SOHO router construction with FreeBSD

FreeBSD による SOHO ルータ構築

Version 1.5

保証免責
本書は記載事項またはそれに関わる事項について、明示的あるいは暗黙的な保証はいたしておりません。
したがいまして、これらを原因として発生した損失や損害についての責任を負いません。

表記について

本書では以下の書体を使用しています。

- イタリック文字

  本文中でのコマンド、ファイル名、変数など可変なパラメータ値を表します。

- 等幅文字

  ファイルの内容やコマンドの入出力例に使います。入力の場合にはボールドで表します。

```
$ cd /usr/src/sys/i386/conf
$ ls
GENERIC         Makefile      OLDCARD       SMP
GENERIC.hints   NOTES         PAE           gethints.awk
$
```

- 省略文字

  ファイルの内容やコマンドの入出力例を省略する場合に'...'を使います。

```
$ vi /etc/rc.conf
  ...
sshd_enable="YES"
named_enable="YES"
  ...
$
```

- プロンプト

  一般または、管理権限を持った実行環境をそれぞれ、'$'(ドル)、'#'(シャープ)のプロンプトで表します。

```
$ su
Password: root's passwd
#
```

目次

1. 概要

本書は安価にインターネット接続環境を構築するため、SOHO ルータの諸元、構築の手順、および後々のカスタマイズ等の情報について記述したものです。

本ルータは、主に以下のサービスを提供します。

- 広帯域、かつ NAPT による複数 PC のインターネット接続性。
- パケットフィルタリングによるアクセスコントロール。
- DHCP によるプライベートアドレスの配布。
- DNS によるアドレス解決機能。

1.1. 本書の目的

本書の目的は、第一に本ルータに関する系統だった情報を提供するためです。設置場所、ルータ諸元、ソフトウェアの実装と設定内容について記述することにより、本ルータのより具体的な構成を把握しやすく努めました。

第二に、変更された設定内容等について履歴を残すためです。すなわち、本書は実際のルータ構成状態と違わぬようにドキュメント保守を推奨するものとします。

第三に、本ルータになんらかの障害が発生した場合に対して管理者、または保守業者への連絡を円滑にするためです。これにより、障害による対応が迅速に行えることを目的としました。

1.2. 対象とする読者

Unix の一般的コマンド、および管理コマンドを使用することができ、vi による編集が可能であることを想定しています。また、実装される各ソフトウェアについて熟知してればなおよいでしょう。本書では、ソフトウェア上の設定に関して、*parameter = value* といった実際の設定情報についてのみ記述します。繰り返しになりますが、これらの設定情報についての詳細は関連マニュアルを参照するべきでしょう。

2. サーバ構成

2.1. 機種情報

機種情報

機種型番	GATEWAY G6-200
ホスト ID	
シリアル番号	
管理番号	

2.2. ハードウェア情報

ハードウェア情報

アーキテクチャ	IA-32
マザーボード	Intel VS440FX (socket8) OEM by Vinus
CPU	PentiumPro 200MHz 82440FX
メモリ	72pin SIMM 32MB × 2
シリアルポート	RS-232C シリアル(D-Sub9 ピン/オス) × 2
ディスク	Western Digital WDC AC21600H × 1(1.5GB)
CD-ROM	TOSHIBA CD-ROM XM-5602B × 1

2.3. ソフトウェア情報

ソフトウェア情報

ホスト名	Masami							
OS	FreeBSD 5.1-RELEASE							
パーティション		**size**	**offset**	**fstype**	**fsize**	**bsize**	**bps/cpg**	**mount**
	a:	307200	0	4.2BSD	2048	16384	19208	/
	b:	262144	307200	swap				swap
	c:	3173121	0	unused	0	0		
	d:	409600	569344	4.2BSD	2048	16384	25608	/var
	e:	1638400	978944	4.2BSD	2048	16384	28552	/usr
	f:	555777	2617344	4.2BSD	2048	16384	34744	/home
パッチ								
ルートパーティション	/dev/ad0s1a							
その他								

2.4. ネットワーク情報

ネットワーク情報

IP アドレス	fxp0: (インターネット側 I/F) pcn0: 172.16.1.1/26 (公開セグメント I/F) fxp1 192.168.253.1/24 (社内セグメント側 I/F) ng0: プロバイダから割当てられるグローバル IP アドレス (インターネット側仮想 I/F)
イーサネットアドレス	fxp0: 00:02:b3:5e:de:6b pcn0: 00:90:99:18:44:8d fxp1: 00:90:27:af:32:69
デフォルトルート	プロバイダ側の対向グローバル IP アドレス
NIS/NIS+ドメイン	なし
DNS ドメイン	hoge.net

2.5. 拠点情報

拠点情報

設置場所	

2.6. 保守情報

保守情報

保守業者	なし

3. ルータ構築情報

3.1. ディストリビューション選択

「Custom」メニューより、以下のディストリビューションを選択しました。

選択したディストリビューション

base	バイナリ基本ディストリビューション(必須)
crypto	基本暗号サービス
doc	その他の FreeBSD オンラインドキュメント
Info	GNU info
man	システムマニュアル
src	全てのソースファイル

