



# **FORCEPOINT**

## **Sidewinder**

### **Command Line Interface Reference Guide**

**8.3.x**

Revision B

# Table of contents

<b>1 About the command line interface.....</b>	<b>3</b>
About the cf command.....	3
Integrated manual pages.....	3
<b>2 Log on at the command line interface.....</b>	<b>5</b>
<b>3 Frequently used commands.....</b>	<b>6</b>
Administrator accounts.....	6
Anti-virus.....	6
Audit.....	7
Configuration backups.....	8
DNS.....	8
Downloads.....	9
Emergency maintenance mode (EMM).....	9
File system.....	10
Firewall self-diagnostics.....	10
General cf commands.....	11
High Availability.....	11
Interfaces.....	11
Licensing.....	12
Manual pages.....	12
McAfee EIA.....	13
Networking.....	13
NTP.....	14
Policy.....	14
Routing.....	15
Security zones and groups.....	16
sendmail.....	16
Shutdown.....	17
Software management.....	17
System.....	18
tcpdump.....	19
Technical support.....	19
Text editors and viewers.....	20
Type Enforcement.....	20
VPN.....	20
<b>4 Available cf areas.....</b>	<b>22</b>

# About the command line interface

---

If you are experienced with UNIX, you can use the Forcepoint™ Sidewinder® command line interface to configure the firewall and perform troubleshooting.

The command line interface supports many firewall-specific commands as well as standard UNIX commands. For example, the `cf` command performs a wide range of firewall configuration tasks.

You can access the command line interface using these methods:

- Locally attached console
- SSH
- Telnet

For more information about these methods, see the *Forcepoint Sidewinder Product Guide*.

## About the `cf` command

---

The `cf` (configure firewall) command configures various areas such as rules, zones, and interfaces. You can use the `cf` command as an alternative to the Admin Console to perform most administration tasks.

To accomplish a task using `cf`, combine the `cf` area with the appropriate command, optional arguments, and optional keys. For more information, see *General `cf` commands*.

*Example:* `cf zone query` displays the configured security zones.



**Tip:** You can use the `cf` command in scripts to automate repetitive configuration tasks or to make configuration changes when the Admin Console is not available.

The `cf` commands and keys ignore dashes, underscores, and capital letters. You can shorten most commands and keys.

*Example:* These commands return the same output:

```
cf policy query dest_zone=external
cf pol q destz=external
```



**Note:** Key values — text to the right of the equals sign — might not ignore dashes, underscores, and capital letters. Key values might be shortened if it represents an enumeration such as an object name.

To view a list of available `cf` areas, enter:

```
cf -h
```

### Related reference

[General `cf` commands](#) on page 11

Use these commands to view `cf` man pages and control the behavior of `cf` commands.

## Integrated manual pages

---

The command line interface includes integrated manual (`man`) pages for most commands.

To view a `man` page, type `man` followed by the name of a command, then press **Enter**.

*Example:* `man ping`

The man page for `cf` provides a full description of all areas available in the `cf` command and the options associated with each area.

- To view the man page for the `cf` command, enter:

```
man cf
```

- To view the man page for a specific `cf` area, enter:

```
man cf_area
```

*Examples:*

- `man cf_policy`
- `man cf_interface`
- To display all commands related to a specific command, enter:

```
man -k command
```

# Log on at the command line interface

---

You must run the `srole` command before you can use most commands.

1. At the logon prompt, type your user name, then press **Enter**. The Password prompt appears.
2. Type your password, then press **Enter**. The User domain prompt appears:  
`firewall_name:User {1} %`
3. Enter the `srole` command to change to the Admn domain.
4. When you are finished, enter the `exit` command to return to the User domain.

# Frequently used commands


This section lists basic UNIX commands and commands that are specific to Sidewinder.

- For additional information about a command, refer to the man page.
- For additional troubleshooting information, see the *Forcepoint Sidewinder Product Guide*.

## Administrator accounts

Use these commands to manage administrator accounts.

**Table 1: Administrator account commands**

Command	Description
<code>man cf_adminuser</code>	Displays the man page for cf adminuser.
<code>cf adminuser add username=<i>username</i> password=<i>password</i> role=admin directory= home/<i>username</i></code>	Creates an administrator account.
<code>cf adminuser add username=<i>username</i> password=<i>password</i> role=adminro directory= home/<i>username</i></code>	Creates a read-only user account. <div> <b>Note:</b> The adminro role is available for firewalls at version 8.3.2 and later.</div>
<code>cf adminuser delete username=<i>username</i></code>	Deletes an administrator account.
<code>cf adminuser modify user=<i>username</i> password=<i>newpassword</i></code>	Changes the password for an administrator account.
<code>cf adminuser query</code>	Displays the administrator user database.

