Objet :	**Snort sous Fedora 6**	Date : Version :	**01/04/07** **1.2**

Description

Installation de Snort (2.6.1) et B.A.S.E (1.3.5) sous Fedora Core 6. La partie la plus importante : la configuration est abordée de manière très superficielle ; cette partie est en cours de rédaction.
Avant toute action, ne connectez pas votre machine snort sur internet sauf à passer par un filtrage purement sortant (proxy ou ipfilter actif). Vous n'avez pas besoin de ports ouverts sur l'interface qui effectuera la capture du trafic à surveiller.
Toutes remarques et suggestions sont les bienvenues
à olivier[à]thebaud.com

Pré requis

Quelques pré requis

- Les explication suivantes sont faites sur une plate-forme Fedora Core 6
- Apache : oui (+PHP5) avec la bibliothèque GD
- MySQL en version 5.x avec le module mysql-dev
- PCRE 6.x (tar xzvf pcre-7.0.tar.gz + ./configure + make + make install)
- Librairie libpcap

Syntaxe utilisée dans le document

/download/ représente le répertoire où vous avez téléchargé les différents composants.
Utilisateur est un nom à personnaliser
Mot_de_passe est aussi à personnaliser
Webserver est le nom de votre machine sur laquelle sera installé Snort

Installation de Snort

Toutes les informations sont disponibles sous leur forme d'origine sur www.snort.org

Télécharger SNORT dans un répertoire temporaire

```
wget http://www.snort.org/dl/current/snort-2.6.1.2.tar.gz
tar xzvf  snort-2.6.1.2.tar.gz
cd snort-2.6.1.2
 ./configure -with-mysql -enable-dynamicplugin
```

Vérifiez bien qu'il n'y ait pas d'erreur en fin de vérification.

```
make
make install
groupadd snort
useradd -g snort snort -s /sbin/nologin
mkdir /etc/snort
mkdir /etc/snort/rules
mkdir /var/log/snort
```

Attention à la commande suivante : le but est de vous placer dans le répertoire décompressé de Snort, pas dans le répertoire /etc en production

```
cd ./etc
cp * /etc/snort
```

➔ Mise à jour des règles SNORT

Il s'agit maintenant de télécharger les dernières règles de traitement de paquets par Snort

```
Wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz
Tar xzvf snortrules-pr-2.4.tar.gz
Cd rules
Cp * /etc/snort/rules
```

➔ Configuration du fichier snort.conf

Le fichier est normalement situé dans /etc/snort/snort.conf
Les lignes à vérifier ou modifier sont :

```
Var HOME_NET x.x.x.x/x
```

La variable HOME_NET doit correspondre à la définition de votre réseau local constitué du réseau IP + masque (exemple : 192.168.0.0/16). Si une interface est dédiée à la capture du réseau, spécifiez précisément l'interface (ex: eth0). Si vous machine doit surveiller le traffic venant vers votre machine, spéciez l'adresse ip (ex : 192.168.0.5/32)

```
Var EXTERNAL_NET any
```

Signifie que vous analysez tout ce qui passe sur votre réseau provenant du réseau EXTERNAL_NET
Cette situation n'est pas idéale dans le cadre où votre machine doit analyser le trafic interne de votre réseau ; réduisez alors la variable HOME_NET à votre interface d'administration.
Gardez à l'esprit que les règles précisent d'analyse généralement le trafic réseau venant de EXTERNAL_NET à destination de HOME_NET (et parfois vers HTTP_SERVERS, par exemple).