3.2. カーネル再構築

/usr/src/sys/i386/conf の GENERIC ファイルをバックアップしてから再構築します。設定内容は、添付資料 **A. カーネルパラメータ**を参照してください。再構築に使用するパラメータファイルは router と命名し、以下のようにカーネルを再構築しました。

```
# cd /usr/src/sys/i386/conf
# config router
Kernel build directory is../compile/router
Don't forget to do a ``make depend''
# cd ../compile/router
# make depend
# make
# make install
# shutdown –r now
```

3.3. ポートコレクション

最新、かつ必要なポートだけをインストールします。最低限 make 作業に必要なものとして、以下のファイルをコピーしました。

make に必要なファイル

/usr/ports/Mk/*	関連 makefile 一式
/usr/ports/Templates/*	makefile から参照されるスクリプト

インストールしたポート

/usr/ports/net/isc-dhcp3	DHCP サーバツール
/usr/ports/net/mpd	netgraph 対応 PPPoE クライアントツール

ポートは、http://www.freebsd.org/ports/index.html 等からダウンロード可能です。

3.4. デーモン

サービス提供に必要と思われる以下のデーモンのみ起動します。OS 起動時のデーモン制御は添付資料 **B. rc.conf 設定パラメータ**を参照してください。

起動デーモン

/sbin/ipmon	パケットロギング・デーモン	
/usr/sbin/named	ネームサーバ (ISC BIND)	8.3.4-REL
/usr/sbin/sshd	SSH デーモン (OpenSSH)	3.6.1p1
/usr/local/sbin/dhcpd	DHCP サーバ (ISC DHCP)	3.0.1rc12
/usr/local/sbin/mpd	netgraph マルチリンク PPP デーモン	3.16
sendmail	SMTP サーバ	8.12.9

3.5. ルーティング

VPN 接続用に 1 つ静的経路を設定しました。

```
# vi /etc/rc.local
route add -net 192.168.243.0 -netmask 255.255.255.0 192.168.253.5
  ...
```

これにより、VPN 接続時には社内セグメントにおける ipfilter のフィルタルールに準じて通信可能となります。

3.6. 時刻同期

社内セグメントの NTP サーバは、tadashi が担当しています。本ルータは、ntpupdate で周期的に時刻同期を行います。

```
# vi /etc/crontab
  ...
0      *      *      *      *      root    ntpdate -s -b tadashi
  ...
```

1 時間毎に cron によって時刻調整が行われ、ntpdate の処理結果は/var/log/messages ファイルに出力されます。

3.7. syslog

基本的にはデフォルト設定としますが、dhcpd、および mpd のログを採取する設定を追加しました。

```
# vi /etc/syslog.conf
  ...
local7.*      /var/log/dhcpd.log
!mpd
*.*           /var/log/mpd.log
  ...
```

3.8. ログ・ローテーション

基本的にはデフォルト設定としますが、ipmon、dhcpd、named、および mpd のログ・ローテーション設定を追加しました。

```
# vi /etc/newsyslog.conf
  ...
/var/log/ipf.log    640   7   *   @T00   J   /var/run/ipmon.pid
/var/log/dhcpd.log  640   5   *   @T00   J
/var/log/named.log  640   5   *   @T00   J   /var/run/named/pid
/var/log/mpd.log    640   5   *   @T00   J
  ...
```

/var/log/ipf.log ファイルを例にすると、毎日 0 時に bzip2 形式にバックアップし、過去 8 日分のログを保存します。そして、/var/run/ipmon.pid ファイル内の PID にハングアップシグナルを送り、ipmon にログがローテートされたことを通知する、という意味になります。

3.9. シリアル接続

COM1 ポートのみシリアル接続が可能となるように設定を変更しました。

```
# vi /etc/ttys
  ...
ttyd0   "/usr/libexec/getty std.9600"  vt100   on  secure
ttyd1   "/usr/libexec/getty std.9600"  dialup  off  secure
ttyd2   "/usr/libexec/getty std.9600"  dialup  off  secure
ttyd3   "/usr/libexec/getty std.9600"  dialup  off  secure
  ...
# kill -HUP 1
```

3.10. 仮想コンソール

基本的にコンソールはシリアル接続で利用しますが、これが利用できない場合を考慮して、1 つだけ仮想コンソールを用意するよう設定を変更しました。

```
# vi /etc/ttys
  ...
ttyv0   "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv1  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv2  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv3  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv4  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv5  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv6  "/usr/libexec/getty Pc"        cons25  on  secure
#ttyv7  "/usr/libexec/getty Pc"        cons25  on  secure
  ...
# kill -HUP 1
```

3.11. rcorder

ipmon の起動順序を変更しました。先に ipmon が起動した後に、cleanvar が実行されると ipmon.pid ファイルが削除される不具合を解消するためです。

```
# vi /etc/rc.d/ipmon
  ...
# REQUIRE: mountcritlocal hostname sysctl cleanvar
  ...
```

4. PPPoE サービス構築

4.1. サービス概要

PPPoE クライアントとして、Powered Internet からユーザ認証を経てグローバルアドレスを取得し、Internet へ接続できるようにします。

4.2. mpd 構築方法

ポートを入手後、tar ボールを/usr/ports/net ディレクトリへ展開します。
mpd ディレクトリ作成後、make install を行います。

インストール後は、/usr/local/etc/mpd ディレクトリの mpd.conf、mpd.link、mpd.secret ファイルを設定します。設定内容は、添付資料 **C. mpd 設定パラメータ**を参照してください。

