

BA8000 Pro
静的IPフィルタリング設定ガイド

BA8000 Pro
株式会社NTT-ME

はじめに

- ・本ガイドはBA8000 Proの静的IPフィルタリング機能の設定方法を説明したものです。
- ・誤ったフィルタを設定すると通信に支障をきたす場合がありますので静的フィルタの設定は十分注意して行って下さい。
 - 通信機会を逃したために生じた損害等の純粋経済的損失については当社はその責任を一切負いませんのでご注意ください。
- ・BA8000 Proでは静的フィルタ機能以外にセキュリティを向上させるための動的フィルタ機能としてダイナミックフィルタリング機能とステートフルパケットインスペクション(SPI)機能を搭載しています。ダイナミックフィルタは「指定したパケットが検出された時に、指定されたパケットを通す」という動作をします。このきっかけとなるフィルタを「トリガ」、トリガによって通過を許可されるフィルタを「アクション」と呼びます。ダイナミックフィルタリング機能は静的フィルタに優先して働きます。したがって、静的フィルタで塞いだポートを動的に開閉するといった場合に使用します。

一方のSPIは各々の通信状態(IPアドレスやシーケンス番号)を記憶し、次に来るべきパケットを予測した上で受信パケットとその予測を比較・検査し不正なパケットと判断された場合は破棄する機能です。ヘッダ情報に基づいたパケットの選別のみしか行わない静的パケットフィルタリングと比較してセキュリティレベルをより一層向上させることができます。これらの機能は静的IPフィルタのセキュリティ機能を補完するものですので必要に応じて両者を併用してご使用ください。

通常LAN WAN方向のSPIは不要です。WAN LAN方向のみ有効にしてご使用ください。LAN WAN方向のSPIを有効にした場合スループットが著しく低下する場合がありますのでご注意ください。

- ・不正アクセス検知機能により送信元・送信先IPアドレスが不正なIP Spoofing攻撃を防御することができます。不正アクセス検知機能はステートフルパケットインスペクションを有効にすることにより機能します。
- ・セキュリティレベルを高めるためには使用する端末のOSやソフトの適切なバージョンアップや適切な運用を行うことが重要です。常に新しい情報を入手し、自己責任において運用を行うようにしてください。
- ・メールの添付ファイルで進入するウィルスは防御できません。端末にウィルス対策ソフトをインストールする等の対策を実施してください。

更新履歴

修正初版 2002年12月24日

BA8000 Proの静的フィルタ機能について

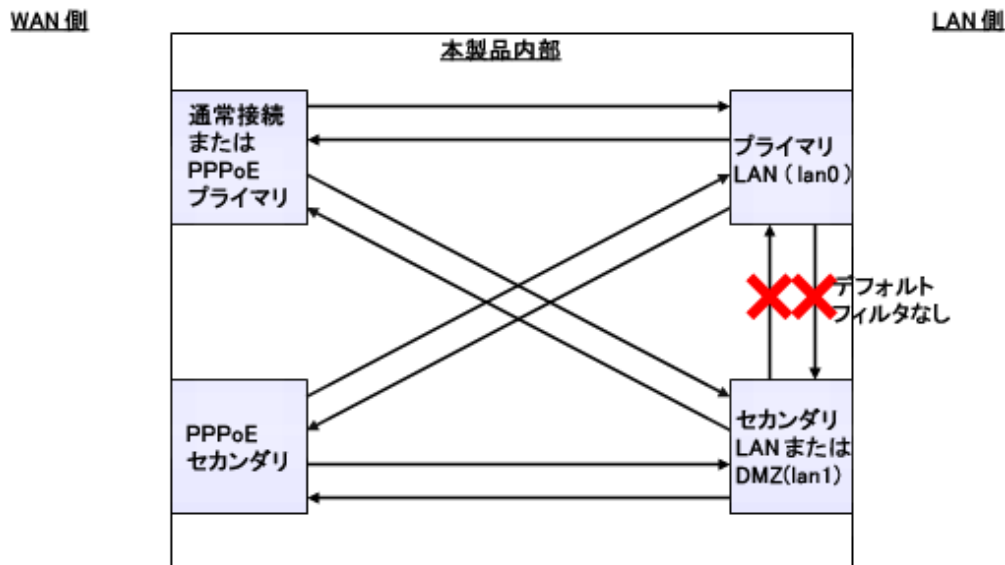
静的フィルタ機能はIPパケットのヘッダ情報に基づいて定常的にパケットの透過/廃棄処理を行う機能です。LAN側の2つの論理インターフェース(LAN0, LAN1)に対して各アカウントのWAN LAN, LAN WAN方向のフィルタを登録することができます。

