INT=vlan1 PROT=ALL
GBLIP=1.1.1.10 ↵
```

ppp0 で受信したパケット ( 外 内 ) の始点アドレスを 192.168.10.200 に書き換えます。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=ENHANCED INT=ppp0 PROT=ALL
REMOTEIP=192.168.10.200 ↵
```

IPsec パススルー IPsec パススルー機能とは、NAT 機器配下にある IPsec 端末が、NAT 機器の先にある IPsec 端末と IPsec 通信ができるようにするための機能です。

通常、エンハンスド NAT では、送信元アドレスに加えて、送信元ポート番号の変換も行いますが、IPsec 通信で使用する ESP パケットにはポート番号の概念がないため、NAT 機器配下に複数の IPsec 端末が接続されている場合、最初に接続してきた IPsec 端末だけが接続できません。

しかし、エンハンスド NAT を使用する際に、PROTOCOL パラメーターで ESP を指定することによって、NAT 機器配下の複数の IPsec 端末が NAT 機器の先にある IPsec 端末と IPsec 通信ができます。

基本動作

1. Private インターフェースで ESP パケットを受信時に送信元 IP アドレス、宛先 IP アドレス、SPI を "Initiate セッション" として作成します。

```
4ddd ESP    IP: 192.168.1.100:3761720968    Rem IP: 192.168.2.100:3761720968
          Gbl IP: 150.100.100.100:0          Gbl Rem IP: 192.168.2.100:0
ESP state ..... initialised
Start time ..... 17:15:46 26-Jan-2010
Seconds to deletion ..... 54
```

2. Public インターフェースで受信した ESP パケットの送信元アドレスと保持している Initiate セッションの宛先アドレスを比較しマッチするセッションが存在する場合、そのセッションを "Establish セッション" として記録されている送信元アドレスにパケットを転送し、その SPI を記録します。

```
4ddd ESP    IP: 192.168.1.100:3761720968    Rem IP: 192.168.2.100:3761720968
          Gbl IP: 150.100.100.100:576906178 Gbl Rem IP: 192.168.2.100:576906178
ESP state ..... established
Start time ..... 17:15:46 26-Jan-2010
Seconds to deletion ..... 1176
```

㇏ マッチする Initiate セッションが複数存在する場合、もっとも古いセッションを選択します。(区別できないセッションが存在すると以下の様な Firewall Notify Event が発生します。)

```
Policy : ips_pass - Notify Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-----
  8 15:03:54 IN  ESP          1 150.100.100.100:576906178 0.0.0.0:0
                                ambiguous match session detected
-----
```

㇏ マッチする Initiate セッションが存在しない場合 (Public 側から通信が開始された場合)、ESP パケットは破棄されます。

### IPsec との併用

本機能と IPsec との併用は可能です。

### NAT-Traversal との併用

本機能と NAT-Traversal との併用は可能です。また、Private 側に NAT-Traversal を使用する端末と IPsec パススルーを使用する端末が混在した環境でも動作可能です。

Private 側にある IPsec 端末からの IPsec 通信をパススルーするには次のようにします。

```
ADD FIREWALL POLICY=IPS_PASS RULE=1 ACTION=NAT INTERFACE=vlan1
    PROTOCOL=ESP NATTYPE=ENHANCED ↵
```

動的にグローバル IP アドレスが割り当てられる構成で本機能を使用する場合、IPsec パススルー向けのエンハンスド NAT ルールに加え、インターフェースエンハンスド NAT を設定する必要があります。

```
ADD FIREWALL POLICY=IPS_PASS NAT=ENHANCED INTERFACE=vlan1
    GBLINTERFACE=ppp0 ↵
```

### ESP ファイアウォールセッションの管理方法について

ルーターは ESP パケットの送信元/宛先 IP アドレスをもとに組み合わせを推測しています。よって、登録した SPI の上り/下りのペアが必ず正しいという保障ができません。これは、2 点間の IPsec 通信では外向きと内向きの 2 つの SA が確立し、互いに独立して存在しているため、IPsec 終端機器以外がペアとなる SPI を知ることができないためです。

このため、以下のような場合はただしく動作しない場合があります。

- 同一宛先の Initiate セッションが複数存在する場合  
一度、間違った組み合わせで ESP セッションが "Establish" となった場合、該当するファイアウォールセッションが削除されるまで誤った宛先に ESP パケットを転送します。

### セッション保持時間について

NAT 対象となっている SA の Lifetime と ESP のファイアウォールセッション保持時間は同期していません。そのため、これらの時間の組み合わせにより以下のような事象が発生します。

1. SA の Lifetime が ESP ファイアウォールセッション保持時間よりも短い場合、SA の Rekey 後に新しい SPI で通信を開始されると新しいファイアウォールセッションが生成されますが、不要になった古いファイアウォールセッションもタイムアウトするまで保持されたままになります。SA の Rekey が頻繁に行われる環境では余分なセッションが数多く存在する場合があります。
2. SA の Lifetime が ESP ファイアウォールセッション保持時間よりも長い場合、SA が存在していても無通信状態が Session Timer 以上続くと ESP のファイアウォールセッションは削除されます。このとき、Private 側からの ESP パケットを受信しない限り Public 側からの ESP パケットは破棄し続けます。

※ ESP のファイアウォールセッション保持時間は、SET FIREWALL POLICY コマンド (107 ページ) の ESPTIMEOUT パラメーターで変更可能です。

### 未サポートプロトコルについて

IPsec プロトコル "AH" はサポートしません。

## リバース NAT

リバース NAT (NATTYPE=REVERSE) は終点アドレスを書き換えます。一般的に認知されている NAT ではなく、パケットを特定のホストにリダイレクトする機能です。

vlan1 で受信したパケットの終点が 1.1.1.126 の場合、これを 1.1.1.10 に強制的に書き換えます。

```
ADD FIREWALL POLICY=net RULE=1 AC=NAT NATTYPE=REVERSE INT=vlan1
REMOTEIP=1.1.1.126 GBLREMOTEIP=1.1.1.10 PROT=ALL ↵
```

## ダブル NAT

ダブル NAT (NATTYPE=DOUBLE) は始点・終点の両方を書き換えます。

始点 192.168.10.100 を 1.1.1.100 に書き換え、終点を 1.1.1.10 に書き換えます。

```
ADD FIRE POLI=net RU=1 AC=NAT NATT=DOUBLE INT=vlan1 IP=192.168.10.100
    GBLIP=1.1.1.100 PROT=ALL GBLREM=1.1.1.10 ↵
```

### ルール NAT のまとめ

ルール NAT の変換パターンについてまとめます。

次表の「プライベート側」「グローバル側」欄に書かれているのは、IP パケットの始点・終点アドレスです。「A B」と書いた場合、「A」が始点、「B」が終点アドレスを示します。また、「IP」「GBLIP」「REMOTEIP」「GBLREMOTEIP」は、ADD FIREWALL POLICY RULE コマンド (63 ページ) のパラメーターです。スクエアブラケット ([ ]) で囲まれているパラメーターは省略が可能を示しています。

たとえば、PRIVATE インターフェースに適用したスタンダード NAT ルールでは、同インターフェースで受信したパケットの始点アドレスが「IP」で終点アドレスが「REMOTEIP」なら、始点アドレスを「GBLIP」に書き換えます。

NAT 種別	向き (I/F 種別)	プライベート側	グローバル側	備考
スタンダード	内 外 (PRIVATE)	IP [RE- MOTEIP]	GBLIP [REMOTEIP]	始点アドレスを IP から GBLIP に 変換
	内 外 (PUBLIC)	IP [RE- MOTEIP]	GBLIP [REMOTEIP]	終点アドレスを GBLIP から IP に 変換
エンハンスド	内 外 (PRIVATE)	[IP] [RE- MOTEIP]	GBLIP [REMOTEIP]	始点アドレスを IP から GBLIP に 変換 (ポートも変換)
	内 外 (PUBLIC)	[IP] RE- MOTEIP	[IP] [GBLRE- MOTEIP]	始点アドレスを GBLREMOTEIP から REMOTEIP に変換 (ポート も変換)
リバース	内 外 (PRIVATE)	[IP] [RE- MOTEIP]	[IP] GBLRE- MOTEIP	終点アドレスを REMOTEIP から GBLREMOTEIP に変換
	内 外 (PUBLIC)	[IP] RE- MOTEIP	[IP] [GBLRE- MOTEIP]	始点アドレスを GBLREMOTEIP から REMOTEIP に変換
ダブル	内 外 (PRIVATE)	IP RE- MOTEIP	GBLIP GBLRE- MOTEIP	始点アドレスを IP から GBLIP に、終点アドレスを REMOTEIP から GBLREMOTEIP に変換
	内 外 (PUBLIC)	IP RE- MOTEIP	GBLIP GBLRE- MOTEIP	始点アドレスを GBLREMOTEIP から REMOTEIP に、終点アドレ スを GBLIP から IP に変換

表 9:

### アクセスリストによるルール

ADD FIREWALL POLICY RULE コマンド (63 ページ) でルールを追加するとき、ファイルに記述した一連のアドレスに対してルールを設定することもできます。この機能 (アクセスリスト) は、対象アドレスが多い場合に便利です。ここでは例として、内部ネットワークからアクセスリストに記載したアドレスへのアクセスを禁止するルールを設定します。

1. 最初に、アクセスさせたくないアドレスの一覧を作成します。EDIT コマンド (「運用・管理」の 234 ページ) 等を用いて次のようなテキストファイルを作成してください。ここではファイル名を「denylist.txt」とします。

```
# Access-list "denylist.txt"
# HOST or NETWORK          NICKNAME
10.20.30.40
22.33.44.55                henna-server
123.45.67.0 - 123.45.67.255 henna-network # comment
```

リストファイルには、一行に一個アドレスを書きます。アドレスには次の 2 つの形式があります。

- 単一アドレス (例: 10.20.30.40)
- アドレス範囲 (例: 123.45.67.0 - 123.45.67.255。2 つの IP アドレスをハイフンで区切ったもの (ハイフンの前後にスペースが必要なので注意してください))

また例のように、アドレスの後に簡単な説明を入れることもできます。説明文字列は SHOW FIREWALL POLICY コマンド (125 ページ) でアクセスリストの内容を見るときに表示されます。  
# (シャープ) 以降はコメントです。

2. 次にアクセスリストをポリシーに登録します。これ以降、アクセスリストを参照するときはファイル名でなく LIST パラメーターで指定した名前 (ここでは「denyto」) を使います。

```
ADD FIREWALL POLICY=mynet LIST=denyto FILE=denylist.txt TYPE=IP ↓
```

3. 最後にアクセスリストを用いて拒否ルールを追加します。この例では、LAN 側 (vlan1) からアクセスリスト「denyto」に記載されているアドレスへの IP 通信をすべて拒否しています。

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=DENY INT=vlan1 PROTO=ALL
LIST=denyto ↓
```

アクセスリスト内の IP アドレスは通信の向きによって次のように解釈されます。

- 外向き通信 (PRIVATE PUBLIC) の場合: 終点アドレス。リスト中のアドレスへのアクセスを禁止または許可する。
- 内向き通信 (PUBLIC PRIVATE) の場合: 始点アドレス。リスト中のアドレスからのアクセスを禁止または許可する。

よって、手順 3 のコマンドは、意味的には次のコマンドと同じになります。

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=DENY INT=vlan1 PROTO=ALL
REMOTEIP=10.20.30.40 ↵
ADD FIREWALL POLICY=mynet RULE=2 ACTION=DENY INT=vlan1 PROTO=ALL
REMOTEIP=22.33.44.55 ↵
ADD FIREWALL POLICY=mynet RULE=3 ACTION=DENY INT=vlan1 PROTO=ALL
REMOTEIP=123.45.67.0-123.45.67.255 ↵
```

また、アクセスリストにはMACアドレスを列挙することもできます。この場合、ADD FIREWALL POLICY LIST コマンド (58 ページ) の TYPE パラメーターには ADDRESS と指定してください。リスト中の MAC アドレスは送信元 MAC アドレスとして扱われます。

### RADIUS サーバーを利用したルール

RADIUS 認証サーバーを利用してファイアウォールのアクセス制御を行うこともできます。これは、RADIUS サーバー側で個々の IP アドレスごとに通信の許可・拒否を登録しておくもので、「望ましくない」Web サイトのリストを中央で管理するような場合に便利です。

最初に RADIUS サーバー側の設定を行います。以下は架空の RADIUS サーバーの設定例です。実際の設定方法については、ご使用の RADIUS サーバーのマニュアルをご覧ください。

1. RADIUS サーバーのクライアントリストに本製品を追加します。また、サーバー・クライアント間の通信で使用する共有パスワードも設定します。

ここでは、本製品の IP アドレスを 192.168.10.1、共有パスワードを himitsu とします。

# client	secret
192.168.10.1	himitsu

2. 次に RADIUS サーバーのユーザーデータベースにアクセス制御対象のアドレスと許可・拒否の設定を登録します。

RADIUS を使用するよう設定した場合、本製品は受信したパケットごとに次のような認証リクエスト (Access-Request パケット) を RADIUS サーバーに送ります。

```
User-Name [ipadd], User-Password allowdeny ↵
```

すなわち、ユーザー名として IP アドレスを角かっこ ([]) で囲んだものを、パスワードとして「allowdeny」を送り、認証を要求します。

ipadd には、外向き通信 (PRIVATE PUBLIC) の場合は終点アドレスが、内向き通信 (PUBLIC PRIVATE) の場合は始点アドレスが入ります。

RADIUS サーバーの設定ファイルを編集して、アクセス制御対象の IP アドレスごとに次のような内容のユーザーエントリーを作成してください。実際の設定ファイルの記述方法については、RADIUS サーバーのドキュメントを参照してください。

属性名	属性値
User-Name	[ipadd]

User-Password	allowdeny
Framed-IP-Address	拒否なら 0.0.0.0、許可なら ipadd

表 10:

ここでは、例として次のようなエントリーを登録したものとします。Framed-IP-Address が 0.0.0.0 なので、どちらも拒否エントリーです。

```
[49.49.49.49]      Password = "allowdeny"
                   Framed-IP-Address = 0.0.0.0

[18.18.18.4]      Password = "allowdeny"
                   Framed-IP-Address = 0.0.0.0
```

3. エントリーの追加が完了したら、RADIUS サーバーを再起動してください。
4. 次に、本製品が RADIUS サーバーを使うように設定します。ここでは、RADIUS サーバーの IP アドレスを 192.168.10.5 とします。

```
ADD RADIUS SERVER=192.168.10.5 SECRET=himitsu ㇏
```

5. 次に、ファイアウォールルールを作成して、RADIUS サーバーを使うよう設定します。  
この例では、LAN 側 (vlan1) から外部へ送られる HTTP のトラフィックについて、終点アドレスをユーザー名として RADIUS サーバーに通信の可否を問い合わせます。ACTION に DENY を指定した場合はデフォルト許可のルールとなり、RADIUS データベースに Framed-IP-Address 「0.0.0.0」として登録されているアドレスだけが拒否されます。一方、ACTION に ALLOW を指定した場合はデフォルト拒否のルールとなり、Framed-IP-Address が自分自身のアドレスと一致するものだけが許可されます。

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=DENY INT=vlan1 PROTO=TCP
PORT=80 LIST=RADIUS ㇏
```

㇏ ALLOW が「デフォルト拒否」で、DENY が「デフォルト許可」というのは逆のようにも思えますが、ALLOW は「RADIUS サーバー上で許可するよう登録されているものだけ」を許可、DENY は「RADIUS サーバー上で拒否するよう登録されているものだけ」を拒否、という意味合いになります。

RADIUS サーバーからの応答は次のように解釈されます。

- ACTION が ALLOW (デフォルト拒否) なら、RADIUS サーバーが Access-Reject を返すか、IP アドレス 0.0.0.0 を返してきた場合は、フローを拒否します。
- ACTION が ALLOW (デフォルト拒否) で、RADIUS サーバーが Access-Accept を返し、なおかつ、有効な IP アドレスを返してきた場合は、フローを許可します。
- ACTION が DENY (デフォルト許可) で、RADIUS サーバーが Access-Reject を返すか、有効な IP アドレスを返してきた場合、フローを許可します。
- ACTION が DENY (デフォルト許可) で、RADIUS サーバーが Access-Accept を返し、なおかつ、IP アドレス 0.0.0.0 を返してきた場合、フローは破棄されます。

## ルールの時間制限

特定の曜日や時間帯だけルールを有効にすることもできます。この機能を利用すれば、平日の営業時間内に限って外部からの Web アクセスを許可するといった設定が可能です。時間制限の設定は、ADD FIREWALL POLICY RULE コマンド (63 ページ) の AFTER、BEFORE、DAYS パラメーターで行います。

次の例では、平日 (月～金) の 9:00～20:00 に限り、外部から内部の Web サーバー (1.2.3.2 へのアクセスを許可します。それ以外の時間帯は、ファイアウォールの基本ルールによりすべてのアクセスが拒否されます。

```
ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=ppp0 PROT=TCP IP=1.2.3.2 PORT=80
DAYS=WEEKDAY AFT=9:00 BEF=20:00 ↵
```

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 1.2.3.2 で終点ポートが 80 のものを、平日 (月～金) の 9:00～20:00 の間に限って通過させる」の意味になります。

ファイアウォールルールでは、TTL パラメーターでルールの有効期間を指定することができます。TTL 指定のルールは、動的なものであり設定ファイルには保存されません。コマンド入力後 TTL で指定した時間が経過すると削除されます。

### 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 (125 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 (112 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 (78 ページ) を使います。

### 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、番号の小さ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。

7. IP アドレスが一致した場合は、時刻をチェックします。現在時刻がルールが有効でない時間帯ならば、該当ルールにはマッチしません。
8. Ethernet または VLAN インターフェースに適用されたルールでハードウェア (MAC アドレス) リストが指定されている場合、新規フローの送信元 MAC アドレスに一致するアドレスがリストに記載されているかどうかをチェックします。一致するアドレスがなかった場合はデフォルトの動作を実行します。
9. ルールで IP リストが指定されている場合、PRIVATE 側からのフローでは終点 IP アドレスが、PUBLIC 側からのフローでは始点 IP アドレスをチェックします。IP リストも RADIUS サーバーも設定されていない場合、ルールのアクションが ALLOW ならば、この時点で新規フローは通過を許可されます。アクションが DENY ならば破棄されます。同様に、IP リストにマッチするアドレスが掲載されていた場合も、アクションが ALLOW なら許可、DENY なら破棄します。
10. IP リストにマッチするアドレスがなく、RADIUS サーバーも設定されていない場合は、アクションが ALLOW なら新規フローは破棄されます。アクションが DENY ならば、PRIVATE 側から開始されたフローは許可され、それ以外の場合はデフォルトの動作を実行します。
11. IP リストにマッチするアドレスがなく、RADIUS サーバーが設定されている場合、新規フローの終点 IP アドレス (PRIVATE 側からのフロー) あるいは始点 IP アドレス (PUBLIC 側からのフロー) について、RADIUS サーバーに問い合わせを行います。RADIUS サーバーの応答は、次のように解釈します。
  - アクションが ALLOW (デフォルト拒否) なら、RADIUS サーバーが Access-Reject を返すか、IP アドレス 0.0.0.0 を返してきた場合は、フローを拒否します。
  - アクションが ALLOW (デフォルト拒否) で、RADIUS サーバーが Access-Accept を返し、なおかつ、有効な IP アドレスを返してきた場合は、フローを許可します。
  - アクションが DENY (デフォルト許可) で、RADIUS サーバーが Access-Reject を返すか、有効な IP アドレスを返してきた場合、フローを許可します。
  - アクションが DENY (デフォルト許可) で、RADIUS サーバーが Access-Accept を返し、なおかつ、IP アドレス 0.0.0.0 を返してきた場合、フローは破棄されます。

## 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。本製品のログ機能や自動通知機能、トリガー機能などを利用すれば、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

(97 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
INAOOTHER	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、INAOOTHER 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
OUTAOOTHER	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、OUTAOOTHER 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 11: 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 380 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 ↓
```