/usr/local/etc/rc.d/mpd.sh の rc スクリプトを以下のように修正します。

```
# vi /usr/local/etc/rc.d/mpd.sh
  ...
    else
      "${DAEMON}" -b -p "${PIDFILE}"
      echo " mpd"
      sleep 2
      /etc/rc.d/ipfilter resync
    fi
  ...
```

mpd が起動する前に、rcorder により ipfilter が先に起動しているため、mpd によって取得されたグローバル IP アドレスを ipfilter のルールと同期させる必要があります。
また、mpd の起動にはすこし時間がかかるので、sleep させてから同期させています。

5. DHCP サービス構築

5.1. サービス概要

PC を社内ネットワークに接続した場合に、プライベート IP アドレス、デフォルトルート等、ネットワーク情報の自動配布を行います。

5.2. isc-dhcpd3 構築方法

ポートを入手後、tar ボールを/usr/ports/net ディレクトリへ展開します。isc-dhcp3-server ディレクトリ作成後、make install を行います。

インストール後は、/usr/local/etc ディレクトリの dhcpd.conf、rc.isc-dhcpd.conf ファイルを設定します。設定内容は、添付資料 **D. dhcpd 設定パラメータ**を参照してください。

5.3. 付記事項

1) リース時間を大幅に長く変更しました。
   NetScreen-Remote で社内から VPN 接続を行うと、リース延長時にインタフェース喪失が検出され、VPN 接続が切断される問題を解決するためです。
2) PXE クライアントに対応しました。
   ネットワーク経由で Linux ブートローダを起動するためです。

6. パケットフィルタリング/NAPT サービス構築

6.1. サービス概要

Internet から到達する不必要なパケットのフィルタリングや、各 PC が Internet に接続できるよう NAPT を行います。また、ドロップされたパケットのログを取得します。

6.2. ipfilter/ipnat/ipmon 構築方法

ipfilter、ipnat、ipmon はカーネルに組み込まれた機能として動作します。

4.2. カーネルの再構築により、関連パラメータを有効化してください。

/etc/ipf.rules、/etc/ipnat.rules ファイルを設定します。設定内容は、添付資料 **E. ipfilter/ipnat 設定パラメータ**を参照してください。

また、ipfilter のフィルタリングルールでログ指定がある場合に、指定ファイルへのログ出力が可能となるように設定を行いました。

6.3. 付記事項

mpd を再起動した場合には、ipfilter のルールに対しても同期しなければなりません。同期させるには、以下のコマンドを実行します。ipnat の NAPT テーブルもクリアした方がよいでしょう。

```
# /sbin/ipf -y
filter sync'd
# /sbin/ipnat -CF -f /etc/ipnat.rules
23 entries flushed from NAT table
9 entries flushed from NAT list
```

mpd は ng0 インタフェースに対向のグローバルアドレスを割当てますが、ipfilter、ipnat では ng0 インタフェースに割当てられた IP アドレスを内部的にマップしているため、同期が必要になります。ipfilter のルールを変更した場合には、以下のように反映する必要があります。

```
# /sbin/ipf -Fa -f /etc/ipf.rules
# /sbin/ipnat -CF -f /etc/ipnat.rules
11 entries flushed from NAT table
2 entries flushed from NAT list
```

6.4. 付記事項

1) IPSec/IKE パケットを通過できるように変更しました。
2) Lucent IPSec パケットを通過できるように変更しました。

7. 遠隔ログインサービス構築

7.1. サービス概要

sshd による遠隔ログインが行えるようにします。

7.2. sshd 構築方法

OS インストール時に **4.1 ディストリビューションの選択**で base を選択すると sshd が自動的にインストールされます。

/etc/ssh/sshd_config ファイルを設定します。設定内容は、添付資料**F. sshd 設定パラメータ**を参照してください。

基本的にはパスワード認証を拒否し、公開鍵認証によるログインを許可します。ログインするためには、接続するクライアントのプロトコルヴァージョン 1 の RSA、プロトコルヴァージョン 2 の RSA、または DSA 公開鍵が本ルータにコピーされていなければなりません。

8. ネームサービス構築

8.1. サービス概要

社内、および公開セグメントの名前解決に関して、スレーブとして動作するようにします。

8.2. named 構築方法

OS インストール時に **4.1 ディストリビューションの選択**で base を選択すると named が自動的にインストールされます。

/etc/namedb/named.conf ファイルを設定します。設定方法は、添付資料 **G. named 設定パラメータ**を参照してください。

8.3. 付記事項

1) 本ルータはスレーブとして動作します。
   マスタは Windows2000 上で動作する DNS サービスです。マスタはゾーンの動的更新をサポートしており、ゾーンが変更されるとスレーブに変更通知を行います。それに伴い、スレーブはゾーン転送をマスタへ要求します。

9. メール配信サービス構築

9.1. サービス概要

本来、本ルータが提供するサービスではありませんが、自身のステータスチェック用メールを配信できるようにします。

9.2. sendmail 構築方法

OS インストール時に **4.1 ディストリビューションの選択**で base を選択すると sendmail が自動的にインストールされます。

/etc/mail ディレクトリ以下の submit.cf、service.switch ファイルを設定します。

submit.cf ファイル

パラメータ	用途
D{MTAHost}[mx.hoge.net]:[mail.hoge.net]	本ルータからメール送信する場合の MTA を定義する。

service.switch ファイル

パラメータ	用途
hosts　files	名前解決にネームサーバを使用しない。 このため hosts ファイルに自身の FQDN を決定できるエントリを追加する必要がある。

