

## Athena FirePAC Data Collection Guide

The following table lists the firewall devices supported by Athena FirePAC and describes the steps required to obtain the configuration data for each type of firewall. Two or three configuration files will be collected for each device. It is convenient to store the configuration files for each device in a separate directory and group them under one parent directory.

| Device Type                                         | Data Collection Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco PIX 6<br>Cisco PIX 7<br>Cisco ASA<br>firewall | <ol style="list-style-type: none"> <li>1. Connect to the PIX device using SSH or telnet.</li> <li>2. Enter the command "enable" and provide the enable password.</li> <li>3. Enter the command "no pager".</li> <li>4. Enter the command "show config" and capture the output to a file called "config.txt".</li> <li>5. Enter the command "show route" and capture the output to a file called "route.txt".</li> </ol>                                                                                                                                                                                                                                                                                         |
| CiscoPIX/ASA-SecurityContext                        | ( Device-administrator can access the admin-context, the system space and all other security-contexts on the device. )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| For Device Administrator.                           | <ol style="list-style-type: none"> <li>1. Connect to the admin-context of the PIX or ASA device using ssh or telnet.</li> <li>2. Enter the command "enable" and provide the enable password.</li> <li>3. Enter the command "changeto system".</li> <li>4. Enter the command "show config" and capture the output to a file called "system.txt"</li> <li>5. Change to the context to be analyzed – Enter the command "changeto context &lt;context-name&gt;"</li> <li>6. Enter the command "no pager"</li> <li>7. Enter the command "show config" and capture the output to a file called "config.txt"</li> <li>8. Enter the command "show route" and capture the output to a file called "route.txt"</li> </ol> |
| CiscoPIX/ASA-SecurityContext                        | ( A context-administrator does not have access to system space and admin-contexts. Accessibility is limited to the context assigned for administration. )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| For Context Administrator                           | <ol style="list-style-type: none"> <li>1. Connect to the security-context on PIX or ASA device using ssh or telnet</li> <li>2. Enter the command "enable" and provide the enable password.</li> <li>3. Enter the command "no pager"</li> <li>4. Enter the command "show config" and capture the output to a file called "config.txt"</li> <li>5. Enter the command "show route" and capture the output to a file called "route.txt"</li> </ol>                                                                                                                                                                                                                                                                  |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco FWSM<br>Supervisor<br>running IOS   | <ol style="list-style-type: none"><li>1. Connect to the supervisor modules of the switch using ssh or telnet.</li><li>2. Enter the command "enable" and provide the enable password</li><li>3. Enter the command "session slot &lt;number&gt; processor &lt;processor-number&gt;". 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.</li><li>4. Enter password to start the FWSM session.</li><li>5. Enter the command "enable" and provide the enable password</li><li>6. Enter the command "show config" and capture the output to a file called "config.txt"</li><li>7. Enter the command "show route" and capture the output to a file called "route.txt"</li></ol> |
| Cisco FWSM<br>Supervisor<br>running CatOS | <ol style="list-style-type: none"><li>1. Connect to the supervisor module of the switch using ssh or telnet.</li><li>2. Enter the command "enable" and provide the enable password</li><li>3. Enter the command "session &lt;module-number&gt;" 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.</li><li>4. Enter password to start the FWSM session.</li><li>5. Enter the command "enable" and provide the enable password</li><li>6. Enter the command "show config" and capture the output to a file called "config.txt"</li><li>7. Enter the command "show route" and capture the output to a file called "route.txt"</li></ol>                                     |
| Juniper<br>Netscreen<br>firewall          | <ol style="list-style-type: none"><li>1. Connect to the Netscreen device using SSH or telnet.</li><li>2. Enter the command "set console page 0".</li><li>3. Enter the command "get config" and capture the output to a file called "config.txt".</li><li>4. Enter the command "get route" and capture the output to a file called "route.txt".</li><li>5. Enter the command "get service" and capture the output to a file called "services.txt".</li></ol>                                                                                                                                                                                                                                                                                                                              |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Platform<br>Checkpoint<br>firewall | <ol style="list-style-type: none"> <li>1. Determine the name of the Secure Platform firewall and the name of the policy package applied to it.</li> <li>2. Connect to the Checkpoint management console.</li> <li>3. Find the directory on the management console host where the Checkpoint management console software is installed. This may be defined by the "\$FWDIR" environment variable.</li> <li>4. Copy the file "\$FWDIR/conf/Objects_5_0.C".</li> <li>5. Copy the file "\$FWDIR/conf/rulebases_5_0.fws".</li> <li>6. Connect to the Secure Platform device using SSH or telnet.</li> <li>7. Enter the command "netstat -rn" and capture the output to a file called "route.txt".</li> </ol> |
| Nokia IPSO<br>Checkpoint<br>firewall      | <ol style="list-style-type: none"> <li>1. Determine the name of the Nokia IPSO firewall and the name of the policy package applied to it.</li> <li>2. Connect to the Checkpoint management console.</li> <li>3. Find the directory on the management console host where the Checkpoint management console software is installed. This may be defined by the "\$FWDIR" environment variable.</li> <li>4. Copy the file "\$FWDIR/conf/Objects_5_0.C".</li> <li>5. Copy the file "\$FWDIR/conf/rulebases_5_0.fws".</li> <li>6. Connect to the Nokia IPSO device using SSH or telnet.</li> <li>7. Enter the command "netstat -rn" and capture the output to a file called "route.txt".</li> </ol>           |
| Crossbeam<br>Checkpoint<br>firewall       | <ol style="list-style-type: none"> <li>1. Determine the name of the Crossbeam firewall and the name of the policy package applied to it.</li> <li>2. Connect to the Checkpoint management console.</li> <li>3. Find the directory on the management console host where the Checkpoint management console software is installed. This may be defined by the "\$FWDIR" environment variable.</li> <li>4. Copy the file "\$FWDIR/conf/Objects_5_0.C".</li> <li>5. Copy the file "\$FWDIR/conf/rulebases_5_0.fws".</li> <li>6. Connect to the Crossbeam device using SSH or telnet.</li> <li>7. Enter the command "netstat -rn" and capture the output to a file called "route.txt".</li> </ol>             |
| Solaris<br>Checkpoint<br>firewall         | <ol style="list-style-type: none"> <li>1. Determine the name of the Solaris firewall and the name of the policy package applied to it.</li> <li>2. Connect to the Checkpoint management console.</li> <li>3. Find the directory on the management console host where the Checkpoint management console software is installed. This may be defined by the "\$FWDIR" environment variable.</li> <li>4. Copy the file "\$FWDIR/conf/Objects_5_0.C".</li> <li>5. Copy the file "\$FWDIR/conf/rulebases_5_0.fws".</li> <li>6. Connect to the Solaris Checkpoint device using SSH or telnet.</li> <li>7. Enter the command "netstat -r -v -n" and capture the output to a file called "route.txt".</li> </ol> |

Linux  
Checkpoint  
firewall

1. Determine the name of the Linux firewall and the name of the policy package applied to it. Connect to the Checkpoint management console.
2. Find the directory on the management console host where the Checkpoint management console software is installed. This may be defined by the "\$FWDIR" environment variable.
3. Copy the file "\$FWDIR/conf/Objects\_5\_0.C".
4. Copy the file "\$FWDIR/conf/rulebases\_5\_0.fws".
5. Connect to the Linux Checkpoint device using SSH or telnet.
6. Enter the command "netstat -rn" and capture the output to a file called "route.txt".