## Anti-virus

Use these commands to manage the anti-virus feature.


**Table 2: Anti-virus commands**

Command	Description
<code>man cf_antivirus</code>	Displays the man page for cf antivirus.
<code>cf antivirus query</code>	Displays the anti-virus configuration.
<code>cf antivirus version</code>	Displays the version of the anti-virus engine and detection definition (DAT) files.
<code>cf daemon restart agent=virus-scan</code>	Restarts the anti-virus engine.
<code>cf antivirus applyavpatch patch=<i>patch_name</i></code>	Installs an anti-virus engine patch without restarting the firewall.
<code>cf antivirus download</code>	Downloads the latest DAT files.

# Audit

Use these commands to configure and view audit.

**Table 3: Audit commands**

Command	Description
<code>cf acl set loglevel=[1–4]</code>	Configures the audit output level for rules to control what is logged: <b>1</b> — Fatal errors only <b>2</b> — [Default] Fatal errors, major errors, and denied rules <b>3</b> — Fatal errors, major errors, denied rules, and allowed rules <b>4</b> — Everything (for troubleshooting only)  <b>Note:</b> See the <i>Policy</i> area for commands about rules.
<code>acat &gt; /var/tmp/audit.txt</code>	Writes the contents of the binary <code>/var/log/audit.raw</code> file to the ASCII text file <code>/var/tmp/audit.txt</code> .
<code>acat /var/log/audit.raw.time1.time2.gz &gt; /var/tmp/audit.txt</code>	Writes the contents of the specified compressed binary audit file to the ASCII text file <code>/var/tmp/audit.txt</code> .
<code>acat -k</code>	Shows all audits in real time.
<code>acat_acls -d</code>	Shows audits for policy denies in real time.
<code>acat_acls -a</code>	Shows audits for policy allows in real time.
<code>acat -c</code>	Displays all the possible options for a <code>sacap_filter</code> .
<code>showaudit -kp</code>	Shows netprobe audits in real time.
<code>showaudit -kH X.X.X.X</code>	Shows audits pertaining to the IP address <code>X.X.X.X</code> in real time.
<code>rollaudit -R d -w</code>	Rolls log files (such as <code>audit.raw</code> ).
<code>cf daemond enable agent=auditdbd</code>	Enables the audit server. Reports will not generate until this server is enabled.
<code>cf usage show type=report_name hours=[1–24]</code>	Displays a usage report for the specified number of hours.
<code>cf usage show type=report_name days=[1–180]</code>	Displays a usage report for the specified number of days.
<code>man cf_usage</code>	Displays the man page for <code>cf usage</code> . This includes the list of usage reports.
<code>cf passport list</code>	Displays the currently issued Passports.
<code>blackhole dump</code>	Lists IP addresses that are currently blackholed by audit responses and IPS responses.

## Related reference

[Policy](#) on page 14

Use these commands to troubleshoot policy issues.

## Configuration backups

Use these commands to create and restore configuration backups.

**Table 4: Configuration backup commands**

Command	Description
<code>cf config backup loc=local filename=<i>filename</i> key=<i>password</i></code>	Saves a configuration backup in the local <code>/var/backups/</code> repository directory.
<code>cf config backup loc=USB filename=<i>filename</i> key=<i>password</i></code>	Saves a configuration backup to a USB drive.
<code>cf config backup loc=remote address=<i>destination</i> user=<i>username</i> password=<i>password</i> key=<i>password</i></code>	Saves a configuration backup to a remote host using SCP.
<code>cf config restore loc=<i>location</i> filename=<i>filename</i> key=<i>password</i></code>	Restores a configuration backup; specify local, remote, or USB.
<code>cf config compare to=<i>filename1</i> from=<i>filename2</i></code>	Displays the differences between two configuration backup files.
<code>cf config getinfo location=<i>local/usb</i> filename=<i>filename</i></code>	Displays meta-information about the specified configuration backup.

## DNS

Use these commands to configure and troubleshoot DNS.