9.3. 付記事項

1) メールサーバの冗長化に伴い、設定変更しました。
   submit.cf の設定により、最初に mx.hoge.net へ接続を試み、セッションが確立しなければ mail.hoge.net へ接続を試みます。

A. カーネルパラメータ

表 A-1 router ファイル

パラメータ	用途
machine i386	
cpu i686_CPU	
ident router	
options SCHED_4BSD	
options INET	IPv4 ネットワーク機能
options FFS	
options SOFTUPDATES	ファイルシステムの高速化
options MD_ROOT	/パーティション用メモリディスクの使用
options COMPAT_43	BSD4.3 の互換性保持(必須)
options NETGRAPH	netgraph 基本コードをカーネルに含める
options NETGRAPH_ETHER	
options NETGRAPH_PPPOE	netgraph に対応した PPPoE を使用
options NETGRAPH_SOCKET	netgraph に対応した socket(2)を使用
options IPFILTER	パケットフィルタ機能をカーネルに含める
options IPFILTER_LOG	パケットフィルタのロギング機能を使用
options IPFILTER_DEFAULT_BLOCK	ルールにマッチしない場合の動作はパケットを拒否
options TCP_DROP_SYNFIN	SYN+FIN フラグが立った TCP パケットをドロップ
options ATA_STATIC_ID	ATA デバイスのコントローラ番号を静的に割当て
device isa	ISA デバイスをサポート
device pci	PCI デバイスをサポート
device fdc	フロッピドライブをサポート
device ata	ATA/ATAAPI デバイスをサポート
device atadisk	ATA ディスクをサポート
device npx	浮動小数点演算エミュレーションをサポート(必須)
device sio	シリアルポートをサポート
device miibus	MII バスをサポート
device fxp	Intel EtherExpress PRO/100B NIC をサポート
device pcn	AMD Am79C97x PCI 10/100 NIC をサポート
device random	乱数発生デバイスをサポート
device loop	ループバックデバイスをサポート
device ether	イーサネットデバイスをサポート
device sl	SLIP をサポート
device ppp	PPP をサポート
device tun	パケットトンネリングをサポート
device pty	擬似 tty をサポート
device md	メモリディスクをサポート
device gif	IPv6/IPv4 のパケットトンネリングをサポート
device faith	IPv6 から IPv4 のリレーをサポート
device bpf	バークレー式パケットフィルタをサポート

B. rc.conf 設定パラメータ

表 B-1 rc.conf ファイル

パラメータ	値
hostname=	“masami”
network_interfaces=	"fxp0 pcn0 fxp1 lo0"
Ifconfig_fxp0=	“up”
Ifconfig_fxp1=	"inet 192.168.253.1 netmask 0xffffff00"
Ifconfig_pcn0=	"inet 172.16.1.1 netmask 0xffffffc0 media 100baseTX mediaopt full-duplex up"
sendmail_enable=	“NONE”
sshd_enable=	“YES”
gateway_enable=	“YES”
Ipfilter_enable=	“YES”
Ipfilter_rules=	“/etc/ipf.rules"
Ipfilter_flags=	“”
Ipmon_enable=	“YES”
Ipmon_flags=	“-P /var/run/ipmon.pid -D /var/log/ipf.log”
ipnat_enable=	“YES”
ipnat_rules=	“/etc/ipnat.rules"
Named_enable=	“YES”
Named_flags=	“-c /etc/namedb/named.conf -u bind"

/etc/defaults/rc.conf には全ての設定パラメータがあり、そのパラメータは、/etc/rc.conf によって上書きされます。/etc/defaults/rc.conf は直接変更せず、/etc/rc.conf または /etc/rc.conf.local に固有の設定を行うべきでしょう。

C. mpd 設定パラメータ

表 C-1 設定ファイル

ファイル名	用途
mpd.conf	PPPoE リンク接続する方法を定義する。
mpd.links	リンクする物理インタフェースを定義する。
mpd.secret	リンク接続時のユーザ認証情報(アカウント/パスワード)を定義する。
mpd.script	リンク接続後に実行されるスクリプトを記述する(未使用)。

表 C-2 mpd.conf ファイル

パラメータ	用途
default: load point	デフォルトのプロファイルを指定する。 ここでは point:で定義されたプロファイルがロードされる。
point:	
new -i ng0 point PPPoE	PPPoE インタフェース名を ng0 とする。
set iface route default	ng0 インタフェースが UP した時に、デフォルトルートを追加する。
set iface disable on-demand	オンデマンド・リンク接続を行わない(常時接続)。
set iface idle 0	アイドル時の自動リンク切断を行わない(常時接続)。
set iface mtu 1454	ng0 インタフェースの MTU 値。
set bundle disable multilink	PPPoE マルチリンク接続を行わない(シングルホーム)。
set bundle authname *yourname*	ISP 接続アカウント名。
set link disable pap chap	本ルータが PPPoE サーバとなる場合、pap/chap 認証は行わない。
set link accept pap chap	本ルータが PPPoE クライアントとなる場合、pap/chap 認証を行う。
set link mtu 1454	PPP フレームの MTU 値。
set link mru 1454	PPP フレームの MRU 値。
set ipcp yes vjcomp	IPCP の Van JacobsonTCP ヘッダ圧縮方式を行う。
set ipcp ranges 0.0.0.0/0	IPCP によって取得される IP アドレス。 DHCP で配布されるので、とりあえず 0.0.0.0/0 を定義しておく。
open iface	インタフェースをオープンしてセッションを開始する。

