

Dictionnaire des commandes NETASQ

version 1.0 – copyright NETASQ 2004

Dictionnaire des lignes de commandes

Description Ce document présente et explicite l'ensemble des commandes IPS-Firewall NETASQ. Chaque description est accompagnée de :

- Commande : grammaire de la commande,
- Usage : emploi des différentes options de la commande,
- Résultat : explication des éventuelles réponses de l'IPS-Firewall,
- Exemple : exemples.

Destinataires Ce dictionnaire est destiné aux partenaires certifiés NETASQ réalisant du support pour leurs clients.

Attention **Les commandes présentées ci-dessous sont des commandes dites de bas niveau. Cela signifie qu'elles constituent la première brique de gestion d'un IPS-Firewall NETASQ. Aucune vérification de la cohérence des commandes n'est réalisée. Cela signifie que les utilisateurs de ces commandes peuvent mettre en péril la stabilité du système.**

Organisation Ce dictionnaire est organisé autour de trois chapitres :

- Commande de diagnostic et maintenance,
- Commande de configuration,
- Commande d'informations diverses.

Index La liste suivante liste l'ensemble des commandes qui sont évoquées dans la suite de ce document :

arp	endialup	globalgen
authd	endns	grep
backupinfo	enevent	halt
certinfo	enfilter	hasstatus
chpwd	engui	ifconfig
cleanfw	enha	ifinfo
clearlog	enkeyboard	ipnat
crlinfo	enldap	netstat
date	ennat	nsrpc
defaultconfig	ennetwork	ntpq
dialupstate	enntp	reboot
df	enobject	setconf
dkill	enservice	sfctl
dmesg	ensnmp	showSAD
dstat	enproxy	showSPD
dumpcert	entimezone	slotinfo
dumproot	enurl	svc
enalarm	envpn	sysctl
enauth	getconf	sysinfo
enavp	getmodel	tcpdump
endhcp	getversion	top
		tproxyd

Commande de diagnostique et de maintenance

Description	Le chapitre suivant explique les différentes commandes indispensables dans les phases de diagnostique et de maintenance.
--------------------	--

Index	La liste suivante liste l'ensemble des commandes qui sont évoquées dans cette section du document :
--------------	---

arp	sysinfo
defaultconfig	tcpdump
dialupstate	top
df	
dkill	
dmesg	
dstat	
dumpcert	
dumproot	
grep	
hasstatus	
ifconfig	
ifinfo	
ipnat	
netstat	
sfctl	
showSAD	
showSPD	
slotinfo	
svc	
sysctl	

arp

Description	Affiche les informations relatives au protocole de résolution d'adresses ARP.
Commande	<pre>arp [-n] [-i interface] hostname arp [-n] [-i interface] -a arp -d hostname [pub] arp -d -a arp -s hostname ether_addr [temp] [pub [only]] arp -S hostname ether_addr [temp] [pub [only]] arp -f filename</pre>
Résultat	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
Exemple	<pre>F2004C09999999999999>arp -d -a 10.x.x.x (10.x.x.x) deleted F2004C09999999999999></pre>

defaultconfig

Description	Permet la remise en configuration par défaut du Firewall et la réinitialisation du mot de passe.
Commande	<pre>defaultconfig f</pre> <pre>defaultconfig [-f] [-b] [-p] [-r]</pre>
Usage	<p>L'envoi de la commande <i>defaultconfig f</i> n'est disponible que pour les versions de firmware comprise entre 4 et 5.0.4. Cette commande restaure la configuration par défaut mais le mot de passe admin n'est pas modifié et le firewall redémarre.</p> <p>L'envoi de la commande <i>defaultconfig -f</i> n'est disponible que pour les versions de firmware supérieures à 5.0.4. Cette commande restaure la configuration par défaut mais le mot de passe admin n'est pas modifié.</p> <p>L'option <i>-b</i> est spécifique au boîtier F100B qui possède une sérigraphie in / dmz / out au lieu de la sérigraphie 1 / 2 / 3.</p> <p>L'option <i>-r</i> redémarre automatiquement l'IPS-Firewall pour la restauration de la configuration.</p> <p>L'option <i>-p</i> permet la réinitialisation du mot de passe admin. Lors de la prochaine connexion, l'administrateur devra se connecter sans mot de passe. Le système demandera alors de le définir.</p> <p>Lorsqu'une restauration des paramètres de configuration par défaut est effectuée la configuration actuelle est sauvegardée dans un fichier nommé « ConfigFiles.old ». Ce fichier peut être utilisé pour restaurer la configuration précédant le « <i>defaultconfig</i> » (en renommant le fichier « ConfigFiles.old » par « ConfigFiles »). La restauration de cette configuration nécessite un redémarrage de l'IPS-Firewall.</p>
Résultat	<p>« Replacing current configuration with the default configuration » : la configuration par défaut a été restaurée, redémarrer le Firewall pour activer les modifications. Le mot de passe admin n'est pas modifié.</p> <p>« Previous defaultconfig found... remove it manually » : taper la commande "rm -R /Firewall/ConfigFiles.old" et recommencer la procédure.</p>
Exemple	<pre>F2004C099999999999>defaultconfig -f -p -r deleting previous backup... replacing current configuration with the default configuration... restoring default password... ##### ## Restore default SRP/SSH password for admin ## ##### Modify SRP/SSH password of user 'admin' successful Shutdown NOW! shutdown: [pid 990] *** FINAL System shutdown message from admin@F2004C099999999999 *** System going down IMMEDIATELY F2004C09999999999999> System shutdown time has arrived</pre>

dialupstate

Description	Permet de connaître l'état des différentes connexions dialup configurées sur le Firewall.
--------------------	---

Commande	dialupstate
-----------------	-------------

Résultat	<p>Dialup « n » : indique l'état de la dialup numérotée « n ».</p> <ul style="list-style-type: none">- not_configured : la dialup n'a pas été confirmée,- off : la dialup est configurée mais arrêtée,- on : la dialup est configurée et activée,- backup : la dialup est configurée pour s'activer si aucune Dialup n'est « up ». <p>Dialup « n » est le terme par défaut utilisé pour désigner la présente Dialup. Si l'utilisateur configure un autre nom</p> <p>State : indique si la dialup est négociée.</p> <ul style="list-style-type: none">- down : la dialup n'est pas (encore) montée,- up : la dialup est correctement montée. <p>Localip : adresse IP de l'extrémité locale du trafic « Dialup ».</p> <p>Remoteip : adresse IP de l'extrémité distante du trafic « Dialup ».</p> <p>Type : type de trafic « Dialup » (PPP, PPTP, PPPoE, PPPoA).</p> <p>ng : interface système sur laquelle est connectée la Dialup.</p>
-----------------	---

Exemple	<pre>F2004C099999999999>dialupstate Dialup0=on state=up localip=120.23.68.45 remoteip=88.79.125.6 type=PPTP ng=ng0 Dialup1=backup state=down Dialup2=off state=down Dialup3=not_configured state=down Dialup4=not_configured state=down Dialup5=not_configured state=down Dialup6=not_configured state=down Dialup7=not_configured state=down F2004C099999999999></pre>
----------------	---

df

Description	Affiche des statistiques relatives au disque dur de l'IPS-Firewall (espace libre, occupée, pourcentage,...)
--------------------	---

Commande	<code>df -h</code>
-----------------	--------------------

Résultat	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
-----------------	--