**Table 5: DNS commands**

Command	Description
<code>cf dns query</code>	Displays the current DNS server configuration.
<code>cf dns status</code>	Displays the status of the firewall-hosted DNS servers.
<code>cf daemon restart agent=named-internet</code>	Restarts the Internet DNS server.
<code>cf daemon restart agent=named-unbound</code>	Restarts the unbound DNS server.
<code>cf dns reload</code>	Reloads DNS zone and configuration files.
<code>cf dns dumpdb</code>	Writes the DNS database in memory to the file specified by <code>named.conf</code> .
<code>cf dns trace</code>	Enables debug tracing to <code>/var/run/named.run.i</code> and <code>/var/run/named.run.u</code> .
<code>cf dns notrace</code>	Disables tracing.
<code>hostname</code>	Displays the firewall host name.
<code>named-checkconf /etc/named.conf. [u/i]</code>	Checks DNS configuration file syntax.



Command	Description
<code>named-checkzone zone /etc/namedb.[i/u]/file.db</code>	Checks a zone file for correct syntax.
<code>dig host.domain.tld</code>	Queries the default DNS server information about host.domain.tld.
<code>dig @X.X.X.X host.domain.tld</code>	Queries the DNS server at X.X.X.X for information about host.domain.tld.
<code>dig zone MX</code>	Queries for the MX record of the specified zone.
<code>dig -x X.X.X.X</code>	Queries for the PTR record of the specified IP address.
<code>tail -f /var/log/daemon.log</code>	Displays logs pertaining to DNS in real time.
<code>tail -f /var/log/daemon.log   grep named</code>	Displays logs for named in real time.
<code>less /etc/named.conf.[i/u]</code>	Views the configuration file for Internet/unbound DNS.
<code>ls /etc/namedb.[i/u]</code>	Lists the directory containing Internet/unbound zones (.db).

## Downloads

Use these commands to download the application database, Geo-Location database, and IPS signatures.

**Table 6: Download commands**

Command	Description
<code>cf appdb download</code>	Downloads the latest application database.
<code>cf appdb version</code>	Displays the current version of the application database.
<code>cf appdb rollback</code>	Reverts to the previously downloaded application database.
<code>cf geolocation download</code>	Downloads the latest Geo-Location database.
<code>cf geolocation version</code>	Displays the current version of the Geo-Location database.
<code>cf ips download</code>	Downloads IPS signatures.
<code>cf message load</code>	Downloads the latest messages from Forcepoint.
<code>cf message version</code>	Displays the current version of the loaded messages from Forcepoint.
<code>cf message list</code>	Displays current messages from Forcepoint.

## Emergency maintenance mode (EMM)

Use these commands to enter and use emergency maintenance mode.

**Table 7: Emergency maintenance mode commands**

Command	Description
<code>shutdown now</code>	Enters emergency maintenance mode (EMM).
<code>cf policy restore_console_access</code>	Restores default Admin Console and Login Console rules when you are locked out of the firewall.

Command	Description
less /var/run/dmesg.boot	Displays the log of system messages from the kernel.
mount -a	Mounts all file systems in /etc/fstab.
fsck	Checks all file systems listed in /etc/fstab.

## File system

Use these commands to display free space and find files in the file system.

**Table 8: File system commands**

Command	Description
df -h	Displays free disk space.
du -a /   sort -nr   more	Displays files and directories sorted from largest to smallest.
find / -type f -name <i>"*name*"</i>	Finds files that include the text name in the file name.
find / -type f -name <i>"*.core*"</i>	Finds application core files.
ls /var/log/crash	Displays kernel crash files (vmcore.<n>.gz).

## Firewall self-diagnostics

Use these commands to manage the firewall self-diagnostics feature.

**Table 9: Firewall self-diagnostics commands**

Command	Description
cf monitord query	Displays the current monitord configuration.
cf monitord set hot_process_threshold= <i>percentage</i>	Sets the CPU usage threshold for processes. If the process reaches that value, it is considered a hot process.
cf monitord set hot_process_audit= <i>on/off</i>	When enabled, generates audit or send an alert when a process goes hot over the configured hot_process_audit_duration.
cf monitord set hot_process_audit_duration= <i>minutes</i>	Sets duration to wait before generating audit or sending an alert about the hot process.
cf monitord set hot_process_diagnostic= <i>on/off</i>	When enabled, restarts the hot process and generates diagnostic if the process continues to be hot over the configured hot_process_diagnostic_duration.
cf monitord set hot_process_diagnostic_duration= <i>minutes</i>	Sets duration to wait before generating diagnostics and restarting the hot process.

