

Athena FirePAC Data Collection Guide

This document describes the various procedures used to acquire the configuration file and log file data for the firewall devices supported by Athena FirePAC. It is convenient to store the configuration/log files for each device in a separate directory and group them under one parent directory.

Configuration File Collection Procedures

The following table describes the steps required to obtain the configuration files for each type of firewall. Two or three configuration files will be collected for each device.

Device Type	Data Collection Procedure
Cisco PIX 6 Cisco PIX 7 Cisco ASA firewall	<ol style="list-style-type: none"> 1. Connect to the PIX device using SSH or telnet. 2. Enter the command "enable" and provide the enable password. 3. Enter the command "no pager". (For ASA and Pix version 7.0(1) and above, use – "terminal pager 0" instead of "no pager" command.) 4. Enter the command "show run" and capture the output to a file called "config.txt". 5. Enter the command "show route" and capture the output to a file called "route.txt".
Cisco IOS	<ol style="list-style-type: none"> 1. Connect to the IOS device using SSH or telnet. 2. Enter the command "enable" and provide the enable password. 3. Enter the command "terminal length 0". 4. Enter the command "show run" and capture the output to a file called "config.txt". 5. Enter the command "terminal ip netmask-format bit-count". 6. Enter the command "show ip route" and capture the output to a file called "route.txt". 7. Enter the command "show ip route vrf <vrfName>" and capture the output to a file called vrf-routes.txt

Athena FirePAC Data Collection Guide

CiscoPIX/ASA- SecurityContext For Device Administrator	<ol style="list-style-type: none">1. Connect to PIX device using ssh or telnet.2. Enter the command "enable" and provide the enable password.3. Enter the command "changeto context <context-name>".4. Enter the command "terminal pager 0".5. Enter the command "show run" and capture the config to a file called "config.txt".6. Enter the command "show route" and capture the output to a file called "route.txt".7. Using "changeto context <context-name>" command, change to a context with administrator privileges before executing the following command.8. Enter the command "changeto system".9. Enter the command "show run" and capture the config to a file called "system.txt".
CiscoPIX/ASA- SecurityContext For Context Administrator	<p>(A context-administrator does not have access to system space and admin-contexts. Accessibility is limited to the context assigned for administration.)</p> <ol style="list-style-type: none">1. Connect to the security-context on PIX or ASA device using ssh or telnet.2. Enter the command "enable" and provide the enable password.3. Enter the command "terminal pager 0".4. Enter the command "show run" and capture the config to a file called "config.txt".5. Enter the command "show route" and capture the output to a file called "route.txt".
Cisco FWSM Supervisor running IOS	<ol style="list-style-type: none">1. Connect to the supervisor modules of the switch using ssh or telnet.2. Enter the command "enable" and provide the enable password.3. Enter the command "session slot <number> processor <processor-number>". If the module-number is unknown, then find it from the output of "show modules" supervisor command. Processor-number is 1 in most cases but can range from 0 to 9.4. Enter password to start the FWSM session.5. Enter the command "enable" and provide the enable password.6. Disable command output paging. FWSM version below 3.1(1) - Enter "no pager" FWSM version 3.1(1) and above - Enter "terminal pager 0"7. Enter the command "show run" and capture the config to a file called "config.txt".8. Enter the command "show route" and capture the output to a file called "route.txt".

<p>Cisco FWSM Supervisor running CatOS</p>	<ol style="list-style-type: none"> 1. Connect to the supervisor module of the switch using ssh or telnet. 2. Enter the command "enable" and provide the enable password. 3. Enter the command "session <module-number>" where the module-number is the slot number of the fws module. If the module-number is unknown, then find it from the output of "show modules" supervisor command. 4. Enter password to start the FWSM session. 5. Enter the command "enable" and provide the enable password. 6. Disable command output paging. FWSM version below 3.1(1) - Enter "no pager" FWSM version 3.1(1) and above - Enter "terminal pager 0" 7. Enter the command "show run" and capture the config to a file called "config.txt". 8. Enter the command "show route" and capture the output to a file called "route.txt".
<p>Juniper Netscreen firewall</p>	<ol style="list-style-type: none"> 1. Connect to the Netscreen device using SSH or telnet. 2. Enter the command "set console page 0". 3. Enter the command "get config" and capture the output to a file called "config.txt". 4. Enter the command "get route" and capture the output to a file called "route.txt". 5. Enter the command "get service" and capture the output to a file called "service.txt".
<p>Netscreen Virtual system</p>	<ol style="list-style-type: none"> 1. Connect to the Netscreen virtual system using SSH, Telnet, or HyperTerminal sessions command-line prompt and provide the Untrust zone interface IP address as the destination IP address for the specific virtual system. Provide the admin user name and password for that virtual system and logon to the virtual system. 2. Enter the command "set console page 0". 3. Enter the command "get config" and capture the output to a file called "config.txt". 4. Enter the command "get route" and capture the output to a file called "route.txt". 5. Enter the command "get service" and capture the output to a file called "services.txt".

