**Software update:**

| **show system info**  **request system software check**  **request system software download version 10.1.4t**  **request system software install version 10.1.4**  **request anti-virus upgrade download latest**  **request anti-virus upgrade install version latest**  **request wildfire upgrade download latest**  **request wildfire upgrade install version latest**  **request restart system** |
| --- |

Passwords and users:

| edit mgt-config  show users  delete users <|non-admin-user|>  set users admin password  set users <user> permissions role-based superuser yes  set users <user> password |
| --- |

Setup L2 interfaces

| set network interface ethernet ethernet1/**#** layer2 lldp enable no |
| --- |

Zones:

| set zone WAN network layer2 ethernet1/1  set zone DMZ network layer2 [ ethernet1/2 ethernet1/3 ethernet1/4 ]  set zone LAN network layer2 ethernet1/9 |
| --- |

Make av profile group:

| edit profiles  # virus  set virus Max decoder ftp action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder http action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder http2 action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder imap action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder pop3 action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder smb action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max decoder smtp action reset-both mlav-action reset-both wildfire-action reset-both  set virus Max mlav-engine-filebased-enabled "Executable Linked Format" mlav-policy-action enable  set virus Max mlav-engine-filebased-enabled "PowerShell Script 1" mlav-policy-action enable  set virus Max mlav-engine-filebased-enabled "PowerShell Script 2" mlav-policy-action enable  set virus Max mlav-engine-filebased-enabled "Windows Executables" mlav-policy-action enable  set virus Max mlav-engine-filebased-enabled "MSOffice" mlav-policy-action enable  # pii  set data-objects pii pattern-type predefined pattern credit-card-numbers file-type any  set data-objects pii pattern-type predefined pattern social-security-numbers file-type any  set data-objects pii pattern-type predefined pattern social-security-numbers-without-dash file-type any  set data-filtering PII data-capture yes rules R1 alert-threshold 0 block-threshold 0 data-object pii direction both log-severity high application any file-type any  top  set profile-group Main virus Max spyware strict vulnerability strict data-filtering PII url-filtering default file-blocking "strict file blocking" wildfire-analysis default |
| --- |

Add system address definition

| set address "System name" ip-netmask 10.10.10.10 |
| --- |

Add av rule

| edit rulebase security  set rules "Rule Name"  from any source any  to DMZ destination "System name"  application [ ssh web-browsing ssl] service application-default  action allow  profile-setting group <group> |
| --- |

Change AV policy for default rule

| edit rulebase default-security-rules  set rules interzone-default action drop log-end yes  set rules intrazone-default action allow log-end yes profile-setting group Main |
| --- |

Fun extras:

| show admins | Show who is logged in |
| --- | --- |
| set cli config-output-format set | Nice output format |
| set deviceconfig system device-telemetry device-health-performance no product-usage no threat-prevention no | Disable telemetry |

Backup config:

| save config to backup.xml  load config from backup.xml  load config last-saved |
| --- |