# General cf commands

---

Use these commands to view cf man pages and control the behavior of cf commands.

**Table 10: cf commands**

Command	Description
man cf	Displays the man page for cf.
man cf_area	Displays the man page for the specified cf area.
cf area command	Runs the specified command.
cf -i ticketID area command	Marks the changes caused by the command with the specified ticket ID.
cf area query	Displays the current configuration of the specified cf area.
cf -option area query	Modifies the output of the query command based on the specified option: <ul style="list-style-type: none"><li>• <b>d delimiter</b> — Displays the output on a single line, separating each element using the specified delimiter.</li><li>• <b>J</b> — Displays the output on a single line, which is useful for piping it to another command, such as grep.</li><li>• <b>K key1,key2</b> — Displays output for the specified keys only.</li><li>• <b>T</b> — Formats the output in a table that contains one column per key.</li></ul>

# High Availability

---

Use these commands to configure and troubleshoot High Availability.

**Table 11: High Availability commands**

Command	Description
man cf_cluster	Displays the man page for cf cluster.
cf cluster failover_status	Displays status of the failover daemon.
cf cluster status	Displays the current registration and daemon status of the cluster.
cf cluster query	Displays peer reservations and global cluster settings.
tcpdump -p	Runs tcpdump on a load-sharing High Availability cluster.

# Interfaces

---

Use these commands to configure network interfaces.

**Table 12: Network interface commands**

Command	Description
man cf_interface	Displays the man page for cf interface.
cf interface q	Displays the network interface and NIC configuration.

Command	Description
<code>cf interface modify name=<i>name</i> addresses=<i>IP1/netmask,IP2/netmask</i></code>	Modifies the IP addresses assigned to the specified interface.
<code>cf interface modify name=<i>name</i> zone=<i>zonename</i></code>	Associates the interface with the specified zone.
<code>cf interface swap hwdevice=<i>NICname1</i> swap_hwdevice=<i>NICname2</i></code>	Swaps configuration settings between two NICs, including the IP address, zones, aliases, and other configured attributes associated with the NIC.
<code>cf interface modify entrytype=<i>nic</i> name=<i>NICname</i> iftype=<i>mediatype</i></code>	Sets the media type for the NIC, such as autoselect or 1000baseTX.

## Licensing

Use these commands to view and configure the firewall license.

**Table 13: Licensing commands**

Command	Description
<code>cf license features</code>	Prints a list of the currently licensed features.
<code>cf license q</code>	Shows the current license configuration.
<code>cf license get</code>	Retrieves master key based on license configuration.
<code>cf license systemID</code>	Displays the system IDs available to be used for license activation. Only one system ID can be used to activate.
<code>cf license read file=<i>filename</i></code>	Reads the license from a file for manual activation.

## Manual pages

Use these commands to find and view manual pages.

**Table 14: Manual page commands**

Command	Description
<code>man <i>command</i></code>	Displays the man page for the specified command.
<code>man cf_<i>command</i></code>	Displays the man page for the specified cf area.
<code>man -k <i>term</i></code>	Lists all man pages that include the specified term.



**Note:** This command does not return cf commands.

# McAfee EIA

Use these commands to troubleshoot McAfee® Endpoint Intelligence Agent (McAfee EIA).



**Note:** The McAfee EIA commands are available for firewalls at version 8.3.2 and later. If you are using McAfee® Network Integrity Agent with a firewall at version 8.3.1 or earlier, see the man page for `cf_nia`.


**Table 15: McAfee EIA commands**


Command	Description
<code>cf eia set enabled=yes/no deploy_mode=static/dynamic</code>	Enables or disables the McAfee EIA feature. Deployment mode is static or dynamic.
<code>cf eia query</code>	Displays the McAfee EIA configuration.
<code>cf eia query all</code>	Displays the configuration settings and entries made on the discovery and executable lists.
<code>cf eia import executable filename=filename</code>	Allows the classification executable entries to be imported from a file.
<code>cf eia query discovery_list</code>	In dynamic deployment, displays the entries in the discovery lists.
<code>cf eia query executable_list</code>	Displays the entries in the executable classification lists.
<code>cf eia purge discovery_list</code>	Removes all entries from the host discovery lists.
<code>cf eia purge executable_list</code>	Removes all entries from the executable classification lists.
<code>cf eia flush gti_cache</code>	Removes all McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation entries from the local firewall cache.