Check Point™
FireWall-1®

Obtaining Object and Rulebase Configuration Files:

1. Determine the name of the Check Point™ firewall and the name of the policy package applied to it.
2. Connect to the Check Point SmartCenter™ management server box using ssh or telnet. Please note this is not the Smart Dashboard client GUI used for connecting to the management server, it is the actual management server where the objects and policy packages exist.
3. Find the directory on the management server box where the Check Point™ management server software is installed. This may be defined by the "\$FWDIR" environment variable.
4. Copy the file "\$FWDIR/conf/objects_5_0.c" to your local system.
Please note there is a similarly named file called "objects.C" in the same directory, which is not the correct file.
5. Copy the file "\$FWDIR/conf/rulebases_5_0.fws" to your local file system.

Obtaining the Routing Table:

Execute the "cpstat" command on the management console as follows:

```
cpstat os -f routing -h a.b.c.d > route.txt
```

Where "a.b.c.d" is the IP address of the firewall module.

On a Provider-1 system, the cpstat command should be executed from the CMA ((Customer Management Add-on) that manages the firewall.

If this command is not available for any reason, then the procedure for obtaining the routing table depends on the platform that is running the Check Point™ FireWall-1® software.

In such a case, connect to the device using SSH or telnet. And depending on the type of platform, you must capture the output of the command indicated below and save it to a file called "route.txt".

Platform	Command
SecurePlatform	netstat -rn
Check Point IPSO Appliance	show route
Nokia IPSO	netstat -rn
Linux	netstat -rn
Solaris	netstat -r -v -n
Crossbeam UTM	netstat -rn

Log Collection Procedures

The log file formats supported by the log analysis are plain text (with extensions like .txt or .log), zip files (.zip), tar files (.tar files), gzip files (.gz or .tar.gz). Any other extensions are considered as plain text log files. Files without any extension are also considered as plain text log files.

WinZip utility cannot compress large files or archives correctly (>4 GB). So use gzip to compress large firewall log files when doing log analysis.

If .gz format is used and if there are several input log files, concatenate the log files in to a single log file before compressing it. Do not create a .gz file that is a sequence of independently compressed members. So if there are 3 log files say "log1.txt", "log2.txt" and "log3.txt", the gzip command line would be "cat log1.txt log2.txt log3.txt | gzip > log_combined.gz". The "log_combined.gz" file would then be the input log file for FirePAC.

The following sections describe the steps required to obtain the log files for each type of firewall.

Check Point™

Multiple mechanisms are supported for obtaining logs from Check Point™ firewalls. Any one of the following may be used, the first method for smaller log data files and the second method for large log data files. If there are multiple log files, you can archive them into a single zip file and specify the zip file as input. FirePAC can automatically read each file from the archive and process all of them. Before using any of the mechanisms below, make sure that "rulebase_uids_in_log" option is enabled under Policy -> Global Properties -> SmartDashboard Customization -> Configure -> Firewall-1 -> General.

1. **Export using SmartView Tracker™:** If the individual firewall module logs are sent to the SmartCenter™ server, then use the SmartView Tracker™ to connect to the SmartCenter™ server. If the firewall module logs are sent to the Log Server, then use the SmartView Tracker™ to connect to the Log Server. Please make sure that the column "Rule UID" is included in the list of columns for export. The Rule UID can be selected from the properties shown when "Query properties" option is enabled (using View->Query Properties). Click "Query" on the top menu, then uncheck "Resolve IP". Export the log using "File->Export" option in the SmartView Tracker. Multiple log files can be combined into an archive and specified as input.
2. **Export using fwm:** Depending on where the individual firewall module logs are sent, this command should be executed either on the SmartCenter™ server or the Log Server. Use a logexport.ini with contents as indicated below and place it in the conf directory (\$FWDIR/conf) on the SmartCenter server or the log server. Use the following command to export the log file.

```
fwm logexport -i <inputfilename> -o <outputfilename> -n
```

Option <Parameter>	Description
-i <inputfilename>	The <inputfilename> file should exist in \$FWDIR/log directory. This is the Check Point raw log data file. There may be more than one log file in this directory.

	The file fw.log is the current log file; other files may be of the form <Date_Time>.log or name given by the user. The log file size is limited to 2GB and every time a log file exceeds this size, it creates a separate log file with name as <Date_Time>.log and resets logging in fw.log file. The files can also be created manually by executing "fw logswitch" on the console. The default file fw.log shall be used when this option is omitted.
-o <outputfilename>	This is the log file in an ASCII format created from the Check Point raw log data files that is more suitable for analysis. This file name should be different than the <inputfilename> and shall be created in the current directory. This is mandatory parameter. You can append .ascii suffix to the input file name. If there are multiple raw log data files, you need to export each of them into an ASCII format, archive all the ASCII log files into a single zip file, transfer it to the Athena FirePAC box and use it as an input. You do not need to extracting them again, FirePAC will automatically read each ASCII log file in the archive and process them one by one.
-n	Disable the name resolution for the IP addresses in the log data. This option is a must when performing usage analysis using FirePAC.