## イベント通知

重大なイベント (攻撃開始など) を自動的に通知するよう設定するには、ENABLE FIREWALL NOTIFY コマンド (96 ページ) を使います。イベントの通知先としては、次のものがあります。

- MANAGER : Manager 権限でログインしているすべての端末画面にメッセージを出力
- SNMP : あらかじめ設定しておいたトラップホストに SNMP トラップを送信
- MAIL : あらかじめ指定しておいたメールアドレスにメールを送信
- PORT : 非同期ポートにメッセージを出力

各通知先は個別にオン・オフできます。デフォルトでは、通知イベント発生時に Manager レベルでログインしているコンソールにメッセージが表示されるようになっています。

イベント発生時に管理者にメールを送るには次のようにします。

1. メール送信のための設定を行います。詳細は「運用・管理」の「メール送信」をご覧ください。

```
SET MAIL HOSTNAME=gw.example.com ↓
```

```
ADD IP DNS PRIMARY=192.168.10.5 ↓
```

2. メールアドレスを指定し、メールによる通知を有効にします。

```
ENABLE FIREWALL NOTIFY=MAIL TO=admin@is.example.com ↓
```

Syn アタックを受けたときに送られてきたメールの例

```
Subject: Firewall message
From: manager@gw.example.com
To: <admin@is.example.com>
Date: Sun, 22 Jul 2001 13:33:19 +0900

22-Jul-2001 13:33:19
  SYN attack from 1xx.43.12.xxx is underway
```

- ✧ メール通知を有効にするには、あらかじめメール送信のための基本設定 (自ホスト名、DNS サーバーの設定) が必要です。詳細は「運用・管理」の「メール送信」をご覧ください。

イベント発生時に SNMP トラップを上げるには次のようにします。ここでは、トラップ送信先として、SNMP マネージャー 192.168.10.5 を設定します。

1. SNMP の設定を行います。詳細は「運用・管理」の「SNMP」をご覧ください。

```
ENABLE SNMP ↓
```

```
CREATE SNMP COMMUNITY=public MANAGER=192.168.10.5 TRAPHOST=192.168.10.5 ↓
```

```
ENABLE SNMP COMMUNITY=public TRAP ↓
```

2. SNMP トラップによるイベント通知を有効にします。

```
ENABLE FIREWALL NOTIFY=SNMP ↓
```

ポートスキャンを受けたときに送られてきたトラップの例

```
172.16.10.1: Enterprise Specific Trap (1) Uptime: 2:19:50
enterprises.207.8.4.4.4.77.1.0 = OCTET STRING: "22-Jul-2001 14:15:47..
Port scan from 12.xx.xx.xx is underway"
```

＼ SNMP トラップによる通知を有効にするには、あらかじめ SNMP の基本設定（SNMP モジュールの有効化、コミュニティの作成、マネージャー/トラップホストの指定、トラップの有効化）が必要です。詳細は「運用・管理」の「SNMP」をご覧ください。

現在有効になっている通知先を確認するには、SHOW FIREWALL コマンド（115 ページ）を実行します。「Enabled Notify Options」に有効な通知先が表示されます。

イベント通知をオフにするには DISABLE FIREWALL NOTIFY コマンド（85 ページ）を使います。

```
DISABLE FIREWALL NOTIFY=MAIL ↓
```

ファイアウォールイベントの履歴を見るには、SHOW FIREWALL EVENT コマンド（122 ページ）を使います。

```
SHOW FIREWALL EVENT ↓
```

大きく分けて、イベントには次の 3 種類があります。上記コマンドを実行すると、すべてのイベントが表示されます。

- 通知（Notify）イベント：攻撃の開始や終了。攻撃の種類については別表を参照
- 拒否（Deny）イベント：ファイアウォールで拒否されたパケット
- 許可（Allow）イベント：ファイアウォールの通過を許可されたパケット

特定イベントの履歴だけを見るには次のようにします。

```
SHOW FIREWALL EVENT=NOTIFY ↓
```

通知イベントには次のような攻撃が含まれます。

攻撃名称	説明
DoS Flood	不要なトラフィックで帯域を占有し、ネットワークサービスを妨害する

Fragment Attack	巨大なフラグメントや再構成できないフラグメントを送りつける
Host Scan	内部ネットワークで稼働中のホストを調べる
IP Spoofing	送信元 IP アドレスを詐称する
Land Attack	始点と終点に同じアドレスを設定した IP パケットによる DOS 攻撃。システムのバグを狙う
Ping of Death	システムのバグをつくもので、特定サイズの Ping パケットを送りつけることによりシステムをクラッシュさせる
Port Scan	ホスト上で稼働中のサービスを調べる
SMTP Third-party Relay	メールの不正中継。宛先とは関係のないドメインのメールサーバーを利用してメールを送信する。spam メールを送信者が送信元を隠すために使用することが多い
Smurf Attack	始点アドレスを詐称（標的のアドレスを設定する）した Ping パケットを中継サイトのディレクティッドブロードキャストアドレスに送り、中継サイトから標的サイトに大量のリプライを送りつけさせる
Spam	spam メール。不要なメールを送りつける。何を spam と見なすかは受信者次第。本製品では、spam リストで指定されたドメイン、メールアドレスからのメールを spam メールと見なす
Syn Attack	TCP の Syn パケットを断続的に送りつけ、ハーフオープンのコネクションを大量に生成し（始点アドレスを詐称するため Syn/Ack への応答はない）、標的システムのコネクションキューを枯渇させる
Tiny Fragment Attack	微小なフラグメントを用いて TCP フラグを 2 個目のフラグメントに入れ、Syn パケットのフィルタリングをくぐりぬけようとする
UDP Port Scan	UDP によるポートスキャン

表 12: 攻撃一覧

## トリガー

ファイアウォールトリガーを使えば、各種攻撃の開始時・終了時にスクリプトを実行させることができます。ファイアウォールトリガーは、CREATE TRIGGER FIREWALL コマンド（「運用・管理」の 168 ページ）で作成します。

次の例では、ポートスキャンの開始を検出したときに管理者にメールを送るよう設定します。メールはサブジェクトのみとし、ファイアウォールトリガーの引数を利用してサブジェクトに攻撃者の IP アドレスとポリシー名が入るようにします。

```
ENABLE TRIGGER ↓
```

```
CREATE TRIGGER=1 FIREWALL=PORTSCAN MODE=START SCRIPT=pscans.scp ↓
```

### スクリプト「pscans.scp」の内容

```
MAIL TO=admin@is.example.com SUBJECT="Portscan from %2 started (Policy %1)"
```

上記トリガーによって送られてきたメールの例

```
Subject: Portscan from 1xx.xx.3x.180 started (Policy mynet)
From: manager@gw.example.com
To: <admin@is.example.com>
Date: Sun, 22 Jul 2001 14:37:21 +0900
```

- ✧ メール機能を使用するためには、あらかじめメール送信のための基本設定（自ホスト名、DNS サーバーの設定）が必要です。詳細は「運用・管理」の「メール送信」をご覧ください。

攻撃検出のしきい値は SET FIREWALL POLICY ATTACK コマンド（108 ページ）で変更できます。

攻撃検出のしきい値は SHOW FIREWALL POLICY ATTACK コマンド（134 ページ）で確認できます。

## アカウンティング

アカウンティング機能を利用すれば、ポリシーごとにトラフィックの記録を取ることができます。

アカウンティングは ENABLE FIREWALL POLICY コマンド（97 ページ）の ACCOUNTING オプションで有効にします。

```
ENABLE FIREWALL POLICY=mynet ACCOUNTING ↓
```

アカウンティング情報を見るには、SHOW FIREWALL ACCOUNTING コマンド（118 ページ）を使います。

```
Manager > show firewall accounting

Policy : mynet
Date/Time   Event   Dir Prot  IP:Port <-> Dest IP:Port /Traffic statistics
-----
22 14:42:17 END      OUT UDP   172.16.28.160:2060 172.16.28.1:53
                Traffic out 1:66 in 1:118
22 14:42:17 END      OUT TCP   172.16.28.160:36399 172.16.48.16:25
                Traffic out 13:846 in 12:967
22 14:44:33 START    OUT UDP   192.168.10.5:65406 172.16.28.1:53
22 14:44:33 END      OUT ICMP  192.168.10.5 172.16.28.1
                Traffic out 1:84 in 1:84
22 14:44:34 END      OUT ICMP  192.168.10.5 172.16.28.1
                Traffic out 1:84 in 1:84
22 14:44:35 END      OUT ICMP  192.168.10.5 172.16.28.1
                Traffic out 1:84 in 1:84
22 14:44:36 END      OUT ICMP  192.168.10.5 172.16.28.1
                Traffic out 1:84 in 1:84
22 14:47:16 START    OUT TCP   192.168.10.50:1031 172.16.28.5:80
22 14:47:17 START    OUT TCP   192.168.10.50:1032 172.16.28.5:80
22 14:47:44 END      IN  ICMP   172.16.28.180 172.16.28.160
                Traffic out 1:28 in 1:28
-----
```

アカウンティング情報はログにも記録されます。ログレベルは 3 です。アカウンティング情報だけを見るには次のようにします。

SHOW LOG TYPE=ACCO ↵

```
Manager > show log type=acco
```

Date/Time	S	Mod	Type	SType	Message
-----					
22 14:42:18	3	FIRE	ACCO	END	UDP 172.16.28.160:2060 172.16.28.1:53 Flow terminated
22 14:42:18	3	FIRE	ACCO	END	Flow traffic out 1:66 in 1:118
22 14:42:18	3	FIRE	ACCO	END	TCP 172.16.28.160:36399 172.16.48.16:25 Flow terminated
22 14:42:18	3	FIRE	ACCO	END	Flow traffic out 13:846 in 12:967
22 14:44:33	3	FIRE	ACCO	START	UDP 192.168.10.5:65406 172.16.28.1:53 Flow started
22 14:44:33	3	FIRE	ACCO	END	ICMP 192.168.10.5 172.16.28.1 Flow terminated
22 14:44:33	3	FIRE	ACCO	END	Flow traffic out 1:84 in 1:84
22 14:44:34	3	FIRE	ACCO	END	ICMP 192.168.10.5 172.16.28.1 Flow terminated
22 14:44:34	3	FIRE	ACCO	END	Flow traffic out 1:84 in 1:84
22 14:44:35	3	FIRE	ACCO	END	ICMP 192.168.10.5 172.16.28.1 Flow terminated
22 14:44:35	3	FIRE	ACCO	END	Flow traffic out 1:84 in 1:84
22 14:44:36	3	FIRE	ACCO	END	ICMP 192.168.10.5 172.16.28.1 Flow terminated
22 14:44:36	3	FIRE	ACCO	END	Flow traffic out 1:84 in 1:84
22 14:47:15	3	FIRE	ACCO	START	TCP 192.168.10.50:1031 172.16.28.5:80 Flow started
22 14:47:16	3	FIRE	ACCO	START	TCP 192.168.10.50:1032 172.16.28.5:80 Flow started
22 14:47:44	3	FIRE	ACCO	END	ICMP 172.16.28.180 172.16.28.160 Flow terminated
22 14:47:44	3	FIRE	ACCO	END	Flow traffic out 1:28 in 1:28
22 14:49:35	3	FIRE	ACCO	END	UDP 192.168.10.5:65406 172.16.28.1:53 Flow terminated
22 14:49:35	3	FIRE	ACCO	END	Flow traffic out 1:70 in 1:190
-----					

## 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 (97 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。

- DEBUG パラメーターは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したもので、ご使用に際しては弊社技術担当にご相談ください。

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( 86 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 (125 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。

## 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 (141 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 (141 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 (141 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 ↵
```

## ダイナミックインターフェース

ファイアウォールを使用するためには、ADD FIREWALL POLICY INTERFACE コマンド (54 ページ) で監視対象インターフェースを指定する必要があります。また、ファイアウォールルールを作成するときや、NAT ルールを設定するときにもインターフェース名の指定が必要です。

eth0、ppp0 のように固定的に設定されているインターフェースの場合は、単にインターフェース名を指定するだけで、外部からダイヤルアップを受け付けているような場合、動的に作成されるインターフェース (PPP テンプレートなどによって作成されるインターフェース) をどのようにして指定するかが問題となります。

動的に作成される PPP インターフェースをファイアウォール関連コマンドで使用するときは、「ダイナミックインターフェーステンプレート」という仕組みを使います。この仕組みを使うと、特定ユーザーが接続してきたときに作成される動的インターフェースに任意の名前 (テンプレート名) を付けることができます。たとえば、ユーザー「pon」が接続してきたときに作成される PPP インターフェースに「pon-if」という名前を付けられます。ADD FIREWALL POLICY INTERFACE コマンド (54 ページ) など、ファイアウォールの設定コマンドでインターフェース名を指定するときは、「DYN-」+テンプレート名で指定することができます。

## テンプレートの作成

ファイアウォールで動的な PPP インターフェースを扱うときは、最初に CREATE FIREWALL POLICY

DYNAMIC コマンド (70 ページ) でテンプレートを作成します。テンプレート名は自由です。

```
CREATE FIREWALL POLICY=net DYNAMIC=dialup_if ↵
```

次に、このテンプレートで参照するインターフェースの対象ユーザーを ADD FIREWALL POLICY DYNAMIC コマンド (52 ページ) で追加します。たとえば、ユーザー white がダイヤルアップしてきたときに作成されるインターフェースを、テンプレート「dialup\_if」として参照したい場合は、次のようにします。

```
ADD FIREWALL POLICY=net DYNAMIC=dialup_if USER=white ↵
```

ㄱ 同じユーザー名を複数のテンプレートに割り当てることはできません。

PPP の認証なしで作成されたインターフェースを参照する場合は、USER パラメーターに NONE を指定します。これは、認証を必要としないすべての PPP インターフェースを対象とすることを示します。

```
ADD FIREWALL POLICY=net DYNAMIC=noauth_if USER=NONE ↵
```

PPP の認証を受けたユーザーすべてを対象とする場合は、USER パラメーターに ANY を指定します。

```
ADD FIREWALL POLICY=net DYNAMIC=alluser USER=ANY ↵
```

1 つのテンプレートで複数のユーザーを対象にすることもできます。その場合は、ADD FIREWALL POLICY DYNAMIC コマンド (52 ページ) を複数回実行してください。たとえば、営業部員がダイヤルアップしてきたときに作成されるインターフェースを「sales.if」という名前で総称するとします。営業部には、hayashi、kobayashi、oobayashi という 3 ユーザーがいるとした場合は、次のように設定します。

```
CREATE FIREWALL POLICY=net DYNAMIC=sales_if ↵
```

```
ADD FIREWALL POLICY=net DYNAMIC=sales_if USER=hayashi ↵
```

```
ADD FIREWALL POLICY=net DYNAMIC=sales_if USER=kobayashi ↵
```

```
ADD FIREWALL POLICY=net DYNAMIC=sales_if USER=oobayashi ↵
```

リストファイルを使ってユーザーをまとめて指定することもできます。最初に EDIT コマンド (「運用・管理」の 234 ページ) 等で次のようなテキストファイルを作成してください。1 行に 1 つユーザーを記述します。拡張子は.txt です。

ファイル newusers.txt

```
nakata
nakano
nakao
nakajima
nakamura
nakayama
```

ファイルを作成したら、ADD FIREWALL POLICY DYNAMIC コマンド (52 ページ) の FILE パラメーターでファイル名を指定します。

```
ADD FIREWALL POLICY=net DYNAMIC=sales_if FILE=newusers.txt ↵
```

ファイル (FILE) で指定したユーザーと、USER パラメーターで指定したユーザーは共存できます。

ダイナミックインターフェーステンプレートから対象ユーザーを削除するには、DELETE FIREWALL POLICY DYNAMIC コマンド (73 ページ) を使います。

```
DELETE FIREWALL POLICY=net DYNAMIC=sales_if USER=oobayashi ↵
```

ダイナミックインターフェーステンプレートからユーザーリストを削除するには、DELETE FIREWALL POLICY DYNAMIC コマンド (73 ページ) の FILE パラメーターを使います。

```
DELETE FIREWALL POLICY=net DYNAMIC=sales_if FILE=newusers.txt ↵
```

ダイナミックインターフェーステンプレートは、DESTROY FIREWALL POLICY DYNAMIC コマンド (82 ページ) で削除します。テンプレートにユーザーが設定されている場合でも削除は可能です。

```
DESTROY FIREWALL POLICY=net DYNAMIC=dialup_if ↵
```

## テンプレートの使用

作成したダイナミックインターフェーステンプレートは、ファイアウォール関連コマンドでインターフェース名を指定する箇所ならどこでも使用できます。そのとき、「DYN-」+テンプレート名の形式で指定します。以下、例を示します。

ファイアウォールポリシーに動的インターフェースを追加する。

```
ADD FIREWALL POLICY=net INTERFACE=DYN-dialup_if TYPE=PRIVATE ↵
```

動的インターフェースから Web サーバー宛てのパケットを通さない。