Exemple	<pre>F2004C09999999999999>df -h Filesystem Size Used Avail Capacity Mounted on /dev/ad0s1a 252M 28M 203M 12% / mfs:36 910K 238K 600K 28% /var /dev/ad0s1f 8.4G 2.7M 7.8G 0% /log F2004C09999999999999></pre>
----------------	--

dkill

Description	Désactive tous les démons sauf le démon SSH.
--------------------	--

Commande	dkill
-----------------	-------

Usage	Attention l'utilisation de cette commande entraîne une instabilité de l'IPS-Firewall (la majeure partie des démons étant arrêtée). Cette commande n'est bien entendu pas recommandée.
--------------	---

Exemple	<pre>F2004C099999999999>dkill F2004C099999999999>dstat alarmd : /var/supervise/alarmd: supervise not running authd : /var/supervise/authd: supervise not running dhclient : /var/supervise/dhclient: supervise not running dhcpd : /var/supervise/dhcpd: supervise not running dns : /var/supervise/dns: supervise not running eventd : /var/supervise/eventd: supervise not running hardwared : /var/supervise/hardwared: supervise not running ldap : /var/supervise/ldap: supervise not running mpd : /var/supervise/mpd: supervise not running ntp : /var/supervise/ntp: supervise not running racoon : /var/supervise/racoon: supervise not running serverd : /var/supervise/serverd: supervise not running sshd : /var/supervise/sshd: down 116 seconds snmpd : /var/supervise/snmp: down 116 seconds tproxyd : /var/supervise/tproxyd: supervise not running F2004C099999999999></pre>
----------------	--

dmesg

Description	Affiche les informations contenues dans le tampon système du noyau.
--------------------	---

Commande	<code>dmesg</code>
-----------------	--------------------

Usage	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
--------------	--

La commande `sysctl -w kern.msgbuf_clear=1` permet la remise à zéro du tampon système du noyau. Cette action peut être intéressante pour faire apparaître les nouveaux messages « noyau ».

Exemple	<pre>F2004C09999999999999>dmesg Copyright (c) 1992-2002 The FreeBSD Project. Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights FreeBSD 4.7 - Netasq Firewall 5.0 Mounting root from ufs:/dev/ad0s1a ASQ engine v2.0 21Mb total memory 14Mb available for dynamic allocator F2004C09999999999999></pre>
----------------	---

dstat

Description	Liste le statut des différents services (daemon)
--------------------	--

Commande	dstat
-----------------	-------

Résultat	<p>« alarmd » : nom du service,</p> <p>« ../../alarmd/ » : chemin d'accès du daemon de supervision vérifiant l'état du service,</p> <p>up, down : état du daemon (actif, inactif),</p> <p>pid xxx : numéro de processus affecté au service lors de son lancement,</p> <p>xxx seconds : temps depuis lequel le service est dans l'état actuel.</p> <p>normally (up ou down) : indique que le démon est actuellement dans un état qui n'est pas son état au démarrage de l'IPS-Firewall.</p> <p>want (up ou down) : indique un état transitoire du démon. Le démon était dans un état (par exemple up) et l'administrateur a fait une demande qui va modifier son état (dans notre exemple arrêt). Le temps que le démon soit dans son état final « dstat » indique toujours son ancien état (dans notre exemple up) mais spécifie qu'il est en train de changer d'état « want ... » (ex : want down).</p>
-----------------	--

Exemple	<pre>F2004C09999999999999>dstat alarmd : /var/supervise/alarmd: up (pid 625) 16893 seconds authd : /var/supervise/authd: down 16897 seconds dhclient : /var/supervise/dhclient: down 16897 seconds dhcpd : /var/supervise/dhcpd: down 16897 seconds dns : /var/supervise/dns: down 16897 seconds eventd : /var/supervise/eventd: up (pid 418) 16897 seconds hardwared : /var/supervise/hardwared: up (pid 417) 16897 seconds ldap : /var/supervise/ldap: down 16897 seconds mpd : /var/supervise/mpd: down 16897 seconds ntp : /var/supervise/ntp: down 16893 seconds racoon : /var/supervise/racoon: down 16897 seconds serverd : /var/supervise/serverd: up (pid 416) 16897 seconds sshd : /var/supervise/sshd: down 16897 seconds snmpd : /var/supervise/snmp: down 16897 seconds tproxyd : /var/supervise/tproxyd: down 16897 seconds F2004C09999999999999></pre>
----------------	---

dumpcert

Description	Vérifie la cohérence entre la licence insérée et le type de l'IPS-Firewall.
Commande	<code>dumpcert</code>
Résultat	Retour du prompt sans message : l'opération s'est exécutée correctement.
Exemple	<pre>F2004C099999999999>dumpcert F2004C099999999999></pre>

dumproot

Description	Permet de sauvegarder ou de restaurer le système en copiant le contenu de la partition active sur la partition passive. Un dumproot exécuté en ayant démarré sur la partition principale sauvegardera la système sur la partition de backup, un dumproot en ayant démarré sur la partition de backup permettra de la restaurer sur la partition principale.
Commande	<code>dumproot [-b]</code>
Usage	L'option <code>-b</code> permet de n'effectuer la commande <i>dumproot</i> qu'au démarrage de l'IPS-Firewall.
Résultat	<p>Retour du prompt sans message : l'opération s'est exécutée correctement.</p> <p>« System busy » : un service est actuellement en train d'effectuer une opération empêchant de figer le système pour le sauvegarder, réessayez ultérieurement.</p>
Exemple	<pre>F2004C099999999999>dumproot F2004C099999999999></pre>

grep

Description	Affiche la ligne contenant les mots-clés définis dans la commande
Commande	<code>grep [options] < pattern > < file ></code>
Usage	Cette commande est une commande native de freeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de freeBSD sur le site web www.freebsd.org .
Exemple	<pre>F2004C09999999999999>grep Address /usr/Firewall/ConfigFiles/network Address=127.0.0.1 Address= Address=82.36.45.56 Address=10.6.4.2 Address=192.168.0.1 Address= PeerAddress= F2004C09999999999999></pre>

hasstatus

Description	Permet d'obtenir des informations sur l'état de la Haute Disponibilité et d'effectuer quelques actions dessus.
--------------------	--

Commande	<code>hasstatus [-s]</code>
-----------------	-----------------------------

Résultat	<p>Dans la section « Global » :</p> <p>pass : mot de passe de l'utilisateur HA. peer_error : erreur de communication avec l'IPS-Firewall passif. priority : priorité définie : 0=none, 1=maître, 2=backup. send_peer_failure : 0=OK, 1=le firewall n'arrive pas à communiquer avec son correspondant.</p> <p>Dans la section « Local/Peer » :</p> <p>slicence : licence haute disponibilité (maître ou backup). licence : licence au format numérique (8=maître, 4=backup).</p>
-----------------	---

Exemple	<pre>F2004C099999999999>hasstatus [-s] Global: ----- pass = motdepasse peer_error= 0 priority = 0 lock_state= 0 need_register= 0 send_peer_failure= 0 backup_active= Main backup_version= 5.0.8 Local: Peer: ----- ----- slicence= Master slicence= Slave licence= 8 licence= 4 sstate= Active sstate= Passive state= 2 state= 1 quality= 100 quality= 100 synced= 1 synced= 1 ha= 1 ha= 1 serial= F100BA999999999999 serial= F100BA9999999999998 version= 5.0.8 version= 5.0.8 asqdump= 2 asqdump= 2 F2004C09999999999999></pre>
----------------	--

ifconfig

Description	Affiche les informations de configuration des interfaces de l'IPS-Firewall.
Commande	<code>ifconfig</code>
Usage	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
Exemple	<pre>F2004C099999999999>ifconfig fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500 inet 82.xx.xx.xx netmask 0xffffffff00 broadcast 82.xx.xx.xx ether 00:02:b3:a8:5b:dd media: Ethernet autoselect (none) status: no carrier ng36: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 ng37: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 ng38: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 ng39: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 F2004C099999999999></pre>

ifinfo

Description	Remonte des informations sur la configuration des interfaces réseaux. A savoir : nom de l'interface défini par l'administrateur, nom réelle de l'interface, adresse et type.
--------------------	--