A sample logexport.ini is available with the Firepac installation distribution. The logexport.ini file content:

```
[Fields_Info]
included_fields=num, date, time, orig, type, action, alert,
i/f_name, i/f_dir, proto, src, dst, service, s_port, len,
rule, rule_uid, icmp-type, icmp-code, h_len, ip_vers,
sys_msgs
```

If the firewall module logs are only locally available within each firewall, then the log files need to be imported in to the SmartView Tracker™ using the "Tools -> Remote Files Management" option and then exported using the "File -> Export" option.

By default logs are sent to the SmartCenter server. If the user has installed a separate log server (Note: Log server is a separate installation from the smart centre server), this log server can be specified as an option for a gateway's logs to be collected.

In the smart dashboard, double click on a checkpoint gateway, under the "Log and master" option, add the log server for the log server option.

Multiple log files can be combined into an archive and specified as input.

Using Check Point LEA (Log Export Api) or any other mechanism: If the Check Point logs are collected using a tool that uses LEA (Log Export Api), which is one part of Check Point™ OPSEC API or any other mechanism, configure the tool so that the logs are in the form of a header line followed by value lines. The field names should be present only in the header line of the log file separated by a separator. All the following lines should contain only the field values separated by a separator. The tool using Log Export API should disable resolving IP addresses to names. The fields exported should include date, time, orig (Name or the IP address of the firewall), rule (rule number). The separator should be either a ";" or a "|" symbol and the same separator that is present in the header line should be used throughout for the field values. An example would be:

```
date | time | orig | src | dst | rule
3Apr2009 | 11:52:35 | Checkpoint-1 | 1.2.3.4 | 4.3.2.1 | 1
4Apr2009 | 12:52:35 | 192.168.1.5 | 1.2.3.4 | 4.3.2.1 | 1
```

Once the logs files are exported, they have to be transferred manually to the system on which FirePAC is running.

Juniper Netscreen

Connect to the Juniper Netscreen firewall using the web GUI. Make sure that the Juniper Netscreen firewall is configured with a valid host name. The "Device Information" section in the Home page shows the "Host Name". If this is empty, use the CLI command "set hostname <name>" to set a valid host name. For FirePAC to process a log file, the "device_id" field should match the host name in the configuration or the "Device IP Address" field should contain the host name specified in the configuration. Examples:

```
May 18 15:59:26 192.168.1.3 ns204: NetScreen device_id=firepac_example
system notification-0025 start_time="2001-04-29 16:46:16" duration=88 policy
id=2 service=icmp proto=1 src zone=Trust dstzone=Untrust action=Tunnel(VPN_3
03) sent=102 rcvd=0 src=192.168.10.10 dst=2.2.2.1 icmp type=8 src_port=1991
dst_port=80 src-xlated ip=192.168.10.10 port=1991 dst-xlated ip=1.1.1.1
port=200
```

```
May 18 15:59:26 firepac_example.test.com ns204: NetScreen device_id=205555
system notification-0025 start_time="2001-04-29 16:46:16" duration=88 policy
id=2 service=icmp proto=1 src zone=Trust dstzone=Untrust action=Tunnel(VPN_3
03) sent=102 rcvd=0 src=192.168.10.10 dst=2.2.2.1 icmp type=8 src_port=1991
dst_port=80 src-xlated ip=192.168.10.10 port=1991 dst-xlated ip=1.1.1.1
port=200
```

In the above examples, the configuration file for the device should have the following statement:

```
set hostname firepac_example
```

Make sure syslog is enabled via the following steps:

- Click on "Configuration->Report Settings" in the GUI
- Select the "syslog" tab

Athena FirePAC Data Collection Guide

- Set the IP address of the system where the syslog service is running
- Set the "Traffic Log" option
- If you have changed the syslog listener port, adjust it, too
- Apply these changes.
- Connect to the system where the syslog service is running. Look at the syslog configuration to see the location where the log files are saved. Change directory to this location and save the log file to a location that can be accessed from the Athena FirePAC.
- Multiple log files can be combined into an archive and specified as input.

Cisco Pix, ASA and FWSM

- Connect to the PIX device using SSH or telnet.
- Enter the command "enable" and provide the enable password.
- Disable command output paging. Command is one of the following.
 - Pix versions below 7.0(1) - Enter "no pager".
 - ASA and Pix versions 7.0(1) and above – Enter "terminal pager 0".
 - FWSM versions below 3.1(1) - Enter "no pager".
 - FWSM versions 3.1(1) and above – Enter "terminal pager 0".
- Then execute the "show access-list" command and capture the output to a file, called "access-list-output.txt".
- Save this file "access-list-output.txt" to a location that can be accessed from Athena FirePAC.

Cisco IOS

- Connect to the IOS device using SSH or telnet.
- Enter the command "enable" and provide the enable password.
- Disable command output paging using "terminal length 0" command.
- Then execute the "show access-list" command and capture the output to a file, called "access-list-output.txt".
- Save this file "access-list-output.txt" to a location that can be accessed from Athena FirePAC.