- ・プロトコル、送信元・送信先IPアドレス、送信元・送信先ポート、tcpフラグでのパケットフィルタリングが可能です。
- ・工場出荷時の静的フィルタの設定ではID:64にすべてを“透過”するエントリを設定しています。このエントリを削除した場合、全てのパケットは遮断されますのでご注意ください。
- ・IDの小さいエントリが優先的に処理されます。
- ・各接続アカウント/方向/LAN論理インターフェース毎に最大64エントリ設定可能です。
- ・静的IPマスカレード機能でも同様の効果がありますので必要に応じて併用してご使用下さい。
- ・送信元、送信先IPアドレスとしてローカルIPアドレス、グローバルIPアドレスいずれを指定することも可能です。LAN側ポートに接続している端末に割り当てたアドレスをそのまま送信元、送信先IPアドレスとして設定してください。
- ・本製品自身のシステム部から送信されるNTP、DHCP、DNSなどのパケットはフィルタ対象にすることはできません。

BA8000 Proの静的フィルタの仕組み

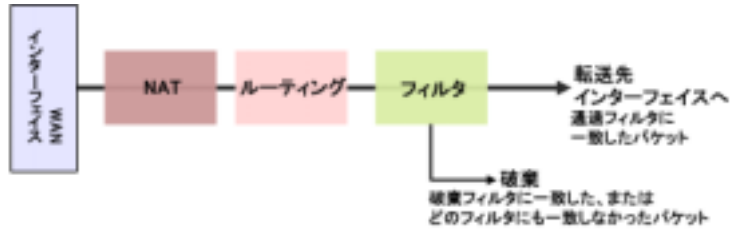
BA8000 ProではWAN側論理インターフェースとしてプライマリ、セカンダリPPPoEセッション、LAN側論理インターフェースとしてプライマリ、セカンダリLANインターフェースを設定することができます。フィルタの組み合わせとしては下図の10通りのフィルタを設定することができます。

このうち、プライマリLAN(lan0)とセカンダリLAN(lan1)間は工場出荷時の設定で遮断されています。これ以外はID64に全てを透過させるエントリがデフォルトで設定されています。プライマリLAN、セカンダリLAN間で通信を行う場合はlan0 lan1に透過のエントリを投入してください。

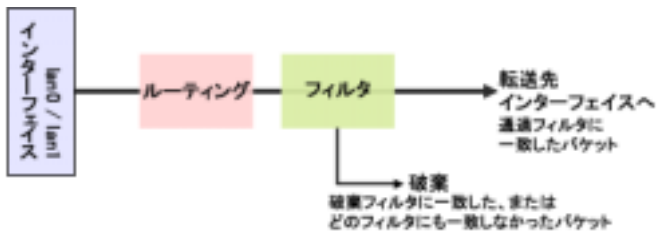


本製品のフィルタ機能は下記のような処理で作用します。

WAN LAN方向の packets の処理はNAT(アドレス変換)、ルーティング処理、フィルタリングの順に行いますのでNAPT端末に対してフィルタの設定を行う場合やマルチNATでグローバル ローカルのアドレス変換を行う際には変換後のローカルアドレスを送信先アドレスとして指定してください。

