

ファイアウォール

| | |
|----------------------------------|----|
| 概要・基本設定 | 3 |
| 基本設定 | 3 |
| インターフェースと基本ルール | 4 |
| ルールの追加 | 6 |
| ルール設定時の注意事項 | 6 |
| トラフィックを制限する | 7 |
| アクセスを許可する | 8 |
| インターフェース NAT | 12 |
| ルール NAT | 22 |
| アクセスリストによるルール | 27 |
| RADIUS サーバーを利用したルール | 28 |
| ルールの時間制限 | 30 |
| ルールの確認・修正・削除 | 31 |
| ルールの処理順序 | 31 |
| ファイアウォールの動作監視 | 32 |
| ログ | 32 |
| イベント通知 | 35 |
| トリガー | 37 |
| アカウンティング | 38 |
| デバッグオプション | 39 |
| セッションの確認 | 40 |
| その他設定 | 42 |
| 設定例 | 43 |
| コマンドリファレンス編 | 47 |
| 機能別コマンド索引 | 47 |
| ADD FIREWALL POLICY APPRULE | 49 |
| ADD FIREWALL POLICY INTERFACE | 51 |
| ADD FIREWALL POLICY LIST | 53 |
| ADD FIREWALL POLICY NAT | 55 |
| ADD FIREWALL POLICY RULE | 58 |
| CREATE FIREWALL POLICY | 63 |
| DELETE FIREWALL POLICY APPRULE | 64 |
| DELETE FIREWALL POLICY INTERFACE | 65 |
| DELETE FIREWALL POLICY LIST | 66 |

| | |
|---|-----|
| DELETE FIREWALL POLICY NAT | 67 |
| DELETE FIREWALL POLICY RULE | 68 |
| DELETE FIREWALL SESSION | 69 |
| DESTROY FIREWALL POLICY | 70 |
| DISABLE FIREWALL | 71 |
| DISABLE FIREWALL NOTIFY | 72 |
| DISABLE FIREWALL POLICY | 73 |
| DISABLE FIREWALL POLICY IDENTPROXY | 75 |
| DISABLE FIREWALL POLICY TCPSETUPPROXY | 76 |
| ENABLE FIREWALL | 77 |
| ENABLE FIREWALL NOTIFY | 78 |
| ENABLE FIREWALL POLICY | 79 |
| ENABLE FIREWALL POLICY IDENTPROXY | 81 |
| ENABLE FIREWALL POLICY TCPSETUPPROXY | 82 |
| SET FIREWALL MAXFRAGMENTS | 83 |
| SET FIREWALL POLICY | 84 |
| SET FIREWALL POLICY ATTACK | 85 |
| SET FIREWALL POLICY RULE | 88 |
| SHOW FIREWALL | 90 |
| SHOW FIREWALL ACCOUNTING | 93 |
| SHOW FIREWALL ARP | 95 |
| SHOW FIREWALL EVENT | 97 |
| SHOW FIREWALL POLICY | 99 |
| SHOW FIREWALL POLICY ATTACK | 106 |
| SHOW FIREWALL SESSION | 108 |

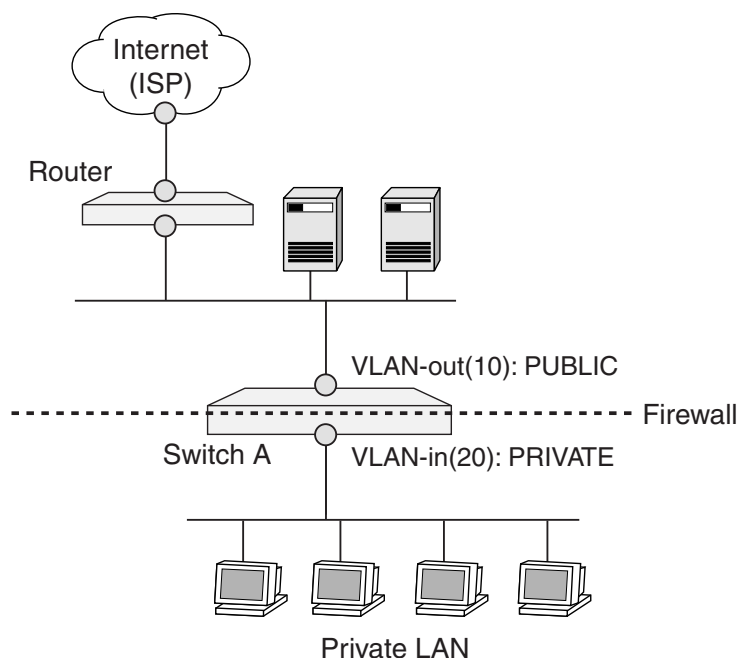
概要・基本設定

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。

- 📎 ファイアウォールを使用するにはフィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要です。
- 📎 ファイアウォール機能は、CPU によるソフトウェア処理で実現されています。そのため、通常のハードウェアルーティング使用時に比べてパフォーマンスが低下します。スループットを重視する場合は、ハードウェア IP フィルターのご使用をお勧めします。一方、ファイアウォールの利点としては、最小限の設定で安全性の高いフィルタリングを行えること、ハードウェア IP フィルターよりも柔軟な設定が可能なこと、パケットのログがとれること、重大イベント発生時の自動通知が可能なことなどが挙げられます。
- 📎 ファイアウォールとハードウェア IP フィルターを同時に使用することはできません。ファイアウォールとソフトウェア IP フィルターの併用は可能です。

基本設定

本製品をファイアウォールとして使用する上で最低限必要な手順は次のとおりです。ここでは次のような構成のネットワークを想定しています。IP の設定までは終わっているものと仮定します。



1. ファイアウォール機能を有効にします。

```
ENABLE FIREWALL ↵
```

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

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

3. ファイアウォールポリシーの適用対象となる IP インターフェースを指定します。内部側 (vlan-in) を PRIVATE、外部側 (vlan-out) を PUBLIC に設定します。

```
ADD FIREWALL POLICY=mynet INT=vlan-in TYPE=PRIVATE ↵
```

```
ADD FIREWALL POLICY=mynet INT=vlan-out TYPE=PUBLIC ↵
```

基本設定は以上です。

これにより、手順 3 で指定したインターフェース間のトラフィックに基本的なルールが適用され、外部 (PUBLIC) から内部 (PRIVATE) にはパケットが転送されなくなります。一方、内部から外部への通信は自由に行うことができます。ステートフルインスペクションにより、内部から通信を開始したときにはその状態が記憶されるため、戻りのパケットを通すために特別な設定をする必要はありません。

本製品では、上記の基本設定に独自のルールを追加することで、内部と外部のインターフェース間のやりとりを制御します。

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

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

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

- Ident プロキシ機能をオフにして、外部メールサーバーなど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 ↵
```

- PUBLIC 側をグローバルアドレス、PRIVATE 側をプライベートアドレスで運用している場合は、ダイナミック ENAT を使うことにより PRIVATE 側から PUBLIC 側への通信が可能になります。

```
ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=vlan-in GBLINT=vlan-out ↵
```

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（58 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。
- NONAT ルール：（本来なら NAT されるトラフィックに）NAT を適用せず、そのまま転送する。

🔒 「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）

- ICMP 転送オフ時、独自ルールで PROTOCOL=ALL を指定しても、ICMP は対象になりません。

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（79 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 転送オン時、拒否・許可ルールで PROTOCOL=ALL を指定しても、ICMP は対象になりません。NAT・NONAT ルールで PROTOCOL=ALL を指定した場合は、ICMP も対象になります。
- 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ソフトウェア 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（58 ページ）を使います。

ルール設定時の注意事項

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。

ルールの設定にあたっては、ルール（ルール番号）が下記の順序になるようにしてください。異なる順序で設定した場合、ルールが正しく機能しないことがあります。

1. 許可・拒否ルール（ACTION=ALLOW と ACTION=DENY）
2. アクセスリストを使用したルール
3. NAT・NONAT ルール（ACTION=NAT と ACTION=NONAT）

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

5つのコマンドは、「vlan-in の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 10.1.1.0～10.1.1.255 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=vlan-in PROT=ALL
REMOTEIP=10.1.1.0-10.1.1.255 ↵
```

このコマンドは、「vlan-in の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 10.1.1.0～10.1.1.255 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 (79 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 192.168.10.5 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=vlan-in PROT=ALL
IP=192.168.10.5 ↵
```

このコマンドは、「vlan-in の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 192.168.10.5 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 (vlan-out) から内部ホスト 172.16.10.10 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=vlan-out PROT=ALL
IP=172.16.10.10 ↵
```

このコマンドは、「vlan-out の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 172.16.10.10 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 (79 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 (vlan-out) から内部の Web サーバー (172.16.10.5 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=vlan-out PROT=TCP
IP=172.16.10.5 PORT=80 ↵
```

このコマンドは、「vlan-out の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 172.16.10.5 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 10.10.10.1 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=vlan-out PROT=ALL
REMOTEIP=10.10.10.1 ↵
```

このコマンドは、「vlan-out の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 10.10.10.1 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、192.168.10.2 と 172.16.10.2 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 (vlan-out) から 172.16.10.2 (実際は 192.168.10.2) 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=vlan-out PROT=ALL
GBLIP=172.16.10.2 IP=192.168.10.2 ↵
```

このコマンドは、「vlan-out 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 172.16.10.2 のものを、終点アドレスを 192.168.10.2 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。また、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。詳細については後述する「スタティック NAT」をご覧ください。

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、192.168.10.2 と 172.16.10.2 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（vlan-out）から 172.16.10.2（実際は 192.168.10.2）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=vlan-out PROT=TCP
    GBLIP=172.16.10.2 GBLPORT=80 IP=192.168.10.2 PORT=80 ↵
```

このコマンドは、「vlan-out 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 172.16.10.2 で終点ポートが 80 番の TCP パケットを、終点アドレスを 192.168.10.2 に書き換えた上で通過させる」の意味になります。