Commande	<code>ifinfo</code>
-----------------	---------------------

Résultat	<p>La commande <i>ifinfo</i> retourne la liste des interfaces et leurs informations associées :</p> <p>Nom de l'interface : nom défini par l'administrateur. Par défaut « in », « out », « dmz », « bridge », « serial », « ipsec ».</p> <p>Statut de l'interface : indique qu'il s'agit ou non d'une interface externe (protected si interne).</p> <p>Nom réel de l'interface : attention les interfaces NETASQ sont numérotés à partir de 0. Exemple : fxp0, rl0... correspondent donc à l'interface sérigraphiée 1 sur le boîtier.</p> <p>Adresse configurée sur l'interface : adresse configurée / masque de réseau.</p> <p>La présentation de la liste des interfaces indique l'appartenance d'une interface à un bridge ou d'un VLAN à une interface. Dans l'exemple ci dessous, le décalage de l'interface « out » indique qu'elle est contenu dans le bridge.</p> <p>Les informations concernant les interfaces PPTP sont dynamiques.</p>
-----------------	---

Exemple	<pre>F2004C09999999999999>ifinfo interface list: bridge 192.168.0.1/255.255.255.0 out (fxp0) dmz1 (protected,fxp2) serial (sl0) ipsec (l01) in (protected,fxp1) 10.0.0.254/255.0.0.0 F2004C09999999999999></pre>
----------------	--

ipnat

Description	Permet d'obtenir des informations sur la translation active sur le Firewall.
Commande	<code>ipnat -l</code>
Usage	L'envoi de la commande <i>ipnat -l</i> liste les règles configurées ainsi que celles en cours d'utilisation.
Résultat	<p>List of active MAP/Redirect filters : liste des règles de translations configurées dans le slot de translation actif. La grammaire de la règle de translation est la suivante [opération][interface][source][translaté]</p> <p>List of active sessions : liste des connexions subissant actuellement une translation. La grammaire de translation est la suivante [opération][source][soucreport][</p>
Exemple	<pre>F2004C09999999999999>ipnat -l List of active MAP/Redirect filters: List of active sessions: F2004C09999999999999></pre>

netstat

Description Affiche l'état des informations réseau reçues par l'IPS-Firewall.

Commande

```
netstat [-AaLnSW] [-f protocol_family | -p protocol]
        [-M core] [-N system]

netstat -i | -I interface [-abdnt] [-f address_family]
        [-M core] [-N system]

netstat -w wait [-I interface] [-d] [-M core] [-N system]

netstat -s [-s] [-z] [-f protocol_family | -p protocol] [-M core]

netstat -i | -I interface -s [-f protocol_family | -p protocol]
        [-M core] [-N system]

netstat -m [-M core] [-N system]

netstat -r [-AanW] [-f address_family] [-M core] [-N system]

netstat -rs [-s] [-M core] [-N system]

netstat -g [-W] [-f address_family] [-M core] [-N system]

netstat -gs [-s] [-f address_family] [-M core] [-N system]
```

Usage Cette commande est une commande native de freeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de freeBSD sur le site web www.freebsd.org.

Exemple

```
F2004C09999999999999>netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 Firewall_loopbac.ldap *.* LISTEN
Active UNIX domain sockets
Address Type Recv-Q Send-Q Inode Conn Refs Nextref Addr
46e518c0 stream 0 0 0 46e51960 0 0
46e51960 stream 0 0 0 46e518c0 0 0
...
...
46e51640 dgram 0 0 0 46d57f00 0 46e516e0
46e516e0 dgram 0 0 0 46d57f00 0 46e51780
46e51780 dgram 0 0 0 46d57f00 0 46e51820
46e51820 dgram 0 0 0 46d57f00 0 0
46d57f00 dgram 0 0 6d9a8c0 0 46e51640 0 /xxx
F2004C09999999999999>
```

sfctl

Description Permet une interaction avec le Module ASQ du Firewall NETASQ.

Attention cette commande touche aux fonctionnalités avancées du Firewall NETASQ. Son utilisation nécessite une bonne connaissance du Firewall. Certaines des commandes peuvent provoquer une coupures des connexions en cours.

Commande

```
sfctl [-F] <type> [-H] <host>
      | [-s] <type> [-H] <host>
      | [-A] <Address>, <name>, <Time>
      | [-a] <Address> | [-a] <name> | [-a] all
```

Usage L'envoi de la commande *sfctl -F <type>* remet à zéro certaines informations sur l'IPS-Firewall. Ces informations peuvent être :

- filter : purge de la liste des règles de filtrages active sur le Firewall. Cette commande coupe toutes les communications et nécessite la réactivation d'un nouveau slot de filtrage avant qu'une prochaine connexion ne puisse retraverser le Firewall.
- state : purge la table de connexion ainsi que la table de Hosts. Cette commande coupe toutes les connexions en cours sauf celle issu ou à destination du Firewall.
- count : purge les informations générées par l'option "compter" présente dans le filtrage.
- stat : purge les informations de statiques.
- All : équivalent de filter + state + count + stat. Cette commande coupe toutes les communications et nécessite la réactivation d'un nouveau slot de filtrage avant qu'une prochaine connexion ne puisse retraverser le Firewall.

L'envoi de la commande *sfctl -s <type>* affiche différentes informations sur l'IPS-Firewall. Ces informations peuvent être :

- filter : liste les règles de filtrages actives (explicites et implicites).
- state : liste le contenu de la table des connexions. attention le retour de cette commande se fait sur la première console du Firewall. Pour obtenir le résultat si la commande est lancée d'une autre console ou en SSH ou en HyperTerminal, tapez la commande : dmesg.
- host : liste la table des hôtes. host = adresse IP de l'hôte, interface : interface sur laquelle l'hôte a été enregistré par le Firewall (déterminé par l'interface sur laquelle le Firewall a reçu le premier paquet provenant de cet hôte), packet : nombre de paquets reçus sur l'interface à destination ou en provenance de cet hôte depuis qu'il a été enregistré par l'IPS-Firewall.
- Byte : idem que packet mais en taille.
- throughput : débit actuellemthroughpur : debit maximum atteint
- user : liste la table des utilisateurs authentifiées. Username : utilisateur authentifié, addr : adresse du host sur lequel s'est authentifié l'utilisateur, timeout : temps restant avant l'expiration de la période d'authentification.

(suite page suivante)

sfctl (suite)

Usage (suite)

- conn : liste la table des connexions du Firewall. client : émetteur de la requête, server : destinataire de la connexion, proto : protocole utilisé, sport : port source, dport : port destination, state : état de la connexion : C_SYN ou S_SYN : la connexion est en cours d'établissement (handshake), DATA : la connexion est établie et des données transitent. CLOSED : la connexion est terminée et va être supprimée de la table. CLOSE : La connexion est en cours de fermeture. RECOVERY : Cette état apparaît lorsqu'une connexion est maintenue après un reboot ou un basculement HA et que le Firewall est toujours en attente d'un paquet issu de cette connexion, plugin : plugin attaché à la connexion

- count : liste les informations générées par l'option "compter" présente dans le filtrage.