## Networking

Use these commands to view networking information and troubleshoot networking problems.

**Table 16: Networking commands**


Command	Description
<code>netstat -in</code>	Displays statistics for network interfaces.  <b>Tip:</b> See <code>man netstat</code> for additional flags.
<code>netstat -I interface -w 5</code>	Shows live statistics for the specified network interface every five seconds.
<code>ifconfig -a</code>	Shows current network interface parameters.
<code>ifconfig bridge0 ether</code>	Shows the MAC address table for the transparent interface, if configured.
<code>cf interface q</code>	Displays the network interface and NIC configuration.
<code>ping X.X.X.X</code>	Pings the specified IP address from the firewall.
<code>arp -a</code>	Shows ARP tables.

Command	Description
	 <b>Tip:</b> To add a static ARP entry, see <code>man arp.conf</code> .
<code>arp -d hostname</code>	Clears the specified ARP entry from the firewall.

## NTP

Use these commands to configure and troubleshoot the NTP (Network Time Protocol) server.

**Table 17: NTP commands**



Command	Description
<code>cf ntp query</code>	Displays the NTP configuration.
<code>cf daemon restart agent=ntp</code>	Restarts the NTP server for the specified zone.
<code>ntpdate -bu <i>time_serverIP</i></code>	Forces immediate synchronization with the specified NTP server.
<code>tcpdump -npi <i>interface</i> udp port 123</code>	Captures NTP traffic (UDP port 123) on the specified network interface.
<code>ntpq</code>	Starts the special NTP query program.   <b>Note:</b> See <code>man ntpq</code> for details.

## Policy

Use these commands to troubleshoot policy issues.

**Table 18: Policy commands**

Command	Description
<code>man cf_policy</code>	Displays the man page for cf policy.
<code>cf policy q   less</code>	Displays the access control rules.
<code>cf appdb list</code>	Displays the applications in the application database that is currently loaded.
<code>cf application query</code>	Displays custom applications.
<code>cf appgroup query</code>	Displays application groups.
<code>cf geolocation list</code>	Displays Geo-Location countries and corresponding country codes.
<code>cf server status</code>	Displays which servers are running.
<code>cf agent query</code>	Displays the agents and their global properties.
<code>cf appfilter query</code>	Displays all Application Defenses.
<code>ipfilter -v</code>	Displays the ipfilter database currently used by the kernel.
<code>cf policy reload</code>	Reloads the ipfilter database being used by the kernel.

Command	Description
	 <b>CAUTION:</b> Active sessions will be dropped.
cf policy repair	Repairs the policy database.
cf policy restore_console_access	Restores default Admin Console and Login Console rules when you are locked out of the firewall.  <b>Tip:</b> If you are unable to log on to your firewall, run this command from emergency maintenance mode. See <i>Emergency maintenance mode (EMM)</i> .
cf policy export > <i>filename</i>	Writes the current policy configuration to a tab-delimited file that can be imported into Microsoft Excel.
cf ssl query table=rule	Displays the SSL rules.

#### Related reference


[Emergency maintenance mode \(EMM\)](#) on page 9

Use these commands to enter and use emergency maintenance mode.

## Routing

Use these commands to configure and troubleshoot static routes.




**Table 19: Routing commands**

Command	Description
route -n get <i>destination</i>	Displays the gateway used to reach the specified destination.
route -n get default	Displays the default route.
tracert -n <i>destination</i>	Displays the route packets take to reach the specified destination.  <b>Tip:</b> For IPv6 addresses, use <code>tracert6</code> .
netstat -nr	Displays the routing tables, including static routes and learned routes. Zones are identified by index.
cf route status	Displays the routing tables, including static routes and learned routes. Zones are identified by name.
cf route query	Displays the configured static routes.
cf route add route= <i>host/mask</i> gateway= <i>gateway</i>	Adds a static route.
cf route delete route= <i>host/mask</i>	Deletes the specified route.

# Security zones and groups

Use these commands to manage zones and zone groups.