外部からのトラフィックを許可するときのパラメーターの指定方法をまとめます

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

表 6: NAT を使っていない場合

| パラメーター | 指定する内容 |
|-----------|---|
| ACTION | 外部から内部への転送を許可するため ALLOW を指定します。 |
| INTERFACE | 外部 (PUBLIC) インターフェースを指定します。 |
| PROTOCOL | 対象となるプロトコルを指定します。TCP、UDP を指定した場合は GBLPORT、PORT の指定も必要です。ALL を指定した場合は ICMP を除くすべての IP パケットが対象となります。また、プロトコル番号による指定も可能です。 |
| IP | 転送後の終点 IP アドレス。パケットの最終的な宛先となるプライベートアドレスで、内部ホストに実際に割り当てられているアドレスを示します。GBLIP で指定したグローバルアドレス (外から見た終点 IP アドレス) に対応するアドレスを指定してください。 |

| | |
|------------|--|
| PORT | 転送後の終点ポート番号。パケットの最終的な宛先となるポート番号で、内部ホストの実際のポート番号です。PROTOCOL に TCP か UDP を指定した場合にのみ必要です。GBLPORT で指定したグローバル側ポート番号（外から見た終点ポート）に対応するポート番号を指定してください。 |
| GBLIP | 転送前の終点グローバル IP アドレス。外部から見た場合の終点 IP アドレスです。NAT 変換後のプライベートアドレス（最終的な宛先アドレス）は IP パラメーターで指定します。 |
| GBLPORT | 転送前の終点グローバルポート番号。外部から見た場合の終点ポート番号です。NAT 変換後のプライベートポート番号（最終的な宛先ポート）は PORT パラメーターで指定します。 |
| REMOTEIP | 始点 IP アドレス。パケットの送信元となる外部ホストの IP アドレスです（範囲指定可）。省略時はすべての始点 IP アドレスが対象となります。 |
| SOURCEPORT | 始点ポート番号。パケットの送信元となる外部ホストのポート番号です（範囲指定可）。PROTOCOL に TCP か UDP を指定した場合のみ有効。省略時はすべての始点ポートが対象となります。 |

表 7: NAT を使っている場合

インターフェース NAT

本製品のファイアウォールには、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、ルーターなどの中継ノードで IP パケットのアドレスを付け替える機能です。スタティック NAT では、プライベートアドレスをグローバルアドレスに 1 対 1 で固定的に変換します。

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 ↵
```

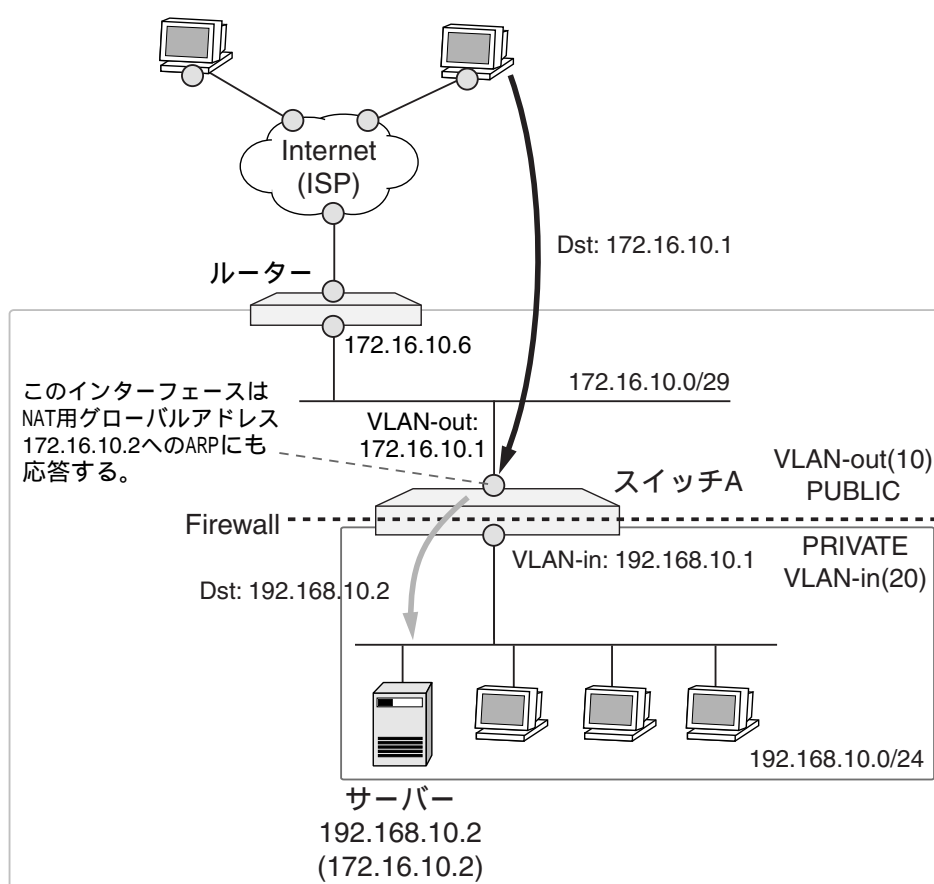
- パケットを「内 IF」から「外 IF」に転送したとき、始点 IP アドレスが「内 IP」であれば「外 IP」に書き換えます。
- パケットを「外 IF」で受信したとき、終点 IP アドレスが「外 IP」であれば「内 IP」に書き換えます。

🔧 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。この例では、「外 IP」に対する ARP request を受信すると、「外 IF」が自身の MAC アドレスで応答します。

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 PROT=プロトコル IP=内 IP GBLIP=外 IP ↵
```

ここでは、次のようなネットワーク構成をもとに、本製品におけるスタティック NAT 設定の要点について解説します。



ここでは、次のような方針で設定を行います。

- ISP からアドレスブロック 172.16.10.0/29 (172.16.10.0 ~ 172.16.10.7) を固定的に割り当てられています。アドレスは 8 個ですが、172.16.10.0 (ネットワークアドレス) と 172.16.10.7 (ブロードキャストアドレス) は使用できないため、端末に設定できるアドレスは 172.16.10.1 ~ 172.16.10.6 の 6 個となります。このうち、172.16.10.6 はすでにルーターの LAN 側 (内側) インターフェースに割り当てられています。

☞ これらのアドレスは実際にはプライベートアドレスですが、ここではグローバルアドレスであると仮定しています。

- ISP とはルーターによって接続されています。ルーターではアドレス変換やパケットフィルタリングを行わず、同ルーターの LAN 側セグメントに接続したスイッチ A (本製品) でファイアウォールを動作させ、ここでアクセス制御を行うものとします。
- スイッチ A の WAN 側 (vlan-out) インターフェースには 172.16.10.1 を割り当てます。これで残るアドレスは 172.16.10.2 ~ 172.16.10.5 の 4 個となります。これらのアドレスはサーバー用に使用しますが、直接サーバーに割り当てることはせずに、スタティック NAT を介して使用します。
- スイッチ A の LAN 側 (vlan-in) インターフェースにはプライベートアドレス 192.168.10.1 を割り当て、クライアントはすべてプライベートアドレスで運用します。
- サーバーにもプライベートアドレスを設定し、スイッチ A の LAN 側セグメントに配置します。サー

バーはルーター・スイッチ A のあるセグメントに置くこともできますが、ファイアウォールで保護したいため、スイッチ A の内側に配置しています。また、外部からアクセスさせるため、スタティック NAT を使って外からはグローバルアドレスを持っているように見せかけます。変換ルールは次のとおりとします。

- サーバー：192.168.10.2 172.16.10.2
- スイッチ A のファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。
- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、ISP から与えられたグローバル IP アドレスのうちの 1 つに変換します。これにより、LAN に接続された複数のコンピューターからインターネットへの同時アクセスが可能になります。

以下、スイッチ A の設定を示します。

1. VLAN を作成します。

```
CREATE VLAN=out VID=10 ↵
CREATE VLAN=in VID=20 ↵
ADD VLAN=out PORT=1 ↵
ADD VLAN=in PORT=2-12 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. LAN 側インターフェース (vlan-in) にプライベート IP アドレスを設定します。

```
ADD IP INT=vlan-in IP=192.168.10.1 MASK=255.255.255.0 ↵
```

4. WAN 側インターフェース (vlan-out) に ISP から割り当てられたグローバルアドレスのうちの 1 つを設定します。

```
ADD IP INT=vlan-out IP=172.16.10.1 MASK=255.255.255.248 ↵
```

5. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 INT=vlan-out NEXT=172.16.10.6 ↵
```

6. ファイアウォールポリシーを作成し、基本設定を行います。

```
ENABLE FIREWALL ↵
CREATE FIREWALL POLICY=net ↵
ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH ↵
DISABLE FIREWALL POLICY=net IDENTPROXY ↵
```

7. ファイアウォールポリシーの適用対象となるインターフェースを指定します。

- LAN 側 (vlan-in) インターフェースを PRIVATE (内部) に設定します。


```
ADD FIREWALL POLICY=net INT=vlan-in TYPE=PRIVATE ↵
```

- WAN 側 (vlan-out) インターフェースを PUBLIC (外部) に設定します。

```
ADD FIREWALL POLICY=net INT=vlan-out TYPE=PUBLIC ↵
```

8. 192.168.10.2 172.16.10.2 のスタティック NAT ルールを設定します。この場合、スタティック NAT 変換は、INT (vlan-in) で受信したパケットが GBLINT (vlan-out) 側にルーティングされたときに行われます。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan-in IP=192.168.10.2
GBLINT=vlan-out GBLIP=172.16.10.2 ↵
```

- ☞ 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。この例では、172.16.10.2 に対する ARP request を受信すると、vlan-out が自身の MAC アドレスで応答します。

9. LAN 側 (vlan-in) ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。グローバルアドレスには、スイッチ A 自身の WAN 側 (vlan-out) インターフェースの IP アドレスを使用します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan-in GBLINT=vlan-out ↵
```

10. 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、サーバーへのパケットを通すための設定を行います。ここでは、172.16.10.2 (192.168.10.2) 宛てのパケットを通過させます。

```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=vlan-out PROT=ALL
GBLIP=172.16.10.2 IP=192.168.10.2 ↵
```

なお、172.16.10.2 の特定ポートだけに通信を限定させたい場合は、PROTOCOL パラメーターでプロトコルを指定し、GBLPORT パラメーターでグローバル側ポート番号を、PORT パラメーターでプライベート側ポート番号を指定します。次の例では HTTP だけを許可しています。

```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=vlan-out PROT=TCP
GBLIP=172.16.10.2 GBLPO=HTTP IP=192.168.10.2 PO=HTTP ↵
```