- qos : liste les informations liées à la qualité de service. (limitation de bande passante).

- stat : liste des informations de statistiques liées au Stateful.

- route : liste les informations concernant le source routing.

- limit : liste des limitations du modèle.

- all : liste toutes les informations détaillées ci-dessus.

L'option `-H` permet de réaliser un filtre sur un hôte en particulier. Cette option ne s'applique pas seule mais en complément de l'option `-s` ou `-F`. Ex : `sfctl -s conn -H 10.0.0.1` : n'affichera que les connexions liées à l'adresse 10.0.0.1, `sfctl -F state -H 10.0.0.1` : supprimera l'adresse 10.0.0.1 de la table des hôtes ainsi que toutes les connexions associées à cette adresse.

L'envoi de la commande `sfctl -T` vous permet d'accéder à un affichage de type « Top » des informations listées par la commande.

Exemple

```
F2004C09999999999999>sfctl -s host
```

```
host:
```

host	interface	rtid	packet	byte	throughput	mthroughput
10.x.xx.x	in	0000	5 p	125 b	88 b/s	167 b/s
10.x.xx.x	out	0000	1 p	15 b	15 b/s	25 b/s
10.x.xx.x	out	0000	0 p	0 b	0 b/s	1 b/s
10.x.xx.x	in	0000	0 p	0 b	0 b/s	1 b/s

```
F2004C09999999999999>
```

showSAD

Description	Permet de lister les Associations de Sécurité VPN actives sur le Firewall et ainsi connaître les tunnels VPN négociés.
--------------------	--

Commande	showSAD
-----------------	---------

Résultat	<p>82.x.x.x 213.x.x.x : Paramètres IP de la SA. Les SA sont unidirectionnelles.</p> <p>spi : Security Policy Index, identifiant unique de la SA</p> <p>reqid : identifiant d'association SA (Security Association) et SP (Security Policy).</p> <p>E: 3des-cbc : algorithme de chiffrement négocié</p> <p>A : hmac-sha1 : algorithme de Hachage négocié</p> <p>state : état de la SA : Cette état peut-être :</p> <ul style="list-style-type: none">- mature : la SA est valide et utilisée.- dying : la SA arrive à la fin de sa période de validité. Si il y a du trafic, une nouvelle SA mature doit se renégocier.- larval : la SA n'est pas encore négociée entièrement. <p>created : date de négociation de la SA, current : date actuel du système.</p> <p>diff : temps depuis lequel la SA été négociée.</p> <p>hard : durée de vie de la SA totale, soft : durée de vie de la SA avant renégociation.</p> <p>current : Quantité de données ayant été chiffrée ou déchiffrée par cette SA, Hard et soft : non utilisé par NETASQ (gestion des durées de vie de SA en fonction de la quantité de données transférée)</p>
-----------------	---

Exemple	<pre>F2004C0999999999999999999999999999>showSAD 82.XX.XX.XX 213.XX.XX.XX esp mode=tunnel spi=12066968 (0x00b82098) reqid=16387 (0x00004003) E:3des-cbc cb915a3a 9e039eef b3b0650f 58abb8bb 34066fb6 73e43119 A:hmac-sha1 72c103e1 a2b8a632 ee98251f ca9a6457 27a16cba replay=4 flags=0x00000000 state=mature created: Dec 26 11:40:40 2003 current= Dec 26 11:47:07 2003 Diff: 387(s) hard=600(s) soft=480(s) last: Dec 26 11:47:00 2003 hard=0(s) soft=0(s) current: 1144(bytes) hard=0(bytes) soft=0(bytes) allocated: 13 hard: 0 soft: 0 sadb seq=1 pid:40889 refcnt=2 82.XX.XX.XX 213.XX.XX.XX esp mode=tunnel spi=254028336 (0x0f242a30) reqid=16388 (0x00004004) E:3des-cbc 2fb9ea2a 02285bcc b0d03cda 6adef35f de2815bb 6ce1e00f A:hmac-sha1 1829ecb2 d4bdd946 8e94599b bcb93074 6e6cde8f replay=4 flags=0x00000000 state=mature created: Dec 26 11:40:40 2003 current= Dec 26 11:47:07 2003 Diff: 387(s) hard=600(s) soft=480(s) last: hard=0(s) soft=0(s) current: 0(bytes) hard=0(bytes) soft=0(bytes) allocated: 0 hard: 0 soft: 0 sadb seq=0 pid:40889 refcnt=1</pre>
----------------	--

showSPD

Description	Affiche les politiques de sécurité (Tunnels VPN) présentes sur l'IPS-Firewall
Commande	<code>showSPD</code>
Résultat	<p>10.x.x.x/24[any] 192.168.x.x [any] any : Adresses IP locales et distantes. [xxx] ports source et destination. En fin de ligne est spécifié le type de trafic autorisé.</p> <p>in/out : sens du trafic (entrant ou sortant).</p> <p>esp/tunnel/10.x.x.x-10.x.x.x/unique#17122 : reqid, identification d'une politique de sécurité (tunnels VPN) par rapport à une SA (Security Association).</p> <p>spid, seq, pid : identifiants de la politique de sécurité (pid : numéro du processus qui a lancé cette politique de sécurité, dans le cas de NETASQ c'est le processus racoon).</p>
Exemple	<pre>F2004C09999999999999>showSPD 10.x.x.x/24[any] 192.168.x.x[any] any in ipsec esp/tunnel/10.x.x.x-10.x.x.x/unique#17122 spid=882 seq=34 pid=67621 refcnt=1 F2004C09999999999999></pre>

slotinfo

Description	Permet une interaction avec les différents slot de configuration du Firewall (Filtrage, Transaltion, VPN, url).
--------------------	---

Commande	<code>slotinfo -a <type> -n <type> -f <type></code> <code>slotinfo</code>
-----------------	--

Usage	<p>L'envoi de la commande <i>slotinfo -a <type></i> permet de connaître le numéro du slot actif pour le type sélectionné.</p> <p>L'envoi de la commande <i>slotinfo -n <type></i> permet de connaître le nom du slot actif pour le type sélectionné.</p> <p>L'envoi de la commande <i>slotinfo -A <numero> <type></i> permet l'activation du slot <numero> pour le type sélectionné.</p> <p>L'envoi de la commande <i>slotinfo -f <type></i> affiche le chemin d'accès complet du slot actif pour le type demandé.</p> <p>L'envoi de la commande <i>slotinfo</i> seule n'est disponible que pour les IPS-Firewalls NETASQ en version supérieure à 5.0.9.</p>
--------------	--

Exemple	<pre>F2004C09999999999999>slotinfo -a filter 10 F2004C09999999999999>slotinfo -n filter pass all F2004C09999999999999>slotinfo -f filter /usr/Firewall/ConfigFiles/Filter/10 F2004C09999999999999></pre>
----------------	--