**Table 20: Zone commands**

Command	Description
cf zone query	Displays zone configuration.
cf zone delete name= <i>name</i>	Deletes the specified zone.  <b>Note:</b> A zone cannot be deleted if it is referenced by any active policy.
cf zone add name= <i>name</i> modes= <i>0–63</i>	Adds a new zone.  <b>Note:</b> For information about modes, see <code>man cf_zone</code> .
region	Displays the zone indexes.
cf zone modify name= <i>name</i> newname= <i>newname</i>	Changes the name of the specified zone.
cf zonegroup query	Displays zone group configuration.
cf zonegroup delete name= <i>name</i>	Deletes the specified zone group.  <b>Note:</b> A zone group cannot be deleted if it is referenced by any active policy.
cf zonegroup add name= <i>name</i> members= <i>zone1,zone2</i>	Creates a zone group.
cf zonegroup modify name= <i>name</i> members= <i>zone1,zone2,zone3</i>	Adds zones to a zone group.

## sendmail

Use these commands to troubleshoot sendmail issues.

**Table 21: sendmail commands**

Command	Description
cf sendmail flush queue= <i>zone</i>	Flushes the mail queue for the specified zone.
cf sendmail rebuild	Rebuilds the sendmail database files.
cf daemon restart agent=sendmail	Restarts the sendmail server.
cf server status sendmail	Displays if sendmail is running and in which zones.
mailq	Displays the mail queues.
tail -f /var/log/maillog	Displays the mail log in real time.
netstat -na   grep LISTEN   grep 25	Displays listens on port 25.



Command	Description
ls /var/spool/mqueue.#	Displays directory for queued mail.
newaliases	Rebuilds the /etc/aliases file.
telnet X.X.X.X 25	Connects to a mail server IP address on port 25 to test SMTP connectivity.
pss sendmail   grep -c sendmail	Displays the number of sendmail processes running.
pss sendmail	Displays if sendmail is accepting connections.

## Shutdown

Use these commands to shut down the firewall.

**Table 22: Shutdown commands**

Command	Description
shutdown -r now	Restarts the firewall immediately.
shutdown -h now	Halts the firewall immediately.
shutdown -p now	Turns off the appliance immediately.
shutdown -s now +30	Schedules a soft shutdown on a load-sharing firewall to direct all connections to the other firewall. The firewall will shut down in 30 minutes.
shutdown now	Causes the firewall to enter emergency maintenance mode.

## Software management

Use these commands to manage software packages.



**Table 23: Software management commands**

Command	Description
man cf_package	Displays the man page for cf package.
cf package list	Displays a summary of installed and loaded software packages.
cf package load source= <i>source</i> packages= <i>package_name</i>	Downloads the specified package.
cf package install packages= <i>package_name</i>	Installs the specified package.
cf package uninstall packages= <i>package_name</i>	Uninstalls the specified package.
cf package load source=cdrom packages= <i>package_name</i>	Loads a package from a CD in the firewall optical drive.
uname -r	Displays the version and patch level.

# System

Use these commands to troubleshoot firewall system issues.


**Table 24: System commands**

Command	Description
top	Displays top CPU processes. Use these commands to view CPU statistics. <ul style="list-style-type: none"><li>• <code>top -P</code> — Displays per CPU usage statistics.</li><li>• <code>top -S</code> — Displays consolidated CPU usage statistics.</li></ul>
man netstat	Displays the man page for netstat.
netstat -na	Displays open ports.
netstat -nap tcp	Displays open TCP ports.
lsof -nPi :port#	Displays listens on the specified <i>port#</i> in a different format than netstat.
sockstat -4lp port#	Displays listens on the specified <i>port#</i> in a different format.
netstat -m	Displays memory management information.
netstat -naf inet	Displays all IPv4 sockets and connections.
netstat -naf inet6	Displays all IPv6 sockets and connections.
netstat -Ana  grep LISTEN	Outputs processes with a PCB number. <div> <b>Note:</b> Run <code>fstat   grep PCB#</code> to find the process responsible for a listen.</div>
uptime	Displays system uptime since the last restart.
vmstat	Displays virtual memory statistics.
connect_mon	Displays the number of current connections by service.
pss   more	Displays all running processes.
pss process_name	Finds a specific process and its process ID.
dmesg	Displays system and hardware information from the system buffer.
kill -HUP pid#	Restarts a process without changing the process ID.
kill pid#	Terminates the process with specified process ID.
kill -9 pid#	Forces a termination of the process with the specified process ID.
setconsole device	Selects the primary console device. The available devices are video, serial, both, or default (which is both).
cf hostname set name=newhostname	Changes the firewall host name. <div> <b>Note:</b> If you change the host name, additional configuration changes are also required. For detailed instructions, see Knowledge Base article <a href="#">8888</a>.</div>

# tcpdump

Use these commands to capture network traffic.