表 C-3 mpd.links ファイル

パラメータ	用途
PPPoE:	mpd.conf 4 行目で識別されるプロファイル名を指定する。
set link type pppoe	リンクタイプを PPPoE とする。
set pppoe iface fxp0	PPPoE とバインドするインタフェース名。
set pppoe service "hoge"	PPPoE サービス名を定義する(任意の文字列 s)。
set pppoe disable incoming	PPPoE サーバとしての接続を拒否する。
set pppoe enable originate	PPPoE クライアントとして接続を行う。

表 C-4 mpd.secret ファイル

パラメータ	用途
yourname *yourpasswd*	1 つ以上の空白/タブで区切ったアカウント名/パスワード。

mpd.secret ファイルは root 以外に内容を読まれないよう、パーミッションを 400 としました。

D. dhcpd 設定パラメータ

表 D-1 dhcpd.conf ファイル

パラメータ	用途
default-lease-time 600; max-lease-time 7200;	デフォルトのリース時間。
ddns-update-style none; log-facility local7;	DDNS 更新を行わない。 syslog ファシリティを local7 とする。
subnet 192.168.253.0 netmask 255.255.255.0 {	社内ネットワーク 192.168.253.0/24 セグメントに対する定義。
range 192.168.253.129 192.168.253.254;	クライアントへ配布する IP アドレス範囲。
default-lease-time 43200; max-lease-time 86400;	このブロックに適用されるデフォルトのリース時間。
option subnet-mask 255.255.255.0;	クライアントへ配布するサブネットマスク。
option broadcast-address 192.168.253.255;	クライアントへ配布するブロードキャストアドレス。
option domain-name "hoge.net";	クライアントへ配布するドメイン名。
option domain-name-servers 192.168.253.5, 192.168.253.1;	クライアントへ配布する DNS サーバの IP アドレス。
option routers 192.168.253.1;	クライアントへ配布するデフォルトルート。
}	
option option-135 code 135 = text;	isc-dhcp2 のオプションである option-135 を isc-dhcp3 でも使用可能とする。
host client_node {	特定のノードに対する定義。PXE クライアント用。
Hardware ethernet *xx*:*xx*:*xx*:*xx*:*xx*:*xx*;	指定した MAC アドレスを持つクライアントからのみ要求に応答する。
next-server 192.168.253.8;	filename を取得する TFTP サーバの IP アドレス。
filename "bpbatch";	TFTP サーバから取得するファイル名(通常ブートローダ)。
option option-135 "-i";	filename に対して-i オプションを渡す(対話式に動作する)。

表 D-2 rc.isc-dhcpd.conf ファイル

パラメータ	用途
dhcpd_options=	
dhcpd_ifaces=fxp1	DHCP を利用する NIC を指定する。

E. ipfilter/ipnat 設定パラメータ

表 E-1 ipf.rules ファイル

パラメータ	用途
block in log quick from any to any with ipopts frag	IP オプションが付加された、または断片化した全ての IP パケットは拒否する。
block in log quick proto tcp from any to any with short	全ての短い TCP パケットは拒否する。
pass in quick on lo0 all pass out quick on lo0 all	ループバックに対する全てのパケットは許可する。
pass in quick proto esp from any to any pass out quick proto esp from any to any pass in quick proto udp from any port = 500 to any pass out quick proto udp from any to any port = 500 pass in quick proto udp from any port = 501 to any pass out quick proto udp from any to any port = 501	IPSec/IKE パケットは許可する。 Lucent IPSec パケットは許可する。
pass in on ng0 all head 100	Internet から入るパケットに対するルールをグループ 100 と定義する。
block in log from 127.0.0.0/8 to any group 100 block in log from 0.0.0.0/32 to any group 100 block in log from 192.168.253.1/24 to any group 100	Internetから入るIP スプーフィングパケットを拒否する。
block in log from 10.0.0.0/8 to any group 100 block in log from 172.16.0.0/12 to any group 100 block in log from 192.168.0.0/16 to any group 100 block in log from 0.0.0.0/8 to any group 100 block in log from 169.254.0.0/16 to any group 100 block in log from 192.0.2.0/24 to any group 100 block in log from 224.0.0.0/4 to any group 100 block in log from 240.0.0.0/4 to any group 100	Internet から入るプライベート IP アドレス (RFC1918) 、DHCP APIPA 、NET-TEST(RFC1166)、およびマルチキャストパケットを拒否する。
block in log quick proto tcp/udp from any port 136 >< 140 to any group 100 block in log quick proto tcp/udp from any to any port 136 >< 140 group 100	Internet から入る NetBIOS パケットを拒否する。
block in log proto udp all group 100	Internet から入る UDP パケットを拒否する。
pass in quick proto tcp all flags A/A group 100	Internetから入る確立済 TCP パケットを許可する。
pass in quick proto tcp from any to any port = 22 flags S/SA group 100 pass in quick proto tcp from any to any port = 80 flags S/SA group 100 pass in log quick proto tcp from any to any port = 443 flags S/SA group 100	Internetから入るssh、www、ssl TCP パケットを許可する。
block return-rst in log quick proto tcp from any to any port = 113 group 100	Internet から入る ident パケットを拒否する。
block in log quick proto tcp all flags S/SA group 100	許可した以外の TCP パケットを拒否する。
pass in proto udp from any port = 53 to any group 100 pass in proto udp from any port = 123 to any group 100	Internet へ出る dns、ntp クエリに対する戻りのパケットを許可する。