Vérifiez si les variables suivantes correspondent à la configuration de votre architecture (par défaut ces variables sont mappées avec la variable HOME_NET) :

- HTTP_SERVERS
- DNS_SERVERS
- SMTP_SERVERS
- SQL_SERVERS
- TELNET_SERVERS
- SNMP_SERVERS

Prêtez une attention également sur la définition des ports, toujours en fonction de votre architecture :

- HTTP_PORT
- SHELLLCODE_PORTS
- ORACLE_PORTS

Modifiez

```
Var RULE_PATH ../rules
```

Par

```
Var RULE_PATH /etc/snort/rules
```

Après la ligne:

```
preprocessor stream4_reassemble
```

Ajoutez :

```
preprocessor stream4_reassemble: both,ports 21 23 25 53 80 110 111 139 143 445
```

Dans la section output, modifez la ligne suivante pour intégrer vos paramètres de base MySQL

```
output database: log, mysql, user=utilisateur
password=mot_de_passe dbname=snort host=localhost
```

➔ Démarrage de Snort en automatique

`Cd /etc/init.d`

Récupérez le script nécessaire pour faire fonctionner snort sous forme de service (le contenu se trouve au format texte ici : http://www.e-watching.net/projet/snort.txt)

```
Copiez-le dans un fichier /etc/init.d/snort
Chmod 755 snort
Chkconfig snort on
```

Dans le fichier snort, vérifiez que la ligne contenant eth0 soit appropriée : votre HOME_NET de snort.conf doit correspondre à l'interface physique déclarée ici (eth0 par défaut).

➔ Configuration de la base de données

Utilisez phpmyadmin pour la création et maintenance de vos bases MySQL
Créez la base *snortdb*,
Créez aussi un utilisateur qui aura tous les privilèges sur cette base snort.
Vérifier que l'utilisateur *snort_user* ait bien les droits sur la base *snortdb*, via localhost
La création des tables se fait en exécutant le fichier `create_mysql` situé dans le répertoire de décompression snort `./schemas`

`mysql -u snort_user -p snort < create_mysql`

`snortdb` est le nom de la base de données créée

Le résultat visible dans phpmyadmin : 16 tables créées dans SNORTDB

➔ Démarrage de Snort

Pour tester le démarrage manuel de Snort et visualiser d'éventuels messages d'erreur

```
Snort -c /etc/snort/snort.conf
```

Si c'est OK, CTRL+C, puis

```
Service snort start
```

Puis

```
ps -ef | grep snort.conf
```

Pour vérifier que le process Snort y soit bien présent.

➔ Webmin & Snort

Si vous souhaitez configurer Snort de manière plus aisée, utilisez le composant Webmin.
http://www.snort.org/dl/contrib/front_ends/webmin_plugin/snort-1.0.wbm
Presque tout ce qu'on vient de faire était disponible via Webmin.

Installation de B.A.S.E. 1.3.5

Toutes les informations sont disponibles sur http://base.secureideas.net/
Effectuez l'installation des composants de composants de graphiques (attention la commande suivante nécessite un accès http:80 sur internet)

```
pear install Image_Graph-alpha Image_Canvas-alpha
Image_Color Numbers_Roman
```

➔ Téléchargez la dernière version d'**ADODB**

```
soit :
     wget
     http://mesh.dl.sourceforge.net/sourceforge/adodb/adodb4
94.tgz
     cd /var/www
     tar -xzvf  /download/adodb492.tgz
soit plus simple :
     yum install php-adodb )
```