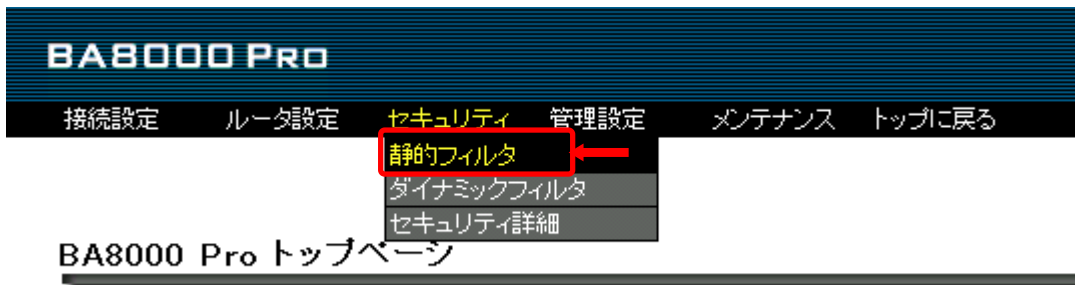


一方LAN WAN方向の packets の処理はルーティング処理、フィルタリングの順になります。



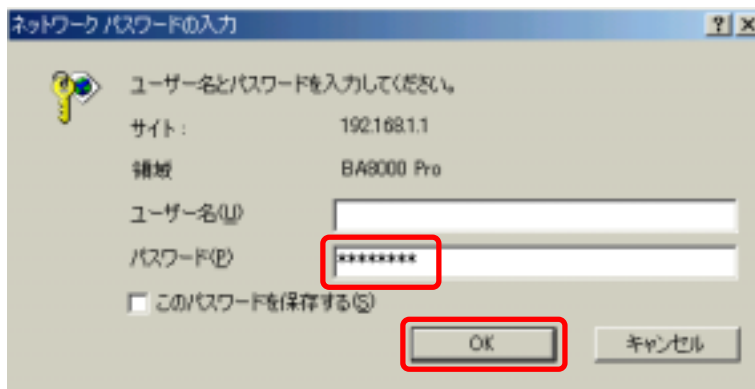
静的フィルタ設定手順

1. WebブラウザのURL欄に「http://192.168.1.1/」と入力し「Enter」キーを押します。
BA8000 Pro設定画面のトップページが表示されますので**[セキュリティ]**の**[静的フィルタ]**を選択して下さい。



ユーザ名/パスワード入力画面が表示されます。パスワード欄に「password」を入力し**[OK]**ボタンをクリックします。

上記は工場出荷時のパスワードです。パスワードを変更している場合は設定してあるパスワードを入力してください。



- 静的フィルタ設定画面で **[アカウント/方向選択]** から設定したい方向を選択し、**[静的フィルタの追加]** をクリックします。

静的フィルタ ?

静的フィルタの設定を行います。

アカウント/方向選択 plala -> LAND ▼

静的フィルタID	動作	プロトコル	tcp フラグ	送信元 アドレス	送信元 ポート	送信先 アドレス	送信先 ポート	修/削
64	pass	*		*	*	*	*	修正 削除

静的フィルタの追加

設定 やり直し

- [静的フィルタの追加/修正]** の各項目を設定して静的フィルタのエントリを作成してください。最後に**[設定]** ボタンを押してください。

静的フィルタの追加/修正 ?

静的フィルタの追加/修正を行います。

静的フィルタID	<input type="text" value="63"/>
動作	<input type="text" value="破棄"/>
プロトコル	<input type="text" value="tcp&udp"/>
tcpフラグチェック	<input type="text" value="tcpフラグチェックしない"/>
tcpフラグ	<input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin
送信元IPアドレス	<input type="text" value="*"/>
送信元ポート	<input type="text" value="137-139"/>
送信先IPアドレス	<input type="text" value="*"/>
送信先ポート	<input type="text" value="*"/>

設定 戻る

ID

静的フィルタのエントリーのID番号を表示します。小さいID番号の番号のエントリが優先処理されます。デフォルトで ID:64にすべてを透過するエントリを設定しています。特定のトラフィックを遮断したい場合はこれより小さいID番号で遮断させるエントリの投入を行ってください。

動作

そのエントリに該当するパケットが検出された場合のBA8000 Proの処理動作を表示します。

- 透過 : そのフィルタに該当されるパケットを通過させます。
- 透過(ログ): そのフィルタに該当されるパケットを通過させ、かつ記録をログ出力します。
- 破棄 : そのフィルタに該当するパケットを破棄します。
- 破棄(ログ): そのフィルタに該当されるパケットを破棄し、かつ記録をログ出力します。