```
ADD FIREWALL POLICY=net RULE=1 AC=DENY INT=DYN-dialup_if PROTO=TCP
PORT=WWW ↵
```

ㄟ ダイナミックインターフェーステンプレートを NAT ルールのグローバルインターフェースとして指定することはできません。

## アプリケーション検出・遮断機能 (Application Detection System : ADS)

ファイル共有ソフトによる P2P 通信は、特定のホストが大量の TCP セッションを使用するため、帯域を占有してしまうことになります。また、ファイル共有ソフトの使用により、意図せず有害なファイルや企業の極秘情報等を拡散させてしまう恐れがあります。

ADS(Application Detection System) 機能は、このような P2P 通信を検知し、必要に応じてブロックすることができる機能です。

ファイアウォールポリシーにおいて WINNY を検出した際、パケットを破棄するように設定するには、

ENABLE FIREWALL POLICY P2PFILTER コマンド (100 ページ) を使います。

ENABLE FIREWALL POLICY=policy P2PFILTER=WINNY ACTION=DENY

ファイアウォールポリシーにおいて WINNY の検出を無効にするには、DISABLE FIREWALL POLICY P2PFILTER コマンド (89 ページ) を使います。

DISABLE FIREWALL POLICY=policy P2PFILTER=WINNY

### サポートする Winny バージョン

本バージョンでは、Winny Ver.2.0b7.1 の検知をサポートしています。

### Winny 関連のログ

Winny 関連のログは 5 種類あり、それぞれの意味は下記のとおりです。

なお、1～3 はログレベル 6 (URGENT) 以下、4～5 はログレベル 0 (DEBUG) で表示が可能です。

1	Winny communication from [source-ipaddr] to [destination-ipaddr] found	ACTION=NOTIFY 指定時、Winny を検知したときに出力されます。 なお、このログが出力されても、該当 TCP セッションは削除されません。
2	Winny communication from [source-ipaddr] to [destination-ipaddr] discarded	ACTION=DENY 指定時、Winny を検知したときに出力されます。 なお、このログが出力された時点で該当 TCP セッションは削除済みとなります。
3	Failed to allocate required memory of Winny han- dler	[firewall-session-id]ADS の処理に必要なメモリーの割り当てに失敗した場合に出力されます。
4	Winny P2P filter handler added [session id]	そのセッションに対する Winny の検疫処理が開始された際に出力されます。
5	Winny P2P filter handler removed [session id]	そのセッションに対する Winny 検疫処理が終了した時点で出力されます。つまり、ACTION=DENY の場合は、Winny 検知後、もしくは THRESHOLD パラメーターで設定した数分の TCP パケット検疫完了後、ACTION=NOTIFY の場合は、THRESHOLD パラメーターで設定した数分の TCP パケットを検疫完了後に出力されます。

表 13: Winny 関連のログ

### 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 を通すには、次のようにします。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場合があります。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には、次のようにします。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 を返すようにするには次のようにします。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 (88 ページ) を実行して ident プロキシ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。

ファイアウォールのデフォルト設定では、PUBLIC・PRIVATE インターフェース間の TCP セッション確立時に TCP Syn パケットの代理応答を行います。一部のアプリケーションではこの動作 (代理応答) によって矛盾が生じることがあります。

その場合は、DISABLE FIREWALL POLICY TCPSETUPPROXY コマンド (90 ページ) で代理応答を無効にしてください。

```
DISABLE FIREWALL POLICY=mynet TCPSETUPPROXY ↵
```

いったん無効にした代理応答を再度イネーブルにするには、ENABLE FIREWALL POLICY TCPSETUP-PROXY コマンド (101 ページ) を使います。

```
ENABLE FIREWALL POLICY=mynet TCPSETUPPROXY ↵
```

## UPnP

本製品は、Universal Plug and Play Architecture Version 1.0 で規定されている Internet Gateway Device (IGD) 1.0 を実装しています。UPnP の設定を行うことにより、Windows Messenger など、UPnP を利用したアプリケーションサービスを使用できるようになります。

ここでは、UPnP の基本的な設定方法について解説します。

- ✧ UPnP を使用するときは、DHCP サーバー機能を有効化し、LAN 側クライアントが DHCP で IP アドレスを取得できるようにしてください。
- ✧ UPnP を使用するときは、ファイアウォールの外側 (PUBLIC 側) インターフェースに「PROTOCOL=ALL」または「PORT=ALL」のルールを設定しないでください。
- ✧ TCP と UDP で同一ポート番号へのポートマッピングの要求が発生した場合、先に要求を受信した方のポートを開放します。
- ✧ UPnP 機能有効時、本製品のユニキャストアドレスを宛先 MAC アドレスに指定された SSDP パケットに応答しません。ENABLE IP MACDISPARITY コマンド (「IP」の 313 ページ) を実行することで、当該の SSDP パケットに応答できるようになります。

## 基本設定

UPnP は、通常のファイアウォールと併用する形で使用します。最初に IP の基本設定までをすませておいてください。

以下、基本的な設定手順を示します。IP の基本設定まではすでにし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=net ↵
```

3. 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。

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

4. Ident プロキシ機能をオフにして、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=net IDENTPROXY ↵
```

5. 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。TYPE パラメーターには、内側を PRIVATE、外側を PUBLIC と指定します。また、UPNPTYPE パラメーターには、内側を LAN、外側を WAN と指定してください。

```
ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE UPNPType=LAN ↵  
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC UPNPType=WAN ↵
```

6. NAT ルールを追加します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↵
```

7. UPnP 機能を有効にします。

```
ENABLE UPNP ↵
```

8. ファイアウォールポリシーに対して UPnP 機能を有効にします。

```
SET FIREWALL POLICY=net UPNP=ENABLED ↵
```

以上で設定は終了です。

- ※ UPnP を使用できるのは、LAN・WAN 一組のインターフェースのみです。たとえば、複数の VLAN を設定していたり、PPPoE マルチセッションを使用しているような場合でも、UPnP を使用できるインターフェースは、LAN 側、WAN 側からそれぞれ 1 つだけとなりますのでご注意ください。

## コマンドリファレンス編

### 機能別コマンド索引

#### 一般コマンド

ADD FIREWALL MONITOR . . . . .	50
DELETE FIREWALL MONITOR . . . . .	71
DISABLE FIREWALL . . . . .	83
DISABLE FIREWALL MONITOR . . . . .	84
ENABLE FIREWALL . . . . .	94
ENABLE FIREWALL MONITOR . . . . .	95
SET FIREWALL MONITOR . . . . .	106
SHOW FIREWALL . . . . .	115
SHOW FIREWALL ACCOUNTING . . . . .	118
SHOW FIREWALL ARP . . . . .	120
SHOW FIREWALL MONITOR . . . . .	124

#### ファイアウォールポリシー

ADD FIREWALL POLICY DYNAMIC . . . . .	52
ADD FIREWALL POLICY INTERFACE . . . . .	54
ADD FIREWALL POLICY UDPPORTTIMEOUT . . . . .	67
CREATE FIREWALL POLICY . . . . .	69
CREATE FIREWALL POLICY DYNAMIC . . . . .	70
DELETE FIREWALL POLICY DYNAMIC . . . . .	73
DELETE FIREWALL POLICY INTERFACE . . . . .	74
DELETE FIREWALL POLICY UDPPORTTIMEOUT . . . . .	79
DESTROY FIREWALL POLICY . . . . .	81
DESTROY FIREWALL POLICY DYNAMIC . . . . .	82
DISABLE FIREWALL POLICY . . . . .	86
DISABLE FIREWALL POLICY P2PFILTER . . . . .	89
DISABLE FIREWALL POLICY TCPSETUPPROXY . . . . .	90
ENABLE FIREWALL POLICY . . . . .	97
ENABLE FIREWALL POLICY P2PFILTER . . . . .	100
ENABLE FIREWALL POLICY TCPSETUPPROXY . . . . .	101
SET FIREWALL MAXFRAGMENTS . . . . .	105
SET FIREWALL POLICY . . . . .	107
SET FIREWALL POLICY UDPPORTTIMEOUT . . . . .	114
SHOW FIREWALL POLICY . . . . .	125
SHOW FIREWALL POLICY P2PFILTER . . . . .	138
SHOW FIREWALL POLICY UDPPORTTIMEOUT . . . . .	139

#### フィルタールール

ADD FIREWALL POLICY APPRULE . . . . .	51
ADD FIREWALL POLICY LIMITRULE . . . . .	56
ADD FIREWALL POLICY RULE . . . . .	63
DELETE FIREWALL POLICY APPRULE . . . . .	72
DELETE FIREWALL POLICY LIMITRULE . . . . .	75
DELETE FIREWALL POLICY RULE . . . . .	78
SET FIREWALL POLICY LIMITRULE . . . . .	111
SET FIREWALL POLICY RULE . . . . .	112
SHOW FIREWALL POLICY LIMITRULE . . . . .	136
<b>ファイアウォール NAT</b>	
ADD FIREWALL POLICY NAT . . . . .	60
DELETE FIREWALL POLICY NAT . . . . .	77
<b>イベント管理</b>	
DISABLE FIREWALL NOTIFY . . . . .	85
ENABLE FIREWALL NOTIFY . . . . .	96
SET FIREWALL POLICY ATTACK . . . . .	108
SHOW FIREWALL EVENT . . . . .	122
SHOW FIREWALL POLICY ATTACK . . . . .	134
<b>アクセスリスト</b>	
ADD FIREWALL POLICY LIST . . . . .	58
DELETE FIREWALL POLICY LIST . . . . .	76
<b>ident プロキシ</b>	
DISABLE FIREWALL POLICY IDENTPROXY . . . . .	88
ENABLE FIREWALL POLICY IDENTPROXY . . . . .	99
<b>ファイアウォールセッション</b>	
DELETE FIREWALL SESSION . . . . .	80
SHOW FIREWALL SESSION . . . . .	141
<b>UPnP</b>	
DISABLE UPNP . . . . .	91
DISABLE UPNP ACTION . . . . .	92
DISABLE UPNP L4PORT . . . . .	93
ENABLE UPNP . . . . .	102
ENABLE UPNP ACTION . . . . .	103
ENABLE UPNP L4PORT . . . . .	104
SHOW UPNP . . . . .	144
SHOW UPNP COUNTER . . . . .	146
SHOW UPNP INTERFACE . . . . .	149

## ADD FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

**ADD FIREWALL MONITOR=monitor-id IP=ipadd COPYTO=ip-interface**

[APPLYTO={PRIVATE|PUBLIC|BOTH}]

*monitor-id*: モニター ID (1～65535)

*ipadd*: IP アドレス

*ip-interface*: IP インターフェース名 (eth0、ppp0 など)

### 解説

ファイアウォールセッションモニタリングの対象アドレスを追加する。

本機能を利用すると、ファイアウォールを通過するパケットをコピーしてキャプチャー端末で受信することができる。本機能は Firewall を通過したパケットをコピーして COPYTO に指定したインターフェースからブロードキャストパケット (FF:FF:FF:FF:FF:FF 宛) として送信する。そのため、copyto に設定されるインターフェースが Switch インターフェースの場合、VLAN を分ける必要がある。なお、ファイアウォールで破棄されたパケットはモニターの対象外。

### パラメーター

**MONITOR** モニター ID (設定の識別子)

**IP** モニター対象の IP アドレス

**COPYTO** モニターしたパケットを出力するインターフェース

**APPLYTO** モニターを設置する場所 (PRIVATE/PUBLIC/BOTH) を指定する。

### 備考・注意事項

モニター数に上限はないが、スループットに影響が発生する。(すべてのセッションをモニターした場合、スループットは半分程度。) また、モニターパケットの重複を回避するため、モニター内容が部分的に重複している場合、あとからの設定が有効になる。

### 関連コマンド

DELETE FIREWALL MONITOR (71 ページ)

DISABLE FIREWALL MONITOR (84 ページ)

ENABLE FIREWALL MONITOR (95 ページ)

SET FIREWALL MONITOR (106 ページ)

SHOW FIREWALL MONITOR (124 ページ)

## 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

**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 (0~65535)

### 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 (72 ページ)

SHOW FIREWALL POLICY (125 ページ)

## ADD FIREWALL POLICY DYNAMIC

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

```
ADD FIREWALL POLICY=policy DYNAMIC=template {FILE=filename|
  USER={username|ANY|NONE}}
```

*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)

*template*: ダイナミックインターフェーステンプレート名 (1～15 文字。空白を含む場合はダブルクォートで囲む)

*filename*: ファイル名 (拡張子は.txt)

*username*: ユーザー名 (1～63 文字)

### 解説

ダイナミックインターフェーステンプレートに対象ユーザーを追加する。

ダイナミックインターフェーステンプレートは、ユーザーがダイヤルアップ接続してきたときに動的に作成される PPP インターフェースをファイアウォールポリシーに追加するためのもの。本コマンドで指定したユーザーが接続してきたときに作成されたインターフェースは、ADD FIREWALL POLICY INTERFACE コマンドでは「DYN-」+テンプレート名で識別される。

同じユーザーを複数のテンプレートに追加することはできない。

### パラメーター

**POLICY** ファイアウォールポリシー名

**DYNAMIC** ダイナミックインターフェーステンプレート名 (CREATE FIREWALL POLICY DYNAMIC コマンドで作成)

**FILE** ユーザーリストファイル。各行に1ユーザーずつ記述したもの。拡張子は.txt。このファイルに記載されたユーザーが接続してきた場合、動的に作成されたインターフェースは「DYN-」+テンプレート名で識別される。

**USER** ダイナミックインターフェースのユーザー名。NONE は認証を必要としないインターフェース。ANY は認証済みのすべてのユーザー。このユーザーが接続してきた場合、動的に作成されたインターフェースは「DYN-」+テンプレート名で識別される。

### 例

PPP ユーザー「pon」のログインによって動的に作成された PPP インターフェースを、ファイアウォールポリシー「net」内では「ponif」の名前で識別できるようにする。

```
CREATE FIREWALL POLICY=net DYNAMIC=ponif
```

```
ADD FIREWALL POLICY=net DYNAMIC=ponif USER=pon
```

### 備考・注意事項

ファイアウォールポリシーからダイナミックインターフェースとして認識されるためには、PPP レベルでユーザー認証を行わなくてはならない。具体的には、PPP テンプレートで AUTHENTICATION パラメーターに EITHER、CHAP、PAP のいずれかを指定すること。

### 関連コマンド

DELETE FIREWALL POLICY DYNAMIC ( 73 ページ )

SHOW FIREWALL POLICY ( 125 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

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

*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 PUBLIC へのパケットはすべて通すが、PUBLIC から PRIVATE へ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 側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。グローバル側インターフェースを METHOD=PASSALL に設定することで、許可ルールの設定を省くことができる。なお PASSALL はスタティック NAT (1 対 1 の NAT) を使用する際にのみ利用可能。

**UPNPTYPE** UPnP 機能を使用する場合、このインターフェースが LAN 側か WAN 側かを指定する。UPnP を使用できるのは、LAN・WAN 一組のインターフェースだけであることに注意。

### 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 vlan1 を、外部側

(PUBLIC) インターフェイスとして ppp0 を追加する。

```
ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
```

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

### 関連コマンド

CREATE FIREWALL POLICY ( 69 ページ )

CREATE FIREWALL POLICY DYNAMIC ( 70 ページ )

DELETE FIREWALL POLICY INTERFACE ( 74 ページ )

ENABLE UPNP ( 102 ページ )

SET FIREWALL POLICY ( 107 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## ADD FIREWALL POLICY LIMITRULE

カテゴリー：ファイアウォール / フィルタールール

**ADD FIREWALL POLICY=*policy* LIMITRULE=*rule-id* SRCIPLIMIT=0..10000**

**[INTERFACE=*interface*] [GBLREMOTEIP=*ipadd*[-*ipadd*]] [IP=*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)

*rule-id*: ルール番号 (1～4294967295)

*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リミットルール (ファイアウォールセッション数の制限) を追加する。ルーターはファイアウォールセッションを作成する際、すべてのリミットルールをチェックし、もし、対象となる通信を行う端末のセッション数が超過する場合、新たなセッションを作成しない。

### パラメーター

**POLICY** リミットルールを設定するファイアウォールポリシー名。

**LIMITRULE** リミットルールの ID。1-4294967295 が設定可能。

**SRCIPLIMIT** ソースアドレスごとのセッションの上限値。

**INTERFACE** リミットルールを適用するインターフェース。本パラメーターを指定しない場合はすべてのインターフェースに適用される。なお、設定されるインターフェースは Firewall Policy に所属している必要がある。指定したインターフェースに所属するすべての端末に対してそれぞれリミットルールが適用される。

**IP** リミットルールの対象となる Private 側の IP アドレス。レンジ指定も可能。デフォルトはすべての IP(Any)

**GBLREMOTEIP** リミットルールの対象となる Public 側の IP アドレス。レンジ指定も可能。デフォルトはすべての IP(Any)

### 例

192.168.1.100-192.168.1.150 から 192.168.2.100 宛てのファイアウォールセッション数を 3 に制限する。

```
ADD FIREWALL POLICY=policy-name LIMITRULE=1 SRCLIMIT=3
```

```
GBLREMOTEIP=192.168.2.100
```

```
IP=192.168.1.100-192.168.1.150
```

### 備考・注意事項

すでに対象セッションが存在する状態でリミットルールを追加しても上限値を超える既存のセッションは削除されないが、新たなセッションは作成されなくなる。

セッションの上限値はソースアドレスごとにカウントされる。対象アドレスを複数設定した場合、それぞれのソース IP アドレスごとに上限値までのセッションが作成される。

Interface を指定した場合、パケットを受信した Interface でリミットルールが適用される。

リミットルール が複数設定され、1 つ以上のリミットルールにマッチするパケットを受信した場合、それらの内の一番低い上限値の Rule が適用される。

ファイアウォールポリシーごとに最大 100 ルールが設定可能。

### 関連コマンド

DELETE FIREWALL POLICY LIMITRULE ( 75 ページ )

SET FIREWALL POLICY LIMITRULE ( 111 ページ )

SHOW FIREWALL POLICY LIMITRULE ( 136 ページ )

## ADD FIREWALL POLICY LIST

カテゴリー：ファイアウォール / アクセスリスト

**ADD FIREWALL POLICY=*policy* LIST=*list-name* FILE=*filename* TYPE={IP|ADDRESS}**

*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)

*list-name*: アクセスリスト名 (1~15 文字。英数字とアンダースコアを使用可能)

*filename*: ファイル名 (拡張子は.txt)

### 解説

ファイアウォールポリシーにアクセスリスト (IP または MAC アドレスの一覧が記述されたテキストファイル) を登録する。

登録したアクセスリストは、ADD FIREWALL POLICY RULE コマンドでルールを追加するときに使用できる。アクセスリストは一行一レコードのテキストファイル。

### パラメーター

**POLICY** ファイアウォールポリシー名

**LIST** アクセスリスト名。この名前は、他のコマンドでアクセスリストを指定するときに使用する。

**FILE** アクセスリストのファイル名。拡張子は.txt。

**TYPE** アクセスリストの種類を示す。IP は IP アドレスリスト、ADDRESS は MAC アドレスリストを示す。

### 例

ポリシー「hq」に IP アドレスリスト「floor1」を登録する。リストファイルは「floor1ac.txt」。

```
ADD FIREWALL POLICY=hq LIST=floor1 TYPE=IP FILE=floor1ac.txt
```

#### IP アドレスリストのサンプル

172.16.10.3 # 単一ホストの IP アドレス

172.30.64.5 www.joge.xxx # IP アドレス、空白 (タブまたはスペース)、ホスト名

172.16.12.0 - 172.16.12.255 foo.bar.xxx network # IP アドレス - IP アドレス  
ネットワーク名 (オプション)

#### MAC アドレスリストのサンプル

00-00-f4-42-01-6b # 単一ホストの MAC アドレス

00-50-56-d9-23-68 vm.birds.net # 単一ホストの MAC アドレス、空白、ホスト名

### 関連コマンド

CREATE FIREWALL POLICY ( 69 ページ )