- ☞ これらのルールを設定しないと、ファイアウォールの基本ルールにより、172.16.10.2 宛てのパケットが vlan-out インターフェースで破棄されてしまいます。

設定は以上です。

ダイナミック NAT

ダイナミック NAT は、ルーターなどの中継ノードで IP パケットのアドレスを付け替える機能です。ダイナミック NAT では、複数のプライベートアドレスを複数のグローバルアドレスに多対多で変換します。アドレス変換時には、あらかじめプールされたグローバルアドレスの中から使用されていないものを動的に選

出します。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。

☞ 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。この例では、「外 IP 範囲」に対する ARP request を受信すると、「外 IF」が自身の MAC アドレスで応答します。

ダイナミック ENAT

ダイナミック ENAT 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 インターフェースを示します。

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

- 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。

```
ADD FIREWALL POLICY=mynet NAT=ENHANCED INT=vlan-in GBLINT=vlan-out ↓
```

このコマンドは、「vlan-in のインターフェースで受信した IP パケットの始点アドレスを vlan-out 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、vlan-out から送信する」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

1 個のグローバルアドレスを ENAT で共有している場合は、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、外部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。

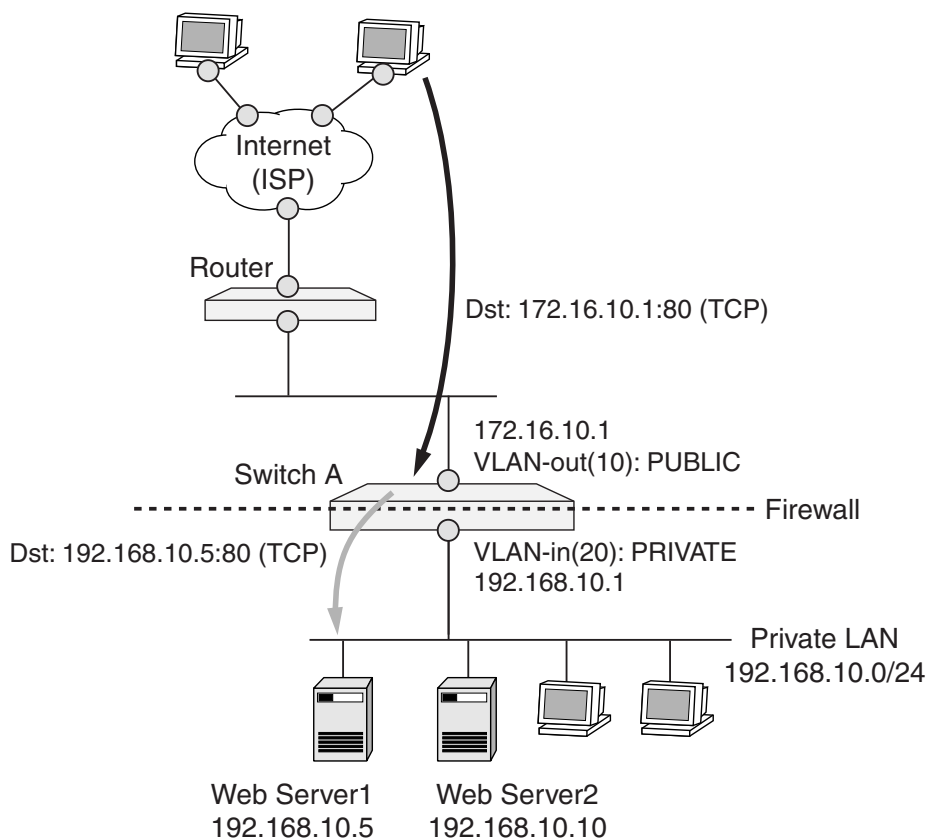
```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=外 IF PROT=プロトコル GBLIP=外 IP  
GBLPORT=外ポート IP=内 IP PORT=内ポート ↓
```

- 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。

🔗 スタティック ENAT の設定は ADD FIREWALL POLICY RULE コマンド（58 ページ）で行います。

🔗 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、スイッチの（外部側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、内部にあるサーバーの 80 番ポートに転送しています。外部のホストからはスイッチ自身が Web サーバーであるかのように見えますが、実際はプライベート IP アドレスを持つ内部の Web サーバーが応答しています。



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. ポート転送機能はENATを使用していることが前提となります。ここでは、PRIVATE インターフェース側の全ホストが、PUBLIC インターフェース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=vlan-in GBLINT=vlan-out ↓
```

2. ポート転送のためのルールを追加します。

```
ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=vlan-out PROT=TCP  
GBLIP=172.16.10.1 GBLPO=80 IP=192.168.10.5 PORT=80 ↓
```

このコマンドは、「vlan-out の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 172.16.10.1 で終点ポートが 80 のものを、アドレス変換してホスト 192.168.10.5 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。

同じ Well-known ポートを使うサーバーを複数公開したい場合、外部からのアクセスはいくらか変則的になりますが、GBLPORT をサーバーごとに変えることで可能となります。ここでは、内部に 192.168.10.5、192.168.10.10 の 2 つの Web サーバーがあるものとします。次の例では、外部から 172.16.10.1 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=vlan-out PROT=TCP GBLIP=172.16.10.1
    GBLPO=80 IP=192.168.10.5 PORT=80 ↵
ADD FIRE POLI=mynet RU=2 AC=ALLOW INT=vlan-out PROT=TCP GBLIP=172.16.10.1
    GBLPO=8080 IP=192.168.10.10 PORT=80 ↵
```

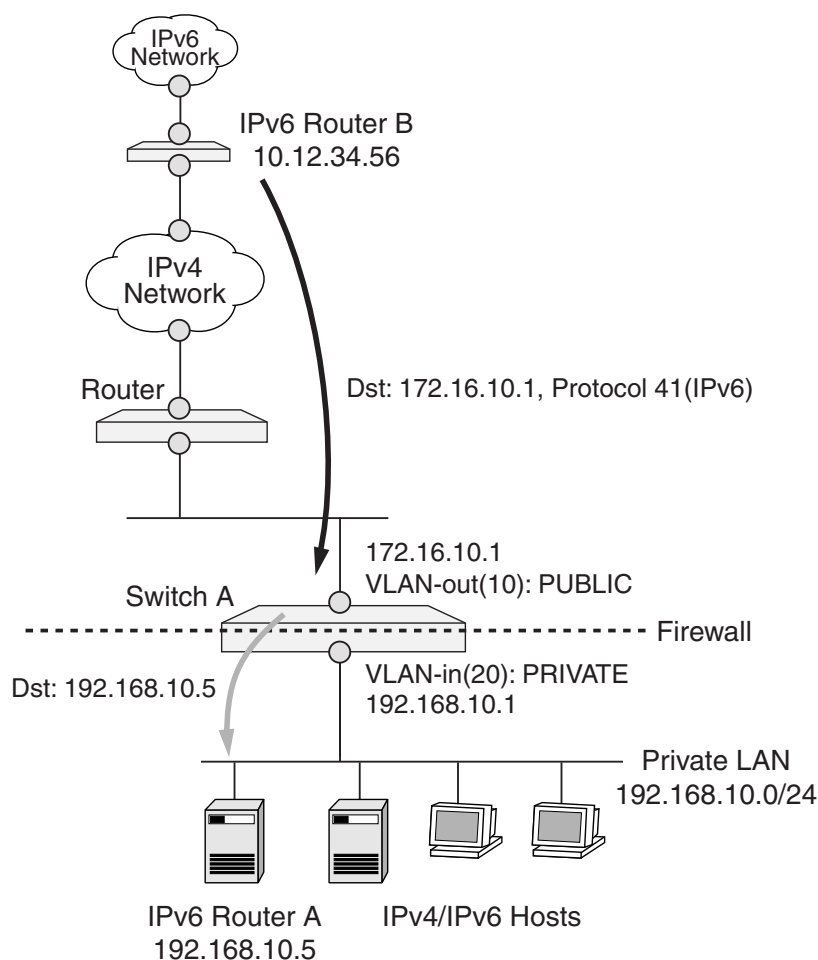
この場合、外部から 192.168.10.10 の Web サーバーにアクセスするには、URL の中でポート番号 8080 を指定する必要があります。ブラウザの URL 欄に次のように入力します。

`http://172.16.10.1:8080/ ...` （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://172.16.10.1/ ...` （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 A (192.168.10.5) が、外部の IPv6 ルーター B (10.12.34.56) との間にトンネルを張り、内部ネットワークを IPv6 ネットワークに接続しています。



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、この環境ではルーター A にはグローバルアドレスがありません。そこで、プロトコル転送機能を利用して、スイッチの外部インターフェース（172.16.10.1）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、内部ネットワークの IPv6 ルーター A に転送する設定を行います。これにより、ルーター B からはスイッチの外部インターフェースが、内部に存在するルーター A のインターフェースに見えます。

```
ADD FIRE POLI=mynet RU=1 AC=ALLOW INT=vlan-out PROTO=41
REMOTEIP=10.12.34.56 GBLIP=172.16.10.1 IP=192.168.10.5 ↵
```

このコマンドは、「vlan-out の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 10.12.34.56 で終点 IP アドレスが 172.16.10.1 のものを、アドレス変換して内部の 192.168.10.5 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

| 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。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:

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 (58 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 (55 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、「エンハンスト NAT」以外は、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対一で変換する。
- エンハンスト 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するもっとも一般的な NAT です。

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)

- 🔗 ルール NAT の設定では、ICMP 転送がオンかオフによって PROTOCOL=ALL の意味が異なります。ICMP 転送がオンのとき、PROTOCOL=ALL は ICMP を含みます。ICMP 転送がオフのとき、PROTOCOL=ALL は ICMP を含みません。これは NONAT ルールも同様です。許可ルール、拒否ルールの場合は、ICMP 転送のオン・オフにかかわらず、PROTOCOL=ALL は ICMP を含みません。

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=vlan-out
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=vlan-out
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。この例では、1.1.1.100 に対する ARP request を受信すると、vlan-out が自身の MAC アドレスで応答します。

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=vlan-in
    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=vlan-in
    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。

vlan-in 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=vlan-in
    PROT=ALL GBLIP=1.1.1.10 ↵
```

vlan-out 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=vlan-out
    PROT=ALL REMOTEIP=192.168.10.200 ↵
```

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。

vlan-in 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=vlan-in
    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=vlan-in 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。