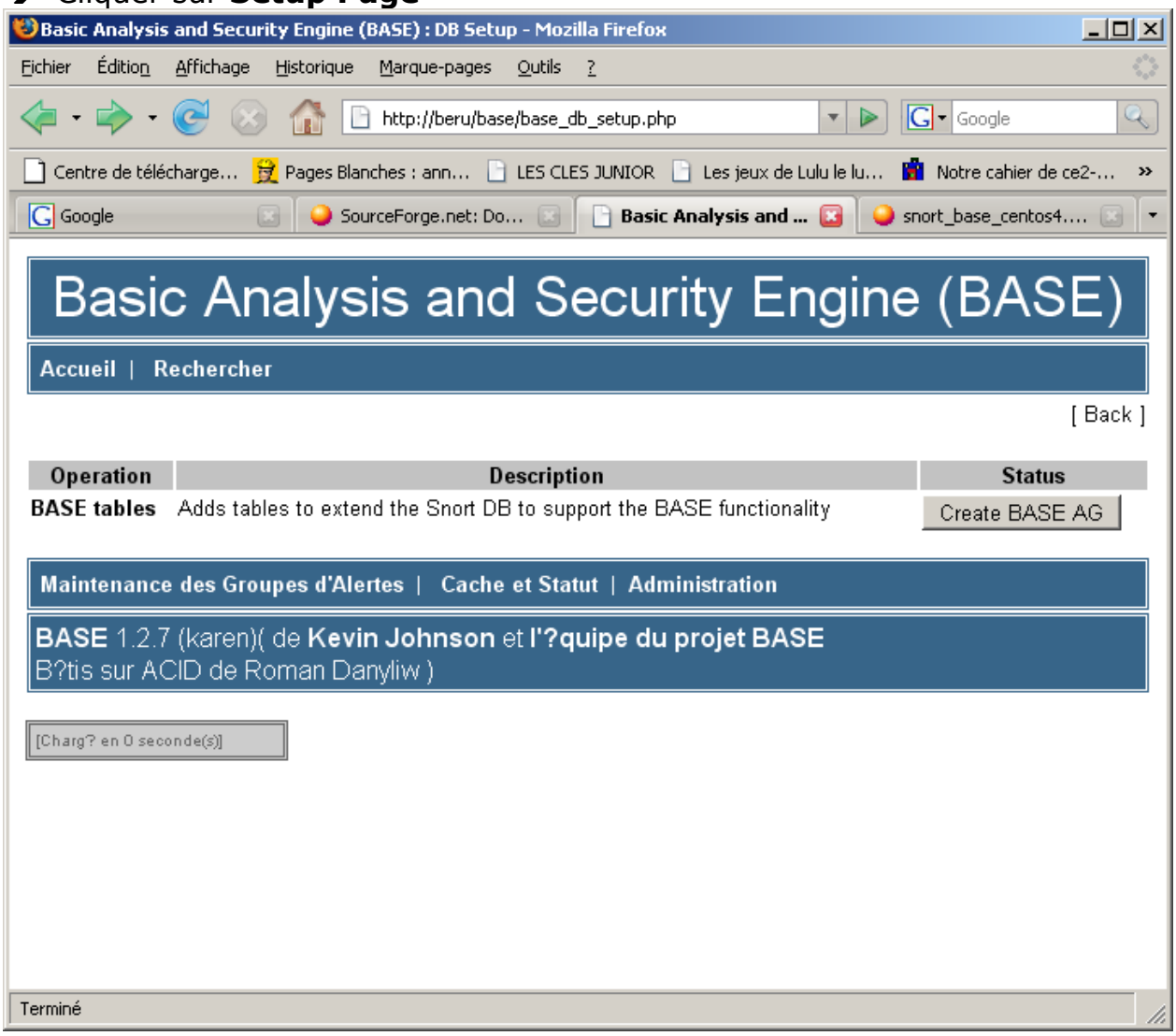
➔ Téléchargez la dernière version de **BASE**

```
Cd /download
wget  http://downloads.sourceforge.net/secureideas/base-
1.2.7.tar.gz?modtime=1163707226&big_mirror=0
cd /var/www/html (où html est le répertoire racine de votre
site web)
tar xzvf /download/base-1.2.7.tar.gz
mv base-1.2.7 base
cd base
cp base_conf.php.dist base_conf.php
```

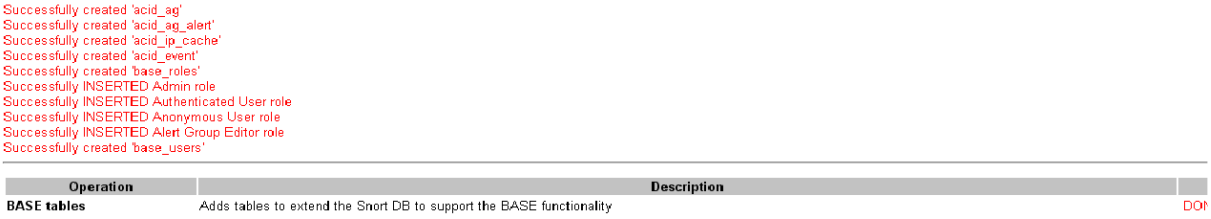
➔ Modifiez le fichier de config de BASE afin de se connecter à la base de données utilisée par Snort : base_conf.php

```
$BASE_urlpath = "/base";

$BASE_Language = 'french';

$Dblib_path = "/var/www/adodb/";
$Dbtype = "mysql";

$alert_dbname   = 'snort';
$alert_host     = 'localhost';
$alert_port     = '';
$alert_user     = 'utilisateur';
$alert_password = 'mot_de_passe';
```