DELETE FIREWALL POLICY LIST ( 76 ページ )

SHOW FIREWALL POLICY ( 125 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

```
ADD FIREWALL POLICY=policy NAT={ENHANCED|STANDARD|ENAPT}
    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。

本製品の NAT 機能には、IP モジュール内蔵の IP NAT と、ファイアウォールモジュール内蔵のファイアウォール NAT があるが、両者は同時使用できない。ファイアウォールを使用するときはファイアウォール NAT を、そうでないときは IP NAT を使う。

また、ファイアウォール NAT には、インターフェース単位で設定するインターフェース NAT と、アドレス単位で指定するルール NAT がある。ルール NAT のほうが詳細な設定が可能だが、通常の用途ではインターフェース NAT で充分。よほど特殊な設定をしたいとき以外はインターフェース NAT をお勧めする。また、両者は併用可能だが、設定の見通しが悪くなるのでどちらか一方だけにしたいほうが望ましい。インターフェース NAT は本コマンドで、ルール NAT は ADD FIREWALL POLICY RULE コマンドで設定する。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り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。ENAPT は Port Restricted Cone NAT 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

vlan1 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=vlan1 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=vlan1 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=vlan1 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、本例のように許可ルールを設定しないと外部から通信を開始できないので注意が必要（あるいは、インターフェースをポリシーに追加するときに METHOD=PASSALL を指定してもよい）。また、GBLINT が Ethernet の場合は ARP やルーティングなどの要素がからんでくるため、他にもマルチホーミングやポリシーフィルターの設定が必要になる。詳細は解説編を参照のこと。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan1 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
```

不特定の LAN 側端末のプライベートアドレスを 1.1.1.11～1.1.1.13 の未使用アドレスに変換するダイナミック NAT の設定。eth0 側において 1.1.1.11～1.1.1.13 への ARP に代理応答するため、プロキシー ARP の設定が必要な点に注意。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan1 GBLINT=eth0
    GBLIP=1.1.1.11-1.1.1.13
ADD IP ROUTE=1.1.1.11 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0
ADD IP ROUTE=1.1.1.12 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0
ADD IP ROUTE=1.1.1.13 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0
```

## 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）。

Port Restricted Cone NAT（ENAPT）使用時、CREATE CONFIG コマンドを実行した場合は、ADD FIREWALL POLICY NAT 行の最後に「GBLIP=WAN 側 IP アドレス」が追加される。WAN 側 IP アドレスが固定 IP アドレスでない場合は、この状態で再起動するとエラーが発生するので、CREATE CONFIG コマンドを実行した後に、EDIT コマンドで「GBLIP=WAN 側 IP アドレス」を削除すること。

## 関連コマンド

CREATE FIREWALL POLICY（69 ページ）  
 DELETE FIREWALL POLICY NAT（77 ページ）  
 SHOW FIREWALL POLICY（125 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

```
ADD FIREWALL POLICY=policy RULE=rule-id ACTION={ALLOW|DENY|NAT|NONAT}
INTERFACE=interface PROTOCOL={protocol|ALL|GRE|OSPF|SA|TCP|UDP|ICMP|ESP}
[IP=ipadd[-ipadd]] [PORT={ALL|port[-port]|port-name}] [GBLIP=ipadd]
[GBLPORT={ALL|port[-port]|port-name}] [REMOTEIP=ipadd[-ipadd]]
[SOURCEPORT={ALL|port[-port]|port-name}] [GBLREMOTEIP=ipadd[-ipadd]]
[LIST={list-name|RADIUS}] [NATTYPE={DOUBLE|ENHANCED|REVERSE|STANDARD}]
[NATMASK=ipadd] [ENCAPSULATION={NONE|IPSEC}] [AFTER=time] [BEFORE=time]
[DAYS=day-list] [TTL=hour:minute]
```

*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 (1~1000)

*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 アドレスまたはネットマスク

*port*: TCP/UDP ポート番号 (0~65535)

*port-name*: サービス名

*list-name*: アクセスリスト名 (1~15 文字。英数字とアンダースコアを使用可能)

*time*: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

*day-list*: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

*hour*: 時間

*minute*: 時間 (分)

### 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、曜日や時刻等にもとづき、PRIVATE・PUBLIC インターフェース間のトラフィック制御 (許可・拒否・NAT 適用) 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。

ファイアウォールの NAT 機能のうち、ルール NAT の設定は本コマンドで行うことができる。ルール NAT とインターフェース NAT を併用している場合は、ルール NAT が優先的に適用される。ただし、見通しが悪くなるので、通常はどちらか一方だけを使うほうがよい。また、ルール NAT は設定が複雑なので、一般的な用途ではインターフェース NAT を使うことをお勧めする。

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。既存ルールと同じ番号を指定した場合は、既存ルールの位置に新規ルールが挿入され、既存ルール以降は番号が1つずつ後ろにずれる。

**ACTION** アクション。ALLOW（通過）、DENY（破棄）、NONAT（NATをかけない）、NAT（ルールNATを適用）から選択する。NATを指定した場合は、NATTYPEパラメーターでNATの種類を指定する。ルールNATは、ADD FIREWALL POLICY NATコマンドで設定したインターフェースNATよりも優先的に適用される。NONAT、NATを指定した場合は、何らかの形でパケットの通過を許可することになるので注意。

**INTERFACE** ルールを適用するIPインターフェース名。ファイアウォールポリシーの管理対象でないインターフェース（ポリシーに追加されていないもの）は指定できない。本パラメーターに（インターフェースNATの）スタティックNATのグローバル側インターフェース（GBLINTERFACE）を指定した場合は、GBLIPパラメーターの指定も必須

**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

**IP** ローカル側IPアドレス。PUBLICインターフェースのルールでは終点アドレス、PRIVATEインターフェースのルールでは始点アドレスを指定する。ハイフン区切りで範囲指定も可能。PUBLICインターフェースにルールを設定する場合、同インターフェースがNATのグローバル側インターフェースであるなら、GBLIPパラメーターでグローバル側終点アドレスを指定し、IPパラメーターでプライベート側終点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。PUBLICインターフェースにルールを設定する場合、同インターフェースがNATのグローバル側インターフェースであるなら、GBLPORTパラメーターでグローバル側の終点ポート番号を指定し、PORTパラメーターでプライベート側の終点ポート番号を指定する。

**GBLIP** NAT使用時のグローバル側終点アドレス。INTERFACEパラメーターにPUBLICインターフェースを指定し、かつ、PUBLICインターフェースがNATのグローバル側インターフェースである場合のみ有効。プライベート側終点アドレスはIPパラメーターで指定する。

**GBLPORT** NAT使用時のグローバル側終点ポート番号またはサービス名。INTERFACEパラメーターにPUBLICインターフェースを指定し、かつ、PUBLICインターフェースがNATのグローバル側インターフェースである場合のみ有効。プライベート側終点ポート番号はPORTパラメーターで指定する。

**REMOTEIP** リモート側IPアドレス。PUBLICインターフェースのルールでは始点アドレス、PRIVATEインターフェースのルールでは終点アドレスを指定する。ハイフン区切りで範囲指定も可能。省略時はすべてのアドレスが対象になる

**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。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になる

**GBLREMOTEIP** リバースNAT、ダブルNAT使用時のリモート側IPアドレス。PUBLICインターフェースのNATルールでは、受信パケットの始点アドレスを指定する。PRIVATEインターフェースのNATルールでは、NAT変換後の終点IPアドレスを指定する。本パラメーターは、ACTIONがNATで、NATTYPEがREVERSEかDOUBLEのときだけ有効。

**LIST** アクセスリスト名を指定する。RADIUSを指定し、なおかつ、RADIUSサーバーが設定されている場合は、RADIUSサーバーを使ってアクセス制御を行う。アクセスリストは、1つのポリシーに4つまで指定可能。IPアドレスリストは、PUBLICからPRIVATEへのフローでは始点アドレスとして、

PRIVATE から PUBLIC へのフローでは終点アドレスとして解釈される。また、MAC アドレスリストは Ethernet インターフェースに関連付けられたルールでのみ有効で、始点 MAC アドレスとして解釈される。

**NATTYPE** NAT の種類。DOUBLE、ENHANCED、REVERSE、STANDARD がある。ACTION パラメーターに NAT を指定したときのみ有効。省略時は STANDARD。

**NATMASK** NAT 時のマスク。ACTION パラメーターに NAT を指定し、NATTYPE パラメーターに DOUBLE、REVERSE、STANDARD のいずれかを指定したときのみ有効。

**ENCAPSULATION** IPSEC を指定した場合、IPsec パケットからオリジナルの IP パケットを取り出したあとでこのルールが適用される。IPsec トンネル終端の IP アドレスが固定されていない場合などを使う。通常は NONE。

**AFTER** 時刻を指定。ルールは同日中の指定した時刻以降にのみ有効。

**BEFORE** 時刻を指定。ルールは同日中の指定した時刻以前にのみ有効。

**DAYS** 曜日を指定。カンマ区切りで複数指定可能。ルールは指定した曜日にのみ有効となる。WEEKDAY は「MON,TUE,WED,THU,FRI」と同義。また、WEEKEND は「SAT,SUN」と同義。省略時は ALL

**TTL** 本ルールの有効期間（時:分）

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
PPTP	1723
VDOLIVE	7000
REALAUDIO	7070
REALVIDEO	7070

表 14: 定義済みのサービス名と TCP/UDP ポート番号

例

LAN ( vlan1 ) 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=vlan1 PROT=UDP PORT=137-139
ADD FIREWALL POLICY=mynet RULE=2 AC=DENY INT=vlan1 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
```

アクセスリスト「myguest」に記述されている IP アドレスからのみ、ppp0 側からのアクセスを許可する

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=ALLOW INT=ppp0 PROTO=ALL
LIST=myguest
```

関連コマンド

CREATE FIREWALL POLICY ( 69 ページ )  
 CREATE FIREWALL POLICY DYNAMIC ( 70 ページ )  
 DELETE FIREWALL POLICY RULE ( 78 ページ )  
 SET FIREWALL POLICY RULE ( 112 ページ )  
 SHOW FIREWALL POLICY ( 125 ページ )

## ADD FIREWALL POLICY UDPPORTTIMEOUT

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

**ADD FIREWALL POLICY=*policy* UDPPORTTIMEOUT=*port* [TIMEOUT={*minutes*|  
DEFAULT}]**

*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*: UDP ポート番号 (1～65535)

*minutes*: 時間 (0～43200 分。0 は 30 秒の意味になる)

### 解説

ファイアウォールポリシーに UDP セッション保持時間の特例エントリーを追加する。

特例エントリーを作成すると、特定のリモート UDP ポートを用いるセッションに対して、通常とは異なるセッション保持時間を適用することができる。

UDP セッション保持時間の決定規則は次のとおり。

(1) 通常、UDP セッションの保持時間は、SET FIREWALL POLICY コマンドの UDPTIMEOUT パラメーターによって決まる (デフォルトは 20 分。ただし、UDP セッションの開始後、外向き・内向きのどちらかのパケット数が 5 個に達したのち、方向に関係なくさらに 1 パケットが転送されるまでは 5 分固定。それ以降になって初めて UDPTIMEOUT の値が使用される点に注意)

(2) ただし、特例エントリーの条件に合致する UDP セッションには、該当エントリーの TIMEOUT パラメーターで指定された保持時間が適用される。また、特例エントリーの保持時間は、該当セッションの最初のパケットから適用される。

(UDP セッションが「特例エントリーの条件に合致する」のは、リモート側 (PUBLIC 側) の UDP ポート番号が、特例エントリーの UDPPORTTIMEOUT パラメーターの値と等しい場合である。リモート側ポート番号とは、PRIVATE PUBLIC のパケットでは終点ポート、PUBLIC PRIVATE のパケットでは始点ポートを意味する)

[例外]

上記 (1) に対する例外として、5060 番ポートを用いる UDP セッションには、セッションの最初のパケットから SET FIREWALL POLICY コマンドの UDPTIMEOUT パラメーターの値が適用される (この例外においては、リモート側ポート・ローカル側ポートのどちらが 5060 番でもよい。もちろん両方とも 5060 番でもよい)

なお、5060 番ポートに対する特例エントリーを作成すると、この例外事項は消滅する。すなわち、リモート側ポートが 5060 番のセッションに対しては特例エントリーの指定が適用されるが、ローカル側ポートのみ 5060 番のセッションに対しては上記 (1) の規則が適用されるようになる。

### パラメーター

**POLICY** ファイアウォールポリシー名

**UDPPORTTIMEOUT** UDP ポート番号。リモート側 (PUBLIC 側) のポート番号を指定する。カンマ区切りで複数指定が可能。

**TIMEOUT** UDP セッションの保持時間(分)。本パラメーターを省略したとき、および、本パラメーターにキーワード DEFAULT を指定したときは、デフォルトの UDP セッション保持時間 (SET FIREWALL POLICY コマンドの UDPTIMEOUT パラメーターで設定した値) が使用される。なお、本コマンドで設定した保持時間は、セッションの最初のパケットから適用される。

### 例

リモート UDP ポート 10000 番の UDP セッションに対して特例エントリーを作成し、該当セッションの 1 パケット目からセッション保持時間「3 分」が適用されるようにする。

```
ADD FIREWALL POLICY=net UDPPORTTIMEOUT=10000 TIMEOUT=3
```

### 関連コマンド

DELETE FIREWALL POLICY UDPPORTTIMEOUT ( 79 ページ )

SET FIREWALL POLICY ( 107 ページ )

SET FIREWALL POLICY UDPPORTTIMEOUT ( 114 ページ )

SHOW FIREWALL POLICY UDPPORTTIMEOUT ( 139 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

**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 ( 54 ページ )

ADD FIREWALL POLICY LIST ( 58 ページ )

ADD FIREWALL POLICY NAT ( 60 ページ )

ADD FIREWALL POLICY RULE ( 63 ページ )

DESTROY FIREWALL POLICY ( 81 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## CREATE FIREWALL POLICY DYNAMIC

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

**CREATE FIREWALL POLICY=*policy* DYNAMIC=*template***

*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)

*template*: ダイナミックインターフェーステンプレート名 (1～15 文字。空白を含む場合はダブルクォートで囲む)

### 解説

ダイナミックインターフェーステンプレートを作成する。

ダイナミックインターフェーステンプレートは、ユーザーがダイヤルアップ接続してきたときに動的作成される PPP インターフェースをファイアウォールポリシーに追加するためのもの。

本コマンドで作成したテンプレートに、ADD FIREWALL POLICY DYNAMIC コマンドで対象ユーザーを追加することにより、指定したユーザーが接続してきたときに作成されたインターフェースを、ADD FIREWALL POLICY INTERFACE コマンドでは「DYN-」+テンプレート名で識別できるようになる。

### パラメーター

**POLICY** ファイアウォールポリシー名

**DYNAMIC** テンプレート名

### 例

PPP ユーザー「joge」が接続してきたときに動的作成される PPP インターフェースを、ファイアウォールポリシー「net」の PRIVATE インターフェースに設定する。

```
CREATE FIREWALL POLICY=net DYNAMIC=pppif
```

```
ADD FIREWALL POLICY=net DYNAMIC=pppif USER=joge
```

```
ADD FIREWALL POLICY=net INTERFACE=dyn-pppif TYPE=PRIVATE
```

### 関連コマンド

ADD FIREWALL POLICY DYNAMIC ( 52 ページ )

DELETE FIREWALL POLICY DYNAMIC ( 73 ページ )

DESTROY FIREWALL POLICY DYNAMIC ( 82 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DELETE FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

**DELETE FIREWALL MONITOR=monitor-id**

*monitor-id*: モニター ID (1 ~ 65535)

### 解説

ファイアウォールセッションモニタリングの対象アドレスを除外する。

### パラメーター

**MONITOR** モニター ID (設定の識別子)

### 関連コマンド

ADD FIREWALL MONITOR ( 50 ページ )  
DISABLE FIREWALL MONITOR ( 84 ページ )  
ENABLE FIREWALL MONITOR ( 95 ページ )  
SET FIREWALL MONITOR ( 106 ページ )  
SHOW FIREWALL MONITOR ( 124 ページ )  
SHOW FIREWALL SESSION ( 141 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

**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 ( 51 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DELETE FIREWALL POLICY DYNAMIC

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

```
DELETE FIREWALL POLICY=policy DYNAMIC=template {FILE=filename|
  USER={username|ALL|NONE}}
```

*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)

*template*: ダイナミックインターフェーステンプレート名 (1～15 文字。空白を含む場合はダブルクォートで囲む)

*filename*: ファイル名 (拡張子は.txt)

*username*: ユーザー名 (1～63 文字)

### 解説

ダイナミックインターフェーステンプレートから対象ユーザーを削除する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**DYNAMIC** ダイナミックインターフェーステンプレート名

**FILE** ユーザーリストファイル。各行に 1 ユーザーずつ記述したもの。拡張子は.txt。

**USER** ユーザー名。NONE は認証を必要としないインターフェース。ANY は認証済みのすべてのユーザー。

### 関連コマンド

ADD FIREWALL POLICY DYNAMIC ( 52 ページ )

DESTROY FIREWALL POLICY DYNAMIC ( 82 ページ )

SHOW FIREWALL POLICY ( 125 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

**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 ( 54 ページ )

CREATE FIREWALL POLICY DYNAMIC ( 70 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DELETE FIREWALL POLICY LIMITRULE

カテゴリー：ファイアウォール / フィルタールール

**DELETE FIREWALL POLICY=*policy* LIMITRULE=*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 ~ 4294967295)

### 解説

ファイアウォールポリシーのリミットルール (ファイアウォールセッション数の制限) を削除する。

### パラメーター

**POLICY** リミットルールを削除するファイアウォールポリシー名。

**LIMITRULE** リミットルールの ID。1-4294967295 が設定可能。

### 関連コマンド

ADD FIREWALL POLICY LIMITRULE ( 56 ページ )

SET FIREWALL POLICY LIMITRULE ( 111 ページ )

SHOW FIREWALL POLICY LIMITRULE ( 136 ページ )

## DELETE FIREWALL POLICY LIST

カテゴリー：ファイアウォール / アクセスリスト

**DELETE FIREWALL POLICY=*policy* LIST=*list-name***

*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)

*list-name*: アクセスリスト名 (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からアクセスリストの登録を解除する。実行すると、アクセスリストを適用しているファイアウォールルールも削除される。

### パラメーター

**POLICY** ファイアウォールポリシー名

**LIST** アクセスリスト名

### 関連コマンド

ADD FIREWALL POLICY LIST ( 58 ページ )

SHOW FIREWALL POLICY ( 125 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

```
DELETE FIREWALL POLICY=policy NAT={ENHANCED|STANDARD|ENAPT}
      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、ENHANCED、ENAPT のいずれか