SVC

Description	Permet une interaction avec le module de supervision des différents services du Firewall.
Commande	<pre>svc -u <chemin_complet/nom_du_service> -d <chemin_complet/nom_du_service> -h <chemin_complet/nom_du_service></pre>
Usage	<p>L'envoi de la commande <code>svc -u <chemin_complet/nom_du_service></code> provoque le démarrage du service concerné.</p> <p>L'envoi de la commande <code>svc -d <chemin_complet/nom_du_service></code> provoque l'arrêt du service concerné.</p> <p>L'envoi de la commande <code>svc -h <chemin_complet/nom_du_service></code> provoque le rechargement du service concerné.</p>
Exemple	<pre>F2004C099999999999>svc -d /var/supervise/alarmd/ F2004C099999999999>svc -u /var/supervise/alarmd/ F2004C099999999999>svc -h /var/supervise/alarmd/ F2004C099999999999></pre>

sysctl

Description	Permet d'afficher ou de définir la configuration du noyau du firmware de l'IPS-Firewall.
Commande	<pre>sysctl [-beNnox] variable[=value] ... sysctl [-beNnox] -a</pre>
Usage	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
Exemple	<pre>kern.osrelease: 4.7-RELEASE-p23 kern.osrevision: 199506 kern.version: FreeBSD 4.7 - Netasq Firewall 5.0 p1003_1b.sigqueue_max: 0 p1003_1b.timer_max: 0 jail.set_hostname_allowed: 1 jail.socket_unixiproute_only: 1 jail.sysvipc_allowed: 0 F2004C09999999999999></pre>

sysinfo

Description	Permet d'obtenir un état détaillé sur la configuration et l'activité du Firewall.
--------------------	---

Commande	sysinfo
-----------------	---------

Usage	Etant donné la grande quantité d'informations remontées par la commande, il est conseillé de rediriger le résultat dans un fichier : sysinfo > /tmp/sysinfo par exemple.
--------------	--

Exemple	<pre>F2004C099999999999>sysinfo ##### # Software informations # ##### current date : 2004-01-30 12:41:01 Serial : F2004C099999999999 Model : F100-B Software : Netasq Firewall software ng38: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 ng39: flags=8890<POINTOPOINT,NOARP,SIMPLEX,MULTICAST> mtu 1500 ##### F2004C099999999999></pre>
----------------	---

tcpdump

Description	Affiche à l'écran l'entête des paquets transitant sur les interfaces de l'IPS-Firewall en fonction d'une expression définie.
--------------------	--

Commande	<pre>tcpdump [-adeflLnNOpqRStuvvX] [-c count] [-C file_size] [-F file] [-i interface] [-m module] [-r file] [-s snaplen] [-T type] [-w file] [-E algo:secret] [-y datalinktype] [expression]</pre>
-----------------	--

Résultat	Cette commande est une commande native de FreeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de FreeBSD sur le site web www.freebsd.org .
-----------------	--

Exemple	<pre>F2004C099999999999>tcpdump -i fxp0 proto esp or port isakmp tcpdump: listening on fxp 74 packets received by filter 0 packets dropped by kernel F2004C099999999999></pre>
----------------	--

top

Description Affiche les processus en cours d'exécution et d'importantes informations sur ceux-ci, telles que l'utilisation de la mémoire et de l'unité centrale. La liste est rafraîchie en temps réel.

Commande top

Résultat Cette commande est une commande native de freeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de freeBSD sur le site web www.freebsd.org.

Exemple last pid: 903; load averages: 0.00, 0.00, 0.00 up 0+04:09:39
15:33:13
9 processes: 1 running, 8 sleeping
CPU states: 0.0% user, 0.0% nice, 0.4% system, 0.0% interrupt, 99.6% idle
Mem: 3280K Active, 7332K Inact, 29M Wired, 3392K Buf, 19M Free
Swap: 257M Total, 257M Free

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
36	admin	10	0	2264K	932K	mfsidl	0:00	0.00%	0.00%	mount_mfs
903	admin	28	0	1840K	1112K	RUN	0:00	0.00%	0.00%	top
732	admin	10	0	2144K	1656K	wait	0:00	0.00%	0.00%	login
877	admin	10	0	1020K	888K	wait	0:00	0.00%	0.00%	bash
701	admin	3	0	944K	640K	ttyin	0:00	0.00%	0.00%	getty
702	admin	3	0	944K	644K	ttyin	0:00	0.00%	0.00%	getty
703	admin	3	0	944K	644K	ttyin	0:00	0.00%	0.00%	getty
465	admin	2	0	276K	144K	poll	0:00	0.00%	0.00%	supervise
457	admin	2	0	276K	132K	poll	0:00	0.00%	0.00%	supervise

Commande de configuration

Description	Ce chapitre présente des commandes indispensables lors de la configuration de l'IPS-Firewall. Notez que nsrpc est un outil particulièrement évolué pour la configuration d'un IPS-Firewall.
--------------------	---

Index	La liste suivante liste l'ensemble des commandes qui sont évoquées dans cette section du document :
--------------	---

chpwd	ensnmp
cleanfw	enproxy
clearlog	entimezone
date	enurl
enalarm	envpn
enauth	getconf
enavp	globalgen
endhcp	nsrpc
endialup	ntpq
endns	setconf
enevent	
enfilter	
engui	
enha	
enkeyboard	
enldap	
ennat	
ennetwork	
enntp	
enobject	
enservice	

chpwd

Description	Permet la modification du mot de passe de l'utilisateur "admin".
Commande	chpwd
Usage	Cette commande est à utiliser dans le cadre d'utilisation du mode single, préférez <i>fwpasswd</i> dans le cas contraire.
Résultat	Un nouveau mot de passe est demandé. Attention minimum 8 caractères. Le firewall redémarre après confirmation du mot de passe
Exemple	<pre>F2004C09999999999999>chpwd You are now with the keyboard langage configured on Firewall ##### ## Change SRP/SSH password for admin ## ##### setting password for admin enter password: verify: Modify SRP/SSH password of user 'admin' successful Firewall Rebooting ! Shutdown NOW! shutdown: [pid 738] *** FINAL System shutdown message from admin@F2004C09999999999999 *** System going down IMMEDIATELY</pre>

cleanfw

Description	Permet la réinitialisation du Firewall. Remise en configuration par défaut + purge des logs.
--------------------	--

Commande	<code>cleanfw</code>
-----------------	----------------------

Usage	Cette commande nécessite le redémarrage de l'IPS-Firewall (cf reboot).
--------------	--

Exemple	<pre>F2004C099999999999>cleanfw F2004C099999999999></pre>
----------------	---

clearlog

Description	Permet la suppression des fichiers de traces stockés sur le Firewall.
--------------------	---

Commande	<code>clearlog < logname ></code>
-----------------	---

Résultat	<p>Type de log :</p> <p>filter : trace de filtrage alarm : traces d'alarmes auth : log d'authentification connection : traces de connexion count : trace de l'option compter filterstat : trace des statistiques de filtrage natstat : trace des statistiques de filtrage plugin : trace générées par l'utilisation des plugins server : trace de l'historique du manager smtp : traces du proxy SMTP system : événements système vpn : traces VPN web : traces générés par le proxy HTTP (filtrage URL)</p>
-----------------	---

Exemple	<pre>F2004C09999999999999>clearlog alarm Log cleared F2004C09999999999999></pre>
----------------	--

date

Description	Permet l'affichage ou la modification de la date du Firewall.
--------------------	---

Commande	Date [-u] [-d] « YYYY-MM-DD hh:mm:ss »
-----------------	--

Usage	L'envoi de la commande <i>date</i> seule renvoie la date actuelle au format NETASQ L'envoi de la commande <i>date -u</i> affiche la date au format UNIX L'envoi de la commande <i>date -d</i> affiche la date au format NETASQ sans fuseau horaire L'envoi de la commande <i>date « YYYY-MM-DD hh:mm:ss »</i> modifie la date actuelle à la date indiquée.
--------------	---

La modification de la date de l'IPS-Firewall est interdite si le service NTP est activé.