block in log proto icmp all group 100 pass in proto icmp all icmp-type 0 group 100	Internet から入る ICMP パケットを拒否する。 Internet から入る ICMP(echo reply)を許可する。
pass in proto icmp all icmp-type 3 group 100	Internet から入る ICMP(destination unreachable)を許可する。
pass out on ng0 all head 200	Internet へ出るパケットに対するルールをグループ 200 と定義する。
block out log from 127.0.0.0/8 to any group 200 block out log from any to 127.0.0.0/8 group 200 block out log from any to 0.0.0.0/32 group 200	Internet へ出る IP スプーフィングパケットを拒否する。
block out log from any to 10.0.0.0/8 group 200 block out log from any to 172.16.0.0/12 group 200 block out log from any to 192.168.0.0/16 group 200 block out log from any to 0.0.0.0/8 group 200 block out log from any to 169.254.0.0/16 group 200 block out log from any to 192.0.2.0/24 group 200 block out log from any to 224.0.0.0/4 group 200 block out log from any to 240.0.0.0/4 group 200	Internet へ出るプライベート IP アドレス(RFC1918)、DHCP APIPA、NET-TEST(RFC1166)、およびマルチキャストパケットを拒否する。
block out log proto tcp/udp from any port 136 >< 140 to any group 200 block out log proto tcp/udp from any to any port 136 >< 140 group 200	Internet へ出る NetBIOS パケットを拒否する。
pass out proto tcp all flags A/A group 200	Internet へ出る確立済 TCP パケットを許可する。
pass out proto tcp from any to any port = 20 flags A/A group 200 pass out quick proto tcp from any to any port = 21 flags S/SA group 200 pass out quick proto tcp from any port = 20 to any flags S/SA group 200 pass out quick proto tcp from any port = 21 to any flags A/A group 200	Internet へ出る ftp パケットと戻りのパケットを許可する。
pass out proto udp from any to any port = 53 group 200 pass out proto udp from any to any port = 123 group 200	Internet へ出る dns、ntp パケットを許可する。
pass out proto tcp all flags S/SA group 200	Internet へ出る TCP パケットを許可する。
block out log proto icmp all group 200 pass out proto icmp all icmp-type 8 group 200	Internet へ出る ICMP パケットを拒否する。 Internet へ出る ICMP(echo request)を許可する。
pass in on fxp1 all head 300	社内セグメントから入るパケットに対するルールをグループ 300 と定義する。
block in log from 127.0.0.0/8 to any group 300 block in log from 192.168.253.1/32 to any group 300 block in log from 0.0.0.0/24 to any group 300	社内セグメントから入る IP スプーフィングパケットを拒否する。
pass out on fxp1 all head 400	社内セグメントへ出るパケットに対するルールをグループ 400 と定義する。
block out log from 127.0.0.0/8 to any group 400 block out log from any to 127.0.0.0/8 group 400 block out log from any to 192.168.253.1/32 group 400	社内セグメントへ出る IP スプーフィングパケットを拒否する。
pass in on pcn0 all head 500	公開セグメントから入るパケットに対するルールをグループ 500 と定義する。