**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（60 ページ）

CREATE FIREWALL POLICY DYNAMIC（70 ページ）

SHOW FIREWALL POLICY（125 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

**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 ( 63 ページ )

SET FIREWALL POLICY RULE ( 112 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DELETE FIREWALL POLICY UDPPORTTIMEOUT

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

**DELETE FIREWALL POLICY=*policy* UDPPORTTIMEOUT=*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)

*port*: UDP ポート番号 (1～65535)

### 解説

ファイアウォールポリシーから UDP セッション保持時間の特例エントリを削除する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**UDPPORTTIMEOUT** UDP ポート番号。ADD FIREWALL POLICY UDPPORTTIMEOUT コマンドで作成した特例エントリのポート番号を指定すること。カンマ区切りで複数指定が可能。

### 例

(すでに作成済みの) リモート UDP ポート 10000 番の UDP セッションに対する特例エントリを削除する。

```
DELETE FIREWALL POLICY=net UDPPORTTIMEOUT=10000
```

### 関連コマンド

ADD FIREWALL POLICY UDPPORTTIMEOUT ( 67 ページ )

SET FIREWALL POLICY UDPPORTTIMEOUT ( 114 ページ )

SHOW FIREWALL POLICY UDPPORTTIMEOUT ( 139 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

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

*session-id*: 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 ( 141 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

**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 ( 69 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DESTROY FIREWALL POLICY DYNAMIC

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

**DESTROY FIREWALL POLICY=*policy* DYNAMIC=*template***

*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)

*template*: ダイナミックインターフェーステンプレート名 (1～15 文字。空白を含む場合はダブルクォートで囲む)

### 解説

ダイナミックインターフェーステンプレートを削除する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**DYNAMIC** ダイナミックインターフェーステンプレート名

### 関連コマンド

ADD FIREWALL POLICY DYNAMIC ( 52 ページ )

CREATE FIREWALL POLICY DYNAMIC ( 70 ページ )

DELETE FIREWALL POLICY DYNAMIC ( 73 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## DISABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

### **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 NOTIFY ( 85 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL ( 94 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL ( 115 ページ )

## DISABLE FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

### **DISABLE FIREWALL MONITOR**

#### 解説

ファイアウォールセッションモニタリングを無効にする。

本機能を利用すると、ファイアウォールを通過するパケットをコピーしてキャプチャー端末で受信することができる。デフォルトは無効。

#### 関連コマンド

ADD FIREWALL MONITOR ( 50 ページ )

DELETE FIREWALL MONITOR ( 71 ページ )

ENABLE FIREWALL MONITOR ( 95 ページ )

SET FIREWALL MONITOR ( 106 ページ )

SHOW FIREWALL MONITOR ( 124 ページ )

## DISABLE FIREWALL NOTIFY

カテゴリー：ファイアウォール / イベント管理

**DISABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|PORT|SNMP}**

### 解説

指定した宛先へのファイアウォールイベント通知を停止する。

### パラメーター

**NOTIFY** 通知先を指定。ALL を指定すると、イベント通知が行われなくなる。

### 関連コマンド

DISABLE FIREWALL ( 83 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL ( 94 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL ( 115 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

```
DISABLE FIREWALL POLICY=policy [ACCOUNTING] [DEBUG={ALL|HTTP|PACKET|PKT|
PROCESS|PROXY|SMTP}] [FRAGMENT={UDP|ICMP}] [ICMP_FORWARDING={ALL|
PARAMETER|PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|UNREACHABLE}]
[LOG={ALLOW|DENY|DENYDUMP|INAICMP|INALLOW|INAOOTHER|INATCP|INAUDP|
INDDICMP|INDDOOTHER|INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|
INDTCP|INDUDP|OUTAICMP|OUTALLOW|OUTAOOTHER|OUTATCP|OUTAUDP|OUTDDICMP|
OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|OUTDENY|OUTDICMP|OUTDOOTHER|OUTDTCP|
OUTDUDP}] [OPTIONS={ALL|RECORD_ROUTE|SECURITY|SOURCEROUTE|TIMESTAMP}]
[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、アカウンティング機能、イベントログ機能、IP オプションの扱いなどの項目がある。

### パラメーター

**POLICY** ファイアウォールポリシー名

**ACCOUNTING** アカウンティング機能を無効にするときに指定する

**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）、HTTP（HTTP プロキシの動作表示）、SMTP（SMTP セッションコマンドの表示）、PROXY（プロキシの動作表示）、ALL（すべて）から選択する。

**FRAGMENT** 指定したプロトコルのフラグメント化パケットを透過しないよう設定する。デフォルトでは、再構成後の IP データサイズ（L4 パケットサイズ）が 1780 バイトを越えるパケットはファイアウォールで破棄される

**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。

**OPTIONS** IP オプション。指定したオプションを含む IP パケットの処理を停止する（IP オプション付きパケットを破棄するようになる）。カンマ区切りで複数指定が可能。デフォルトでは IP オプション付きパケットはすべて破棄される。

**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=myspolicy ICMP_FORWARDING=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 を有効にしても内部からの PING がとらなくなる。

## 関連コマンド

DISABLE FIREWALL ( 83 ページ )

DISABLE FIREWALL NOTIFY ( 85 ページ )

ENABLE FIREWALL ( 94 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL ( 115 ページ )

SHOW FIREWALL POLICY ( 125 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

**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 プロキシ機能を無効にする。

ident プロキシは、ファイアウォール有効時に、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 (99 ページ)

## DISABLE FIREWALL POLICY P2PFILTER

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

**DISABLE FIREWALL POLICY=*policy* P2PFILTER={WINNY}**

*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において指定した P2P アプリケーションの検知を無効にする。

### パラメーター

**POLICY** ファイアウォールポリシー名

**P2PFILTER** 検知する P2P アプリケーションを指定

### 例

ファイアウォールポリシーにおいて WINNY の検出を無効にする。

DISABLE FIREWALL POLICY=*policy* P2PFILTER=WINNY

### 関連コマンド

ENABLE FIREWALL POLICY P2PFILTER ( 100 ページ )

SHOW FIREWALL POLICY P2PFILTER ( 138 ページ )

## DISABLE FIREWALL POLICY TCPSETUPPROXY

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

**DISABLE FIREWALL POLICY=*policy* TCPSETUPPROXY**

*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

指定したファイアウォールポリシーにおいて、PUBLIC 側からの TCP SYN パケットに対する代理応答を無効にする。デフォルトは有効。

ファイアウォールのデフォルト設定では、PUBLIC・PRIVATE インターフェース間の TCP セッション確立時に TCP SYN パケットの代理応答を行うが、一部のアプリケーションではこの動作（代理応答）によって矛盾が生じることがある。その場合は、本コマンドで代理応答を行わないよう設定できる。

### 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

ENABLE FIREWALL POLICY TCPSETUPPROXY（101 ページ）

SHOW FIREWALL（115 ページ）

SHOW FIREWALL POLICY（125 ページ）

## DISABLE UPNP

カテゴリー：ファイアウォール / UPnP

### **DISABLE UPNP**

#### 解説

UPnP ( Universal Plug and Play ) モジュールを無効にする。デフォルトは無効。

#### 関連コマンド

ENABLE UPNP ( 102 ページ )

## DISABLE UPNP ACTION

カテゴリー：ファイアウォール / UPnP

**DISABLE UPNP FWPOLICY=*policy* INTERFACE=*interface* ACTION=*action-name***

*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

*action-name*: UPnP Action の名前

### 解説

指定したインターフェースで UPnP Action を無効にする。デフォルトは有効。

### パラメーター

**FWPOLICY** ファイアウォールポリシー名

**INTERFACE** IP インターフェース名

**ACTION** UPnP Action の名前。指定できる名前は、SHOW UPNP INTERFACE コマンドで参照できる。

### 関連コマンド

DISABLE UPNP L4PORT ( 93 ページ )

ENABLE UPNP ACTION ( 103 ページ )

ENABLE UPNP L4PORT ( 104 ページ )

SHOW UPNP ( 144 ページ )

SHOW UPNP INTERFACE ( 149 ページ )

## DISABLE UPNP L4PORT

カテゴリー：ファイアウォール / UPnP

**DISABLE UPNP L4PORT={0-65535}**

### 解説

UPnP において、指定した L4 ポートを無効にする。デフォルトではすべてのポートが有効。

### パラメーター

**L4PORT** レイヤー 4 ポート番号

### 関連コマンド

DISABLE UPNP ACTION ( 92 ページ )

ENABLE UPNP ACTION ( 103 ページ )

ENABLE UPNP L4PORT ( 104 ページ )

## ENABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

### **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 ( 83 ページ )

DISABLE FIREWALL NOTIFY ( 85 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL ( 115 ページ )

## ENABLE FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

### **ENABLE FIREWALL MONITOR**

#### 解説

ファイアウォールセッションモニタリングを有効にする。

本機能を利用すると、ファイアウォールを通過するパケットをコピーしてキャプチャー端末で受信することができる。デフォルトは無効。

#### 関連コマンド

ADD FIREWALL MONITOR ( 50 ページ )

DELETE FIREWALL MONITOR ( 71 ページ )

DISABLE FIREWALL MONITOR ( 84 ページ )

SET FIREWALL MONITOR ( 106 ページ )

SHOW FIREWALL MONITOR ( 124 ページ )

## ENABLE FIREWALL NOTIFY

カテゴリー：ファイアウォール / イベント管理

**ENABLE FIREWALL NOTIFY**={**ALL**|**MAIL**|**MANAGER**|**PORT**|**SNMP**}[,...]  
 [PORT=*asyn-number*] [TO=*email-addr*]

*email-addr*: 電子メールアドレス

*asyn-number*: 非同期ポート番号 (0)

### 解説

ファイアウォールイベントの通知先を有効にする。

デフォルトでは Manager 権限でログインしているすべてのユーザーの端末にメッセージを出力する。

### パラメーター

**NOTIFY** イベントの通知先を指定する。カンマ区切りで複数指定が可能。MANAGER は、Manager 権限でログインしているすべてのユーザー端末に通知メッセージを出力する。MAIL (メール通知) を指定した場合は、TO パラメーターでメールアドレスを指定する。また、メール送信機能の設定も必要。PORT (非同期ポートに出力) を指定した場合は、PORT パラメーターで非同期ポートの番号を指定する。同ポートは端末接続に適した設定になっている必要がある。SNMP を指定した場合は、SNMP トラップホストに SNMP トラップが送信される。デフォルトは MANAGER。

**PORT** 通知メッセージの出力先非同期ポート。NOTIFY=PORT のときのみ有効

**TO** 通知メッセージのメール送信先アドレス。NOTIFY=MAIL のときのみ有効

### 関連コマンド

DISABLE FIREWALL (83 ページ)

DISABLE FIREWALL NOTIFY (85 ページ)

DISABLE FIREWALL POLICY (86 ページ)

ENABLE FIREWALL (94 ページ)

ENABLE FIREWALL POLICY (97 ページ)

SHOW FIREWALL (115 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

```
ENABLE FIREWALL POLICY=policy [ACCOUNTING] [DEBUG={ALL|HTTP|PACKET|PKT|
PROCESS|PROXY|SMTP}] [FRAGMENT={UDP|ICMP}] [ICMP_FORWARDING={ALL|
PARAMETER|PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|UNREACHABLE}]
[LOG={ALLOW|DENY|DENYDUMP|INAIcmp|INALLOW|INAOOTHER|INATCP|INAUDP|
INDDICMP|INDDOTHER|INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|
INDTCP|INDUDP|OUTAIcmp|OUTALLOW|OUTAOOTHER|OUTATCP|OUTAUDP|OUTDDICMP|
OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|OUTDENY|OUTDICMP|OUTDOTHER|OUTDTCP|
OUTDUDP}] [OPTIONS={ALL|ROUTER_ALERT|RECORD_ROUTE|SECURITY|SOURCEROUTE|
TIMESTAMP}] [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、アカウントिंग機能、イベントログ機能、IP オプションの扱い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

**ACCOUNTING** アカウンティング機能を有効にするときに指定する。アカウンティング情報はログにも出力される（ログレベルは3（INFO））。

**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）、HTTP（HTTP プロキシの動作表示）、SMTP（SMTP セッションコマンドの表示）、PROXY（プロキシの動作表示）、ALL（すべて）から選択する。

**FRAGMENT** 指定したプロトコルのフラグメント化パケットを透過するよう設定する。デフォルトでは、再構成後の IP データサイズ（L4 パケットサイズ）が 1780 バイトを越えるパケットはファイアウォールで破棄される。

**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。

**OPTIONS** ここで指定した IP オプション付きのパケットを処理するよう設定する。カンマ区切りで複数指定が可能。デフォルトでは IP オプション付きパケットはすべて破棄する。

**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=myspolicy 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=myspollicy LOG=DENY
```

## 関連コマンド

DISABLE FIREWALL ( 83 ページ )

DISABLE FIREWALL NOTIFY ( 85 ページ )

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL ( 94 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

SHOW FIREWALL ( 115 ページ )

SHOW FIREWALL POLICY ( 125 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

**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 プロキシ機能を有効にする。

ident プロキシは、ファイアウォール有効時に、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（88 ページ）

## ENABLE FIREWALL POLICY P2PFILTER

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

**ENABLE FIREWALL POLICY**=*policy* **P2PFILTER**=**{WINNY}** **ACTION**=**{NOTIFY|DENY}**  
 [THRESHOLD=1..255]

*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において指定した P2P アプリケーションの検知を有効にする。

### パラメーター

**POLICY** ファイアウォールポリシー名

**P2PFILTER** 検知する P2P アプリケーションを指定

**ACTION** P2P を検知した際のアクション。NOTIFY または DENY（破棄する）。NOTIFY を指定した場合、検知した旨をファイアウォールイベントとログに出力する

**THRESHOLD** 検疫開始後、何パケット数分監視するかを指定するパラメーター。ADS 機能の検疫は、TCP セッションごとに 3-way handshake 後から開始される。ADS は、ファイアウォールを通過するすべてのパケットが検疫対象となるため、パラメーターで設定したパケット数は、方向には依存せずすべての TCP パケットがカウントの対象となる。デフォルトは 20。また、ACTION=DENY を設定した場合、Winny を検知すると、THRESHOLD パラメーターで設定した数の検知が満了していても監視を終了し、TCP セッションの削除処理に移る。ACTION=NOTIFY を設定した場合は、Winny 検知後も THRESHOLD パラメーターで設定した数が満了するまで監視を続ける。

### 例

ファイアウォールポリシーにおいて WINNY を検出した際、パケットを破棄するように設定する。

```
ENABLE FIREWALL POLICY=policy P2PFILTER=WINNY ACTION=DENY
```

### 関連コマンド

DISABLE FIREWALL POLICY P2PFILTER（89 ページ）

SHOW FIREWALL POLICY P2PFILTER（138 ページ）

## ENABLE FIREWALL POLICY TCPSETUPPROXY

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

**ENABLE FIREWALL POLICY=*policy* TCPSETUPPROXY**

*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

指定したファイアウォールポリシーにおいて、PUBLIC 側からの TCP SYN パケットに対する代理応答を有効にする。デフォルトは有効。

ファイアウォールのデフォルト設定では、PUBLIC・PRIVATE インターフェース間の TCP セッション確立時に TCP SYN パケットの代理応答を行うが、一部のアプリケーションではこの動作（代理応答）によって矛盾が生じることがある。その場合は、DISABLE FIREWALL POLICY TCPSETUPPROXY コマンドで代理応答を行わないよう設定できる。

### 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

DISABLE FIREWALL POLICY TCPSETUPPROXY（90 ページ）

SHOW FIREWALL（115 ページ）

SHOW FIREWALL POLICY（125 ページ）

## ENABLE UPNP

カテゴリー：ファイアウォール / UPnP

### ENABLE UPNP

#### 解説

UPnP ( Universal Plug and Play ) モジュールを有効にする。デフォルトは無効。

UPnP 機能を使用するには、本コマンドでモジュールを有効にするだけでなく、ADD FIREWALL POLICY INTERFACE コマンドの UPNPType パラメーターで UPnP を使用するインターフェースを指定し、SET FIREWALL POLICY コマンドの UPNP パラメーターでポリシーに対しても UPnP を有効化する必要がある。

#### 備考・注意事項

UPnP を使用するときは、DHCP サーバー機能を有効化して、LAN 側クライアントが DHCP で IP アドレスを取得できるようにしておくこと。

#### 関連コマンド

ADD FIREWALL POLICY INTERFACE ( 54 ページ )

DISABLE UPNP ( 91 ページ )

SET FIREWALL POLICY ( 107 ページ )

## ENABLE UPNP ACTION

カテゴリー：ファイアウォール / UPnP

**ENABLE UPNP FWPOLICY=*policy* INTERFACE=*interface* ACTION=*action-name***

*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

*action-name*: UPnP Action の名前

### 解説

指定したインターフェースで UPnP Action を有効にする。デフォルトは有効。

### パラメーター

**FWPOLICY** ファイアウォールポリシー名

**INTERFACE** IP インターフェース名

**ACTION** UPnP Action の名前。指定できる名前は、SHOW UPNP INTERFACE コマンドで参照できる。

### 関連コマンド

DISABLE UPNP ACTION ( 92 ページ )

DISABLE UPNP L4PORT ( 93 ページ )

ENABLE UPNP L4PORT ( 104 ページ )

SHOW UPNP ( 144 ページ )

SHOW UPNP INTERFACE ( 149 ページ )

## ENABLE UPNP L4PORT

カテゴリー：ファイアウォール / UPnP

**ENABLE UPNP L4PORT={0-65535}**

### 解説

UPnPにおいて、指定した L4 ポートを有効にする。DISABLE UPNP L4PORT で無効にした場合のみ使用する。デフォルトではすべてのポートが有効。

### パラメーター

**L4PORT** レイヤー 4 ポート番号

### 関連コマンド

DISABLE UPNP ACTION ( 92 ページ )

DISABLE UPNP L4PORT ( 93 ページ )

ENABLE UPNP ACTION ( 103 ページ )

## SET FIREWALL MAXFRAGMENTS

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

**SET FIREWALL MAXFRAGMENTS=8..50**

### 解説

特定プロトコルのフラグメント化パケットを透過するよう設定している場合( ENABLE FIREWALL POLICY コマンドの FRAGMENT オプションで設定 ) 許可するフラグメントの最大数を設定する。

### パラメーター

**MAXFRAGMENTS** 許可するフラグメントの最大数。フラグメント化パケット透過に設定している場合であっても、本パラメーターの値より多くのフラグメントに分割されているパケットはファイアウォールで破棄される。デフォルトは 20。フラグメント化パケット不透過に設定している場合( デフォルト ) は、再構成後の IP データサイズ ( L4 パケットサイズ ) が 1780 バイトを越えるか、フラグメントの数が 8 個を超えるパケットはファイアウォールで破棄される。

### 関連コマンド

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL ( 115 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## SET FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