プロトコル

フィルタの対象となるプロトコルを表示します。tcp, udp, tcp&udpの場合は以下の**[フラグ]**や**[ポート]**も関連します。

- * (すべて) : すべてのパケットが対象になります。
- icmp : icmpパケット(pingなど)が対象になります
- tcp : tcpパケットが対象になります。(, , , を設定してください)
- udp : udpパケットが対象になります。(, , を設定してください)
- tcp&udp : tcpとudpパケットが対象になります。(, , , を設定してください)

tcpフラグチェック

プロトコルが「tcp」または「tcp&udp」の場合に、tcpフラグに関するルールを設定します。

[tcpフラグチェックしない]

フラグをルールに加えません。通常はこれを選択してください。以下の<tcpフラグ>は設定しないでください。

[以下のtcpフラグを持つパケットをフィルタ対象とする]

以下の<tcpフラグ>で選択したフラグを持つパケットをフィルタ対象とします。

[以下のtcpフラグだけを持つパケットをフィルタ対象とする]

以下の<tcpフラグ>で選択したフラグだけを持つパケットをフィルタ対象とします

tcpフラグ

上記**[プロトコル]**欄が**[tcp]**または**[tcp&udp]**の場合、ここに示されたすべてのtcpフラグを持つパケットがフィルタの対象になります。指定がない場合はフラグの状態は関係ありません。

tcpフラグ : <tcpフラグチェック>で選択したルールに基づいて、「urg」「ack」「psh」「rst」「syn」「fin」の中から適切なものにチェックを入れます。

送信元IPアドレス

フィルタの対象となる送信元IPアドレスを表示します。

送信元IPアドレス(例)	説明
*	すべてのIPアドレス
192.168.1.3	特定のホストアドレス
192.168.1.0/24	ネットワークアドレス(24ビットマスク)
192.168.1.3-192.168.1.33	範囲指定 スペース無しでハイフン“-”区切り
192.168.1.3, 192.168.1.8	列挙指定 スペース無しで“,”区切り(3つまで)*

送信元ポート

上記[プロトコル]欄が[tcp][udp]または[tcp&udp]の場合、フィルタの対象となる送信元ポートを表示します。

送信元ポート(例)	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“-”区切り
80,8080	列挙指定 スペース無しで“,”区切り(3つまで)*

送信先IPアドレス

フィルタの対象となる送信先IPアドレスを入力します。IPアドレスの指定方法は、送信元IPアドレス例を参照してください。

送信先ポート

上記[プロトコル]欄が[tcp][udp]または[tcp&udp]の場合、フィルタの対象となる送信元ポートを表示します。ポートの指定方法は、送信元ポート例を参照してください。

送信元IPアドレス(例)	説明
*	すべてのIPアドレス
192.168.1.3	特定のホストアドレス
192.168.1.0/24	ネットワークアドレス(24ビットマスク)
192.168.1.3-192.168.1.33	範囲指定 スペース無しでハイフン“-”区切り
192.168.1.3, 192.168.1.8	列挙指定 スペース無しで“,”区切り(3つまで)*

3. 設定内容を確認し、最後に**[設定]**ボタンをクリックしてください。

静的フィルタ



静的フィルタの設定を行います。

アカウント/方向選択

plala -> LAN0

静的フィルタID	動作	プロトコル	tcp フラグ	送信元 アドレス	送信元 ポート	送信先 アドレス	送信先 ポート	修/削
63	discard	udp&tcp		*	137-139	*	*	修正 削除
64	pass	*		*	*	*	*	修正 削除

静的フィルタの追加

設定

やり直し

静的フィルタ設定例

凡例

WAN : 実際の表示は、設定したアカウント名が表示されます。
 LAN0 : プライマリLAN
 LAN1 : セカンダリLAN

[設定例1] Windowsで使用するNetBios系のトラフィックを遮断するフィルタ設定

方向: LAN0 WAN、 LAN1 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	137-139
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	137-139	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

方向: WAN LAN0、 WAN LAN1

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	137-139
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	137-139	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例2] Windowsで使用するSMBサービスのトラフィックを遮断するフィルタ設定