**Table 25: tcpdump commands**

Command	Description
man tcpdump	Displays the man page for tcpdump.  <b>Tip:</b> See also <a href="http://www.tcpdump.org">http://www.tcpdump.org</a> .
tcpdump -npi <i>em0</i> host X.X.X.X	Displays packets on the specified interface sent to or received from the specified host.
tcpdump -npi <i>em0</i> -Xs 1500 port <i>y</i>	Displays up to 1,500 bytes of packet headers (except link level) and packet data for the specified port on the specified interface.
tcpdump -npi <i>em0</i> -w <i>filename</i>	Writes a raw packet dump to <i>filename</i> in the current working directory.
tcpdump -npi <i>em0</i> -w <i>filename</i> -s 0	Captures all bytes and writes a raw packet dump to <i>filename</i> in the current working directory.
tcpdump -p	Runs tcpdump in non-promiscuous mode.

## Technical support

These commands might be useful when you contact technical support.

**Table 26: Technical support commands**

Command	Description
ktrace -p <i>pid#</i>	Starts a trace of the process with the specified process ID.
ktrace -c <i>pid#</i>	Stops a process trace.
kill -6 <i>pid#</i>	Terminates a process and dumps a core file of the process.
sysctl -w kern.corefile='%N.core.%P'	Configures the firewall to include the process ID in the file name of core files. Allows multiple core files to coexist without overwriting each other.  <b>Note:</b> Use <code>sysctl -w kern.corefile='%N.core'</code> to return to the previous operating mode.

# Text editors and viewers

Use these commands to view and edit text files.

**Table 27: Text editor and viewer commands**

Command	Description
<code>vi filename</code>	Edits the specified file with vi.
<code>emacs filename</code>	Edits the specified file with emacs.
<code>less filename</code>	Views the contents of the specified text file.
<code>view filename</code>	Views the contents of the specified text file with a read-only version of vi.
<code>cat filename</code>	Creates or displays the specified file.
<code>edit filename</code>	Edits the specified file with edit.

## Type Enforcement

Use these commands to view and modify Type Enforcement.


**Table 28: Type Enforcement commands**

Command	Description
<code>ll (lowercase L)</code>	Displays Type Enforcement for the files in the current directory.
<code>ps -axZ</code>	Displays TE domain information.
<code>chtype creator.type filename</code>	Changes the Type Enforcement for a file.

## VPN

Use these commands to view and troubleshoot VPNs.

**Table 29: VPN commands**



Command	Description
<code>cf ipsec q</code>	Displays all configured VPNs.
<code>cf ipsec policydump</code>	Displays active VPNs.
<code>cf ipsec reload [flush=1]</code>	Flushes all existing keys and policy, then reloads the VPNs.  <b>Note:</b> This command closes all open VPN connections.
<code>cf pool q</code>	Displays client address pools.
<code>showaudit -vk</code>	Displays audits pertaining to VPNs in real time.
<code>netstat -na   grep 500</code>	Displays listens for port 500 (ISAKMP) connections.





Command	Description
<code>tcpdump -npi em0 udp port 500 or proto 50 or proto 51</code>	Displays ISAKMP, ESP (IP Proto 50), or AH (IP Proto 51) traffic on network interface em0.
<code>tcpdump -npi em0 udp port 4500</code>	Displays NAT-T traffic on network interface em0.


# Available cf areas

The following table lists the cf areas, showing the primary commands available for each area.