```
SET FIREWALL MONITOR=monitor-id [IP=ipadd] [COPYTO=ip-interface]  
[APPLYTO={PRIVATE|PUBLIC|BOTH}]
```

*monitor-id*: モニター ID (1～65535)

*ipadd*: IP アドレス

*ip-interface*: IP インターフェース名 (eth0、ppp0 など)

### 解説

ファイアウォールセッションモニタリングの設定を変更する。

### パラメーター

**MONITOR** モニター ID (設定の識別子)

**IP** モニター対象の IP アドレス

**COPYTO** モニターしたパケットを出力するインターフェース

**APPLYTO** モニターを設置する場所 (PRIVATE/PUBLIC/BOTH) を指定する。

### 備考・注意事項

モニター数に上限はないが、スループットに影響が発生する。(すべてのセッションをモニターした場合、スループットは半分程度。) また、モニターパケットの重複を回避するため、モニター内容が部分的に重複している場合、あとからの設定が有効になる。

### 関連コマンド

ADD FIREWALL MONITOR ( 50 ページ )

DELETE FIREWALL MONITOR ( 71 ページ )

DISABLE FIREWALL MONITOR ( 84 ページ )

ENABLE FIREWALL MONITOR ( 95 ページ )

SHOW FIREWALL MONITOR ( 124 ページ )

## SET 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

```
SET FIREWALL POLICY=policy [FTPDATAPOrt={RFC|ANY}] [TCPTIMEOUT=minutes]
[UDPTIMEOUT=minutes] [OTHERTIMEOUT=minutes] [UPNP={ENABLED|DISABLED}]
[ESPTIMEOUT=minutes]
```

*minutes*: 時間 (0 ~ 43200 分。0 は 30 秒の意味になる)

*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

ファイアウォールセッションの保持時間を変更する。

一定時間通信が行われなかったセッションは、セッションテーブルから削除される。

### パラメーター

**POLICY** ファイアウォールポリシー名

**FTPDATAPOrt** ANY を指定すると、Public 側からの FTP データ用ポートとしてすべてのポートを許可する。RFC を指定すると、20 番以外は拒否する。デフォルトは RFC

**TCPTIMEOUT** TCP セッションの保持時間 (分)。デフォルトは 60 分

**UDPTIMEOUT** UDP セッションの保持時間 (分)。デフォルトは 20 分。本パラメーターの設定は、UDP セッションの開始後、外向き・内向きのどちらかのパケット数が 5 個に達したのち、方向に関係なくさらに 1 パケットが転送された時点から適用される。それまでの間、セッション保持時間は 5 分固定。なお、例外として、5060 番ポートを用いる UDP セッションには、最初のパケットから本パラメーターの値が適用される (この例外においては、リモート側ポート・ローカル側ポートのどちらが 5060 番でもよい。もちろん両方とも 5060 番でもよい)。また、ADD FIREWALL POLICY UDPPORTTIMEOUT コマンドを使用すると、特定のリモートポートを用いる UDP セッションに特例的な保持時間を適用することもできる。

**OTHERTIMEOUT** TCP、UDP 以外のセッションの保持時間 (分)。デフォルトは 20 分

**UPNP** このポリシーで UPnP 機能を使用する場合は ENABLED、使用しない場合は DISABLED を指定する。

**ESPTIMEOUT** ESP セッションの保持時間 (分)。デフォルトは 20 分

### 関連コマンド

ADD FIREWALL POLICY INTERFACE (54 ページ)

ADD FIREWALL POLICY UDPPORTTIMEOUT (67 ページ)

DELETE FIREWALL SESSION (80 ページ)

ENABLE UPNP (102 ページ)

SHOW FIREWALL POLICY (125 ページ)

## SET FIREWALL POLICY ATTACK

カテゴリー：ファイアウォール / イベント管理

```
SET FIREWALL POLICY=policy ATTACK={DOSFLOOD|FRAGMENT|HOSTSCAN|IPSPLOOF|
LAND|PINGOFDEATH|PORTSCAN|SMTPRELAY|SMURF|SMURFAMP|SPAM|SYNATTACK|
TCPTINY|UDPATACK} [INTRIGGER=count] [OUTTRIGGER=count] [DETAIL=count]
[TIME=minutes]
```

*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)

*count*: 個数 (0～4294967295)

*minutes*: 時間 (1～4294967295 分)

### 解説

攻撃検出機能のしきい値を設定する。

攻撃イベントの頻度がしきい値を超えた場合は、通知イベントを発生し、またファイアウォールトリガーを発動する。

しきい値の設定は、頻度を計算するための基準期間 (分) と、期間内のイベント数を指定することによって行う。しきい値は、PUBLIC 側からの攻撃に対するものと、PRIVATE 側からの攻撃に対するものを個別に設定可能。

ファイアウォールは、基準期間ごとに攻撃イベントの記録回数をチェックし、回数がしきい値を上回ると通知イベント「start of attack」(攻撃開始)を発生させる。また、攻撃開始のファイアウォールトリガーを起動する。

攻撃開始後もイベントの頻度がしきい値を上回り続けている場合は、基準期間ごとに通知イベント「attack in progress」(攻撃進行中)を発生させる。

その後、基準期間内のイベント数がしきい値を下回った場合は、通知イベント「end of attack」(攻撃終了)を発生させ、また攻撃終了のファイアウォールトリガーを起動する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**ATTACK** 攻撃の種類。別表を参照

**INTRIGGER** PUBLIC 側からの攻撃に対するしきい値。TIME パラメーターで指定した期間内に INTRIGGER 個を超える PUBLIC 側からの攻撃イベントが記録された場合、通知イベントが発動される。

**OUTTRIGGER** PRIVATE 側からの攻撃に対するしきい値。TIME パラメーターで指定した期間内に OUTTRIGGER 個を超える PRIVATE 側からの攻撃イベントが記録された場合、通知イベントが発動される。

**DETAIL** 通知イベント発生時に保存しておくパケットの数。保存されたパケットの内容は SHOW FIREWALL EVENT コマンドで見ることができる。

**TIME** 攻撃イベントの頻度を計算するための基準期間 (分)

DOSFLOOD	サービス妨害（DOS）攻撃。不要なトラフィックを送りつける
FRAGMENT	フラグメント攻撃。巨大なフラグメントや再構成できないフラグメントを送りつける
HOSTSCAN	ホストスキャン。内部ネットワークで稼働中のホストを調べる
IPSPOOF	IP スプーフィング。始点 IP アドレスを詐称する
LAND	LAND 攻撃。始点と終点に同じアドレスを設定した IP パケットによる DOS 攻撃。システムのバグを狙うもの
PINGOFDEATH	特定サイズの PING パケットを送りつけることによりシステムをクラッシュさせる。システムのバグを狙うもの
PORTSCAN	ポートスキャン。ホスト上で稼働中のサービスを調べる
SMTPRELAY	メールリレー。関係のないドメインのメールサーバーに別ドメイン宛てのメールを中継させようとする
SMURF	Smurf 攻撃。始点アドレスを詐称（標的のアドレスを設定する）した PING パケットを中継サイトのディレクティッドブロードキャストアドレスに送り、中継サイトから標的サイトに大量のリプライを送りつけさせる
SMURFAMP	Smurf Amp 攻撃。TCP Syn による Smurf 攻撃
SPAM	spam メール。不要なメールを送りつける
SYNATTACK	Syn フラッド。始点 IP アドレスを詐称した TCP Syn パケットを断続的に送りつけ、標的システムの TCP コネクションキューを枯渇させる
TCPTINY	Tiny Fragment 攻撃。微小なフラグメントを用いて TCP フラグを 2 個目のフラグメントに入れ、Syn パケットのフィルタリングをくぐりぬけようとする
UDPATACK	UDP によるポートスキャン

表 15: 攻撃一覧

ATTACK	INTRIGGER	OUTTRIGGER	TIME	DETAIL	イベント名
DOSFLOOD	80	160	2	5	DOSATTACK
FRAGMENT	1	1	2	0	FRAGMENT
HOSTSCAN	64	128	2	5	HOSTSCAN
IPSPOOF	1	1	2	0	DOSATTACK
LAND	1	1	2	0	DOSATTACK
OTHER	64	128	2	5	DOSATTACK
PINGOFDEATH	1	1	2	0	DOSATTACK
PORTSCAN	64	128	2	5	PORTSCAN
SMTPRELAY	1	1	2	5	SMTPATTACK
SMURF	1	1	2	0	SMURFATTACK
SMURFAMP	1	1	2	5	SMTPATTACK
SPAM	1	1	2	5	SMTPATTACK
SYNATTACK	32	128	2	5	SYNATTACK
TCPTINY	1	1	2	0	TCPATTACK

UDPATTACK	32	128	2	5	DOSATTACK
-----------	----	-----	---	---	-----------

表 16: 攻撃検出しきい値のデフォルト設定

例

外部からのポートスキャンイベントが 5 分間に 100 個以上発生したら通知するよう設定する。

```
SET FIREWALL POLICY=mypolicy ATTACK=PORTSCAN INTRIGGER=100 TIME=5
```

備考・注意事項

イベントの通知先は ENABLE FIREWALL NOTIFY コマンドで設定する。

関連コマンド

CREATE TRIGGER FIREWALL (「運用・管理」の 168 ページ)

ENABLE FIREWALL NOTIFY (96 ページ)

SHOW FIREWALL POLICY ATTACK (134 ページ)

## SET FIREWALL POLICY LIMITRULE

カテゴリー：ファイアウォール / フィルタールール

```
SET FIREWALL POLICY=policy LIMITRULE=rule-id [SRCIPLIMIT=0..10000]  
[INTERFACE=interface] [GBLREMOTEIP=ipadd[-ipadd]] [IP=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)

*rule-id*: ルール番号 (1～4294967295)

*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のリミットルール (ファイアウォールセッション数の制限) の設定を変更する。

### パラメーター

**POLICY** リミットルールを変更するファイアウォールポリシー名。

**LIMITRULE** リミットルールの ID。1-4294967295 が設定可能。

**SRCIPLIMIT** ソースアドレスごとのセッションの上限値。

**INTERFACE** リミットルールを適用するインターフェース。本パラメータを指定しない場合はすべてのインターフェースに適用される。なお、設定されるインターフェースは Firewall Policy に所属している必要がある。

**IP** リミットルールの対象となる Private 側の IP アドレス。レンジ指定も可能。デフォルトはすべての IP(Any)

**GBLREMOTEIP** リミットルールの対象となる Public 側の IP アドレス。レンジ指定も可能。デフォルトはすべての IP(Any)

### 関連コマンド

ADD FIREWALL POLICY LIMITRULE ( 56 ページ )

DELETE FIREWALL POLICY LIMITRULE ( 75 ページ )

SHOW FIREWALL POLICY LIMITRULE ( 136 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

```
SET FIREWALL POLICY=policy RULE=rule-id [ PROTOCOL={protocol|ALL|GRE|OSPF|
SA|TCP|UDP|ICMP|ESP}] [ IP=ipadd[-ipadd]] [ PORT={ALL|port[-port]|
port-name}] [ GBLIP=ipadd] [ GBLPORT={ALL|port[-port]|port-name}]
[ REMOTEIP=ipadd[-ipadd]] [ SOURCEPORT={ALL|port[-port]|port-name}]
[ GBLREMOTEIP=ipadd[-ipadd]] [ NATMASK=ipadd] [ ENCAPSULATION={NONE|IPSEC}]
[ AFTER=time] [ BEFORE=time] [ DAYS=day-list] [ TTL=hour:minutes]
```

*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 アドレスまたはネットマスク

*port*: TCP/UDP ポート番号 (0～65535)

*port-name*: サービス名

*time*: 時刻 (hh:mm の形式。hh は時 (0～23) mm は分 (0～59))

*day-list*: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

*hour*: 時間

*minutes*: 時間 (分)

### 解説

ファイアウォールルールを設定を変更する。

### 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

**IP** ローカル側 IP アドレス。PUBLIC インターフェースのルールでは終点アドレス、PRIVATE インターフェースのルールでは始点アドレスを指定する。ハイフン区切りで範囲指定も可能。PUBLIC インターフェースにルールを設定する場合、同インターフェースが NAT のグローバル側インターフェースであるなら、GBLIP パラメーターでグローバル側終点アドレスを指定し、IP パラメーターでプライベート側終点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。PUBLIC インターフェースにルールを設定する場合、同インターフェースが NAT のグローバル側インターフェースであるなら、GBLPORT パラメーターでグローバル側の終点ポート番号を指定し、PORT パラメーターでプライベート側の終点ポート番号を指定する。

**GBLIP** NAT 使用時のグローバル側終点アドレス。INTERFACE パラメーターに PUBLIC インターフェースを指定し、かつ、PUBLIC インターフェースが NAT のグローバル側インターフェースである場合

のみ有効。プライベート側終点アドレスは IP パラメーターで指定する。

**GBLPORT** NAT 使用時のグローバル側終点ポート番号またはサービス名。INTERFACE パラメーターに PUBLIC インターフェースを指定し、かつ、PUBLIC インターフェースが NAT のグローバル側インターフェースである場合のみ有効。プライベート側終点ポート番号は PORT パラメーターで指定する。

**REMOTEIP** リモート側 IP アドレス。PUBLIC インターフェースのルールでは始点アドレス、PRIVATE インターフェースのルールでは終点アドレスを指定する。ハイフン区切りで範囲指定も可能。省略時はすべてのアドレスが対象になる

**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。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になる

**GBLREMOTEIP** リバース NAT、ダブル NAT 使用時のリモート側 IP アドレス。PUBLIC インターフェースの NAT ルールでは、受信パケットの始点アドレスを指定する。PRIVATE インターフェースの NAT ルールでは、NAT 変換後の終点 IP アドレスを指定する。本パラメーターは、ACTION が NAT で、NATTYPE が REVERSE か DOUBLE のときだけ有効。

**NATMASK** NAT 時のマスク。ADD FIREWALL POLICY RULE コマンドの ACTION パラメーターに NAT を指定し、NATTYPE パラメーターに DOUBLE、REVERSE、STANDARD のいずれかを指定したときのみ有効。

**ENCAPSULATION** IPSEC を指定した場合、IPsec パケットからオリジナルの IP パケットを取り出したあとでこのルールが適用される。IPsec トンネル終端の IP アドレスが固定されていない場合などに使う。通常は NONE。

**AFTER** 時刻を指定。ルールは同日中の指定した時刻以降にのみ有効。

**BEFORE** 時刻を指定。ルールは同日中の指定した時刻以前にのみ有効。

**DAYS** 曜日を指定。カンマ区切りで複数指定可能。ルールは指定した曜日にのみ有効となる。WEEKDAY は「MON,TUE,WED,THU,FRI」と同義。また、WEEKEND は「SAT,SUN」と同義。省略時は ALL

**TTL** 本ルールの有効期間（時:分）

## 関連コマンド

ADD FIREWALL POLICY RULE ( 63 ページ )

DELETE FIREWALL POLICY RULE ( 78 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## SET FIREWALL POLICY UDPPORTTIMEOUT

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

**SET FIREWALL POLICY=*policy* UDPPORTTIMEOUT=*port* TIMEOUT={*minutes*|DEFAULT}**

*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*: UDP ポート番号 (1～65535)

*minutes*: 時間 (0～43200 分。0 は 30 秒の意味になる)

### 解説

UDP セッション保持時間の特例エントリーを変更する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**UDPPORTTIMEOUT** UDP ポート番号。ADD FIREWALL POLICY UDPPORTTIMEOUT コマンドで作成した特例エントリーのポート番号を指定すること。カンマ区切りで複数指定が可能。

**TIMEOUT** UDP セッションの保持時間 (分)。本パラメーターにキーワード DEFAULT を指定したときは、デフォルトの UDP セッション保持時間 (SET FIREWALL POLICY コマンドの UDPTIMEOUT パラメーターで設定した値) が使用される。なお、本コマンドで設定した保持時間は、セッションの最初のパケットから適用される。

### 例

(すでに作成済みの) リモート UDP ポート 10000 番の UDP セッションに対する特例エントリーを変更し、該当セッションの 1 パケット目からデフォルトのセッション保持時間が適用されるようにする。

```
SET FIREWALL POLICY=net UDPPORTTIMEOUT=10000 TIMEOUT=DEFAULT
```

### 関連コマンド

ADD FIREWALL POLICY UDPPORTTIMEOUT ( 67 ページ )

DELETE FIREWALL POLICY UDPPORTTIMEOUT ( 79 ページ )

SET FIREWALL POLICY ( 107 ページ )

SHOW FIREWALL POLICY UDPPORTTIMEOUT ( 139 ページ )

## SHOW FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

### 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
Enabled Notify Options .... manager
SIP ALG enabled ..... FALSE
SNMP Session Report ..... disabled
Maximum Packet Fragments .. 20
Sessions:
  Maximum ..... 14217
  Peak ..... 0
  Active ..... 0
  Peak ESP..... 0
  Active ESP..... 0

Policy : ips_pass
  TCP Timeout (s) ..... 3600
  UDP Timeout (s) ..... 1200
  ESP Timeout (s) ..... 1200
  Other Timeout (s) ..... 1200
  ICMP Unreachable Timeout (s) ..... 0
  TCP Handshake Timeout Mode ..... Normal
  SMTP Domain ..... not set
  TCP Setup Proxy ..... enabled
  TCP MSS Adjustment ..... disabled
  UPNP ..... disabled
    WAN interfaces ..... none
    LAN interfaces ..... none
    Maximum port maps ..... 250
  SIP ALG ..... disabled
  Number of Limitrules ..... 0
  Private Interface : vlan1
  Public Interface  : ppp0
    Method ..... dynamic
    NAT ..... enhanced

```