Exemple	<pre>F2004C099999999999>date "2004-01-15 15:37:29" zone=GMT tz=+0000 ntp=Off F2004C099999999999>date -u Thu Jan 15 15:37:32 GMT 2004 F2004C099999999999>date -d 2004-01-15 15:37:34 F2004C099999999999>date "2004-01-16" "2004-01-16 15:37:47" zone=GMT tz=+0000 ntp=Off F2004C099999999999></pre>
----------------	---

enalarm

Description	Permet de recharger les paramètres de configuration des alarmes et des traces après modification du fichier /Firewall/ConfigFiles/alarm ou /Firewall/ConfigFiles/asq.
--------------------	---

Commande	<code>enalarm</code>
-----------------	----------------------

Exemple	<pre>F2004C099999999999>enalarm F2004C099999999999></pre>
----------------	---

enauth

Description	Permet de recharger les paramètres de configuration de l'authentification du fichier /Firewall/ConfigFiles/auth.
Commande	<code>enauth</code>
Exemple	<pre>F2004C09999999999999>enauth F2004C09999999999999></pre>

enavp

Description	Permet de recharger les paramètres de configuration du service anti-virus après modification du fichier /Firewall/ConfigFiles/AVP/avp.
Commande	<code>enavp</code>
Résultat	« enavp: kavdaemon is missing » : si ce message apparaît, la fonction antivirus n'est pas active sur ce firewall.
Exemple	<pre>F2004C099999999999>enavp F2004C099999999999></pre>

endhcp

Description	Permet de recharger les paramètres de configuration du serveur DHCP après modification du fichier /Firewall/ConfigFiles/dhcp.
Commande	<code>endhcp</code>
Exemple	<pre>F2004C099999999999>endhcp F2004C099999999999></pre>

endialup

Description	Permet de recharger les paramètres de configuration des dialup après modification du fichier /Firewall/ConfigFiles/network en version 5 ou /Firewall/ConfigFiles/dialup en version inférieure à 5.
Commande	<code>endialup</code>
Résultat	Toutes les connexions dialup sont renégociées. Attention la connexion Internet, le filtrage de NAT et les tunnels VPN en cours sont réinitialisés.
Exemple	<pre>F2004C099999999999>endialup F2004C099999999999></pre>

endns

Description	Permet de recharger les paramètres de configuration du service DNS après modification du fichier /Firewall/ConfigFiles/dns.
Commande	<code>endns</code>
Exemple	<pre>F2004C09999999999999> endns F2004C09999999999999></pre>

enevent

Description	Permet de recharger les paramètres de configuration des programmations événementielles (ex : programmation horaire de slot) après modification des fichiers du répertoire « Event ».
--------------------	--

Commande	<code>enevent</code>
-----------------	----------------------

Exemple	<pre>F2004C099999999999> enevent F2004C099999999999></pre>
----------------	--

enfilter

Description	Permet l'activation ou la réactivation après modification d'un slot de filtrage.
Commande	<pre>enfilter [-f] < -u slotnumber > enfilter on enfilter off</pre>
Usage	<p>L'envoi de la commande <i>enfilter XX</i> permet d'activer le slot de filtrage n° XX (les slots de filtrage sont nommés de 01 à 10).</p> <p>L'envoi de la commande <i>enfilter -u</i> permet la réactivation du slot actuellement actif. Cela est notamment utilisé après une modification du slot actif.</p> <p>L'option <i>-f</i> permet de forcer l'activation du slot de filtrage défini.</p> <p>L'envoi de la commande <i>enfilter off</i> permet de désactiver le filtrage de l'IPS-Firewall. L'IPS-Firewall NETASQ se comporte alors comme un « pass all ».</p> <p>L'envoi de la commande <i>enfilter on</i> permet de réactiver le dernier slot de filtrage actif.</p>
Résultat	<p>« Current slot » = nom du slot : l'opération a réussi et le slot est actif.</p> <p>« Error : reactivatind previous slot » : L'opération n'a pu être effectuée, le slot de filtrage actif avant le passage de la commande a été réactivé. Lors de ce type d'erreur, un message plus explicite sur la raison de l'erreur est remonté.</p>
Exemple	<pre>F2004C09999999999999>enfilter 10 current slot = pass all F2004C09999999999999></pre>

engui

Description	Permet la réactivation du serveur d'administration de l'IPS-Firewall gérant les connexions au Firewall par les outils de la suite d'administration du Firewall (Manager, Monitor, Reporter, Collector, Global Update).
--------------------	--

Commande	engui
-----------------	-------

Exemple	F2004C099999999999>engui F2004C099999999999>
----------------	---

enha

Description	Permet de recharger les paramètres de configuration de la haute disponibilité après modification du fichier /Firewall/ConfigFiles/highavailability.
Commande	<code>enha</code>
Résultat	« HA isn't enabled! » : ce message vous indique le Haute disponibilité n'est pas disponible sur votre boîtier.
Exemple	<pre>F2004C09999999999999>enha F2004C09999999999999></pre>

enkeyboard

Description	Permet de recharger les paramètres de configuration du clavier après modification du fichier /Firewall/ConfigFiles/language.
--------------------	--

Commande	enkeyboard
-----------------	------------

Exemple	F2004C099999999999>enkeyboard F2004C099999999999>
----------------	--

enldap

Description	Permet de recharger les paramètres de configuration de la base LDAP après modification du fichier /Firewall/ConfigFiles/ldap.
Commande	<code>enldap</code>
Exemple	<pre>F2004C09999999999999>enldap F2004C09999999999999></pre>

ennat

Description	Permet l'activation ou la réactivation après modification d'un slot de Translation.
--------------------	---

Commande	<code>ennat -u < slotnumber ></code>
-----------------	--

Usage	<p>L'envoi de la commande <i>ennat XX</i> permet d'activer le slot de translation n° XX (les slots de translation sont nommés de 01 à 10).</p> <p>L'envoi de la commande <i>ennat 00</i> désactive la translation d'adresse.</p> <p>L'option <i>-u</i> vide la table des sessions NAT.</p>
--------------	--

Résultat	<p>« Current slot » = nom du slot : l'opération a réussi et le slot est actif.</p> <p>« Error : reactivatind previous slot » : L'opération n'a pu être effectuée, le slot de translation actif avant le passage de la commande a été réactivé. Lors de ce type d'erreur, un message plus explicite sur la raison de l'erreur est remonté.</p>
-----------------	---

Exemple	<pre>F2004C09999999999999>ennat 01 Current slot = slot nat 10 F2004C09999999999999></pre>
----------------	---

ennetwork

Description	Permet de recharger les paramètres de configuration du Réseau après modification du fichier /Firewall/ConfigFiles/network.
Commande	<code>ennetwork [-r]</code>
Usage	L'option <code>-r</code> permet d'activer les modifications réseau uniquement relative au routage.
Exemple	<pre>F2004C099999999999>ennetwork F2004C099999999999></pre>

enntp

Description	Permet de recharger les paramètres de configuration du service NTP après modification du fichier /Firewall/ConfigFiles/ntp.
Commande	enntp
Exemple	F2004C09999999999999>enntp F2004C09999999999999>

enobject

Description	Permet de recharger la liste des objets du Firewall après modification d'un des fichiers contenant les définitions d'objets : /Firewall/ConfigFiles/object : fichier comprenant les objets : machines, réseau, services et protocoles. /Firewall/ConfigFiles/networkgroup : fichier comprenant les objets : groupe de réseaux /Firewall/ConfigFiles/servicegroup : fichier comprenant les objets : groupe de services. /Firewall/ConfigFiles/hostgroup : fichier comprenant les objets : groupe de machines.
--------------------	--