➔ Se connecter sur http:///webserver/base
➔ Cliquer sur **Setup Page**



➔ Puis sur **Create BASE AG**



➔ Cliquez sur **HOME** pour revenir à la page principale de Statistiques

Test initial de la configuration globale

➔ Depuis un poste Windows, faites un
`ping -l 1024 adresse_ip`

où adresse_ip est une adresse ip de la machine snort ou capturée par snort.

Cette commande ping doit générer des erreurs `ICMP Large ICMP Packet`

Mise à jour automatique des règles avec oinkmaster

Les règles de détection sont mises à jour régulièrement sur le site de Snort. Plusieurs façon de les mettre à jour :

1- vous les télécharger sur le site après avoir ouvert un compte gratuit sur www.snort.org, vous disposerez des dernières règles avec 5 jours de retard.
2- Vous souscrivez un abonnement payant (de 30 à 400 $) auprès de Snort (SoureFire VRT) afin d'avoir les toutes dernières règles vérifiées.
3- Vous pouvez aussi récupérer d'autres règles issue d'une communauté OpenSource Bleeding Edge Threats (http://www.bleedingsnort.com)

Dans les deux premiers cas, la première étape est d'installer un outils complémentaire de télécharger et d'installation des règles Snort : OinkMaster (http://oinkmaster.sourceforge.net)

➔ Sous Linux, lancez

```
wget http://prdownloads.sourceforge.net/oinkmaster/oinkmaster-2.0.tar.gz?download
tar xzvf oinkmaster-2.0.tar.gz
cd oinkmaster-2.0
cp oinkmaster.pl /usr/local/bin
cp oikmaster.conf /etc
```

➔ Modifiez le fichier oinkmaster.conf, et notamment la ligne

```
url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-CURRENT.tar.gz
```

Remplacez **<oinkcode>** par le code Oink fourni sur le site Snort (visualisable dans vos préférences utilisateurs)

➔ Modifier les permissions pour l'utilisateur Snort afin que celui-ci ait les droits de mettre à jour les fichiers de règles.

```
chown –R snort:snort /etc/snort/rules
```

➔

La mise à jour des règles peut-être lancée manuellement comme ceci :

```
oinkmaster.pl –o /etc/snort/rules
```

➔ L'intérêt est bien sûr de planifier cette mise à jour en éditant le fichier /etc/crontab et d'ajouter la ligne

```
30 8 * * * /usr/local/bin/oinkmaster.pl –o /etc/snort/rules
```

Génération de rapports de détection avec SnortALog 2.4

En complément de B.A.S.E., SnortALog est un addon puissant permettant de tirer des statistiques globales sur l'activité de détection de Snort, plus compréhensibles pour des non-informaticiens.

Attention à bien vous assurer des pré-requis suivants (http://jeremy.chartier.free.fr/snortalog/requirements.html) :

- GD-1.19.tar.gz
- GDGraph-1.39.tar.gz
- GDTextUtil-0.85.tar.gz
- Htmldoc-1.8.23
- HTML-HTMLDoc-0.07
- Tk-800-024.tar.gz
- Perl-Tk-800.024-2.i386.rpm
- http://ftp.belnet.be/packages/dries.ulyssis.org/fedora/fc6/i386/RPMS.dries/perl-Net-Whois-IP-1.02-1.fc6.rf.noarch.rpm