```

Method ..... enhanced interface
Private Interface ..... vlan1
Global IP ..... 150.100.100.100

```

Status	ファイアウォール機能の有効 (enabled)・無効 (disabled)
Enabled Notify Options	ファイアウォールイベントの通知先/方法。mail (メールアドレス)、manager (Manager 権限でログインしているユーザーの画面)、port (非同期ポート)、snmp (SNMP トラップ)、all (すべて)、none (なし) がある
Notify Port	イベント通知先の非同期ポート。通知先に port が含まれている場合のみ表示される
Notify Mail To	イベント通知先メールアドレス。通知先に mail が含まれている場合のみ表示される
Sessions	ESP セッション数
Maximum	最大ファイアウォールセッション保持数
Peak	瞬間最大ファイアウォールセッション保持数
Active	アクティブなファイアウォールセッション保持数
Peak ESP	瞬間最大 ESP セッション保持数
Active ESP	アクティブな ESP セッション保持数
Policy	ファイアウォールポリシー名
TCP Timeout (s)	TCP セッションの保持時間
UDP Timeout (s)	UDP セッションの保持時間
ESP Timeout (s)	ESP セッションの保持時間
Other Timeout (s)	TCP/UDP 以外のセッションの保持時間
Spam Source Files	spam リストファイル
SMTP Domain	SMTP プロキシが使用するドメイン名
SMTP Relaying	(SMTP プロキシ) メールリレーを許可するかどうか
TCP Setup Proxy	PUBLIC 側からの TCP SYN パケットに対する代理応答機能 (TCP セットアッププロキシ) の有効・無効
UPnP	UPnP 機能の有効・無効
UPnP/WAN interfaces	UPnP における WAN 側インターフェース
UPnP/LAN interfaces	UPnP における LAN 側インターフェース
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)
Proxy	アプリケーションゲートウェイの対象プロトコル
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 17:

### 関連コマンド

ADD FIREWALL POLICY INTERFACE ( 54 ページ )

CREATE FIREWALL POLICY ( 69 ページ )

DELETE FIREWALL POLICY INTERFACE ( 74 ページ )

DESTROY FIREWALL POLICY ( 81 ページ )

DISABLE FIREWALL ( 83 ページ )

ENABLE FIREWALL ( 94 ページ )

## SHOW FIREWALL ACCOUNTING

カテゴリー：ファイアウォール / 一般コマンド

**SHOW FIREWALL ACCOUNTING** [POLICY=*policy*] [REVERSE=*count*] [TAIL=*count*]

*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)

*count*: 個数 (1~60)

### 解説

ファイアウォールのアカウントリング記録を表示する。

アカウントリングを有効にするには、ENABLE FIREWALL POLICY コマンドの ACCOUNTING オプションを使う。

### パラメーター

**POLICY** ファイアウォールポリシー名

**REVERSE** レコードを逆順 (新しい順) で表示する。数値を指定した場合、指定した数のレコードだけが表示される。

**TAIL** 最新レコードだけを表示する。数値を指定した場合、指定した数のレコードだけが表示される。

### 入力・出力・画面例

```
Manager > show firewall accounting
```

```
Policy : mynet
```

```
Date/Time   Event   Dir Prot  IP:Port <-> Dest IP:Port /Traffic statistics
```

```
-----
22 14:42:17 END      OUT UDP   172.16.28.160:2060 172.16.28.1:53
                        Traffic out 1:66 in 1:118
22 14:42:17 END      OUT TCP   172.16.28.160:36399 172.16.48.16:25
                        Traffic out 13:846 in 12:967
22 14:44:33 START    OUT UDP   192.168.10.5:65406 172.16.28.1:53
22 14:44:33 END      OUT ICMP  192.168.10.5 172.16.28.1
                        Traffic out 1:84 in 1:84
22 14:44:34 END      OUT ICMP  192.168.10.5 172.16.28.1
                        Traffic out 1:84 in 1:84
22 14:44:35 END      OUT ICMP  192.168.10.5 172.16.28.1
                        Traffic out 1:84 in 1:84
22 14:44:36 END      OUT ICMP  192.168.10.5 172.16.28.1
                        Traffic out 1:84 in 1:84
22 14:47:16 START    OUT TCP   192.168.10.50:1031 172.16.28.5:80
22 14:47:17 START    OUT TCP   192.168.10.50:1032 172.16.28.5:80
22 14:47:44 END      IN  ICMP   172.16.28.180 172.16.28.160
```

Traffic out 1:28 in 1:28

Policy	ファイアウォールポリシー名
Date/Time	日時
Event	イベント。START か END
Dir	トラフィックフローの方向。IN か OUT
Prot	プロトコル。ICMP、TCP、UDP あるいは IP プロトコル番号
IP:Port	始点 IP アドレスとポート
Dest IP:Port	終点 IP アドレスとポート
Traffic statistics	該当トラフィックフローのパケット数・オクテット数統計。「方向 パケット数:オクテット数」の形式

表 18:

### 備考・注意事項

アカウンティング情報はログにもレベル 3 (INFO) で記録される。

### 関連コマンド

DISABLE FIREWALL POLICY ( 86 ページ )

ENABLE FIREWALL POLICY ( 97 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## SHOW FIREWALL ARP

カテゴリー：ファイアウォール / 一般コマンド

**SHOW FIREWALL ARP** [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 NAT 用 IP アドレスのうち、本製品が ARP 応答すべきアドレスの一覧を表示する。

### パラメーター

**POLICY** ファイアウォールポリシー名

### 入力・出力・画面例

Manager > show firewall arp					
IP (range)	ARP Interfaces Policy	NAT Type	Int	Gbl Int	Rule
10.10.10.2	Public net	Int based	vlan10	vlan20	-

IP (range)	本製品が ARP 応答すべき NAT 用アドレス
ARP Interfaces	本ポリシーに所属しているインターフェースのうち、該当アドレスへの ARP に応答すべきインターフェース。Public ( Gbl Int 欄に表示されている PUBLIC インターフェース )、All Public ( すべての PUBLIC インターフェース )、Private ( Int 欄に表示されている PRIVATE インターフェース )、All Private ( すべての PRIVATE インターフェース ) のいずれか
NAT Type	NAT の種類。Int Based ( インターフェース NAT )、Rule ( ルール NAT ) のいずれか
Int	NAT 設定における PRIVATE インターフェース。ルール NAT の場合は、NAT ルールを適用したインターフェースを示す。「-」は、NAT ルールが PUBLIC インターフェースに適用されていることを示す
Gbl Int	NAT 設定における PUBLIC インターフェース。ルール NAT の場合は、NAT ルールを適用したインターフェースを示す。「-」は、NAT ルールが PRIVATE インターフェースに適用されていることを示す

Rule	ルール NAT のルール番号
Policy	ファイアウォールポリシー名

表 19:

### 関連コマンド

ADD FIREWALL POLICY NAT ( 60 ページ )

ADD FIREWALL POLICY RULE ( 63 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## SHOW FIREWALL EVENT

カテゴリー：ファイアウォール / イベント管理

**SHOW FIREWALL EVENT** [= {ALLOW|DENY|NOTIFY}] [POLICY=*policy*]  
[REVERSE=*count*] [TAIL=*count*]

*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)

*count*: 個数 (1~60)

### 解説

ファイアウォールイベントの記録を表示する。

### パラメーター

**EVENT** 表示するイベントの種類を指定。ALLOW (許可イベント)、DENY (拒否イベント)、NOTIFY (通知イベント。攻撃など) から選択。無指定時はすべてのイベントを表示する。

**POLICY** ファイアウォールポリシー名

**REVERSE** レコードを逆順 (新しい順) で表示する。数値を指定した場合、指定した数のレコードだけが表示される。

**TAIL** 最新レコードだけを表示する。数値を指定した場合、指定した数のレコードだけが表示される。

### 入力・出力・画面例

```
Manager > show firewall event

Policy : fish - Notify Events:
  No event information currently recorded

Policy : fish - Deny Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-----
 1 08:03:35 IN  TCP        3 194.84.221.83:2891 200.100.10.1:111
                Policy rejected
                4500003c caa44000 2e062fd5 c254dd53 c8640a01 0b4b006f 21b46235
                00000000 a0027d78 94570000 020405b4 0402080a 0a124a3f 00000000 0
1030300
 3 09:25:12 IN  TCP        2 202.84.198.12:2561 200.100.10.1:53
                Policy rejected
                4500003c e7444000 33061d7c ca54c60c c8640a01 0a010035 8340fec2
                00000000 a0027d78 677d0000 020405b4 0402080a 0d0e86ce 00000000 0
1030300
 5 18:01:28 IN  TCP        1 211.251.62.2:1755 200.100.10.1:111
                Policy rejected
```

```

4500003c 125c4000 300673c8 d3fb3e02 c8640a01 06db006f e6277340
00000000 a0027d78 f5990000 020405b4 0402080a 02b7acf3 00000000 0
1030300
-----

Policy : fish - Allow Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-----
5 22:13:59 IN  TCP          1 100.10.248.90:3131 8999 192.168.102.2:80
              TCP session started
5 22:53:22 OUT UDP          1 192.168.102.11:123 27786 80.3.102.102:123
              UDP flow started
-----

```

Policy	ファイアウォールポリシー名
Date/Time	日時
Dir	トラフィックフローの方向。IN か OUT
Prot	プロトコル。ICMP、TCP、UDP あるいは IP プロトコル番号
Number	イベント発生回数
IP:Port	始点 IP アドレスとポート
Dest IP:Port	終点 IP アドレスとポート
Reason	イベント記録の理由
IP Header	イベントを発生させた IP パケットヘッダーの 16 進ダンプ

表 20:

### 関連コマンド

DISABLE FIREWALL NOTIFY ( 85 ページ )

ENABLE FIREWALL NOTIFY ( 96 ページ )

SHOW FIREWALL ACCOUNTING ( 118 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

SHOW FIREWALL SESSION ( 141 ページ )

## SHOW FIREWALL MONITOR

カテゴリー：ファイアウォール / 一般コマンド

### SHOW FIREWALL MONITOR

#### 解説

ファイアウォールセッションモニタリングの情報を表示する。

#### 入力・出力・画面例

```

Manager > show firewall monitor

Firewall Monitoring

Status..... enabled

Monitor IP                Apply to    Copy to    In(pkts)    Out(pkts)
-----
1      192.168.1.1          PRIVATE    VLAN2       0            0
2      192.168.1.2          PRIVATE    VLAN2      24           26
-----

```

Status	ファイアウォールセッションモニタリングの有効 (enabled)・無効 (disabled)
Monitor	モニター ID
IP	モニター対象の IP アドレス
Copy to	モニターしたパケットを出力するインターフェース
Apply to	モニターを設置する場所 (PRIVATE/PUBLIC/BOTH)
In	キャプチャーされた内向きパケット数。再起動時にリセットされる
Out	キャプチャーされた外向きパケット数。再起動時にリセットされる

表 21:

#### 関連コマンド

ADD FIREWALL MONITOR ( 50 ページ )

DELETE FIREWALL MONITOR ( 71 ページ )

DISABLE FIREWALL MONITOR ( 84 ページ )

ENABLE FIREWALL MONITOR ( 95 ページ )

SET FIREWALL MONITOR ( 106 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

**SHOW FIREWALL POLICY=*policy*** [COUNTER] [DYNAMIC] [LIST] [SUMMARY] [USER]

*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。

**DYNAMIC** ダイナミックインターフェーステンプレートの情報を表示する。

**LIST** アクセスリストの情報を表示する。

**SUMMARY** サマリー情報を表示する。

**USER** ダイナミックインターフェースのユーザー情報を表示する。

### 入力・出力・画面例

```
Manager > show firewall policy

Policy : ips_pass
  TCP Timeout (s) ..... 3600
  UDP Timeout (s) ..... 1200
  ESP Timeout (s) ..... 1200
  Other Timeout (s) ..... 1200
  ICMP Unreachable Timeout (s) ..... 0
  TCP Handshake Timeout Mode ..... Normal
  MAC Cache Timeout (m) ..... 1440
  RADIUS Limit ..... 100
  Accounting ..... disabled
  Enabled Logging Options ..... none
  Enabled Debug Options ..... none
  Enabled Debug Modes ..... none
  Enabled Debug IP Address ..... none
  Identification Protocol Proxy ..... enabled
  Enabled IP options ..... none
  Enhanced Fragment Handling ..... none
  Enabled ICMP forwarding ..... none
  Receive of ICMP PINGS ..... enabled
  Number of Notifications ..... 0
  Number of Deny Events ..... 0
```

## SHOW FIREWALL POLICY

```

Number of Allow Events ..... 0
Number of Active TCP Opens ..... 0
Number of Active Sessions ..... 0
Cache Hits ..... 0
Discarded ICMP Packets ..... 0
SMTP Domain ..... not set
FTP Data Port ..... RFC enforced
TCP Setup Proxy ..... enabled
TCP MSS Adjustment ..... disabled
UPNP ..... disabled
  WAN interfaces ..... none
  LAN interfaces ..... none
  Maximum port maps ..... 250
SIP ALG ..... disabled
P2P Filter ..... enabled
Number of Limitrules ..... 0
Private Interface : vlan1
  Trust Private ..... yes
  Rule ..... 1
    Action ..... nat
    NAT type ..... enhanced
    Protocol ..... ESP
    Global IP ..... 150.100.100.100
    Days ..... all
Public Interface : ppp0
  Method ..... dynamic
  NAT ..... enhanced
    Method ..... enhanced interface
    Private Interface ..... vlan1
    Global IP ..... 150.100.100.100

Manager> show firewall policy counter

Policy : ips_pass
  TCP Timeout (s) ..... 3600
  UDP Timeout (s) ..... 1200
  ESP Timeout (s) ..... 1200
  Other Timeout (s) ..... 1200
  ICMP Unreachable Timeout (s) ..... 0
  TCP Handshake Timeout Mode ..... Normal
  MAC Cache Timeout (m) ..... 1440
  RADIUS Limit ..... 100
  Accounting ..... disabled
  Enabled Logging Options ..... none
  Enabled Debug Options ..... none
  Enabled Debug Modes ..... none
  Enabled Debug IP Address ..... none
  Identification Protocol Proxy ..... enabled
  Enabled IP options ..... none
  Enhanced Fragment Handling ..... none
  Enabled ICMP forwarding ..... none

```

```

Receive of ICMP PINGS ..... enabled
Number of Notifications ..... 0
Number of Deny Events ..... 0
Number of Allow Events ..... 0
Number of Active TCP Opens ..... 0
Number of Active Sessions ..... 0
Cache Hits ..... 0
Discarded ICMP Packets ..... 0
SMTP Domain ..... not set
FTP Data Port ..... RFC enforced
TCP Setup Proxy ..... enabled
TCP MSS Adjustment ..... disabled
UPNP ..... disabled
  WAN interfaces ..... none
  LAN interfaces ..... none
  Maximum port maps ..... 250
  Number Port Mappings ..... 0
  Spawned Sessions ..... 0
SIP ALG ..... disabled
Number of Limitrules ..... 0
Private Interface : vlan1
  Total Packets Received ..... 0
  Number Flows Started ..... 0
  Number Cache Hits ..... 0
  Number Dropped Packets ..... 0
  Number Unknown IP Protocols ..... 0
  Number Bad ICMP Packets ..... 0
  Number Dumped ICMP Packets ..... 0
  Number Spoofing Packets ..... 0
  Number Dropped GBLIP is Zero .... 0
  Number No Spare Entries ..... 0
  Number FTP Port Commands ..... 0
  Number Bad FTP Port Commands .... 0
  Number ESP Sessions Initiated ... 0
  Number ESP Sessions Established . 0
  Number ESP Sessions Peak ..... 0
  Number ESP Sessions ..... 0
  Number Ambiguous ESP Sessions ... 0
  Rule ..... 1
    Action ..... nat
    NAT type ..... enhanced
    Protocol ..... ESP
    Global IP ..... 150.100.100.100
    Number Hits ..... 0
    Days ..... all
Public Interface : ppp0
  Method ..... dynamic
  Total Packets Received ..... 0
  Number Flows Started ..... 0
  Number Cache Hits ..... 0
  Number Dropped Packets ..... 0

```