- 「向き」欄の「I/F 種別」は、ルールを適用するインターフェースが PRIVATE 側であるか、PUBLIC 側であることを示しています。
- 「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。
- 「IP」「GBLIP」「REMOTEIP」「GBLREMOTEIP」「NATMASK」は、ADD FIREWALL POLICY RULE コマンド (58 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可能です。また、パラメーター名の後の「*」は、アドレスの範囲指定が可能なことを示しています。「*」の付いていないパラメーターには、単一アドレスを指定しなくてはなりません。
- 「A/B」という表現は、「A」と「B」をビットごとに AND 演算した結果を示します。「A」は IP アドレス、「B」はネットマスクです。
- 「備考」欄の「Src」「Dst」は、それぞれ IP パケットの始点アドレス、終点アドレスを示しています。また、「=」は左辺と右辺が等しいことを示します。
- 「備考」欄では、パケットが変換されるための条件と、どのような変換が行われるかを文章で説明しています。なお、(省略可能な) 条件パラメーターを省略した場合、そのパラメーターの値は ANY (すべてにマッチ) となります。
- 「備考」欄における「X/NATMASK=Y/NATMASK」という表現は、IP アドレス「X」が CIDR 表記「Y/NATMASK」で表される IP アドレス範囲に収まっている、という意味になります。

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 [RE- MOTEIP*] | Src = IP, Dst = REMOTEIP のとき、Src を IP から GBLIP に変換する。GBLREMOTEIP は使用不可 |
| | 内 外 (PUBLIC) | IP [RE- MOTEIP*] | GBLIP [RE- MOTEIP*] | Src = REMOTEIP, Dst = GBLIP のとき、Dst を GBLIP から IP に変換する。GBLREMOTEIP は使用不可 |

| | | | | | |
|--|----------------|------------------------------|---------------------------------|------------------------------------|---|
| ス タ ン ダ ー ド ・ サ ブ ネ ッ ト | 内 (PRIVATE) | 外 [RE- MOTEIP*] | IP/NATMASK [RE- MOTEIP*] | SKIP/NATMASK [RE- MOTEIP*] | NATMASK = IP/NATMASK, Dst = RE- MOTEIP のとき、Src のサブネット部だけを IP/NATMASK から GBLIP/NATMASK に変換 する。GBLREMOTEIP は使用不可 |
| | 内 (PUBLIC) | 外 [RE- MOTEIP*] | IP/NATMASK [RE- MOTEIP*] | SKIP/NATMASK [RE- MOTEIP*] | REMOTEIP, Dst/NATMASK = GBLIP/NATMASK のとき、Dst のサブネット部 だけを GBLIP/NATMASK から IP/NATMASK に変 換する。GBLREMOTEIP は使用不可 |
| エ ン ハ ン ス ト | 内 (PRIVATE) | 外 [RE- MOTEIP*] | [IP*] [RE- MOTEIP*] | GBLIP [RE- MOTEIP*] | Src = IP, Dst = REMOTEIP のとき、Src を IP から GBLIP に変換（ポートも変換）する。GBLREMOTEIP は使用不可 |
| | 内 (PUBLIC) | 外 RE- MOTEIP | [IP*] [GBLRE- MOTEIP*] | [IP*] [GBLRE- MOTEIP*] | Src = GBLREMOTEIP, Dst = IP のとき、Src を GBLREMOTEIP から REMOTEIP に変換する（ポート も変換）する。GBLIP は使用不可 |
| リ バ ー ス | 内 (PRIVATE) | 外 [RE- MOTEIP*] | [IP] [RE- MOTEIP*] | [IP] [GBLRE- MOTEIP] | Src = IP, Dst = REMOTEIP のとき、Dst を RE- MOTEIP から GBLREMOTEIP に変換する。GBLIP は使用不可 |
| | 内 (PUBLIC) | 外 RE- MOTEIP | [IP] [RE- MOTEIP] | [IP] [GBLRE- MOTEIP] | Src = GBLREMOTEIP, Dst = IP のとき、Src を GBLREMOTEIP から REMOTEIP に変換する。 GBLIP は使用不可 |
| リ バ ー ス ・ サ ブ ネ ッ ト | 内 (PRIVATE) | 外 [RE- MOTEIP/NATMASK] | [IP] [RE- MOTEIP/NATMASK] | [IP] [GBLRE- MOTEIP/NATMASK] | Src = IP, Dst/NATMASK = RE- MOTEIP/NATMASK のとき、Dst のサブネット 部だけを REMOTEIP/NATMASK から GBLRE- MOTEIP/NATMASK に変換する。GBLIP は使用不 可 |
| | 内 (PUBLIC) | 外 [RE- MOTEIP/NATMASK] | [IP] [RE- MOTEIP/NATMASK] | [IP] [GBLRE- MOTEIP/NATMASK] | Src/NATMASK = GBLREMOTEIP/NATMASK, Dst = IP のとき、Src のサブネット部だけを GBLRE- MOTEIP/NATMASK から REMOTEIP/NATMASK に変換する。GBLIP は使用不可 |
| ダ ブ ル | 内 (PRIVATE) | 外 [RE- MOTEIP*] | IP [RE- MOTEIP*] | GBLIP [GBLRE- MOTEIP] | Src = IP, Dst = REMOTEIP のとき、Src を IP から GBLIP に、Dst を REMOTEIP から GBLREMOTEIP に変換する |

| | | | | |
|---------------------------|-----|---|---|---|
| ダブ ル・ サブ ネッ ト | 内 外 | IP (PUBLIC) RE- MOTEIP | GBLIP GBLRE- MOTEIP | Src = GBLREMOTEIP, Dst = GBLIP のとき、Src を GBLREMOTEIP から REMOTEIP に、Dst を GBLIP から IP に変換する |
| | 内 外 | IP/NATMASK (PRIVATE) RE- MOTEIP/NATMASK | GBLIP/NATMASK GBLRE- MOTEIP/NATMASK | Src/NATMASK = IP/NATMASK, Dst/NATMASK = REMOTEIP/NATMASK のとき、Src のサブネット部 だけを IP/NATMASK から GBLIP/NATMASK に、 Dst/NATMASK のサブネット部だけを REMOTEIP/NATMASK から GBLREMOTEIP/NATMASK に変換する |
| | 内 外 | IP/NATMASK (PUBLIC) RE- MOTEIP/NATMASK | GBLIP/NATMASK GBLRE- MOTEIP/NATMASK | Src/NATMASK = GBLREMOTEIP/NATMASK, Dst/NATMASK = GBLIP/NATMASK のとき、Src のサブネット部だけを GBLREMOTEIP/NATMASK から REMOTEIP/NATMASK に、Dst のサブネット 部だけを GBLIP/NATMASK から IP/NATMASK に 変換する |

表 9:

アクセスリストによるルール

ADD FIREWALL POLICY RULE コマンド (58 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。

- 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 228 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
10.30.1.23
172.25.150.150             henna-server
172.30.100.0 - 172.30.100.255 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: 192.168.1.5)
- アドレス範囲 (例: 192.168.1.0 - 192.168.1.255。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 (99 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。

- 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、VLAN「inside」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=vlan-inside
    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=vlan-inside PROTO=ALL
    REMOTEIP=10.30.1.23 ↓
ADD FIREWALL POLICY=mynet RULE=2 ACTION=DENY INT=vlan-inside PROTO=ALL
    REMOTEIP=172.25.150.150 ↓
ADD FIREWALL POLICY=mynet RULE=3 ACTION=DENY INT=vlan-inside PROTO=ALL
    REMOTEIP=172.30.100.0-172.30.100.255 ↓
```

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 (53 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。この機能を使うと、許可・拒否する IP アドレスを RADIUS サーバー側で集中管理できます。

以下、RADIUS ルールの基本的な設定手順について説明します。RADIUS ルールを使用するには、最初に RADIUS サーバーの設定を行い、次に本製品の設定を行います。ここでは、架空の RADIUS サーバーを例に説明しますが、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 (本製品) 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 192.168.10.1 {
    secret      = himitsu
    shortname   = kkSwitch
}
```

2. RADIUS サーバーのユーザーデータベースに、許可・拒否する IP アドレスを登録します。IP アドレスごとに次のような内容のユーザーエントリ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 | 備考 |
|-------------------|--------------------|---|
| User-Name | [ipadd] | IP アドレスを角カッコ ([]) で囲んだもの。外向き通信のときは終点アドレス、内向き通信のときは始点アドレスを指定する |
| User-Password | allowdeny | 固定値。パスワード不一致のときは Access-Reject が返るため、結果的にパケットが拒否されるので注意（ただし、PRIVATE 側 DENY ルールでは許可されます） |
| Framed-IP-Address | 0.0.0.0 以外の任意のアドレス | 0.0.0.0 を指定した場合、あるいは、Framed-IP-Address 属性が返ってこない場合、パケットが拒否されるので注意 |

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。これは、IP アドレス 10.1.1.5 と 10.1.3.125 を許可し、それ以外を拒否するという設定です。

```
[10.1.1.5]      Auth-Type := Local, User-Password == "allowdeny"
                  Framed-IP-Address = 1.1.1.1

[10.1.3.125]   Auth-Type := Local, User-Password == "allowdeny"
                  Framed-IP-Address = 1.1.1.1
```

3. エントリーの追加が完了したら、RADIUS サーバーを起動または再起動してください。
4. 本製品が使う RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。ここでは、RADIUS サーバーの IP アドレスを 192.168.10.130 とします。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

5. RADIUS ルールを作成します。「LIST=RADIUS」が RADIUS サーバーを使うための指定です。PUBLIC インターフェースに対して「LIST=RADIUS」を指定した場合、ACTION パラメーターは意味を持ちません。ALLOW か DENY のどちらを指定しても同じ動作（デフォルト拒否）になります。この例では、vlan-out で受信したパケットのうち、始点アドレスが RADIUS サーバーに登録されているものだけを許可し、その他のパケットは拒否します。