➔ Téléchargement :

```
Wget http://jeremy.chartier.free.fr/snortalog/downloads/snortalog/snortalog_v2.4.1.tgz
Tar xzvf snortalog_v2.4.1.tgz
Yum install htmldoc
Yum install perl-Tk
```

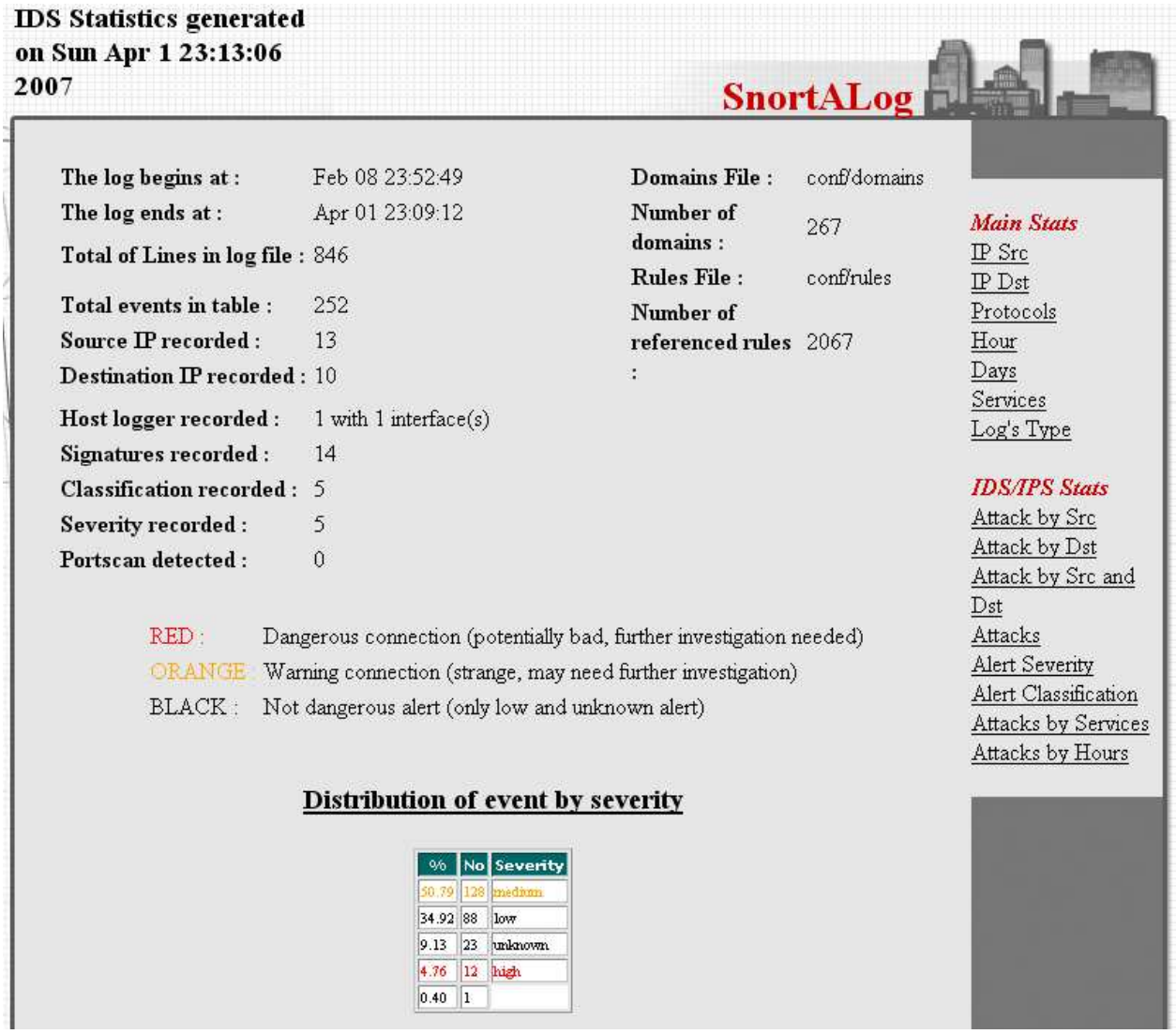
➔ Le but est ensuite de rendre accessible le répertoire SnortALog depuis Apache.

```
mv snortalog ./var/www/html
```