```

Number Unknown IP Protocols ..... 0
Number Bad ICMP Packets ..... 0
Number Dropped ICMP Packets ..... 0
Number Spoofing Packets ..... 0
Number Dropped GBLIP is Zero .... 0
Number No Spare Entries ..... 0
Number FTP Port Commands ..... 0
Number Bad FTP Port Commands .... 0
Number ESP Dropped Packets ..... 0
NAT ..... enhanced
  Method ..... enhanced interface
  Private Interface ..... vlan1
  Global IP ..... 150.100.100.100

```

Policy	ファイアウォールポリシー名
TCP Timeout (s)	TCP セッションのタイムアウト (秒)
UDP Timeout (s)	UDP フローのタイムアウト (秒)
ESP Timeout (s)	ESP セッションのタイムアウト (秒)
Other Timeout (s)	TCP、UDP 以外のフローのタイムアウト (秒)
Accounting	アカウントिंग機能の有効・無効
Enabled Logging Options	ログに記録するイベントの一覧。allow、deny、denydump、in-aicmp、inallow、inaother、inatcp、inaudp、inddicmp、inddothet、inddtcp、inddudp、inddump、inddeny、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 プロキシ機能の有効・無効
Enabled IP options	転送する IP オプションの一覧。all、record_route、security、sourceroute、timestamp、none
Enhanced Fragment Handling	フラグメント化を許可するプロトコル
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 Notifications	イベント通知の発生回数
Number of Deny Events	拒否イベント数
Number of Allow Events	許可イベント数
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

Spam Source Files	spam リストファイル
SMTP Domain	内部 SMTP サーバーのドメイン名
FTP Data Port	Public 側からの FTP データ用ポートとして 20 番以外を許可するかどうか。(SET FIREWALL POLICY コマンドの FTPDATAPOORT の設定。) RFC enforced (拒否) または RFC not enforced (許可)
SMTP Relaying	(SMTP プロキシ) メールリレーを許可するかどうか
TCP Setup Proxy	PUBLIC 側からの TCP SYN パケットに対する代理応答機能 (TCP セットアッププロキシ) の有効・無効
P2P Filter	P2P フィルターの状態。enabled (有効) または disabled (無効)
Proxy	アプリケーションプロキシタイプ
Proxy/IP	PRIVATE (内部) 側アプリケーションサーバーの IP アドレス
Proxy/Direction	アプリケーションプロキシの通信許可方向
Dynamic Template	本ポリシーに関連付けられたダイナミックインターフェーステンプレート名
IP List	本ポリシーに関連付けられた IP アドレスリスト名
Hardware List	本ポリシーに関連付けられた MAC アドレスリスト名
File name	リストファイル名
Number IP hosts	リストに記載されている IP ホスト数
Number Networks	リストに記載されている IP ネットワーク数
Number MAC addresses	リストに記載されている MAC アドレス数
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。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
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)
IP	ローカル側 IP アドレス
Protocol	IP プロトコルタイプ
Port	終点ポート
Global IP	NAT 有効時のグローバル終点アドレス

Global Port	NAT 有効時のグローバル終点ポート
Remote IP	リモート側 IP アドレス
Source Port	始点ポート
Days	ルールが有効な曜日。mon、tue、wed、thu、fri、sat、sun、all のいずれか
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
After	ルールが有効な時間。この時間以降に有効
Before	ルールが有効な時間。この時間以前に有効

表 22:

Policy	ファイアウォールポリシー名
TCP Timeout (s)	TCP セッションのタイムアウト (秒)
UDP Timeout (s)	UDP フローのタイムアウト (秒)
ESP Timeout (s)	ESP セッションのタイムアウト (秒)
Other Timeout (s)	TCP、UDP 以外のフローのタイムアウト (秒)
Accounting	アカウント機能の有効・無効
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、inddeny、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 プロキシ機能の有効・無効
Enabled IP options	転送する IP オプションの一覧。all、record_route、security、sourceroute、timestamp、none
Enhanced Fragment Handling	フラグメント化を許可するプロトコル
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 Notifications	イベント通知の発生回数
Number of Deny Events	拒否イベント数
Number of Allow Events	許可イベント数
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
Spam Source Files	spam リストファイル
SMTP Domain	内部 SMTP サーバーのドメイン名
SMTP Relaying	(SMTP プロキシ) メールリレーを許可するかどうか
TCP Setup Proxy	PUBLIC 側からの TCP SYN パケットに対する代理応答機能 (TCP セットアッププロキシ) の有効・無効
UPNP	UPnP 機能の有効・無効
UPNP/WAN Interface	UPnP における WAN 側インターフェース
UPNP/LAN Interface	UPnP における LAN 側インターフェース
Proxy	アプリケーションプロキシタイプ
Proxy/IP	PRIVATE (内部) 側アプリケーションサーバーの IP アドレス
Proxy/Direction	アプリケーションプロキシの通信許可方向
Dynamic Template	本ポリシーに関連付けられたダイナミックインターフェーステンプレート名
IP List	本ポリシーに関連付けられた IP アドレスリスト名
Hardware List	本ポリシーに関連付けられた MAC アドレスリスト名
File name	リストファイル名
Number IP hosts	リストに記載されている IP ホスト数
Number Networks	リストに記載されている IP ネットワーク数
Number MAC addresses	リストに記載されている MAC アドレス数
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
Number ESP Sessions Initiated	作成中の ESP セッション数
Number ESP Sessions Established	確立した ESP セッション数

Number ESP Sessions Peak	瞬間最大 ESP セッション数
Number ESP Sessions	現在アクティブな ESP セッション数
Number Ambiguous ESP Sessions	区別できない Initiate ESP セッション数
Number ESP Dropped Packets	適合するセッションが無く破棄された ESP パケット数
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。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
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)
IP	ローカル側 IP アドレス
Protocol	IP プロトコルタイプ
Port	終点ポート
Global IP	NAT 有効時のグローバル終点アドレス
Global Port	NAT 有効時のグローバル終点ポート
Remote IP	リモート側 IP アドレス
Source Port	始点ポート
Number Hits	ヒット数
Days	ルールが有効な曜日。mon、tue、wed、thu、fri、sat、sun、all のいずれか
After	ルールが有効な時間。この時間以降に有効
Before	ルールが有効な時間。この時間以前に有効

表 23: COUNTER オプション

Policy	ファイアウォールポリシー名
Dynamic Template	本ポリシーに関連付けられたダイナミックインターフェーステンプレート名
File name/Users	テンプレートに関連付けられたユーザーリストファイル名とユーザー名一覧
Users	テンプレートに関連付けられたユーザー名の一覧

表 24: DYNAMIC オプション

Policy	ファイアウォールポリシー名
--------	---------------

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）
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）
MAC address	MAC アドレスリストに記載された MAC アドレスの一覧
IP	IP アドレスリストに記載された IP アドレス、ネットワークアドレスの一覧
Label	アドレスに関連付けられたホスト名

表 25: LIST オプション

Policy	ファイアウォールポリシー名
Dynamic Template	本ポリシーに関連付けられたダイナミックインターフェーステンプレート名
Users	テンプレートに関連付けられたユーザー名の一覧

表 26: USER オプション

### 関連コマンド

ADD FIREWALL POLICY INTERFACE ( 54 ページ )  
 ADD FIREWALL POLICY LIST ( 58 ページ )  
 ADD FIREWALL POLICY NAT ( 60 ページ )  
 ADD FIREWALL POLICY RULE ( 63 ページ )  
 CREATE FIREWALL POLICY ( 69 ページ )  
 DELETE FIREWALL POLICY INTERFACE ( 74 ページ )  
 DELETE FIREWALL POLICY LIST ( 76 ページ )  
 DELETE FIREWALL POLICY NAT ( 77 ページ )  
 DELETE FIREWALL POLICY RULE ( 78 ページ )  
 DESTROY FIREWALL POLICY ( 81 ページ )  
 DISABLE FIREWALL NOTIFY ( 85 ページ )  
 DISABLE FIREWALL POLICY ( 86 ページ )  
 ENABLE FIREWALL NOTIFY ( 96 ページ )  
 ENABLE FIREWALL POLICY ( 97 ページ )  
 SET FIREWALL POLICY RULE ( 112 ページ )  
 SHOW FIREWALL ( 115 ページ )  
 SHOW FIREWALL EVENT ( 122 ページ )

## SHOW FIREWALL POLICY ATTACK

カテゴリー：ファイアウォール / イベント管理

**SHOW FIREWALL POLICY**[=*policy*] **ATTACK**

*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

攻撃検出機能の設定を表示する。

### パラメーター

**POLICY** ファイアウォールポリシー名

### 入力・出力・画面例

```
Manager > show firewall policy attack
```

Policy : fish  
Current Attack Setup

Attack	In Trigger	Out Tigger	Time Period (mins)	Detailed Logged
dosflood	80	160	2	5
fragment	1	1	2	0
hostscan	64	128	2	5
ipspoof	1	1	2	0
land	1	1	2	0
other	64	128	2	5
pingofdeath	1	1	2	0
portscan	64	128	2	5
smurf	1	1	2	0
synattack	32	128	2	5
tcptiny	1	1	2	0
udpattack	32	128	2	5
smtprelay	1	1	2	5
smurfamp	1	1	2	5
spam	1	1	2	5

Policy	ファイアウォールポリシー名
Attack Logged	ログに記録する攻撃の種類

In Trigger	PUBLIC 側からの攻撃に対するしきい値
Out Trigger	PRIVATE 側からの攻撃に対するしきい値
Time Period (mins)	イベントカウンターの集計期間
Detailed	拒否イベントキューに記録するパケットの数

表 27:

### 関連コマンド

SET FIREWALL POLICY ATTACK ( 108 ページ )

## SHOW FIREWALL POLICY LIMITRULE

カテゴリー：ファイアウォール / フィルタールール

**SHOW FIREWALL POLICY=*policy* LIMITRULE[=*rule-id*[-*rule-id*]]** [DETAIL]

*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 (1～4294967295)

### 解説

ファイアウォールポリシーのリミットルール (ファイアウォールセッション数の制限) についての情報を表示する。

### パラメーター

**POLICY** リミットルールを表示するファイアウォールポリシー名。

**LIMITRULE** リミットルールの ID。1-4294967295 が設定可能。省略すると、指定したファイアウォールポリシーのすべてのリミットルールが表示される。

**DETAIL** 詳細な情報を表示する。

### 入力・出力・画面例

```
Manager > show firewall policy limitrule

Policy=AT_Field
-----
Limitrule 1
-----
Interface ..... vlan2
IP ..... all
GBL Remote IP ..... all
Source IP Limit ..... 12
Limitrule 2
-----
Interface ..... all
IP ..... all
GBL Remote IP ..... all
Source IP Limit ..... 30

Manager > show firewall policy limitrule detail

Policy=Nerv_office
-----
Limitrule 1
-----
```

Interface .....	vlan1
IP .....	202.36.164.113
GBL Remote IP .....	all
Source IP Limit .....	1
-----	
Per Source IP Count	
Source IP Address	Active Sessions
202.36.164.113 .....	1
-----	
Limitrule 2	
-----	
Interface .....	all
IP .....	all
GBL Remote IP .....	all
Source IP Limit .....	12
-----	
Per Source IP Count	
Source IP Address	Active Sessions
101.111.12.13 .....	5
101.111.12.1 .....	12
202.36.164.113 .....	1

Policy	ファイアウォールポリシー名
Limitrule	リミットルールの ID
Interface	リミットルールが適用されているインターフェース
IP	リミットルールの対象となる Private 側の IP アドレス
GBL Remote IP	リミットルールの対象となる Public 側の IP アドレス
Source IP Limit	ソースアドレスごとのセッションの上限値
Per Source IP Count	リミットルールが適用されたセッションのデバイス単位での集計
Source IP Address	セッションを開始したデバイスの IP アドレス
Active Sessions	デバイスによって開始された、現在アクティブなセッションの数

表 28:

### 関連コマンド

ADD FIREWALL POLICY LIMITRULE ( 56 ページ )

DELETE FIREWALL POLICY LIMITRULE ( 75 ページ )

SET FIREWALL POLICY LIMITRULE ( 111 ページ )

## SHOW FIREWALL POLICY P2PFILTER

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

**SHOW FIREWALL POLICY=*policy* P2PFILTER={WINNY}**

*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

P2P フィルターの状態を表示する。

### パラメーター

**POLICY** ファイアウォールポリシー名

**P2PFILTER** 検知する P2P アプリケーションを指定

### 入力・出力・画面例

Policy : test			
Current P2P Filter Setup			
Application	Threshold	Hits	Status
-----	-----	-----	-----
Winny	20	160	notify
-----	-----	-----	-----

Application	P2P アプリケーションの種類
Threshold	ENABLE FIREWALL POLICY P2PFILTER コマンドで設定した THRESHOLD パラメーターの設定数
Hits	検出された P2P パケット数
Status	P2P フィルターの状態

表 29:

### 関連コマンド

DISABLE FIREWALL POLICY P2PFILTER ( 89 ページ )

ENABLE FIREWALL POLICY P2PFILTER ( 100 ページ )

## SHOW FIREWALL POLICY UDPPORTTIMEOUT

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

**SHOW FIREWALL POLICY**[=*policy*] **UDPPORTTIMEOUT**

*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

UDP セッション保持時間の特例エントリ一覧を表示する。

### パラメーター

**POLICY** ファイアウォールポリシー名。省略時はすべてのポリシーが対象となる。

### 入力・出力・画面例

```
Manager > show firewall policy=net udpporttimeout
Policy : net
  Default UDP Timeout (s) : 1200
  Number of Configured UDP Port Timeouts : 3

  UDP Port          Timeout (s)
  -----
    10000            180
    12345            480
    40001            default
  -----
```

Policy	ファイアウォールポリシー名
Default UDP Timeout (s)	該当ポリシーにおけるデフォルトの UDP セッション保持時間（秒）
Number of Configured UDP Port Timeouts	該当ポリシーにおける特例エントリーの数
UDP Port	特例エントリーの対象となるリモート側 UDP ポート番号
Timeout (s)	該当エントリーのセッション保持時間（秒）。default は「Default UDP Timeout (s)」の値を用いることを示す

表 30:

### 関連コマンド

ADD FIREWALL POLICY UDPPORTTIMEOUT ( 67 ページ )

DELETE FIREWALL POLICY UDPPORTTIMEOUT ( 79 ページ )

SET FIREWALL POLICY ( 107 ページ )

SET FIREWALL POLICY UDPPORTTIMEOUT ( 114 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

**SHOW FIREWALL SESSION**[=*session-id*] [POLICY=*policy*] [COUNTER]  
 [PORT={*port*[-*port*]|*port-name*}] [PROTOCOL={*protocol*|ALL|ICMP|GRE|EGP|OSPF|  
 SA|TCP|UDP|ESP}] [SUMMARY]

*session-id*: 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)

*port-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 : ips_pass
```

```
Current Sessions
```

```
-----
2e82 ESP   IP: 192.168.100.254:2749543927 Rem IP: 200.1.1.1:2749543927
      Gbl IP: 150.100.100.100:1441824829 Gbl Rem IP: 200.1.1.1:1441824829
      ESP state ..... established
      Start time ..... 17:23:44 16-Mar-2010
      Seconds to deletion ..... 1194
-----
```

```
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終点 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
ESP state	ESP セッションの状態。Initialised、established 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 31:

関連コマンド

DELETE FIREWALL SESSION ( 80 ページ )

SHOW FIREWALL EVENT ( 122 ページ )

SHOW FIREWALL POLICY ( 125 ページ )

## SHOW UPNP

カテゴリー：ファイアウォール / UPnP

### SHOW UPNP

#### 解説

UPnP（Universal Plug and Play）モジュールの情報を表示する。

#### 入力・出力・画面例

```
Manager > show upnp

UPNP
-----
Status:                               Enabled
Time to next advertisement:           341
Disabled TCP/UDP ports for UPnP:      none
-----

Services and Devices:
Device                               Service                               Interface
-----
InternetGatewayDevice               Layer3Forwarding                     igd-0
  LANDevice                          vlan1-0
  WANDevice                          WANCommonInterfaceConfig            eth0
    WANConnectionDevice              WANIPConnection                     eth0-0
-----
```

Status	UPnP モジュールの有効・無効
Time to next advertisement	次回デバイスとサービスを広報するまでの時間（秒）
Disabled TCP/UDP ports for UPnP	UPnP での利用を無効にした TCP/UDP ポート番号
Device	使用可能な UPnP デバイス
Service	提供中の UPnP サービス
Interface	デバイス/サービスと関連付けられているインターフェース。 「igd-x」は、Internet Gateway Device を表す論理インターフェース

表 32:

#### 関連コマンド

DISABLE UPNP（91 ページ）

ENABLE UPNP ( 102 ページ )

SHOW UPNP COUNTER

カテゴリー：ファイアウォール / UPnP

SHOW UPNP COUNTER

解説

UPnP ( Universal Plug and Play ) モジュールの統計カウンターを表示する。

入力・出力・画面例

```
Manager > show upnp counter

UPnP Counters
-----

UDP
  inDatagrams ..... 0          outDatagrams ..... 0
  inMcastDatagrams ..... 0      outMcastDatagrams ..... 10
  inUcastDatagrams ..... 0      outUcastDatagrams ..... 0
  inDatagramsDropped ..... 0

HTTP
  httpReqs ..... 0             httpResps ..... 0
  httpReqsRefused ..... 0      httpRespsFailed ..... 0

Discovery
  mSearchReqs ..... 0          mSearchResps ..... 0
  mSearchReqsErrors ..... 0    notifyAliveMsgs ..... 10
                                notifyByebyeMsgs ..... 0

Description
  descReqs ..... 0             descResps ..... 0
  deviceDescReqs ..... 0       deviceDescResps ..... 0
  serviceDescReqs ..... 0      serviceDescResps ..... 0
  descErrors ..... 0

Control
  actionReqs ..... 0           actionResps ..... 0
  actionErrors ..... 0

Eventing
  subscrReqs ..... 0           subscrResps ..... 0
  newSubscrReqs ..... 0        eventsNotified ..... 0
  renewSubscrReqs ..... 0
  cancelSubscrReqs ..... 0
  subscrErrors ..... 0
```

-----	
UDP セクション	UDP カウンター
inDatagrams	UDP パケット受信総数
inMcastDatagrams	マルチキャスト UDP パケット受信数
inUcastDatagrams	ユニキャスト UDP パケット受信数
inDatagramsDropped	UDP パケット破棄数
outDatagrams	UDP パケット送信総数
outMcastDatagrams	マルチキャスト UDP パケット送信数
outUcastDatagrams	ユニキャスト UDP パケット送信数
HTTP セクション	HTTP カウンター
httpReqs	HTTP リクエスト受信数
httpReqsRefused	HTTP リクエスト拒否数
httpResps	HTTP レスpons送信数
httpRespsFailed	HTTP レスpons失敗数
Discovery セクション	Discovery フェーズカウンター
mSearchReqs	M-Search リクエスト受信数
mSearchReqsErrors	エラーを含む M-Search リクエスト受信数
mSearchResps	M-Search レスpons送信数
notifyAliveMsgs	notify alive メッセージ送信数
notifyByebyeMsgs	notify byebye メッセージ送信数
Description セクション	Description フェーズカウンター
descReqs	Description リクエスト総数
deviceDescReqs	Device Description リクエスト総数
serviceDescReqs	Service Description リクエスト総数
descErrors	エラーを含む Description リクエスト受信数
descResps	Description レスpons送信数
deviceDescResps	Device Description 送信数
serviceDescResps	Service Description 送信数
Control セクション	Control フェーズカウンター
actionReqs	Action リクエスト受信総数
actionErrors	エラーを含む Action リクエスト受信数
actionResps	Action レスpons送信数
Eventing セクション	Eventing フェーズカウンター
subscrReqs	Subscription リクエスト受信総数
newSubscrReqs	新規 Subscription リクエスト受信数
renewSubscrReqs	更新 Subscription リクエスト受信数
cancelSubscrReqs	取消 Subscription リクエスト受信数

subscrErrors	エラーを含む Subscription リクエスト受信数
subscrResps	Subscription レスポンス送信数
eventsNotified	Event Notification 総数

表 33:

### 関連コマンド

DISABLE UPNP ( 91 ページ )

ENABLE UPNP ( 102 ページ )

## SHOW UPNP INTERFACE

カテゴリー：ファイアウォール / UPnP

**SHOW UPNP FWPOLICY=*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

### 解説

UPnP（Universal Plug and Play）に使用されているインターフェースの情報を表示する。

### パラメーター

**FWPOLICY** ファイアウォールポリシー名

**INTERFACE** IP インターフェース名

### 入力・出力・画面例

```
Manager > show upnp fwpolicy=net interface=all

UPNP Interfaces
-----
Firewall Policy:          net
-----
Interface:                vlan1-0
UPnP Device:              LANDevice:1
UPnP Service:             n/a
Subscriptions:            n/a
Subscriber Notifications: n/a

Interface:                eth0-0
UPnP Device:              WANConnectionDevice:1
UPnP Service:             WANIPConnection:1
Subscriptions:            0
Subscriber Notifications: 0

Interface:                eth0
UPnP Device:              WANDevice:1
UPnP Service:             WANCommonInterfaceConfig:1
Subscriptions:            0
Subscriber Notifications: 0

Interface:                igd-0
UPnP Device:              InternetGatewayDevice:1
```

## SHOW UPNP INTERFACE

```
UPnP Service:                Layer3Forwarding:1
Subscriptions:                0
Subscriber Notifications: 0

-----

Manager > show upnp fwpolicy=net interface=eth0

UPNP Interfaces
-----
Firewall Policy:              net
-----
Interface:                    eth0
UPnP Device:                  WANDevice:1
UPnP Service:                 WANCommonInterfaceConfig:1
Subscriptions:                0
Subscriber Notifications: 0

-----

Actions:                      Invoked:      Action Status
GetCommonLinkProperties       0          Enabled
GetTotalBytesSent             0          Enabled
GetTotalBytesReceived         0          Enabled
GetTotalPacketsSent           0          Enabled
GetTotalPacketsReceived       0          Enabled

Evented State Variables:
PhysicalLinkStatus            Up

Non-evented State Variables:
WANAccessType                  Ethernet
Layer1UpstreamMaxBitRate      100000000
Layer1DownstreamMaxBitRate    100000000
MaximumActiveConnections      1
TotalBytesSent                 0
TotalBytesReceived             0
TotalPacketsSent               0
TotalPacketsReceived           0

-----
```

Firewall policy	UPnP で使用するファイアウォールポリシー名
Interface	デバイス/サービスと関連付けられているインターフェース。「igd-x」は Internet Gateway Device を表す論理インターフェース
UPnP Device	UPnP デバイス名
UPnP Service	UPnP サービス名
Evented State Variables	イベント通知を行う状態変数。状態が変化したときイベントメッセージが送信される

Non-evented State variables	イベント通知を行わない状態変数。状態が変化してもイベントメッセージは送信されない
-----------------------------	--

表 34:

関連コマンド

- DISABLE UPNP ( 91 ページ )
- ENABLE UPNP ( 102 ページ )
- SHOW UPNP ( 144 ページ )