**Table 30: Available cf areas**

cf area	Area description
accelerator	Manages cryptographic acceleration devices.
acl	Manages the access control list (ACL) daemon.
adminuser	Manages administrator accounts.
agent	Configures global agent attributes for proxies, servers, and filters.
antivirus	Manages the anti-virus engine and the virus scanning service.
appdb	Manages the application database.
appfilter	Manages individual Application Defenses and Application Defense groups.
appgroup	Manages application groups.
application	Manages custom applications.
audit	Configures auditing, including auditbot (response), email, filter options, and network defenses.
auth	Manages authenticators.
catgroups	Manages IPS signature groups.
cert	Manages certificates, private keys, and certificate identities.
cluster	Displays the current status and connection state of a High Availability cluster and registers a secondary/standby to a High Availability cluster primary.
cmd	Configures global settings for the certificate management server on the firewall.
commandcenter	Manages registration with a Forcepoint Sidewinder Control Center Management Server.
config	Creates and restores configuration backups.
crontab	Configures the status (enabled/disabled) and frequency of the available cron jobs.  <b>Note:</b> For information on default cron jobs, see Knowledge Base article <a href="#">9226</a> .
daemond	Configures daemond and stops or restarts agents.  <b>Note:</b> Disabled agents remain stopped until the next policy apply. A policy apply occurs every time a change to rules, rule elements, or the system clock is saved.
dhcrelay	Manages the DHCP Relay agent, which forwards DHCP and BOOTP requests from one subnet to another.
dns	Manages firewall DNS settings.
domain	Manages domain network objects.
eia	Manages McAfee EIA. This area is available for firewalls at version 8.3.2 and later.

cf area	Area description
	 <b>Note:</b> For firewalls at version 8.3.0 or 8.3.1, use the <i>nla</i> cf command.
epo	Manages McAfee® ePolicy Orchestrator® settings.
export	Manages the audit export utility.
externalgroup	Manages external authentication groups.
fips	Enables and disables FIPS 140-2 compliance mode, and examines the default_SSL_cert to verify FIPS 140-2 compliance.
geolocation	Manages Geo-Location network objects and general Geo-Location settings.
host	Manages host network objects.
hostname	Manages the firewall host name.  <b>Note:</b> If you change the host name, additional configuration changes are also required. For detailed instructions, see Knowledge Base article <a href="#">8888</a> .
ids	Manages the shunning service. Available settings include IDS entries that specify an IP address of an IDS (Intrusion Detection Server), a shared password, and a timeout value that identifies the amount of seconds to shun an IP address.
interface	Manages network interfaces.
ipaddr	Manages IP address network objects.
iprange	Manages IP address range network objects.
ips	Manages IPS signatures.  <b>Note:</b> This is different from IPS Attack Responses, which are controlled using cf audit.
ipsec	Manages VPN definitions.
ipsresponse	Manages how the firewall responds if its signature-based IPS inspection detects an intrusion.
ipssig	Enables or disables individual IPS signatures.
knownhosts	Manages the SSH known hosts database.
lca	Manages the local (firewall-hosted) certificate authority. This feature is not widely used.
license	Manages the firewall license.
message	Displays and manages settings for messages from Forcepoint.
monitord	Manages settings for identifying and acting on CPU-intensive processes.
netgroup	Manages network object groups (netgroups).
netmap	Manages netmap network objects.
nla	Manages McAfee® Network Integrity Agent settings. This area is available for firewall version 8.3.0 or 8.3.1.  <b>Note:</b> For firewalls at version 8.3.2 and later, use the <i>eia</i> cf command.

cf area	Area description
ntp	Manages the NTP (Network Time Protocol) server.
package	Manages software packages. <div>  <b>Note:</b> Avoid using autorun and autoload, as they require specific parameters to run. Use install, uninstall, and rollback instead.         </div>
passport	Manages the Passport authenticator.
policy	Manages rules and rule groups, and exports rule elements.
pool	Manages client address pools used for dynamic client addressing in IPsec VPN definitions.
qos	Manages Quality of Service (QoS) policy.
reports	Manages audit reports.
route	Manages static network routes.
sendmail	Provides limited utilities for sendmail, including rebuilding database files and flushing queues.
server	Displays server state information.
snmp	Manages Simple Network Management Protocol (SNMP) settings.
smartfilter	Manages SmartFilter web filtering settings.
ssl	Manages SSL rules and assigns SSL certificates for firewall administrative sessions (for example, Admin Console connections).
subnet	Manages subnet network objects.
timeperiod	Manages time period objects.
timezone	Configures the time zone.
trustedsource	Manages McAfee® Global Threat Intelligence™ (McAfee GTI) settings.
udb	Manages the authentication user database.
ups	Manages uninterruptible power supply (UPS) settings.
urltranslation	Manages URL translation rules.
usage	Displays usage reports.
usergroup	Manages user groups that are stored in the user database.
utt	Manages the UDP to TCP tunnel configuration.
zone	Manages security zones.
zonegroup	Manages security zone groups.