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=DENY INT=vlan-out PROTO=ALL
LIST=RADIUS ↵
```

- ☞ PUBLIC インターフェースに設定した RADIUS ルールでは、ACTION パラメーターは意味を持ちません。DENY、ALLOW のどちらを指定しても、「デフォルト拒否」になります。一方、PRIVATE インターフェースに設定した RADIUS ルールでは、DENY を指定した場合「デフォルト許可」、ALLOW を指定した場合は「デフォルト拒否」になります。詳しくは次節「許可・拒否の決定基準」をご覧ください。

許可・拒否の決定基準

RADIUS ルールの処理では、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、PRIVATE インターフェースに設定したルールでは終点アドレスが、PUBLIC インターフェースに設定したルールでは始点アドレスが入ります。

RADIUS サーバーからの応答とパケットの許可・拒否は次のようになります。

「PUBLIC 側」、「PRIVATE 側」はそれぞれ、「PUBLIC インターフェースに設定したルール」、「PRIVATE インターフェースに設定したルール」を示します。「DENY」、「ALLOW」はルールのアクションです。また、はパケットが許可されることを、×はパケットが拒否されることを示しています。また、ここでは「!=」を「等しくない」、「==」を「等しい」の意味で使っています。

| RADIUS サーバーの応答 | PUBLIC 側 | | PRIVATE 側 | |
|--|----------|-------|-----------|-------|
| | DENY | ALLOW | DENY | ALLOW |
| Access-Accept (Framed-IP-Address != 0.0.0.0) | | | | |
| Access-Accept (Framed-IP-Address == 0.0.0.0) | × | × | × | × |
| Access-Accept (Framed-IP-Address なし) | × | × | × | × |
| Access-Reject | × | × | | × |
| 問い合わせがタイムアウト | × | × | | × |

表 11:

- PUBLIC インターフェースに設定した RADIUS ルールでは、ACTION パラメーターは意味を持ちません。DENY、ALLOW のどちらを指定しても、「デフォルト拒否」になります。すなわち、「Framed-IP-Address != 0.0.0.0」として RADIUS サーバーに登録されているアドレスだけが許可され、その他のアドレスはすべて拒否されます。
- 一方、PRIVATE インターフェースに設定した RADIUS ルールでは、DENY を指定した場合「デフォルト許可」、ALLOW を指定した場合は「デフォルト拒否」になります。
 - PRIVATE 側 DENY ルールでは、「Framed-IP-Address == 0.0.0.0」として RADIUS サーバーに登録されているアドレスだけが拒否され、その他はすべて許可されます。
 - PRIVATE 側 ALLOW ルールでは、「Framed-IP-Address != 0.0.0.0」として RADIUS サーバーに登録されているアドレスだけが許可され、その他のアドレスはすべて拒否されます。

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 (58 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（172.16.10.5 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=vlan-out PROT=TCP IP=172.16.10.5
PORT=80 DAYS=WEEKDAY AFT=9:00 BEF=20:00 ↵
```

このコマンドは、「vlan-out の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 172.16.10.5 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。

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（99 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（88 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（68 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. 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。
 - RADIUS サーバーが Access-Accept を返し、なおかつ、Framed-IP-Address として「0.0.0.0」以外のアドレスを返してきた場合は、フローを許可します。また、PRIVATE 側からのフローに限っては、RADIUS サーバーが Access-Reject を返してきた場合と、RADIUS サーバーへの問い合わせがタイムアウトした場合も該当フローを許可します。
 - それ以外の場合は、フローを拒否します。次に、フローが拒否される場合の例を挙げます。
 - － RADIUS サーバーが Access-Accept を返し、なおかつ、Framed-IP-Address として「0.0.0.0」を返してきた場合は、フローを拒否します。
 - － RADIUS サーバーが Access-Accept を返し、なおかつ、Framed-IP-Address を返してこなかった場合は、フローを拒否します。
 - － PUBLIC 側からのフローに対して、RADIUS サーバーが Access-Reject を返してきた場合は、該当フローを拒否します。
 - － PUBLIC 側からのフローに対して、RADIUS サーバーへの問い合わせがタイムアウトした場合は、該当フローを拒否します。

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 (79 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 12: 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、INAOOTHER、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 384 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（78 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
- ASYN：コンソール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=kkSwitch.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@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@kkSwitch.example.com
To: <admin@example.com>
Date: Sun, 22 Jul 2001 13:33:19 +0900

22-Jul-2001 13:33:19
  SYN attack from 1xx.xx.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 (90 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 (72 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 (97 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動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 | ホスト上で稼動中のサービスを調べる |
| 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 |
| 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 13: 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 164 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@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 199.xx.xx.180 started (Policy mynet)
From: manager@kkSwitch.example.com
To: <admin@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 (85 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 (106 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 (79 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 (93 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 (79 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すので、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(73 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(99 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 (108 ページ) を使います。

```
Manager > show firewall session
```

```
Policy : net
```

```
Current Sessions
```

```
-----
3f41 TCP      IP: 192.168.20.200:65534      Remote IP: 192.168.10.100:23
      Gbl IP: 192.168.20.200:65534  Gbl Remote IP: 192.168.10.100:23
      TCP state ..... established
      Start time ..... 11:17:15 11-Jun-2002
      Seconds to deletion ..... 3504
5d1f TCP      IP: 192.168.20.200:65533      Remote IP: 192.168.10.103:22
      Gbl IP: 192.168.20.200:65533  Gbl Remote IP: 192.168.10.103:22
      TCP state ..... synSent
      Start time ..... 11:17:58 11-Jun-2002
      Seconds to deletion ..... 510
b310 UDP      IP: 192.168.20.200:65532      Remote IP: 192.168.10.100:53
      Gbl IP: 192.168.20.200:65532  Gbl Remote IP: 192.168.10.100:53
      Start time ..... 11:19:25 11-Jun-2002
      Seconds to deletion ..... 300
-----
```

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 (108 ページ) に COUNTER オプションを付けます。

```
Manager > show firewall session counter
```

```
Policy : net
```

```
Current Sessions
```

```
-----
3f41 TCP      IP: 192.168.20.200:65534      Remote IP: 192.168.10.100:23
      Gbl IP: 192.168.20.200:65534  Gbl Remote IP: 192.168.10.100:23
      Packets from private IP ..... 22
      Octets from private IP ..... 1420
      Packets to private IP ..... 21
      Octets to private IP ..... 1664
      TCP state ..... established
      Start time ..... 11:17:15 11-Jun-2002
      Seconds to deletion ..... 3474
5d1f TCP      IP: 192.168.20.200:65533      Remote IP: 192.168.10.103:22
      Gbl IP: 192.168.20.200:65533  Gbl Remote IP: 192.168.10.103:22
      Packets from private IP ..... 4
      Octets from private IP ..... 240
      Packets to private IP ..... 0
      Octets to private IP ..... 0
      TCP state ..... synSent
      Start time ..... 11:17:58 11-Jun-2002
      Seconds to deletion ..... 480
b310 UDP      IP: 192.168.20.200:65532      Remote IP: 192.168.10.100:53
      Gbl IP: 192.168.20.200:65532  Gbl Remote IP: 192.168.10.100:53
      Packets from private IP ..... 1
-----
```

```

Octets from private IP ..... 73
Packets to private IP ..... 1
Octets to private IP ..... 165
Start time ..... 11:19:25 11-Jun-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 (108 ページ) で該当セッションの ID (上図の太字の部分) を確認してから、次のコマンドを実行します。

```
DELETE FIREWALL SESSION=2826 ↵
```

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、ソフトウェア IP フィルターを併用してください。ソフトウェア 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 (vlan-out) 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。ソフトウェア IP フィルターの詳細については、「IP」の「ソフトウェア IP フィルター」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=vlan-out 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_FORWARDING=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 (75 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 (76 ページ) で代理応答を無効にしてください。

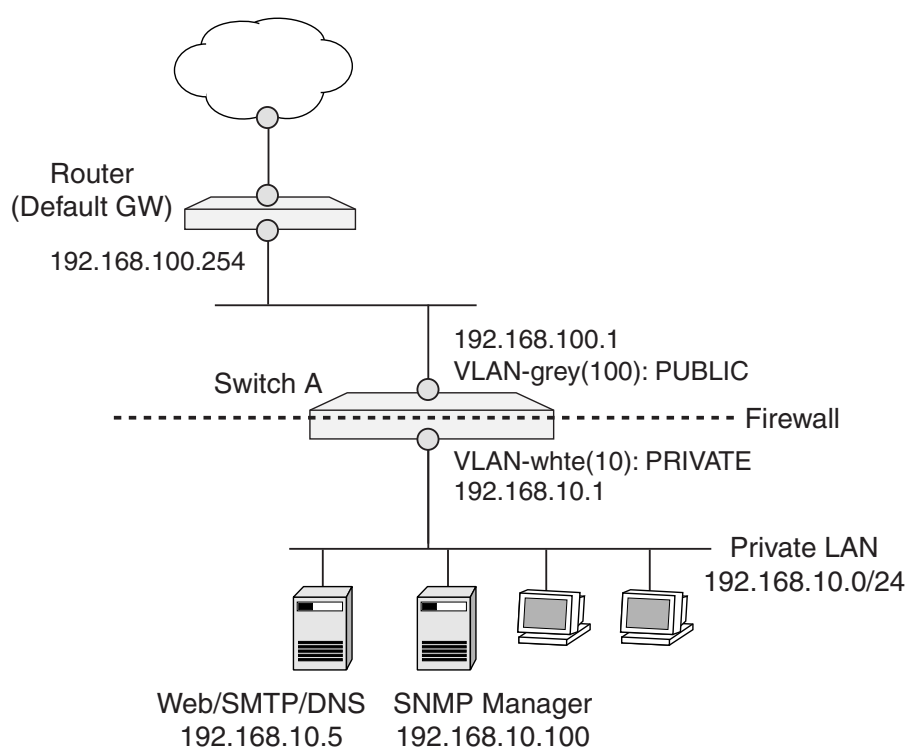
```
DISABLE FIREWALL POLICY=mynet TCPSETUPPROXY ↵
```

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 TCPSETUPPROXY コマンド (82 ページ) を使います。

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

設定例

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



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

- ICMP は Ping(echo/echo reply) と Unreachable のみ双方向とも許可。
- UDP は双方向とも禁止。ただし、UDP の DNS サービス (53) のみ双方向とも許可する。
- TCP は内部から外部へのみコネクションを張ることができる。ただし、以下は例外とする。
 - － 内部の DNS サーバー (192.168.10.5) の DNS サービス (53) には外部から TCP のコネクションを張れる。
 - － 内部のメールサーバー (192.168.10.5) の SMTP サービス (25) には外部から TCP のコネクションを張れる。
 - － 内部の Web サーバー (192.168.10.5) の HTTP サービス (80) には外部から TCP のコネクションを張れる。ただし、時間を朝 10:00 ~ 夜 21:00 に限定する。
- vlan-white を PRIVATE、vlan-grey を PUBLIC インターフェースとして設定する。
- ファイアウォールでブロックしたパケットをログに記録する。
- ポートスキャンなどの不正行為を受けた場合は、SNMP トラップでマネージャーステーション (192.168.10.100) に通知する。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=grey VID=100 ↵
ADD VLAN=white PORT=1-23 ↵
ADD VLAN=grey PORT=24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-grey IP=192.168.100.1 MASK=255.255.255.0 ↵
```

4. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-grey
NEXT=192.168.100.254 ↵
```

5. ファイアウォールを有効にします。

```
ENABLE FIREWALL ↵
```

6. ファイアウォールポリシーを作成します。

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

7. ファイアウォールで拒否したパケットをログに記録するように設定します。

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

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

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

9. ファイアウォールポリシーの適用対象となるインターフェースを指定します。

- vlan-white を PRIVATE (内部) インターフェースに設定します。

```
ADD FIREWALL POLICY=mypol INT=vlan-white TYPE=PRIVATE ↵
```

- vlan-grey を PUBLIC (外部) インターフェースに設定します。

```
ADD FIREWALL POLICY=mypol INT=vlan-grey TYPE=PUBLIC ↵
```

10. 以下、ポリシーの詳細設定を行います。

- ICMP echo/echo reply と Unreachable を双方向で許可します。

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

- UDP は、DNS サービス (53) のみ双方向で許可します。

```
ADD FIREWALL POLICY=myspol RULE=1 ACTION=ALLOW INT=vlan-white
  PROT=UDP PORT=DNS ↓
```

```
ADD FIREWALL POLICY=myspol RULE=2 ACTION=ALLOW INT=vlan-grey
  PROT=UDP PORT=DNS ↓
```

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

```
ADD FIREWALL POLICY=myspol RULE=3 ACTION=DENY INT=vlan-white
  PROT=UDP PORT=ALL ↓
```

- 内部のDNSサーバー（192.168.10.5）のDNSサービス（53）には外部からTCPのコネクションを張れるようにします。

```
ADD FIREWALL POLICY=myspol RULE=4 ACTION=ALLOW INT=vlan-grey
  IP=192.168.10.5 PROT=TCP PORT=DNS ↓
```

- 内部のメールサーバー（192.168.10.5）のSMTPサービス（25）には外部からTCPのコネクションを張れるようにします。

```
ADD FIREWALL POLICY=myspol RULE=5 ACTION=ALLOW INT=vlan-grey
  IP=192.168.10.5 PROT=TCP PORT=SMTP ↓
```

- 内部のWebサーバー（192.168.10.5）のHTTPサービス（80）には外部からTCPのコネクションを張れるようにします。ただし、時間を朝10:00～夜20:59に制限します。

```
ADD FIRE POLI=myspol RU=6 AC=ALLOW INT=vlan-grey IP=192.168.10.5
  PROT=TCP PO=WWW AFTER=9:59 BEFORE=21:00 ↓
```

11. 不正行為を受けたときは、SNMPトラップで通知するよう設定します。SMTPコミュニティ名は大文字小文字を区別するので注意してください。

```
ENABLE SNMP ↓
CREATE SNMP COMMUNITY=public ↓
ENABLE SNMP COMMUNITY=public TRAP ↓
ADD SNMP COMMUNITY=public MANAGER=192.168.10.100
  TRAPHOST=192.168.10.100 ↓
ENABLE FIREWALL NOTIFY=SNMP ↓
```

設定は以上です。

コマンドリファレンス編

機能別コマンド索引

一般コマンド

| | |
|------------------------------------|----|
| DISABLE FIREWALL | 71 |
| ENABLE FIREWALL | 77 |
| SHOW FIREWALL | 90 |
| SHOW FIREWALL ACCOUNTING | 93 |
| SHOW FIREWALL ARP | 95 |

ファイアウォールポリシー

| | |
|---|----|
| ADD FIREWALL POLICY INTERFACE | 51 |
| CREATE FIREWALL POLICY | 63 |
| DELETE FIREWALL POLICY INTERFACE | 65 |
| DESTROY FIREWALL POLICY | 70 |
| DISABLE FIREWALL POLICY | 73 |
| DISABLE FIREWALL POLICY TCPSETUPPROXY | 76 |
| ENABLE FIREWALL POLICY | 79 |
| ENABLE FIREWALL POLICY TCPSETUPPROXY | 82 |
| SET FIREWALL MAXFRAGMENTS | 83 |
| SET FIREWALL POLICY | 84 |
| SHOW FIREWALL POLICY | 99 |

フィルタールール

| | |
|--|----|
| ADD FIREWALL POLICY APPRULE | 49 |
| ADD FIREWALL POLICY RULE | 58 |
| DELETE FIREWALL POLICY APPRULE | 64 |
| DELETE FIREWALL POLICY RULE | 68 |
| SET FIREWALL POLICY RULE | 88 |

ファイアウォール NAT

| | |
|--------------------------------------|----|
| ADD FIREWALL POLICY NAT | 55 |
| DELETE FIREWALL POLICY NAT | 67 |

イベント管理

| | |
|---------------------------------------|-----|
| DISABLE FIREWALL NOTIFY | 72 |
| ENABLE FIREWALL NOTIFY | 78 |
| SET FIREWALL POLICY ATTACK | 85 |
| SHOW FIREWALL EVENT | 97 |
| SHOW FIREWALL POLICY ATTACK | 106 |

アクセスリスト

| | |
|------------------------------------|----|
| ADD FIREWALL POLICY LIST | 53 |
|------------------------------------|----|

| | |
|--|-----|
| DELETE FIREWALL POLICY LIST | 66 |
| ident プロキシー | |
| DISABLE FIREWALL POLICY IDENTPROXY | 75 |
| ENABLE FIREWALL POLICY IDENTPROXY | 81 |
| ファイアウォールセッション | |
| DELETE FIREWALL SESSION | 69 |
| SHOW FIREWALL SESSION | 108 |

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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
ADD FIREWALL POLICY=policy APPRULE=app-rule-id ACTION={ALLOW|DENY}
      INTERFACE=vlan-if 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)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

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

VLAN out 側からの FTP PUT (STOR) を禁止する。

```
ADD FIREWALL POLI=mynet APPRULE=1 ACT=DENY INT=vlan-out APP=FTP
      COMMAND=PUT
```

関連コマンド

DELETE FIREWALL POLICY APPRULE (64 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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

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

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

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

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 にパケットを転送する。PASSALL を指定した場合は、ファイアウォールによるフィルタリングは行われない。PASSALL は、スタティック NAT を使用するインターフェースで使用する。

例

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

ADD FIREWALL POLICY INTERFACE

```
ADD FIREWALL POLICY=protector INT=vlan-white TYPE=PRIVATE  
ADD FIREWALL POLICY=protector INT=vlan-red TYPE=PUBLIC
```

関連コマンド

CREATE FIREWALL POLICY (63 ページ)
DELETE FIREWALL POLICY INTERFACE (65 ページ)
SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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.com # 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.com 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 (63 ページ)

DELETE FIREWALL POLICY LIST (66 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
ADD FIREWALL POLICY=policy NAT={ENHANCED|STANDARD} INTERFACE=vlan-if
GBLINTERFACE=vlan-if [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)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

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 NAT ルールを追加する。

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。

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

不特定のvlan-in側端末のプライベートアドレスをvlan-outのグローバルアドレスに変換するダイナミックENATの設定

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan-in GBLINT=vlan-out
```

上記ダイナミックENATにスタティックENAT(ポート転送)の設定を加えた例。vlan-outに割り当てられたアドレス1.1.1.1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=vlan-in GBLINT=vlan-out
ADD FIRE POLI=net RU=1 AC=ALLOW INT=vlan-out PROT=TCP GBLIP=1.1.1.1
GBLPORT=80 IP=192.168.10.5 PORT=80
```

vlan-in側端末192.168.10.10をvlan-out側では1.1.1.10に見せかけるスタティックNATの設定。NAT用アドレス1.1.1.10が実インターフェースに割り当てられていない場合、本製品は1.1.1.10へのARP Requestに自動的に応答する。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan-in GBLINT=vlan-out
IP=192.168.10.10 GBLIP=1.1.1.10
```

不特定のvlan-in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。NAT用アドレス1.1.1.11~1.1.1.13が実インターフェースに割り当てられていない場

合、本製品は 1.1.1.11 ~ 1.1.1.13 への ARP Request に自動的に応答する。

```
ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan-in GBLINT=vlan-out  
GBLIP=1.1.1.11-1.1.1.13
```

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)。

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 に自動的に応答する。

関連コマンド

CREATE FIREWALL POLICY (63 ページ)

DELETE FIREWALL POLICY NAT (67 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
ADD FIREWALL POLICY=policy RULE=rule-id ACTION={ALLOW|DENY|NAT|NONAT}
INTERFACE=vlan-if PROTOCOL={protocol|ALL|GRE|OSPF|SA|TCP|UDP}
[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] [AFTER=time] [BEFORE=time] [DAYS=day-list]
```

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)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

protocol: IP プロトコル番号 (0~255)

ipadd: IP アドレス

port: TCP/UDP ポート番号 (0~65535)

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)

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。ルールは番号の小さい順に検索され、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

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。なお、INTERFACE パラメーターで PUBLIC インターフェースを指定し、LIST パラメーターに RADIUS を指定した場合、アクションの指定は意味を持たない。ALLOW、DENY のどちらを指定しても同じ意味 (デフォルト拒否) になる。詳しくは解説編を参照。

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 インターフェースのルールでは始点アドレスとして、

PRIVATE インターフェースのルール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。

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

| 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 |
| 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

VLAN in 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=vlan-in PROT=UDP
PORT=137-139
ADD FIREWALL POLICY=mynet RULE=2 AC=DENY INT=vlan-in PROT=TCP
PORT=137-139
```

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

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=vlan-out 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、VLAN out 側からのパケットを通過させる。

```
ADD FIREWALL POLICY=mynet RULE=1 AC=ALLOW INT=vlan-out 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、VLAN out 側からのアクセスを許可する