block in log from 127.0.0.0/8 to any group 500 block in log from 0.0.0.0/32 to any group 500 block in log from 192.168.253.1/24 to any group 500	公開セグメントから入るIPスプーフィングパケットを拒否する。
block in log from 10.0.0.0/8 to any group 500 block in log from 192.168.0.0/16 to any group 500 block in log from 0.0.0.0/8 to any group 500 block in log from 169.254.0.0/16 to any group 500 block in log from 192.0.2.0/24 to any group 500 block in log from 224.0.0.0/4 to any group 500 block in log from 240.0.0.0/4 to any group 500	公開セグメントから入るプライベート IP アドレス(RFC1918)、DHCP APIPA、NET-TEST(RFC1166)、およびマルチキャストパケットを拒否する。
block in log quick proto tcp/udp from any port 136 >< 140 to any group 500 block in log quick proto tcp/udp from any to any port 136 >< 140 group 500	公開セグメントから入るNetBIOS パケットを拒否する。
pass in quick proto tcp all flags A/A group 500	公開セグメントから入る確立済TCP パケットを許可する。
pass in log quick proto tcp from any to any port = 25 flags S/SA group 500	公開セグメントから入る smtp パケットを許可する。
block return-rst in log quick proto tcp from any to any port = 113 group 500	公開セグメントから入る ident パケットを拒否する。
block in log quick proto tcp all flags S/SA group 500	許可した以外の TCP パケットを拒否する。
pass in proto udp from 172.16.1.10 to 192.168.253.5 port = 53 keep state group 500	公開セグメントの 172.16.1.10 から入る 192.168.253.5 宛てのDNS パケットとその戻りを許可する。
pass in proto udp from any port = 123 to any group 500	公開セグメントから入る ntp パケットを許可する。
block in log proto icmp all group 500 pass in proto icmp all icmp-type 0 group 500	公開セグメントから入るICMP パケットを拒否する。 公開セグメントから入るICMP(echo reply)を許可する。
pass in proto icmp all icmp-type 3 group 500	公開セグメントから入るICMP(destination unreachable)を許可する。
pass out on pcn0 all head 600	公開セグメントへ出るパケットに対するルールをグループ 600 と定義する。
block out log from 127.0.0.0/8 to any group 600 block out log from any to 127.0.0.0/8 group 600 block out log from any to 0.0.0.0/32 group 600	公開セグメントへ出る IP スプーフィングパケットを拒否する。
block out log from any to 10.0.0.0/8 group 600 block out log from any to 192.168.0.0/16 group 600 block out log from any to 0.0.0.0/8 group 600 block out log from any to 169.254.0.0/16 group 600 block out log from any to 192.0.2.0/24 group 600 block out log from any to 224.0.0.0/4 group 600 block out log from any to 240.0.0.0/4 group 600	公開セグメントへ出るプライベートIPアドレス(RFC1918)、DHCP APIPA、NET-TEST(RFC1166)、およびマルチキャストパケットを拒否する。
block out log proto tcp/udp from any port 136 >< 140 to any group 600 block out log proto tcp/udp from any to any port 136 >< 140 group 600	公開セグメントへ出る NetBIOS パケットを拒否する。
pass out proto tcp all flags A/A group 600	公開セグメントへ出る確立済TCP パケットを許可する。
pass out proto udp from any to any port = 123 group 600	公開セグメントへ出る ntp パケットを許可する。
pass out proto tcp all flags S/SA group 600	公開セグメントへ出る TCP パケットを許可する。

block out log proto icmp all group 600 pass out proto icmp all icmp-type 8 group 600	公開セグメントへ出る ICMP パケットを拒否する。 公開セグメントへ出る ICMP(echo request)を許可する。

表 E-2 ipnat.rules ファイル

パラメータ	用途
map ng0 192.168.253.0/24 -> 0/32 portmap tcp/udp auto mssclamp 1414 map ng0 192.168.253.0/24 -> 0/32 mssclamp 1414	192.168.253.0/24 の IP アドレスを持ったパケットを NAPT する。
map ng0 172.16.1.0/26 -> 0/32 portmap tcp/udp auto mssclamp 1414 map ng0 172.16.1.0/26 -> 0/32 mssclamp 1414	172.16.1.0/26 の IP アドレスを持ったパケットを NAPT する。
map ng0 192.168.243.0/24 -> 0/32 portmap tcp/udp auto mssclamp 1414 map ng0 192.168.243.0/24 -> 0/32 mssclamp 1414	192.168.243.0/24 の IP アドレスを持ったパケットを NAPT する。
rdr ng0 0.0.0.0/0 port 80 -> 172.16.1.10 port 80	Internet から入る 80 ポートを 172.16.1.10:80 へ静的 NAT する。
rdr ng0 0.0.0.0/0 port 443 -> 192.168.253.5 port 443	Internet から入る 443 ポートを 192.168.253.5:443 へ静的 NAT する。
rdr ng0 0.0.0.0/0 port 17777 -> 192.168.253.5port 443	Internet から入る 17777 ポートを 192.168.253.5:443 へ静的 NAT する。

mssclamp は NAPT を行う際に TCP の MSS(Maximum Segment Size)を指定するオプションです。これは、PMTUD Black Hole(RFC2923)に対応するために設定しました。