➔ Pour lancer une première analyse manuelle par Snortalog, lancez la commande suivante depuis le répertoire /va/www/html. La commande ci-dessous génère un rapport au format Web à partir du fichier alert créé par Snort.

```
cat /var/log/snort/alert | ./snortalog.pl -r -i -o resultat.html -report
```

➔ Vous accèderez au fichier web généré depuis http://serveur_web/snortalog/resultat.html



IDS Statistics generated on Sun Apr 1 23:13:06 2007

SnortALog

The log begins at :	Feb 08 23:52:49	**Domains File :**	conf/domains
The log ends at :	Apr 01 23:09:12	**Number of domains :**	267
Total of Lines in log file :	846	**Rules File :**	conf/rules
Total events in table :	252	**Number of referenced rules :**	2067
Source IP recorded :	13		
Destination IP recorded :	10		
Host logger recorded :	1 with 1 interface(s)		
Signatures recorded :	14		
Classification recorded :	5		
Severity recorded :	5		
Portscan detected :	0		

RED : Dangerous connection (potentially bad, further investigation needed)
ORANGE : Warning connection (strange, may need further investigation)
BLACK : Not dangerous alert (only low and unknown alert)

Main Stats
IP Src
IP Dst
Protocols
Hour
Days
Services
Log's Type

IDS/IPS Stats
Attack by Src
Attack by Dst
Attack by Src and Dst
Attacks
Alert Severity
Alert Classification
Attacks by Services
Attacks by Hours

Distribution of event by severity

%	No	Severity
50.79	128	medium
34.92	88	low
9.13	23	unknown
4.76	12	high
0.40	1	

Ressources (autre que www.snort.org !!!)

Site OinkMaster :
http://oinkmaster.sourceforge.net/
Doc Oinkmaster :
http://www.snort.org/docs/setup_guides/Installing_and_configuring_OinkMaster.pdf

Installation de Snort,Base, MySql, Apache, …
http://www.internetsecurityguru.com/documents

Communauté OpenSource sur des règles Snort
http://www.bleedingsnort.com

Améliorations à envisager/en cours dans le document

- Sécurisation de l'installation de Snort + BASE (+MySQL)
- Sécurisation de l'installation de SnortAlog
- Utilisation/configuration des alertes BASE et groupes d'utilisateur
- Le plus important : paramètrage de Snort.conf
- Utilisation et modifications des règles Snort pour une personnalisation "entreprise"

Annexes

A – fichier de lancement de snort (dispo sur www.e-watching.net/projets/snort.txt)

```
#!/bin/sh
#
# chkconfig: 2345 99 82
# description: Starts and stops the snort intrusion detection system
#
# config: /etc/snort/snort.conf
# processname: snort

# Source function library
. /etc/rc.d/init.d/functions

BASE=snort
DAEMON="-D"
INTERFACE="-i eth0"
CONF="/etc/snort/snort.conf"

# Check that $BASE exists.
[ -f /usr/local/bin/$BASE ] || exit 0

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

RETVAL=0
# See how we were called.
case "$1" in
  start)
        if [ -n "`/sbin/pidof $BASE`" ]; then
                echo -n $"$BASE: already running"
                echo ""
                exit $RETVAL
        fi
        echo -n "Starting snort service: "
        /usr/local/bin/$BASE $INTERFACE -c $CONF $DAEMON
        sleep 1
        action "" /sbin/pidof $BASE
        RETVAL=$?
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/snort
        ;;
  stop)
        echo -n "Shutting down snort service: "
        killproc $BASE
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/snort
        ;;
  restart|reload)
        $0 stop
        $0 start
        RETVAL=$?
```

```
        ;;
  status)
        status $BASE
        RETVAL=$?
        ;;
  *)
        echo "Usage: snort {start|stop|restart|reload|status}"
        exit 1
esac

exit $RETVAL
```