```
ADD FIREWALL POLICY=mynet RULE=1 ACTION=ALLOW INT=vlan-out PROTO=ALL
LIST=myguest
```

備考・注意事項

「PROTOCOL=ALL」の意味は、アクション（ACTION）と ICMP 転送のオン・オフによって異なる。ICMP 転送がオフのときは、アクションに関係なく「PROTOCOL=ALL」は ICMP を含まない。ICMP 転送がオンのとき、ALLOW、DENY アクションでは「PROTOCOL=ALL」に ICMP を含まないが、NAT、NONAT アクションでは ICMP を含む。ICMP 転送のオン・オフは、ENABLE FIREWALL POLICY コマンド、DISABLE FIREWALL POLICY コマンドの ICMP_FORWARDING パラメーターで設定する。ルールの設定にあたっては、ルール（ルール番号）が下記の順序になるようにすること。異なる順序で設定した場合、ルールが正しく機能しないことがあるので注意。

1. 許可・拒否ルール（ACTION=ALLOW と ACTION=DENY）
2. アクセスリストを使用したルール
3. NAT・NONAT ルール（ACTION=NAT と ACTION=NONAT）

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 に自動的に応答する。

関連コマンド

[CREATE FIREWALL POLICY \(63 ページ \)](#)

[DELETE FIREWALL POLICY RULE \(68 ページ \)](#)

[SET FIREWALL POLICY RULE \(88 ページ \)](#)

[SHOW FIREWALL POLICY \(99 ページ \)](#)

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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (51 ページ)

ADD FIREWALL POLICY LIST (53 ページ)

ADD FIREWALL POLICY NAT (55 ページ)

ADD FIREWALL POLICY RULE (58 ページ)

DESTROY FIREWALL POLICY (70 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (49 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

DELETE FIREWALL POLICY=*policy* INTERFACE=*vlan-if*

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)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

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 (51 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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。

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 (53 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
DELETE FIREWALL POLICY=policy NAT={ENHANCED|STANDARD} INTERFACE=vlan-if
      GBLINTERFACE=vlan-if [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)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または PPP インターフェース

ipadd: IP アドレス

解説

ファイアウォールポリシーからインターフェース NAT ルールを削除する。

パラメーター

POLICY ファイアウォールポリシー名

NAT NAT の種類。STANDARD または ENHANCED

INTERFACE プライベート側 IP インターフェース

IP スタティック (1 対 1) NAT 時のプライベート側 IP アドレスを指定する。NAT=STANDARD の場合のみ有効

GBLINTERFACE グローバル側 IP インターフェース

関連コマンド

ADD FIREWALL POLICY NAT (55 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (58 ページ)

SET FIREWALL POLICY RULE (88 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (108 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (63 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL POLICY (99 ページ)

DISABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (72 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL (77 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL (90 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

DISABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|ASYN|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 (71 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL (77 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL (90 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
DISABLE FIREWALL POLICY=policy [ACCOUNTING] [DEBUG={ALL|ARP|PACKET|PKT|
PROCESS}] [FRAGMENT={UDP|ICMP|OTHER}] [ICMP_FORWARDING={ALL|PARAMETER|
PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|UNREACHABLE}] [LOG={ALLOW|DENY|
DENYDUMP|INAIICMP|INALLOW|INAOOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|
INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|INDUDP|OUTAIICMP|
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、アカウントティング機能、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。ARP (ARP Request の情報表示)、PKT、PACKET (パケット先頭 56 バイトのダンプ表示)、PROCESS (パケット処理過程の表示)、ALL (すべて) から選択する。

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。カンマ区切りで複数指定可能。デフォルトはすべて不透過。不透過の場合、再構成後の IP データサイズ (L4 パケットサイズ) が 1660 バイトを超えるか、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。透過の場合、再構成後サイズの制限はないが、フラグメントの数が SET FIREWALL MAXFRAGMENTS コマンドで設定した値 (デフォルトは 20 個) を超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=mypolicy 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 (71 ページ)

DISABLE FIREWALL NOTIFY (72 ページ)

ENABLE FIREWALL (77 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SET FIREWALL MAXFRAGMENTS (83 ページ)

SHOW FIREWALL (90 ページ)

DISABLE FIREWALL POLICY IDENTPROXY

カテゴリー：ファイアウォール / ident プロキシー

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

DISABLE FIREWALL POLICY=*policy* IDENTPROXY

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

解説

ident プロキシー機能を無効にする。

ident プロキシーは、ファイアウォール有効時に、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 (81 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（82 ページ）

SHOW FIREWALL（90 ページ）

SHOW FIREWALL POLICY（99 ページ）

ENABLE FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (71 ページ)

DISABLE FIREWALL NOTIFY (72 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL (90 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

ENABLE FIREWALL NOTIFY={**ALL**|**MAIL**|**MANAGER**|**ASYN**|**SNMP**}[, ...]
 [ASYN=*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。ASYN (非同期ポートに出力) を指定した場合は、ASYN 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。

ASYN 通知メッセージの出力先非同期ポート。NOTIFY=ASYN 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 (71 ページ)

DISABLE FIREWALL NOTIFY (72 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL (77 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL (90 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
ENABLE FIREWALL POLICY=policy [ACCOUNTING] [DEBUG={ALL|ARP|PACKET|PKT|
PROCESS}] [FRAGMENT={UDP|ICMP|OTHER}] [ICMP_FORWARDING={ALL|PARAMETER|
PING|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|UNREACHABLE}] [LOG={ALLOW|DENY|
DENYDUMP|INAICTMP|INALLOW|INAOOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|
INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|INDUDP|OUTAICTMP|
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。ARP (ARP Request の情報表示)、PKT、PACKET (パケット先頭 56 バイトのダンプ表示)、PROCESS (パケット処理過程の表示)、ALL (すべて) から選択する。

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。カンマ区切りで複数指定可能。デフォルトはすべて不透過。不透過の場合、再構成後の IP データサイズ (L4 パケットサイズ) が 1660 バイトを超えるか、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。透過の場合、再構成後サイズの制限はないが、フラグメントの数が SET FIREWALL MAXFRAGMENTS コマンドで設定した値 (デフォルトは 20 個) を超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_FORWARDING=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=myspolicy LOG=DENY
```

備考・注意事項

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すので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE FIREWALL (71 ページ)

DISABLE FIREWALL NOTIFY (72 ページ)

DISABLE FIREWALL POLICY (73 ページ)

ENABLE FIREWALL (77 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

SET FIREWALL MAXFRAGMENTS (83 ページ)

SHOW FIREWALL (90 ページ)

ENABLE FIREWALL POLICY IDENTPROXY

カテゴリー：ファイアウォール / ident プロキシー

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

ENABLE FIREWALL POLICY=*policy* IDENTPROXY

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

解説

ident プロキシー機能を有効にする。

ident プロキシーは、ファイアウォール有効時に、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 (75 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 (76 ページ)

SHOW FIREWALL (90 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 1660 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 (73 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL (90 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

SET FIREWALL POLICY=*policy* [TCPTIMEOUT=*minutes*] [UDPTIMEOUT=*minutes*]
[OTHERTIMEOUT=*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

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。

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

関連コマンド

DELETE FIREWALL SESSION (69 ページ)

SHOW FIREWALL POLICY (99 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

備考：本機能はサポート対象外です

```
SET FIREWALL POLICY=policy ATTACK={DOSFLOOD|FRAGMENT|HOSTSCAN|IPSPHOOF|
LAND|PINGOFDEATH|PORTSCAN|SMURF|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 |
| 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 |
| 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 |
| UDPATTACK | 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 |
| SMURF | 1 | 1 | 2 | 0 | SMURFATTACK |
| 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 個を超え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 164 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

SHOW FIREWALL POLICY ATTACK (106 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

```
SET FIREWALL POLICY=policy RULE=rule-id [PROTOCOL={protocol|ALL|GRE|OSPF|
SA|TCP|UDP}] [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] [AFTER=time] [BEFORE=time]
[DAYS=day-list]
```

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

rule-id: ルール番号 (1~299)

protocol: IP プロトコル番号 (0~255)

ipadd: IP アドレス

port: TCP/UDP ポート番号 (0~65535)

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)

解説

ファイアウォールルールの設定を変更する。

パラメーター

POLICY ファイアウォールポリシー名

RULE ルール番号

PROTOCOL IP プロトコル。定義済みのプロトコル名かプロトコル番号で指定。TCP、UDP を指定したときは、PORT パラメーターも必須

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。

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

備考・注意事項

「PROTOCOL=ALL」の意味は、アクション (ACTION) と ICMP 転送のオン・オフによって異なる。ICMP 転送がオフのときは、アクションに関係なく「PROTOCOL=ALL」は ICMP を含まない。ICMP 転送がオンのとき、ALLOW、DENY アクションでは「PROTOCOL=ALL」に ICMP を含まないが、NAT、NONAT アクションでは ICMP を含む。ICMP 転送のオン・オフは、ENABLE FIREWALL POLICY コマンド、DISABLE FIREWALL POLICY コマンドの ICMP_FORWARDING パラメーターで設定する。ルールの設定にあたっては、ルール (ルール番号) が下記の順序になるようにすること。異なる順序で設定した場合、ルールが正しく機能しないことがあるので注意。

1. 許可・拒否ルール (ACTION=ALLOW と ACTION=DENY)
2. アクセスリストを使用したルール
3. NAT・NONAT ルール (ACTION=NAT と ACTION=NONAT)

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 に自動的に応答する。

関連コマンド

ADD FIREWALL POLICY RULE (58 ページ)

DELETE FIREWALL POLICY RULE (68 ページ)

SHOW FIREWALL POLICY (99 ページ)

SHOW FIREWALL

カテゴリー：ファイアウォール / 一般コマンド

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 ..... 15251
  Peak ..... 0
  Active ..... 0

Policy : test
  TCP Timeout (s) ..... 3600
  UDP 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
  SIP ALG ..... disabled
  Number of Limitrules ..... 0
  Private Interface : vlan1
  Public Interface  : vlan2
  Method ..... dynamic
```