F. sshd 設定パラメータ

表 F-1 sshd_config ファイル

パラメータ	用途
Port 22	sshd がリスニングするポート番号を定義する。
Protocol 1,2	サポートするプロトコルヴァージョンを定義する。
ListenAddress 0.0.0.0	sshd がリスニングするアドレスを定義する。
HostKey /etc/ssh/ssh_host_key HostKey /etc/ssh/ssh_host_dsa_key	ホスト秘密鍵のファイルを定義する。プロトコルヴァージョン 1 は ssh_host_key、ヴァージョン 2 は ssh_host_dsa_key を使用する。
KeyRegenerationInterval 3600	サーバ鍵が使用された場合の再生成間隔を定義する。(プロトコルヴァージョン 1 のみ)。
ServerKeyBits 768	サーバ鍵のビット数を定義する(プロトコルヴァージョン 1 のみ)。
SyslogFacility AUTH	syslog のファシリティを定義する。
LogLevel INFO	ログメッセージの冗長レベルを定義する。
LoginGraceTime 120	ログインまでの猶予時間を定義する。
PermitRootLogin no	root でのログインを許可しない。
StrictModes yes	ログインを許可する前に、ユーザファイル、およびホームディレクトリの所有者と権限を検査する。
RSAAuthentication yes	RSA 認証を許可する(プロトコルヴァージョン 1 のみ)。
PubkeyAuthentication yes	公開鍵認証を許可する(プロトコルヴァージョン 2 のみ)。
AuthorizedKeysFile .ssh/authorized_keys	ユーザ認証時の公開鍵ファイルを定義する。
RhostsAuthentication no	rhosts、および/etc/hosts.equiv を使用した認証を許可しない(プロトコルヴァージョン 1 のみ)。
IgnoreRhosts yes	RhostsRSAAuthentication、または HostbasedAuthentication 認証時に.rhosts、または.shosts を使用しない。
RhostsRSAAuthentication no	rhosts、および/etc/hosts.equiv を使用した認証を許可しない(プロトコルヴァージョン 1 のみ)。
HostbasedAuthentication no	公開鍵ホスト認証成功後 rhosts、または/etc/hosts.equiv 認証を許可しない(プロトコルヴァージョン 2 のみ)。
IgnoreUserKnownHosts no	RhostsRSAAuthentication、または HostbasedAuthentication 認証時に$HOME/.ssh/known_hosts ファイルを使用しない。
PasswordAuthentication no	パスワード認証を許可しない。
PermitEmptyPasswords no	パスワード認証時の空パスワードによるログインを許可しない。
ChallengeResponseAuthentication no	チャレンジ・レスポンス認証を許可しない。
KerberosAuthentication no	ケルベロス認証を許可しない。
KerberosOrLocalPasswd yes	ケルベロス認証経由のパスワード認証失敗時、/etc/passwd などの別のローカル機構で確認する。
KerberosTicketCleanup yes	チケット用キャッシュをログアウト時に自動的に消去する。
AFSTokenPassing no	AFS トークンを無効化する。
KerberosTgtPassing no	ケルベロス TGT を無効化する。
X11Forwarding no	X11 転送を許可しない。
X11DisplayOffset 10	sshd が X11 転送時、使用するディスプレイ番号を定義する。
X11UseLocalhost yes	sshd が転送された X11 サーバをローカルホストにバインドする。
PrintMotd yes	ログイン時に/etc/motd を表示する。
PrintLastLog yes	ログイン時に前回のログイン日時を表示する。
KeepAlive yes	クライアントへ TCP keepalive メッセージを送信する。
UseLogin no	ログイン時に login(1)プログラムを使用しない。

UsePrivilegeSeparation yes	ログイン時に sshd を root ではない別ユーザの権限を持った子プロセスを生成する。
PermitUserEnvironment no	ログイン時にユーザの環境変数を変更することを許可しない。
Compression yes	圧縮を許可する。
MaxStartups 10	sshd が認証されていない段階の最大接続数を定義する。
Banner /some/path	バナーを表示するファイル名を定義する(プロトコルヴァージョン 2 のみ)。
VerifyReverseMapping no	リモートホストの正引き/逆引きを検査しない。
Subsystem smtp /usr/libexec/sftp-server	外部サブシステムとして sftp を定義する。

G.namd 設定パラメータ

表 G-1 named.conf ファイル

パラメータ	用途
options {	
version "";	bind のヴァージョンを隠す。
directory "/etc/namedb";	bind の作業ディレクトリを定義する。
pid-file "/var/run/named/pid";	bind の PID を保存するファイルを定義する。
check-names slave ignore;	スレーブゾーンの名前検査を行わない。 マスタが Windows2000 DNS で `_'を含んだホスト名がゾーン転送されるため、警告メッセージを抑止する。
forward first;	最初に内部ゾーンを検索し、レコードを見つけることができなければ forwarders にクエリを転送する。

forwarders {
210.xxx.xxx.xxx;
65.xxx.xxx.xxx;
};
	ISP から提供されているネームサーバのリストを定義する。

};	

zone “.” {
type hint;
file "named.root";
};
	ルートサーバのヒントゾーンを定義。

zone "0.0.127.in-addr.arpa" {
type master;
file "master/localhost.rev";
};
	本ルータ自身の逆引きゾーンを定義。

zone "hoge.net" {
type slave;
file "slave/hoge.net.zone";
masters { 192.168.253.5; };
};
	内部向け hoge.net の正引きゾーンを定義。

zone "253.168.192.in-addr.arpa" {
type slave;
file "slave/253.168.192.in-addr.arpa.zone";
masters { 192.168.253.5; };
};
	内部向け 192.168.253.0/24 の逆引きゾーンを定義。
	(社内用セグメント)

zone "243.168.192.in-addr.arpa" {
type slave;
file slave/243.168.192.in-addr.arpa.zone";
masters { 192.168.253.5; };
};
	内部向け 192.168.243.0/24 の逆引きゾーンを定義。
	(VPN 用セグメント)

zone "1.16.172.in-addr.arpa" {
type slave;
file "slave/1.16.172.in-addr.arpa.zone";
masters { 192.168.1.5; };
};
	内部向け 172.16.1.0/26 の逆引きゾーンを定義。
	(公開用セグメント)

SOHO router construction with FreeBSD

改版履歴

Version 1.0	2004/01/10	新規作成。
Version 1.1	2004/03/10	ネットワーク構成の変更に伴う修正。
Version 1.2	2004/04/16	5.3.5 節に追記。
Version 1.3	2004/07/26	「D. dhcpd 設定パラメータ」、「E. ipfilter 設定パラメータ」、「F. ipnat 設定パラメータ」を変更。
Version 1.4	2004/08/10	「4.8. ログ・ローテーション」節に追記。
Version 1.5	2004/09/29	拠点変更に伴う表記を修正。

製作

Isidore.

本書は 2004 年 9 月現在の情報を元に作成されております。本書に記載されております内容は、許可なく変更されることがあります。