

Design

- Network Ports used for communication
- Log Files location Check Point

Network Ports used for communication

Introduction

This drawing should give you an overview of the used R80 and R77 ports respectively communication flows. It should give you an overview of how different Check Point modules communicate with each other. Furthermore, services that are used for firewall operation are also considered. These firewall services are also partially mapped as implied rules in the set on the firewall.

Link

Thank you Heiko Ankenbrand for creating such a valuable overview:

<https://www.ankenbrand24.de/index.php/articles/check-point-articel/arcitecture/r80-communication-ports/>

Overview

<http://www.ankenbrand24.de/wp-content/uploads/2019/03/ports.png>

Download

https://www.ankenbrand24.de/wp-content/uploads/2019/12/Ports_1.5a.pdf

Log Files location Check Point

Here are the different Log File locations on a Check Point Appliance:

| Feature | File Location |
|---|--|
| Alerts | <code>/var/log/send_alert.*</code> |
| Command auditing | <code>/var/log/asgaudit.log*</code> |
| CPD | <code>\$CPDIR/log/cpd.elg</code> |
| Distribution | <code>/var/log/dist_mode.log*</code> |
| Dynamic Routing | <code>/var/log/routed.log</code> |
| Expert mode shell auditing | <code>/var/log/command_logger.log*</code> |
| FWD | <code>\$FWDIR/log/fwd.elg</code> |
| FWK | <code>\$FWDIR/log/fwk.elg.*</code> |
| <u>Gaia</u> Cli shClosed auditing | <code>/var/log/auditlog*</code> |
| <u>Gaia</u> Cli sh First Time Configuration Wizard | <code>/var/log/ftw_install.log</code> |
| General | <code>/var/log/messages*</code> |
| <u>SMO</u> Cli sh Image Cloning | <code>/var/log/image_clone.log.dbg*</code> |
| Installation | <code>/var/log/start_mbs.log</code> |
| Installation - OS | <code>/var/log/anaconda.log</code> |
| Log Servers | <code>/var/log/log_servers*</code> |
| Policy | <code>\$FWDIR/log/cpha_policy.log.*</code> |
| Reboot logs | <code>/var/log/reboot.log</code> |
| SGM Configuration Pull Configuration | <code>\$FWDIR/log/blade_config.*</code> |
| VPND | <code>\$FWDIR/log/vpnd.elg*</code> |