| | |
|------------------------------|---|
| 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。 |
| SIP ALG enabled | 未サポート |
| SNMP Session Report | 未サポート |
| Maximum Packet Fragments | 許可するフラグメントの最大数 |
| Sessions セクション | ファイアウォールセッション数の情報が表示される |
| Maximum | 最大セッション数 |
| Peak | ピーク時セッション数 |
| Active | 現在のセッション数 |
| 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 |
| Other Timeout (s) | TCP/UDP 以外のセッションの保持時間 |
| ICMP Unreachable Timeout (s) | 未サポート |
| TCP Handshake Timeout Mode | TCP 3 ウェイハンドシェイクにおける未確立 TCP セッションの処理モード。Syn Attack への対策として、未確立セッションに割り当てたリソースをどのように解放していくかを示す。Normal (通常のタイムアウト時間を使う)、Semi Aggressive (攻撃元と思われるホストとの未確立セッションには、通常より短いタイムアウト時間を適用)、Aggressive (すべての未確立セッションに通常より短いタイムアウト時間を適用) のいずれか |
| 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 |
| SIP ALG | 未サポート |
| Number of Limitrules | 未サポート |
| 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 (VLAN) |

| | |
|-----------------------|--|
| Public Interface | PUBLIC (外部) インターフェース名 (VLAN) |
| Method | PUBLIC-PRIVATE 間のパケット転送方式。dynamic (ダイナミックパケットフィルタリング) か passall (フィルタリングしない)。 |
| NAT | NAT の種別。standard (アドレス変換) か enhanced (アドレス・ポート変換)。以下、NAT 有効時のみ表示。 |
| NAT/Method | NAT の方式。static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか |
| NAT/Private Interface | NAT のプライベート側インターフェース |
| NAT/IP | NAT のプライベート側 IP アドレス |
| NAT Global IP | NAT のグローバル側 IP アドレス |

表 17:

関連コマンド

ADD FIREWALL POLICY INTERFACE (51 ページ)

CREATE FIREWALL POLICY (63 ページ)

DELETE FIREWALL POLICY INTERFACE (65 ページ)

DESTROY FIREWALL POLICY (70 ページ)

DISABLE FIREWALL (71 ページ)

ENABLE FIREWALL (77 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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ING記録を表示する。

アカウントING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

アカウントリ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 (73 ページ)

ENABLE FIREWALL POLICY (79 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 (55 ページ)

ADD FIREWALL POLICY RULE (58 ページ)

SHOW FIREWALL POLICY (99 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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。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) から選択する。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 (72 ページ)

ENABLE FIREWALL NOTIFY (78 ページ)

SHOW FIREWALL ACCOUNTING (93 ページ)

SHOW FIREWALL POLICY (99 ページ)

SHOW FIREWALL SESSION (108 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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

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

解説

ファイアウォールポリシーの詳細な設定情報・統計情報等を表示する。

パラメーター

POLICY ファイアウォールポリシー名

COUNTER 統計カウンター情報を表示する。

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。

入力・出力・画面例

```
Manager > show firewall policy

Policy : fish
TCP Timeout (s) ..... 3600
UDP Timeout (s) ..... 1200
Other Timeout (s) ..... 1200
TCP Handshake Timeout Mode ..... Normal
Accounting ..... disabled
Enabled Logging Options ..... inanother deny
Enabled Debug Options ..... none
Identification Protocol Proxy ..... disabled
Enabled IP options ..... none
Enhanced Fragment Handling ..... none
Enabled ICMP forwarding ..... unreachable ping timeexceeded
Receive of ICMP PINGS ..... enabled
Number of Notifications ..... 0
Number of Deny Events ..... 6
Number of Allow Events ..... 2560
Number of Active TCP Opens ..... 0
Number of Active Sessions ..... 9
Cache Hits ..... 111235
Discarded ICMP Packets ..... 0
SMTP Domains ..... not set
TCP Setup Proxy ..... enabled
```

SHOW FIREWALL POLICY

```

IP List : BadHosts
File name ..... accesslist.txt
Number IP hosts ..... 15
Number Networks ..... 0
Private Interface : vlan10
Rule ..... 1
  Action ..... deny
  Protocol ..... TCP
  Port ..... 137 - 139
  Global Port ..... all
  Days ..... all
Rule ..... 2
  Action ..... deny
  Protocol ..... UDP
  Port ..... 137 - 139
  Global Port ..... all
  Days ..... all
Rule ..... 3
  Action ..... deny
  Protocol ..... TCP
  Port ..... 445
  Global Port ..... all
  Days ..... all
Rule ..... 4
  Action ..... deny
  Protocol ..... UDP
  Port ..... 445
  Global Port ..... all
  Days ..... all
Public Interface : vlan20
Method ..... dynamic
Proxy ..... smtp
  Private Interface ..... eth0
  IP ..... 192.168.102.10
  Direction ..... both
  Days ..... all
NAT ..... enhanced
  Method ..... enhanced dynamic
  Private Interface ..... eth0
  Global IP ..... 200.100.10.1
Rule ..... 5
  Action ..... deny
  Protocol ..... TCP
  Port ..... 22
  Global Port ..... all
  Days ..... all

```

| Policy | ファイアウォールポリシー名 |
|-------------|----------------------|
| TCP Timeout | TCP セッションのタイムアウト (秒) |

| | |
|-------------------------------|--|
| UDP Timeout | UDP フローのタイムアウト (秒) |
| Other Timeout | TCP、UDP 以外のフローのタイムアウト (秒) |
| TCP Handshake Timeout Mode | TCP 3 ウェイハンドシェイクにおける未確立 TCP セッションの処理モード。Syn Attack への対策として、未確立セッションに割り当てたリソースをどのように解放していくかを示す。Normal (通常のタイムアウト時間を使う) Semi Aggressive (攻撃元と思われるホストとの未確立セッションには、通常より短いタイムアウト時間を適用) Aggressive (すべての未確立セッションに通常より短いタイムアウト時間を適用) のいずれか |
| 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、deny-dump、inaicmp、inallow、inaother、inatcp、inaudp、inddicmp、inddoother、inddtcp、inddudp、inddump、inddeny、indicmp、indother、indtcp、indudp、outaicmp、outallow、outaother、outatcp、outaudp、outddicmp、outddother、outddtcp、outddudp、outddump、outdeny、outdicmp、outdoother、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、arp、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 |
| 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 |
| 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。none、static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか。NAT 有効時のみ表示 |
| NAT/Private Interface | NAT のプライベート側インターフェース |
| NAT/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 |
| Radius Lookup | RADIUS サーバーを使用したルールの場合に enabled と表示される |
| 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側 IP 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 21:

| | |
|-------------|------------------------|
| Policy | ファイアウォールポリシー名 |
| TCP Timeout | TCP セッションのタイムアウト (秒) |
| UDP Timeout | UDP フローのタイムアウト (秒) |

| | |
|-------------------------------|---|
| Other Timeout | TCP、UDP 以外のフローのタイムアウト（秒） |
| TCP Handshake Timeout Mode | TCP 3 ウェイハンドシェークにおける未確立 TCP セッションの処理モード。Syn Attack への対策として、未確立セッションに割り当てたリソースをどのように解放していくかを示す。Normal（通常のタイムアウト時間を使う）、Semi Aggressive（攻撃元と思われるホストとの未確立セッションには、通常より短いタイムアウト時間を適用）、Aggressive（すべての未確立セッションに通常より短いタイムアウト時間を適用）のいずれか |
| 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、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、arp、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 | 自身宛での 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 |
| 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 |
| 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 |
| Method | PUBLIC-PRIVATE間のパケット転送方式。dynamic か passall |
| NAT | NAT の種別。standard (アドレス変換) か enhanced (アドレス・ポート変換)。NAT 有効時のみ表示 |
| NAT/Method | NAT の方式。none、static、dynamic、enhanced static、enhanced dynamic、enhanced interface のいずれか。NAT 有効時のみ表示 |
| NAT/Private Interface | NAT のプライベート側インターフェース |
| NAT/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 |
| Radius Lookup | RADIUS サーバーを使用したルールの場合に enabled と表示される |
| 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 22: COUNTER 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 23: LIST オプション

関連コマンド

ADD FIREWALL POLICY INTERFACE (51 ページ)
 ADD FIREWALL POLICY LIST (53 ページ)
 ADD FIREWALL POLICY NAT (55 ページ)
 ADD FIREWALL POLICY RULE (58 ページ)
 CREATE FIREWALL POLICY (63 ページ)
 DELETE FIREWALL POLICY INTERFACE (65 ページ)
 DELETE FIREWALL POLICY LIST (66 ページ)
 DELETE FIREWALL POLICY NAT (67 ページ)
 DELETE FIREWALL POLICY RULE (68 ページ)
 DESTROY FIREWALL POLICY (70 ページ)
 DISABLE FIREWALL NOTIFY (72 ページ)
 DISABLE FIREWALL POLICY (73 ページ)
 ENABLE FIREWALL NOTIFY (78 ページ)
 ENABLE FIREWALL POLICY (79 ページ)
 SET FIREWALL POLICY RULE (88 ページ)
 SHOW FIREWALL (90 ページ)
 SHOW FIREWALL EVENT (97 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

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 : test
```

```
Current Attack Setup
```

| Attack | In Trigger | Out Trigger | 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 24:

関連コマンド

SET FIREWALL POLICY ATTACK (85 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

備考：フィーチャーライセンス AT-FL-02 または AT-FL-02-B が必要

SHOW FIREWALL SESSION[=*session-id*] [*POLICY=policy*] [*COUNTER*]
 [PORT={*port*[-*port*]|*port-name*}] [*PROTOCOL*={|*protocol*|ALL|ICMP|OSPF|TCP|
 UDP|}] [*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 カウンター情報を表示する。

PORT TCP/UDP ポート番号またはサービス名。ハイフン区切りで範囲指定が可能。指定時は、該当ポート/サービスを使用するセッションだけが表示される。

PROTOCOL IP プロトコル。指定時は該当プロトコルのセッションだけが表示される。

SUMMARY サマリー情報を表示する。

入力・出力・画面例

```
Manager > show firewall session
```

```
Policy : tuna
```

```
Current Sessions
```

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



```

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

```

Manager > show firewall session counter

Policy : net

Current Sessions

```

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

```

| |
|-------|
| ----- |
|-------|

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

表 25:

関連コマンド

DELETE FIREWALL SESSION (69 ページ)

SHOW FIREWALL EVENT (97 ページ)

SHOW FIREWALL POLICY (99 ページ)