Commande	enobject
-----------------	----------

Exemple	F2004C099999999999>enobject F2004C099999999999>
----------------	--

enservice

Description	Permet de recharger la configuration des services après une modification du fichier /Firewall/Configfiles/network dans la section « Service ».
--------------------	--

Commande	<code>enservice</code>
-----------------	------------------------

Exemple	<pre>F2004C099999999999>enservice F2004C099999999999></pre>
----------------	---

ensnmp

Description	Permet de recharger les paramètres de configuration du service SNMP après modification du fichier /Firewall/ConfigFiles/snmp.
Commande	<code>ensnmp</code>
Exemple	<pre>F2004C09999999999999>ensnmp F2004C09999999999999></pre>

enproxy

Description	Permet de recharger les paramètres de configuration des proxy HTTP et SMTP après modification du fichier /Firewall/ConfigFiles/httpproxy, /Firewall/ConfigFiles/smtpproxy ou /Firewall/ConfigFiles/proxy.
--------------------	---

Commande	enproxy
-----------------	---------

Exemple	F2004C09999999999999>enproxy F2004C09999999999999>
----------------	---

entimezone

Description	Permet de modifier ou de lister les paramètres de configuration du Fuseau horaire du Firewall.
--------------------	--

Commande	<code>entimezone [-l] [-s] <zone_name></code>
-----------------	---

Usage	<p>L'envoi de la commande <i>entimezone -l</i> liste les différents fuseau horaire disponible.</p> <p>L'envoi de la commande <i>entimezone -s <zone_name></i> change le fuseau horaire de l'IPS-Firewall pour être prise en compte et une synchronisation de l'IPS-Firewall passif dans le cas d'une utilisation en haute disponibilité.</p>
--------------	--

Exemple	<pre>F2004C09999999999999>entimezone -l Africa/ Africa/Algiers Africa/Luanda Africa/Porto-Novo Africa/Gaborone Africa/Ouagadougou Africa/Bujumbura Pacific/Midway Pacific/Wake Pacific/Efate Pacific/Wallis Pacific/Honolulu Pacific/Easter Pacific/Galapagos WET F2004C09999999999999>entimezone -s Europe/Paris timezone change : GMT -> Europe/Paris. Need reboot. If HA is enabled, need HA sy nchronisation F2004C09999999999999></pre>
----------------	--

enurl

Description	Permet l'activation ou la réactivation après modification d'un slot de filtrage URL.
Commande	<code>enurl < slotnumber ></code>
Usage	<p>L'envoi de la commande <i>enurl XX</i> permet d'activer le slot de filtrage d'URL n° XX (les slots de filtrage d'URL sont nommés de 01 à 10).</p> <p>L'envoi de la commande <i>enurl 00</i> désactive de proxy HTTP. Si une commande <i>enurl XX</i> est passée alors que le proxy HTTP est désactivé, cela active le proxy.</p>
Résultat	<p>« Current slot » = nom du slot : l'opération a réussi et le slot est actif.</p> <p>« Error : reactivatind previous slot » : L'opération n'a pu être effectuée, le slot de filtrage actif avant le passage de la commande a été réactivé. Lors de ce type d'erreur, un message plus explicite sur la raison de l'erreur est remonté.</p>
Exemple	<pre>F2004C09999999999999>enurl 01 F2004C09999999999999></pre>

envpn

Description	Permet l'activation ou la réactivation après modification d'un slot de configuration VPN.
Commande	<pre>envpn [-u] < slotnumber > envpn off</pre>
Usage	<p>L'envoi de la commande <i>envpn XX</i> permet d'activer le slot de configuration VPN n° XX (les slots de configuration VPN sont nommés de 01 à 10).</p> <p>L'option <i>-u</i> permet la réactivation du slot actuellement actif. Cela est notamment utilisé après une modification du slot actif.</p> <p>L'envoi de la commande <i>envpn off</i> permet de désactiver les tunnels VPN sur l'IPS-Firewall.</p>
Résultat	<p>« Current slot » = nom du slot : l'opération a réussi et le slot est actif.</p> <p>« Error : reactivatind previous slot » : L'opération n'a pu être effectuée, le slot de configuration VPN actif avant le passage de la commande a été réactivé. Lors de ce type d'erreur, un message plus explicite sur la raison de l'erreur est remonté.</p>
Exemple	<pre>F2004C09999999999999>envpn 01 F2004C09999999999999></pre>

fwpasswd

Description	Permet la modification du mot de passe de l'utilisateur "admin".
--------------------	--

Commande	fwpasswd
-----------------	----------

Usage	L'envoi de la commande <i>fwpasswd</i> donne accès au menu de configuration du mot de passe de l'utilisateur « admin ». Il est nécessaire de redémarrer l'IPS-Firewall pour que les modifications soient prises en compte.
--------------	--

Exemple	<pre>F2004C099999999999>fwpasswd ##### ## Change SRP/SSH password for admin ## ##### setting password for admin enter password: verify: Modify SRP/SSH password of user 'admin' successful F2004C099999999999></pre>
----------------	--

getconf

Description	Retourne la valeur du champ défini par la commande.
Commande	<pre>getconf [-i < index >] < file > < section > < item > [< default >] getconf -l < file > < section > < item > [< default >]</pre>
Usage	<p>L'envoi de la commande <i>getconf</i> <i><file></i> <i><section></i> <i><item></i> permet d'afficher la valeur du token <i><item></i> de la section <i><section></i> dans le fichier de configuration <i><file></i>.</p> <p>Dans certains cas, le token en question peut posséder plusieurs valeurs, l'option <i>-i</i> permet alors de spécifier quelle valeur doit être affichée.</p> <p>L'option <i>-l</i> permet de spécifier que le fichier que l'on souhaite interroger est la licence de l'IPS-Firewall.</p> <p>Le terme [<i><default></i>] permet de spécifier la valeur devant être retournée si un des termes (file, section ou item) défini dans la commande n'est pas trouvé par l'IPS-Firewall.</p>
Exemple	<pre>F2004C09999999999999>getconf /usr/Firewall/ConfigFiles/network ethernet1 Address 10.X.X.XF2004C0999999999999></pre>

globalgen

Description	Permet de forcer la détection du nombre d'interfaces disponibles. Cette commande est généralement utilisée après avoir ajouter des interfaces réseaux dans le Firewall.
Commande	<code>globalgen</code>
Usage	Attention, cette commande peut entraîner le réordonnancement des interfaces.
Résultat	« globalgen: x interfaces detected » où x représente le nombre d'interfaces détectées par le système. Attention, les interfaces non comprises dans la licence du Firewall ne sont pas détectées par cette commande.
Exemple	<pre>F2004C099999999999>globalgen globalgen: 3 interfaces detected F2004C099999999999></pre>

nsrpc

Description	Accès au Firewall Manager en ligne de commande.
--------------------	---

Commande	<code>nsrpc [-f] [-r] <user>@127.0.0.1</code>
-----------------	---

Usage	L'envoi de la commande <i>nsrpc admin@127.0.0.1</i> vous permet de vous connectez en tant qu'utilisateur « admin » sur l'IPS-Firewall sur lequel vous effectuez la commande. Il est possible de se connecter à distance sur un autre IPS-Firewall. La commande est alors la suivante <i>nsrpc admin@10.x.x.x</i> si l'IPS-Firewall possède l'adresse IP 10.x.x.x.
--------------	---

L'option `-f` permet de forcer la connexion de l'utilisateur « admin ».

L'option `-r` permet de spécifier les droits auxquels l'utilisateur veut avoir accès. La liste des droits se présente alors sous une chaîne de droits séparés par une virgule sans espace. Les droits que vous pouvez spécifier sont les suivants : modify, base, other, log, filter, vpn, url, pki, object, user, admin.