方向: LAN0 WAN、 LAN1 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	445
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	445	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

方向: WAN LAN0、 WAN LAN1

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	445
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	445	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例3] LAN0及びLAN1においてWindowsで使用するMicrosoft DCE Locatorサービスのトラフィックを遮断するフィルタ設定

方向:LAN0 WAN、 LAN1 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	135
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	135	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

方向:WAN LAN0、 WAN LAN1

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	*	135
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	135	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例4] LAN0内の特定の端末(LAN0:192.168.1.10)のインターネット接続を禁止するフィルタ設定

方向:LAN0 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
63	遮断	*	Tcpフラグチェックしない	192.168.1.10	*	*	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例5] LAN0内の特定の端末(LAN0:192.168.1.10)のみインターネット接続を許可するフィルタ設定

方向:LAN0 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
63	通過	*	Tcpフラグチェックしない	192.168.1.10	*	*	*
64	遮断	*	Tcpフラグチェックしない	*	*	*	*

[設定例6] LAN0内の特定の端末(LAN0:192.168.1.10)のWebアクセスを禁止するフィルタ設定

方向:LAN0 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
63	遮断	Tcp&udp	Tcpフラグチェックしない	192.168.1.10	*	*	80
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例7] LAN0内の特定の端末(LAN0:192.168.1.10)のWebアクセスのみ許可するフィルタ設定

方向:LAN0 WAN

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
63	許可	Tcp&udp	Tcpフラグチェックしない	192.168.1.10	*	*	80
64	遮断	*	Tcpフラグチェックしない	*	*	*	*

[設定例8] LAN0内のサーバ端末(LAN0:192.168.1.10)へのWAN側からのアクセスはWebアクセスのみ許可するフィルタ設定

方向:WAN LAN0

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
62	透過	Tcp&udp	Tcpフラグチェックしない	*	*	192.168.1.10	80
63	遮断	Tcp&udp	Tcpフラグチェックしない	*	*	192.168.1.10	*
64	通過	*	Tcpフラグチェックしない	*	*	*	*

[設定例9] LAN0上の端末からLAN1の端末へアクセスを許可するフィルタ設定

方向:LAN0 LAN1

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
64	通過	*	Tcpフラグチェックしない	*	*	*	*

方向:LAN1 LAN0

ID	動作	プロトコル	Tcpフラグ	送信元		送信先	
				IPアドレス	ポート	IPアドレス	ポート
64	通過	*	Tcpフラグチェックしない	*	*	*	*

静的フィルタ機能をご利用いただく上での注意事項

- ・IPマスカレード(NAPT)端末のみ使用する場合はWAN LAN方向の通信に対しては通常、静的フィルタの設定を行う必要はありません。(NAPTが簡易ファイアウォールとして機能します)
- ・WAN LAN方向の静的フィルタの設定が必要になるのは以下の端末に対してです。
静的IPマスカレード、マルチNATによりポートフォワーディングの設定を行った端末
DMZネットワーク内の端末
- ・静的フィルタのエントリ数が多いほどスループットが低下します。エントリ数を極力少なくするように設定を行ってください。
- ・DMZネットワークに対するフィルタはlan1のインターフェースを指定して設定してください。
- ・多くのフィルタでログ記録を指定した場合やログ記録を指定したフィルタに該当するパケットが多い場合大量のログが生成されることによりスループットが低下したり、ログの内容が頻繁に書き換わる等の弊害を生じます。ログを記録するフィルタは極力少なくしてください。
- ・異なる接続アカウント/方向や、誤ったフィルタを設定すると通信に支障をきたす場合がありますので、静的フィルタの設定は十分に注意して行ってください。
- ・送信元IPアドレスが不正なIP Spoofing攻撃に対しては本製品の不正アクセス検知機能により防御することができます。

[付録] tcp, udpで使用するポート番号一覧

ポート番号	説明
20	ftp(Default Data)
21	ftp(Control)
23	telnet
25	smtp
53	dns
70	gopher
79	finger
80	http
110	pop3
113	ident
119	nntp
123	ntp
194	irc
443	https