Exemple	<pre>F2004C09999999999999>nsrpc admin@127.0.0.1 Welcome to Netasq Cipher/SRP client Enter password: Connecting to 127.0.0.1... Using SRP authentication only. User=admin Level="modify,base,other,log,filter,vpn,url,pki,object,user,admin" SessionLevel="modify,base,other,log,filter,vpn,url,pki,object,user,admin" Netasq></pre>
----------------	---

ntpq

Description	Interpréteur de commande ntp
Commande	<code>ntpq [-dinp] [-c cmd] host ...</code>
Résultat	Cette commande est une commande native de freeBSD (système sur lequel le NSBSD NETASQ est bâti). Pour obtenir plus d'informations reportez-vous à la documentation de freeBSD sur le site web www.freebsd.org .
Exemple	<pre>F2004C09999999999999>ntpq ntpq> ntpq>quit F2004C09999999999999></pre>

setconf

Description	Permet de définir une valeur pour un champ dans un fichier donné.
Commande	<code>setconf < file > < section > < item > < value ></code>
Usage	L'envoi de la commande <i>setconf</i> <i><file></i> <i><section></i> <i><item></i> <i><value></i> permet de spécifier la valeur <i><value></i> du token <i><item></i> de la section <i><section></i> du fichier <i><file></i> .
Exemple	<pre>F2004C099999999999>setconf /usr/Firewall/ConfigFiles/network Ethernet1 Address 10.x.x.x F2004C099999999999></pre>

Commande d'informations diverses

Description	Ce chapitre présente quelques commandes complémentaires aux deux chapitres précédents. Ces commandes ne sont pas spécifiquement associées au diagnostic, la maintenance ou la configuration mais participe tout de même à l'utilisation de l'IPS-Firewall
--------------------	---

Index	La liste suivante liste l'ensemble des commandes qui sont évoquées dans cette section du document :
--------------	---

	<code>authd</code> <code>backupinfo</code> <code>certinfo</code> <code>crlinfo</code> <code>getmodel</code> <code>getversion</code> <code>halt</code> <code>reboot</code> <code>tproxyd</code>
--	--

authd

Description	Affiche les informations de configuration correspondant au module d'authentification des IPS-Firewalls NETASQ.
--------------------	--

Commande	<code>authd -s</code>
-----------------	-----------------------

Exemple	<pre>F2004C099999999999>authd -s Webserver up : Ezadmin shared F2004C099999999999></pre>
----------------	---

backupinfo

Description	Permet de connaître la version de la partition de Backup permettant la sauvegarde et la restauration du système.
--------------------	--

Commande	<code>backupinfo</code>
-----------------	-------------------------

Résultat	<p>Active : partition sur laquelle le système est démarré (Main / Backup) BackupVersion : Version de la partition inactive Date : Date de création de la partition inactive</p> <p>Si le résultat est : No backup partition found, soit le Firewall n'est pas équipé d'une partition de backup ou aucune sauvegarde système n'a été faite.</p>
-----------------	--

Exemple	<pre>F1003D011690999999>backupinfo Active=Main BackupVersion="5.0.7.1" Date="2003-12-09 16:02:04" F2004C099999999999></pre>
----------------	---

certinfo

Description	Affiche les informations relatives au certificat défini dans la commande.
Commande	<code>certinfo < certfile ></code>
Résultat	Cette commande affiche entre autres le résultat de la fonction de hachage (Hash), la version du certificat, les algorithmes de signature et de chiffrement (SignatureAlgorithm, PublicKeyAlgorithm)...
Exemple	<pre>F2004C099999999999>certinfo netasq.ca [Global] Hash=cb7b190d Version=03 SerialNumber=00 SignatureAlgorithm=md5WithRSAEncryption Issuer="/C=FR/ST=Nord/O=NETASQ - Secure Internet Connectivity/OU=NETASQ Firewall Certification Authority/L=Villeneuve d'Ascq" NotBefore="May 14 12:15:25 2002 GMT" NotAfter="May 14 12:15:25 2022 GMT" Subject="/C=FR/ST=Nord/O=NETASQ - Secure Internet Connectivity/OU=NETASQ Firewal l Certification Authority/L=Villeneuve d'Ascq" PublicKeyAlgorithm=rsaEncryption SignatureAlgorithm=md5WithRSAEncryption F2004C099999999999></pre>

crlinfo

Description	Affiche les informations relatives à la CRL définie dans la commande.
Commande	<code>crlinfo < crlfile ></code>
Résultat	Cette commande affiche entre autres le résultat de la fonction de hachage (Hash), la version de la CRL, les algorithmes de signature (SignatureAlgorithm) et les certificats révoqués (RevokedCertificates).
Exemple	<pre>F2004C09999999999999>crlinfo netasq_crl.pem [Global] Hash=99b2031a Version=02 Issuer="/C=FR/ST=NORD/O=NETASQ/OU=NPI/L=VDA" LastUpdate="Feb 18 15:08:45 2004 GMT" NextUpdate="Mar 20 15:08:45 2004 GMT" SignatureAlgorithm=md5WithRSAEncryption [RevokedCertificates] F2004C09999999999999></pre>

getmodel

Description	Permet de connaître le modèle de Firewall.
--------------------	--

Commande	getmodel
-----------------	----------

Exemple	<pre>F2004C099999999999>getmodel F100-B F2004C099999999999></pre>
----------------	---

getversion

Description	Permet d'obtenir la version actuelle du Firewall.
--------------------	---

Commande	getversion
-----------------	------------

Exemple	<pre>F2004C099999999999>getversion Firewall software version 5.0.7.1 F2004C099999999999></pre>
----------------	--

halt

Description	Provoque un arrêt de l'IPS-Firewall. Attention aucune confirmation n'est demandée. L'action d'arrêt de l'IPS-Firewall entraîne le basculement des IPS-Firewalls en haute disponibilité si besoin (si l'IPS-Firewall actif s'arrête).
--------------------	--

Commande	<code>halt</code>
-----------------	-------------------

Exemple	<pre>1003D011690200701>halt Shutdown NOW! shutdown: [pid 829] *** FINAL System shutdown message from admin@F2004C0999999999999 *** System going down IMMEDIATELY</pre>
----------------	--

reboot

Description	Provoque un redémarrage de l'IPS-Firewall. Attention aucune confirmation n'est demandée. L'action de redémarrage de l'IPS-Firewall stoppe le monitoring de la HA.
--------------------	---

Commande	reboot
-----------------	--------

Exemple	<pre>F2004C099999999999>reboot Shutdown NOW! shutdown: [pid 712] *** FINAL System shutdown message from admin@F2004C099999999999 *** System going down IMMEDIATELY F2004C099999999999> System shutdown time has arrived</pre>
----------------	---

tproxyd

Description	Affiche les informations de configuration correspondant aux proxies NETASQ.
Commande	<code>tproxyd [-s] [-l]</code>
Usage	<p>L'envoi de la commande <i>tproxyd -s</i> affiche la configuration actuelle des différents proxies de l'IPS-Firewall NETASQ.</p> <p>L'envoi de la commande <i>tproxy -l</i> affiche la configuration actuelle des règles de filtrage d'URLs.</p>
Exemple	<pre>F2004C09999999999999>tproxyd -s Authentication disable url : IP (authd redirect) Real transparent proxy disable -- Antiviral : disable -- Http proxy : disable -- Smtip proxy : disable F2004C09999999999999></pre>